

Protect your organization from ransomware

What is ransomware?

Ransomware is a type of cyber threat in which attackers exploit a victim's data or critical infrastructure and demand monetary ransom. In recent years, ransomware attacks have become more common and increasingly sophisticated—exploding into a full-blown underground economy. Cybercriminals are economically motivated to continue ransomware attacks, as many victims, desperate to get their data back, simply pay the ransom. What's more, the ransomware economy has given rise to more malicious actors offering tools and expertise.

Impacts include:

- Business disruption
- Reputational damage
- Financial loss
- Loss of data

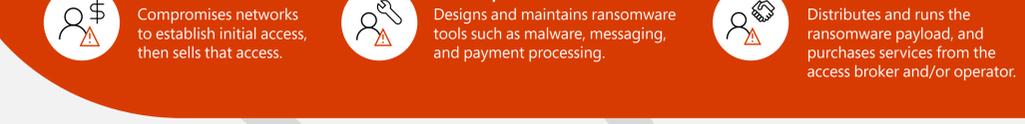
Microsoft security researchers have tracked a 130.4% increase in organizations that have encountered ransomware over the last year.

The underground ransomware economy

Criminals have realized how lucrative ransomware is and have created an entire underground economy to sell their expertise as ransomware-as-a-service. Operators typically charge a monthly fee to affiliates (or customers) and have a profit-sharing model that drives up ransomware prices.

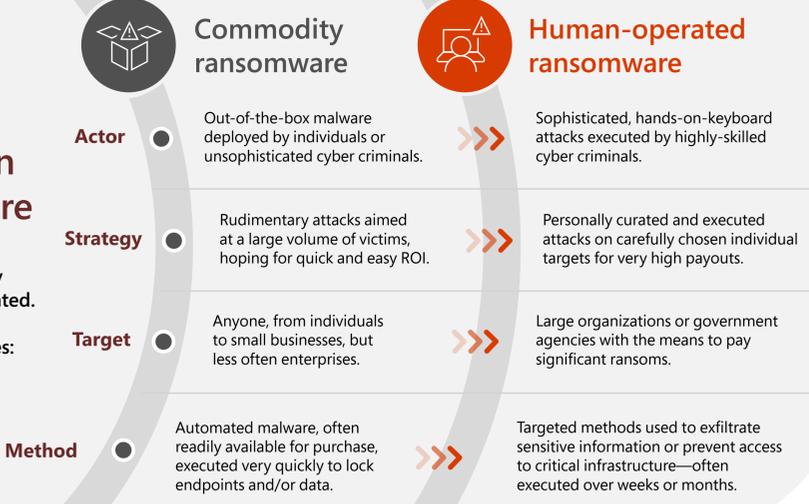
For example:

DarkSide ransomware operators take a 25% cut of the ransom for amounts below \$500,000 but only take a 10% cut for ransoms above \$5,000,000.



The evolution of ransomware

Ransomware evolves quickly, and is constantly growing more sophisticated. Today, ransomware falls into two major categories:



The phases of a ransomware attack

When developing a mitigation strategy, take into account every stage of ransomware attacks.

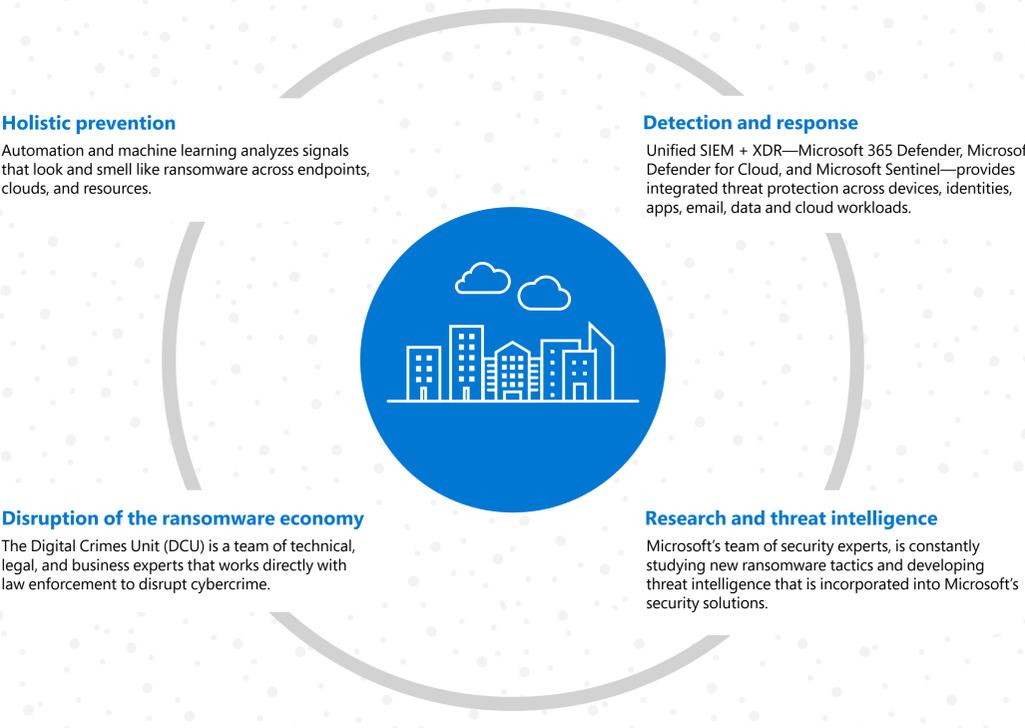


Best practices

- Build a security culture**: Assume breach and adopt zero trust. Build resiliency with regular training and strong processes that empower people to make the right decisions.
- Remediate a recovery plan**: Prepare a recovery plan with solutions that work holistically. Deploy data backup capabilities that let you resume operations as quickly as possible.
- Stop ransomware in its tracks**: Invest in ransomware prevention with comprehensive solutions that work together and with your environment to block ransomware before it harms your business.

How Microsoft disrupts ransomware

Ransomware is more than isolated incidents at specific organizations—it's an entire industry. We need to fight it on every front: in each organization, in ransomware infrastructure, in courtrooms, and in research.



Ready to learn more?

- Microsoft 365 Defender**: Secure your end-user identities, including cloud identities, endpoints, cloud apps, and email and documents. [Learn more >>](#)
- Microsoft Defender for Cloud**: Protect your multi-cloud and hybrid cloud workloads including servers, storage, databases, containers, and more. [Learn more >>](#)
- Microsoft Sentinel**: Get intelligent security analytics including your entire enterprise, including all your security solutions, with cloud-native SIEM. [Learn more >>](#)

Contact SCHNEIDER IT MANAGEMENT

Get free consultancy on your Microsoft Security needs.