Microsoft Security

Three ways to protect yourself from ransomware

Modern ransomware defense requires a lot more than just setting up detection measures.

Ransomware attackers extort victims by breaking into their systems and threatening the disruption of business operations and/or destruction of access to critical data and systems. The attacks can be devastating, and the criminals behind them grow bolder and more sophisticated every day.

Effective defense against today's more sinister and effective human-operated ransomware requires more than just detection measures. To protect against ransomware, IT security teams and security operations centers (SOC) must become less attractive to criminals.

Here are three ransomware protection best practices you can start implementing today:

1

Prepare to defend and recover

Adopt an internal culture of Zero Trust, with assumed breach, while deploying a system of data recovery, backup, and secure access.

The Zero Trust approach

In a Zero Trust environment you must never trust and always verify. You must fully authenticate, authorize, and encrypt every access request before access is granted.

Verify explicitly

Always authenticate and authorize based on all data available including the user, the device, the location, the service, the data, and the network.

Limit user access

Use the principle of least privilege to limit a user's access to what is required to complete a given task in a predetermined amount of time on an as-needed basis.

Assume breach

Embrace a security culture that acts as though cyberattacks are actively occurring. Constantly monitor your environment so you can protect against threats in real time.

The six dimensions of Zero Trust security

1. **Identities** — Verify users with multi-factor authentication protocols before granting access to resources.
2. **Devices** — Make sure only managed and compliant devices are allowed to connect.
3. **Data** — Protect data from accidental and malicious leaks.
4. **Apps** — Harden application security to reduce risks.
5. **Infrastructure** — Keep private data centers and public cloud infrastructures secured.
6. **Networks** — Constantly assess your security posture and take action when threats are detected.

Protect your critical data from unauthorized access and destruction

Secure Backups

- Back up all critical systems automatically on a regular schedule.
- Protect backups against deliberate erasure and encryption.
- 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 and teach users how to recover their own files to reduce delays and recovery costs.
- Designate Protected Folders.
- Eliminate broad* write/delete permissions for business-critical data and take steps to make sure broad permissions don't reappear.

* In this context, broad means permission has been granted to many users.

2

Protect identities from compromise

Minimize the potential for credential theft and lateral movement, where attackers attempt to find cloud admin privileges, with the implementation of a privileged access strategy should an attacker gain entry.

Safeguarding network credentials

Ransomware shakedowns are impossible without access to a network. To an attacker, network credentials are more important than any other aspect of the attack process—even the use of malware itself.

The first step in your ransomware defense plan should be a comprehensive audit of your organization's network credentials.

Once you understand your level of exposure, you can also use tools like BloodHound to identify and close possible attack paths.

Preventing lateral movement

Lateral movement is the technique attackers use to evade detection while searching for assets to exfiltrate or destroy. Because lateral movement resembles benign network behavior, it can be difficult to detect.

You can limit lateral movement opportunities by running services as a Local System, which allows applications to maintain high privileges locally while preventing attackers from using them. You can also randomize Local Administrator passwords to eliminate the chance of attackers exploiting local accounts with shared passwords.

The five pillars of a privileged access strategy

1. Enforcing end-to-end session security for administration portals.
2. Protecting and monitoring identity systems to prevent escalation attacks.
3. Detecting and mitigating lateral movement among compromised devices.
4. Insisting on time-based and approval-based role activations.
5. Limiting standing access to sensitive data or access to critical configuration settings.

3

Prevent, detect, and respond to threats

Defend against threats across all workloads by leveraging comprehensive prevention, detection, and response capabilities with integrated security information and event management (SIEM) and extended detection and response (XDR) capabilities.

Typical attack vectors

Remote Access

When attackers target remote access solutions (RDP, VDI, VPN, etc.) to enter an environment and run ongoing operations to damage internal resources.

Email & Collaboration

When attackers attempt to enter an environment by convincing users to run malicious code attached to an email or file-sharing service.

Endpoints

When attackers target internet-exposed endpoints as a way to access an organization's assets.

Accounts

When attackers use stolen access credentials—usernames and passwords—to gain access to an environment.

Help prevent attackers from getting in

Remote Access

- Maintain software and appliance updates
- Enforce Zero Trust user and device validation
- Configure security for third-party VPN solutions
- Publish on-premises web apps

Email & Collaboration

- Implement advanced email security
- Enable attack surface reduction rules to block common attack techniques
- Scan attachments for macro-based threats

Endpoints

- Block known threats with attack surface reduction rules
- Maintain your software so that it is updated and supported
- Isolate, disable, or retire insecure systems and protocols
- Block unexpected traffic with host-based firewalls and network defenses

Accounts

- Enforce strong multi-factor authentication (MFA) or passwordless sign-on for all users
- Increase password security

Detection and response

Maintain constant vigilance
Use integrated SIEM and XDR to provide high quality alerts and minimize friction and manual steps during response.

Batten down legacy systems
Older systems lacking security controls like antivirus and endpoint detection and response solutions can allow attackers to perform the entire ransomware and exfiltration attack chain from a single system.

If it's not possible to configure your security tools to the legacy system, then you must isolate the system either physically (through a firewall) or logically (by removing credential overlap with other systems).

Don't ignore commodity malware
Classic automated ransomware may lack the sophistication of hands-on-keyboard attacks, but that doesn't make it any less dangerous.

Watch out for adversary disabling security
Monitor your environment for adversary disabling security (often part of an attack chain) like event log clearing—especially the Security Event log and PowerShell Operational logs—and the disabling of security tools and controls (associated with some groups).

Learn more on how to protect yourself from ransomware.

To get the latest news from Microsoft Security, go to https://www.microsoft.com/en-us/security/business/security-insider/.

Share this infographic

Microsoft