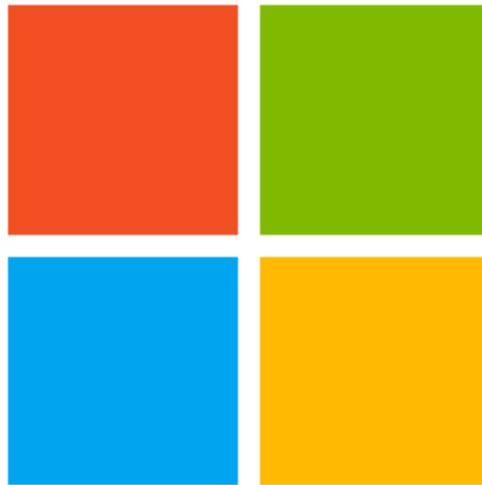


# Human-operated ransomware

---

[docs.microsoft.com/en-us/security/compass/human-operated-ransomware](https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware)



- Article
- 02/19/2022
- 3 minutes to read
- 

## In this article

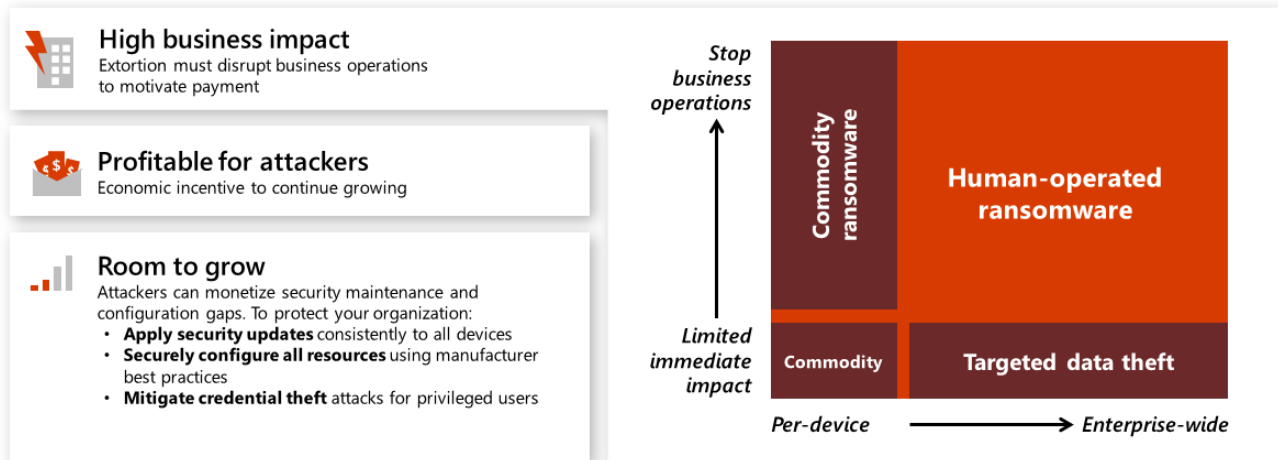
---

Ransomware is a type of extortion attack that destroys or encrypts files and folders, preventing access to critical data. Commodity ransomware typically spreads like a virus that infects devices and only requires malware remediation. Human-operated ransomware is the result of an active attack by cybercriminals that infiltrate an organization's on-premises or cloud IT infrastructure, elevate their privileges, and deploy ransomware to critical data.

These "hands-on-keyboard" attacks target an organization rather than a single device and leverage human attackers' knowledge of common system and security misconfigurations to infiltrate the organization, navigate the enterprise network, and adapt to the environment and its weaknesses as they go. Hallmarks of these human-operated ransomware attacks typically include credential theft and lateral movement and can result in deployment of a ransomware payload to high business impact resources the attackers choose.

These attacks can be catastrophic to business operations and are difficult to clean up, requiring complete adversary eviction to protect against future attacks. Unlike commodity ransomware that only requires malware remediation, human-operated ransomware will continue to threaten your business operations after the initial encounter.

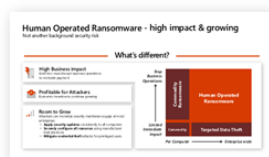
This figure shows how this extortion-based attack that uses maintenance and security configuration gaps and privileged access is growing in impact and likelihood.



## Protect your organization against ransomware and extortion

For a comprehensive view of ransomware and extortion and how to protect your organization, use the information in the [Human-Operated Ransomware Mitigation Project Plan](#) PowerPoint presentation.

Here's a summary of the guidance:



### Stakes have changed with No End in Sight

Massive growth trajectory from:

- **Attacker profitability** to fund and incent future attacks.
- **Lack of resistance** from legal, technical, or security obstacles.



### Attacks have weaknesses – Successful extortion relies on:

- **Denying alternatives to payments** – They must prevent you from restoring from backups.
- **Getting asset access** – Rapid lateral traversal across the enterprise (e.g. IT admin privileges).



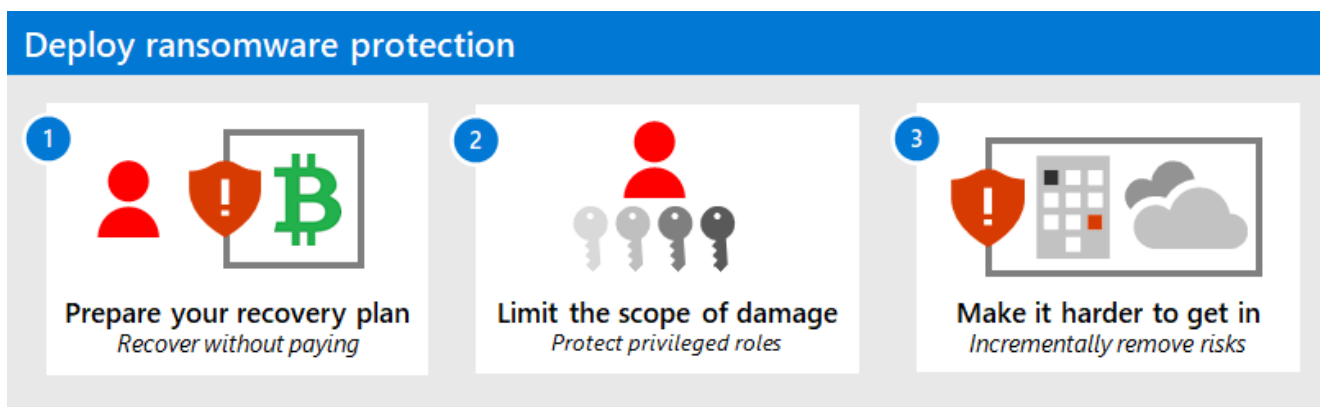
### Focus on **attack weaknesses** first:

1. **Restore critical business operations** – Ensure ability to rapidly restore backups and business processes.
2. **Protect admins** – Strengthen privileged access security.
3. **Entry points** - Prioritize fastest and most effective mitigation of entry points (continually increase attacker cost/friction).

- The stakes of ransomware and extortion-based attacks are high.
- However, the attacks have weaknesses that can mitigate your likelihood of being attacked.
- There are three phases to configure your infrastructure to exploit attack weaknesses.

For the three phases to exploit attack weaknesses, see the [Protect your organization against ransomware and extortion](#) solution to **quickly** configure your IT infrastructure for the best protection:

1. Prepare your organization to recover from an attack without having to pay the ransom.
2. Limit the scope of damage of an attack by protecting privileged roles.
3. Make it harder for an attacker to get into your environment by incrementally removing risks.



Download the [Protect your organization from ransomware poster](#) for an overview of the three phases as layers of protection against ransomware attackers.

Use this poster as a checklist to deploy features and services for layers of protection and mitigation against ransomware attacks.



Layers of protection and mitigation

### Prevent attackers from getting in

#### Remote access

- ❑ Maintain software and appliance updates
- ❑ Enforce [Zero Trust](#) user and device validation with Azure AD Conditional Access.
- ❑ Configure security for third-party VPN solutions.
- ❑ Deploy Azure Point-to-Site (P2S) VPN.
- ❑ Publish on-premises web apps with Azure AD Application Proxy.
- ❑ Secure access to Azure resources with [Azure Bastion](#).

#### Email and collaboration

- ❑ Enable AMSI for Office VBA.
- ❑ Implement Advanced Email security using [Defender for Office 365](#).
- ❑ [Enable attack surface reduction \(ASR\)](#) rules to block common attack techniques.

#### Endpoints

- ❑ Block known threats with ASR rules, [tamper protection](#), and [block at first sight](#).
- ❑ Apply [Security Baselines](#) to harden internet-facing Windows servers and clients and Office applications.
- ❑ Maintain your software so that it is updated and supported.
- ❑ Isolate, disable, or retire insecure systems and protocols.
- ❑ Block unsuspected traffic with host-based firewalls and network defenses.

#### Accounts

- ❑ Enforce strong MFA or passwordless sign-in for all users
- ❑ Increase password security with [Azure AD Password Protection](#)

Audit and monitor to find and fix deviations from baseline security and potential attacks

Situation
Keep them out
Mitigation goal
Services, devices, and user accounts are hardened against typical attack vectors.
Mitigation success
It's too difficult for attackers to compromise a device or get any valid user account credentials.

---

### Prevent an attacker from escalating their privileges

#### Privileged access strategy

- ❑ Enforce end-to-end session security for administration portals using [Azure AD Conditional Access](#).
- ❑ Protect and monitor identity systems to prevent escalation attacks.
- ❑ Detect and mitigate lateral traversal with compromised devices.
- ❑ Use [Azure AD Privileged Identity Management](#) time-based and approval-based role activation.
- ❑ Use [Privileged Access Management \(PAM\)](#) to limit standing access to sensitive data or access to critical configuration settings.

#### Detection and response

- ❑ Prioritize common entry points:
  - ❑ Use integrated Extended Detection and Response (EDR) tools like Microsoft 365 Defender and Azure Sentinel to provide high quality alerts and minimize friction and manual steps during response.
  - ❑ Monitor for brute-force attempts like password spray.
  - ❑ Don't ignore commodity malware.
- ❑ Monitor for an adversary disabling security (this is often part of an attack chain), such as:
  - ❑ Event log clearing, especially the Security Event log and PowerShell Operational logs.
  - ❑ Disabling of security tools and controls (associated with some groups).
- ❑ Integrate outside experts into processes to supplement expertise, such as the [Microsoft Detection and Response Team \(DART\)](#).
- ❑ Rapidly isolate compromised computers using [Defender for Endpoint](#).

Situation
Oh, no! They're in!
Mitigation goal
Limit the blast radius of the attacker by protecting admin and priority accounts and quickly responding to attacks.
Mitigation success
It's too hard for attackers to get any admin or priority account credentials and perform admin tasks without being detected.

---

### Protect your critical data from access and destruction

#### Secure backups

- ❑ Backup all critical systems automatically on a regular schedule.
- ❑ Protect backups against deliberate erasure and encryption:
  - ❑ Strong Protection: Require out of band steps (MFA or PIN) before modifying online backups (such as [Azure Backup](#))
  - ❑ Strongest Protection: Store backups in online immutable storage (such as [Azure Blob](#)) and/or fully offline or off-site.
- ❑ Regularly exercise your business continuity/disaster recovery (BC/DR) plan.
- ❑ Protect supporting documents required for recovery such as restoration procedure documents, your configuration management database (CMDB), and network diagrams.

#### Data protection

- ❑ Migrate your organization to the cloud:
  - ❑ Move user data to cloud solutions like OneDrive/SharePoint to take advantage of [versioning and recycle bin capabilities](#).
  - ❑ Educate users on how to [recover their files](#) by themselves to reduce delays and cost of recovery.
  - ❑ Designate [Protected Folders](#).
- ❑ Review your permissions:
  - ❑ Discover broad write/delete permissions on file shares, SharePoint, and other solutions. Broad is defined as many users having write or delete permissions for business-critical data.
  - ❑ Reduce broad permissions while meeting business collaboration requirements.
  - ❑ Rapidly isolate compromised computers using [Defender for Endpoint](#).

Situation
Oh, no! They've escalated privileges!
Mitigation
Minimize the financial leverage the attacker has on your organization through tight permissions, encryption, and immutable offline backups.
Mitigation success
It costs less for your organization to recover from an attack than to pay the ransom.

---

#### Ransomable assets

#### Rapidly protect against ransomware and extortion

Get the details on how to plan and implement the three layers of protection and mitigation against ransomware.

For additional guidance, visit aka.ms/ransomware. Date of last update: August 2021. © 2021 Microsoft Corporation. All rights reserved.

## Additional ransomware resources

Key information from Microsoft:

- [The growing threat of ransomware](#), Microsoft On the Issues blog post on July 20, 2021
- [Rapidly protect against ransomware and extortion](#)
- [2021 Microsoft Digital Defense Report](#) (see pages 10-19)
- [Ransomware: A pervasive and ongoing threat](#) threat analytics report in the Microsoft 365 Defender portal
- [Microsoft's Detection and Response Team \(DART\) ransomware approach and best practices and case study](#)

Microsoft 365:

- [Deploy ransomware protection for your Microsoft 365 tenant](#)
- [Maximize Ransomware Resiliency with Azure and Microsoft 365](#)
- [Recover from a ransomware attack](#)
- [Malware and ransomware protection](#)

- [Protect your Windows 10 PC from ransomware](#)
- [Handling ransomware in SharePoint Online](#)
- [Threat analytics reports for ransomware](#) in the Microsoft 365 Defender portal

Microsoft 365 Defender:

[Find ransomware with advanced hunting](#)

Microsoft Defender for Cloud Apps:

[Create anomaly detection policies in Defender for Cloud Apps](#)

Microsoft Azure:

Microsoft Security team blog posts:

- [3 steps to prevent and recover from ransomware \(September 2021\)](#)
- [A guide to combatting human-operated ransomware: Part 1 \(September 2021\)](#)

Key steps on how Microsoft's Detection and Response Team (DART) conducts ransomware incident investigations.

- [A guide to combatting human-operated ransomware: Part 2 \(September 2021\)](#)

Recommendations and best practices.

- [Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats \(May 2021\)](#)

See the **Ransomware** section.

- [Human-operated ransomware attacks: A preventable disaster \(March 2020\)](#)

Includes attack chain analyses of actual attacks.

- [Ransomware response—to pay or not to pay? \(December 2019\)](#)
- [Norsk Hydro responds to ransomware attack with transparency \(December 2019\)](#)