Ransomware Protection Guide

This guide outlines best practices on how to protect and defend against ransomware attacks leveraging the Microsoft security stack.

CRITICALSTART®

Ransomware attacks are not only becoming more sophisticated, but also more frequent.

These five major attacks took place in the first five months of 2022:

- ✓ **January 5th – Bernalillo County, New Mexico**
- ✓ **February 23rd – Nvidia**
- ✓ **March 1st – Toyota Motors**
- ✓ **April 17th – Cost Rica Government**
- ✓ **May 24th – SpiceJet**

Microsoft security researchers have tracked a 13.4% increase in organizations that have encountered ransomware over the last year.

Critical Start simplifies breach prevention seamlessly with Microsoft security controls by providing SOC services and solutions that flex to your business objectives and security vision, regardless of complexity.

CRITICALSTART®

Prevent Malware Delivery

Best Practices

Ransomware infections usually start with email, through a malicious URL or attachment. You can mitigate their impact by implementing network services such as:

- ✓ Filtering email and spam to block malicious emails and remove executable attachments
- ✓ Intercepting proxies and utilizing safe browsing lists within browsers to block known malicious websites
- ✓ Deploying Internet security gateways, which can inspect content in certain protocols (including some encrypted protocols) for known malware

Suggested Solution

Attackers hide malicious website links in emails or other files. Safe Links and Safe Attachments Policies, part of Microsoft Defender for Office 365, can help protect your organization by providing time-of-click verification of web addresses (URLs) and attachments in email messages and Microsoft Office applications. such as SharePoint and Teams.

You can protect against ransomware by creating one or more mail flow rules to block file extensions that are commonly used for ransomware. A good starting point is to create two rules:

Safe Attachments Policy:

Block file types that could contain ransomware or other malicious code. Below is a common list of executables which we recommend blocking:

Setting	Block file types that could contain ransomware or other malicious code
Name	Anti-ransomware rule: block file types
Apply this rule if...	Any attachment... file extension matches...
Specify words or phrases	Add these file types: ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh, exe, pif
Do the following...	Block the message

Safe Links Policy:

Safe Links is a feature in Defender for Office 365 that provides URL scanning and rewriting of inbound email messages in mail flow and time-of-click verification of URLs and links in email messages and other locations.

Setting or option	Recommended setting
Name	Safe links policy for all recipients in the domain
Select the action for unknown potentially malicious URLs in messages	Select On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.
Apply real-time URL scanning for suspicious links and links that point to files	Select this box.
Applied to	The recipient domain is . . . select your domain.

CRITICALSTART®

Prevent Spread and Malicious Code Execution

Best Practices

Adopt a zero-trust approach. Assume that malware will reach your organization's devices. We suggest you take steps to prevent malware from running at device-level by implementing security features such as:

- ✓ Antivirus
- ✓ Exploit protection
- ✓ Attack surface reduction
- ✓ Application control
- ✓ Hardware-based isolation

Suggested Solution

Enable Cloud-Backed Rapid Detection

Microsoft Defender for Endpoint provides cloud-delivered protection for near-instant detection and blocking of new and emerging threats. Dedicated protection is updated based on machine learning, human and automated big-data analysis, and in-depth threat resistance research. LEARN MORE

Enable Always-on scanning for advance file and process behavior monitoring

Microsoft Defender for Endpoint's next-generation protection capabilities provide always-on scanning, using advanced file and process behavior monitoring and other heuristics (also known as "real-time protection"). With advanced in-memory capabilities, as well as Attack Surface Reduction controls and network protection capabilities, this tool can also prevent file-less malware. LEARN MORE

Block malware at first sight

A new antivirus capability from Microsoft Defender for Endpoint called Block at First Sight, provides critical malware protection. Approximately 96% of all malware files detected and blocked by these antivirus capabilities are observed only once in the world. If a threat is unknown and metadata about the threat isn't enough, we've configured the antivirus features to automatically collect and scan the sample in the Microsoft cloud to analyze it for zero-day threats. This includes running the suspicious file in a virtualized environment. LEARN MORE

Enable Attack Surface Reduction (ASR)

Attack surface reduction rules target certain software behaviors, such as:

- ✓ Launching executable files and scripts that attempt to download or run files
- ✓ Running obfuscated or otherwise suspicious scripts
- ✓ Performing behaviors that apps don't usually initiate during normal day-to-day work

Such software behaviors are sometimes seen in legitimate applications; however, these behaviors are often considered risky because they are commonly abused by attackers through malware. Attack surface reduction rules can constrain risky behaviors and help keep your organization safe. LEARN MORE

Enforce Application Control

Application Control helps mitigate security threats by restricting the applications that users can run and the code that runs in the system core (kernel This tool also allows you to create policies to block unsigned scripts and MSIs and force Windows PowerShell to run in Constrained Language mode. LEARN MORE

Enforce Auto-Security Updates

Ensure Security Updates are downloaded automatically and installed during Automatic mode, when the device isn't in use or running on battery power. LEARN MORE

Secure Access & Protect Sensitive Data

Best Practices

Use Data Loss Prevention (DLP) rules and policies to determine which files and data are considered confidential, critical, or sensitive, and then protect those files from being accessed, shared or transmitted.

Suggested Solution

Enforce Zero Trust for User + Device Validation

Configure Microsoft Azure AD Identity security features, such as device-compliance, location-based and user risk-based Conditional Access policies and Azure multi-factor authentication (MFA) for sensitive data access.

Enable Office 365 Message Encryption

Office 365 Advanced Message Encryption provides additional protection by allowing message expiration and revocation. You can also create multiple templates for encrypted emails originating from your organization.

Enable File- Level Encryption and Access Control

Microsoft Information Protection uses encryption, identity, and authorization policies to protect your sensitive files. Protection (such as encryption and access rights) is applied by using Rights Management, which stays with the documents and emails, independently of the location—inside or outside your organization, networks, file servers, and applications. This information protection solution keeps you in control of your data, even when it is shared with other people.

Implement Controlled Folder Access

Protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders.

CRITICALSTART®

Protect Against Ransomware with SIEM + XDR + MDR

Best Practices

Combine the breadth of Microsoft Sentinel™ cloud-native SIEM with the depth of Critical Start's MDR for Microsoft 365 Defender to help defend against attacks that take advantage of today's diverse, distributed and complex environments.

Apart from better response planning, security leaders are putting their faith in data: 88% agreed that better capture and analysis of detection data is one of their most effective tools for preventing successful ransomware attacks.

– The State of Security 2022

A single tool cannot detect and protect against ransomware and other cyber risks. However, combining the power of SIEM, XDR and MDR gives you unmatched visibility to detect every threat and resolve every alert.

Suggested Solution

SIEM: A single pane of glass

- ✓ Security information and event management (SIEM) ingests event logs and offers a single view of this data with additional insights. SIEMs can help you resolve misconfigurations, compensate for operational flaws and other engineering errors—benefits you cannot get from an MDR solution alone. When a potential issue is detected, a SIEM can log additional information, generate an alert and instruct other security controls to stop an attacker's progress. SIEM tools can also help you meet regulatory requirements by collecting and aggregating data from across your IT infrastructure into a centralized platform where it can be reviewed by security analysts.

XDR: Holistic protection against cyberattacks, unauthorized access and misuse

- ✓ Extended detection and response (XDR) breaks down traditional security silos to deliver detection and response across all data sources, including endpoint, network and cloud data, while applying analytics and automation to address increasingly sophisticated threats. This technology helps your team identify hidden threats proactively and quickly and track those threats across any source or location within the organization, increasing productivity and helping you get more out of your security investment.

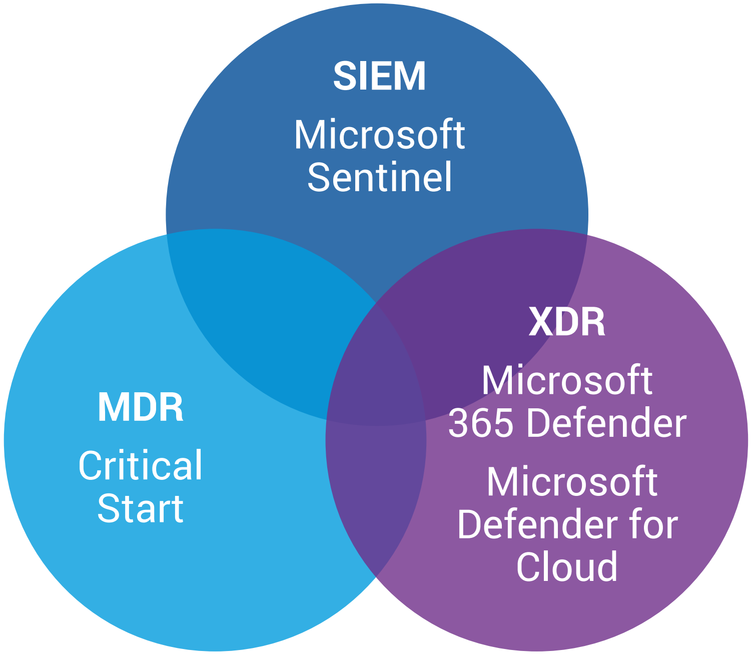
MDR: Maximizing the Value and Effectiveness of SIEM + XDR

- ✓ As stand-alone tools, SIEM and XDR have limitations and challenges—primarily, they require people who know how to use them effectively.
- ✓ For a successful SIEM implementation, you must make choices about what to ingest based on the value of your data and make adjustments as your needs change. Critical Start MDR for SIEM simplifies this process by prioritizing data based on what we have observed with other customers and MITRE ATT&CK® coverage, then our trust-oriented approach to MDR eliminates false positives at scale to streamline the investigation and response process. We become deeply familiar with your business and take the entire SIEM journey with you-- from onboarding to personalization to investigation to continuously maturing your security platform—to ensure the best outcomes.
- ✓ To successfully implement XDR, you also need human talent to parse through intelligence, apply analytics and separate real incidents from the noise. Otherwise, attackers will continue to find new ways to get through your defenses.

Bringing It All Together

As a Microsoft MXDR partner, Critical Start leverages deep Microsoft experience to eliminate the pain of deployment and stays by your side as we identify new risks. Our integrated threat and detection and response services give you unmatched visibility across your Microsoft ecosystem to detect every threat and resolve every incident:

- ✓ Our **Microsoft Consulting Services** team offers workshops focused on helping you achieve your broader security objectives with SIEM + XDR, including helping you gain visibility into immediate threats across email, identity, and data, plus clarity and support on how to upgrade your security posture for the long term.
- ✓ Our U.S.-based **Security Operations Center (SOC)** provides 24x7x365 alert triage, analysis and response, backed by a one-hour SLA for mean time to detect (MTTD) and mean time to respond (MTTR).
- ✓ Our **Trusted Behavior Registry™ (TBR)**, a proprietary technology within our Zero Trust Analytics Platform™ (ZTAP™), eliminates false positives – the largest volume of alerts – at scale and allows humans to investigate and resolve all remaining alerts of all priorities. (This is especially important for ransomware attacks such as LockBit ransomware which disguise themselves as low-level alerts.)
- ✓ CRITICAL**START® Threat Navigator** maps IOCs to the MITRE ATT&CK® Framework for visibility into detection coverage from your security controls and current adversarial activity in your environment.
- ✓ Our **Cyber Research Unit (CRU)** curates original and third-party threat intel to develop and enrich new detections and IOCs.



CRITICALSTART®

Critical Start Services & Solutions for Microsoft Security

Critical Start simplifies breach prevention seamlessly with Microsoft security controls by providing SOC services and solutions that flex to your business objectives and cybersecurity vision, regardless of the complexity.

Our services and solutions, coupled with Microsoft's world-class threat intelligence and cutting-edge security portfolio, extends the capabilities of your in-house security staff to help you stay ahead of advanced threats.

ZTAP/TBR

Our trust-oriented approach leverages the Zero Trust Analytics Platform (ZTAP) platform to collect, understand, and resolve every alert. Our Trusted Behavior Registry (TBR) reduces false positives by enabling us to auto-resolve false positives – the largest volume of alerts – at scale. And, ZTAP strengthens our investigation of unknown alerts to ensure the escalation of the alerts that really require the attention of your security team.

MOBILESOC®

Now, you can fully triage and contain alerts from anywhere. Collaborate with Critical Start analysts in near real-time from within our iOS and Android mobile app. Review their analysis and corrective measures and take your own direct action immediately with information gathered in our platform to reduce attacker dwell time.

THE HUMAN ELEMENT

We provide 24x7x365 human-led end-to-end monitoring, investigation, and remediation of alerts. This includes a dedicated customer success manager for continued optimization of your MDR service. Our Customer Success Team works with you on an ongoing basis to learn your security needs so that we can optimize your services and security tools for optimal threat detection and response.

Microsoft Security Best Practices + Critical Start Managed Detection & Response (MDR)

Prevent Malware Delivery

EMAIL / COLLABORATION

ENDPOINT

REMOTE ACCESS

ACCOUNTS

Defender for Office 365

- ✓ Safe Attachments
- ✓ Safe Links
- ✓ Safe Attachments
- ✓ Anti-phishing Protection

Defender for Endpoint

- ✓ Threat & Vulnerability Management
- ✓ Attack Surface Reduction
- ✓ Endpoint Detection and Response
- ✓ Microsoft Secure Score for Devices

Prevent Spread and Execution

EMAIL / COLLABORATION

ENDPOINT

REMOTE ACCESS

ACCOUNTS

Defender for Endpoint

- ✓ Next-generation Protection
- ✓ Block at First Sight
- ✓ Always-on Scanning
- ✓ Automated Investigation and Remediation

Defender for Office 365

- ✓ Real-time Detections
- ✓ Automated Investigation and Response

Protect Sensitive Data

DATA PROTECTION & BACKUPS

SECURE ACCESS

Azure AD Identity Security Features

- ✓ Azure AD Conditional Access policies
- ✓ Azure AD Multi-Factor Authentication
- ✓ Azure AD Identity Protection

Microsoft Information Protection

- ✓ Office 365 Message Encryption
- ✓ Endpoint Data Loss Prevention
- ✓ Controlled Folder Access

Azure Backup and OneDrive

- ✓ OneDrive for Business Restore Feature
- ✓ Azure Backup Hybrid Recovery Services

Azure Sentinel

CLOUD SIEM →

Managed Detection and Response

- ✓ Zero Trust Analytics Platform (ZTAP) & Trusted Behavior Registry (TBR)
- ✓ MobileSOC
- ✓ 24x7x365 Monitoring

→ → CRITICALSTART®

CRITICALSTART®

SUMMARY

Following our suggested best practices will help better secure your enterprise against ransomware attacks, but remember to always stay vigilant. As we have seen cyber criminals can find new vectors and vulnerabilities to exploit, so you must continuously assess your environment for risks and vulnerabilities. Critical Start can help. Our Cybersecurity Consulting offerings are based on a three-phase process (Assess/Respond/Defend) that helps secure your infrastructure on-premise or in the cloud, meets compliance standards, and reduces your exposure.

For more details about our MDR and Cybersecurity Consulting offerings, visit **www.criticalstart.com.**