

Velosio®



The Business Leader's Guide to Ransomware

With cyber attacks on the rise, C-suite leaders must join forces with IT to transform their ransomware strategies. This guide will help you understand what you're up against, so you can protect your company for years to come.



Contents

Introduction	3
Foreword	4
1. What, Exactly, is Ransomware?	6
2. How Does Ransomware Work?	11
3. Ransomware Trends: Facts, Stats, & Emerging Threats	16
4. Six High-Profile Attacks and Lessons Learned	21
5. Ransomware Protection Best Practices	28
6. Is Cloud Storage Safe from Ransomware?	35
7. How the Microsoft Ecosystem Safeguards Your Data from Ransomware	40
8. Protecting On-Premises Microsoft Dynamics from Ransomware	65
9. Guidance for Selecting Anti-Ransomware Tools	73
10. Practical Approaches for Detecting Ransomware	80
11. Recovering from a Ransomware Attack	87
12. Elements of a World-Class Ransomware Strategy	94
13. Future-Proofing Your Business Against Ransomware	98



Introduction

While the threat of ransomware is nothing new, it has changed into something far more sinister (and costly).

Threat actors have abandoned low-stakes spray-and-pray tactics to track down bigger targets with deeper pockets and more skin in the game.

They're using AI and machine learning to wage targeted attacks on supply chains, public utilities, and orgs with digital assets they'd pay anything to protect,

Aspiring threat actors face few barriers when it comes to entering the "industry." Ransomware-as-a-service, or RaaS, has made cybercrime accessible to the masses.

Anyone can launch an attack by purchasing affordable, pre-built components or, by hiring "freelancers" for one-off gigs, Upwork style.

All of those modernization efforts paid off in spades. Per Microsoft, ransomware is now the most lucrative game in cyber crime.

Global cybercrime costs are expected to hit an annual rate of \$10.5 trillion by 2025 – based on the current growth rate – ~15% per year. To put those numbers in perspective, the ransomware economy is responsible for driving the largest transfer of economic wealth in history.

Of course, any big win for ransomware represents a crushing blow to the victim behind the windfall. IBM experts say the average cost of a data breach surged to a record high of \$4.24M in 2021.

That said, threat actors are winning not because they're all dark web masterminds with access to "secret" tech. They're winning because they're constantly adapting their strategy based on current conditions.

With new strains emerging and old tactics evolving, leaders must follow suit and embrace a modern, AI-driven ransomware strategy.

In this comprehensive guide, we'll explain how ransomware works, why you should care, and what it takes to defend against this growing threat.

Foreword

Dear Reader,

According to the World Economic Forum Global Cybersecurity Outlook 2022, 80% of IT leaders see ransomware as a “dangerous and evolving threat to public safety.”

And, IT leaders surveyed in the Allianz Risk Barometer 2022 cited “cyber incidents” like ransomware attacks, cloud outages, and data breaches, as their top business concern — beating out COVID, climate change, and supply chain disruptions.

Non-technical business leaders know this, too. And most have some sort of strategy in place. The problem is, it’s not working.

Cybercriminals are leveling up like crazy. Yet, we’re still seeing tons of companies defending themselves with legacy solutions.

Then, they become victims either because leaders are too entrenched in the status quo — or they lack the knowledge, support, and even the vocabulary they need to get the ball rolling on security transformation.


That disconnect between IT and the C-suite is a massive risk to the business — on multiple fronts.

First, ransomware isn’t just an IT problem. It’s on everyone to develop a strong security culture, come up with recovery plans, and proactively strengthen your security posture.

Second, when IT and leadership teams don’t communicate, you end up with an environment that doesn’t work for its users. And as a result, it becomes a barrier to achieving critical objectives.

For example, your CISO might know everything about AI threat detection or protecting data transmissions across 5G networks. However, that knowledge is only valuable if it can be leveraged toward a specific outcome.

Poor alignment also leads to poor decisions — like what we’re starting to see as CXOs brace for recession. According to a recent Gartner survey, IT spend hasn’t kept pace with inflation.



While very few companies are eliminating security budgets, they are missing an opportunity to build resilience – which may have serious long-term implications on things like growth or agility. Ramping up IT investments is actually one of the best ways to shield the business from financial losses during a downturn.

With all that in mind, our goal with this ebook was to help close that gap. We wanted to give non-technical leaders deeper insight into what modern security strategies should look like.

We also included examples that illustrate how different stakeholders support their company's Zero Trust strategy.

Finally, we wanted to highlight embedded security as an asset in its own right. For example, as a Microsoft Partner, security provides tremendous value to Velosio clients – given the nature of our services.

For instance, if you're managing critical data in the cloud or optimizing workflows, clients need assurance that digital assets are protected.

- Carolyn Norton, Director of Cloud



Chapter 1: What is Ransomware?

Our first chapter explains what, exactly, ransomware is, how it works, and why you should make it a critical priority. You'll learn about different types of ransomware, common targets, and what kind of havoc attacks can wreak on your business.

Ransomware is a type of digital extortion

that essentially follows the template for kidnapping – with critical data standing in for a human victim.

Attackers blackmail their targets into paying a ransom – threatening to release the data if they fail to pay before the deadline.

This means, organizations are put in a tough position – facing the threat of reputational damage, fines, or litigation if they refuse to play along.

Advances in technology not only support the citizen data scientist and the citizen developer, but the citizen cybercriminal, too. Which means, ransomware is a growing threat.

This first chapter will explain what ransomware is and why it's a serious and growing threat that touches all digital investments and strategies.

What, Exactly, is Ransomware?

Ransomware is a type of malicious software (malware) that “infects” a device and encrypts its files, rendering them unusable.

Cybercriminals will then demand a ransom in exchange for decryption – blocking users' access until they receive payment – along with the threat of leaking or selling stolen data or log-in credentials if the payment is not received within the specified timeframe.

Ransomware itself is code that when inserted into a system encrypts the files on the system/ server. It's important to understand that this isn't “basic” encryption, it's far more sophisticated.

This encryption blocks the user/administrator/ owner from accessing the files. Without the encryption key, the data will never be accessible.

Typically, the malware uses a custom or specialized form of encryption, which makes it a lot harder to crack the code. And it's this particular quality that makes ransomware such a threat.

If the code followed a more predictable pattern, you'd presumably be able to hire an expert to decode your files for a lot less than the cost of paying the ransom. Unfortunately, it would take far too long to crack the code — if it happens at all — and you'd miss the deadline.

Types of Ransomware

Now, ransomware comes in several different flavors.

- **Crypto.** The most common type of ransomware, crypto (as in encryption, not crypto currency) attacks encrypt files, rendering them inaccessible without a decryption key.
- **Locker.** Locker attacks lock users out of their system, preventing them from accessing files. Here, users will be presented with a lock screen that displays the ransom demand, often with a countdown clock to give users a sense of urgency.
- **Scareware.** Scareware attacks use false claims – think pop-ups that claim there's a virus or some other problem with your device and direct you to a second location where you can solve the problem. Some scareware attacks lock you out of your device, others hit you with a ton of pop-up spam, without causing serious damage.

- **Doxware/leakware.** These types of attacks threaten to leak personal information or IP to the public, prompting victims to pay the ransom to prevent sensitive data from falling into the wrong hands.
- **RaaS.** Ransomware-as-a-service (RaaS) is a bit different from the types of ransomware we just mentioned. But – it's a rising trend that's essentially driving a major digital transformation within the cybercrime space.

Basically, RaaS allows malware developers to monetize their creations using a subscription-based billing model (get it, like SaaS) or by requiring customers to register an account to access the ransomware.

This means that bad actors don't need to have tech skills to launch the infections — they simply give developers a cut of the proceeds. The developers themselves face few risks, as the customers are the ones launching the attacks and making the threats.

Who Does Ransomware Target?

First of all, ransomware doesn't necessarily need a specific target to spread across the web. However, the real money comes from human-operated ransomware, where hackers deploy hands-on attacks targeting victims based on potential impact.

In some cases, attackers seek out organizations that are more likely to have small security teams or a distributed user base, making it easier to penetrate their cyber-defenses. Think — government agencies, universities, and small businesses.

According to a 2021 World Economic Forum report, government and education are at the greatest risk of experiencing a malware attack – this is likely due to the fact that public sector institutions have fewer resources for fending off cyber attacks than their private sector counterparts.

Another report estimates that 82% of ransomware attacks target SMBs (orgs with fewer than 1000 employees).

While certain organizations may find themselves more vulnerable to ransomware attacks, that doesn't mean everyone else is safe.



Anyone can become a victim – though it’s worth noting, there are certain qualities that make some organizations more attractive to threat actors than others:

■ **Orgs in possession of sensitive data.**

Cybercriminals often look for organizations with a lot to lose – think orgs that handle sensitive data or valuable IP. This is a key reason why professional services firms are among the industries most at risk. Here, the idea is, the victim is likely to pay the ransom ASAP to avoid legal and reputational ramifications of a data leak.

■ **Companies with fewer security protections.** Cybercriminals often target organizations they perceive as having weak security measures and smaller teams. This includes small businesses, companies with outdated websites or legacy technology, even universities – which are vulnerable due to their high volume of file-sharing.

■ **Businesses in Western markets.** Corporations operating in the US, Canada, the UK, and Western Europe are often targets due


to their wealth and reliance on cloud-based tools and devices. While these companies often have stronger security protections than SMBs and public sector entities, attackers are likely to get a larger payout if they succeed.

■ **Organizations that are likely to pay quickly.**

Attackers also look for targets that have the means and the motivation to pay the ransom right away. This group includes government agencies, hospitals, banks, and utilities – orgs that need immediate access to the compromised files and will worry about the financial impact later.

Keep in mind, these are just some general factors cybercriminals might use to pick their next target. All organizations, public or private, SMB or enterprise, regardless of industry can be the target of a ransomware attack.

Another factor is motive. Most ransomware attacks are financially motivated, but in some cases, threat actors are motivated by politics or personal beliefs – aka “hacktivism.”



For some, it's a matter of social justice, for others, it's an act of terrorism, war, or an opportunity sow chaos – and any profits are a secondary benefit.

As an example, back in January 2022, Microsoft's Threat Intelligence Center (MSTIC) identified evidence of destructive malware targeting Ukrainian organizations – designed to render infected devices inoperable, rather than collect a ransom.

At the time, the team was unable to connect the attacks to any specific group – though given the ongoing situation with Russia, all signs point toward “nation state attack.”

The Business Impact of Ransomware

Organizations that fall victim to ransomware attacks can lose thousands of dollars (possibly more, depending on the target) by paying the initial ransom.

Some businesses can afford the financial hit.

In certain cases, cyber insurance claims can help businesses recoup some of their losses. In others, law enforcement is able to recover at least some of the ransom.

But, even in those best case scenarios, ransomware attacks can have a negative impact on the business long-term. We're talking: reputational damage, diminished revenue, and the loss of customers, talent, and strategic partners. In some cases, the business is forced to shut down altogether.

Typically, ransomware is designed to infect a device and spread throughout the entire network – encrypting file servers, databases, and connected devices and apps – quickly

shutting down an organization's operations. So, there, you're potentially taking a serious hit to productivity and potential earnings that can impact the bottom line for months, even years to come.

In some cases, ransomware attacks can lead to legal or regulatory actions — serious fines, class action lawsuits, etc. that can easily bankrupt a company.

And then, there's the issue of trust and public perception. If customers feel that they can't trust you to keep their data safe, they'll take their business somewhere else. This loss of trust was a big deal for retailers like Target and TJ Maxx, but imagine a data breach on that scale if you're, say, a wealth management firm or a healthcare provider.

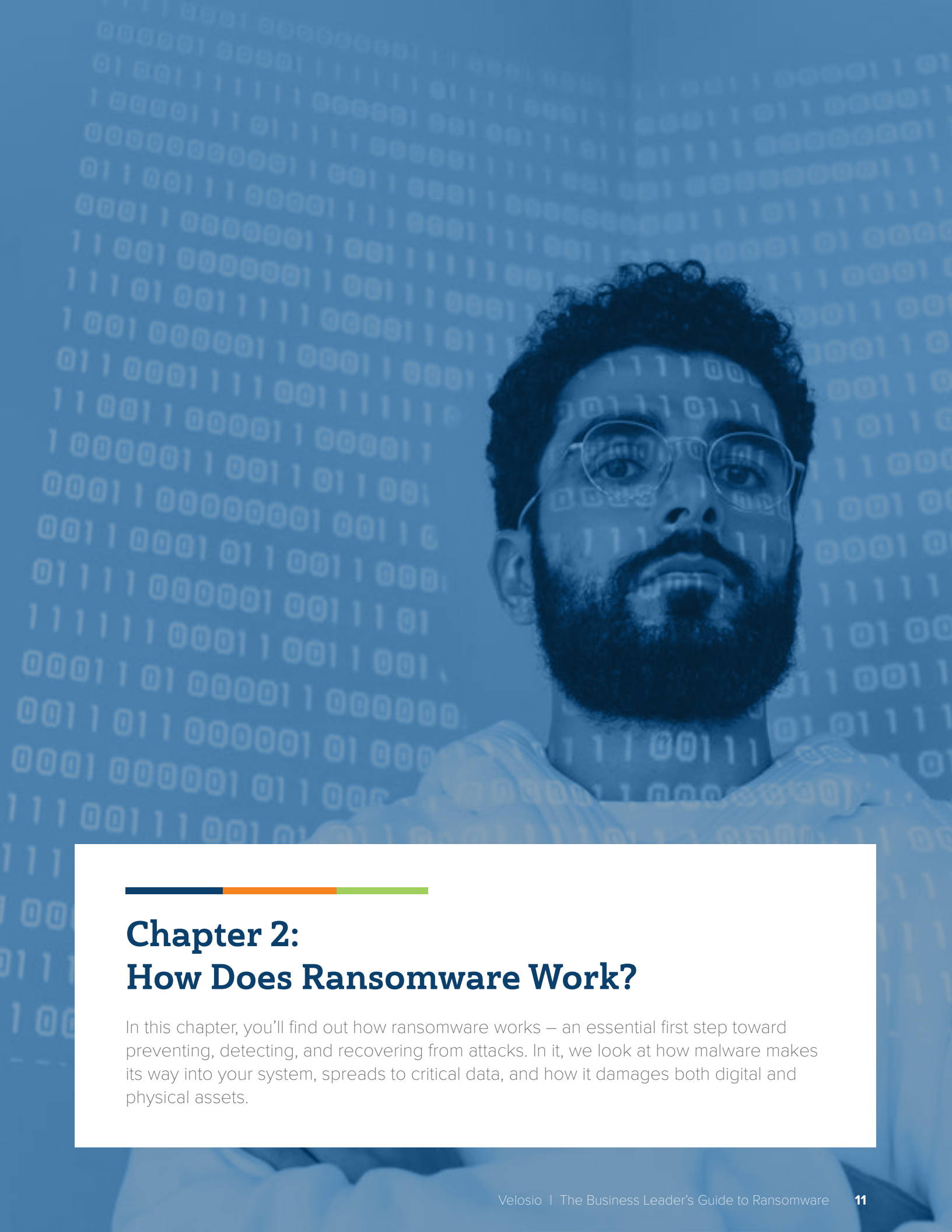
Final Thoughts

Just as the rapid pace of change is driving digital transformation and reshaping customer expectations and market conditions — it's also exacerbating the frequency and severity of ransomware attacks.

Attacks might happen in cyberspace, the impacts of ransomware have “IRL” implications.


Orgs need to be aware of this threat and take proper action in order to arm themselves. Otherwise, they could face serious damage — to the brand and the bottom line, of course, but also to physical infrastructure, equipment, and real human lives.

In chapter two, we'll explain how ransomware works to give you a better sense of how attackers launch and deploy ransomware – and what malware does once inside your system.



Chapter 2: How Does Ransomware Work?

In this chapter, you'll find out how ransomware works – an essential first step toward preventing, detecting, and recovering from attacks. In it, we look at how malware makes its way into your system, spreads to critical data, and how it damages both digital and physical assets.



Ransomware attacks generally work like this: cybercriminals launch targeted attacks, using malware designed to encrypt the victim's files and, potentially, lock them out of critical programs or devices.

They'll then hold those files hostage until the ransom is paid (though, unsurprisingly, there's no guarantee they'll keep their word).

If victims don't pay the ransom by the deadline, the attacker will leak the files, sell the data, or take some other damaging action.

So, that's the short answer.

There's a lot more that goes into launching a successful ransomware attack – and a lot that happens once that ransomware lands inside your system.

Here, we'll walk you through the ransomware lifecycle, one step at a time.

How Do Ransomware Attacks Work?

Ransomware often spreads via phishing emails (or, increasingly, text messages) containing links or attachments. Think — fake emails from Netflix, your bank, even the IRS or fake ads containing malicious links that unleash the malware on the target device.

It can also be spread via drive-by downloading, which infects users when they visit an infected website. During that visit, malware is automatically downloaded without the victim's knowledge.

This method used to be much more common (in the days before technology made it possible to launch targeted attacks promising bigger

payouts). And — it's a key reason why Google now sends you a warning any time you land on an unsecured website.

In any case, the malware is introduced to your network through an executable file and from there, encrypts the victim's data/files.

The hijacker then sends the “ransom” demand — A request for payment, along with a deadline, typically in cryptocurrency, upon receipt the victim will receive a key to decrypt the files.

From there, the attacker typically makes a threat that reads something like this: if the ransom isn't received by X date, the files will either be destroyed or sold off.”

Inside the Ransomware Lifecycle

Now that we've gone over some background info, let's walk through the “typical” ransomware lifecycle to give you an idea of how an attack might play out from beginning to end.

While every situation is different, ransomware attacks tend to follow the same basic trajectory.

Regardless, getting familiar with the ransomware lifecycle can help you better understand how malicious code operates within your system — an important first step toward protecting your org from attacks.

The Ransomware Lifecycle



Initiate the Attack

First, the hacker writes or modifies ransomware code based on the system they're attacking. Then, they'll establish a distribution method — or how they'll launch the attack — email, SMS, Active Directory (AD), executable, etc. — and gain initial access.

This can be done in a variety of ways — by setting up malicious websites, exploiting vulnerabilities in your remote desktop connections, or launching a direct attack on weak points in a specific piece of software (i.e. an unsupported app or a system that's overdue for an update).

That said, the most common points of entry are phishing/smishing campaigns that distribute an access trojan like TrickBot, Bazar, or QakBot. Attackers tend to target the less technical staff


because they're more likely to click the link or enter contact information. It's also worth noting that the more users you have in your organization, the more vulnerable it is to a user-targeted attack.

All it takes is one mistake from a single user and hackers can execute the code and infect the entire system.

Exploit, Expand, Understand

Once the ransomware has gained initial access to your system, the code will establish a line of communication back to the hacker. Think — offensive security tools like Metasploit or Cobalt Strike or a remote access tool (RAT) that allow them to establish remote access to your system.

This stage is about mapping out your local



system to determine what they currently have access to, then expanding outward — acquiring additional data and credentials before activating the attack.

The attacker might use this communication line to download additional malware to your system — which could start making lateral moves across your digital ecosystem right away gathering as much data as possible. Or — the malware could lay in waiting for several months — allowing the attacker to strike at the perfect moment.

Ultimately, this is a recon mission where cyberattackers are figuring out how to get the most ransom for their efforts.

Data Exfiltration and Extortion

At this stage in the game, ransomware attackers shift their focus from identifying valuable files and data to actually stealing it.

Per IBM's 2022 X-Force Threat report, almost every ransomware attack X-Force IR has responded to since 2019 has used the double extortion tactic, where attackers steal a victim's data before the malware activates its encryption routine.

This gives hackers an opportunity to make two demands. First, encrypting the victim's files and demanding payment in exchange for decryption. And second, by demanding that the victim pays an additional ransom to prevent the attacker from leaking their data online.

While double extortion attacks are still more common, cyberattackers are increasingly adding on extra layers of extortion — launching triple extortion attacks where attackers demand payment from anyone who might be affected if the victim's data is leaked.

There's also quadruple extortion — where attackers leak or destroy the victim's data if

they report the incident — whether to law enforcement or the media.

The IBM report also found a fair amount of variation among ransomware attackers where data exfiltration is concerned.

Most operators use tools like RClone and WinSCP, but it seems that custom exfiltration tools are becoming more common — as well as command-line tools like bitsadmin.

Activation and Encryption

At this point, the cyberattacker executes the attack remotely or the victim activates the code, say, by clicking an infected link. Either way, this is the moment in which the payload executes and encrypts the files.

Which means, orgs need to move quickly to mitigate potential damage and recover from the attack.

Ideally, you already have a plan in place for containing the damage and getting things back on track — otherwise, you could be looking at hours, days, or weeks of downtime — which, of course, is disastrous for your reputation and your bottom line.

At the same time, a solid action plan won't necessarily keep you safe. For example, ransomware designed specifically to go after backup systems might also encrypt or delete backup files — preventing a smooth recovery.

In that case, decrypting the data is unlikely — so your only options are moving forward without that data, paying the ransom, or recovering from an older backup or replica.

Ransom Request

At this stage, the victim is presented with a

message explaining how things are supposed to go down — ransom demands, amount, timeframe, a wallet/transfer method for sending the money, and, of course, the consequences of non-compliance.

Depending on the form of currency and how the funds are dispersed it's often sent into the digital void. It's important to note that cryptocurrency is largely untraceable due to the decentralized nature of the blockchain.

Payment (Or Not...) and Recovery

At this point, things can go a couple different ways. If you opt to pay the ransom, your files are decrypted (well, at least they're supposed to be), you'll report the breach to law enforcement, update your CyberSec reports, and, hopefully, learn from this experience.

Recovering funds is rare, but it is possible. Law enforcement has had some success here — most notably with the Colonial Pipeline attack). In that instance, law enforcement was able to recover 63.7 of the 75 BTC (or \$2.3M) as the price of Bitcoin dropped shortly after the attack.

So, yeah, even if everything goes according to plan, you could face major losses based on crypto's inherent volatility alone.

If you don't pay the ransom, you lose the stolen data, and valuable IP and/or customer data is released into the wild, sold, or both. Your company's reputation takes a big hit. You'll likely lose customers and the public's trust (aka it'll be so much harder to replace customers after they jump ship). And then, there's the matter of regulatory fines, lawsuits, and losses.

Now, keep in mind that paying the ransom or even recovering data from a backup doesn't mean you're in the clear.

Resale is still a possibility even with payment. There's not always definitive proof that the attacker doesn't have an unencrypted copy of the data. And — the more valuable the information, the higher the risk of resale.

There could still be ransomware code or malicious files hanging around in your system and you'll want to make sure you remove them — and seal up any remaining security gaps or vulnerabilities before moving forward.

That said, the attack itself can give you an idea of what type of ransomware hit your system, making it easier to track down and remove. But — it's a good idea to do this inside an isolated sandbox environment to clean up your system to protect against the risk of reactivation.

Final Thoughts

Even with the best protections in place, there's always a chance that malware will somehow find its way into your system.

A critical first step in mounting a strong defense against ransomware is learning how it works. Understanding how ransomware works — from infiltration to activation, encryption, and beyond — can help you map out critical endpoints, identities, apps, and devices, so you can better secure them.

More importantly, it allows you to ensure that security is embedded in the flow of daily work — both by making security a central part of your culture and by embracing solutions that make it easy for everyone to practice good habits.

In chapter three, we'll take things in a different direction and look at the high-level ransomware trends shaping the current and future threat landscape.



Chapter 3: Ransomware Trends: Facts, Stats, & Emerging Threats

The last few years have brought dramatic changes to the ransomware landscape – from the rise of big data to the peak-COVID embrace of cloud computing and remote work. In chapter 3, we look at how those changes are playing out in the “ransomware community” and what that means for your business.

According to Microsoft, ransomware has become more sophisticated – and in many ways, more dangerous.

Remote networks, the IoT, and supply chain software are uniquely vulnerable to attack. Attackers are more organized than ever, and have access to technologies and tools that enable them to net bigger payouts by targeting victims with deep pockets and a high-profile.

So, while we're seeing more attacks make headlines, total attacks are down.

In some ways, things are getting better – but overall, the ransomware situation is a real mixed bag. On the one hand, there's a lot more to be afraid of. But, on the other, there are now way more resources, tactics, and tools available that can help you stay safe.

In this chapter, we'll try to make sense of the ransomware landscape – as it stands today.

Ransomware in 2022

Here are a few stats that paint a clearer picture of where ransomware stands right now:

- **Sophos' 2021 State of Ransomware survey revealed that 37% of participants were hit by ransomware attacks in 2021** – down from 51% the year before. The survey also found that while total attacks were down, the average cost of recovering from an attack was roughly \$1.85M – which accounts for things like down-time and missed opportunities, along with the ransom itself.
- CrowdStrike reports that the number of attacks that resulted in stolen data being leaked to the public increased by more than 80% from 2020 to 2021. Ransom demands

are up, too. In 2021, the average ransom was about \$570k – a more than 500% increase from 2020. At the high-end, ransom demands can hit \$50M+.

- According to another CrowdStrike report, SMBs are particularly vulnerable. Many have valuable IP, vulnerable networks, and a lot to lose. While many struggle to pay ransoms, the legal, regulatory, and reputational ramifications can easily level their business and they may believe they have no other option.
- What's more, when attackers are successful, 80% of victims did paid the ransom were attacked again shortly after. So – we're seeing some vulnerable companies suffer additional blows as they recover.

At a glance, these numbers are absolutely terrifying. But, they don't necessarily mean you're doomed.

A March 2022 Zerto report asserts that orgs are better equipped than ever to fend off ransomware attacks. Though researchers also noted that significant gaps remain — particularly when it comes to IoT networks, remote devices, and keeping pace with an innovative new breed of attackers.

The point is, preparation is key. In the next few sections, we'll discuss three key ransomware trends and what they mean for your business in 2022 — and beyond.

1. Ransomware Gangs Grow Up and Get Organized

Attackers are shifting away from high-volume ransomware attacks and instead, moving toward customized attacks, tailored around specific targets more likely to deliver bigger payouts on a shorter timeline.

One of the key reasons for this shift is that ransomware is becoming more accessible to non-technical cybercriminals — a trend that echoes what’s happening in every industry. Widespread access to drag-and-drop development tools and open-source code are accelerating the generation and spread of new variants — and fueling the growth of two ransomware industries: the cybercrime syndicate and the ransomware service provider.

Once considered a criminal cottage industry, Ransom Operations, or RansomOps, has evolved into a complex underground market — boasting more specialized talent and sophisticated technologies than ever, along with a whole host of innovative solutions currently redefining the space. Ransomware rings, or “gangs,” now run like real-deal businesses — with CEOs, middle managers, sales reps, marketers, and so on.

The big danger with RansomOps is that these attackers are invested, and often spend several weeks or months preparing for deployment — in other words, attacks are treated like any large-scale business project — with all of the planning, deliverables, and KPIs that come with the territory.

To put things in perspective, in 2021, just six ransomware groups were responsible for nearly 300 data breaches, collectively netting a cool \$45M.

Second, you’ve got the rise of ransomware-as-a-service, or RaaS (which Microsoft describes as a sort of gig economy for cyber criminals).

Here, organized threat actors have set up one-stop shops on the dark web where ransomware developers can monetize their creations.

Aspiring attackers can purchase custom suites of ready-to-launch malware, designed with a specific target in mind. Or — they can buy generic malware and make a few tweaks using low-code/no-code solutions.


Either way, amateurs can launch pro-grade schemes that are more likely to fool discerning recipients — and deliver the ransom payments they’re after.

RaaS is a massive industry with service providers embracing the marketplace and subscription-based models that have become popular in recent years.

And many are careful about who can access their platform and purchase services. DarkSide, for example, requires prospective customers to complete a multi-step application process and internally, uses a set of predefined standards to determine who they’ll lease their software to.

Customers who pass the screening can buy or lease a package that fits their needs, deploy the attack, collect the ransom and move on as if nothing happened.

What makes RaaS attacks especially scary is that anyone with a grudge, financial incentive, or political motivation can wage an attack. With RansomOps, you have an Initial Access Broker (IAB) who lays the groundwork, often infiltrating the network, then setting it up for a large attack. This step maximizes the damage of the payload.



The RaaS provider, on the other hand, is responsible for creating, managing, and selling/leasing the payload, and affiliates are the ones carrying out the attacks.

While you can't prevent bad actors from trying to break into your system, your best bet is disrupting attacks as early in the chain as possible.

2. Remote Work Poses a Serious Threat

2020's rapid shift to remote work expanded the attack surface, legacy security models were ill-equipped to protect remote employees and more workers were accessing company networks/apps from unsecured personal devices. All of this unlocked new opportunities for threat actors to attack – with many breaking in via VPN connections.

We're now halfway through 2022 and still in the midst of a global pandemic. So, while we've more or less settled into remote work, ransomware attacks on individual devices aren't letting up.

According to a recent Microsoft report, phishing remains the root cause of most data breaches – responsible for a whopping 70% of attacks. On top of that, phishing and SMISHing attacks have increased in scope, scale, and frequency since COVID hit in March 2020.

Remote work poses a heightened threat for ransomware attacks – even with VPNs, VLANs, and other virtualization tools that separate the personal from the professional.

This is, in large part, due to the fact that it's impossible to control all employee actions in any given company device or system. One infected email sent to an employee account – and

opened outside the virtualized environment – could lock the entire system. And – with proper precautions in place, one wrong click could infect the entire environment, locking company files and putting the company in jeopardy.

What's more, remote teams are increasingly using personal devices to conduct business. So, even with strict protections in place, vulnerabilities from older hardware and unprotected software can slip through the cracks.

Without administrative control over the system, companies can't enforce updates or patches on all at-risk systems and devices connected to the network. VPNs offer some protection, but it's not 100%, and threat actors can still break in with the right set of tools.

This risk can be minimized, though not fully eradicated, by ditching BYOD or personal device policies for remote work.

Removing the ability for employees to have “free rein” over the device (install or use any software without restrictions or unrestricted access to the internet), can reduce the risk of an attacker taking over the system due to the use of access control and other restrictions. But – there's still the risk that an email could come to an employee's company account, and through lack of security awareness or just a good phish, the employee will click on it.

Another serious threat is unintended sabotage. This is less about ransomware itself, but more about the fact that employee devices may be used by other members of their household who could unintentionally unleash havoc on the entire enterprise – with no knowledge of the destruction they've caused.

The Microsoft report re-emphasizes the critical importance of embracing Zero Trust – an approach that assumes any user or device on a

network has been compromised and continuously verifies its security.

3. IoT, OT, and the Supply Chain Are Under Attack

Per Microsoft analysts, the need for better cybersecurity protections for OT and the IoT came into clear focus last year, due to several high-profile attacks that hit a water treatment plant, an oil pipeline, surveillance systems, and networks of connected devices, among others.

A recent Anchore survey found that supply chain software attacks targeted three in five companies and just 38% said this type of attack did not impact their business in 2021.

According to IBM, manufacturing was the most attacked industry of last year — taking the crown from financial services. Over 60% of operational technology (OT) attacks hit manufacturing companies, while 36% of all OT attacks were ransomware. That same report revealed that recon efforts against OT equipment increased by more than 2200% between January 2021 and September 2021.

While IoT, OT, and supply chain networks clearly have a target on their backs, Microsoft researchers emphasized that, despite the risks, investing in these technologies remains an urgent priority.

In a joint survey with the Ponemon Institute, 68% of respondents said OT/IoT adoption is central to long-term business success and over 30% said they were unwilling to slow down adoption because of security concerns. Yet, 60% of that same group admitted that OT/IoT devices were the least secure part of their company's digital infrastructure.

According to Bain & Company's 2022 Global

Machinery & Equipment report, these technologies play a critical role in helping industrial organizations embrace a more modern business model. Analysts say that IoT/OT innovation supports sustainability goals, allows orgs to focus on building solutions for more niche, specialized use cases, and explore new service models.

The Microsoft-Ponemon survey also stresses that many of these security gaps are a visibility problem. Addressing that issue is a significant first step in the right direction, laying the groundwork for mapping and securing every endpoint, asset, and device in the network.

Final Thoughts

As you can see, the state of ransomware — and cybersecurity on the whole — is well, kind of a mess.

Remote work, along with growing adoption of IoT devices, greater reliance on the cloud, and poor security practices mean opportunities for bad actors have exploded.

On top of that, innovations in the RansomOps space have made launching an attack easier for anyone looking to break into cybercrime.

The good news is, the solutions already exist. Things like Zero Trust, AI/ML-based protections, even just working cybersecurity best practices and literacy into your company culture.

Now, it's a lot to tackle all at once. We'll ease into specific solutions and strategies later on.

For now, we'll take a look at some of the biggest attacks in recent memory — and what you might learn from cybersecurity mishaps gone public.



Chapter 4: Six High-Profile Ransomware Attacks & Lessons Learned

Every other day, another high-profile ransomware attack makes its way into headlines. While it's easy to walk away from the news cycle feeling hopeless, each major attack offers key lessons you can use to protect yourself against expensive, catastrophic worst case scenarios. This chapter looks at six large-scale attacks on real companies – and what you can learn from them.

Manufacturers, SMBs with valuable IP, and companies that rely on IoT devices are among those most at risk becoming ransomware victims.

However, cyberattackers don't discriminate and will go after orgs in every industry on the planet.

Consulting firms, non-profits, big meat – anything with the potential to deliver a big payout. Or, at the very least, give them something they can sell on the dark web.

This chapter zooms in on six high-profile attacks and what you can learn from them.

1. SolarWinds Ransomware Attack

The SolarWinds cyberattack is one of the most infamous and far-reaching ransomware campaigns in history.

The breach first began in September 2019 with an initial dry run – the threat actor injected test code into SolarWinds' Orion software, a suite of network management and monitoring tools used by a segment of high-value accounts, including the US government.

Then, in February 2020, the attacker injected trojanized code into a file that was then distributed by SolarWinds, as part of an Orion update.

The attack was found to be perpetrated by Russian hacking group, Nobelium, as part of a targeted espionage campaign. Nobelium is particularly skilled at backdoor attacks that evade detection. SolarWinds had no idea anything was wrong until November 2020, when cybersecurity firm FireEye detected an intrusion within its systems.

The compromised Orion software enabled the threat actor to gain access to FireEye's Microsoft cloud platforms. And – in December 2020, Microsoft, FireEye, SolarWinds, and others began working with the US government as part of an emergency response.

Lessons learned:

- **Minimize third-party risks.** According to Microsoft, security leaders are beginning to pay more attention to supply chain risks. While traditional vetting measures can help reduce risk during the selection process, they don't mitigate risk or enforce compliance in real-time.

Here, hackers inserted malicious code into a third-party system — Orion — with access to the SolarWinds network. Extending Zero Trust best practices like using least-privileged access and verifying explicitly to third-party partners and vendors can help, as can frequent audits and robust monitoring systems.

- **Keep an eye on all code & components.** Organizations must take proactive measures to keep malicious code out of software products. These include things like disabling forking, scanning and auditing your repository, setting automated alerts for vulnerable dependencies, tightly managing developer credentials and access permissions, whitelisting IP addresses, revoking external contributor permissions after a project. The list goes on.

- **Closely monitor outgoing traffic.** Organizations should implement the same kinds of protections to monitor outbound traffic as inbound traffic. The idea is, even if you configure your network to only grant access to approved users, devices, etc., you'll still see new systems and devices connecting to your network all the time.

Implementing solutions like Defender for Endpoint, Defender for Office 365, and Antivirus software can help you keep stealth attacks out of your system and make it easier to spot unauthorized users, bad configurations, and unusual traffic.

2. Colonial Pipeline Ransomware Attack

In May 2021, the Colonial Pipeline Company was hit by a ransomware attack, forcing the oil pipeline system to shut down operations for almost a full week — dealing a serious blow to critical infrastructure.

Because the Texas-based pipeline supplies much of the eastern and southeastern United States with gas and jet fuel, the disruption forced some gas stations to shut down, while others experienced miles-long lines of panicked customers.

Within hours of the attack, Colonial Pipeline paid ~\$44M in ransom, a figure that doesn't account for downtime, recovery costs, and reputational damage.

Later, the incident was attributed to the Russian ransomware gang, REvil, which offers ransomware-as-a-service to clients. Hackers gained access to the Colonial Pipeline network using compromised credentials to log into an inactive VPN account.

Lessons learned:

- **Enable MFA.** Colonial Pipeline Chief Executive Joseph Blount explained to a US Senate committee that at the time of the attack, the legacy VPN hackers used to enter the system only had single-factor authentication

enabled. Blount emphasized that the password linked to the account wasn't a default password like "Colonial123."


The problem is, password complexity doesn't matter in cases of credential theft. Something as simple as multi-factor authentication (MFA) could have prevented this attack from happening in the first place.

- **Swap your VPN for a secure portal.** Hackers often use VPNs to gain access to a target network. Once they're in, it's relatively easy to move laterally across the system. Worse, if you share information with external clients or 3rd-party vendors through your VPN, threat actors can break into their systems, too. Ultimately, your best bet is ditching your VPN for a more secure solution that provides greater visibility and more control.
- **Implement an automated review system.** An automated internal review system provides visibility into individual accounts, access permissions, and usage, as well as the devices, assets, and apps in your network.

The legacy VPN used in the Colonial Pipeline attack was inactive, albeit, still connected to the rest of the network. AI-driven analytics and automated alerts would have been a game-changer, here — flagging the VPN and allowing IT to intervene before something happened.

3. CNA Financial Ransomware Attack

In March 2021, CNA Financial was hit by a ransomware attack that ended up encrypting an estimated 15k of its systems. The attack began



when an employee downloaded a fake browser update from a legit website containing the Phoenix CryptoLocker ransomware strain.

The attacker was then able to obtain access credentials and move laterally through the system.

The \$40M ransom payment set a record at the time that still stands today.

While experts and law enforcement generally advise against making ransom payments, CNA leaders felt that they didn't have other options. The attack disabled such a large share of the company's IT infrastructure, that paying the ransom seemed like the fastest path to recovery.

Lessons learned:

- **Make cybersecurity education a priority.** Arguably, the most important lesson you can learn from this attack is the need to better educate employees about cybersecurity. While attackers might deploy sophisticated tactics once they've gained access to a network, they often gain entry through basic methods like phishing. The person who downloaded the ransomware likely had no idea they were putting the company at risk.
- **Implement rapid threat detection.** When businesses can detect anomalies, vulnerabilities, and breaches in real-time, they can take action faster and mitigate potential damage.
- **Develop cyber attack playbooks.** While prevention is the best medicine, there's no way to guarantee that you won't become a ransomware victim at some point. Putting together incident response plans for different scenarios (data breaches, stolen credentials, how to handle ransom demands, etc.) facilitates smart decisions and quick action when disaster strikes.

4. JBS USA Ransomware Attack

On May 30, 2021, JBS Foods was hit by an organized ransomware attack, forcing temporary closures of all its US beef plants, one Canadian plant, as well as beef and lamb kill operations in Australia.

The organization paid an \$11M ransom and was able to fully restore global operations by June 3 using backups. Given that JBS Foods is the world's largest meat supplier, this incident could have caused far more damage.

DHS classifies food suppliers as "critical infrastructure," as attacks on major suppliers could lead to prolonged shortages and price increases.

According to the FBI, the attack likely came from a Russian ransomware gang known as REvil. Like Colonial Pipeline, JBS is among the 85% of critical infrastructure that is privately-owned — which indicates that the attack was part of a broader strategy aimed at companies that control critical supply chains.

And — because consumers depend on commodities like food and fuel, those companies are likely to pay large ransoms to get things back on track.

Lessons learned:

- **Implement an incident response plan.** JBS reportedly spends over \$200M per year on IT. Reps said those investments — along with robust security protections, protocols, redundant systems and encrypted backup servers — were key in helping them recover relatively quickly following the attack.

Equally important was the fact that the JBS team knew exactly what to do from the moment they learned of the attack.

- **Automate ID governance.** With a large manufacturer like JBS, new employees, vendors, and partners are always coming and going, so manual provisioning can easily lead to over-provisioning, shadow accounts, and inactive IDs — all of which introduce serious compliance challenges and security threats.

Automating identity governance allows orgs to outsource provisioning, de-provisioning, access approvals, and more — significantly reducing the risk of noncompliance and preventing bad actors from accessing sensitive data and apps.

- **Secure non-human identities.** Non-human identities include IoT and mobile devices, social media and service accounts, and “secrets” like API keys, passwords, and certificates. Organizations can protect their stack by implementing IAM capabilities at the edge, storing privileged credentials and keys away from devices (preventing lateral movement), and using endpoint privilege management tools.

5. Planned Parenthood Ransomware Attack

In October 2021, Planned Parenthood Los Angeles fell victim to a ransomware attack that exposed medical information of 400k patients — many of whom visit the organization’s network of health centers for sensitive matters — sexually transmitted diseases, contraception, abortions.

Healthcare orgs (particularly small, outpatient clinics) are prime targets for attackers looking to

sell PHI/PII on the Dark Web, demand a ransom, or leak data for political or malicious purposes.

Cyber attacks on health care organizations are always scary, because they put real lives at risk. Service disruptions prevent patients from receiving critical care, while data leaks can threaten their reputation or physical safety.

On the business side, class action lawsuits (like the one PPLA is facing right now) and HIPAA violations can take down a non-profit clinic in no time.

Regardless of where you stand on the Supreme Court’s decision to overturn *Roe v. Wade*, this attack is particularly concerning — especially given the fact that RaaS marketplaces allow anyone to buy malware, credentials, exploits, and other “tools” that make it easy to launch a DIY attack on any organization (or individual) for less than \$10.

Lessons learned:

- **Run regular risk assessments.** Continuous risk assessment is one of the best ways to find and fix vulnerabilities before threat actors can exploit them. Ultimately, though, you’ll need to be able to measure and calculate risks in real-time — so you mitigate threats and make plans to eliminate them.

- **Embrace integrated threat protection.** According to Microsoft, unmonitored internet-facing systems are easy targets for human-operated attacks — with recent attacks spreading payloads throughout environments containing user credentials, inboxes, endpoints, and web apps.

Experts advise healthcare orgs to implement solutions with XDR and SIEM capabilities like Microsoft Defender Advanced Threat Protection (ATP), Microsoft Sentinel, and Microsoft Defender for Cloud. This

enables them to detect, investigate, and respond to threats from a single dashboard.

- **Practice good cyber hygiene.** Microsoft also recommends that orgs continue to enforce security hygiene practices such as tamper protection, minimal privileges, and using firewalls to prevent lateral movement. On the identity side, solutions like Azure AD allow users to set up conditional access policies, enable single-sign on, and monitor ID-related security risks.

You can also secure privileged access to seal off unauthorized pathways, making it easier to monitor access and usage and protect against targeted data theft. Entra Verified ID allows you to provision and verify decentralized credentials – preventing credential abuse.

6. Accenture

On July 30, 2021, Accenture detected irregular activity in its system indicating a breach, and immediately isolated and contained the incident. Luckily, the firm was able to maintain business continuity through effective planning, protocols, and quick action.

By August 11, Accenture confirmed in a statement to CNN that all systems had been fully restored and that neither the firm's operations nor its clients' systems were impacted by the attack.

Then – they were hit with the second part of what turned out to be a double extortion attack.

Someone claiming to be part of the LockBit gang was posting screenshots, threatening to publish 2400 stolen files (or 6TB) unless the firm paid a \$50M ransom within four hours.

The stolen data contained case studies, PowerPoints, proprietary data, even information about how a cyber incident might affect Accenture and its clients.

Accenture believes that this attack led to several chain attacks on its clients' systems. Initially, the culprit was thought to be the LockBit gang – though some experts believe it was an inside job, as recent investigations revealed no evidence that LockBit was behind the attack.

Lessons learned:

- **Centralize cybersecurity efforts.** Organizations need to put up a unified front against cyber attacks. And building an effective security operations center (SOC) is one of the best ways to do that. Accenture's SOC protocols and controls enabled the firm to ID irregular activity in one of its environments, contained the infected files, and isolated the impacted servers – allowing them to quickly restore operations.
- **Protect your customers.** One of the best ways to avoid double extortion is by implementing a Zero Trust architecture. For example, reducing the size of the attack surface, limiting lateral movement, and continuous monitoring put some distance between attackers and your customers.
- **Be transparent.** Accenture has been quiet about the incident and has never officially confirmed nor denied that it paid the ransom. But silence only further erodes trust among clients – and the general public. It's better to acknowledge what happened, address the problem, then communicate what steps you've taken to protect client data moving forward.

Final Thoughts

While most of us understand that ransomware attacks cause real pain in the real world, they seem like rare occurrences – you know, things that happen to other companies.

This list only represents a fraction of the victims that actually made headlines – the reality is, organizations of all shapes, sizes, and sectors, get hit by attacks every day – and pay dearly for it.

The reality is, ransomware attacks happen so often, only the biggest breaches make the news.

In the next section, we'll share some ransomware prevention and protection best practices for keeping threat actors from entering your system in the first place.



Chapter 5: Ransomware Protection Best Practices

A “good” ransomware strategy will protect your business from all possible angles. In this section, we cover six best practices that belong in all modern ransomware plans – from segmentation and backups to identity, access, and layers of redundant protections.

While there's always the possibility of something sinister slipping through the cracks, a comprehensive defense plan goes a long way in keeping your business safe from ransomware attacks.

But – you should understand that “protection” is more than prevention.

Your goal isn't just to keep attackers out of your system. It's transforming your network into an impenetrable fortress – building resilience through end-to-end protection, a cyber-aware culture, and micro-segmented architecture would-be attackers find unattractive.

With that in mind, let's take a look at six ransomware best practices that can help you minimize your risk.

Establish End-to-End Visibility

Like so many digital strategies, implementing Zero Trust best practices starts with end-to-end visibility (hey, you can't protect what you can't see).

So here, your goal is establishing a clear picture of your entire digital footprint, and from

there, filling any obvious gaps that could put your organization at risk.

A few ways you can improve visibility across your entire digital estate:

Conduct an initial assessment

Once you've mapped out your entire estate, you'll want to perform an initial assessment to determine where your security posture stands right now.

Today's digital organizations, that increasingly enable work-from-anywhere and utilize cloud services, open up a greater range of possible entry points for ransomware campaigns. The entirety of your attack surface must be mapped out and have security controls enabled across every endpoint, device, application, workload, user, etc. connected to your network.

It's about creating an airtight defense that keeps threat actors from entering the system. You want to be able to look at the entire estate and immediately know exactly which assets and data sets are most valuable to attackers.

What vulnerabilities might they exploit to gain access to your system? Once a threat actor has infiltrated your system, what paths might they take during the lateral movement phase?



Identify data & assets

Microsoft experts advise organizations to identify critical business assets, data, and processes.

They also emphasize that it's important to confirm the appropriate team members truly understand where they "live" and how to keep them safe, so that proper controls can be implemented to protect and rapidly restore them.

Uncover (and address) blind spots & gaps

From there, start identifying blind spots and gaps that could put your organization at risk. Think – cloud usage and shadow IT.

You'll want to make sure that you have full coverage across all security layers: endpoints, apps, identities, infrastructure, etc. Your goal is comprehensive protection.

Use anti-virus and anti-malware software and implement security policies that prevent known payloads from launching. Implement XDR and SIEM solutions to stay on top of emerging threats and unusual activity. You get the idea.

Harden Your Security Posture

Once you've gotten the lay of the land, torn down security silos, and flagged critical blindspots and gaps, it's time to start hardening your security posture.

While this isn't a comprehensive list, here are some of the most important things you can do to strengthen your defenses:

Keep up with patching & updates

In 2019, an estimated 60% of data breaches involved unpatched vulnerabilities. Staying on top of patches and software upgrades is another one of those simple prevention methods that can go a long way in keeping your organization safe from ransomware and other threats.

But, as CPO Magazine points out, keeping up with patching and updates requires orgs to balance the need for robust security protections with the need to minimize business disruptions, and the need to ensure IT staff is focused on high-impact work.

As such, your best bet is automating updates, as well as choosing software that automatically delivers updates without requiring IT to manually take action.

Eliminate configuration errors

According to a recent CrowdStrike report, the most common cause of cloud-based ransomware attacks, breaches, and other intrusions is poor configuration. See, when parts of your infrastructure are no longer receiving routine maintenance or security updates, solutions like SIEM, XDR, monitoring, and so on can't protect those environments.

Many of these issues stem from errors made during basic admin tasks. So, you'll want to set up infrastructure with default patterns that make it easy to set up and manage accounts, security groups, roles, etc.

Segment your network

Another thing you can do to limit the scope of damage is break your network into smaller sub-networks, or segments. This allows admins



to apply granular controls and policies to specific parts of the network.

Admins gain more visibility into data flows, usage, and can identify and act on vulnerabilities/incidents faster. It also prevents threat actors from moving laterally through the system.

Make Identity and Access Management a Priority

According to a recent Microsoft report, identity has become one of the most important lines of defense against ransomware. From a protection perspective, preventing ID abuse is critical. It's also the first place you'll want to investigate in the event of a security incident.

A few things you can do to prevent ransomware from entering your system:

Implement MFA (at minimum)

Microsoft estimates that basic protections like SSO and MFA are effective in blocking close to 99% of attacks.

Now, while that sounds some sort of silver bullet, only about 20% of businesses fully implement said protections. Meaning, most ransomware attacks could have been stopped if identity and access management (IAM) was a priority from the get-go.

Still, victim-blaming isn't productive. Even if it were, it's only your first line of defense and there may be other culprits.

Use the least privilege principle & right-sized access

Make sure you restrict access permissions, deny access to unauthorized devices, and block app installations from standard users. Solutions like Entra Verified ID, Azure AD, and Entra Permissions Management make it easier to verify credentials, automate provisioning, and monitor usage.

Lock down admin paths

Attackers often exploit weaknesses in privileged access security during targeted attacks. The benefit is, threat actors can get into the system via privileged accounts or workstations and quickly gain access to critical business assets. Securing privileged access seals off unauthorized pathways, makes it easier to monitor access and usage and better protect against targeted data theft.

Make things easy on end-users

Finally, you'll want to make it easy for users to follow best practices.

Implementing SSO, passwordless sign-in, secure collaboration tools, etc. — all of these small conveniences add up and generate bigger gains for the entire org. When employees have instant access to the apps, data, and docs they need to do their work, without running through a long list of increasingly complex passwords, they get more done in less time.

What's more, it also prevents them from seeking out unauthorized solutions that introduce risks to your network.

Supporting end-users points back to the need for org-wide collaboration. IT must understand

end-user requirements in context to design the systems and processes that keep them safe and help them achieve key goals.

Always Backup Your Files

Backing up all files and maintaining copies of those backups in a secure, separate location is one of the most important things you can do to prevent your data from being stolen, encrypted, and held for ransom. A few things to keep in mind as you put together your backup strategy:

- **Avoid long backup cycles.** Data backups should be performed on a routine basis — though not all data sets will need to be backed up on the same schedule.
- **Follow the “3-2-1-1 backup rule.”** The 3-2-1-1 rule breaks down as follows: you’ll keep three or more copies of your data in different locations, use two different storage mediums, store one copy off-site (different cloud or external hard drive), and store one or more immutable copies using an indelible storage method.

This approach may seem a bit excessive, but it ensures that a vulnerability in one backup won’t compromise the other copies. This makes it easier to bounce back from an attack and limits the amount of damage it can cause. You can wipe the device and reinstall a copy of the backup.

- **Clearly document backup policies & procedures.** Make sure that backup policies are clearly defined, documented, and communicated to the team. Documentation should include things like strategies, goals, processes, tools, individual responsibilities, retention schedules, backup timing, etc.

- **Perform regular testing.** Finally, it’s important that you perform regular tests to ensure that your backups haven’t been compromised. Again, frequency depends on several factors: data volume, assets, etc.

Educate and Train Your Team

Employees can be your greatest risk or your best line of defense when it comes to ransomware attacks.

Poorly-trained employees can undermine even the most sophisticated protections. All it takes is one person downloading an infected file or clicking a malicious link and, just like that, bad actors gain access to your network.

The good news is, arming your team with some basic skills is one of the best (and easiest) ways to defend your business from ransomware attacks.

Ad-hoc cyber security training won’t cut it. Gartner recommends building an adaptive, ongoing program that connects cyber education and awareness programs to business outcomes — just like any other business strategy.

Here’s a look at what that might entail:

Initially, your goal is showing employees how individual actions are directly linked to protecting the organization and its customers from ransomware. Educate employees about current threats — ransomware gangs, recent breaches, business interruption vulnerabilities, etc.

How to ID phishing attempts

Train employees how to spot phishing emails, texts, social media messages, apps, and websites. Small things like looking at grammar usage, salutations (i.e.: Dear Sir/Madam), and sender emails (i.e.: bankofamerica@gmail.com) or hovering over links for more info before clicking can go a long way in preventing malware from infiltrating your network.

Best practices around BYOD, remote access, and removable media use

Remote-hybrid work has increased the threat of ransomware — with more threat actors capitalizing on unsecured personal devices, Remote Desktop and VPN vulnerabilities, and things like USB devices.

It's important that your training efforts focus on ensuring that employees are aware of the risks that come with their devices and what they can do to stay safe.

How to report & respond to known threats

Another critical element in any ransomware training program is reporting and responding to cyber incidents. Make sure you teach employees what they should do if they receive a suspicious email or link — who they should report it to, how to forward that information, etc.

Your strategy should also include guidance for what people need to do if they make a mistake (otherwise, they may try to cover it up out of fear they'll be punished).

Develop Your Ransomware Response Plan (or Several)

While prevention is the best medicine, there's no way to guarantee that you won't fall victim to ransomware at one point or another. As such, our last "ransomware protection best practice," looks beyond prevention and focuses instead on preparation.

Bridget Quinn Choi, Principal at Booz Allen Hamilton, told Protocol that organizations often have ransomware recovery plans in place, but there are lots of gaps when it comes to response times and achieving business continuity post-disaster. She says that many times, these gaps are driven by unclear objectives, a lack of testing, and a poor understanding of what's expected in an incident response.

After COVID and everything we've seen since those initial lockdowns, the only thing we can count on is more uncertainty.

Putting together incident response plans for different scenarios (i.e. data breaches, compromised backups, stolen credentials) can facilitate smart decision-making and quick action when disaster strikes — no matter what kind of disaster is on the horizon.

At a bare minimum, you'll want to cover business continuity, data protection, and how to respond to a ransomware attack.

But — it's worth noting that cyber incidents come in many different "flavors" and you'll want to consider those nuances as you develop a response plan. Like, how will you:

- Respond to ransom demands?
- Report incidents to law enforcement?

- Inform customers that there's been a breach?
- Check backups and critical systems for infection?
- Quarantine infected systems and files?
- Get up and running?
- Etc.?

Your incident response plan will be informed by your business model, strategy, and the regulations that dictate how these things are done within your industry.

But – you'll want to make sure that you clearly define and document your game plan, communicate it to key employees, and run routine stress tests to ensure that you're ready to fend off threat actors of all stripes – sophisticated gangs, commodity attackers, or something in-between.

Final Thoughts

Look, the best way to avoid becoming a ransomware victim is to be proactive about prevention.


But – as we mentioned back in chapter two, there's always the possibility that ransomware attackers will find some unknown vulnerability or use some new tactic that allows them to bypass your defenses – even if you've done everything right.

Next up, we'll talk about the impact of ransomware on cloud-based apps and assets.



Chapter 6: Is Cloud Storage Safe from Ransomware?

While the cloud is now widely considered safer than on-prem legacy systems, this environment still boasts its fair share of threats. Here, we break down the biggest ransomware risks of doing business in the cloud and share some actionable advice for staying safe in today's complex and chaotic security landscape.



Is cloud storage safe from ransomware attacks? The short answer is, it depends on... well, several things.

Though, we're not sure that this question is worth exploring anymore.

The conversation around "cloud safety" has changed – and whether or not the cloud is definitively safe is beside the point.

See, the cloud has transformed the way we communicate, collaborate, and access information — both at work and in our personal lives. And, there's no going back.

That means, despite whatever risks come with the territory, the cloud is one of the most essential parts of running a business in the "digital age."

It represents the first step toward digital transformation — and the gateway to achieving its biggest benefits: visibility, agility, resilience, and the data-driven decisions and automations organizations need to win in these complex conditions. In other words, you need to be there.

At the same time, you need to be aware of the risks of doing business in the cloud. And — more importantly how to protect your data, your business, and your customers from ransomware attacks. Here's what you need to know:

Biggest Ransomware Threats to Cloud Storage

Ransomware attacks are all over the news — from politically-motivated hit jobs to high-profile data breaches to the rise of ransomware gangs and dark web malware marketplaces.

It kind of feels like becoming a victim is

inevitable.

It's important to understand that, yes, ransomware threats are everywhere. Yes, threat attackers are becoming more coordinated and sophisticated — demanding and receiving higher payouts.

And yes, the enterprise cloud environment has evolved into this sprawling, complex network with thousands of endpoints, configurations, and potential vulnerabilities.

At the same time, most of today's most advanced ransomware attacks still rely on their targets making rookie mistakes. They're entering systems through unprotected software, stolen credentials, and the malicious phishing links that show up in employee inboxes. In other words, ransomware is still a very preventable problem.

With that in mind, let's look at the key ransomware risks orgs should know about before planning their journey to the cloud.

Misconfigurations

According to the National Security Agency (NSA), roughly one in six data breaches can be attributed to misconfigurations. Palo Alto Networks research found that misconfigurations were the cause of 65% of known cloud security incidents.

Even at the low end of that spectrum, preventable vulnerabilities like unpatched systems, disabled monitoring or logging protections, default passwords, and unprotected storage are opening the door to a large number of threat actors.

Per IBM's 2021 X-Force report misconfigured APIs are often responsible for credential exposure via public cloud repositories — with shadow IT contributing to more than half of the incidents researchers analyzed.

Weak identity and access management (IAM)

According to the Cloud Security Alliance Top Threats to Cloud Computing report, insufficient identity and access management is among the top security threats to cloud-based systems.

Palo Alto Networks also found that there's a significant gap between the "principle of least privilege" and the reality of most orgs' IAM policies – researchers found that 99% of cloud roles, permissions, resources, and services granted users excessive permissions – most of which were largely unused.

Cloud ransomware

Cloud ransomware (aka Ransomcloud) is another serious threat to your organization.

Attackers often gain access by phishing individual employee accounts through email or malicious downloads like fake updates – which rely on human-error to create an opening for threat actors to access the organization's cloud storage solutions.

Or – they might take advantage of the file-syncing capabilities common with most cloud storage solutions – files stored on local devices are automatically saved to the cloud and updated when changes are made.

This approach, known as file-sync piggybacking, installs a program that doesn't contain the malware payload. Instead, it runs in the background and installs the ransomware.

Once installed, the user typically receives a pop-up notification that looks like a legitimate permission request from a trusted app (i.e. Slack, Teams) – and if they accept, it activates the payload.

From there, threat actors move laterally through the system, encrypting or extracting data.

Ransomcloud attacks on providers

Hackers don't just target individual organizations – going after the provider has the potential to be much more lucrative.

Threat actors might target a specific cloud provider to identify security vulnerabilities (for later attacks) or launch brute-force attacks that bypass logins and other protections.

Attacks against the cloud provider are especially damaging as they put the entire platform at risk – and if successful, attackers could potentially demand ransoms from all customers that use that service.


These are far from the only threats you need to worry about – but it's a good starting point for making sure you cover all of your bases.

Yes, the Cloud is Vulnerable to Ransomware - No, On-Prem isn't Safer

Another Palo Alto Networks report forecasts that ransomware attackers are evolving their tactics, techniques, and procedures (or TTPs) to be even more cloud-native than they already are.

While that does mean cloud storage is becoming more vulnerable to ransomware – this revelation doesn't set off any major alarm bells.

As cloud adoption continues to ramp up, it only



follows that threat actors are responding to that shift by making some tweaks to their approach. It's common sense.

Many orgs, particularly those operating in industries like professional services, health care, banking, wealth management, etc. have long followed the common wisdom that the best way to protect sensitive information is to keep things analog.

But — big data has gotten way too big for any organization to manage via spreadsheets and physical filing systems.

These days, avoiding the cloud out of fear doesn't keep you safe from ransomware. In fact, it prevents you from realizing critical benefits such as cost-savings, real-time insights, and the ability to leverage AI and automation only made possible by migrating to the cloud.

It also opens the door to several risks that stand to do much more damage than the typical cloud-based attack. For instance, it's harder to detect and respond to threats quickly enough to mitigate potential damage.

It's also harder to protect and manage on-prem data — not to mention verify its integrity, ensure that it meets regulatory, auditing, or consumer privacy requirements. All of which can lead to serious reputational, financial, and legal damage — or even force your business to shut down.

The bottom line? On-prem systems are a liability.

Without the cloud, companies can't meet customer demands or keep up with competitors — let alone protect themselves against a new class of cyber criminals, who, let's face it, have already mastered the latest cloud-based tech and their intelligent capabilities.

How Cloud-Based Solutions Keep You Safe From Ransomware Attacks

While cloud storage is vulnerable to ransomware attacks, your best defense against threat actors lies with the same technologies already transforming other key parts of your business.

Think — data management solutions, advanced analytics, AI, machine learning, and automation. A few examples:

End-to-end visibility — and end-to-end protections. Similar to how cloud-based ERP systems centralize your data and make it easier to manage your business, a unified platform and end-to-end visibility represent the first line of defense when it comes to protecting against ransomware and other security threats.

Before migrating to the cloud, e-commerce company, QNET regularly dealt with threats to its on-prem infrastructure — which housed valuable customer data like credit card numbers and identifying details. Weekly DDoS attacks led to significant revenue losses and downtime — and left the company vulnerable to data leaks and phishing attacks.

CISO Egal Egal explains that while QNET had invested in several best-in-breed security solutions (from different vendors), none of those products could provide an end-to-end view of the entire IT environment.

CTO Ameer Deen adds that the lack of visibility had a chilling effect on his team — they were afraid that any efforts to respond to incoming threats might make things worse.

QNET replaced those third-party security tools with Microsoft 365 E5 and migrated IT operations to Azure. Today, Deen says the company is able to make informed, proactive decisions that strengthen its security posture — all thanks to Microsoft Defender for Cloud, Defender for Endpoint, and Sentinel.

AI-driven insights. AI-powered XDRs (extended detection and response) provide unified threat intelligence across every end-point in your ecosystem. They work across products, services, and clouds, support process automation, and help IT teams identify threats — and perform deep investigations to better understand those threats in full context.

Different orgs will also use different types of analytics solutions to identify and act on cyber threats based on factors like business model, regulations, and the unique risks of operating within a specific industry. For example, a financial services firm might use AI insights to mitigate fraud risks or detect unusual transactions and behaviors.

Automated enforcement, detection, and response. Automation also plays an important role in protecting your company against cloud-based attacks — it's used to prevent, detect, contain, and act on incoming threats.

For example, independent insurance agency Martin & Zerfoss implemented Defender for Business to consolidate its fragmented security solutions and safely enable remote work.

At the time, the company hadn't fully migrated to the cloud — citing concerns about their lack of expertise and challenges keeping customer data safe.

Combined with Azure Active Directory, Defender for Business gives Martin & Zerfoss a comprehensive view of all devices, users, and

systems both on-premise and in the cloud.

Defender can automatically raise alerts and prioritize actions, while automated investigation and resolution features streamline threat management and empower users to quickly intervene, if needed.

Finally, Deloitte brings up a critical point: without proper implementation, oversight, and governance, the transformative capabilities of AI/ML and automation expose serious vulnerabilities — opening the door to bad actors both inside and outside your organization.

In other words, your cloud-based ransomware protections are only as good as your organization's underlying data, policies, and cybersecurity culture.

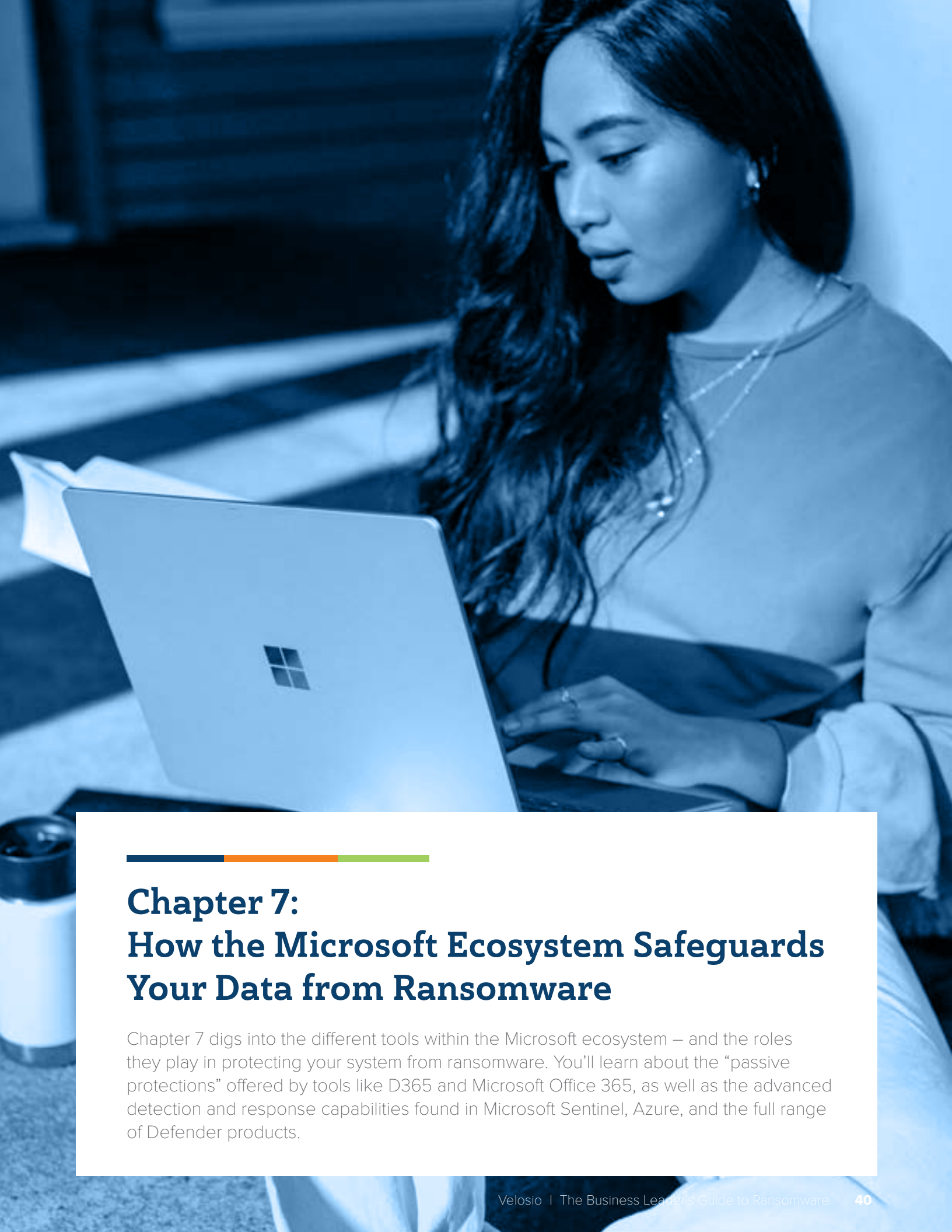
The point is, cloud-based solutions are super effective when it comes to protecting your data — if you have a robust cybersecurity program in place, strong policies, and ongoing support from real human professionals.

Final Thoughts

On the whole, cloud storage is safer than relying on analog or on-prem alternatives. But that doesn't mean it's safe by default. Ultimately, it doesn't really make sense to think about whether or not the cloud is safe from ransomware in such black and white terms.

It's not a question of cloud vs. on-prem — it's a matter of choosing cloud solutions that help you achieve critical business goals AND protect your business from ransomware attacks and other cyber threats.

Speaking of cloud-based solutions, in chapter seven, we take a deep dive into the Microsoft ecosystem and examine the ransomware protections embedded directly in the stack.



Chapter 7: How the Microsoft Ecosystem Safeguards Your Data from Ransomware

Chapter 7 digs into the different tools within the Microsoft ecosystem – and the roles they play in protecting your system from ransomware. You’ll learn about the “passive protections” offered by tools like D365 and Microsoft Office 365, as well as the advanced detection and response capabilities found in Microsoft Sentinel, Azure, and the full range of Defender products.

It's a well-documented fact: Microsoft is all-in on cybersecurity.

There's the Microsoft Compromise Recovery Security Practice (CRSP) — a collaborative effort between Microsoft and its customers to investigate an attack and incorporate key findings into the recovery process (and later, the MS ecosystem).

They have a dedicated Digital Crimes Unit. Internal experts are currently working on an ongoing investigation into ransomware attacks on Ukraine.

And, last year, the company pledged to invest \$20B into cybersecurity initiatives over the next five years — a significant increase from the \$1B in annual security spending that has been the norm for years.

Below, we'll explain Microsoft's approach to fighting ransomware — across its entire ecosystem. Then, we'll shine a light on how those efforts show up in individual solutions like D365, Azure, and the rest of the gang.

How Microsoft Protects Against Ransomware

Per this interactive cloud security piece, Microsoft detects, on average, around 1.5M attempted attacks on its system every single day.

Each recorded attempt, plus billions of data points related to phishing scams, cyber crime rings, ransomware attacks, and threat actor tactics are compiled and studied as part of an ongoing learning process — helping Microsoft get ahead of emerging threats and better protect its customers.

All data is fed into Microsoft's intelligent security graph — where it can be analyzed in context with high-profile attacks, emerging threats, and the evolving global threat landscape.

Key findings are then applied to Microsoft products like D365, Azure, Microsoft 365, and the rest — and as a result, the whole ecosystem benefits from this sort of “group immunity.”

Additionally, Microsoft's fight against ransomware extends beyond the product ecosystem — with experts working to disrupt the growing ransomware economy on four main fronts:

- 1. Holistic ransomware prevention.** Microsoft uses AI/ML and automation to analyze ransomware signals across all clouds, apps, and endpoints. Solutions include Microsoft 365 Defender, Sentinel, and Defender for Cloud — which now comes with adaptive AI protection to defend against human-operated ransomware attacks.
- 2. Detection & response.** Microsoft offers unified Security Information and Event Management (SIEM) and extended detection response (XDR) solutions that provide integrated threat protection across apps, devices, identities, and data and cloud workloads.
- 3. Disrupting the ransomware economy.** Microsoft's Digital Crimes Unit (DCU) is a team of experts that works with law enforcement to disrupt cybercrime, support ransomware victims, and advise on legislative matters.
- 4. Threat intelligence & ongoing research.** Finally, Microsoft's team of dedicated experts study ransomware tactics and develop threat intelligence solutions that, eventually, become embedded into its core product offerings.

Before we move on, it's important to note that while Microsoft's products are loaded with strong security protections, tech alone won't safeguard your data from ransomware.

Now, let's discuss how those cybersecurity investments translate to different parts of the MS stack.

1. Azure

Today's businesses are up against an increasingly organized and sophisticated attacker ecosystem.

Human-operated attacks exploit vulnerable services and network configuration weaknesses to deploy ransomware payloads, exfiltrate data, and steal credentials. And those threat actors move FAST.

That means, you can't afford to leave security gaps wide open. Nor can you continue allowing silos to block the end-to-end visibility you need to detect and respond to threats. Without a unified solution, ransomware can wreak a ton of havoc on your system, before there's any indication of a breach.

Moving to Azure is one of the most effective ways to protect your business from ransomware.

You can manage your entire threat surface from one central hub, leverage AI and machine learning to lock down every asset in your network, and implement granular controls across the whole estate.

Azure Native Protections

Azure spans something like 200 products across a wide range of use cases – data analytics, IoT, compute, cloud storage, AI & ma-

chine learning, and more.

Some solutions are explicitly designed to support cybersecurity initiatives – DDoS protection, data governance, anomaly detection, a key vault for cloud apps. Others focus on other areas like building chatbots or ML models, cloud storage, or DevOps.

Regardless, all 200+ Azure solutions and services come embedded with native security protections, along with dashboards, automations, and custom controls, and tons of built-in intelligence that make it easy to detect, respond to, and recover from cyber threats.

Here are some of the highlights:

- **Built-in security & management.** Visibility is everything when it comes to risk management. See, when businesses are able to detect anomalies, vulnerabilities, and breaches in real-time, they can take action faster and mitigate potential damage. Azure solutions include built-in analytics and controls that provide total observability and reinforce policies and compliance requirements.
- **Multi-factor and passwordless authentication.** Simple security measures like multi-factor authentication (MFA) and single sign-on (SSO) go a long way when it comes to defending against identity-based ransomware attacks. In fact, Microsoft estimates that these basic protections are effective against about 98% of attacks. Azure allows admins to quickly set up MFA, SSO, and passwordless authentication, minimizing risk to Azure resources and the integrations, apps, and devices linked to your account.
- **Azure Firewall.** Azure Firewall protects against common attack vectors like phishing emails and drive-by downloads. It automatically detects threats in unencrypted traffic and uses TLS inspection to ID incoming

attacks in encrypted traffic. Its intrusion detection and prevention system (IDPS) uses signatures to monitor activity, block attempted attacks, and generate alerts.

- **Azure DDoS Protection.** Azure DDoS Protection safeguards apps and resources from distributed denial of service (DDoS) attacks. It continuously monitors traffic patterns and analyzes them against the thresholds outlined in your DDoS policy, while adaptive threat intelligence automatically IDs and responds to attacks.

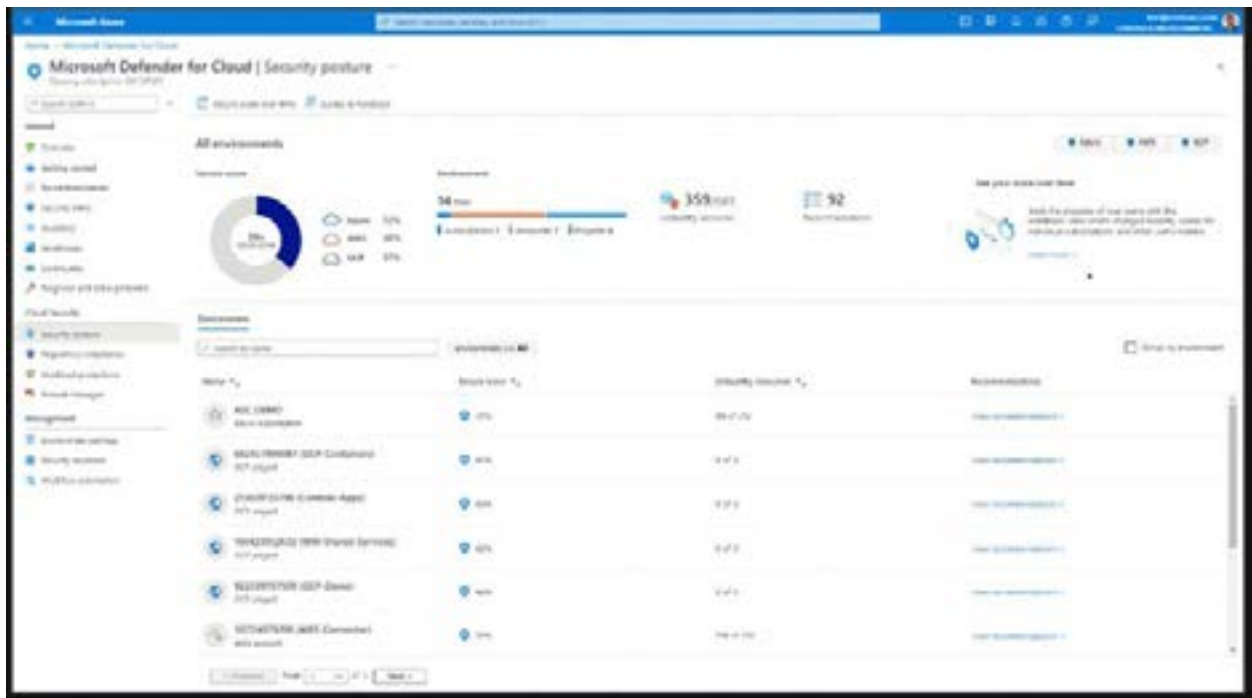
Microsoft Defender for Azure Cloud

Microsoft Defender for Cloud is a unified security system that protects hybrid and multi-cloud

environments from ransomware attacks with built-in extended detection and response (XDR) capabilities, continuous monitoring, and prioritized alerts. Inside you'll find:

- **Secure score.** Defender continually monitors cloud assets and subscriptions for vulnerabilities and aggregates findings into a numeric score, allowing you to understand where your security posture stands at any time.

You can click the score for more details re: which resources need attention. Below, you can see the score breakdown for one specific subscription. You can then navigate to Microsoft Defender for Cloud's Recommendations page to learn how to remediate those issues.



- Threat protection alerts.** Defender for Cloud includes advanced behavioral analytics, machine learning, plus insights from Microsoft’s Intelligent Security Graph – which work together to identify ransomware attacks, zero-day exploits, and other threats. The platform continuously monitors all databases, networks, servers, and cloud services, scanning for incoming attacks and tracking post-breach activities. Additionally, Defender offers interactive tools and contextual insights to help users streamline the investigation process.

- Policy management.** Defender for Cloud allows you manage security policies across hybrid workloads in one central location. Inside the Compliance Center you can add and store custom security policies based on which conditions you’d like to control (and how), then add them to new subscriptions upon installation.



- Automate & orchestrate security workflows.** Integration with Azure Logic Apps allows users to quickly automate workflows that address common security threats. You’ll also have the option to create playbooks for specific actions like triggering automated incident responses, routing alerts to a specific person, or enforcing compliance.

Microsoft Sentinel

Microsoft Sentinel is a cloud-based security information and event management (SIEM) solution that uses built-in intelligence to detect, investigate, and respond to threats across your entire threat surface ASAP. It uses built-in connectors to capture raw data from all users, apps, devices, and servers running on-prem or in any cloud environment.

Key capabilities include:

- **Advanced analytics.** Sentinel's built-in AI analyzes data points across all connected sources against historical data to correlate alerts into incidents. The platform will then look for patterns and signals that point toward known and unknown threats, and will send out alerts when action is required.
- **Threat hunting.** Sentinel includes hunting search-and-query tools built on the MITRE framework that allow you to proactively search for security threats lurking in your data before the system triggers an alert.

- **Investigation.** Sentinel allows you to investigate specific incidents by searching for a specific case or scrolling through the incidents page and from there, leverage its built-in graph to investigate threats with AI. This allows you to identify suspicious behavior at scale, find the root cause of an attack, and understand the scope and impact of malware across your system. Below, you'll see a list of exploration queries for deepening your search based on what you're trying to learn.



- **Notebooks.** Microsoft Sentinel notebooks allow you to do more with your Sentinel data like work with Python ML features or create custom visualizations.
- **Security automation & orchestration.** Microsoft Sentinel also allows you to automate controls and threat responses with its user-friendly playbooks tool. There you'll be able to set custom rules and actions, as well as run plays on-demand.

Microsoft Azure Cloud solutions allow organizations to embrace a proactive, holistic approach to dealing with the rising threat of ransomware. But, it can be challenging to figure out what kinds of protections you'll actually need.

2. Dynamics 365 Sets the Stage for End-to-End Ransomware Protection

Dynamics 365 includes several built-in capabilities that protect your data from ransomware attacks, fraud, and regulatory non-compliance. Users can automate core processes, define rules and controls, and access and act on real-time insights when the system detects a threat.

Modern cloud ERPs house everything from core financials, valuable IP, and sensitive data, to the collaboration apps, customer records, and email accounts employees use every day.

Having that unified system in place is a prerequisite for any kind of digital transformation. You'll need an org-wide data ecosystem and deep integration across your entire network to benefit from now-essential tech like AI, ML, real-time data streams, and intelligent automations.

At the same time, it's a major liability.

ERPs contain mountains of valuable data and power the full spectrum of daily operations, so naturally, they're a frequent target for ransomware attacks.

Microsoft Dynamics 365 consolidates your entire business into a single cloud-based platform – allowing you to manage, control, and secure all apps, devices, accounts, and data on a holistic level. That's a big deal when it comes to defending against ransomware.

We know that threat actors exploit security gaps created by outdated, on-prem tech, and siloed systems, platforms, and processes.

We also know that shadow IT, unsecured endpoints, unsupported apps, and so many other vulnerabilities make it easy for attackers to slide right into your system and do some serious damage.

Cyber criminals often use distributed denial-of-service (DDoS) attacks to target ERPs linked to critical infrastructure or services (Colonial Pipeline is a prime example). Attackers go after public-facing endpoints, rendering resources like power grids or industrial production lines unusable.

ERPs can also be susceptible to phishing, credential theft, or cloud ransomware attacks as they typically connect to file storage, email, and other productivity apps.

Dynamics 365 provides end-to-end visibility across the entire business — an important first step toward building a strong Zero Trust policy.

This allows IT to map out the entire estate — devices, identities, data, infrastructure, etc. — they didn't miss any shadow apps or stray endpoints. Admins can then start monitoring user behavior, identifying vulnerabilities, and analyzing the metadata to learn more about the movement and origins of previous attacks.

From there, they can start adding in multi-layered protections like data encryption, multi-factor authentication, firewalls, SIEM and XDR, etc. to prevent hackers from moving laterally through the system — or worse, hiding in some dark corner for months, waiting to strike.

And later, IT can start actively hunting for threats, investigating incidents, and using real-time analytics to find and fix vulnerabilities that put the business at risk.

Built-In Security Features & Configurations

Out-of-the-box, Dynamics 365 apps come with the same basic application and data security protections including:

- Data isolation
- Data encryption
- Access controls
- Real-time monitoring
- Multi-factor authentication
- Data auditing

D365 Finance & Operations includes everything we just mentioned – but because it's built to support large enterprises, subscribers gain access to Microsoft Lifecycle Services (LCS) for configuring, monitoring, and managing your security environment.

Inside, you'll find several advanced features, embedded AI, built-in automations, testing and diagnostics tools, a business process modeler, and more.

The idea is, that the bigger the organization, the harder it is to identify, much less secure, all of the moving pieces connected to your network. Dynamics 365 Business Central caters to SMBs, which, in most cases, don't need all of these extra features to detect and prevent ransomware attacks.

But – D365 BC offers limited reporting capabilities and few out-of-the-box automations. You'll definitely want to set up the Power BI integration ASAP to ensure that you're able to get that granular visibility into your entire business.

It's not a bad idea to sign up for Power Automate, as well as Azure solutions like

Microsoft Sentinel, Defender for Cloud, or Azure DDoS Protection, either.

Read our post on D365's security capabilities for a closer look at specific features.

Dynamics 365 Can't Fight Ransomware Alone

So, the D365 suite includes both ERP and CRM modules (aka Dynamics 365 Customer Engagement, or CE). For enterprise users, modules are purchased a la carte — allowing them to build a flexible system that aligns with their specific needs.

While D365 modules can be purchased and used on their own, they're part of a broader ecosystem. It's designed so that users start with the ERP “base,” then add on CE apps to support specific business units like sales, HR, or marketing. D365 CE doesn't include LCS – and as a standalone solution, it's siloed-off from critical financial data and operational processes – so benefits are limited to things like access permissions and data encryption.

D365 also integrates seamlessly with Microsoft 365 and can be extended with Azure and the Power Platform. We've talked about this idea of combining Microsoft apps with each other and the core ERP to unlock new capabilities in the past — but that layered construction is crucially important when it comes to cybersecurity.

While every stack is different, you'll need to make sure that threat protection, threat intelligence, automation, and policy enforcement are embedded across your entire network.

To give you a sense of what that might look like, here's Microsoft's Zero Trust architecture:



Whether you opt for D365 BC or F&O, Microsoft Dynamics 365 provides a strong foundation for building a secure digital workspace in the cloud.

It's also worth noting that half-baked security strategies, small configuration errors, excessive permissions, and other cyber missteps can override Microsoft's built-in ransomware protections.

For best results, you'll want to work with a Microsoft partner (like Velosio) that specializes in your industry and has deep expertise in both cybersecurity and Dynamics 365.

Essentially, you're looking for an expert who can help you put together a secure digital ecosystem – with D365 at its core.

3. Microsoft 365

Microsoft 365 protects data and digital resources from ransomware in multiple layers.

The Microsoft 365 apps themselves come with baked-in defenses that protect customer data

from phishing, spoofing, data corruption, and ransomware encryption. For example, OneDrive, Teams, and SharePoint Online all include built-in virus protection, built-in versioning, and recovery tools.

Microsoft Teams lets admins define data loss prevention policies that can be used to block users from sharing sensitive info via channels and chat logs, while SharePoint and OneDrive protect docs and data both in-transit and at-rest.

The list goes on.

But — protecting your system from malware extends beyond the embedded security features that come standard with MS365 apps. Microsoft 365 Threat Protection actually spans a wide range of security solutions — covering all devices, apps, identities, workloads, endpoints, and data.

This includes tenant-level controls (Exchange Online) – as well as a cloud-based service infrastructure designed to prevent, detect, and act on incoming threats.

Here's a look at some of those solutions – and what they can do to protect your MS 365 apps and the data, assets, and workloads connected to those core productivity tools.

Defender for Microsoft 365

Defender for Microsoft 365 is a unified defense suite built for today's biggest ransomware threats. It includes everything from threat detection, prevention, investigation, and response across all identities, apps, email accounts, and endpoints – essentially, covering the entire attack chain.

In a 2020 blog post, Microsoft explains that human-operated ransomware campaigns typically start with unsophisticated “commodity” ransomware like trojans that do set off detection alerts and are then quickly triaged by IT without a full investigation.

Additionally, anti-virus solutions might block the initial payloads – but attackers often deploy different payloads until they're successful. Or – use stolen credentials to enter the system and disable protections.

Defender for Microsoft 365 draws on years of research into high-profile attacks – using key findings to build a solution that addresses all infrastructure weaknesses threat actors might exploit, harden assets, and understand the entire “story” behind each attack.

Inside, you'll find a ton of impressive features. The incident overview portal combines related alerts from all products, apps, and devices into a single dashboard view.



You can also investigate individual alerts within a system-wide incident. For example, here's an alert for suspected credential theft.

For example, here's an alert for suspected credential theft. It tells you the type of incident (in this case, credential access), the severity, technique, and source – plus a brief description of what that all means.

The screenshot shows a Microsoft 365 Defender alert interface. At the top, it says "Alerts > Suspected credential theft activity". The main alert title is "Suspected credential theft activity" with a lightning bolt icon and a note "This alert is part of incident (1136)". A button labeled "Actions" is visible. Below this, a table lists the following details: Severity: Medium; Category: Credential Access; Technique: T1003: Credential Dumping, T1075: Run the Hash; Detection source: EDR; Detection technology: Behavioral. A note in the top right corner states "Automated investigation is not applicable to alert type".

Description
This program exhibits suspect characteristics potentially associated with credential theft. Once obtained, these credentials are often used in lateral movement activities to infiltrate other machines and servers in the network.

Alert process tree

The process tree diagram shows a sequence of processes: `svchost.exe` (parent), `csrss.exe` (child), `cmd.exe` (child), and `cmd.exe` (child). A note at the bottom of the tree reads: "Detected as hash (2a046c22-40c6b6d2) by Windows Defender 4/27/2020 10:00:00 AM. This file detection entry ID: 71".

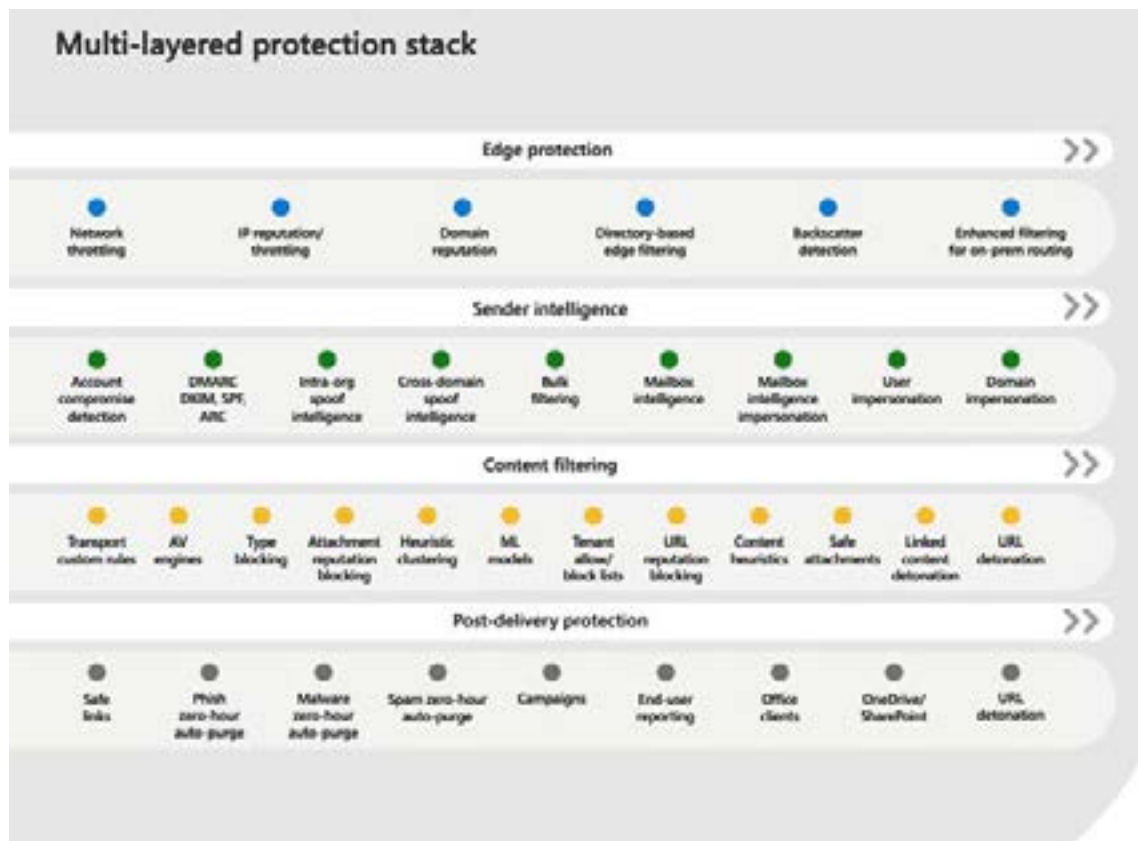
Microsoft 365 Defender allows users to set up AI-driven automations to automatically respond to threats, combine & organize incident data for quick analysis, remediate infected assets back to a baseline security state – without human intervention.

It also supports cross-product threat-hunting – which allows security teams to proactively search for signs of compromise by leveraging institutional knowledge to create and run custom queries.

Defender for Office 365

Microsoft Defender for Office 365 is a cloud-based solution that's part of the broader Microsoft 365 Defender ecosystem, designed to protect against threats to email and collaboration apps.

It uses built-in AI to identify suspicious files and content and analyzes attack patterns and activities to identify ransomware campaigns. Defender for Office 365 uses a multi-layered protection stack, designed to prevent attacks like credential phishing, email compromise, and advanced malware from infiltrating your system.



Defender for Endpoint

Microsoft Defender for Office 365 is a cloud-based solution that's part of the broader Microsoft 365 Defender ecosystem, designed to protect against threats to email and collaboration apps.

Defender for Endpoint represents yet another Defender 365 service, this time focusing on preventing, detecting, investigating, and responding to advanced threats at the network level.

Inside, you'll find advanced cloud security analytics, endpoint behavioral sensors, built-in threat intelligence.

Together, these capabilities enable you to ID threat actor tools, tactics, and patterns that can then be used to trigger alerts and inform your defense strategy.

Defender for Endpoint also includes features that make it easy to discover unsecured endpoints and devices connected to your network.

You can onboard and secure those devices using integrated workflows. Or – investigate potential threats lurking on newly-discovered devices.

Microsoft Intune

Microsoft Intune is a cloud-based mobile device management (MDM) and mobile app management (MAM).

It's designed to help organizations manage and control how company-issued laptops, phones, and tablets are used, as well as define access permissions to critical apps and data.

Intune lets you deploy apps like Teams, Outlook, or Excel to personal and company-owned devices, without threatening data security. You can create custom app protection policies, provision apps from your own private app store, and automate policy deployment across all apps in your network.

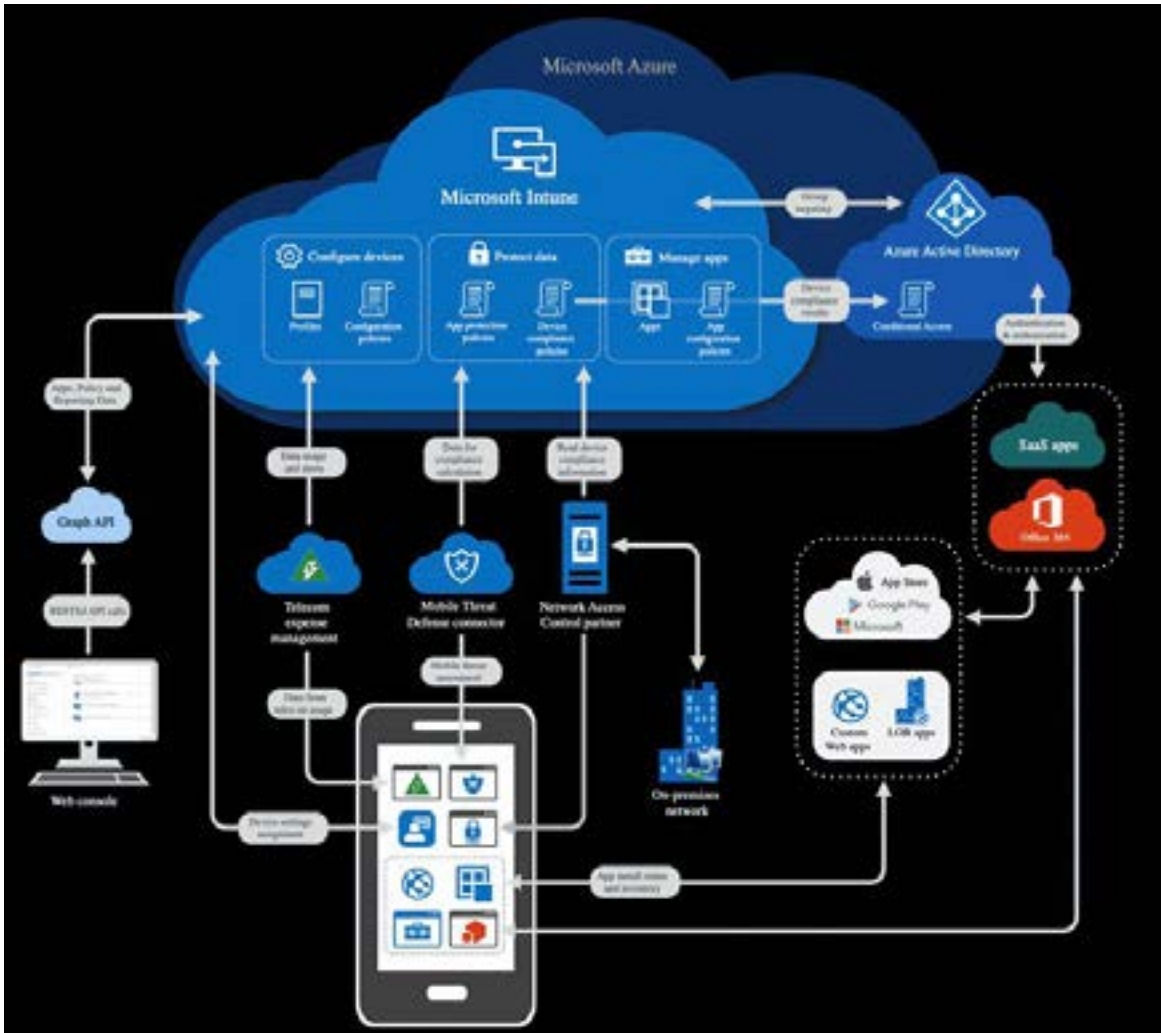
That means, you can set up compliance or conditional access policies, and when they're ready, you can deploy them to all user and device groups. Devices will automatically receive policies – so long as they're connected to the internet.

Intune also integrates with Azure AD, allowing Intune to access AD for device storage and permissions, enable conditional access to email or Microsoft 365 apps, and manage everything from inside the Defender for Endpoint admin center.

For example, you'll define device compliance policies with Intune. The platform evaluates each device against the requirements outlined in the policy and sends status reports to both Intune and Azure AD. Then, within AD, decisions are made re: whether to block or allow access to resources from the device in question.

You can also integrate Intune with Microsoft Defender for Endpoint and review a list of security tasks that identify at-risk devices and prescribe a set of steps for minimizing those risks.

Here's a look at the architecture to give you a better sense of how Intune works with AD, Defender for Endpoint, and the rest of the Microsoft ecosystem.



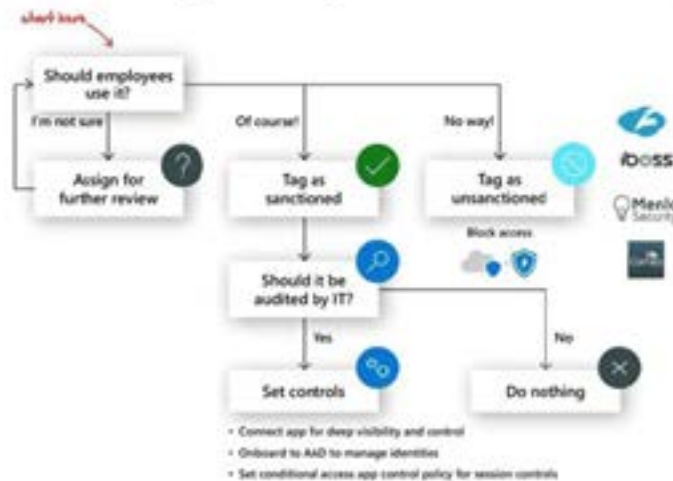
Microsoft Cloud App Security

Another solution, Microsoft Cloud App Security leverages a built-in catalog of over 17k public apps – along with usage data across all users, devices, applications, and IP addresses in your digital environment.

You can use Cloud App Security to discover and identify cloud app usage and identify instances of shadow IT, regulatory noncompliance, unpatched apps, and more.

Here's a graphic that breaks down how you might use this solution to manage newly discovered shadow apps:

Take action: Manage newly discovered cloud apps



Ultimately, Microsoft 365 apps offer many layers of protection that, together, support secure remote work, detect and prevent viruses, block malware, and allow users to respond to threats in real-time.

But – it's important to note that these capabilities only go so far. Even secure apps such as OneDrive, Teams, and Outlook can still be infected by malware.

It's on you to educate your team, implement the right policies, and enable identity, endpoint, and device-level protections (on top of locking down the rest of your digital estate) to effectively protect your business from ransomware attacks.


4. OneDrive

While most attempts fail, ransomware attackers target cloud-based file storage platforms all the time.

Cloud attacks are seriously lucrative – and well worth the effort. Even just one successful attack can deliver a massive payout.

And, in a lot of cases, it also presents an opportunity for cybercriminals to leverage shared vulnerabilities to collect ransoms from other companies using the same cloud provider.

Microsoft's OneDrive for Business (ODB) is well-equipped to defend against these threats. The file storage solution comes with built-in ransomware detection, real-time monitoring,



and extra protections for sensitive data like credit card numbers, IP, and customer and employee records.

Extra Protection for Sensitive Documents & Data

ODB safeguards your files with several baked-in protections — advanced encryption, sensitivity labels, rights management, multi-factor authentication, etc. Microsoft also maintains compliance with privacy laws like GDPR and CCPA, and ISO/IEC 27018 (aka international cloud privacy standards).

Data is protected in-transit via transport layer security (TLS) and Microsoft only permits users to access OneDrive files via secure, authenticated connections. As an example, if you try to access an HTTP site, you'll automatically be redirected to HTTPS.

While at rest, files are encrypted with a unique AES256 key (stored in Azure Key Vault). Microsoft also provides network and identity protections, while sensors, surveillance cameras, and security officers protect its global network of physical data centers.

Additionally, OneDrive and Microsoft 365 include real-time security monitoring systems trained to detect anomalies, issues, and incidents and automatically take action against threats.

However, it's important to note that OneDrive security breaches do sometimes happen — but does that mean OneDrive for Business is a security risk? Yes and no.

Any cloud-based file sharing service can fall victim to ransomware. It's impossible (even for Microsoft) to prepare for every theoretical vulnerability and the threat landscape is constantly evolving.

But — most OneDrive breaches are caused by human error. The best thing you can do is build a holistic strategy spanning everything from training and to insider risk management, and Zero Trust device and identity policies.

Data Loss Prevention & Post-Attack Recovery

While OneDrive for Business provides several features and functions that can help you bounce back from a ransomware attack, let's get real clear about something super important: ODB is not a backup tool.

A quick Google search or scroll through Reddit will immediately highlight that ODB's backup capabilities are an ongoing source of confusion.

MS365 subscribers get 1TB of OneDrive storage for backing up files and photos, plus access to its advanced security features. Which, let's face it, definitely sounds like a backup solution.

However, OneDrive's data loss and recovery protections are designed to serve as a temporary safeguard against unexpected incidents or outages.

Meaning, if you lose your laptop or your account gets hacked you can use Known Folder Move to quickly recover files and get back to work with minimal data loss.

If OneDrive detects any unusual activity, you'll get an alert via MS365. That might mean the algorithm found malware in your system or identified unauthorized file sharing. Or, maybe you delete a bunch of old files from the cloud backup and the system needs to confirm this is an intentional choice.

Users can restore files for up to 30 days after

incidents such as ransomware attacks and breaches, file corruption, or unintentional edits or deletions. But — certain ransomware strains are capable of copying and encrypting a file, then removing the original document — and its entire version history.

File restoration hinges on whether the malware attack occurred within the 30-day timeframe. Meaning, if files were infected 45 days ago, you can't turn back the clock with file versioning, that data is gone.

The alerts should prevent this from happening — but you'll definitely need a more robust (and permanent) backup solution to protect data, support recovery efforts and ensure continuity.

Secure, Seamless Collaboration

OneDrive for Business enforces security best practices, supports seamless collaboration, and provides easy access to the docs and data employees and stakeholders need to do their jobs.

Admins can define security policies at the global level, set expiration dates, create custom passwords, and block downloads — either from unknown sources, specific sites, or just in general.

These controls free end-users from the burdens of enforcing compliance requirements or making judgment calls about what they're able to share with stakeholders on an individual basis.

Users can create, modify, access, and share files from any device or location — even if recipients don't have a Microsoft account.

In that case, users can use SSO, biometrics, or Entra Verified ID — the brand-new decentralized identity platform to verify identities.

They can also use the mobile app to capture data from analog sources (think whiteboards, receipts, and the full spectrum of paper docs).

All data — regardless of source — is searchable, protected, and unified and can be used to inform decisions, identify risks, and develop proactive, agile strategies across your entire business.

OneDrive for Business is part of a broader effort across the entire Microsoft ecosystem to ensure that users stay in control of their data. Its baked-in security protections are seriously impressive but they can't protect your business on their own, nor can they make up for poor cyber hygiene.


5. Microsoft Entra

Microsoft Entra is a brand-new product family that includes all identity and access management capabilities — the familiar Azure AD, plus new CIEM and decentralized identity protections.

It's a rebrand of Microsoft Identity Solutions — designed to tackle identity and access management (IAM) on multiple fronts — without adding friction to workflows and daily interactions.

Crucially, Entra was built with modern cyber threats in mind — ransomware gangs, nation-state attacks, cloud-specific vulnerabilities, and so on.

Microsoft's 2021 Cyber Signals report declared identity the "new battleground." Researchers say there's this "dangerous" gap between identity-focused ransomware attacks and preparedness of would-be victims.



Proofpoint researchers seem to agree, noting that Microsoft 365 and Google Workspace accounts and single sign-on (SSO) apps are heavily targeted by ransomware attackers because they house valuable data, user credentials, and business communication logs.

Threat actors still rely on simple tactics like phishing and social engineering to steal easily-guessed (or default) passwords.

What's especially troubling is, even if just one person sets their password to something like "password," hackers can penetrate the network and access even more valuable credentials, steal and encrypt even more data, and, in turn, demand higher ransoms from multiple targets.

All three Entra solutions protect identities against ransomware attacks across complex, multi-cloud environments. Here's how:

Azure Active Directory (AD)

Microsoft Azure Active Directory (aka Azure AD) is a comprehensive, cloud-based IAM solution designed to support application access permissions, directory management, and advanced ID protection. Azure AD offers a unified platform for managing and securing identities across all user groups, apps, and devices — both on-premises and in the cloud.

Real-time insights into content usage, incoming threats, and unusual behavior allows users across the entire organization to avoid blind spots that put them at risk — and take the appropriate action.

IT teams benefit from greater visibility, tighter controls, and built-in automations that simplify and reinforce identity governance, provide secure, hands-off user provisioning, and apply adaptive access policies based on real-time risks.

On the end-user side, Azure AD actively supports team productivity. SSO, for example, allows employees, partners, clients, customers, etc. to access everything they need with one login.

There's also the option to go passwordless — using biometrics to access critical apps and info. Either way, users aren't spending their time juggling a bunch of usernames and passwords. Nor are they signing into multiple apps every day.

Entra Permissions Management

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution for monitoring, managing, and protecting identities and permissions across all apps and services in one centralized hub.

Permissions Management offers granular visibility into all actions performed by every identity, app, or resource and tight IAM controls across all cloud environments (Azure services, of course, but also Google Cloud, AWS, and others) connected to your network.

The platform also makes it easy to assess permissions risk by evaluating permissions against actual usage, track anomalies and generate detailed forensic reports, and establish and enforce right-size permissions based on real user needs.

Microsoft Entra Verified ID

Microsoft Entra Verified ID (currently in public preview) is a decentralized identity solution that helps orgs quickly issue and authenticate users credentials. Think — personally identifiable information (PII), certifications, degree requirements, work history, and other key details. And at the same time, ensures that individual

users are in control of their own identities – and protected on an individual basis.

Decentralized identity represents a shift away from companies owning all credentials to users controlling their digital identities themselves.

Instead, a decentralized network of businesses, institutions, organizations, governments, and individuals serve as issuers and verifiers for verifiable identity credentials, while the end-users themselves grant permissions and manage access through their own digital wallet.

How it works is:

- Each verifiable credential is a signed container of identity data provided by an organization (the issuer) that has the authority to verify identity claims and grant digitally-signed credentials to end-users.
- Users will then receive the request for credentials (sent by the issuer), approve and sign the claim cryptographically using their private key, then pass it on to the verifier.
- The verifier is another (independent) organization responsible for requesting proof of ID claims and making sure that user credentials satisfy requirements.

This diagram breaks down the basic relationship between these three players (check out Microsoft’s Decentralized Identity white paper for full details re: what, why, and how Verified ID works):



Per a recent Bank Info Security article, the rise of decentralized ransomware attacks demand decentralized protections. When orgs rely on centralized IAM solutions and perimeter defenses (i.e. network-level firewalls), any type of ransomware — be it well-known strains or new variants — can cause significant damage.

If attackers steal credentials from a single user and deploy malware capable of spreading, it can rip through your entire system, your customers’ systems, and, potentially, the systems of any other orgs that use the same apps or cloud provider.


When protections are applied at the individual level, and verified by a trusted, independent party, malware can’t move laterally through your system. That makes it much harder for attackers to tunnel into a different network with shared vulnerabilities.

Together, the three Entra apps help users beef up ransomware protections per Zero Trust best practices – without introducing unnecessary complexity or friction to administrators or users.

Businesses can build a comprehensive environment for managing credentials, verifying user identities, and making access decisions based on real-time threat assessments. But – they’ll need to map out your threat landscape and lock down every endpoint to capture the full range of benefits the Entra suite has to offer.

6. SharePoint

SharePoint simplifies collaboration and knowledge sharing between internal and external stakeholders by offering a secure environment for building custom websites, apps, portals, even your own “modern intranet.”



Built-in security protections make it easy for users to manage access permissions and devices, secure sensitive customer data, and block incoming ransomware attacks.

Many organizations have amassed all of these cloud-based tools — some complementary, others competing — in an effort to address the needs of every department, team, or stakeholder group.

What ends up happening is, businesses are stuck managing ever-expanding data sets across multiple silos. And as a result — open the door to ransomware attacks and other threats that put the business at risk.

SharePoint directly addresses issues like poor alignment, lack of visibility, and productivity-blocking silos. Instead, users get a unified solution that allows organizations to build custom websites, portals, newsfeeds, and knowledge bases for every project team, business unit, partner, or customer segment.

What's more, users can securely collaborate with internal and external stakeholders — on any device, no matter the location.

In this post, we'll discuss SharePoint's built-in security features and the platform's role in strengthening your overall security posture.

SharePoint's main benefit is that it makes it easy for users to access the information they need to do their jobs. The platform aims to simplify collaboration and knowledge sharing — offering a safe environment for building custom websites, apps, portals, and knowledge bases.

Built-in security features allow admins to secure sensitive customer data, manage users and devices, and defend themselves against incoming cyber attacks.

Here's a quick look at how SharePoint protects your company from ransomware.

Centralized Administration

According to recent Proofpoint research, SharePoint, OneDrive, and other enterprise cloud services are prime targets for phishing and brute-force attacks — with threat actors gaining entry via compromised or default accounts. What's more, Proofpoint researchers found, is once ransomware attackers infiltrate the system, they can encrypt SharePoint and OneDrive files in a way that makes them impossible to recover from autosave versions or the recycle bin.

Microsoft automatically takes measures to protect your data — your data is protected both in-transit and at-rest, data is continuously validated, and there's baked-in virus detection and version control capabilities. But — those protections aren't enough on their own — particularly if identity and access management (IAM) isn't a priority.

SharePoint Online allows users to manage content, data, sites, and users from a single interface — either in the Microsoft 365 admin center or via PowerShell (instructions for getting started here).

Admins can manage sharing setting at the organization-level, set different authorization levels, and define collaboration parameters with guests on documents, teams, and sites.

Admins can set rules that control how information is accessed and shared, as well as automate tasks like data governance and document management. And —they can incorporate audit policies and compliance requirements into your SharePoint settings.

That way, team members can work faster – without constantly worrying about security issues or inadvertently introducing your org to cybersecurity risks.

Seamless & Secure Access

Diginomica discusses the need for organizations to create “curated clouds,” where individual cloud solutions are aligned with end-user, department, and org-wide goals.

Essentially, orgs should focus on building cloud environments for each stakeholder group designed around localized requirements, needs, and functions – with predefined service levels and expectations re: data use, access, etc.

Per this recent Microsoft security guide, striking the right balance between security and employee productivity is key when it comes to maintaining strong security protections in a complex digital environment.

SharePoint allows business leaders to do just that. Admins can easily provide all users with seamless access to the apps and services they need in a customizable environment – without the risks associated with excessive permissions.

For example, Blue Diamond Growers (BDG) moved from SharePoint 2010 to SharePoint Online as part of a broader cloud migration effort.

BDG’s Microsoft partner quickly rebranded all of BDG’s sites using SharePoints themes and custom web design app and trained employees to use the Teams integration – which enabled the almond supplier to fast-track adoption and boost collaboration.

While the initial goal of this project was to

improve productivity and collaboration, BDG was able to strengthen data security, automate critical business processes, and better protect against threats thanks to features like Microsoft Defender and Single Sign-On.

Reporting Tools for Monitoring Suspicious Activity

Today’s business landscape is defined by sprawling data sets, distributed workforces, and thousands of apps, devices, and services.

Securing the entire digital ecosystem has never been more challenging – nor so critical for protecting against ransomware attacks and other risks that could easily take down your business.

According to a recent Splunk report, security teams must have a global view of all assets, teams, and data within the business. See, without end-to-end visibility, security pros spend a good chunk of their time reacting to incidents after the fact. Which means financial losses, downtime, and reputational damage are inevitabilities.

SharePoint’s baked-in reporting tools like audit logs and usage reports play a key role in preventing and detecting ransomware attacks – but you’ll likely need to invest in solutions like Power BI, Microsoft Sentinel, Azure DDoS Protection, or Defender for Cloud to empower IT teams to take action against threats in real-time.

Ultimately, SharePoint works best when combined with other Microsoft solutions. For instance, the Power Platform provides granular insights and custom automations that can help orgs better detect and act on incoming threats. Azure makes it easier to work with data and test for vulnerabilities. Entra tackles all things IAM.

The list goes on, but the point is, SharePoint is one of many layers that prevent threat actors from breaking into your system.

7. Power Platform

The Microsoft Power Platform allows users to work with data and build custom apps, websites, and automations that protect your organization, surface detailed insights that detect anomalies and threats in real-time, and embed security protections into your creations.

All Power Platform solutions operate on a security model provided by Microsoft Dataverse that protects data privacy and integrity, while at the same time, makes it easy for users to access and share critical information.

Individual users are only able to work with data assets they're already authorized to use, and built-in security features ensure that your citizen developers aren't empowering hackers to wage a full scale ransomware campaign on your system — or your customers'.

Here's how Power BI, Power Automate, and the rest of the gang help keep your business safe

from ransomware on multiple dimensions:

Power BI

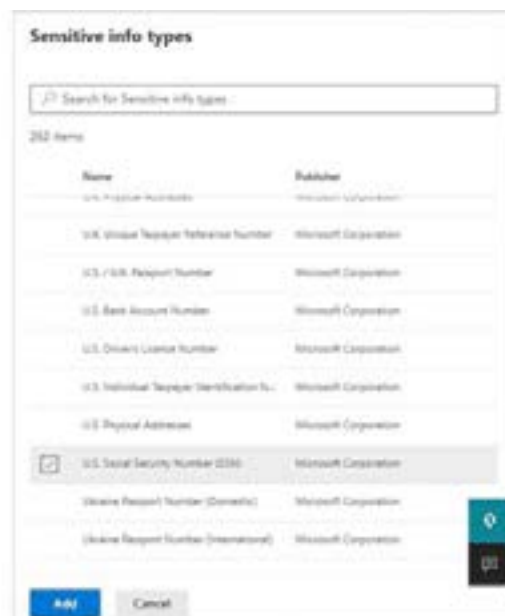
From a ransomware standpoint, Power BI gives users the granular visibility they need to detect, prevent, and respond to ransomware attacks across the entire security estate.

It's embedded with industry-leading security features like data encryption, real-time monitoring, and sensitivity labeling — offering additional protections for valuable data.

Power BI's new data mart feature allows users to run relational database analytics, build reports and semantic models, and manage end-to-end data ingestion, prep, and SQL exploration.

You can also control data governance with row level security (RLS) and sensitivity labels.

And —you can track data lineage and metadata by integrating data marts with Microsoft Purview. You can also make data available to specific groups and “certify” and promote specific data marts so users can find the trusted insights they need.



You can incorporate Power BI data into existing tools like Outlook, PowerPoint, Teams, and Dynamics 365 and use the same data protections (i.e. sensitivity labels, data lineage and impact analysis) you'll find inside MS365 across all Power BI dashboards, reports, and dataflows.

Microsoft also just launched DLP policies for Power BI, which automatically detects sensitive data uploads using the built-in data loss prevention (DLP) policies you'll find inside SharePoint, Teams, OneDrive, etc.



Power Apps

According to Microsoft's guide to planning a Power Apps project, security protections come into play during the architectural design stage (after you've completed the planning phase and come up with a conceptual design).

This is where you'll figure out how to store your data, what your data structure will look like, and how to integrate the app with existing apps and systems. There are four different security layers you can set up in your app:

- **App-level security restricts access to the app, but doesn't protect data storage.** How data is secured depends on the built-in capabilities of the data sources linked to the app.

- **Form-level security is used to control access to model-driven app forms.** This allows you to grant or restrict access to specific forms, as well as how they can view or modify data based on their role.
- **Record-level security is used to assign access to specific records.** There are four different types of access you can choose from: create, read, update, and delete, aka CRUD (cute, right?). You can also set additional privileges within Dataverse to define which tasks users with access to a particular record can do.
- **Field-level security allows you to set up security protections within a single record** — much like if you were to define a security setting for a single column in an Excel sheet.

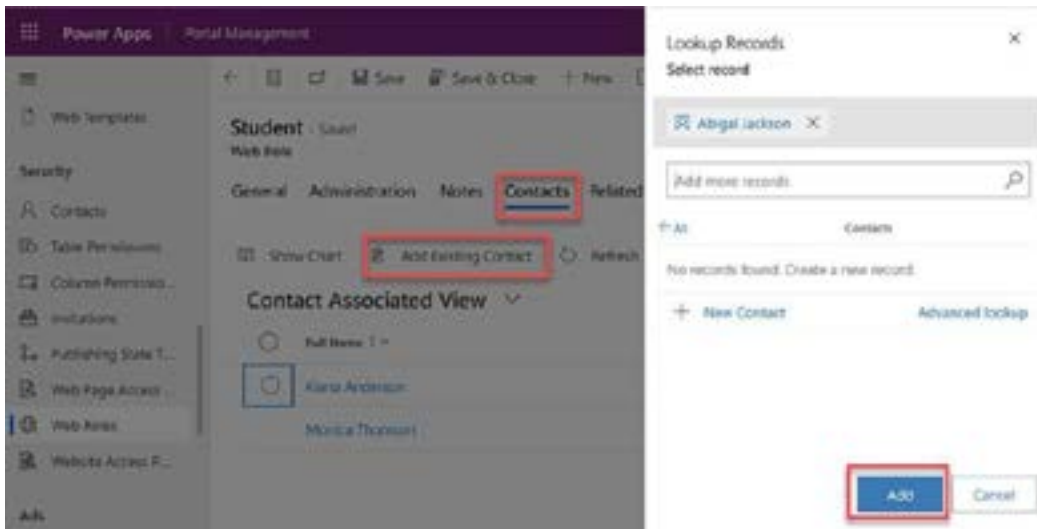
Power Pages

Power Pages, just launched in public preview, is a secure low-code website builder you can use to create, publish, and host web portals, external sites, and private intranets.

Like Power Apps, Power Pages has a robust security model in place to protect critical data — though the specific security features are slightly different.

- **Authenticate users.** As with Power Apps Portals, you'll configure authentication in Power Pages from your Dataverse contact records. The platform also integrates with Azure Active Directory, LinkedIn, and other authentication providers.

- **Set role-based permissions.** First, you'll need to configure and assign web roles via the Portal Management app. Then from there, you can set table and page permissions to control who has access to specific Dataverse records and pages by associating them to individual web roles.



Provide external access. You can invite contact to sites/portals, set invitation expiry dates, if needed, and automatically assign invitees to an account upon activation. And — you can also configure external contacts using local authentication via Azure AD.

Power Automate

In a recent white paper, *Evolving Zero Trust*, Microsoft explains that automation plays a central role in protecting your business against ransomware, malware, and other cloud-based threats.

Security solutions with intelligent automation capabilities are helping organizations safeguard critical assets against ransomware attacks. It's becoming impossible for humans to manually patch systems, detect threats, and take proactive action before disaster strikes.

Power Automate users can strengthen their security posture with custom workflows that perform routine tasks like resource provisioning, onboarding, and access reviews.

There's also the AI Builder, which allows you to build, train, and publish different types of AI

models — incorporate them into custom apps. Models can be trained to predict outcomes, classify data, and carry out automated workflows via Power Automate.

So, you might integrate security data from various sources to build a solution that can automatically flag unusual behavior, detect malware, or raise alerts if there's evidence of fraud. Or — leverage AI and ML to enforce data governance or carry out sequences that prevent, detect, contain, and act on incoming ransomware threats.

Power BI unlocks custom insights, providing granular visibility into the security metrics most valuable to you. Power Automate can be used to detect and respond to threats, reinforce policies, and protect data.

And, low-code platforms, Power Pages and Power Apps make it easy for your teams to quickly build and deploy solutions without creating an opening for threat actors.

Final thoughts

As you can see, all of the products and services in the Microsoft ecosystem are embedded with cutting edge ransomware protections. At the same time, it's important to remember that you can't rely on built-in protections alone.

You'll also need to make cybersecurity part of your culture — and prioritize training and development initiatives outside of the IT department.

Beyond that, cybersecurity hinges on good data, end-to-end visibility, and tight integration across the entire digital ecosystem.


The point is, there are so many moving pieces that must come together to build the kind of modern, robust ransomware strategy you need to protect your business. Microsoft's modular ecosystem can help you achieve that — quickly, and without any unnecessary complications or expense.

In chapter eight, we'll discuss some of the ways you can protect on-premises Microsoft Dynamics systems — as you transition to the cloud, of course.



Chapter 8: Protecting On-Premises Microsoft Dynamics from Ransomware

There's no denying that your business is safer in the cloud, the fact is, many businesses still rely on legacy systems to perform their day-to-day work. In this section, we focus on how to protect on-prem Microsoft Dynamics ERP systems from ransomware threats both from the cloud and within your organization.



Despite what some legacy holdouts may still believe, on-premises systems aren't more secure than their counterparts in the cloud.

On-prem tech is vulnerable to many of the same threats facing cloud-based apps and services — and then some. It's now seen as a liability — posing a serious threat to customers, partners, and even your org's chances at long-term survival.

Companies using legacy ERPs also face additional risks due to silos, blind spots, and a lack of real-time data syncing. That, in turn, means they can't detect and respond to threats quickly enough to ensure a quick recovery — and avoid the devastation of a fast-moving attack.

Without proper protections in place, cloud based ransomware can infect on-prem systems via phishing and credential theft, brute force and backdoor attacks, and other more sophisticated methods.

In these next few sections, we'll explain how to protect on-premises Microsoft Dynamics (and other legacy tech) from ransomware, as you nail down the logistics of migrating to the cloud for real.

How ransomware impacts on-premises systems

Okay, it's rare for a company to operate without relying on any cloud-based tools.

Even if you're still using an on-premises Microsoft Dynamics ERP, your company probably conducts some business in the cloud.

Consider the tools your teams use on the job. They're definitely using email, and likely a handful of productivity apps like Microsoft Teams, Trello, or Google Workspace. Your sales team probably uses some sort of cloud CRM like D365 Sales or Salesforce. And, maybe there's an HR person that uses a payroll integration that syncs payment data back to your core financials. You get the idea.

What that means is, your on-prem ERP is directly linked to the cloud — which means that data is now exposed to the same risks facing cloud storage solutions and web apps.

Cloud services are managed by a vendor, security is included in your subscription.

It's rare that the average SaaS tool is the source of a serious breach or ransomware attack, given that it's in your provider's best interest to protect its users from data leaks, fraud, and malware — because, well, it's bad for your business.

Still, breaches happen. Vulnerabilities always exist, and sometimes, threat actors exploit them before vendors have time to come up with a fix.

Look at the SolarWinds attack. Trojanized code was inserted into a file later distributed as part of an Orion software update. Thousands of customers downloaded the malware, and the company had no idea for several months — until one customer's security system picked up on signs there had been a breach.

Keep in mind, malware infections spread in both directions. Compromised on-prem files can propagate cloud environments and infect apps and services containing customer data, communication logs, trade secrets, IP, etc.

Lock down legacy systems

Older, on-prem systems tend not to include security features that come standard with newer, cloud-based solutions like endpoint detection, antivirus protections, and adaptive threat intelligence.

Unfortunately, those poor protections make it easy for attackers to run the entire ransomware and data exfiltration attack chain from one system, with little effort. As you might imagine, finding these glaring vulnerabilities in the wild is a small victory for threat actors – a chance to make some easy money.

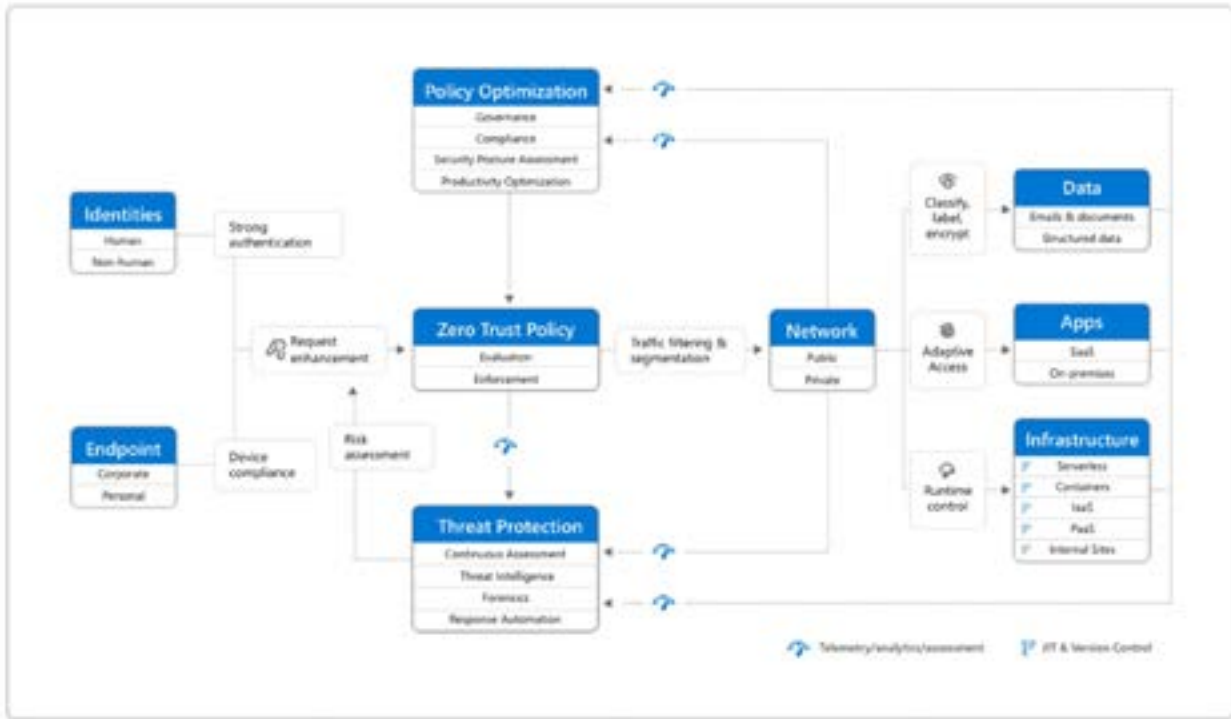
Though legacy ERPs and old school security solutions can be a huge liability, there's a lot you can do to harden your security posture. Microsoft recommends starting with some general best practices, such as:

- **Conducting routine security assessments.** Use tools like Microsoft Secure Score to continuously monitor and improve your security posture.
- **Blocking downloads to risky or unmanaged devices.** Blocking downloads to risky devices can help you avoid things like data theft, insider threats, and threat actor interceptions.
- **Segmenting your networks.** Firewalls work to block lateral movement – preventing malware from spreading between environments and minimizing the potential damage of an attack.

- **Protect data on all physical devices.** Requiring complex passwords, using multi-factor authentication, encrypting data, and limiting login attempts.
- **Train employees in basic cyber hygiene practices.** Make sure everyone knows how to respond to a cyber incident, comply with regulatory requirements, and how to properly erase data so that it doesn't become a liability.
- **Establishing conditional access policies and session controls.** You might also set conditional access policies that ensure that only authorized users and devices have access to apps.

Beyond those basics, you'll need to establish end-to-end coverage across the entire network – including all endpoints, identities, devices, machines, apps, databases, subscriptions, APIs, connectors, configurations – anything linked to your digital footprint.

If you're not sure where to look, we recommend checking out the Zero Trust framework, which breaks coverage into individual "security pillars," pictured in the screenshot below:



Unify all assets, apps, & resources in one hybrid environment

The first step toward gaining control of your security posture is combining everything into one hybrid environment. That way you can manage and secure your entire ecosystem from a "single pane of glass."

As an example, when butter giant Land O'Lakes sought to improve its security posture, the company needed a way to combine old and new solutions in a flexible hybrid workspace – without the friction and frustration of more fragmented solutions.

Land O'Lakes combined several solutions to simplify security operations across its complex landscape. Together, Microsoft Sentinel and Defender for Cloud provide a single source of truth for monitoring and securing the entire digital estate.

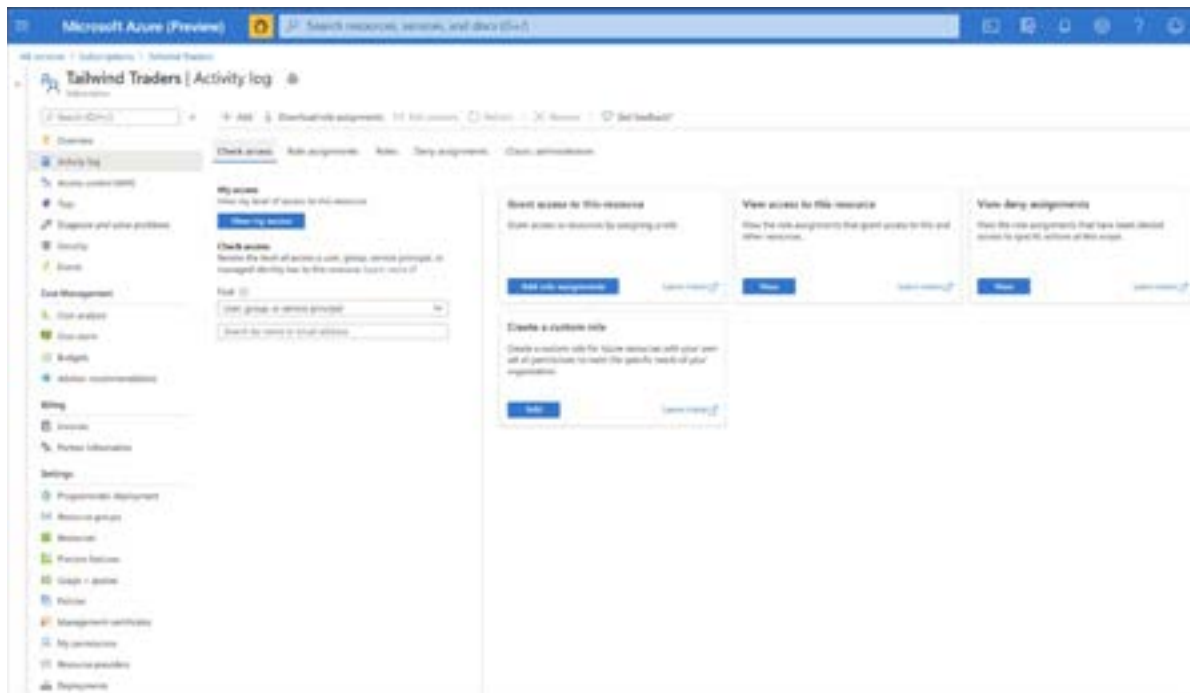
They also use Azure Kubernetes Service (AKS) to proactively manage massive datasets stored in secure containers, while Defender for Containers and Sentinel offer granular visibility into the company's expansive container ecosystem and its workloads, spanning a diverse range of environments.

Defender for Cloud made it possible for the Land O’Lakes team to find and fix bad containers before deployment, while Azure DevOps allowed them to establish, automate, and enforce best practices preventing the kinds of minor errors that cause problems later on.

Senior Security Engineer Michael Marsh said the company immediately saw the “connectedness” of the Microsoft environment a major advantage over other solutions – noting it picked up signals other stacks may have missed.

You might also look toward something like Azure Arc, which is designed to unify disparate apps, tools, machines, and devices – online and off – in one cohesive hybrid ecosystem, making it easier to develop, manage, and secure all resources from one place.

Arc aggregates security data from all connected resources – whether that’s “ephemeral” Kubernetes clusters, Linux Servers, on-prem Microsoft Dynamics software, or the homegrown legacy apps still attached to your stack.



There’s also Microsoft Defender for Servers, which is an add-on subscription for Microsoft Defender for Cloud. It’s a package of enhanced features designed to help organizations better manage on-prem machines in hybrid environments.

Enable real-time monitoring

Within the Microsoft ecosystem, you’ll find several tools that enable real-time monitoring across your entire threat landscape.

Microsoft Sentinel offers continuous monitoring across all assets – with a core focus on intelligent detection and response.

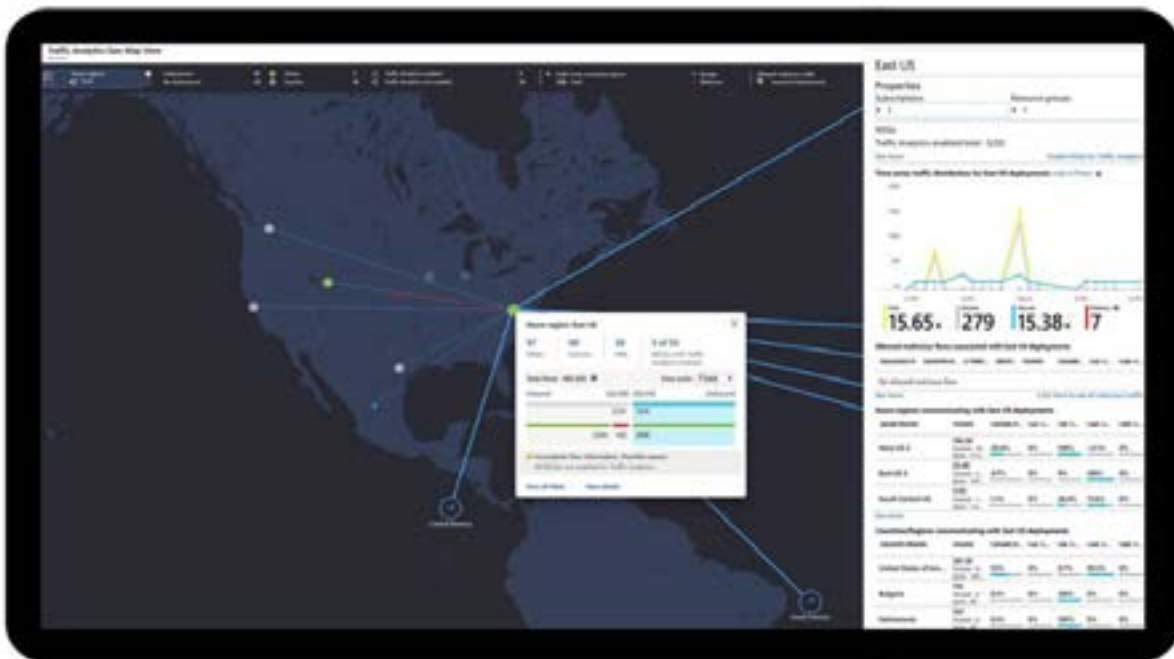
Defender for Cloud protects hybrid environments and workloads – continuously scanning systems for vulnerabilities. Its built-in AI then serves up recommendations for fixing issues – and even suggesting security policies you can implement and enforce across all resources in a matter of clicks.

Defender for Endpoint, on the other hand, offers full detection coverage across the entire attack chain, discovering endpoints and devices connected to your network. Azure Monitor is used mainly for optimizing asset performance – offering a unified solution for storing, monitoring, and managing the operational telemetry across your entire

network – and the apps and infrastructure that support critical operations.

Users can capture data from both on-premises and cloud environments, set up alerts, and use ML-powered insights to identify problems and explore solutions.

In the screenshot below, you can see Azure Monitor's Map View, which allows users to monitor, diagnose, and resolve networking issues without logging into individual virtual machines (VMs). They can also trigger packet captures, analyze group flow logs, and establish tighter network controls based on the platform's super granular performance insights.



As the Land O'Lakes case study made clear, Microsoft's Security tools were made for layering.

Each security tool in Microsoft's expansive stack captures different insights and applies them in different ways – protecting your digital estate from different angles – be it governance, DevOps, detection, discovery, or response.

Ultimately, the tools you end up with depends on your environment. For example, a company that leans heavily on IoT devices and legacy equipment will have different needs than a professional services firm mostly operating in the cloud but still using a handful of on-prem databases.

Keep up with patching, updates, & routine tasks

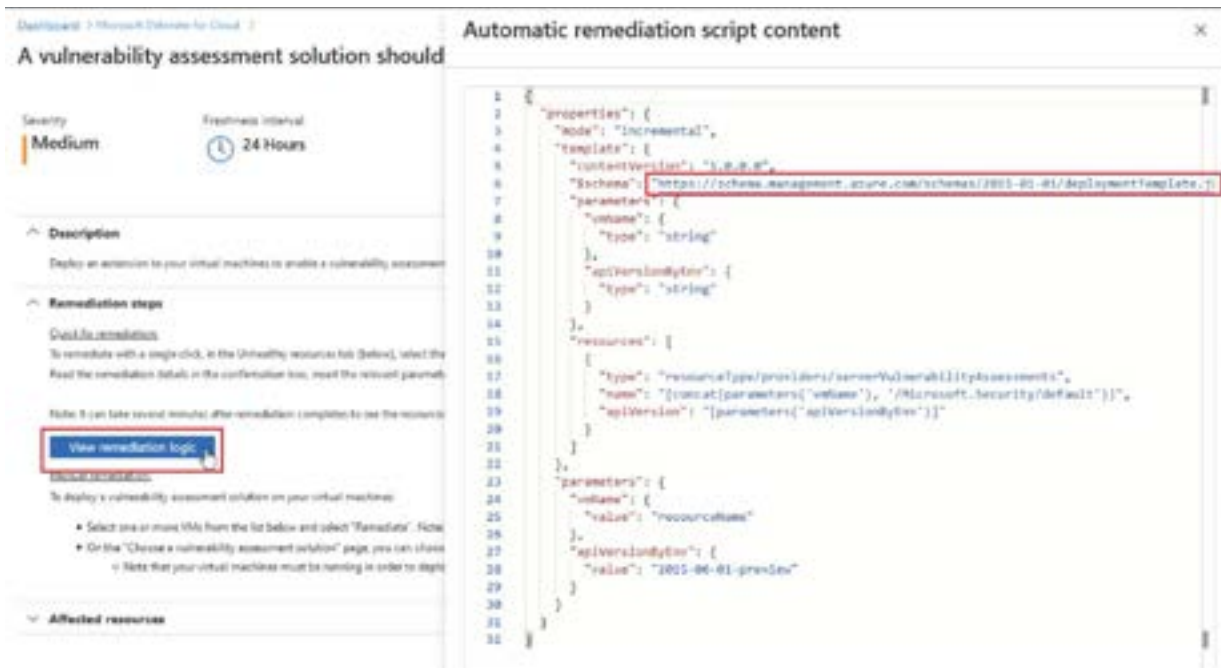
One of the advantages of using a cloud-based ERP like D365 is that updates happen automatically — minimizing the risk that unsupported legacy apps or one missed update will leave your entire organization vulnerable to an attack.

If you're using an on-prem version of Dynamics, you'll need to be extra vigilant when it comes to locking down their system, performing backups, and scheduling updates. Always install all security updates ASAP, as they fix known vulnerabilities.

You'll also want to automate and streamline processes whenever possible. It's way too easy to skip that routine update, fail to remove PII data per consumer privacy regulations, or overlook that one exposed endpoint that ends up taking down the whole system.

Microsoft offers several options for automating software updates, patches, and performing time-consuming, error-prone IT tasks.

For example, Defender for Cloud, Endpoint, Servers, etc. come with a vulnerability assessment tool that allows users to turn recommended remediation steps into automation scripts.





Final thoughts

Just because you're not 100% in the cloud, doesn't mean you're safe from ransomware attacks.

Regardless of where you are in your journey to the cloud, ransomware represents an urgent threat that needs to be addressed before you do anything else.

That said, hybrid environments can be tricky – particularly when you've got a legacy ERP like Dynamics NAV or AX supporting all of your digital operations. Remember, these solutions were built on last generation's infrastructure, and therefore, aren't equipped to unlock the “transformative” potential that today's solutions have to offer.


From a security standpoint, focusing on unity and coverage should be enough to keep you safe as you sort things out. But – you'll need to move to a cloud ERP to unlock the full range of benefits a proactive, intelligent ransomware strategy can provide.

In chapter 9, we'll take a break from specific strategies to provide some guidance re: anti-ransomware tool selection.



Chapter 9: Guidance for Selecting Anti-Ransomware Tools

This section focuses on identifying and implementing the right ransomware stack for your organization. We discuss topics like defining requirements, evaluating vendors and solutions, testing ransomware tools under various conditions.



Keeping up with the tools and solution providers in an ever-expanding and evolving ransomware landscape is, well, a lot for security teams to take on.

While some security pros might enjoy the process of researching and testing new technologies, these employees are already overwhelmed with day-to-day work.

On top of that, implementing the right ransomware stack is a time-sensitive matter. The more time your team spends evaluating potential solutions, the more opportunities cyber criminals have to exploit vulnerabilities in existing solutions.

Below, we'll discuss key considerations and selection criteria for ransomware solutions — so you can lock down your system ASAP.

1. Define your requirements

Defining your requirements is something you should do before researching any potential solution.

It doesn't matter whether it's a strategic new hire, a managed services provider, or a few choice investments in your ransomware defense strategy, you need to figure out what you're looking for before starting your search.

You'll want to make sure that your ransomware stack addresses the full spectrum of risk vectors — and that it aligns with the specific needs and challenges of your business.

Think — identity and access management, threat intelligence, security automation, and so on — as well as any requirements specific to your industry, business model, or how you run your business.

For example, if you operate in an industry with strict compliance requirements (i.e. financial services, healthcare) or handle a lot of valuable customer data, trade secrets, or IP (i.e. professional services, tech, retail) you'll want to look for solutions that can help you meet those additional requirements — say, automated data governance or regulatory compliance.

Look at your entire system (we're talking: performing a full-on audit) and make sure you can answer the following questions:

- What solutions are already in place?
- What are your security goals?
- What's missing?
- Which solutions are falling short? Why?
- Is it an issue of fragmentation? Poor coverage?

At this initial stage, you'll want to be as detailed as possible. This will help you limit the number of solutions you test at the same time and ensure that you're focusing your efforts/resources on relevant solutions.

2. Map your current security posture

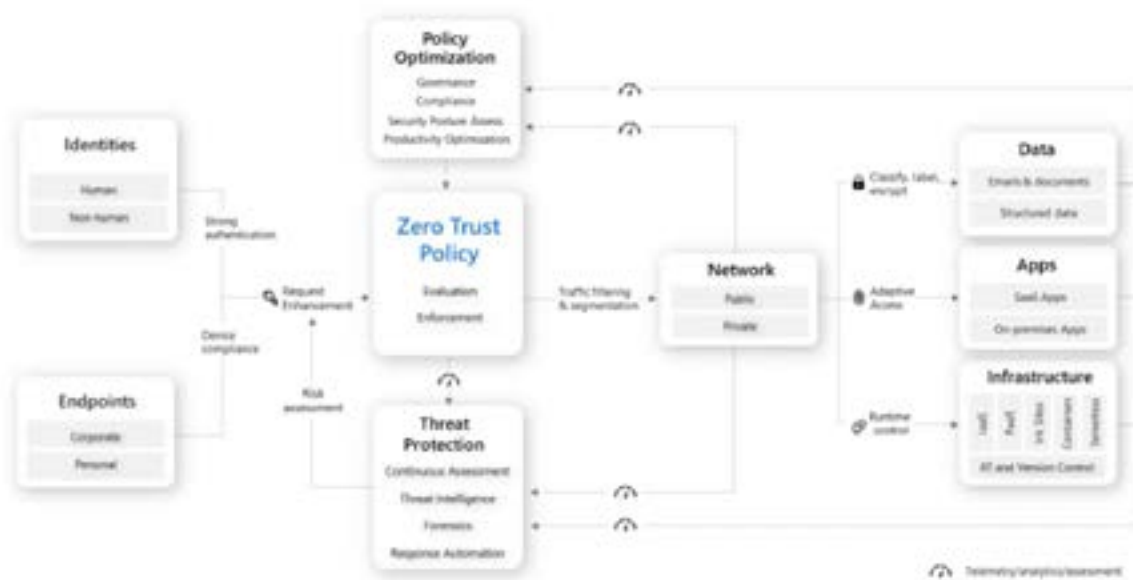
Next, you'll want to put together a map of your current digital estate. This includes assets, identities, networks, devices, and any existing security solutions, as well as any gaps or vulnerabilities that need to be addressed.

Aim to uncover blind spots, identify shadow IT and identities, identify risk vectors and data flows.

We recommend using the Zero Trust architecture to help guide this process. The framework is built on the following nine security

pillars — all of which will need to be addressed in your stack to effectively defend against ransomware:

- Identity
- Endpoints
- Networks
- Apps
- Data
- Infrastructure
- Policy optimization
- Policy enforcement
- Threat protection



This gives you a starting point you can use to start evaluating solutions that specifically address your security needs.


According to Secureworks, threat actors target gaps between layers – processes, tools, etc. – leaving businesses vulnerable, even after implementing intelligent solutions and robust protections.

Implementing a Zero Trust allows you to systematically seal those gaps and avoid costly breaches or other incidents that could have been prevented. So, ultimately, you'll want to

make sure that your solution(s) covers all of these pillars, plus any unique business requirements that might impact your security posture.

3. Evaluate vendors and ransomware tools

Once you've established a set of baseline requirements, you'll want to use that info to learn what options are out there.



According to Velosio Director of Cloud Carolyn Norton, organizations should, at a minimum, make sure that they're evaluating solutions and vendors that offer SIEM, XDR, and EDR functionality — and that those core capabilities can be unified in a single pane of glass.

Analyze open source and commercial tools available in the market based on your requirements.

Here are a few examples of questions you might ask to find the best-fit solutions:

- **Does this solution offer comprehensive protection?** In other words, does it cover the entire network or just parts of it? For example, a traditional EDR (endpoint detection and response) solution focuses exclusively on endpoints, whereas modern XDR solutions (extended detection and response) covers endpoints, as well as cloud, network, and third-party data.
- **Is it reliable?** Look at things like uptime, bugs, and crashes that could leave you temporarily exposed to threat actors. Additionally, you'll want to make sure that potential solutions don't conflict with existing software, which could lead to malfunction or suspended protections.
- **Is it easy to use?** You don't want to invest in solutions that require special skills in order to detect and respond to threats. Instead, look for solutions that make it easy for everyone to follow ransomware best practices, create and enforce policies, and evolve the strategy alongside the rapidly changing threat landscape.
- **Does it provide quality protection?** You want to ensure that potential solutions are up to the challenge of protecting your system from all possible threats. Look at things

like how often the vendor releases updates, whether security solutions have an impact on device/process/software performance, and whether they're able to effectively remove malware from your system. You'll also want to look at malware detection and response capabilities. For example, does it include AI and automation capabilities that can quickly isolate infected systems and remediate damage? Does it provide real-time alerts?

- **Does the vendor continuously invest in research and development?** This is important because it ensures that your vendor is committed to protecting its customers against existing, emerging, and future threats. You want to make sure that you're investing in solutions that will last for years to come — and that your vendor won't abandon you after the initial implementation.
- **What is the cost and potential impact of each solution?** You'll want to run a cost-benefit analysis before investing in a solution — or even dedicating limited time and resources into testing and trials.

You might include additional questions in your evaluation process, depending on what you're trying to achieve with your anti-ransomware investments.

But — the idea here is to gather enough information to put together a short list of tools you'd like to test before making any big commitments.

4. Come up with a plan for evaluating & testing potential solutions

Once you've narrowed your search, you'll want to take potential solutions for a test drive before making a final decision.

Keep in mind, you'll want to follow a systematic testing process, evaluating solutions against the same criteria and under the same conditions. This is super important as it allows you to effectively compare solutions and find the best option(s) for your business needs.

Tools should solve for the specific needs you outlined before getting started. Those might include:

- Improving productivity and accuracy
- Automating manual processes
- Gaining more granular visibility across your digital estate
- Improving asset discovery
- Increasing the speed of detection and response

You might consider running a pilot program. Many vendors use proof of concept evaluation criteria to help organizations understand how solutions work in context with a particular industry or use case. But, those are just a starting point – a template that doesn't include the specific requirements unique to your business.

A pilot program allows you to test solutions in a limited capacity – and measure the real impact they have on your business.

You should also set up sandbox environments to learn more about how solutions perform under various conditions.

For example, you might use predictive modeling capabilities to simulate different threat scenarios and evaluate how each solution responds against specific criteria – speed, accuracy, whatever.

5. Focus on centralizing security operations

Avoid taking a “best-in-breed” approach to security.

See, fragmentation slows you down, creates data issues, and locks critical insights inside silos. It's fundamentally at odds with the agility and end-to-end visibility you need to protect yourself in this complex, high-risk environment.

According to Splunk, modern security operations centers (SOCs) must include a common workspace for everyone in the organization. This is crucial, as it removes the need to switch between different tools, eliminates silos, and gives everyone a complete picture of where the security posture stands at any given moment.

As an example, Duck Creek Technologies replaced its existing SIEM solution with Microsoft Azure Sentinel and was able to gain end-to-end visibility across its entire digital estate.

While Duck Creek's old SIEM also ran on Azure, it wasn't natively integrated — which meant it was missing some critical functions — like the ability to pull real-time reports or integrate telemetry and log data with other security insights.

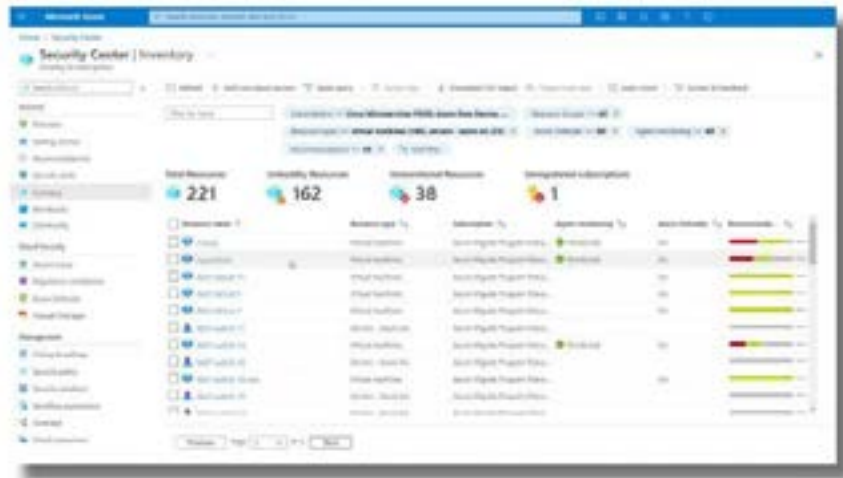
As such, combining Microsoft-based data with Azure Sentinel was a game-changer. Defender for Endpoint allowed the Duck Creek team to

quickly make adjustments to security policies when COVID forced them to go remote.

And, on top of that, the company can now monitor user activity, log-in patterns, etc. at a glance, from a single pane of glass — providing extra assurance that employees can work remotely, at scale — without taking on any additional risk.

Microsoft’s security solutions can all be managed through the Azure Security Center, which provides centralized monitoring and management across the entire estate.

In the below screenshot, you can see an inventory of all resources across on-premises and cloud environments — all managed using Azure Arc via Azure Security Center.



You can also set information protection controls in the Microsoft 365 Compliance Center by creating policies, automating data labeling and classification, and enforcing custom rules using

a series of triggers and actions to encrypt files, limit access, or restrict the use of third-party apps.



Setting information protection controls in the Microsoft 365 compliance center

Example of a policy being enforced as user tries to share content

Final thoughts

While tools will vary by organization, you'll want to make sure that you cover all possible vulnerabilities — from multiple angles.

Again, the Zero Trust security pillars are a great starting point for figuring out what to look for when evaluating potential solutions.

You can also take this series of self-assessments to determine the maturity of your ransomware strategy — and what it'll take to improve your defenses against ransomware.

In chapter 10, we'll hone in on ransomware detection methods that set the stage for smooth response, and ultimately, recovery.



Chapter 10: Practical Approaches for Detecting Ransomware

In chapter 10, we look at some practical tips for detecting ransomware early in the game -- and, more importantly, preventing attacks from happening in the first place. In it, we explain how to prepare your team, leverage the right set of tools, and more.

Like any virus, early detection and swift action is your best bet for making a full recovery after a ransomware attack.

The thing about ransomware is, it tends to hide out in your system until the threat actor decides to launch the payload. Ransomware might lie dormant for a few days or several months.

But often the aim is to catch victims off-guard so hackers can move quickly through the system before anyone catches on.

That way, they can steal more data, encrypt more files, and demand higher ransoms from desperate victims willing to pay almost anything to get their business back on track.

In these next few sections, we'll look at some of the steps you can take to level up your ransomware detection game – and get ready to take action against incoming threats before any real damage is done.

Ransomware is a moving target: you need different types of detection

Cybercriminals are constantly evolving their strategy based on lessons learned from prior attacks, new tools and tactics, and fellow “practitioners.” This means, you'll need to approach detection from all sides in order to take action against threats.

According to CrowdStrike, there are three main ways to detect ransomware — and you'll need to incorporate them all into your strategy so nothing falls through the cracks. Here's a quick look at each type and where it fits into the broader detection and response strategy:

1. Signature. Malware comes with a unique signature that includes IP addresses and domain names, as well as other identifying factors. Signature detection tools analyze the active files running on a machine against a library of pre-existing signatures to identify the presence of known malware. This approach focuses exclusively on known threats, leaving systems wide open to new variants and novel strains.

2. Behavior. Ransomware behaves in unusual ways — moving laterally across the network, opening and encrypting files. Behavioral detection tools monitor systems, flag unusual activity, and sound the alarms when human intervention is needed.

3. Abnormal traffic. Abnormal traffic detection is similar to behavior, but focuses on detecting unusual activity at the network level. These days, many ransomware attacks follow a two-pronged approach — first, stealing valuable data for resale or leverage, then encrypting the data and demanding that victims pay a ransom.

This double extortion model results in large data transfers to external systems. But — even if the ransomware is set up to conceal those transfers, it may still generate network traffic that can be tracked.

Tools with abnormal traffic detection capabilities allow you to follow a trail back to the ransomware hiding inside a specific machine — then delete it and start working toward recovery.

Embrace relentless monitoring

Organizations need both a high-level view across all networks, devices, identities, environments, endpoints, etc. – anything connected to their business, however tangentially – to prevent, detect, and respond to security threats – and granular visibility into each of these components.

According to Microsoft's Azure Defenses ebook, ransomware triggers some obvious changes in your system – lockouts, alerts, or notable changes in basic system behavior. Common signs of an attack include:

- Odd behavior of applications or devices
- Inability to access certain files or information
- Presence of a .TXT file – often this is a sign that your attacker left a ransom note
- Unusual traffic or log-in activity
- Failed attempts to access folders or files
- Unauthorized software has been installed
- Random accounts have been created/provisioned

While many of these signs seem like obvious evidence of ransomware, they can easily slip through the cracks if you're not working from a unified security stack.

Cyber criminals target different risk vectors. Cloud environments and storage solutions are the most common ransomware targets, as are misconfigurations and unpatched software.

Attackers scan for vulnerabilities they can use as access points – they don't necessarily care whether that entry point is a weak spot in your infrastructure, an unsupported legacy app, or a cyber-unaware employee.

Different signs also show up in different places – security logs, identity and access management platforms, individual SaaS apps, etc.

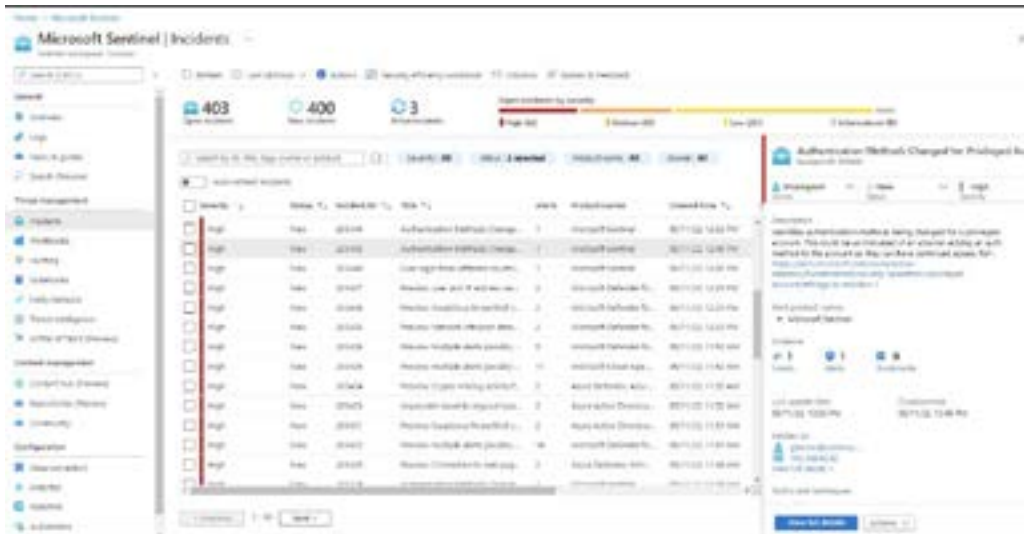
When you've got security silos or poorly-integrated solutions, you don't have the visibility you need to look for high-level patterns that indicate there's been an attack. You can't identify and fix vulnerabilities before they become a problem or proactively make improvements that can strengthen your overall security posture.

Now, different orgs might use different types of analytics solutions to identify and act on cyber threats. Those solutions should be chosen based on factors like business model, regulations, and the unique risks of operating within a specific industry.

For example, financial services firms might use AI insights to mitigate fraud risks or detect unusual transactions and behaviors.

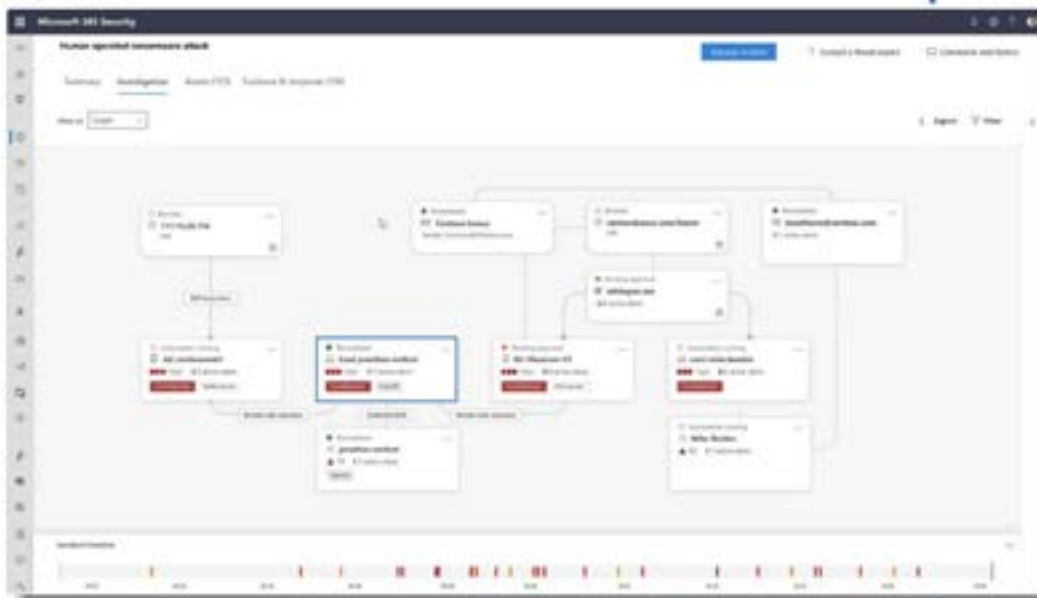
But, when it comes to detection and response, Microsoft's SIEM and XDR solutions – Azure Sentinel and Microsoft Defender – play a critical role in helping you identify and contain ransomware.

Microsoft Sentinel comes with 200+ built-in connectors that enable estate-wide monitoring across all apps, devices, users, and environments – both on-prem and in the cloud. Users can easily detect threats using the platform's built-in analytics and gain contextual and behavioral insights into threat actors and threats.



The screenshot below depicts an investigation into a human-operated ransomware attack via Microsoft Defender. The XDR solution can identify and contain breaches discovered on a

specific endpoint, and from there, take steps to return the infected device back to a trustworthy state before connecting back to the network.



Prepare employees – reaction time is everything

Detection isn't just about tools. Just look at the SolarWinds attack. At the time of the breach, everything was working as it was supposed to. Yet, the Orion update still became the point of infection. The incident wasn't so much a failure

of technology, as it was a failure of people and processes.

While effective detection capabilities are crucial when it comes to detecting attacks, cyber-hygiene is just as important – if not more.

Employees should always be on the lookout for anomalies like unfamiliar data or odd-looking

files to aid in ransomware detection. And, of course, they should be trained in best practices such as never entering credentials into unsecured websites or how to identify potential phishing campaigns.

Beyond the basics, organizations should put together a comprehensive response plan – with playbooks for dealing with different scenarios.

For example, monitoring is a total game-changer for customers. But – only if employees are prepared to properly work with real-time insights and take action against threats. It's important to understand that there's much more to this process than implementing an SIEM or setting up a security operations center (SOC).

Organizations must ensure that the proper configurations and procedures are in place – and that employees understand how to use monitoring tools, AI, and machine learning – and are empowered to move quickly in response to an attack.

They should also test users' understanding of risk. For example, running simulations that test their response to phishing campaigns or how to contain threats, based on which attack vector was used as the initial entry point.

Automate threat detection & response

According to a Forrester report commissioned by Secureworks, organizations face many security challenges including detecting and responding to unknown threats and attacks.

60% of respondents reported their lack of understanding in this area is currently limiting their ability to adequately secure their digital estate, while 59% said their lack of expertise is

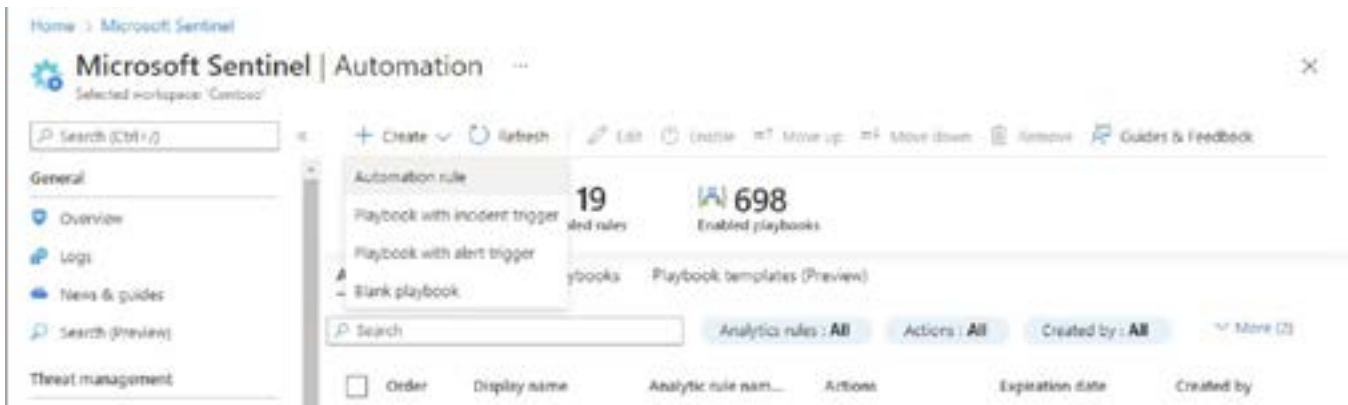
preventing them from reaching security goals. 23% of IT leaders admitted security operations rely on several manual processes – which leads to scalability issues, among other problems.

This data highlights the urgent need for organizations to streamline and automate security operations – particularly as orgs, already short on time, struggle to master the skills needed to stay safe in today's complex security environment.

Automation plays a key role in protecting your company against cyberthreats. It's used to prevent, detect, contain, and act on incoming threats. It's also become a vitally important tool for coping with the growing number and sophistication of cybersecurity threats.

According to Zero Trust principles, automation simplifies and strengthens an organization's security posture. Cloud-based intelligence and AI can detect and respond to anomalies in real-time, while automated alerting and remediation capabilities can reduce the mean time to response (MTTR) to incoming attacks.

With Microsoft Sentinel, users can correlate alerts into incidents and automate and orchestrate common tasks using custom playbooks. Playbooks are designed to help SOC analysts and engineers automate and simplify tasks like data ingestion and enrichment, investigations, and remediation. They allow users to set up custom automation rules to triage incidents, assign action items to the right person, and label incidents as known false positives, severe threats, etc.



Set up actionable alerts

Building on the themes of AI and automation, you'll want to set up alerts on high-risk anomalies or behaviors so that nothing suspicious falls through the cracks.

Some solutions provide contextual alerts and insights into attacker behaviors. For example, Microsoft Defender can raise alerts and prioritize actions, keeping businesses safe in the cloud – while also saving admins a ton of time.

For example, the platform can automatically detect unusual activity and send alerts to relevant users. Those users can then take action to stop the virus from spreading to critical docs, data, IP, etc. – containing the threat, removing the malware, and restoring the impacted data from a safe backup.

But – one 2021 Microsoft Security blog brings up an important consideration: you'll want to make sure you take steps to reduce “alert fatigue” within your organization. Otherwise, your people will stop paying attention after one too many false positives. According to the blog post, Microsoft already employs several strategies via its integrated SIEM and XDR solutions to minimize alert fatigue among customers.

For example, native integration between ransomware solutions allows customers to connect the dots between disparate data sources and threat signals, grouping alerts from across the threat landscape to tell a complete story about what happened and why.

Azure Sentinel's built-in machine learning automatically detects and analyzes threats – identifying combinations of suspicious behaviors and actions at different stages in the kill chain. It then uses those findings to reduce signal noise and improve alert quality over time.



Final thoughts

Ransomware detection best practices and tools help companies detect malware early in the game, allowing them to contain the threat and take steps to re-establish business continuity before any serious damage is done.

But – it's important to understand that early detection won't do you much good if you're not prepared to take action. Ransomware moves fast. Every second you lose is potentially a major blow to business continuity and the bottom line.

We're talking: data loss, irreparable damage to critical documents or IP, credential theft, data leaks that involve customers or partners – and all of the fallout that comes with the territory.

In chapter 11, we'll stick with this theme, and look at some of the steps you can take to ensure a swift post-breach recovery – with minimal damage to your business.



Chapter 11: Recovering from a Ransomware Attack

With the right strategy in place, an agile security practice, and the power of good data, you can bounce back quickly after a ransomware attack. In this chapter, we'll walk you through the response and recovery process, one step at a time.

Despite your best efforts, there's always the chance that bad actors – and their malware – end up in your system. It's not the end of the world, so long as you're prepared.

Now, your immediate goal is containing the threat, protecting stakeholders, and getting things up and running ASAP to minimize potential damage or business disruptions.

But, that's just the first step.

Once you've got things under control, you'll need to remove the malware, restore data from backups, and address any existing vulnerabilities.

Later, you might launch an in-depth investigation to better understand what happened and why.

Here, we walk you through the response and recovery process – one step at a time.

What to do immediately after a ransomware attack

Employees should be prepared to follow the documented incident response plan – first checking to see if backups have been impacted and whether it's possible to contain and mitigate the threat right away.

Now, if immediate mitigation isn't a possibility you'll need to work through a few more steps. Here's a quick rundown of the ones outlined in the CISA framework:

1. Contact the Authorities and an Attorney ASAP

If your company has been hit by ransomware attack, employees should immediately notify

senior management and the legal department of the attack.

Getting an attorney involved from the get-go is important as it ensures the investigation is protected by attorney-client privilege and can help orgs reduce the risk of getting hit with regulatory fines or class action lawsuits.

According to MIT, federal agencies may be able to help you recover lost data. In some cases, they may be able to trace attacks to a variant that has been decrypted – allowing you to avoid payment and recover your data – or recover ransom funds (though in some cases like Colonial Pipeline, some funds may be lost due to Bitcoin's inherent volatility).

Determine which systems, accounts, files, emails, etc. were infected
Isolate and contain any files, software, devices directly impacted by the attack, as well as anything that may be connected to those infected systems – remote desktops, VPNs, other cloud-based assets, etc.

2. Determine Which Systems, Accounts, Files, Emails, etc. Were Infected

Isolate and contain any files, software, devices directly impacted by the attack, as well as anything that may be connected to those infected systems – remote desktops, VPNs, other cloud-based assets, etc.

3. Try to Identify the Variant

Some strains of ransomware can compromise system stability. In these cases, avoid updates and reboots until ransomware has been successfully removed – otherwise, your files could remain locked in an unrecoverable state.

Check out the No More Ransom Project website to find out more about the strain, the

attacker, and, potentially, gain access to a free decryption key.

4. Investigate All Threat Prevention and Detection Solutions

Check all security analytics tools, logs, etc. for evidence of a compromise such as precursor malware, unusual activity, or trigger files across the entire network. You'll also want to see if you can determine the attack style and/or find out more about how this particular strain behaves and spreads.

5. Gather Logs and Evidence

Collect logs and evidence and take a system memory capture of any devices impacted by the incident, taking extra care to preserve evidence for deeper analysis and investigation.

Keep in mind, you'll want to capture as much evidence as you can before moving forward with the recovery to aid law enforcement, cyber insurers, and external security experts in their investigation.

6. Disconnect Infected and At-Risk Systems from WiFi, the Rest of Your System

Next, you'll want to disconnect any infected backups and at-risk systems. Attackers typically go after backup systems because they know victims will immediately try to recover critical documents and data so they can avoid paying the ransom or succumbing to additional extortion threats.

You'll also want to avoid connecting backups to infected systems or devices and quarantine any backups that may be compromised – otherwise, you're just helping the threat actor make quick work of your network.

7. Take Steps to Reestablish Business Continuity

While it makes sense that companies tend to focus their ransomware strategy on prevention and detection, reestablishing continuity should be a top priority. Bring systems back online as soon as possible.

Test any systems you suspect have been infected before bringing them back online. Document procedures used to resolve issues.

8. Make a Decision About Paying the Ransom

Determining whether or not to pay the ransom is a difficult decision. In some cases, payment may be the fastest, most cost effective path to recovery. However, there's no guarantee that making the payment will result in the safe return of your data and it may make you more susceptible to future attacks.

Whether paying the ransom is the right decision depends on several factors – it's generally frowned upon (FBI, experts say it encourages ransomware attackers to continue this behavior).

You'll want to perform a quick cost-benefit analysis based on the scenario, potential outcomes, and from there, make a decision with harm reduction in mind.

Additionally, HBR recommends that orgs ask themselves the following questions when making this call:

- Are there backups available?
- Or will you need a decryption key to unlock that data?
- How sensitive is the data that has been stolen/encrypted/accessed?
- Are the costs of non-payment something you're willing to take on?

- These might include negative publicity, reputational damage, business disruption, etc.
- Is the threat actor connected to a company on the US Treasury OFAC list? If so, it could be illegal to pay the ransom under US law.

Note that your initial “response” is different from your long-term “recovery.” At this stage in the game, you’re trying to triage the situation so you get up and running again – and buy yourself some time to explore permanent solutions.

Ransomware Containment & Eradication

Once a system is identified as “infected,” it needs to be removed from the network and quarantined – away from cloud environments, apps, services, wifi, etc.

Failing to isolate ASAP can lead to more damage, as ransomware will continue to spread through the digital estate and encrypt more files.

According to an IBM white paper, you’ll want to run endpoint detection and response (EDR) immediately following the attack. This will help you isolate infected systems and keep them online, allowing you to retain critical evidence and data, without causing further harm to the system.

If you don’t have an EDR solution, you may have to terminate access to the network. It’s a last resort that can lead to data loss, but it minimizes potential damage to other parts of the network.

The eradication phase focuses on removing ransomware from infected systems. In some cases, the process is relatively short, whereas in others, removing ransomware is a complex,

lengthy process. It all depends on the scope of the attack and how much damage was done.

Some ransomware variants can make infected systems unstable – so you’ll want to avoid reboots or updates and keep systems online until you’ve successfully removed the malware.

Post-Breach Recovery

After you’ve completed the containment and eradication process, your next move is to work through the following steps to restore your system:

Secure Communication Channels

After experiencing a ransomware attack – particularly one involving a systemic identity compromise – you’ll want to go ahead and assume all communication channels have been infected.

Before taking any additional action, you’ll want to make sure that your team can communicate securely – allowing you to proceed with your investigation and recovery without the threat actor’s knowledge.

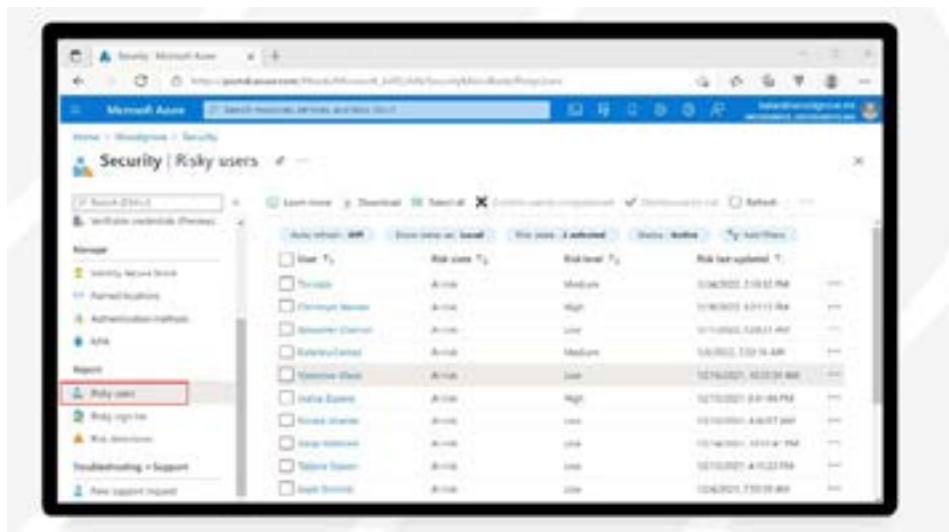
Re-Establish Credential Hygiene

Most ransomware attacks are identity-based, so you’ll want to make sure that your post-attack recovery focuses on strengthening identity and access management protections.

If you haven’t already, implement multi-factor authentication (MFA), single sign-on, and update access permissions, and simplify identity management and governance.

Solutions like Azure AD allow you to configure conditional access policies based on contextual factors like device, user, and real-time risk intelligence, and automate policy governance and provisioning.

You can even run reports that identify “risky users,” events, and log-in attempts and take immediate action against suspicious activity.



Patch Vulnerabilities, Update Software, & Restore Data from Backups

Microsoft’s Detection and Response Team (DART) recommends updating all apps and services post-breach and implementing an inventory and asset solution such as Endpoint Configuration Manager so that you can manage all updates, patches, and installs from one place moving forward.

Use offline backup files to restore data and reconnect to the system, taking extra precautions to avoid reinfection. It’s a good idea to perform this task in a sandbox environment to minimize your risk. Additionally, you’ll want to make sure that you verify the status of your backups at the time of recovery.

In the IBM paper mentioned above, experts warn that there’s a chance that attackers have been hanging out in your system for months, encrypting backups.

Or – they may lie dormant for even longer,

planting persistence mechanisms into backups. Make sure you store backups in a separate location and check them regularly – ensuring that they haven’t been tampered with.

You’ll also want to avoid making policy exceptions for specific users or business units that make it possible to avoid patching vulnerabilities.

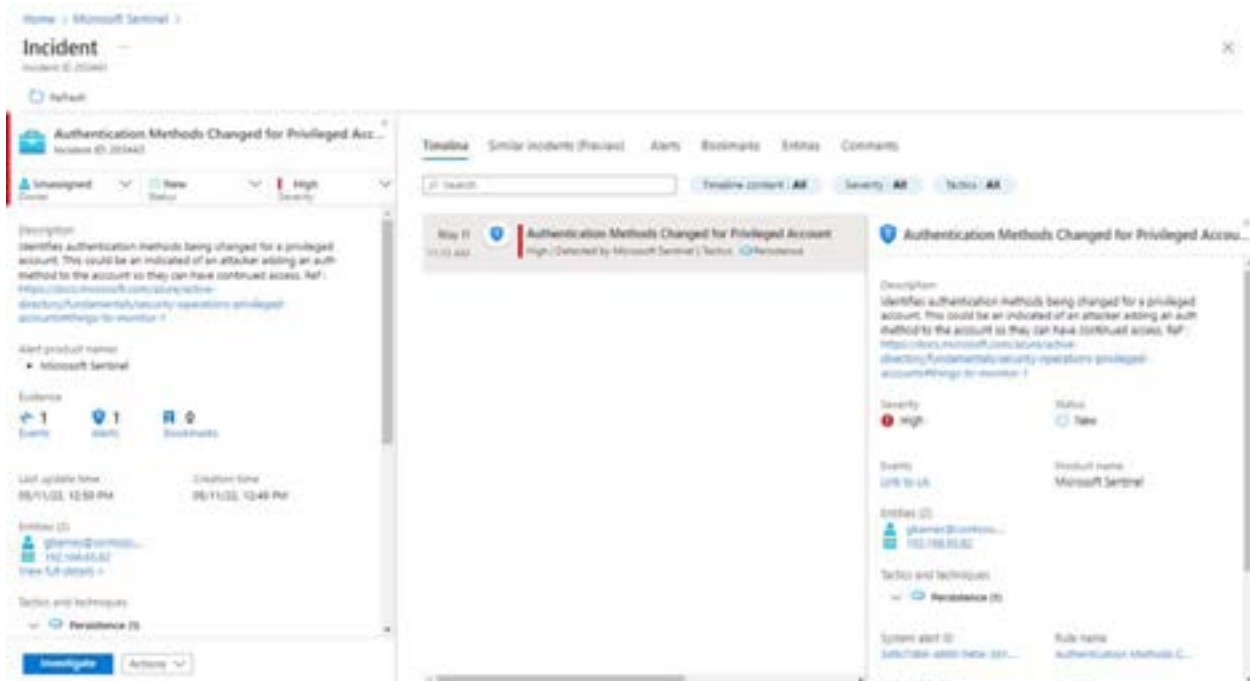
In the short-term, DART advises orgs to isolate vulnerable apps and devices to avoid getting hit by a follow-up attack. Though, long-term, security experts recommend adapting your acquisitions process so that you only work with vendors that provide adequate protections. Conduct a Deeper Investigation
Microsoft experts recommend investigating the compromised environment – after ensuring that you can communicate and collaborate securely.

Sentinel comes with deep investigation tools to help users understand the scope of the attack and identify the root cause behind the incident.

The built-in dashboard allows you to search for incidents – filtering by severity, compromised

entities, trigger events, or other factors.

You can review a timeline of the incident to learn how the attack went down. Or, review similar incidents to learn more about the attack in a broader context.



Advanced threat hunting – process that involves proactively searching for the presence of threat actors, malware, etc. within the digital environment.

Meet with Stakeholders to Discuss Lessons Learned

Yeah, you do need to talk about what happened – it's the first step toward making changes so that this won't happen again.

Document lessons learned from the incident and use them to refine your ransomware policies and procedures so you're better prepared for future attacks.

Update Your Security Processes

The last step in your post-incident recovery is making sure you can respond quickly and confidently to future attacks.

Or better yet, avoid them in the first place. If you haven't already, implement a Zero Trust policy.

According to Microsoft experts, recovering from a cyber incident means forcing security changes that should have been implemented a long time ago. Often, what should have been a years-long process of incremental updates must happen within a matter of weeks.

This process also involves significant behavioral and operational changes – which, of course,

tend to be the hardest changes any organization will have to make. Things like how to administrate the environment, deploy machines, or monitor identities, activity, and data.

For example, you might look for a detection and response platform to help with monitoring and preventing issues.

But, if you're already using the latest and greatest tools, you'll need to focus on training your teams, making sure they're using tools properly, that they understand how to interpret data, etc.

Finally, document the new game plan, communicate changes to your team, and make sure that leadership supports and enforces it.

Final Thoughts

Recovering from a ransomware attack is a multi-step process that requires a lot of planning and preparation, as well as the right set of tools.

As you put together your plans, you'll want to make sure that you consider the potential ripple effects of an attack.

In chapter 12, we'll focus on the big-picture and look at the key ingredients of a world-class ransomware strategy.

Chapter 12: Elements of a World-Class Ransomware Strategy

This chapter will focus on the key ingredients to include in any modern ransomware strategy. In it, we use the Zero Trust framework as the basis for our hypothetical game plan — with the understanding that each business will take its own approach to defending against ransomware.

Today’s chaotic threat environment demands a whole new approach to cyber security — built on the Zero Trust framework.

Zero Trust is a set of policies based on the underlying principle, “never trust, always verify.” It’s flexible, adaptable, and fast-moving.

Now, it’s important to understand that Zero Trust doesn’t represent any one strategy, solution, or technology.

It’s more of a template orgs can use to establish trust between resources and users in real-time, as needed — as well as continuously revalidate those connections.

In these next few sections, we’ll explain what that actually looks like in practice.

Establish end-to-end coverage

Data from Deloitte’s 2022 “Future of Cyber” survey revealed that end-to-end visibility across complex systems is key to balancing security requirements with digital transformation goals. Experts warn that the stakes of getting this wrong include operational disruptions, reputational damage, diminished equity valuations, among other disasters.

Done right, Zero Trust provides the assurance that you’ve covered all of your bases — so that unexpected threats and vulnerabilities won’t catch you by surprise later on. The framework is designed in such a way that ransomware protections are added to your

estate one layer at a time — until each of the following “security pillars” have been accounted for:

- Identity
- Data
- Endpoints
- Network
- Applications
- Devices
- Infrastructure

We’ve covered these pillars in a previous post on anti-ransomware tool guidance, and you can also find them throughout the Microsoft Security content, downloads, and documentation.

That said, if you’re coming at this with zero Zero Trust experience to speak of, you might want to look into the Microsoft RaMP initiative — which offers technical deployment guidance across a handful of high-priority areas:

Initiative	Steps
Top priority User access and productivity	Critical security modernization initiatives 1. Explicitly validate trust for all access requests <ul style="list-style-type: none">• Identities• Endpoints (devices)• Apps• Network
Data, compliance and governance	2. Ransomware recovery readiness 3. Data
Modernize security operations	4. Streamline response 5. Unify visibility 6. Reduce manual effort
As needed	Additional initiatives based on Operational Technology (OT) or IIoT usage, on-premises and cloud adoption, and security for in-house app development:
OT and Industrial IoT	<ul style="list-style-type: none">• Discover• Protect• Monitor
Datacenter & DevOps Security	<ul style="list-style-type: none">• Security Hygiene• Reduce Legacy Risk• DevOps Integration• Microsegmentation

While the RaMP initiative does address all elements of the Zero Trust architecture, the idea is to help organizations focus on high-impact areas first.

You'll start with identities and endpoints – because they represent the biggest threat to your business. Then, you'll work your way through apps, networks, and so on.

Integration is everything

Integration is central to all digital strategies — and ransomware is no exception.

Zero Trust hinges on establishing unity and integration across the entire digital estate — offering the end-to-end visibility, actionable insights, and agility needed to defend against ransomware.

This concept should be familiar to those of you leading AI- or cloud-driven transformations.

Beyond making sure that your estate is fully-protected and 100% free of gaps and silos that can get you in trouble, you'll want to avoid leaning on too many solutions. And, instead, aim to invest in interoperable tools that cover multiple pillars.

Fragmented security solutions can result in coverage gaps and unnecessary complexity — creating extra work for IT and introducing new risks to your system.

It's harder to detect incidents as they're happening, let alone mount a proactive defense against future threats based on suspicious patterns and anomalies flagged by your system's AI.

Alternatively, if companies implement security

measures that add friction to daily workflows, employees will find workarounds in the form of unsanctioned apps (aka shadow IT).

Either way, orgs are essentially serving valuable documents and data to attackers simply by making things harder than they should be.

These factors — among others — are the key reason why we put so much emphasis on the “Microsoft ecosystem.”

These solutions are designed to work together, as a single ransomware-fighting unit.

Business leaders pick and choose the capabilities they need to protect their entire estate — whether you need to protect remote teams, IoT and OT networks, or complex hybrid set-ups that span on-prem servers and cloud-based services.


Control access with policy

Historically, identity and access controls existed in this binary where the decision to “allow” or “deny” requests was based on absolutes.

For example, internal traffic is inherently trustworthy, while external traffic is a threat — without considering the contextual factors that determine what risk that user poses to the business.

Strong governance is directly connected to the success of your Zero Trust initiatives.

According to a Microsoft paper, Evolving Zero Trust, the best Zero Trust strategies are built on governance models designed to enforce data integrity through continuous monitoring and improvement.



In a 2021 McKinsey piece, analysts call security as code (SaC) the “best (and maybe only)” way to secure cloud apps and systems.

These solutions allow users to implement security protections at speed and scale, setting system-wide rules that automatically enforce compliance, generate value, and mitigate risk.

The main advantage of SaC tools is, they offer more control over security and save IT teams a ton of time. For example, security policies may be translated into processes any time there’s a change made to the source code.

Use automation to streamline, strengthen, & sustain your security posture

Automation is now a prerequisite for establishing a strong, sustainable security posture. Consider the sheer volume of security alerts and notifications alone and you can see why automation is the only way to ensure that your organization is always prepared to take immediate action in the face of a threat.

Security automation plays a key role in dealing with routine IT tasks such as provisioning, scripting, and performing access reviews – all without human intervention.

Leading orgs use security automation in more advanced ways. Think – using machine learning models to orchestrate adaptive defense strategies that take proactive action against threats.

Automation also enables businesses to quickly recover from an attack by allowing you to

rapidly contain and remove malware from your environment – and rebuild once you get the green light to move forward.

Accenture experts say automation increases resilience capabilities on all fronts – prevention, detection, response, and recovery.

Use proven business needs to inform your Zero Trust plan

In its 2021 Future of Cyber report, Deloitte experts explain that Zero Trust is designed for all organizations – regardless of size, sector, budget, or business goals.

But, they emphasize that it is absolutely not a one-size-fits-all framework. So, the challenge there becomes about ensuring that your ransomware strategy aligns with your actual business goals.

Final thoughts

As mentioned above, Zero Trust doesn’t represent the full picture of your best possible ransomware strategy.


Instead, it offers a template that can offer a strong foundation for a tailored, defense against evolving threats – if you can manage to get everything else right.

In our final installment, we’ll look toward the future and discuss some of the steps you can take to ensure that your ransomware strategy has what it takes to defend against future threats – even if we don’t know what those threats will look like.



Chapter 13: Future-Proofing Your Business Against Ransomware

Creating the kind of ransomware strategy that prevents and protects against future unknowns is a daunting prospect — even for the savviest security pros. Here's how to build a flexible, forward-looking ransomware strategy that will keep your business safe for years to come.



Future-proofing your ransomware strategy – or, any strategy for that matter – is mostly about cultivating the conditions that enable quick decisions and real-time response.

Here, we'll share some practical tips for building a forward-looking strategy for navigating a landscape riddled with “unknown unknowns,” hidden threats, and a lot more complexity.

Size up your security posture, fix problems, & fill gaps

Data from a recent Axonius survey found that two-thirds of organizations are spending more on SaaS apps year-over-year. That same share of respondents also say rising SaaS investments have introduced more complexity and security threats to their business.

More SaaS apps in the stack means companies have more critical data, documents, and processes flowing through their digital estates than ever before. In turn, attackers have more opportunities to exploit vulnerabilities – wreaking havoc on enterprise systems, as well as any users, devices, customers, or partners connected to those networks.

Beyond SaaS apps, the explosion of big data, an influx of personal and IoT devices, and expanding hybrid cloud ecosystems are having a similar impact on orgs' overall security posture.

The first step toward building a future-proof ransomware strategy is to get a clear picture of where things stand right now.

Initially, you'll want to identify the following elements so you can start putting together a comprehensive map of your network, including all:

- Assets
- Data
- Devices
- Applications & services
- Identities & credentials
- Existing security solutions
- Vulnerabilities
- Security silos & gaps
- Etc.

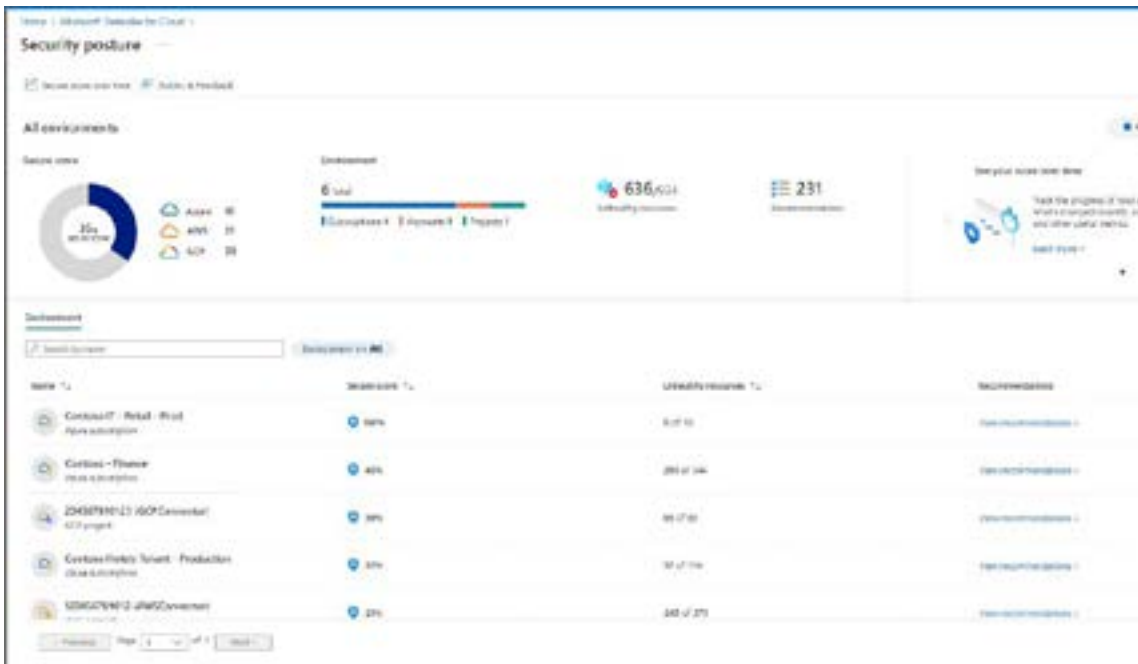
Microsoft offers a self-evaluation tool you can use to get a sense of where your security posture stands today, and, from there, make any necessary changes to improve your overall strategy – whether you're already a customer or not.

Existing customers benefit from a wealth of assessment tools embedded directly into its expansive product catalog.

For example, Defender for Endpoint comes with a Device Discovery feature, which allows you to take an inventory of all assets, perform vulnerability scans on discovered devices, ID shadow IT, and use the platform's AI-generated recommendations to prioritize and remediate risks.

Or – if you're already using Microsoft Defender for Cloud, you can use the built-in visual reporting tools to learn more about vulnerabilities across your entire digital estate.

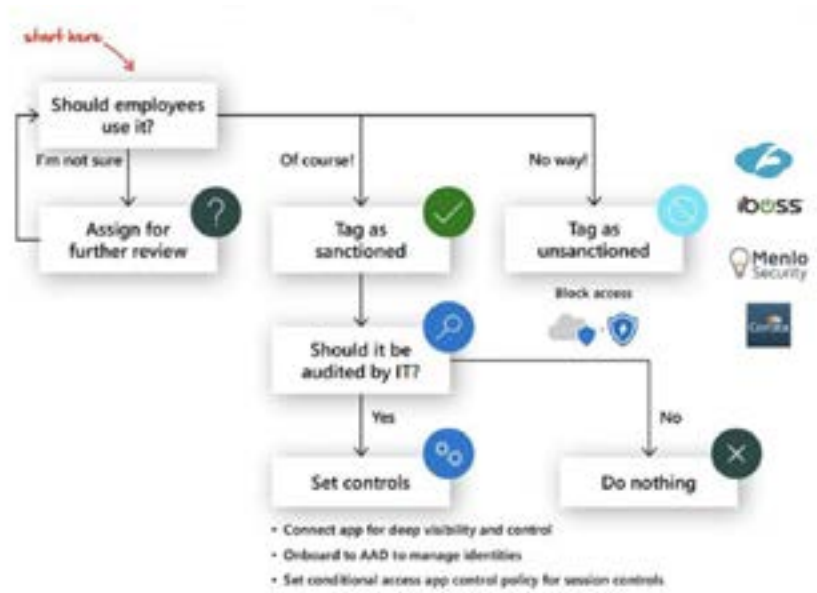
For example, the Security Posture dashboard offers an at-a-glance assessment of your overall standing – with the option to drill down into each app, subscription, or cloud environment, as per the screenshot below.




If you click “view recommendations” for, say, “GCP Connector,” you’ll then get a list of actions you can take to make that Google Project more secure – ensuring that it doesn’t become a gateway for threat actors to access your Azure subscriptions, D365 apps, or customer data.

Another option is Microsoft Cloud App Security. This platform helps users ID risky usage patterns, spot signs of breach or exfiltration, and manage newly discovered cloud apps.

Users can then use their findings to take action. Per a 2021 Microsoft blog post, business leaders need to decide which apps are appropriate for employee use, which apps pose a threat, and start setting defined policies to gain control over their network. You might use a framework like this to standardize decision making re: access controls, sanctions, and more:





Ultimately, you're trying to paint a clear picture of your entire threat surface that can then be used to develop a robust plan spanning every asset, user, endpoint, etc. in your network.

Implement intelligent, proactive solutions

According to the World Economic Forum 2022 Global Cybersecurity Outlook, 81% of survey respondents say digital transformation is the main factor when it comes to improving cyber resilience. This points back to the ongoing theme of becoming a data-driven organization – and really working to build a mature data strategy.

Per Palo Alto Networks' 2022 Future of Threat Intelligence report, predictive intelligence is an absolute must.

When businesses can detect anomalies, vulnerabilities, and breaches in real-time, implement automations that take immediate action against incoming threats, they're able mitigate potential damage and quickly bounce back from an attack relatively unscathed.

You'll want to make sure you're using solutions that continuously evaluate the threat landscape, perform ongoing risk assessments, and enforce compliance and data governance requirements.

These solutions enable users to identify and investigate unusual traffic patterns, login attempts, and unauthorized activity, find and fix shadow IT and identities before threat actors can exploit them, and make changes to their security strategy as the threat landscape evolves.

Predictive intelligence tools also allow users to build incident response plans using real data and predictive models – that way you can train your team to act quickly in the event of an attack, stress test your plans, and implement measures that minimize damage and support business continuity.

Security automation is another critical piece of your ransomware defense strategy. Algorithms can be trained to systematically detect, analyze, remediate cyber incidents, prioritize alerts, and contain malware without human intervention.

Per one recent Splunk blog post, many solutions can automatically fix known issues without human intervention, triage breach situations, and prioritize alerts so that humans can take action in a timely manner.

In turn, security teams can then take a more proactive approach to managing threats, since automation frees up resources and time better spent on high-value tasks.

For example, Johnson & Johnson used Azure Bot Service, an NLP service dubbed LUIS, and a cloud-based API that generates relevant question-and-answer layers based on existing data to build an end-to-end chatbot platform, Genie the Genius.

Each Genie chatbot runs on its own service – separate from the rest of the bots – and uses its own resources.

That way, if one J&J bot gets hit with a breach or a ransomware attack, it won't spread to the others – or the rest of the enterprise.

Microsoft's low-code solutions enabled J&J to quickly deploy this large-scale chatbot platform – quickly, using templates and built-in automations – but crucially, it also allowed the organization to implement security controls like

authentication, policy enforcement, and SSL across all bots in the network.

Look ahead at emerging tech, trends, & a changing threat landscape

There's no question that the threat landscape will continue to evolve.

Threat actors will keep updating their tactics and leveraging new technologies – wreaking havoc on victims in ways we can't yet imagine. And – as such, you want to make sure you're always looped into the latest happenings in the ransomware space.

For example, what's going on within the ransomware community, both in context with your industry and just in general? Are there new strains? Ransomware business models? Are phishing strategies targeting different platforms or embracing new formats?

Now, the takeaway here should be more than “keeping up with current events is good for business.” It's more about implementing solutions that keep you tuned into the things that matter most from a security standpoint, so that you can continuously optimize your ransomware strategy based on the threats of the moment.

Building on that, you'll also want to consider how upcoming tech investments will impact your security posture. And, taking it one step further, what steps you'll need to take to accommodate the new security requirements that come with those hypothetical investments.

Are there any planned digital transformation projects in the works? For instance, are you

considering how to incorporate blockchain into your business model or developing a Web3 project?

How, then, might these new elements alter existing ransomware strategies? And, more crucially, what kind of plans are already in place to ensure that security is baked into every project from the get-go?

Finally, you'll also want to think about the risks and opportunities emerging tech might bring to the threat landscape. That means, assessing the risks new tech might introduce to your business and what it'll take to protect those new, virtual worlds from the threat actors trying so hard to exploit them.

How will you handle cybersecurity in the metaverse? Or at the edge. Or, in a 5- or 6G world with way more data than you're already dealing with?

Even if you're not sure about, say, investing in the metaverse right now, it's still worth looking at the “next big thing” from a practical standpoint so you're ready to hit the ground running if things change.

Look at CCC Group. Following a successful CRM implementation, the organization decided to embrace a “data-first mindset,” empowering teams with unified analytics and accessible visual reporting tools.

The group is using data to decide which products to develop and which markets to pursue. But they're also using those insights to build a new strategy with data governance at its core. In turn, this has allowed the company to drive cultural change and transformation, and use analytics to prepare for the future.



Final thoughts

Preparing for the future in a threat landscape defined by fast-paced change and “unknown unknowns” is a daunting prospect. And, sadly, the best advice we can offer is to keep moving.

Tons of companies, even huge enterprises with top talent and massive IT budgets, become ransomware victims simply because they get too comfortable.

Ultimately, your best bet is to focus on the soft stuff. Think – culture, training, and employee enablement. It’s these things that will help people develop the mindset and skills they’ll need to succeed – in 2025 or 2045.



Conclusion

While the latest ransomware stats are alarming, there's a lot you can do to protect your company, customers, and bottom line from ransomware devastation.

That said, organizations must transform their entire ransomware strategy – or get pummeled by lawsuits, losses, and more security-savvy competitors.

That is, if ransomware attackers don't wipe out your business first.

Velosio is a Microsoft Gold Partner offering a wide range of services from consulting and ERP implementation to proprietary solutions that expand on Microsoft's off-the-shelf capabilities.

While we're not a cybersecurity company, security is embedded into everything we do. Which in turn, allows us to get them up and running faster and ensures that they get the most from their investments.

Check out Microsoft's Zero Trust Maturity Assessment to get started. It's a quick, self-guided quiz designed to give you a sense of where your security posture stands today – and what your next steps might look like.

Or, you can contact us directly and chat with one of our experts.

Velosio can analyze your environment to get a sense of what is going on, both on-premises and in the cloud.

We help you gain a full-picture view of your environment and determine the next best steps by measuring the risk to your digital assets and the likelihood of network assets being taken down.

We also help you evaluate the consequences of losing important data or entire systems, and how long it will take for your organization to recover.

We'll help you design and implement a game plan that not only protects against ransomware, but generates real value for your business and its customers.

It can be difficult to figure out what solutions you need and how to implement them – let alone establish strong governance models or leverage security automation.

Works Cited

3 Steps to Stop Employees From Taking Cyber Bait, <https://emtemp.gcom.cloud/ngw/globalassets/en/publications/documents/3-steps-to-stop-employees-taking-cyber-bait.pdf>. Accessed 25 October 2022.

Microsoft Azure: Cloud Computing Services, <https://azure.microsoft.com/en-us/>. Accessed 25 October 2022.

The No More Ransom Project: Home, <https://www.nomoreransom.org/>. Accessed 27 October 2022.
Microsoft Azure: Cloud Computing Services, <https://azure.microsoft.com/en-us/>. Accessed 6 November 2022.

MITRE ATT&CK®, <https://attack.mitre.org/>. Accessed 6 November 2022.

Power Automate, <https://powerautomate.microsoft.com/>. Accessed 6 November 2022.

Microsoft Power Platform: Business Application Platform, <https://powerplatform.microsoft.com/en-us/>. Accessed 7 November 2022.

Microsoft Power Pages, <https://powerpages.microsoft.com/en-us/>. Accessed 7 November 2022.

“???” ??? - YouTube, 17 January 2022, https://www.genetec.com/binaries/content/assets/genetec/ebooks/ebook_en_cybersecurity.pdf. Accessed 6 November 2022.

“...” ... - YouTube, 17 January 2019, <https://docs.microsoft.com/en-us/power-apps/guidance/planning/introduction>. Accessed 7 November 2022.

“The 10 Biggest Ransomware Attacks of 2021.” Touro College Illinois, 12 November 2021, <https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php>. Accessed 24 October 2022.

“About the SharePoint admin role in Microsoft 365 - SharePoint in Microsoft 365.” Microsoft Learn, 22 August 2022, <https://docs.microsoft.com/en-us/sharepoint/sharepoint-admin-role>. Accessed 7 November 2022.

“About the SharePoint admin role in Microsoft 365 - SharePoint in Microsoft 365.” Microsoft Learn, 22 August 2022, <https://docs.microsoft.com/en-us/sharepoint/sharepoint-admin-role>. Accessed 7 November 2022.

“Addressing all stages of the risk lifecycle in financial services - Microsoft in Business Blogs.” Microsoft Cloud Blogs, 13 April 2022, <https://cloudblogs.microsoft.com/industry-blog/microsoft-in-business/financial-services/2022/04/13/addressing-all-stages-of-the-risk-lifecycle-in-financial-services/>. Accessed 25 October 2022.

Works Cited

“Addressing all stages of the risk lifecycle in financial services - Microsoft in Business Blogs.” Microsoft Cloud Blogs, 13 April 2022, <https://cloudblogs.microsoft.com/industry-blog/microsoft-in-business/financial-services/2022/04/13/addressing-all-stages-of-the-risk-lifecycle-in-financial-services/>. Accessed 27 October 2022.

“AI-driven adaptive protection against human-operated ransomware.” Microsoft, 15 November 2021, <https://www.microsoft.com/security/blog/2021/11/15/ai-driven-adaptive-protection-against-human-operated-ransomware/>. Accessed 25 October 2022.

“AI-driven adaptive protection against human-operated ransomware.” Microsoft, 15 November 2021, <https://www.microsoft.com/security/blog/2021/11/15/ai-driven-adaptive-protection-against-human-operated-ransomware/>. Accessed 6 November 2022.

“AI models and business scenarios - AI Builder.” Microsoft Learn, 31 May 2022, <https://docs.microsoft.com/en-us/ai-builder/model-types>. Accessed 7 November 2022.

Alder, Steve. “Planned Parenthood Los Angeles Facing Class Action Lawsuit Over October 2021 Ransomware Attack.” HIPAA Journal, 14 December 2021, <https://www.hipaajournal.com/planned-parenthood-los-angeles-facing-class-action-lawsuit-over-october-2021-ransomware-attack/>. Accessed 25 October 2022.

“Allianz Risk Barometer | AGCS.” Allianz Global Corporate & Specialty (AGCS), <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html>. Accessed 25 October 2022.

“Allianz Risk Barometer | AGCS.” Allianz Global Corporate & Specialty (AGCS), <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html>. Accessed 25 October 2022.

“Allianz Risk Barometer | AGCS.” Allianz Global Corporate & Specialty (AGCS), <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press.html>. Accessed 6 November 2022.

Anderson, Bill, et al. “Enforcing Ransomware Protections with the Power Platform.” Velosio, 12 July 2022, <https://www.velosio.com/blog/enforcing-ransomware-protections-with-the-microsoft-power-platform/>. Accessed 25 October 2022.

Anderson, Bill, et al. “Enforcing Ransomware Protections with the Power Platform.” Velosio, 12 July 2022, <https://www.velosio.com/blog/enforcing-ransomware-protections-with-the-microsoft-power-platform/>. Accessed 6 November 2022.

Anderson, Bill, et al. “Getting to the Cloud Can Reduce Cyber Security Risks for Professional Services Firms.” Velosio, 15 December 2020, <https://www.velosio.com/blog/reduce-cyber-security-risks-for-professional-services-firms/>. Accessed 24 October 2022.

Works Cited

Anderson, Bill, et al. "Getting to the Cloud Can Reduce Cyber Security Risks for Professional Services Firms." Velosio, 15 December 2020, <https://www.velosio.com/blog/reduce-cyber-security-risks-for-professional-services-firms/>. Accessed 7 November 2022.

Anderson, Bill, et al. "How Azure Helps Organizations Protect Against Ransomware Attacks." Velosio, 7 July 2022, <https://www.velosio.com/blog/how-azure-helps-organizations-protect-against-ransomware-attacks/>. Accessed 25 October 2022.

Anderson, Bill, et al. "SharePoint Improves Productivity for Professional Services Firms." Velosio, 2 June 2022, <https://www.velosio.com/blog/sharepoint-improves-productivity-for-professional-services-firms/>. Accessed 7 November 2022.

Anderson, Bill, et al. "6 Recent High-Profile Ransomware Attack Examples." Velosio, 11 August 2022, <https://www.velosio.com/blog/6-high-profile-ransomware-attack-examples-and-what-you-can-learn-from-them/>. Accessed 26 October 2022.

Anderson, Bill, et al. "What is single sign-on? | Velosio ViewPoint Video Blog." Velosio, 13 April 2022, <https://www.velosio.com/blog/what-is-single-sign-on-velosio-viewpoint-video-blog/>. Accessed 25 October 2022.

Anderson, Bill, et al. "What is single sign-on? | Velosio ViewPoint Video Blog." Velosio, 13 April 2022, <https://www.velosio.com/blog/what-is-single-sign-on-velosio-viewpoint-video-blog/>. Accessed 6 November 2022.

Anderson, Bill, et al. "What is single sign-on? | Velosio ViewPoint Video Blog." Velosio, 13 April 2022, <https://www.velosio.com/blog/what-is-single-sign-on-velosio-viewpoint-video-blog/>. Accessed 6 November 2022.

"Anti-phishing protection - Office 365." Microsoft Learn, 27 September 2022, <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection?view=o365-worldwide>. Accessed 6 November 2022.

"Anti-phishing protection - Office 365." Microsoft Learn, 27 September 2022, <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection?view=o365-worldwide>. Accessed 6 November 2022.

"Application Security in Business Central - Business Central." Microsoft Learn, 30 September 2022, <https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/security-application>. Accessed 6 November 2022.

Works Cited

Arghire, Ionut. "FBI Confirms REvil Ransomware Involved in JBS Attack." SecurityWeek, 3 June 2021, <https://www.securityweek.com/fbi-confirms-revil-ransomware-involved-jbs-attack>. Accessed 25 October 2022.

Asatryan, Davit. "5 keys to protecting OneDrive users." Help Net Security, 11 June 2020, <https://www.helpnetsecurity.com/2020/06/11/onedrive-security/>. Accessed 6 November 2022.

"Automating threat actor tracking: Understanding attacker behavior for intelligence and contextual alerting." Microsoft, 1 April 2021, <https://www.microsoft.com/security/blog/2021/04/01/automating-threat-actor-tracking-understanding-attacker-behavior-for-intelligence-and-contextual-alerting/>. Accessed 27 October 2022.

"Azure Active Directory - Microsoft Entra." Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory>. Accessed 25 October 2022.

"Azure Active Directory - Microsoft Entra." Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory>. Accessed 6 November 2022.

"Azure AD Identity Protection." Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-identity-protection>. Accessed 7 November 2022.

"Azure Arc – Hybrid and Multi-Cloud Management and Solution." Microsoft Azure, <https://azure.microsoft.com/en-us/products/azure-arc/#customer-stories>. Accessed 26 October 2022.

"Azure Arc – Hybrid and Multi-Cloud Management and Solution." Microsoft Azure, <https://azure.microsoft.com/en-us/products/azure-arc/#use-cases>. Accessed 7 November 2022.

"Azure DDoS Protection and Mitigation Services." Microsoft Azure, <https://azure.microsoft.com/en-us/services/ddos-protection/#features>. Accessed 6 November 2022.

"Azure DDoS Protection and Mitigation Services." Microsoft Azure, <https://azure.microsoft.com/en-us/services/ddos-protection/>. Accessed 7 November 2022.

"Azure Firewall – Cloud Network Security Solutions." Microsoft Azure, <https://azure.microsoft.com/en-us/services/azure-firewall/#features>. Accessed 6 November 2022.

"Azure Monitor - Modern Observability Tools." Microsoft Azure, <https://azure.microsoft.com/en-us/products/monitor/#partners>. Accessed 26 October 2022.

"Azure Monitor - Modern Observability Tools." Microsoft Azure, <https://azure.microsoft.com/en-us/products/monitor/#partners>. Accessed 7 November 2022.

Works Cited

“Azure Sentinel – Cloud-native SIEM Solution.” Microsoft Azure, <https://azure.microsoft.com/en-us/services/microsoft-sentinel/#overview>. Accessed 6 November 2022.

“Azure Sentinel – Cloud-native SIEM Solution.” Microsoft Azure, <https://azure.microsoft.com/en-us/services/microsoft-sentinel/>. Accessed 7 November 2022.

Baker, Kurt. “10 Pro Tips to Prevent Ransomware.” CrowdStrike, <https://www.crowdstrike.com/cybersecurity-101/ransomware/how-to-prevent-ransomware/>. Accessed 25 October 2022.

Banks, Martin. “Drowning in cloud silos? Time to think about the Curated Cloud.” Diginomica, 15 June 2022, <https://diginomica.com/drowning-cloud-silos-time-think-about-curated-cloud>. Accessed 7 November 2022.

“Becoming resilient by understanding cybersecurity risks: Part 2.” Microsoft, <https://www.microsoft.com/security/blog/2020/12/17/becoming-resilient-by-understanding-cybersecurity-risks-part-2/>. Accessed 25 October 2022.

Bharti, Gautam. “Create a Power BI datamart in minutes | Microsoft Power BI Blog.” Microsoft Power BI, 23 June 2022, <https://powerbi.microsoft.com/en-us/blog/create-a-power-bi-datamart-in-minutes/>. Accessed 7 November 2022.

Bisson, David. “Accenture Responds Following LockBit Ransomware Attack.” Cybereason, 12 August 2021, <https://www.cybereason.com/blog/accenture-responds-following-lockbit-ransomware-attack>. Accessed 25 October 2022.

“bitsadmin.” Microsoft Learn, 29 July 2021, <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/bitsadmin>. Accessed 24 October 2022.

Brown, Sara. “How to respond to a ransomware attack: Advice from a federal agent.” MIT Sloan, 19 January 2022, <https://mitsloan.mit.edu/ideas-made-to-matter/how-to-respond-to-a-ransomware-attack-advice-a-federal-agent>. Accessed 27 October 2022.

“Built-in virus protection in SharePoint Online, OneDrive, and Microsoft Teams - Office 365.” Microsoft Learn, 1 November 2022, <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/virus-detection-in-spo?view=o365-worldwide>. Accessed 6 November 2022.

“Built-in virus protection in SharePoint Online, OneDrive, and Microsoft Teams - Office 365.” Microsoft Learn, 1 November 2022, <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/virus-detection-in-spo?view=o365-worldwide>. Accessed 7 November 2022.

Works Cited

Chen, Jay. "Ransomware in Public Clouds: How TTPs Could Change." Unit 42, 16 May 2022, <https://unit42.paloaltonetworks.com/ransomware-in-public-clouds/>. Accessed 25 October 2022.

"CISA MS-ISAC Ransomware Guide." CISA, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf. Accessed 27 October 2022.

"CISA MS-ISAC Ransomware Guide." CISA, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf. Accessed 27 October 2022.

"CISOs Can Accelerate the Business." Splunk, <https://www.splunk.com/pdfs/ebooks/5-key-ways-ciso-can-accelerate-the-business.pdf>. Accessed 7 November 2022.

"Cloud Backup Services – Microsoft OneDrive." Microsoft, https://www.microsoft.com/microsoft-365/onedrive/pc-cloud-backup?ocid=oo_support_mix_marvel_ups_support_smconedrive_inline_cloudbackup. Accessed 6 November 2022.

"Cloud data security measures in SharePoint & OneDrive - SharePoint in Microsoft 365." Microsoft Learn, 25 August 2022, <https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data>. Accessed 7 November 2022.

"Cloud Security." Microsoft Azure, <https://azure.microsoft.com/en-us/product-categories/security/>. Accessed 25 October 2022.

"Cloud Security." Microsoft Azure, <https://azure.microsoft.com/en-us/product-categories/security/>. Accessed 6 November 2022.

Cobb, Jeff. "What Microsoft's \$20B investment in cybersecurity means for the talent gap - The SHI Hub." SHI Blog, 7 September 2021, <https://blog.shi.com/cybersecurity/what-microsofts-20b-investment-in-cybersecurity-means-for-the-talent-gap/>. Accessed 25 October 2022.

Cobb, Jeff. "What Microsoft's \$20B investment in cybersecurity means for the talent gap - The SHI Hub." SHI Blog, 7 September 2021, <https://blog.shi.com/cybersecurity/what-microsofts-20b-investment-in-cybersecurity-means-for-the-talent-gap/>. Accessed 6 November 2022.

"Conditional Access in Azure Active Directory." Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-conditional-access>. Accessed 27 October 2022.

"Configure a contact for use on a portal - Power Apps." Microsoft Learn, 12 October 2022, <https://docs.microsoft.com/en-us/power-apps/maker/portals/configure/configure-contacts>. Accessed 7 November 2022.

Works Cited

“Configure authentication in Power Pages.” Microsoft Learn, 12 October 2022, <https://docs.microsoft.com/en-us/power-pages/security/configure-portal-authentication>. Accessed 7 November 2022.

“Configure web roles in Power Pages.” Microsoft Learn, 12 October 2022, <https://docs.microsoft.com/en-us/power-pages/security/create-web-roles>. Accessed 7 November 2022.

“Configure web roles in Power Pages.” Microsoft Learn, 12 October 2022, <https://docs.microsoft.com/en-us/power-pages/security/create-web-roles>. Accessed 7 November 2022.

“Configuring table permissions in Power Pages.” Microsoft Learn, 12 October 2022, <https://docs.microsoft.com/en-us/power-pages/security/table-permissions>. Accessed 7 November 2022.

“Connect to the services you use with Power BI - Power BI.” Microsoft Learn, 18 August 2022, <https://docs.microsoft.com/en-us/power-bi/connect-data/service-connect-to-services>. Accessed 6 November 2022.

“Cost of a data breach 2022.” IBM, <https://www.ibm.com/security/data-breach/>. Accessed 6 November 2022.

“CRSP: The emergency team fighting cyber attacks beside customers.” Microsoft, 9 June 2021, <https://www.microsoft.com/security/blog/2021/06/09/crsp-the-emergency-team-fighting-cyber-attacks-beside-customers/>. Accessed 25 October 2022.

“CRSP: The emergency team fighting cyber attacks beside customers.” Microsoft, 9 June 2021, <https://www.microsoft.com/security/blog/2021/06/09/crsp-the-emergency-team-fighting-cyber-attacks-beside-customers/>. Accessed 6 November 2022.

Cupp, Deb. “Digital transformation is no longer just a competitive edge, but critical for business resilience | Transform.” Microsoft News, 6 May 2021, <https://news.microsoft.com/transform/digital-transformation-is-no-longer-just-a-competitive-edge-but-critical-for-business-resilience/>. Accessed 25 October 2022.

“Cyber Resilience | Security Insider.” Microsoft, 13 May 2022, <https://www.microsoft.com/en-us/security/business/security-insider/uncategorized/cyber-resilience/>. Accessed 27 October 2022.

“Cybersecurity Challenges in Asset Management Firms.” Deloitte, 14 October 2022, <https://www2.deloitte.com/us/en/pages/advisory/articles/asset-management-firms-facing-higher-cybersecurity-risk.html>. Accessed 25 October 2022.

Works Cited

“Cyber Signals: Issue 1.” Microsoft, 9 February 2022, <https://www.microsoft.com/en-us/security/business/security-insider/cyber-signals-1/summary-issue1/?culture=en-us&country=US>. Accessed 25 October 2022.

“Cyber Signals: Issue 1.” Microsoft, 9 February 2022, <https://www.microsoft.com/en-us/security/business/security-insider/cyber-signals-1/summary-issue1/?culture=en-us&country=US>. Accessed 6 November 2022.

“DarkSide Ransomware as a Service (RaaS) - United States Department of State.” State Department, 4 November 2021, <https://www.state.gov/darkside-ransomware-as-a-service-raas/>. Accessed 24 October 2022.

“DarkSide Ransomware as a Service (RaaS) - United States Department of State.” State Department, 4 November 2021, <https://www.state.gov/darkside-ransomware-as-a-service-raas/>. Accessed 24 October 2022.

“DART: the Microsoft cybersecurity team we hope you never meet.” Microsoft, 25 March 2019, <https://www.microsoft.com/security/blog/2019/03/25/dart-the-microsoft-cybersecurity-team-we-hope-you-never-meet/>. Accessed 27 October 2022.

“Data loss prevention and Microsoft Teams - Microsoft Purview (compliance).” Microsoft Learn, 28 October 2022, <https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide>. Accessed 6 November 2022.

“Data Protection with Microsoft Privacy Principles.” Microsoft, <https://www.microsoft.com/en-us/trust-center/privacy>. Accessed 6 November 2022.

“Data Security in Business Central - Business Central.” Microsoft Learn, 15 February 2022, <https://docs.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/data-security?tabs=database-level>. Accessed 6 November 2022.

“Decentralized Identity.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY>. Accessed 7 November 2022.

“Decentralized Identity.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY>. Accessed 7 November 2022.

“Defend and deter - Microsoft On the Issues.” The Official Microsoft Blog, 30 May 2021, <https://blogs.microsoft.com/on-the-issues/2021/05/30/nobelium-cybersecurity-cyberattacks-phishing/>. Accessed 25 October 2022.

Works Cited

“Defender for Cloud’s integrated vulnerability assessment solution for Azure, hybrid, and multicloud machines.” Microsoft Learn, 12 October 2022, <https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm>. Accessed 26 October 2022.

“Defender for Cloud’s integrated vulnerability assessment solution for Azure, hybrid, and multicloud machines.” Microsoft Learn, 31 October 2022, <https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm>. Accessed 7 November 2022.

“Definitive guide to ransomware 2022.” IBM, <https://www.ibm.com/downloads/cas/EV6NAQR4>. Accessed 27 October 2022.

“Destructive malware targeting Ukrainian organizations.” Microsoft, 15 January 2022, <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>. Accessed 24 October 2022.

“Destructive malware targeting Ukrainian organizations.” Microsoft, 15 January 2022, <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>. Accessed 25 October 2022.

“Destructive malware targeting Ukrainian organizations.” Microsoft, 15 January 2022, <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>. Accessed 6 November 2022.

“Destructive malware targeting Ukrainian organizations.” Microsoft, 15 January 2022, <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>. Accessed 6 November 2022.

“Device discovery overview.” Microsoft Learn, 29 September 2022, <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/device-discovery?view=o365-worldwide>. Accessed 27 October 2022.

“Digital Crimes Unit: Leading the fight against cybercrime.” Microsoft News, 3 May 2022, <https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/>. Accessed 25 October 2022.

“Digital Crimes Unit: Leading the fight against cybercrime.” Microsoft News, 3 May 2022, <https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/>. Accessed 6 November 2022.

Works Cited

“Directory of Azure Cloud Services.” Microsoft Azure, <https://azure.microsoft.com/en-us/services/>. Accessed 6 November 2022.

Drapkin, Aaron. “82% of Ransomware Attacks Target Small Businesses, Report Reveals.” Tech.co, 7 February 2022, <https://tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals>. Accessed 24 October 2022.

“Dynamics 365 Business Central - Microsoft Cloud ERP.” Velosio, <https://www.velosio.com/products/dynamics-365-business-central/>. Accessed 6 November 2022.

“Enabling remote work at Microsoft.” Microsoft, <https://www.microsoft.com/en-us/insidetrack/enabling-remote-work-at-microsoft>. Accessed 24 October 2022.

“Evolving Zero Trust – Microsoft Position Paper.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Accessed 27 October 2022.

“Evolving Zero Trust – Microsoft Position Paper.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Accessed 27 October 2022.

“Evolving Zero Trust – Microsoft Position Paper.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Accessed 27 October 2022.

“Evolving Zero Trust – Microsoft Position Paper.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Accessed 6 November 2022.

“Evolving Zero Trust – Microsoft Position Paper.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Accessed 6 November 2022.

“Evolving Zero Trust – Microsoft Position Paper.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Accessed 6 November 2022.

“Evolving Zero Trust – Microsoft Position Paper.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Accessed 7 November 2022.

“Evolving Zero Trust – Microsoft Position Paper.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>. Accessed 7 November 2022.

“5 Biggest Ransomware Attacks in History.” Swiss Cyber Institute, 27 September 2021, <https://swisscyberinstitute.com/blog/5-biggest-ransomware-attacks-in-history/>. Accessed 24 October 2022.

Works Cited

Fritz, Anton. "Detect upload of sensitive information to Power BI using Microsoft 365 data loss prevention policies." Microsoft Power BI, 4 April 2022, <https://powerbi.microsoft.com/en-us/blog/detect-upload-of-sensitive-information-to-power-bi-using-microsoft-365-data-loss-prevention-policies/>. Accessed 7 November 2022.

Fritz, Anton. "Detect upload of sensitive information to Power BI using Microsoft 365 data loss prevention policies." Microsoft Power BI, 4 April 2022, <https://powerbi.microsoft.com/en-us/blog/detect-upload-of-sensitive-information-to-power-bi-using-microsoft-365-data-loss-prevention-policies/>. Accessed 7 November 2022.

Fritz, Anton. "Detect upload of sensitive information to Power BI using Microsoft 365 data loss prevention policies." Microsoft Power BI, 4 April 2022, <https://powerbi.microsoft.com/en-us/blog/detect-upload-of-sensitive-information-to-power-bi-using-microsoft-365-data-loss-prevention-policies/>. Accessed 7 November 2022.

Gaga, Lady, and Bradley Cooper. "???" ??? - YouTube, 17 January 2022, <https://www.microsoft.com/en-us/security/business?rtc=1>. Accessed 24 October 2022.

Gaga, Lady, and Bradley Cooper. "???" ??? - YouTube, 17 January 2022, https://www.ibm.com/downloads/cas/ADLMYLAZ?_ga=2.267108489.620381187.1650593767-1434335883.1650502901. Accessed 24 October 2022.

Gaga, Lady, and Bradley Cooper. "???" ??? - YouTube, 17 January 2022, <https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperRansomwareRealitiesSMB.pdf>. Accessed 24 October 2022.

Gaga, Lady, and Bradley Cooper. "???" ??? - YouTube, 17 January 2022, https://www.ibm.com/downloads/cas/ADLMYLAZ?_ga=2.267108489.620381187.1650593767-1434335883.1650502901. Accessed 24 October 2022.

Gaga, Lady, and Bradley Cooper. "???" ??? - YouTube, 17 January 2022, https://www.bain.com/globalassets/noindex/2022/bain_report_machinery-and-equipment-report-2022.pdf. Accessed 24 October 2022.

"Gartner Survey of Over 2,000 CIOs Reveals the Need to Accelerate Time to Value from Digital Investments." Gartner, 18 October 2022, <https://www.gartner.com/en/newsroom/press-releases/2022-10-18-gartner-survey-of-over-2000-cios-reveals-the-need-to-accelerate-time-to-value-from-digital-investments>. Accessed 6 November 2022.

Works Cited

“General Data Protection Regulation, GDPR Overview.” Microsoft, <https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview>. Accessed 6 November 2022.

Germain, John. “Duck Creek Technologies increases security and visibility with multiple Microsoft security layers.” Microsoft Customer Stories, 21 January 2021, <https://customers.microsoft.com/en-us/story/863023-duck-creek-technologies-professional-services-azure-sentinel?culture=en-us&country=US>. Accessed 26 October 2022.

“Global almond supplier engages with AgreeYa to drive digital transformation.” Microsoft Customer Stories, 9 December 2021, <https://customers.microsoft.com/en-us/story/1447698806553284174-bluedia-mondgrowers-agreeyasolutions-microsoft365>. Accessed 7 November 2022.

“Global Cybersecurity Outlook 2022 | weforum.org.” weforum.org, 1 January 2022, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf. Accessed 25 October 2022.

“Global Cybersecurity Outlook 2022 | weforum.org.” weforum.org, 1 January 2022, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf. Accessed 27 October 2022.

“Global Cybersecurity Outlook 2022 | weforum.org.” weforum.org, 1 January 2022, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf. Accessed 6 November 2022.

“The growing threat of ransomware - Microsoft On the Issues.” The Official Microsoft Blog, 20 July 2021, <https://blogs.microsoft.com/on-the-issues/2021/07/20/the-growing-threat-of-ransomware/>. Accessed 27 October 2022.

“The growing threat of ransomware - Microsoft On the Issues.” The Official Microsoft Blog, 20 July 2021, <https://blogs.microsoft.com/on-the-issues/2021/07/20/the-growing-threat-of-ransomware/>. Accessed 6 November 2022.

Guide, Step. “Even the Most Advanced Threats Rely on Unpatched Systems.” The Hacker News, 9 June 2022, <https://thehackernews.com/2022/06/even-most-advanced-threats-rely-on.html>. Accessed 25 October 2022.

Hallum, Chris. “New research shows IoT and OT innovation is critical to business but comes with significant risks.” Microsoft, 8 December 2021, <https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/>. Accessed 24 October 2022.

Works Cited

Harding, Joanna. "Uncover your blind spots: seamlessly control cloud usage risks to your organization." Microsoft Tech Community, 9 March 2021, <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/uncover-your-blind-spots-seamlessly-control-cloud-usage-risks-to/ba-p/2157447>. Accessed 25 October 2022.

Harding, Joanna. "Uncover your blind spots: seamlessly control cloud usage risks to your organization." Microsoft Tech Community, 9 March 2021, <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/uncover-your-blind-spots-seamlessly-control-cloud-usage-risks-to/ba-p/2157447>. Accessed 26 October 2022.

Harding, Joanna. "Uncover your blind spots: seamlessly control cloud usage risks to your organization." Microsoft Tech Community, 9 March 2021, <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/uncover-your-blind-spots-seamlessly-control-cloud-usage-risks-to/ba-p/2157447>. Accessed 27 October 2022.

Harding, Joanna. "Uncover your blind spots: seamlessly control cloud usage risks to your organization." Microsoft Tech Community, 9 March 2021, <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/uncover-your-blind-spots-seamlessly-control-cloud-usage-risks-to/ba-p/2157447>. Accessed 6 November 2022.

Harding, Joanna. "Uncover your blind spots: seamlessly control cloud usage risks to your organization." Microsoft Tech Community, 9 March 2021, <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/uncover-your-blind-spots-seamlessly-control-cloud-usage-risks-to/ba-p/2157447>. Accessed 6 November 2022.

Harding, Joanna. "Uncover your blind spots: seamlessly control cloud usage risks to your organization." Microsoft Tech Community, 9 March 2021, <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/uncover-your-blind-spots-seamlessly-control-cloud-usage-risks-to/ba-p/2157447>. Accessed 7 November 2022.

Hogan, Amy. "How cyberattacks are changing according to new Microsoft Digital Defense Report." Microsoft, 11 October 2021, <https://www.microsoft.com/security/blog/2021/10/11/how-cyberattacks-are-changing-according-to-new-microsoft-digital-defense-report/>. Accessed 24 October 2022.

"Home." YouTube, <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-risk-future-of-cyber-survey.pdf>. Accessed 27 October 2022.

"Home." YouTube, <https://docs.google.com/document/d/1z0aiC2vWIESFbKItiQautmeiqTymww8vMgd0A-N319A/edit>. Accessed 27 October 2022.

Works Cited

“Home.” YouTube, <https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview?source=recommendations>. Accessed 27 October 2022.

“Home.” YouTube, <https://dsimg.ubm-us.net/envelope/435853/719113/The%20Future%20of%20Threat%20Intelligence.pdf>. Accessed 27 October 2022.

“Home.” YouTube, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/state-security-automation.pdf?utm_source=marketo&utm_medium=email&utm_campaign=Global-DA-EN-2021-12-06-7014u000001hDpDAAU-P3-Cortex-the-state-of-SOAR-automation. Accessed 27 October 2022.

“Home.” YouTube, <https://customers.microsoft.com/en-us/story/1541638065841628581-ccc-group-retailers-azure-en-poland>. Accessed 27 October 2022.

“How common are ransomware attacks?” The World Economic Forum, 26 November 2021, <https://www.weforum.org/agenda/2021/11/industries-affected-ransomware-cybersecurity-cybercrime/>. Accessed 24 October 2022.

“How OneDrive safeguards your data in the cloud.” Microsoft Support, <https://support.microsoft.com/en-us/office/how-onedrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1>. Accessed 6 November 2022.

“How to improve risk management using Zero Trust architecture.” Microsoft, 23 May 2022, <https://www.microsoft.com/security/blog/2022/05/23/how-to-improve-risk-management-using-zero-trust-architecture/>. Accessed 25 October 2022.

“Human-operated ransomware.” Microsoft Learn, 30 August 2022, <https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware>. Accessed 24 October 2022.

“Human-operated ransomware attacks: A preventable disaster.” Microsoft, 5 March 2020, <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>. Accessed 6 November 2022.

“Human-operated ransomware attacks: A preventable disaster.” Microsoft, 5 March 2020, <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>. Accessed 6 November 2022.

“Human-operated ransomware attacks: A preventable disaster.” Microsoft, 5 March 2020, <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>. Accessed 6 November 2022.

Works Cited

“Identity and Access.” Microsoft, <https://www.microsoft.com/en-us/security/business/solutions/identity-access>. Accessed 7 November 2022.

Ikeda, Scott. “Colonial Fuel Pipeline Ransomware Attack That Caused Gas Shortages in Eastern U.S. May Be the Work of Amateurs.” CPO Magazine, 12 May 2021, <https://www.cpomagazine.com/cyber-security/colonial-fuel-pipeline-ransomware-attack-that-caused-gas-shortages-in-eastern-u-s-may-be-the-work-of-amateurs/>. Accessed 6 November 2022.

“Increasing resilience against Solorigate and other sophisticated attacks with Microsoft Defender.” Microsoft, 14 January 2021, <https://www.microsoft.com/security/blog/2021/01/14/increasing-resilience-against-solorigate-and-other-sophisticated-attacks-with-microsoft-defender/?culture=en-us&country=US#Protecting-on-premises-cloud-infrastructure>. Accessed 26 October 2022.

“Investigate incidents with Microsoft Sentinel.” Microsoft Learn, 26 July 2022, <https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>. Accessed 6 November 2022.

“Investigate incidents with Microsoft Sentinel.” Microsoft Learn, 26 July 2022, <https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>. Accessed 6 November 2022.

“Investigate incidents with Microsoft Sentinel.” Microsoft Learn, 26 July 2022, <https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>. Accessed 7 November 2022.

“Invite contacts to your portals - Power Apps.” Microsoft Learn, 12 October 2022, <https://docs.microsoft.com/en-us/power-apps/maker/portals/configure/invite-contacts>. Accessed 7 November 2022.

“ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud - Microsoft Compliance.” Microsoft Learn, 20 September 2022, <https://docs.microsoft.com/en-us/compliance/regulatory/offering-ISO-27018?view=o365-worldwide>. Accessed 6 November 2022.

“Is the New Battleground.” Microsoft News, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWUGFg>. Accessed 25 October 2022.

“Is the New Battleground.” Microsoft News, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWUGFg>. Accessed 6 November 2022.

“IT Modernization to Reduce Ransomware Risk.” Accenture, 23 August 2022, <https://www.accenture.com/us-en/blogs/cloud-computing/fight-ransomware-with-it-modernization>. Accessed 27 October 2022.

Kelly, Stephanie, and Jessica Resnick. “One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators.” Reuters, 8 June 2021, <https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/>. Accessed 25 October 2022.

Works Cited

“The Key to Risk Intelligence: Visibility.” SecurityScorecard, 29 June 2022, <https://securityscorecard.com/blog/the-key-to-risk-intelligence-visibility>. Accessed 25 October 2022.

Kovar, Joseph F. “Mandiant: No Evidence Of LockBit 2.0 Ransomware Attack ‘At This Point.’” CRN, 6 June 2022, <https://www.crn.com/news/security/mandiant-no-evidence-of-lockbit-2-0-ransomware-attack-at-this-point->. Accessed 25 October 2022.

Koziol, Jack. “How Training Employees About Ransomware Can Mitigate Cyber Risk.” Forbes, 28 April 2022, <https://www.forbes.com/advisor/business/training-employees-about-ransomware/>. Accessed 25 October 2022.

Kråkhede, Jesper. “Microsoft security experts outline next steps after compromise recovery.” Microsoft, 10 May 2022, <https://www.microsoft.com/security/blog/2022/05/10/microsoft-security-experts-outline-next-steps-after-compromise-recovery/>. Accessed 27 October 2022.

Kråkhede, Jesper. “Microsoft security experts outline next steps after compromise recovery.” Microsoft, 10 May 2022, <https://www.microsoft.com/security/blog/2022/05/10/microsoft-security-experts-outline-next-steps-after-compromise-recovery/>. Accessed 27 October 2022.

Kråkhede, Jesper. “Microsoft security experts outline next steps after compromise recovery.” Microsoft, 10 May 2022, <https://www.microsoft.com/security/blog/2022/05/10/microsoft-security-experts-outline-next-steps-after-compromise-recovery/>. Accessed 27 October 2022.

Krispin, David, et al. “Proofpoint Discovers Potentially Dangerous Microsoft Office 365 Functionality that can Ransom Files Stored on SharePoint and OneDrive.” Proofpoint, 16 June 2022, <https://www.proofpoint.com/us/blog/cloud-security/proofpoint-discovers-potentially-dangerous-microsoft-office-365-functionality>. Accessed 7 November 2022.

“Land O’Lakes, Inc. shares the recipe for multicloud protection: Microsoft Defender for Containers, related solutions.” Microsoft Customer Stories, 2 August 2022, <https://customers.microsoft.com/en-us/story/1532036609741605119-land-o-lakes-consumer-goods-microsoft-security-solutions>. Accessed 26 October 2022.

“Learn about insider risk management - Microsoft Purview (compliance).” Microsoft Learn, 31 October 2022, <https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide>. Accessed 6 November 2022.

Works Cited

Lemos, Robert. "The Market Is Teeming: Bargains on Dark Web Give Novice Cybercriminals a Quick Start." Dark Reading, 21 July 2022, <https://www.darkreading.com/threat-intelligence/market-bargains-dark-web-novice-cybercriminals-quick-start>. Accessed 25 October 2022.

Linn, Allison. "Securing the cloud | Microsoft Story Labs." Microsoft News, <https://news.microsoft.com/stories/cloud-security/>. Accessed 25 October 2022.

Linn, Allison. "Securing the cloud | Microsoft Story Labs." Microsoft News, <https://news.microsoft.com/stories/cloud-security/>. Accessed 6 November 2022.

Lourenco, Rafael. "Cybersecurity Improvements May Be the Best Customer Experience Tool You're Not Using." CPO Magazine, 14 October 2021, <https://www.cpomagazine.com/cyber-security/cybersecurity-improvements-may-be-the-best-customer-experience-tool-youre-not-using/>. Accessed 25 October 2022.

"Malware and ransomware protection in Microsoft 365 - Microsoft Service Assurance." Microsoft Learn, 22 September 2022, <https://docs.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection>. Accessed 6 November 2022.

"Manage devices with Intune." Microsoft Learn, 22 September 2022, <https://docs.microsoft.com/en-us/microsoft-365/solutions/manage-devices-with-intune-overview?view=o365-worldwide#coordinating-endpoint-management-with-zero-trust-identity-and-device-access-policies>. Accessed 6 November 2022.

"Manage endpoint security in Microsoft Intune." Microsoft Learn, 1 September 2022, <https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security#review-security-tasks-from-microsoft-defender-for-endpoint>. Accessed 6 November 2022.

"Mar29-Ransomware Infographic_033122-April8." Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4VD4j?culture=en-us&country=US>. Accessed 25 October 2022.

"Mar29-Ransomware Infographic_033122-April8." Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4VD4j?culture=en-us&country=US>. Accessed 6 November 2022.

"MARCH 2022." Zerto, <https://www.zerto.com/wp-content/uploads/2022/04/ESG-eBook-Zerto-Ransomware-Preparedness-March-2022.pdf>. Accessed 24 October 2022.

McKeon, Jill. "Cyberattacks Against Health Plans, Business Associates Increase." Health IT Security, 31 January 2022, <https://healthitsecurity.com/news/cyberattacks-against-health-plans-business-associates-increase>. Accessed 25 October 2022.

Works Cited

McKeon, Jill. "Key Differences Between PHI and PII, How They Impact HIPAA Compliance." Health IT Security, 17 September 2021, <https://healthitsecurity.com/news/key-differences-between-phi-and-pii-how-they-impact-hipaa-compliance>. Accessed 25 October 2022.

McKie, Amy. "Surviving the Storm: 8 Steps for Creating a Disaster Recovery Plan ..." Velosio, 31 March 2022, <https://www.velosio.com/blog/disaster-recovery-plan-template/>. Accessed 25 October 2022.

McKie, Amy. "Surviving the Storm: 8 Steps for Creating a Disaster Recovery Plan ..." Velosio, 31 March 2022, <https://www.velosio.com/blog/disaster-recovery-plan-template/>. Accessed 6 November 2022.

Mehrotra, Kartikay, and William Turton. "CNA Financial Paid \$40 Million in Ransom After March Cyberattack." Bloomberg.com, 20 May 2021, <https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack#xj4y7vzkg>. Accessed 25 October 2022.

"Microsoft 365 admin center activity reports - Microsoft 365 admin." Microsoft Learn, 25 October 2022, <https://docs.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports?view=o365-worldwide>. Accessed 7 November 2022.

"Microsoft Azure Cloud Services - Azure Managed Services." Velosio, <https://www.velosio.com/expertise/azure-cloud-services/>. Accessed 6 November 2022.

"Microsoft Azure Cloud Services - Azure Managed Services." Velosio, <https://www.velosio.com/expertise/azure-cloud-services/>. Accessed 7 November 2022.

"Microsoft Customer Story-Johnson & Johnson transforms business through intelligent automation." Microsoft Customer Stories, 23 May 2022, <https://customers.microsoft.com/en-us/story/1507762742083750162-johnson-pharmaceuticals-azure-en-united-states>. Accessed 27 October 2022.

"Microsoft Defender for Cloud - CSPM & CWPP." Microsoft Azure, <https://azure.microsoft.com/en-us/services/defender-for-cloud/>. Accessed 6 November 2022.

"Microsoft Defender for Cloud - CSPM & CWPP." Microsoft Azure, <https://azure.microsoft.com/en-us/services/defender-for-cloud/>. Accessed 7 November 2022.

"Microsoft Defender for Endpoint." Microsoft Learn, 29 September 2022, <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide>. Accessed 6 November 2022.

Works Cited

“Microsoft Defender for Office 365 service description - Service Descriptions.” Microsoft Learn, 2 September 2022, <https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description>. Accessed 6 November 2022.

“Microsoft Digital Defense Report OCTOBER 2021.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFli>. Accessed 27 October 2022.

“Microsoft Digital Defense Report OCTOBER 2021.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFli>. Accessed 6 November 2022.

“Microsoft Dynamics 365 Finance and Operations.” Velosio, <https://www.velosio.com/products/dynamics-365-finance/>. Accessed 6 November 2022.

“Microsoft Entra Permissions Management.” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-permissions-management>. Accessed 25 October 2022.

“Microsoft Entra Permissions Management.” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-permissions-management>. Accessed 6 November 2022.

“Microsoft Entra Verified ID.” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-verified-id>. Accessed 25 October 2022.

“Microsoft Entra Verified ID.” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-verified-id>. Accessed 6 November 2022.

“Microsoft Entra Verified ID.” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-verified-id>. Accessed 7 November 2022.

“Microsoft Entra Verified ID.” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-verified-id>. Accessed 7 November 2022.

“Microsoft Office 365 | Microsoft Productivity Software.” Velosio, <https://www.velosio.com/products/microsoft-office-365/>. Accessed 6 November 2022.

“Microsoft Office 365 | Microsoft Productivity Software.” Velosio, <https://www.velosio.com/products/microsoft-office-365/>. Accessed 6 November 2022.

“Microsoft OneDrive Cloud Storage and File Sharing.” Microsoft, <https://www.microsoft.com/en-us/microsoft-365/onedrive/onedrive-for-business>. Accessed 6 November 2022.

Works Cited

“Microsoft Power Automate | Power Platform.” Velosio, <https://www.velosio.com/products/microsoft-power-platform/power-automate/>. Accessed 7 November 2022.

“Microsoft Power BI | Business Intelligence Solution.” Velosio, <https://www.velosio.com/products/microsoft-power-platform/power-bi/>. Accessed 7 November 2022.

“Microsoft Research Report Final 1.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWREzU>. Accessed 24 October 2022.

“Microsoft Secure Score.” Microsoft Learn, 19 October 2022, <https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score>. Accessed 26 October 2022.

“Microsoft Security CISO Insider Issue 1.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWUje9>. Accessed 7 November 2022.

“Microsoft Zero Trust Maturity Assessment Quiz.” Microsoft, <https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool?activetab=solution-wizard;primaryr1>. Accessed 27 October 2022.

“Microsoft Zero Trust Maturity Assessment Quiz.” Microsoft, <https://www.microsoft.com/en-us/security/business/zero-trust/maturity-model-assessment-tool?activetab=solution-wizard;primaryr1>. Accessed 6 November 2022.

“Modern SOC.” Splunk, https://www.splunk.com/en_us/pdfs/resources/e-book/10-essential-capabilities-of-a-modern-soc.pdf. Accessed 26 October 2022.

Morrison, Sara. “JBS Foods, the meat supplier hit by a ransomware attack, admits it paid \$11 million in ransom.” Vox, 10 June 2021, <https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers>. Accessed 25 October 2022.

“Multifactor Authentication (MFA).” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-mfa-multi-factor-authentication>. Accessed 25 October 2022.

“Multifactor Authentication (MFA).” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-mfa-multi-factor-authentication>. Accessed 27 October 2022.

Nase, John Paulo. “???” ??? - YouTube, 17 January 2022, <https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-jbs-cyberattack>. Accessed 25 October 2022.

Works Cited

- Nase, John Paulo. “???” ??? - YouTube, 17 January 2022, <https://go.crowdstrike.com/rs/281-OBQ-266/images/eBookProtectorsoftheCloudEng.pdf>. Accessed 25 October 2022.
- Nase, John Paulo. “???” ??? - YouTube, 17 January 2022, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4XVMS?culture=en-us&country=US>. Accessed 25 October 2022.
- Nase, John Paulo. “???” ??? - YouTube, 17 January 2022, <https://www.protocol.com/braintrust/ransomware-lessons-for-executives-cybersecurity?rebellitem=14#rebellitem14>. Accessed 25 October 2022.
- Nase, John Paulo. “???” ??? - YouTube, 17 January 2022, <https://cloudhealth.vmware.com/content/dam/digitalmarketing/cloudhealth/pdfs/The-State-of-Cloud-Security-Risk-Compliance-and-Misconfigurations.pdf>. Accessed 25 October 2022.
- Nase, John Paulo. “???” ??? - YouTube, 17 January 2022, <https://s3.amazonaws.com/content-production.cloudsecurityalliance/zyaqubn85bt9mfnh5uv6f2n3x6mj?response-content-disposition=inline%3B%20filename%3D%22TopThreatstoCloudComputingPandemicEleven060622.pdf%22%3B%20filename%2A%3DUTF-8%27%27TopThreatstoCloudCompu>. Accessed 25 October 2022.
- Nase, John Paulo. “???” ??? - YouTube, 17 January 2022, https://customers.microsoft.com/en-us/story/1485503925982078204-qnet-retailers-security-solution?ocid=eml_pg346823_gdc_comm_mw&mkt_tok=MTU3LUdRRS0zODIAAAGFC9KbwhL3QS3eHvgrMruG_HGmtsG6KYsygyyRbUWp3NRL_ypZu7_I9BbMQJm7jMZM-UQIFDEsvQld08nwvsDf4yrNuoWEwL6L8G_j6. Accessed 25 October 2022.
- Nase, John Paulo. “???” ??? - YouTube, 17 January 2022, https://customers.microsoft.com/en-us/story/1477343163449418453-martin-zerfoss-insurance-defender-for-business?icid=SMB_feature_security. Accessed 25 October 2022.
- “New Research from Axonius Finds Despite SaaS Spend Eclipsing IaaS, SaaS Security Not a Priority... Yet.” Axonius, 31 August 2022, <https://www.axonius.com/press-releases/axonius-announces-new-research-on-saas-security>. Accessed 27 October 2022.
- Norton, Carolyn, et al. “The Risk of On-Premises for Businesses with Small IT Teams.” Velosio, 21 July 2022, <https://www.velosio.com/blog/risk-of-on-premises-solutions/>. Accessed 26 October 2022.
- “117,298 613 375 Anatomy of an external attack surface: +41% +33% 18,378 15 <10% 53% 560,000+ +74% 1 new +33% 23 1.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4VjO9>. Accessed 7 November 2022.
- “On-premise to Microsoft Dynamics 365 Cloud CRM.” Velosio, <https://www.velosio.com/products/dynamics-365-crm/>. Accessed 6 November 2022.

Works Cited

“Page permissions in Power Pages.” Microsoft Learn, 4 October 2022, <https://docs.microsoft.com/en-us/power-pages/security/page-security>. Accessed 7 November 2022.

“Passwordless authentication.” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication>. Accessed 6 November 2022.

“Power Automate.” Power Automate, <https://dynamics.microsoft.com/en-us/guidedtour/power-platform/power-automate/3/3>. Accessed 7 November 2022.

“Power Pages security.” Microsoft Learn, 12 October 2022, <https://docs.microsoft.com/en-us/power-pages/security/power-pages-security>. Accessed 7 November 2022.

“Ransomcloud.” Infosecurity Magazine, <https://www.infosecurity-magazine.com/opinions/ransom-cloud-ransomwares-cloud/>. Accessed 25 October 2022.

“Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself.” Microsoft, 9 May 2022, <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>. Accessed 24 October 2022.

“Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself.” Microsoft, 9 May 2022, <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#cloud-hardening>. Accessed 25 October 2022.

“Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself.” Microsoft, 9 May 2022, <https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/#cloud-hardening>. Accessed 6 November 2022.

“Ransomware attack on Planned Parenthood LA exposes info for 400000 patients.” The Verge, 2 December 2021, <https://www.theverge.com/2021/12/2/22814635/planned-parenthood-ransomware-malware-attack-abortion-rights-data-leak>. Accessed 25 October 2022.

“Ransomware demands soar by 518% in 2021 | News.” GRC World Forums, 13 August 2021, <https://www.grcworldforums.com/ransomware/ransomware-demands-soar-by-518-in-2021/2357.article>. Accessed 24 October 2022.

“Ransomware Detection Defined: Attack Types & Techniques.” CrowdStrike, 21 March 2022, <https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-detection/>. Accessed 27 October 2022.

Works Cited

“Ransomware — FBI.” FBI, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware>. Accessed 25 October 2022.

“Ransomware groups continue to target healthcare, critical services; here’s how to reduce risk.” Microsoft, 28 April 2020, <https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/#vulnerable-and-unmonitored-internet-facing-systems>. Accessed 25 October 2022.

Rashid, Adeeb. “Cyber Security and the Metaverse: Patrolling the New Digital World.” Security Intelligence, 4 August 2022, <https://securityintelligence.com/posts/metaverse-cybersecurity-concerns/>. Accessed 27 October 2022.

“The regulatory compliance dashboard in Microsoft Defender for Cloud.” Microsoft Learn, 18 October 2022, <https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages>. Accessed 6 November 2022.

“Restore your OneDrive.” Microsoft Support, <https://support.microsoft.com/en-us/office/restore-your-one-drive-fa231298-759d-41cf-bcd0-25ac53eb8a15>. Accessed 6 November 2022.

“Scenarios for using Conditional Access with Microsoft Intune - Microsoft Intune.” Microsoft Learn, 19 April 2022, <https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use>. Accessed 6 November 2022.

Schläpfer, Patrick. “The Evolution of Cybercrime: Why the Dark Web is Supercharging the Threat Landscape and How to Fight Back | HP Wolf Security.” HP Wolf Security Blog, 21 July 2022, <https://threatresearch.ext.hp.com/evolution-of-cybercrime-report/>. Accessed 27 October 2022.

“SCI MDO Solution Brief - Prevention & Detection.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWSD6b>. Accessed 6 November 2022.

“Secure access for a connected world—meet Microsoft Entra.” Microsoft, 31 May 2022, <https://www.microsoft.com/security/blog/2022/05/31/secure-access-for-a-connected-worldmeet-microsoft-entra/>. Accessed 6 November 2022.

“Securing cloud workloads for speed and agility.” McKinsey, 22 July 2021, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/security-as-code-the-best-and-maybe-only-path-to-securing-cloud-applications-and-systems>. Accessed 27 October 2022.

“Securing Microsoft’s network with an internet-first, Zero Trust model.” Microsoft, 16 April 2021, <https://www.microsoft.com/en-us/insidetrack/securing-microsofts-network-with-an-internetfirst-zero-trust-model>. Accessed 24 October 2022.

Works Cited

- “Securing privileged access overview.” Microsoft Learn, 7 September 2022, <https://docs.microsoft.com/en-us/security/compass/overview>. Accessed 25 October 2022.
- “Securing privileged access overview.” Microsoft Learn, 7 September 2022, <https://docs.microsoft.com/en-us/security/compass/overview>. Accessed 25 October 2022.
- “Security and data access (Microsoft Dataverse) - Power Apps.” Microsoft Learn, 15 February 2022, <https://docs.microsoft.com/en-us/power-apps/developer/data-platform/security-model>. Accessed 7 November 2022.
- “Security measures for protecting data - Dynamics 365 Fraud Protection.” Microsoft Learn, 14 June 2022, <https://docs.microsoft.com/en-us/dynamics365/fraud-protection/compliance-and-security>. Accessed 25 October 2022.
- “Security measures for protecting data - Dynamics 365 Fraud Protection.” Microsoft Learn, 14 June 2022, <https://docs.microsoft.com/en-us/dynamics365/fraud-protection/compliance-and-security>. Accessed 6 November 2022.
- “Security Operations Self-Assessment Tool.” Microsoft, <https://www.microsoft.com/en-us/security/business/threat-protection/security-operations-assessment?activetab=solution-wizard:primaryr2>. Accessed 26 October 2022.
- “Security posture for Microsoft Defender for Cloud.” Microsoft Learn, 19 July 2022, <https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>. Accessed 6 November 2022.
- “Security posture for Microsoft Defender for Cloud.” Microsoft Learn, 19 July 2022, <https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>. Accessed 6 November 2022.
- “Services | Business Software & Technology Consulting Services.” Velosio, <https://www.velosio.com/products/>. Accessed 6 November 2022.
- Sharton, Brenda R. “Ransomware Attacks Are Spiking. Is Your Company Prepared?” Harvard Business Review, 20 May 2021, <https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared>. Accessed 27 October 2022.
- Shevchenko, Yana, and David Buxton. “Do we need XDR?” Kaspersky, 24 March 2022, <https://www.kaspersky.com/blog/do-you-need-xdr/43993/>. Accessed 25 October 2022.
- Simpson, Andrew G. “Meat Producer JBS Paid \$11M in Ransom to Cyber Attackers.” Insurance Journal, 10 June 2021, <https://www.insurancejournal.com/news/national/2021/06/10/618052.htm>. Accessed 25 October 2022.

Works Cited

“Single Sign-On (SSO): Secure App Access Solutions.” Microsoft, <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-single-sign-on>. Accessed 6 November 2022.

“Sodinokibi/REvil Ransomware Gang Hit Acer with \$50M Ransom Demand.” Cybereason, 23 March 2021, <https://www.cybereason.com/blog/sodinokibi/revil-ransomware-gang-hit-acer-with-50m-ransom-demand>. Accessed 24 October 2022.

“So it *is* a backup? : r/onedrive.” Reddit, 29 May 2022, https://www.reddit.com/r/onedrive/comments/v0fs3s/so_it_is_a_backup/. Accessed 6 November 2022.

“SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic).” GAO, 22 April 2021, <https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic>. Accessed 25 October 2022.

“Sophos State of Ransomware 2021.” Sophos, <https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469>. Accessed 24 October 2022.

“Threat Protection - SIEM and XDR Tools.” Microsoft, <https://www.microsoft.com/en-us/security/business/threat-protection>. Accessed 25 October 2022.

“Threat Protection - SIEM and XDR Tools.” Microsoft, <https://www.microsoft.com/en-us/security/business/threat-protection>. Accessed 25 October 2022.

“Threat Protection - SIEM and XDR Tools.” Microsoft, <https://www.microsoft.com/en-us/security/business/threat-protection>. Accessed 25 October 2022.

“Threat Protection - SIEM and XDR Tools.” Microsoft, <https://www.microsoft.com/en-us/security/business/threat-protection>. Accessed 6 November 2022.

“Threat Protection - SIEM and XDR Tools.” Microsoft, <https://www.microsoft.com/en-us/security/business/threat-protection>. Accessed 6 November 2022.

Torres, Daniel, and Bill Anderson. “Learn How Microsoft 365 Detects Ransomware Attacks.” Velosio, 19 January 2021, <https://www.velosio.com/blog/microsoft-onedrive-speed-recovery-from-ransomware-attack/>. Accessed 6 November 2022.

Torres, Daniel, and Bill Anderson. “Microsoft Dynamics 365 Security - D365 Security Best Practices.” Velosio, 3 November 2021, <https://www.velosio.com/blog/microsoft-dynamics-365-security/>. Accessed 6 November 2022.

Works Cited

Torres, Daniel, and Phil Wittmer. "An Overview of Microsoft Dynamics Lifecycle Services." Velosio, 3 November 2021, <https://www.velosio.com/blog/microsoft-dynamics-365-lifecycle-services/>. Accessed 6 November 2022.

Truta, Filip. "60% of Breaches in 2019 Involved Unpatched Vulnerabilities." Security Boulevard, 31 October 2019, <https://securityboulevard.com/2019/10/60-of-breaches-in-2019-involved-unpatched-vulnerabilities/>. Accessed 25 October 2022.

Turton, William, and Kartikay Mehrotra. "Colonial Pipeline Cyber Attack: Hackers Used Compromised Password." Bloomberg.com, 4 June 2021, <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>. Accessed 24 October 2022.

"2021 IBM Security X-Force Cloud Threat Landscape Report." IBM, <https://www.ibm.com/downloads/cas/WMDZOWK6>. Accessed 25 October 2022.

"2022 Security Trends: Software Supply Chain Survey • Anchore." Anchore, 19 January 2022, <https://anchore.com/blog/2022-security-trends-software-supply-chain-survey/>. Accessed 24 October 2022.

Ulagaratchagan, Arun. "Democratize enterprise analytics with Microsoft Power BI | Microsoft Power BI Blog." Microsoft Power BI, 24 May 2022, <https://powerbi.microsoft.com/en-us/blog/democratize-enterprise-analytics-with-microsoft-power-bi/>. Accessed 7 November 2022.

"Understanding security policies, initiatives, and recommendations in Microsoft Defender for Cloud." Microsoft Learn, 18 October 2022, <https://learn.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept>. Accessed 26 October 2022.

"Understanding security policies, initiatives, and recommendations in Microsoft Defender for Cloud." Microsoft Learn, 18 October 2022, <https://learn.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept>. Accessed 26 October 2022.

"Use Microsoft and Azure security resources to help recover from systemic identity compromise." Microsoft Learn, 12 October 2022, <https://docs.microsoft.com/en-us/azure/security/fundamentals/recover-from-identity-compromise#establish-secure-communications>. Accessed 27 October 2022.

"Use playbooks with automation rules in Microsoft Sentinel." Microsoft Learn, 28 September 2022, <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC>. Accessed 6 November 2022.

Wafula, Innocent. "6 strategies to reduce cybersecurity alert fatigue in your SOC." Microsoft, 17 February 2021, <https://www.microsoft.com/security/blog/2021/02/17/6-strategies-to-reduce-cybersecurity-alert-fatigue-in-your-soc/?culture=en-us&country=US>. Accessed 27 October 2022.

Works Cited

Weinert, Alex. "Protecting Microsoft 365 from on-premises attacks - Microsoft Community Hub." Microsoft Tech Community, 18 December 2020, <https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754>. Accessed 26 October 2022.

"What are Double and Triple Extortion Ransomware Attacks - RH-ISAC." RH-ISAC, 16 February 2022, <https://www.rhisac.org/ransomware/ransomware-double-and-triple-extortion/>. Accessed 24 October 2022.

"What is Azure Active Directory? - Microsoft Entra." Microsoft Learn, 14 September 2022, <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is>. Accessed 25 October 2022.

"What is Configuration Manager? - Configuration Manager." Microsoft Learn, 4 October 2022, <https://docs.microsoft.com/en-us/mem/configmgr/core/understand/introduction>. Accessed 27 October 2022.

"What is Microsoft 365 Defender?" Microsoft Learn, 25 October 2022, <https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide>. Accessed 6 November 2022.

"What is Microsoft 365 Defender?" Microsoft Learn, 25 October 2022, <https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide>. Accessed 6 November 2022.

"What is Microsoft Defender for Cloud? - Microsoft Defender for Cloud." Microsoft Learn, 18 October 2022, <https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction>. Accessed 26 October 2022.

"What is Microsoft Intune." Microsoft Learn, 31 October 2022, <https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>. Accessed 6 November 2022.

"What is Microsoft Intune." Microsoft Learn, 31 October 2022, <https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>. Accessed 6 November 2022.

"What is Microsoft Sentinel?" Microsoft Learn, 18 July 2022, <https://docs.microsoft.com/en-us/azure/sentinel/overview>. Accessed 25 October 2022.

"What is Microsoft Sentinel?" Microsoft Learn, 18 July 2022, <https://docs.microsoft.com/en-us/azure/sentinel/overview#correlate-alerts-into-incidents-by-using-analytics-rules>. Accessed 27 October 2022.

"What is Microsoft Sentinel?" Microsoft Learn, 18 July 2022, <https://docs.microsoft.com/en-us/azure/sentinel/overview>. Accessed 6 November 2022.

Works Cited

“What is Microsoft Sentinel?” Microsoft Learn, 18 July 2022, <https://docs.microsoft.com/en-us/azure/sentinel/overview>. Accessed 7 November 2022.

“What is Microsoft Sentinel?” Microsoft Learn, 18 July 2022, <https://docs.microsoft.com/en-us/azure/sentinel/overview#correlate-alerts-into-incidents-by-using-analytics-rules>. Accessed 7 November 2022.

“What Is Network Segmentation?” Palo Alto Networks, <https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation>. Accessed 25 October 2022.

“What Is Security Automation? An Introduction.” Splunk, https://www.splunk.com/en_us/data-insider/what-is-security-automation.html. Accessed 27 October 2022.

Wietharn, Jason, et al. “Are Firms Really Ditching Traditional, On-premises ERP for Cloud-Based Systems?” Velosio, 10 January 2022, <https://www.velosio.com/blog/ditching-on-premise-erp-for-cloud-based-systems/>. Accessed 25 October 2022.

Wietharn, Jason, et al. “Benefits of a Dynamics 365 On-Premise to Cloud Migration.” Velosio, 15 September 2021, <https://www.velosio.com/blog/dynamics-365-on-premise-to-cloud-migration/>. Accessed 25 October 2022.

Wietharn, Jason, et al. “Benefits of a Dynamics 365 On-Premise to Cloud Migration.” Velosio, 15 September 2021, <https://www.velosio.com/blog/dynamics-365-on-premise-to-cloud-migration/>. Accessed 25 October 2022.

Wietharn, Jason, et al. “Benefits of a Dynamics 365 On-Premise to Cloud Migration.” Velosio, 15 September 2021, <https://www.velosio.com/blog/dynamics-365-on-premise-to-cloud-migration/>. Accessed 26 October 2022.

Wietharn, Jason, et al. “Dynamics 365 Modules Explained - Comprehensive Buyers Guide.” Velosio, 27 October 2021, <https://www.velosio.com/blog/dynamics-365-modules-buyers-guide/>. Accessed 6 November 2022.

Wietharn, Jason, et al. “Dynamics 365 Modules Explained - Comprehensive Buyers Guide.” Velosio, 27 October 2021, <https://www.velosio.com/blog/dynamics-365-modules-buyers-guide/>. Accessed 6 November 2022.

Wietharn, Jason, et al. “Dynamics 365 Modules Explained - Comprehensive Buyers Guide.” Velosio, 27 October 2021, <https://www.velosio.com/blog/dynamics-365-modules-buyers-guide/>. Accessed 6 November 2022.

Works Cited

Wietharn, Jason, et al. “How Does Microsoft 365 Protect Data from Ransomware?” Velosio, 15 July 2022, <https://www.velosio.com/blog/how-does-microsoft-365-protect-data-from-ransomware/>. Accessed 25 October 2022.

Wietharn, Jason, et al. “How Does Microsoft 365 Protect Data from Ransomware?” Velosio, 15 July 2022, <https://www.velosio.com/blog/how-does-microsoft-365-protect-data-from-ransomware/>. Accessed 6 November 2022.

Wietharn, Jason, et al. “How Entra Safeguards Your Business From Ransomware.” Velosio, 11 July 2022, <https://www.velosio.com/blog/how-entra-safeguards-your-business-from-ransomware/>. Accessed 25 October 2022.

Wietharn, Jason, et al. “How SharePoint Helps Companies Avoid Ransomware Attacks.” Velosio, 14 July 2022, <https://www.velosio.com/blog/how-sharepoint-helps-companies-avoid-ransomware-attacks/>. Accessed 25 October 2022.

Wietharn, Jason, et al. “Microsoft Dynamics 365 Security - D365 Security Best Practices.” Velosio, 3 November 2021, <https://www.velosio.com/blog/microsoft-dynamics-365-security/>. Accessed 25 October 2022.

Wietharn, Jason, et al. “OneDrive for Business Protects Documents from Ransomware.” Velosio, 14 July 2022, <https://www.velosio.com/blog/how-onedrive-for-business-protects-documents-and-data-from-ransomware/>. Accessed 25 October 2022.

Wietharn, Jason, et al. “Ransomware Protection Best Practices.” Velosio, 9 September 2022, <https://www.velosio.com/blog/ransomware-protection-best-practices/>. Accessed 27 October 2022.

Wietharn, Jason, et al. “Ransomware Protection in Microsoft Dynamics 365.” Velosio, 17 July 2022, <https://www.velosio.com/blog/ransomware-protection-in-microsoft-dynamics-365/>. Accessed 25 October 2022.

Wietharn, Jason, and Phil Wittmer. “How to Recover from a Ransomware Attack.” Velosio, 16 September 2022, <https://www.velosio.com/blog/how-to-recover-from-a-ransomware-attack/>. Accessed 27 October 2022.

Wittmer, Phil. “Microsoft 365 for Professional Services Firms.” Velosio, 27 June 2022, <https://www.velosio.com/blog/microsoft-365-new-improved-and-more-powerful-than-you-remember/>. Accessed 6 November 2022.

Wittmer, Phil. “Microsoft Teams and SharePoint.” Velosio, 8 June 2022, <https://www.velosio.com/blog/microsoft-teams-and-sharepoint/>. Accessed 7 November 2022.

Works Cited

Wittmer, Phil, and Carolyn Norton. “How to Protect Your Company from Cybersecurity Threats—In 2022 ...” Velosio, 10 March 2022, <https://www.velosio.com/blog/how-to-protect-your-company-from-cybersecurity-threats-in-2022-and-beyond/>. Accessed 24 October 2022.

Wittmer, Phil, and Carolyn Norton. “How to Protect Your Company from Cybersecurity Threats—In 2022 and Beyond.” Velosio, 10 March 2022, <https://www.velosio.com/blog/how-to-protect-your-company-from-cybersecurity-threats-in-2022-and-beyond/>. Accessed 25 October 2022.

Wittmer, Phil, and Carolyn Norton. “Is Cloud Storage Safe from Ransomware?” Velosio, 10 July 2022, <https://www.velosio.com/blog/is-cloud-storage-safe-from-ransomware/>. Accessed 26 October 2022.

Wittmer, Phil, and Carolyn Norton. “Is Cloud Storage Safe from Ransomware?” Velosio, 10 July 2022, <https://www.velosio.com/blog/is-cloud-storage-safe-from-ransomware/>. Accessed 6 November 2022.

Wittmer, Phil, and Carolyn Norton. “Ransomware Trends - Ransomware Stats, Facts & Threats.” Velosio, 13 June 2022, <https://www.velosio.com/blog/ransomware-trends-2022-stats-facts-todays-biggest-threats/>. Accessed 6 November 2022.

Wittmer, Phil, and Carolyn Norton. “Ransomware Trends - Ransomware Stats, Facts & Threats.” Velosio, 13 June 2022, <https://www.velosio.com/blog/ransomware-trends-2022-stats-facts-todays-biggest-threats/>. Accessed 7 November 2022.

Wittmer, Phil, and Jason Wietharn. “Microsoft Ecosystem Ransomware Protection.” Velosio, 18 July 2022, <https://www.velosio.com/blog/how-the-microsoft-ecosystem-safeguards-your-data-from-ransomware-attacks/>. Accessed 27 October 2022.

Xu, Howie. “How AI Is Useful — and Not Useful — for Cybersecurity.” Dark Reading, 9 June 2022, <https://www.darkreading.com/attacks-breaches/how-ai-is-useful-and-not-useful-for-cybersecurity>. Accessed 25 October 2022.

“Zero Trust Essentials eBook.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWlrfk>. Accessed 7 November 2022.

“Zero Trust Essentials eBook.” Microsoft, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWlrfk>. Accessed 7 November 2022.

“Zero Trust Model - Modern Security Architecture.” Microsoft, <https://www.microsoft.com/en-us/security/business/zero-trust>. Accessed 25 October 2022.

“Zero Trust Model - Modern Security Architecture.” Microsoft, <https://www.microsoft.com/en-us/security/business/zero-trust?rtc=1>. Accessed 25 October 2022.



Works Cited

“Zero Trust Model - Modern Security Architecture.” Microsoft, <https://www.microsoft.com/en-us/security/business/zero-trust?rtc=1>. Accessed 27 October 2022.

“Zero Trust Model - Modern Security Architecture.” Microsoft, <https://www.microsoft.com/en-us/security/business/zero-trust>. Accessed 27 October 2022.

“Zero Trust Model - Modern Security Architecture.” Microsoft, <https://www.microsoft.com/en-us/security/business/zero-trust>. Accessed 7 November 2022.

“Zero Trust Rapid Modernization Plan.” Microsoft Learn, 26 August 2022, <https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview?source=recommendations>. Accessed 7 November 2022.