Microsoft Azure

Azure Defenses for Ransomware Attack

September 2021

@2021, Microsoft Corporation. All rights reserved. This document is provided "as-is".
This document does not provide you with any legal rights to Microsoft products or services.

Microsoft Azure

Acknowledgements

Author

Charles Iheagwara, Principal Program Manager

Contributors

Mark Simos, Director of Business Strategy

Jack Richins, Principal Program Manager

Yuri Diogenes, Principal Program Manager

Utsav Raghuvanshi, Program Manager II

Sriram Iyer, Principal Program Manager

Kemba Walden, Assistant General Counsel

Amrita Satapathy, Principal Program Manager

Terry Lanfear, Principal Content Developer

Joe Davies, Senior Technical Writer

@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

Table of Contents

Executive Summary	1
Ransomware: *A growing threat*	2
Ransomware Evolution: *Current model vastly expands extortion scope*	8
Azure Provides Native Ransomware Protections	9
Preparing for Ransomware Attacks: *Stay ahead of attackers*	15
Preparing for Quick Recovery: *Restore business operations fast*	22
Detecting Ransomware Attacks: *Accelerate detection with the right tools*	23
Responding to Ransomware Attacks: *Increase effectiveness with practiced IR teams*	25
Road to Recovery: *Microsoft experts provide insights*	26
Conclusion	28

@2021, Microsoft Corporation. All rights reserved.

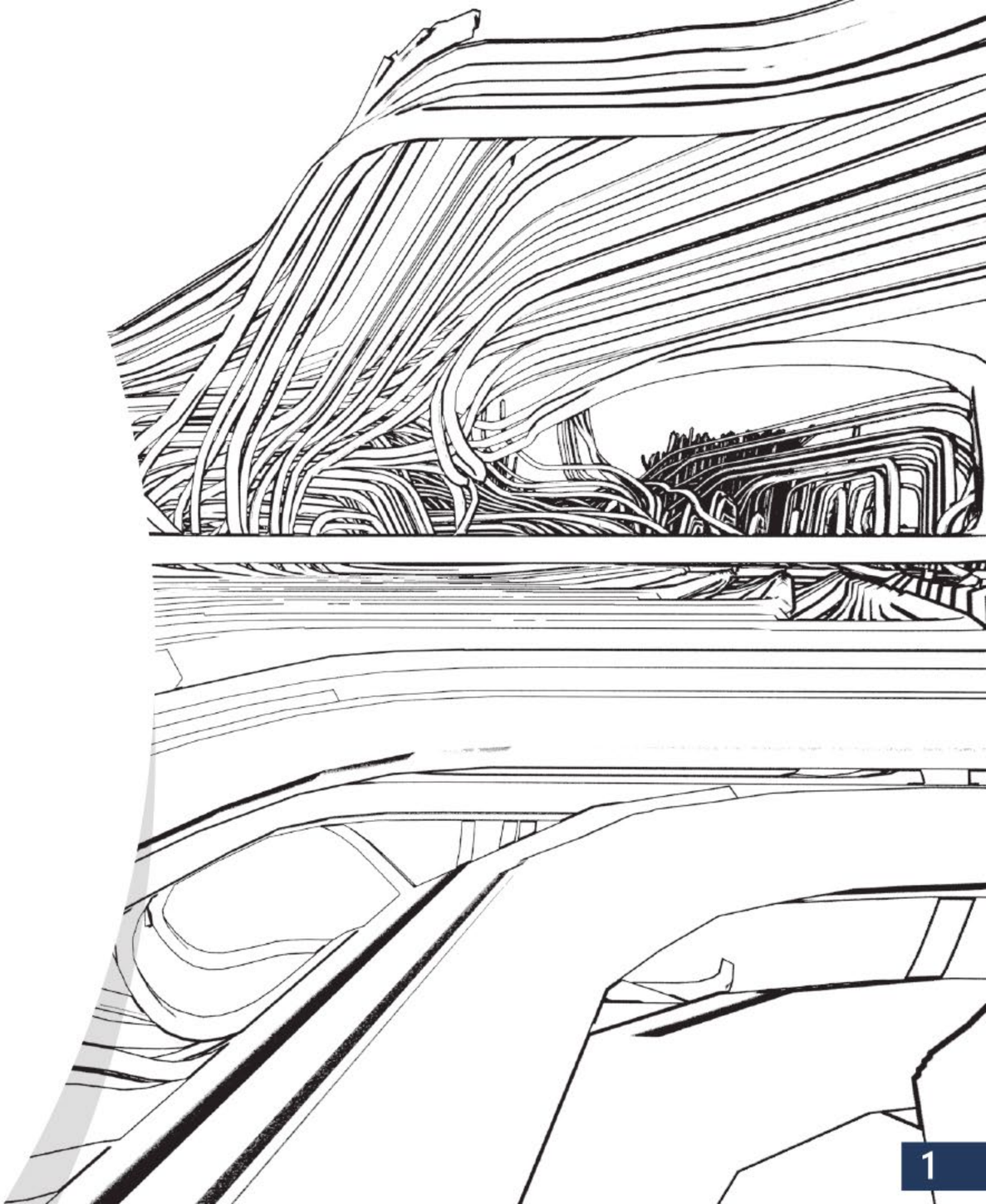
Executive Summary

Ransomware and extortion are a high profit, low-cost business which has a debilitating impact on targeted organizations, national security, economic security, and public health and safety. What started as simple single-PC ransomware has grown to include a variety of extortion techniques directed at all types of corporate networks and cloud platforms.

To ensure customers running on Azure cloud are protected against ransomware attacks, Microsoft has invested heavily on the security of our cloud platforms and has provided you the security controls you need to protect your Azure cloud workloads.

By leveraging Azure native ransomware protections and implementing the best practices recommended in this eBook, you are taking measures that ensures your organization is optimally positioned to prevent, protect and detect potential ransomware attacks on your Azure assets.

This eBook lays out key Azure native capabilities and defenses for ransomware attacks and guidance on how to proactively leverage these to protect your assets on Azure cloud.



@2021, Microsoft Corporation. All rights reserved.

Ransomware: *A growing threat*

Ransomware attacks have become one of the biggest security challenges facing businesses today. When successful, ransomware attacks can cripple a business core IT infrastructure's capacity and cause destruction that could have a debilitating impact on the physical, economic security or safety of a business. Ransomware attacks are targeted to businesses of all types. This requires that all businesses take preventive measures to ensure protection.

Recent trends on the number of attacks are quite alarming. While 2020 was not a good year for ransomware attacks on businesses, 2021 started on a bad trajectory. On May 7, the Colonial Pipeline (Colonial) attack shutdown services such as pipeline transportation of diesel and gasoline, and jet fuel was also temporarily halted. Colonial shut the critical fuel network supplying the populous eastern states.

Historically, cyberattacks were seen as a sophisticated set of actions targeting particular industries, which left the remaining industries believing they were outside the scope of cybercrime, and without context about which cybersecurity threats they should prepare for. Ransomware represents a major shift in this threat landscape, and it's made cyberattacks a very real and omnipresent danger for everyone. Encrypted and lost files and threatening ransom notes have now become the top-of-mind fear for most executive teams.

Ransomware's economic model capitalizes on the misperception that a ransomware attack is solely a malware incident. Whereas in reality ransomware is a breach involving human adversaries attacking a network.

For many organizations, the cost to rebuild from scratch after a ransomware incident far outweighs the original ransom demanded. With a limited understanding of the threat landscape and how ransomware operates, paying the ransom seems like the better business decision to return to operations. However, the real damage is often done when the cybercriminal exfiltrates files for release or sale, while leaving backdoors in the network for future criminal activity—and these risks persist whether or not the ransom is paid.

@2021, Microsoft Corporation. All rights reserved.

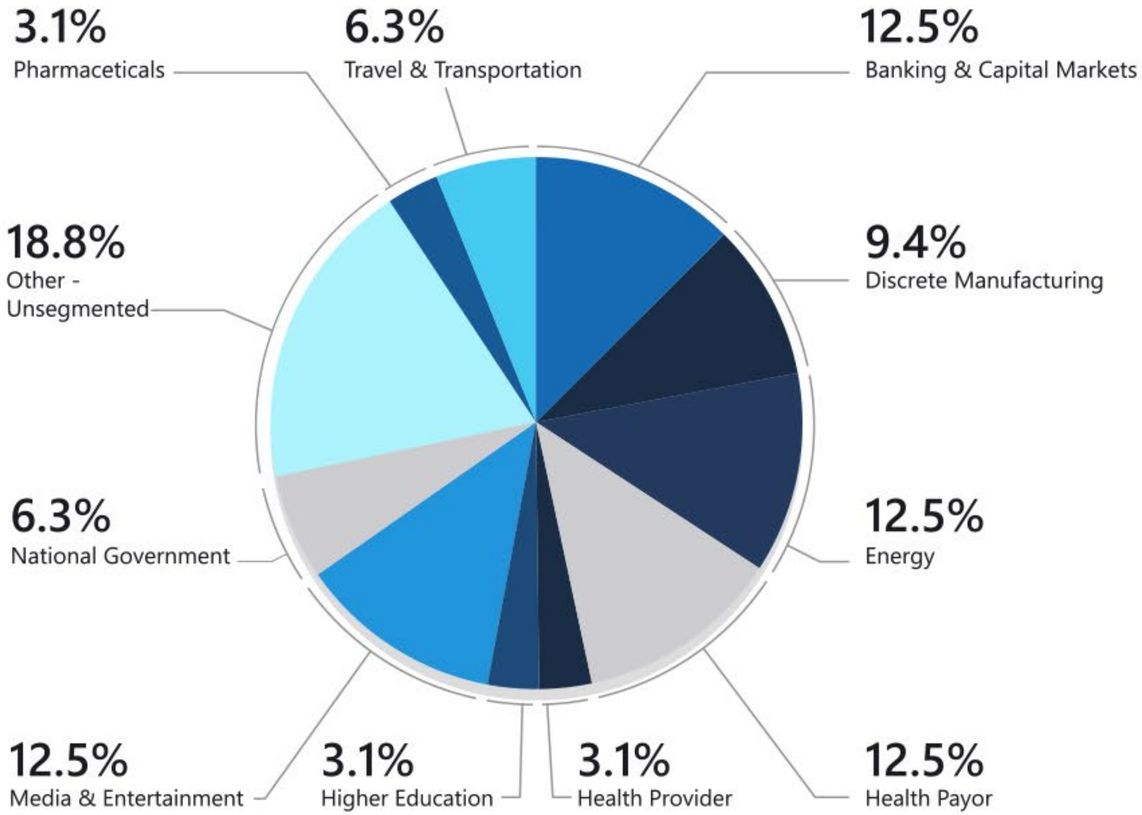
Ransomware explained

Ransomware is a type of malware that infects a computer and restricts a user's access to the infected system or specific files in order to extort them for money. After the target system has been compromised, it typically locks out most interaction and displays an on-screen alert, typically stating that the system has been locked or that all of their files have been encrypted. It then demands a substantial ransom be paid before the system is released or files decrypted.

Ransomware will typically exploit the weaknesses or vulnerabilities in your organization's IT systems or infrastructures to succeed. The attacks are so obvious that it does not take much investigation to confirm that your business has been attacked or that an incident should be declared. The exception would be a spam email that demands ransom in exchange for supposedly compromising materials. In this case, these types of incidents should be dealt with as spam unless the email contains highly specific information.

Who can be targeted by ransomware bad actors?

Any business or organization that operates an IT system with data in it can be attacked. Although individuals can be targeted in a ransomware attack, most attacks are targeted at businesses. While the Colonial ransomware attack of May 2021 drew considerable public attention, our Detection and Response team's ransomware engagement data shows that the energy sector represents one of the most targeted sectors, along with the financial, healthcare, and entertainment sectors. And despite continued promises not to attack hospitals or healthcare companies during the pandemic, as shown in Figure 1, healthcare remains the number one target of human operated ransomware.



Healthcare (Providers plus Payors) 15.6%,
Energy 12.5%,
Financial 12.5%,
Media & Entertainment 12.5%

Figure 1: Percentage Distribution of Key Sectors Targeted in Recent Ransomware Attacks

@2021, Microsoft Corporation. All rights reserved.

How can my assets in the cloud be targeted?

When attacking cloud infrastructure, adversaries often attack multiple resources to try to obtain access to customer data or company secrets. The cloud kill chain model (Figure 2) explains how attackers attempt to gain access to any of your resources running in the public cloud through a four-step process: exposure, access, lateral movement, and actions.

1. Exposure is where attackers look for opportunities to gain access to your infrastructure. For example, attackers know customer-facing applications must be open for legitimate users to access them. Those applications are exposed to the Internet and therefore susceptible to attacks.
2. Attackers will try to exploit an exposure to gain access to your public cloud infrastructure. This can be done through compromised user credentials, compromised instances, or misconfigured resources.
3. During the lateral movement stage, attackers discover what resources they have access to and what the scope of that access is. Successful attacks on instances give attackers access to databases and other sensitive information. The attacker then searches for additional credentials. Azure Defender data shows that without a security tool to quickly notify you of the attack, it takes organizations on average 101 days to discover a breach. Meanwhile, in just 24-48 hours after a breach, the attacker will usually have complete control of the network.
4. The actions an attacker takes after lateral movement are largely dependent on the resources they were able to gain access to during the lateral movement phase. Attackers can take actions that cause data exfiltration, data loss or launch other attacks. For enterprises, the average financial impact of data loss is now reaching $1.23 million.

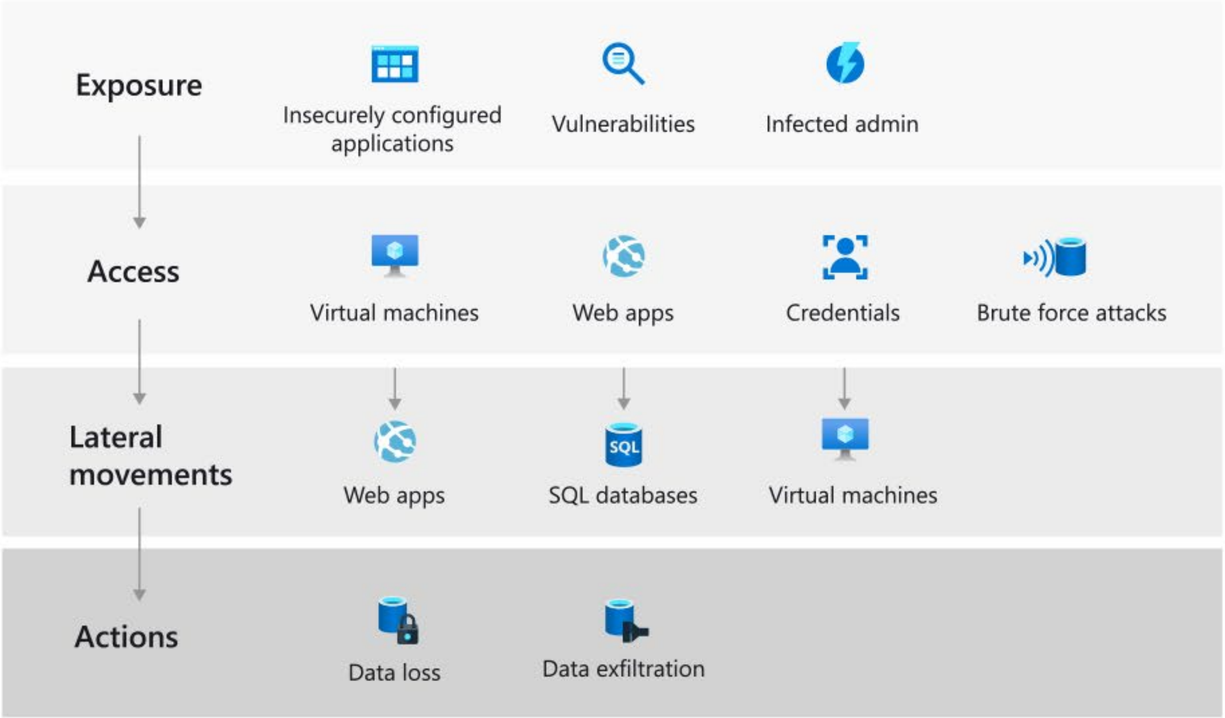


Figure 2: The Cloud Kill Chain Model

@2021, Microsoft Corporation. All rights reserved.

Why do ransomware attacks succeed?

There are several reasons why ransomware attacks succeed. Businesses that are vulnerable often fall victim to ransomware attacks. The following are some of the attack critical success factors:

- The attack surface has increased as more and more businesses offer more services through digital outlets
- There is a considerable ease of obtaining off-the-shelf malware, Ransomware-as-a-Service (RaaS)
- With the above, the option to use cryptocurrency for blackmail payments has opened new avenues for exploit
- Expansion of computers and their usage in different workplaces (local school districts, police departments, police squad cars, etc.) each of which is a potential access point for malware, resulting in potential attack surface
- Prevalence of old, outdated, and antiquated infrastructure systems and software
- Poor patch management regimen
- Outdated or very old operating systems that are close to or have gone beyond end-of-support dates
- Lack of resources to modernize the IT footprint
- Knowledge gap
- Lack of skilled staff and key personnel overdependency
- Poor security architecture

As illustrated in Figure 3, attackers use different techniques, such as RDP brute force attack to exploit the vulnerabilities.

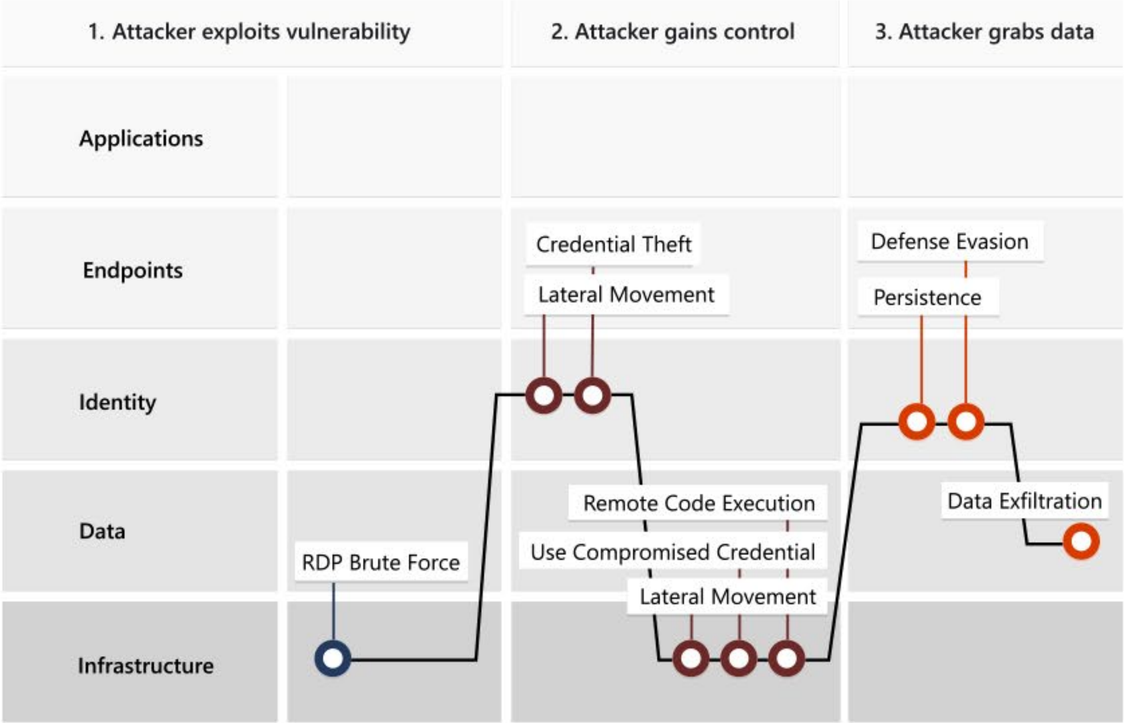


Figure 3: Ransomware Compromise Technique

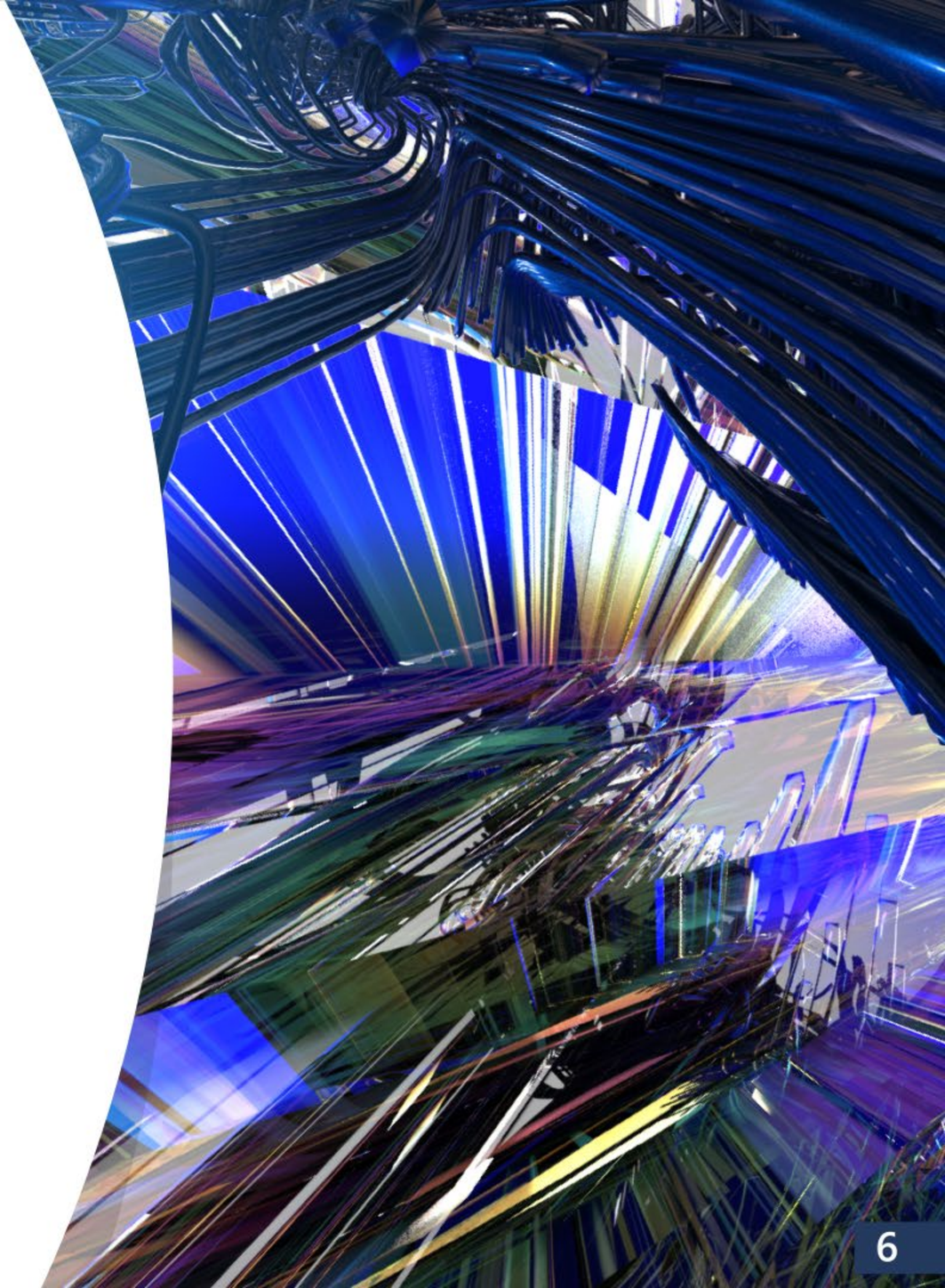
@2021, Microsoft Corporation. All rights reserved.

Should you pay ransom if attacked?

There are varying opinions on what the best option is when confronted with this vexing demand. The Federal Bureau of Investigation (FBI) **advises victims not to pay ransom but to instead be vigilant and take proactive measures to secure their data before an attack**. They contend that paying doesn't guarantee that locked systems and encrypted data will be released again. The FBI says another reason not to pay is that payments to cyber criminals incentivizes them to continue to attack organizations.

Nevertheless, some victims elect to pay the ransom demand even though system and data access is not guaranteed after paying the ransom. By paying, such organizations take the calculated risk to pay in hopes of getting back their system and data and quickly resuming normal operations. Part of the calculation is reduction in collateral costs such as lost productivity, decreased revenue over time, exposure of sensitive data, and potential reputational damage.

In the end, the best way to prevent paying ransom is not to fall victim by implementing preventive measures and having tool saturation to protect your organization from every step that the attacker takes wholly or incrementally to hack into your system. In addition, having the ability to recover impacted assets will ensure restoration of business operations in a timely fashion. Azure cloud has a robust set of tools to guide you all the way.



@2021, Microsoft Corporation. All rights reserved.

What is the typical cost to a business?

The impact of a ransomware attack on any organization is difficult to quantify accurately. However, depending on the scope and type, the impact is multi-dimensional (see Figure 4) and is broadly expressed in:

- Loss of data access
- Business operation disruption
- Financial loss
- Intellectual property theft
- Compromised customer trust/tarnished reputation

Colonial Pipeline paid about $4.4 million in ransom to have their data released. This does not include the cost of downtime, lost productivity, lost sales and the cost of restoring services. More broadly, a significant impact is the "**knock-on effect**" of impacting high numbers of businesses and organizations of all kinds including towns and cities in their local areas. The financial impact is also staggering. According to Microsoft, the global cost associated with ransomware recovery is projected to exceed $20 billion in 2021.

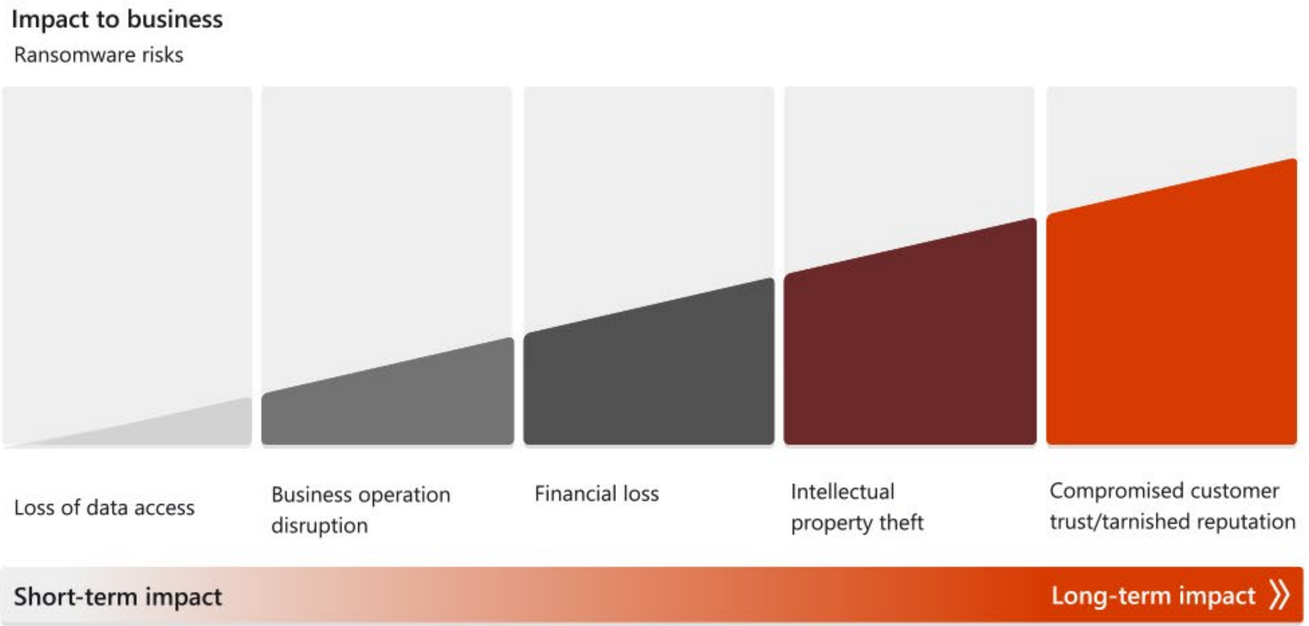


Figure 4: Impact of Ransomware Attack to Business

@2021, Microsoft Corporation. All rights reserved.

How did ransomware evolve as a business?

Since the first known ransomware attack was disclosed in 1989, much of the industry has significantly changed not just with the number of attacks occurring every year and the sophistication of those attacks, but the emergence and evolution of new ransomware business models. The two common types are "**Commodity Ransomware**" and "**Human Operated Ransomware**." Each has its distinctive attributes.

Commodity ransomware attacks target individuals, are pre-programmed, opportunistic and are unlikely to cause business disruption. Human operated ransomware is sometimes referred to as "big game ransomware," a term that implies cybercriminals select specific networks for their value proposition and then hunt for entry vectors. This approach has been the exception, not the rule, in most major ransomware attacks in the past year. Cybercriminals perform massive wide-ranging sweeps of the internet, searching for vulnerable entry points. Or they enter networks via "commodity" trojans and then "bank" this access for a time and purpose that's advantageous to them.

While ransomware existed in small pockets before, the business model didn't take off at scale until the introduction of cryptolocker in 2013, which kicked off a surge in this opportunistic, single device way of monetizing cybercrime.

The most recent phase in ransomware evolution, as illustrated in Figure 5, can be traced to WannaCry and (Not)Petya that fused large scale compromise techniques with an encryption payload that demanded a ransom payment in exchange for the decryption key.

This fusion inspired the new generation of human operated ransomware that started popping up around June 2019, and vastly expanded the ransomware business model into an enterprise scale operation blending targeted attack techniques and the extortion business model (threatening disclosure of data and/or encryption in exchange for payment).

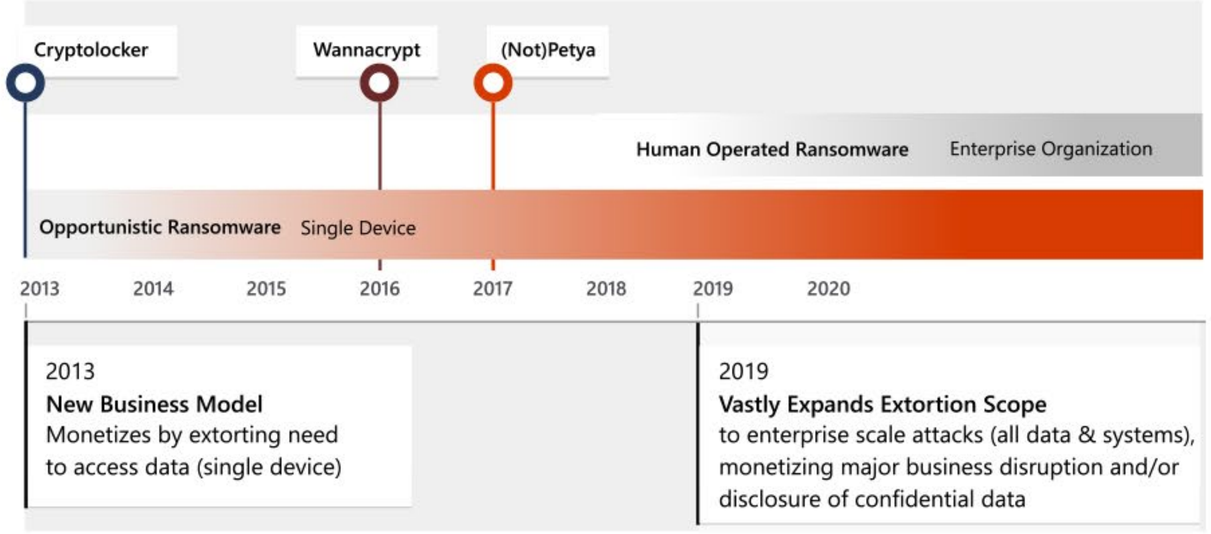


Figure 5: Evolution of Ransomware Models

@2021, Microsoft Corporation. All rights reserved.

Azure Provides Native Ransomware Protections

Microsoft has invested in Azure native security capabilities that organizations can leverage to defeat ransomware attack techniques found in both high volume everyday/commodity and sophisticated targeted attacks.

Native Security Controls

Key capabilities include:

Native Threat Detection

Azure Defender provides high quality threat detection and response capabilities, also called Extended Detection and Response – XDR.

This helps you:

- Avoid wasting time and talent of scarce security resources to build custom alerts using raw activity logs.
- Ensure effective security monitoring, which often enables security teams to rapidly approve use of Azure services.

Passwordless and Multi-Factor Authentication

Azure MFA, Azure AD Authenticator App, and Windows Hello provide these capabilities.

This helps protect accounts against commonly seen password attacks (which account for 99.9% of the volume of identity attacks we see in Azure AD). While no security is perfect, eliminating password-only attack vectors dramatically lowers the ransomware attack risk to Azure resources.

Native Firewall and Network Security

Microsoft built native DDoS attack mitigations, Azure Firewall, Web Application Firewall (WAF), and many other controls into Azure.

These security 'as a service' help simplify the configuration and implementation of security controls. These give organizations the choice of using native services or virtual appliances versions of familiar vendor capabilities to simplify their Azure security.

Native Security Controls

Integration with existing security capabilities

Native Threat Detection (& SIEM)

Secure Azure, Azure AD, Windows, Linux, iOS, Android, SaaS apps
+ correlate with cloud native SIEM
+ SOAR + UEBA (Azure Sentinel)

Passwordless and Multi-Factor Authentication (MFA)

Secure Azure, Azure AD, Windows, Linux, iOS, Android, SaaS apps + correlate with cloud native SIEM + SOAR + UEBA (Azure Sentinel)

Native Firewall and Network Security

Protect business-critical assets with Azure Firewall, DDoS protection & integrated WAF.

@2021, Microsoft Corporation. All rights reserved.

Azure Provides Native Ransomware Protections

Azure Defender, is a built-in tool that provides threat protection for workloads running in Azure, on-premises, and in other clouds

Integrated with Security Center, **Azure Defender protects your hybrid data, cloud native services and servers from ransomware and other threats**; and integrates with your existing security workflows like your SIEM solution and Microsoft's vast threat intelligence to streamline threat mitigation.

Azure Defender delivers protection for all resources from directly within the Azure experience and extends protection to on-premises and multi-cloud virtual machines and SQL databases using Azure Arc.

- Protects Azure services
- Protects hybrid workloads
- Streamlines security with AI and automation
- Detects and blocks advanced malware and threats for Linux and Windows servers on any cloud
- Protects cloud-native services from threats
- Protects data services against ransomware attacks
- Protects your managed and unmanaged IoT / operational technology (OT) devices with continuous asset discovery, vulnerability management and threat monitoring

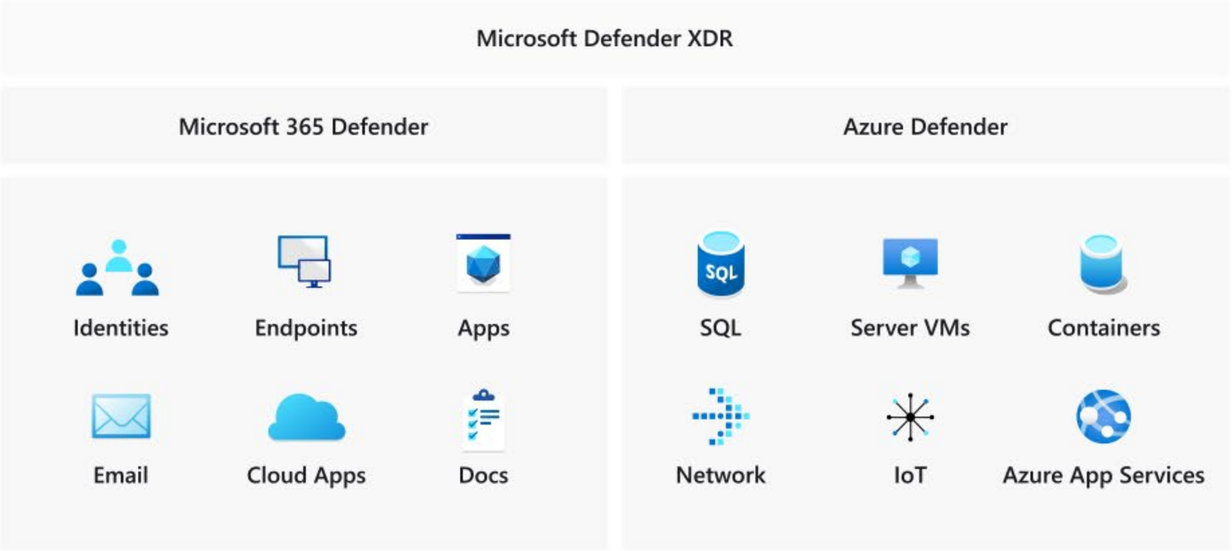


Figure 6: The Microsoft Defender XDR Product Suites

@2021, Microsoft Corporation. All rights reserved.

Azure Provides Native Ransomware Protections

Azure Sentinel helps to create a complete view of a kill chain

With Sentinel you can connect to any of your security sources using built-in connectors and industry standards and then take advantage of artificial intelligence to correlate multiple low fidelity signals spanning multiple sources to **create a complete view of a ransomware kill chain and prioritized alerts**, so that defenders can accelerate their time to evict adversaries.

Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

- **Collect data at cloud scale** across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds
- **Investigate threats with artificial intelligence**, and hunt for suspicious activities at scale, tapping into years of cybersecurity work at Microsoft.
- **Detect previously undetected threats**, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence
- **Respond to incidents rapidly** with built-in orchestration and automation of common tasks

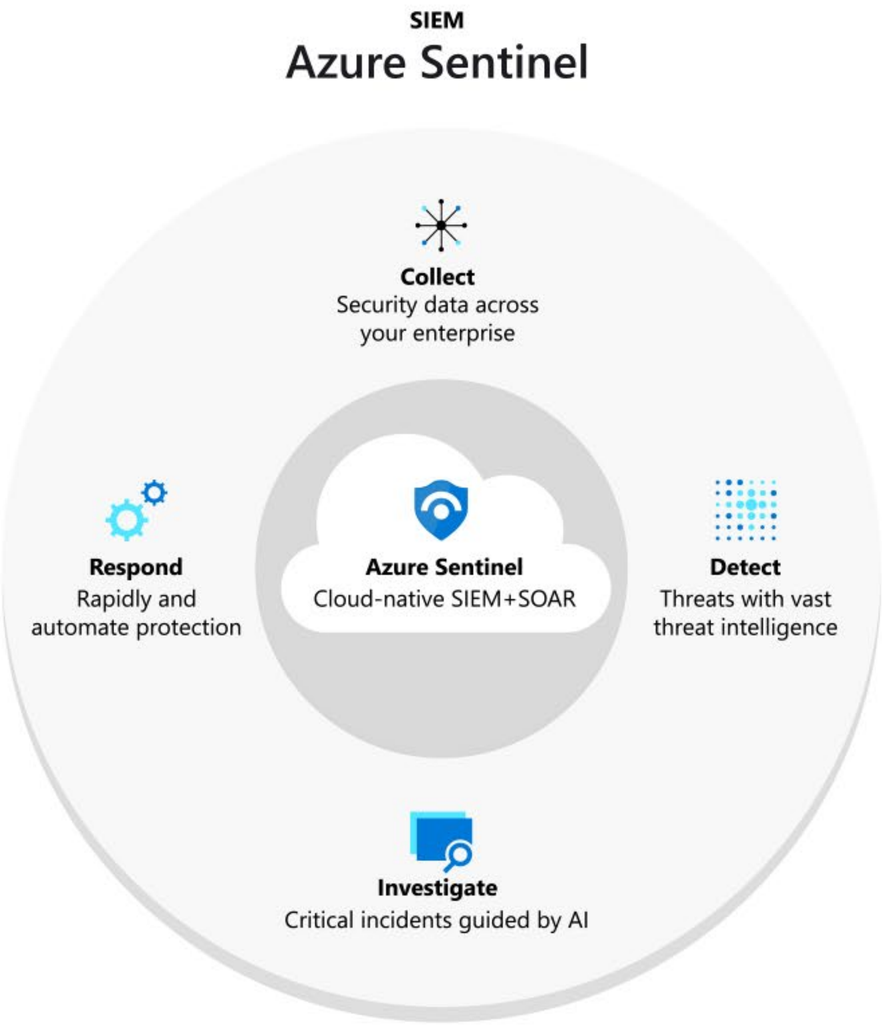


Figure 7: Microsoft Sentinel SIEM Tool

@2021, Microsoft Corporation. All rights reserved.

Azure Provides Native Ransomware Protections

Azure Security Center provides you the tools to detect and block ransomware, advanced malware and threats for your resources

Keeping your resources safe is a joint effort between your cloud provider, Azure, and you, the customer. You have to make sure your workloads are secure as you move to the cloud. When you move to IaaS (infrastructure as a service) there is more customer responsibility than there was in PaaS (platform as a service), and SaaS (software as a service). Azure Security Center provides you the tools needed to harden your network, secure your services and make sure you're on top of your security posture.

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads in the cloud whether they're in Azure or not - as well as on premises.

Azure Security Center's threat protection enables you to detect and prevent threats at the IaaS layer, non-Azure servers as well as for PaaS in Azure.

Security Center's threat protection includes fusion kill-chain analysis, which automatically correlates alerts in your environment based on cyber kill-chain analysis, to help you better understand the full story of an attack campaign, where it started and what kind of impact it had on your resources.

Key Features:

Continuous security assessment

Identify Windows and Linux machines with missing security updates, insecure OS settings and vulnerable Azure configurations. Add optional watchlists or events you want to monitor.

Industry's most extensive threat intelligence

Tap into the Microsoft Intelligent Security Graph, which uses trillions of signals from Microsoft services and systems around the globe to identify new and evolving threats.

Prioritized alerts and attack timelines

Focus on the most critical threats first with prioritized alerts and incidents that are mapped into a single attack campaign.

Actionable recommendations

Remediate security vulnerabilities quickly with prioritized, actionable security recommendations.

Advanced analytics and machine learning

Use built-in behavioural analytics and machine learning to identify known attack patterns and post-breach activity.

Streamlined investigation

Quickly investigate the scope and impact of an attack with a visual, interactive experience. Use ad hoc queries for deeper exploration of security data.

Centralized policy management

Ensure compliance with company or regulatory security requirements by centrally managing security policies across all your hybrid cloud workloads.

Adaptive application control

Block malware and other unwanted applications by applying whitelisting recommendations adapted to your specific workloads and powered by machine learning.

Automation and orchestration

Automate common security workflows to address threats quickly using built-in integration with Azure Logic Apps. Create security playbooks that can route alerts to existing ticketing system or trigger incident response actions.

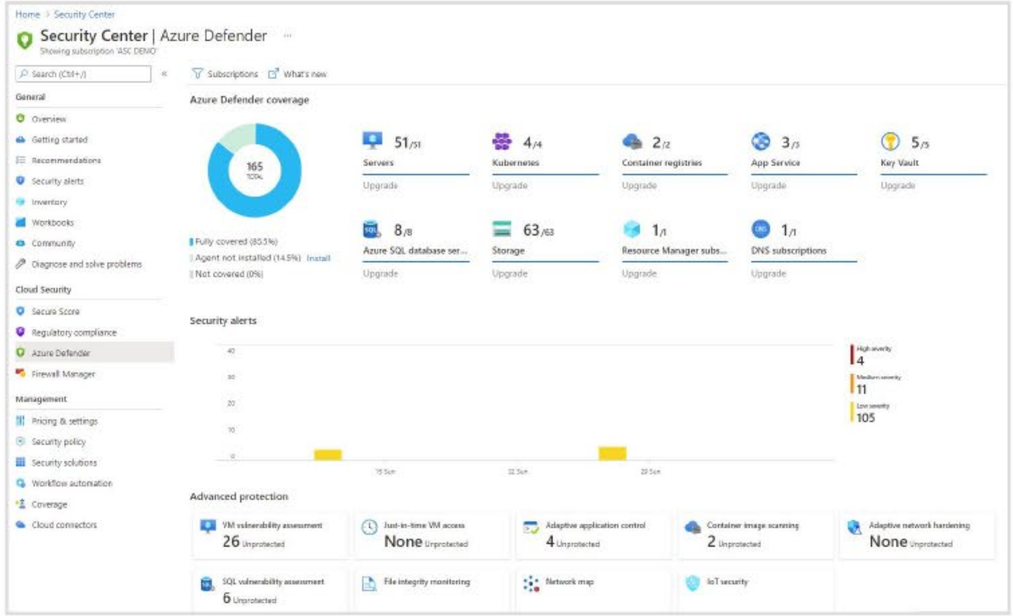
@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

Azure Provides Native Ransomware Protections

Native Threat Prevention with Azure Defender

Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, and more. When Azure Defender detects a threat in any area of your environment, it generates a security alert. These alerts describe details of the affected resources, suggested remediation steps, and in some cases an option to trigger a Logic App in response.

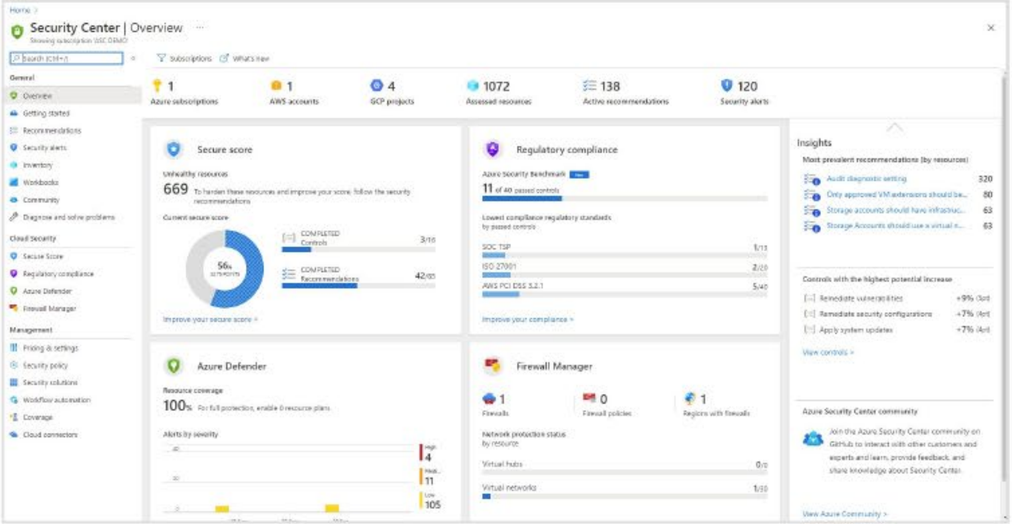


The alert below is an example of a detected Petya ransomware alert:

Detected Petya ransomware indicators	1	Microsoft		06/28/17	Active	High ...

Native Threat Detection with Azure Security Center

Azure Security Center scans virtual machines across an Azure subscription and makes a recommendation to deploy endpoint protection where an existing solution is not detected. This recommendation can be accessed via the Recommendations section as shown below.



@2021, Microsoft Corporation. All rights reserved.

Azure Provides Native Ransomware Protections

Azure Native Backup Solution Protects Your Data

One important way that organizations can help protect against losses in a ransomware attack is to have a backup of business-critical information in case other defenses fail. Since ransomware attackers have invested heavily into neutralizing backup applications and operating system features like volume shadow copy, it is critical to have backups that are inaccessible to a malicious attacker. **With a flexible business continuity and disaster recovery solution, industry-leading data protection and security tools, Azure cloud offers secure services to protect your data:**

Azure Backup

Azure Backup service provides simple, secure, and cost-effective solution to back up your Azure Virtual Machine (VM). Currently, Azure Backup supports backing up of all the disks (OS and Data disks) in a VM using backup solution for Azure VM.

Azure Disaster Recovery

With disaster recovery from on-premises to the cloud, or from one cloud to another, you can avoid downtime and keep your applications up and running.

Built-in Security and Management in Azure

To be successful in the cloud era, enterprises must have visibility and metrics, and controls on every component to pinpoint issues efficiently, optimize and scale effectively, while having the assurance the security, compliance and polices are in place to ensure the velocity.

Guaranteed and Protected Access to Your Data

Azure has a lengthy period of experience managing global data centers, which are backed by Microsoft's $15 billion infrastructure investment that is continuously evaluated and improved – with ongoing investments.

Key Features:

- Azure comes with Locally Redundant Storage (LRS), where data is stored locally, as well as Geo Redundant Storage (GRS) in a second region
- All data stored on Azure is protected by an advanced encryption process, and all Microsoft's data centers have two-tier authentication, proxy card access readers, biometric scanners
- Azure has more certifications than any other public cloud provider on the market, including ISO 27001, HIPAA, FedRAMP, SOC 1, SOC 2, and many international specifications

Guaranteed:

Microsoft offers 99.5-99.9% uptime on their services. Read the full SLA for more details.

All of the above are some very good reasons to trust Microsoft—and Azure—with your data.

@2021, Microsoft Corporation. All rights reserved.

Preparing for Ransomware Attacks: *Stay ahead of attackers*

Adopt a cybersecurity framework

A good place to start is to adopt Azure Security Benchmark to secure the Azure environment. Azure Security Benchmark is Azure's own security control framework based on industry-based security control frameworks such as NIST SP800-53, CIS Controls v7.1. It provides organizations guidance on how to configure Azure and Azure services and implement the security controls. Organizations can use Azure Security Center to monitor their live Azure environment status with all the Azure Security Benchmark controls.

Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

Azure ID	CIS Controls v7.1 ID(s)	NIST SP 800-53 r4 ID(s)
NS-1	9.2, 9.4, 14.1, 14.2, 14.3	AC-4, CA-3, SC-7

(Example: Azure Security Benchmark control framework mapping)

Azure Security Benchmark
Network Security (**NS**)
Identity Management (**IM**)
Priviliged Access (**PA**)
Data Protection (**DP**)
Asset Management (**AM**)
Logging and Threat Detection (**LT**)
Incident Response (**IR**)
Posture and Vulnerability Management (**PV**)
Endpoint Security (**ES**)
Backup and Recovery (**BR**)
Governance and Strategy (**GS**)

@2021, Microsoft Corporation. All rights reserved.

Preparing for Ransomware Attacks:
Stay ahead of attackers

Prioritized Mitigation

Based on our experience with ransomware attacks, we've found that prioritization should focus on: 1) prepare, 2) limit, 3) prevent. This may seem counterintuitive, since most people want to simply prevent an attack and move on. But the unfortunate truth is that we must assume breach (a key Zero Trust principle) and focus on reliably mitigating the most damage first. This prioritization is critical because of the high likelihood of a worst-case scenario with ransomware. While it's not a pleasant truth to accept, we're facing creative and motivated human attackers who are adept at finding a way to control the complex real-world environments in which we operate. Against that reality, it's important to prepare for the worst and establish frameworks to contain and prevent attackers' ability to get what they're after.

While these priorities should govern what to do first, we encourage organizations to ***run as many steps in parallel as possible*** (including pulling quick wins forward from step 1 whenever you can).

Step 1

Make it harder to get in: incrementally remove risks

Prevent a ransomware attacker from entering your environment and rapidly respond to incidents to remove attacker access before they can steal and encrypt data. This will cause attackers to fail earlier and more often, undermining the profit of their attacks. While prevention is the preferred outcome, it is a continuous journey and it may not be possible to achieve 100% prevention and rapid response across real-world organizations (complex multi-platform and multi-cloud estate with distributed IT responsibilities).

To achieve this, organizations should identify and execute quick wins to strengthen security controls to prevent entry, and rapidly detect/evict attackers while implementing a sustained program that helps them stay secure.

Microsoft recommends organizations follow the principles outlined in the Zero Trust strategy here.

Against Ransomware, organizations should prioritize:

a). **Improving security hygiene** by focusing efforts on attack surface reduction, threat and vulnerability management for assets in their estate.

b). **Implementing protection, detection and response controls** for their digital assets that can protect against commodity and advanced threats, provide visibility and alerting on attacker activity and respond to active threats.

@2021, Microsoft Corporation. All rights reserved.

Preparing for Ransomware Attacks: *Stay ahead of attackers*

Step 2

Limit Scope of Damage:
Protect Privileged Roles (starting with IT Admins)

Ensure you have strong controls (prevent, detect, respond) for privileged accounts like IT Admins and other roles with control of business-critical systems. This slows and/or blocks attackers from gaining complete access to your resources to steal and encrypt them. Taking away the attacker's ability to use IT Admin accounts as a shortcut to resources will drastically lower the chances they are successful at attacking you and demanding payment.

Organizations should have elevated security for privileged accounts (tightly protect, closely monitor, and rapidly respond to incidents related to these roles).
See Microsoft's recommended steps at https://aka.ms/sparoadmap that covers:

- End to End Session Security (including multi-factor authentication (MFA) for admins)
- Protect and Monitor Identity Systems
- Mitigate Lateral Traversal
- Rapid Threat Response

@2021, Microsoft Corporation. All rights reserved.

Preparing for Ransomware Attacks:
Stay ahead of attackers

Step 3

Prepare your recovery plan: Recover without paying

There are a wide variety of technical controls that should be in place to protect, detect and respond to ransomware incidents with a strong emphasis on prevention. This should include some or all of the following essential tools.

Plan for the worst-case scenario and expect that it will happen (at all levels of the organization). This will both help your organization and others in the world you depend on:

a) **Limit damage for the worst-case scenario**

While restoring all systems from backups is highly disruptive to business, this is more effective and efficient than trying to recover using (low quality) attacker-provided decryption tools after paying to get the key.

Note: Paying is an uncertain path. You have no formal or legal guarantee that the key works on all files, the tools will work effectively, or that the attacker (who may be an amateur affiliate using a professional's toolkit) will act in good faith.

b) **Limit the financial return for attackers**

If an organization can restore business operations without paying the attackers, the attack has effectively failed and resulted in zero return on investment (ROI) for the attackers. This makes it less likely that they will target the organization in the future (and deprives them of additional funding to attack others).

Note: The attackers may still attempt to extort the organization through data disclosure or abusing/selling the stolen data, but this gives them less leverage than if they have the only access path to your data and systems.

To realize this, organizations should ensure they:

1. **Register Risk**
   Add ransomware to risk register as high likelihood and high impact scenario. Track mitigation status via Enterprise Risk Management (ERM) assessment cycle.

2. **Define and Backup Critical Business Assets**
   Define systems required for critical business operations and automatically back them up on a regular schedule (including correct backup of critical dependencies like Active Directory).

3. **Protect backups** against deliberate erasure and encryption with offline storage, immutable storage, and/or out of band steps (MFA or PIN) before modifying/erasing online backups.

4. **Test 'Recover from Zero' Scenario**
   Test to ensure your business continuity / disaster recovery (BC/DR) can rapidly bring critical business operations online from zero functionality (all systems down). Conduct practice exercise(s) to validate cross-team processes and technical procedures, including out of band employee and customer communications (assume all email/chat/etc. is down).

   a). **IMPORTANT:** Protect (or print) supporting documents and systems required for recovery including restoration procedure documents, CMDBs, network diagrams, SolarWinds instances, etc. Attackers destroy these regularly.

5. **Reduce on-premises exposure** by moving data to cloud services with automatic backup & self-service rollback.

@2021, Microsoft Corporation. All rights reserved.

Promote awareness and ensure there is no knowledge gap

There are a number of activities that may be undertaken to prepare for potential ransomware incidents.

Educate end-users on the dangers of ransomware

As most ransomware variants rely on end-users to install the ransomware or connect to compromised Web sites, all end-users should be educated about the dangers. This would typically be part of annual security awareness training, as well as ad hoc training available through the company's learning management systems. The awareness training should also extend to the company's customers via the company's portals or other appropriate channels.

Educate security operations center (SOC) analysts and others on how to respond to ransomware incidents

SOC analysts and others involved in ransomware incidents should know the fundamentals of malicious software and ransomware specifically. They should be aware of major variants/families of ransomware, along with some of their typical characteristics. Customer call center staff should also be aware of how to handle ransomware reports from the company's end-users and customers.

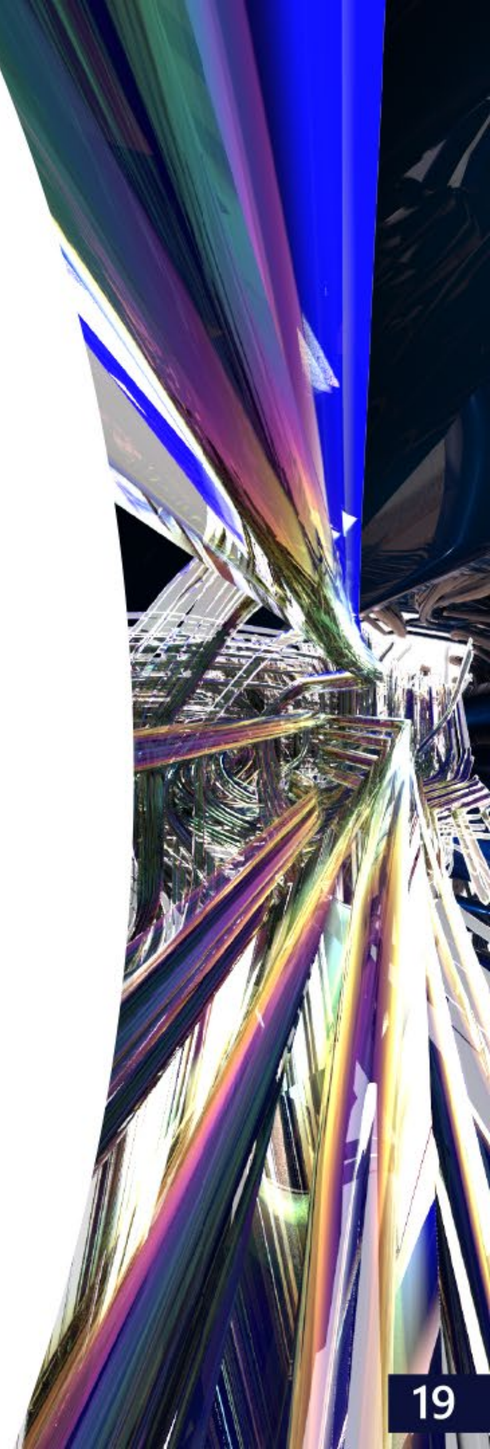
Ensure that you have appropriate technical controls in place

There are a wide variety of technical controls that should be in place to protect, detect and respond to ransomware incidents with a strong emphasis on prevention. At a minimum, security operations center (SOC) analysts should have access to the telemetry generated by antimalware systems in the company, understand what preventive measures are in place, understand the infrastructure targeted by ransomware, and be able to assist the company teams to take appropriate action.

This should include some or all of the following essential tools:

Detective and preventive tools

- Enterprise server antimalware product suites (such as Azure Defender)
- Network antimalware solutions (such as Microsoft Antimalware for Azure)
- Security data analytics platforms (such as Azure Monitor, Azure Sentinel)
- Next generation intrusion detection and prevention systems
- Next generation firewall (NGFW)



@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

Preparing for Ransomware Attacks:
Stay ahead of attackers

Malware analysis and response toolkits

- Automated malware analysis systems with support for most major end-user and server operating systems in the organization
- Static and dynamic malware analysis tools
- Digital forensics software and hardware
- Non-Organizational Internet access (e.g. 4G dongle)

For maximum effectiveness, SOC analysts should have extensive access to almost all antimalware platforms through their native interfaces in addition to unified telemetry within the security data analysis platforms. **The platform for Azure native Antimalware for Azure Cloud Services and Virtual Machines provides step-by-step guides on how to accomplish this.**

Enrichment and intelligence sources

- Online and offline threat and malware intelligence sources (such as Azure Sentinel, Azure Network Watcher)
- Azure Active Directory and other authentication systems (and related logs)
- Internal Configuration Management Databases (CMDBs) containing endpoint device info

Data protection

Implement data protection to ensure rapid and reliable recovery from a ransomware attack + block some techniques.

Designate Protected Folders to make it more difficult for unauthorized applications to modify the data in these folders.

Review Permissions to reduce risk from broad access enabling ransomware

- **Discover broad write/delete permissions** on fileshares, SharePoint, and other solutions
- **Reduce broad permissions** while meeting business collaboration requirements
- **Audit and monitor** to ensure broad permissions don't reappear

Secure backups

Ensure critical systems are backed up and backups are protected against deliberate attacker erasure/encryption.

Backup all critical systems automatically on a regular schedule.

Ensure Rapid Recovery of business operations by regularly exercising business continuity / disaster recovery (BC/DR) plan.

Protect supporting documents required for recovery such as restoration procedure documents, CMDB, and network diagrams.

Protect backups against deliberate erasure and encryption.

- **Strong Protection** – Require out of band steps (like MUA/MFA) before modifying online backups (e.g. Azure Backup)
- **Strongest Protection** Isolate backups from online / production workloads to enhance the protection of backup data

@2021, Microsoft Corporation. All rights reserved.

Preparing for Ransomware Attacks:
Stay ahead of attackers

Establish an incident handling process

Ensure your organization undertakes a number of activities roughly following the incident response steps and guidance described in the US National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (Special Publication 800-61r2) to prepare for potential ransomware incidents.

As illustrated in Figure 8, these steps include:

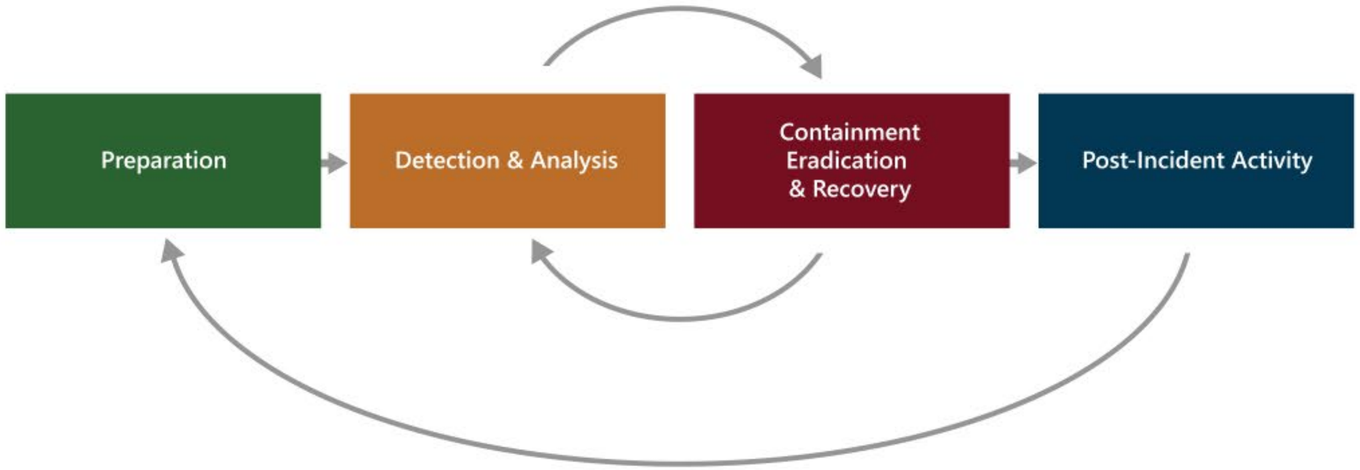


Figure 8: NIST SP 800-61r2 Incident Response Life Cycle

1. **Preparation:**
   This stage describes the various measures that should be put into place prior to an incident. This may include both technical preparations (such as the implementation of suitable security controls and other technologies) and non-technical preparations (such as the preparation of processes and procedures).

2. **Triggers / Detection:**
   This stage describes how this type of incident may be detected and what triggers may be available that should be used to initiate either further investigation or the declaration of an incident. These are generally separated into high-confidence and low-confidence triggers.

3. **Investigation / Analysis:**
   This stage describes the activities that should be undertaken to investigate and analyze available data when it is not clear that an incident has occurred, with the goal of either confirming that an incident should be declared or concluded that an incident has not occurred.

4. **Incident Declaration:**
   This stage covers the steps that must be taken to declare an incident, typically with the raising of a ticket within the enterprise incident management (ticketing) system and directing the ticket to the appropriate personnel for further evaluation and action.

5. **Containment / Mitigation:**
   This stage covers the steps that may be taken either by the Security Operations Center (SOC), or by others, to contain or mitigate (stop) the incident from continuing to occur or limiting the effect of the incident using available tools, techniques and procedures.

6. **Remediation / Recovery:**
   This stage covers the steps that may be taken to remediate or recover from damage that was caused by the incident before it was contained and mitigated.

7. **Post-Incident Activity:**
   This stage covers the activities that should be performed once the incident has been closed. This can include capturing the final narrative associated with the incident as well as identifying lessons learned.

@2021, Microsoft Corporation. All rights reserved.

Preparing for Quick Recovery: *Restore business operations fast*

Ensure that you have appropriate processes and procedures in place

Almost all ransomware incidents result in the need to restore compromised systems. So appropriate and tested backup and restore processes and procedures should be in place for most systems. In addition, suitable containment strategies and procedures should be put in place to stop ransomware from spreading and recovery from ransomware attacks.

Ensure that you have well-documented procedures for engaging any third-party support, particularly support from threat intelligence providers, antimalware solution providers and from the malware analysis provider. These contacts may be useful if the ransomware variant may have known weaknesses or decryption tools may be available.

In addition, recovery documents need to be in an offline/immutable storage as they are a key target of ransomware.

The Azure platform provides backup and recovery options through Azure Backup as well as built-in within various data services and workloads.

Isolated backups with Azure Backup

- Azure Virtual Machines
- Databases in Azure VMs: SQL, SAP HANA
- Azure Database for PostgreSQL
- On-premises Windows Servers (back up to cloud using Microsoft Azure Recovery Services (MARS) agent)

Local (operational) backups with Azure Backup

- Azure Files
- Azure Blobs
- Azure Disks

Built-in backups from Azure services

- Data services like Azure Databases (SQL, MySQL, MariaDB, PostgreSQL), Cosmos DB and ANF offer built-in backup capabilities

@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

Detecting Ransomware Attacks:
Accelerate detection with the right tools

There are several potential triggers that may indicate a ransomware incident. Unlike many other types of malware, most will be higher-confidence triggers, such as lockouts and displays of on-screen alerts (where little additional investigation or analysis should be required prior to the declaration of an incident), rather than lower-confidence triggers (where more investigation or analysis would likely be required before an incident should be declared).

In general, such infections are obvious from basic system behavior, the absence of key system or user files and the demand for ransom. In this case, the analyst should consider whether to immediately declare and escalate the incident, including taking any automated actions to mitigate the attack.

Azure Defender provides high quality threat detection and response capabilities, also called Extended Detection and Response – XDR.

End-to-end security solutions

Protect your enterprise from advanced threats across hybrid cloud workloads

Azure Defender
Provides high quality threat detection and response capabilities, also called Extended Detection and Response -XDR

Security Center
Unify security management and enable advanced threat protection across hybrid cloud workloads

Azure Sentinel
Standing watch, by your side. Intelligent security analytics for your entire enterprise

Azure Firewall
Network traffic is subjected to the configured firewall rules

Key Vault
Safeguard and maintain control of keys and other secrets

Application Gateway
Build secure, scalable and highly available web front ends in Azure

Azure Information Protection
Better protect your sensitive information - anytime, anywhere

VPN Gateway
Establish secure, cross-premises connectivity

Azure Active Directory
Synchronize on-premises directories and enable single sign-on

DDoS Protection
Protect your applications from Distributed Denial of Service (DDoS) attacks

Azure Dedicated HSM
Manage hardware security modules that you use in the cloud

@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

Detecting Ransomware Attacks:
Accelerate detection with the right tools

Ensure rapid detection and remediation of common attacks on VMs, SQL Servers, Web applications, and identity.

Prioritize Common Entry Points - Ransomware (and other) operators favor Endpoint/Email/Identity + RDP

Integrated XDR

Use integrated Extended Detection and Response (XDR) tools like Azure Defender to provide high quality alerts and minimize friction and manual steps during response.

Brute Force

Monitor for brute force attempts like password spray.

Monitor for Adversary Disabling Security - This is often part of a Human Operated Ransomware (HumOR) attack chain

Event Logs Clearing

Especially the Security Event log and PowerShell Operational logs.

Disabling of security tools/controls

(associated with some groups).

Don't Ignore Commodity Malware - Ransomware attackers regularly purchase access to target organizations from dark markets.

Integrate outside experts - Integrate outside experts into processes to supplement expertise, such as Microsoft Detection and Response Team (DART).

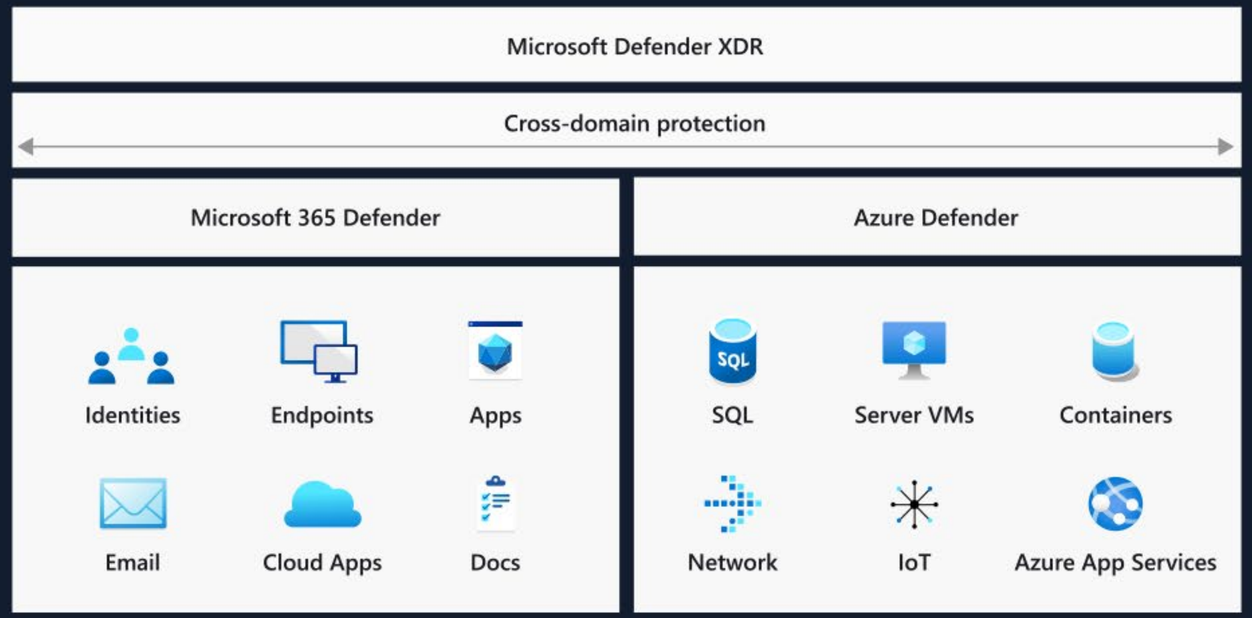
Rapidly isolate - Rapidly isolate compromised computers using Defender for Endpoint in on-premises deployment.

SIEM and XDR - get the best of both worlds

What if you had visibility into threats across all your resources, AI that stitched signals together and told you what's most important, and the ability to respond swiftly across the organization?

In Microsoft Defender, the most comprehensive XDR solution on the market, Microsoft 365 Defender comes together with Azure Defender, a built-in tool that provides protection for hybrid data, cloud-native services and servers.

View intelligent security analytics for your entire enterprise in a single console by integrating Microsoft Defender and third-party security solutions with Azure Sentinel, our cloud-native SIEM.



@2021, Microsoft Corporation. All rights reserved.

Responding to Ransomware Attacks:
Increase effectiveness with practiced IR teams

Incident declaration

Once a successful ransomware infection has been confirmed, the analyst should verify if this represents a new incident or is related to an existing incident. Look for currently-open tickets that indicate similar incidents. If so, update the current incident ticket with new information in the ticketing system. If this is a new incident, an incident should be declared in the relevant ticketing system and escalated to the appropriate teams or providers to contain and mitigate the incident. Be mindful that managing ransomware incidents may require actions taken by multiple IT and security teams. Where possible, ensure that the ticket is clearly identified as a ransomware incident to guide workflow.

Containment / Mitigation

In general, various server/endpoint antimalware, email antimalware and network protection solutions should be configured to automatically contain and mitigate known ransomware. There may be cases, however, where the specific ransomware variant has been able to bypass such protections and successfully infect target systems.

Microsoft provides extensive resources to help update your incident response processes on the Top Azure Security Best Practices.

The following are recommended actions to contain or mitigate a declared incident involving ransomware where automated actions taken by antimalware systems have been unsuccessful:

1. Engage antimalware vendors through standard support processes
2. Manually add hashes and other information associated with malware to antimalware systems
3. Apply antimalware vendor updates
4. Contain affected systems until they can be remediated
5. Disable compromised accounts
6. Perform root cause analysis
7. Apply relevant patches and configuration changes on affected systems
8. Block ransomware communications using internal and external controls
9. Purge cached content

@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

Road to Recovery: *Microsoft experts provide insights*

Microsoft's Detection and Response Team will help protect you from attacks

Understanding and fixing the fundamental security issues that led to the compromise in the first place should be a priority for ransomware victims.

Integrate outside experts - into processes to supplement expertise, such as Microsoft Detection and Response Team (DART). The DART engages with customers around the world, helping to protect and harden against attacks before they occur, as well as investigating and remediating when an attack has occurred.

Customers can engage our security experts directly from within Microsoft Defender Security Center for timely and accurate response. Experts provide insights needed to better understand the complex threats affecting your organization, from alert inquiries, potentially compromised devices, root cause of a suspicious network connection, to additional threat intelligence regarding ongoing advanced persistent threat campaigns.

@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

Road to Recovery: *Microsoft experts provide insights*

Microsoft is ready to assist your company in returning to safe operations.

Microsoft performs hundreds of compromise recoveries and has a tried-and-true methodology. Not only will it get you to a more secure position, it affords you the opportunity to consider your long-term strategy rather than reacting to the situation.

Microsoft provides Rapid Ransomware Recovery services. Under this, assistance is provided in all areas such as restoration of identity services, remediation and hardening and with monitoring deployment to help victims of ransomware attacks to return to normal business in the shortest possible timeframe.

Our Rapid Ransomware Recovery services are treated as "Confidential" for the duration of the engagement. Rapid Ransomware Recovery engagements are exclusively delivered by the WW Compromise Recovery Security Practice (CRSP), part of the Azure Cloud & AI Domain. For more information you can contact CRSP at Request contact about Azure security.

@2021, Microsoft Corporation. All rights reserved.

Conclusion

Microsoft focuses heavily on both the security of our cloud, and providing you the security controls you need to protect your cloud workloads. As a leader in cybersecurity, we embrace our responsibility to make the world a safer place. This is reflected in our comprehensive approach to ransomware prevention and detection in our security framework, designs, products, legal efforts, industry partnerships, and services.

We look forward to partnering with you in addressing ransomware protection, detection and prevention in a holistic manner.

@2021, Microsoft Corporation. All rights reserved.

Additional Resources

Microsoft Cloud Adoption Framework for Azure

Build great solutions with the Microsoft Azure Well-Architected Framework

Azure Top Security Best Practices

Security Baselines

Resource Center | Microsoft Azure

Azure Migration Guide

Security Compliance Management

Azure Security Control – Incident Response

Zero Trust Guidance Center

Azure Web Application Firewall

Azure VPN gateway

Azure Multi-Factor Authentication (MFA)

Azure AD Identity Protection

Azure AD Conditional Access

Azure Security Center documentation

To report a ransomware breach, contact the FBI at:

IC3 Complaint Referral Form

@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

Connect with us!

- AskAzureSecurity@microsoft.com
- www.microsoft.com/services

For detailed information on how Microsoft secures our cloud, visit the service trust portal (https://servicetrust.microsoft.com/).

@2021, Microsoft Corporation. All rights reserved.

Microsoft Azure

We embrace our responsibility to create a safer world that enables organizations to digitally transform. We Have Your Back!

Thank You

@2021, Microsoft Corporation. All rights reserved.