Three Ways to Protect Yourself from Ransomware

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

1 PREPARE TO DEFEND AND RECOVER

Zero Trust Approach

Verify Explicitly

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

Six Dimensions of Zero Trust Security

IDENTITIES
Verify users with multi-factor authentication protocols before granting access to resources

DEVICES
Make sure only managed and compliant devices are allowed to connect

DATA
Protect data from accidental and malicious leaks

APPS
Harden application security to reduce risks

INFRASTRUCTURE
Keep private data centers and public cloud infrastructures secured

NETWORKS
Constantly assess your security posture and take action when threats are detected

Protect 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

2 PROTECT ENTITIES FROM COMPROMISE

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 ransomeware 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 exiltrate 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

Five Pillars of 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

Typical Attack Vectors and How to Prevent Attacks

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

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

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

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

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

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

ACCOUNTS
When attackers use stolen access credentials-usernames and passwords-to gain access to an environment

1. Enforce strong multi-factor authentication (MFA) or passwordless sign-on for all users

Detection and Response

Maintain Constant Vigilance

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

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

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)

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)

About Armor

Armor is a global cybersecurity company. As a trusted partner to more than 1,500 firms in over 40 countries, Armor offers cybersecurity and compliance consulting, professional services, and managed services. We provide unparalleled insight into threats and help you respond quickly and effectively.

Contact Us

Request a Free Cyber Health Check

ARMOR®

WWW.ARMOR.COM