THE WEAK LINK IN YOUR KILL CHAIN - LATERAL MOVEMENT

Detect and stop malicious east-west traffic

Strong perimeter-focused network security is essential to any successful security strategy. Stopping an intrusion or malware at the edge of the network is critical. This shouldn't be a surprise to anyone however many organizations stop here – they miss the concept that perimeter-focused protection is ill-equipped to stop today's targeted attacks and advanced threats. Today's attackers are skilled and understand the security tools you are using to protect your network. They use evasion tactics to bypass even the best perimeter defenses. Once inside the network, perimeter-focused security has no visibility to the attack and is oblivious to its existence. The threat is free to move laterally across the network with little chance of being detected.

You need counter measures to ensure that malicious activity moving across your network from infected machines is detected and dealt with appropriately. Trend Micro™ Deep Discovery™ and TippingPoint solutions will work together to detect and prevent lateral movement.

Deep Discovery will:

- Inspect network traffic between client networks and critical server networks
- Receive alerts on Lateral Movement activities
- View Lateral Movement alerts alongside alerts from other attack phases

TippingPoint will:

- Deploy inline between client networks and critical server networks
- Receive alerts on attempted and thwarted Lateral Movement activities
- Leverage configuration options to easily go from detection to prevention

Monitoring lateral movement across protocols like SMB, RDP, SNMP, IRC is critical. If you don't have tool that monitors these protocols you could be blind to an existing attack. On average, a threat will go several months undetected due to the perimeter-focused security strategy. Once the threat gets into the network there aren't any monitoring this traffic, because the assumption is that the perimeter tools blocked all the attacks. Deep Discovery is designed to sit off a SPAN or TAP port so that it can monitor not only inbound and outbound traffic but also traffic moving across the network monitoring over 100 protocols and all ports. This broad visibility will help prevent undetected malware from moving freely across the network. Deep Discovery will share its findings with the IPS to provide real-time enforcement and remediation.

Trend Micro TippingPoint and Deep Discovery solutions combine to provide Integrated Advanced Threat Prevention giving you:

- Operational Simplicity
- Preemptive Threat Prevention
- Threat Insight and Prioritization
- Real-Time Enforcement and Remediation

Trend Micro™ Deep Discovery
100%
Breach Detection Rate
- 2017 -
NSS LABS
RECOMMENDED
RECOMMENDED
4 years in a row

Trend Micro™ TippingPoint®
RECOMMENDED
99.6% Security Effectiveness
NSS LABS
RECOMMENDED
NSS Labs 2017
NGIPS Group Test

Powered by XGen™ security

POWERED BY XGen™ SECURITY

Trend Micro products and solutions are powered by XGen™ security, a smart, optimized and connected security approach.

TREND MICRO™

Securing Your Journey to the Cloud