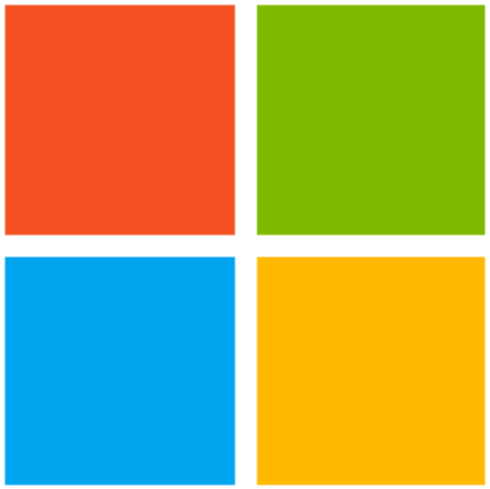
# Human-operated ransomware





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

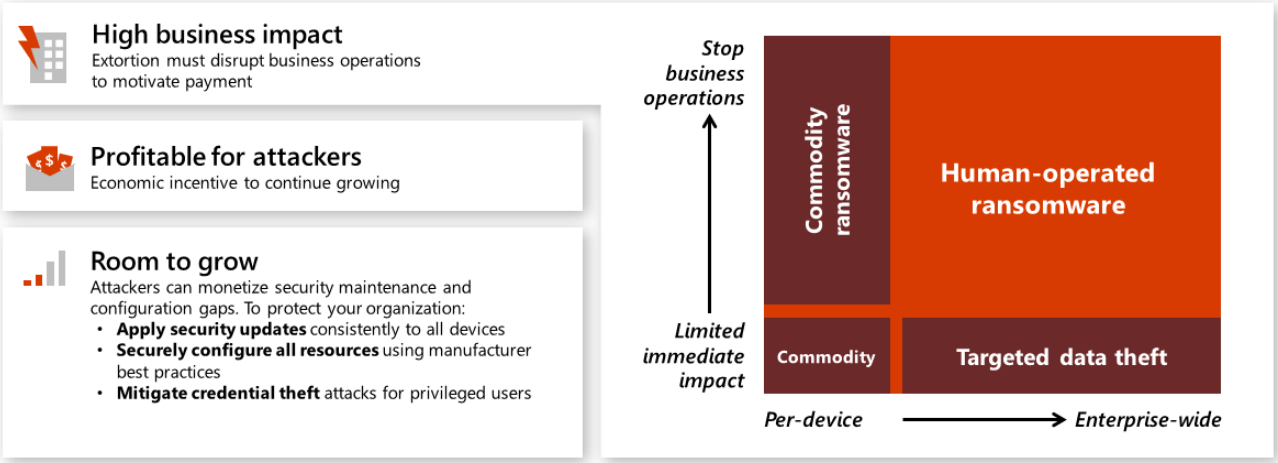
## In this article

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.

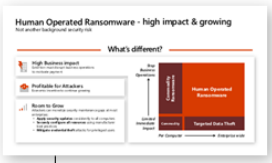
This figure shows how this extortion-based attack that uses maintenance and security configuration gaps and privileged access is growing in impact and likelihood.




## 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:**

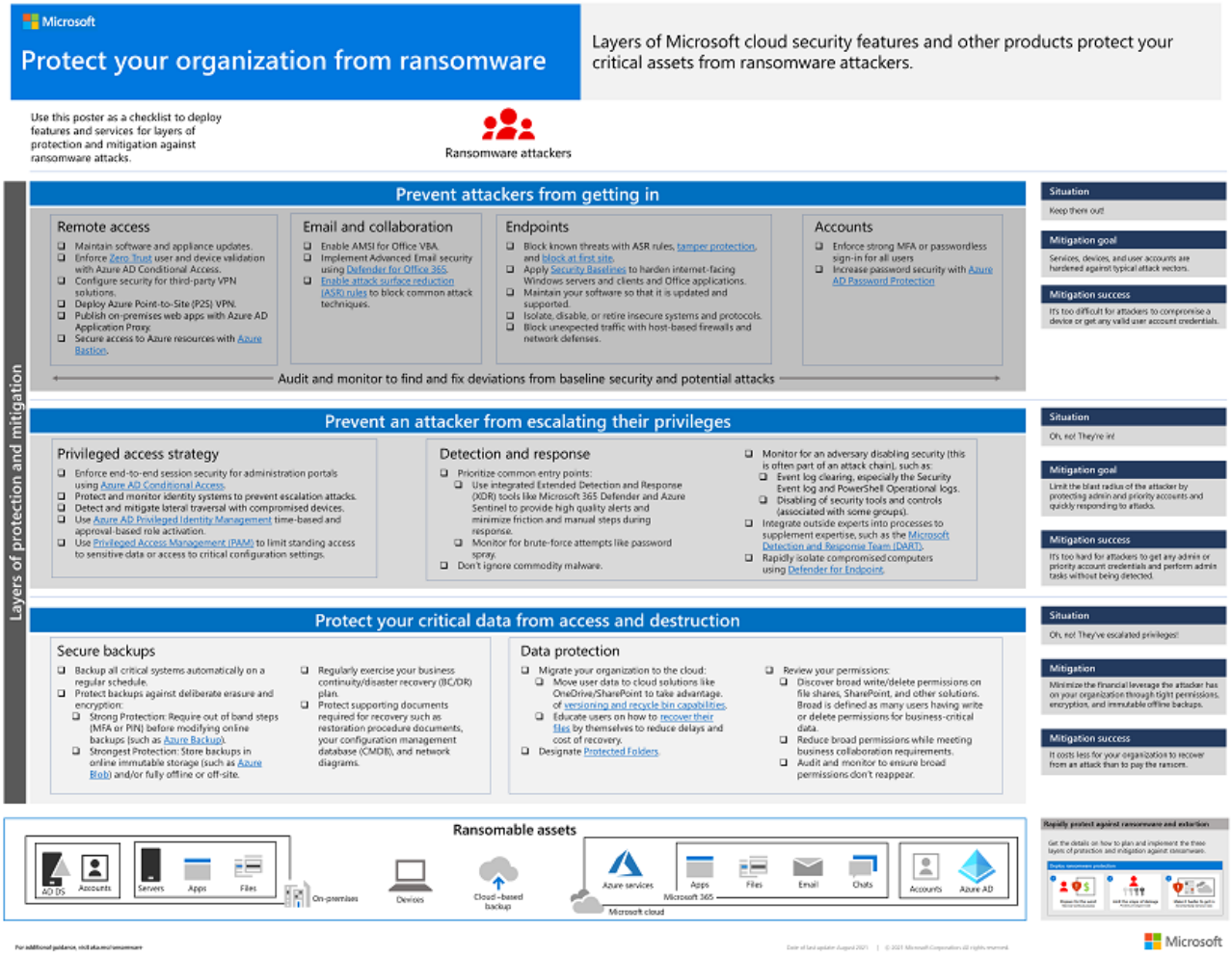
1. ***Restore critical business operations*** – Ensure ability to rapidly restore backups and business processes.
2. ***Protect admins*** – Strengthen privileged access security.
3. ***Entry points*** - Prioritize fastest and most effective mitigation of entry points (continually increase attacker cost/friction).

- 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.




## 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)