Three ways to protect yourself from ransomware

Modern ransomware defense

Don't ignore commodity malware or older systems lacking security controls. Three ways to protect against ransomware:

Prepare to defend and recover

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

Subsegmenting network

Subsegmenting the network prevents attackers from moving laterally between systems.

Protecting and monitoring identity systems to prevent escalation attacks.

Adopt an internal culture of零信任security.

Prepare to defend and recover

Be prepared to defend and recover from a ransomware attack.

Secure Backups

Protect backups against unauthorized access and destruction.

RDP, VDI, and appliance updates

Maintain your network defenses and appliances so that they are updated and supported.

Isolate, disable, and block known threats

Isolate, disable, and block known threats.

Remote Access

Help prevent attackers from getting into your organization's assets.

Accounts

Increase password and multi-factor authentication requirements.

Email & Attachments

Scan attachments for malicious content.

Batten down legacy systems

Don't ignore commodity malware or older systems lacking security controls.

Embrace a security culture

Assume breach and prepare to defend and recover.

Verify explicitly

In a Zero Trust environment you must never trust and always verify.

Verify explicitly

Limit user access and authorization based on all data and context.

In a Zero Trust environment you must never trust and always verify.

Prepare to defend and recover

Be prepared to defend and recover from a ransomware attack.

Verify explicitly

In a Zero Trust environment you must never trust and always verify.

Batten down legacy systems

Don't ignore commodity malware or older systems lacking security controls.

Embrace a security culture

Assume breach and prepare to defend and recover.