Breaking the Ransomware Kill Chain

Five steps to block lateral movement

Ransomware doesn't spread by breaching a single machine or device. Cybercriminals use this strain of malware to encrypt as much of a network as possible and ensure victims pay the ransom.

Every 2 seconds

By 2031, ransomware is expected to attack a business, consumer, or device every 2 seconds.

Cybersecurity Ventures Ransomware Market Report

Are you confident in your existing network security?

If you still rely on legacy firewalls for segmentation, you can't stop ransomware from spreading across your network and locking you out of critical applications and infrastructure.

The ransomware kill chain

1. **Initial foothold** — (Spear) Phishing or vulnerable services
2. **Lateral movement** — Spread across the network for maximum impact
3. **Exfiltration** — Find and steal valuable data
4. **Encryption** — PKI for encryption to prevent cracking
5. **Ransom note** — Wallpaper, email, ransom .txt file, etc.
6. **Impact** — Data, financial, brand, etc.

Breaches are inevitable

You need a security solution that detects threats in east-west data center traffic and blocks lateral movement.

Break the chain

Prepare by identifying every application and asset running in your IT environment

Prevent by creating rules to block common ransomware propagation techniques

Detect by receiving alerts about any attempts to gain access to segmented applications and backups

Remediate by initiating thread containment and quarantine measures when an attack is detected

Recover with visualization capabilities that support phased recovery strategies

In 2022, ransomware attacks rose almost 13%, an increase as big as the past five years combined.

Verizon 2022 Data Breach Investigations Report

If you're not prepared to defend against more frequent attacks and more costly ransom demands, it's time to incorporate segmentation and visibility into your defense strategy.

Learn more

 | Support | Published 05/23