Trend Micro

NETWORK DEFENSE

Go Beyond the Known and Unknown

Today's more connected world and changing IT landscape is extending your enterprise network as the adoption of virtualization and cloud technologies grows, and high performance requirements transcend the capabilities of traditional network perimeter defenses. In addition to riskier user behavior and more sophisticated threats including ransomware and zero-day attacks, the increase of connected internet of things (IoT) and industrial IoT devices poses a unique security challenge for enterprises who may find that network-based security is their only protection for these devices for which endpoint security cannot be applied.

With a lack of automation, visibility, operational efficiency, and qualified staff to deal with critical threats, traditional defenses and disparate single-technology solutions are insufficient to tackle the massive volume and variety of threats you are facing.

Those threats that you are facing can be simplified into three classifications; **known, unknown, and undisclosed**.

Known vulnerabilities are known to the public and to security tools. These vulnerabilities or threats are added to reputation databases, addressed by physical and virtual patches, have security pattern files written for them, or have exploit signatures created to block them. Even though vulnerabilities are known, many still get through—usually through unpatched software. "Through 2020, 99 percent of the vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year."* Limited resources to implement patches and end-of-life systems are the major reasons why systems remain unpatched.

* Source: "Cyber Risk Report 2016" Hewlett Packard Enterprise February 2016

Heartbleed is a serious vulnerability in the popular OpenSSL cryptographic software library which allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the internet. In 2017, it was reported that around 200,000 unpatched systems were still susceptible to the Heartbleed vulnerability, which has been around since April 2014, when it originally affected two thirds of the world's web servers.*

*Source: The Register, "It's 2017 and 200,000 services still have unpatched Heartbleeds"

Unknown threats are often designed to impact a single system or a small group of hosts. These targeted attacks often include a multi-vector attack consisting of emails, links, downloads, lateral movement, etc. In 2015, an RSA employee opened the Excel attachment from an email in a junk folder, which contained a threat. This threat opened a back door into Adobe Flash, and through lateral movement within the network, the attacker was able to target the SecurID two-factor authentication product.*

*Source: Bank Info Security

Unknown threats have never before been seen and are usually created to specifically target an individual or enterprise. These targeted attacks and advanced threats are customized to evade your conventional security defenses, and remain hidden while stealing your sensitive data or encrypting critical data until ransom demands are met.

Undisclosed vulnerabilities are a hybrid between known and unknown. These vulnerabilities are usually known by some security researchers and the impacted software vendors. Until software is patched, enterprises are at risk of threat actors exploiting vulnerabilities to gain access or launch attacks.

A critical flaw in the VertX and Edge lines of door controllers from HID Global was found in 2015 by a researcher, who reported it to a bug bounty program. This vulnerability allowed remote attackers to execute arbitrary code on vulnerable installations, which would give them the ability to execute code with root privileges. While the vulnerability was known by a few and unknown to all others, many enterprise networks who used the HID Global door controllers were at risk.*

*Source: Trend Micro Simply Security Blog. "Let Me Get That Door for You: Remote Root Vulnerability in HID Door Controllers"

SMART. OPTIMIZED. CONNECTED.

Today's next-generation intrusion prevention solutions (IPS) are ineffective against many advanced threats, leaving you overwhelmed as you manage risk and recover from attacks. Originally designed for physical, on premise networks, they can increase your exposure to risk with inconsistent security in your cloud environment. A lack of automation and integration with other security components can also leave you with a slow and siloed response across security teams and tools. Only complete visibility into all network traffic and activity, and a layered connected threat defense will keep you ahead of today's threats that either ransom or compromise sensitive data, communications, and/or intellectual property.

Trend Micro™ Network Defense, powered by XGen™ security, goes beyond next-gen IPS to provide a blend of cross-generational techniques that apply the right technology at the right time to deliver integrated detection and prevention of known, unknown, and undisclosed threats. XGen security protects your network with a **smart**, **optimized**, and **connected** security technology approach.

Smarter Protection

Network Defense solutions deliver faster time to protection against known, unknown, and undisclosed threats. Trend Micro can protect against known vulnerabilities and all potential attack permutations inline at wire speed with minimal false positives. With an average of ***61 days*** protection ahead of a vendor patch, Trend Micro protects against undisclosed vulnerabilities through exclusive access to vulnerability information from the Zero Day Initiative™, the world's largest bug bounty program. Trend Micro also leverages patented machine learning techniques to identify, analyze, block, and convert unknown threats or suspicious objects into known threats moving inbound, outbound, or laterally across the network. By mimicking an enterprise's corporate desktop image, Trend Micro can trick malware into fully executing in a custom sandbox for complete malware analysis, including payload and command and control (C&C) communications.

Optimized for Today's Dynamic Environment

Network Defense solutions deliver high performance and automated protection that fits your hybrid environment. Trend Micro provides unparalleled performance in a small physical footprint for large data centers and high capacity enterprise networks, delivering up to 120 Gbps inspection throughput with low latency. Enterprises can secure their cloud environments with a host-based IPS solution that integrates with major cloud and container platforms and applies shared intelligence leveraged across Trend Micro Network Defense solutions. With the growing number of industrial internet of things (IIoT) endpoints on the network not designed with security in mind, Trend Micro can detect and block specific traffic protocols and software vulnerabilities unique to IIoT devices and environments at the network level when endpoint security measures cannot be applied.

Automated and Connected

Network Defense solutions are connected through real-time sharing of threat intelligence, centralized threat insights, and automated remediation. Trend Micro™ Connected Threat Defense™ provides threat information that's shared across all Trend Micro solutions and any other complementary third-party security and incident response tools for coordinated policy optimization. Our threat insights provide centralized visibility on critical threat information to help enterprises prioritize response measures by quickly understanding the threats impacting their network and identifying those that need immediate attention. Network Defense threat intelligence is fueled by the Trend Micro™ Smart Protection Network™ that mines data around the clock and across the globe to ensure that your network is always protected.

Trend Micro™ TippingPoint™ – Uses a combination of technologies such as deep packet inspection, threat reputation and machine learning to detect and block known threats at wire speed.

Trend Micro™ Deep Discovery™ – Detects unknown threats moving inbound, outbound, or laterally across the network by monitoring all ports and over 100 protocols, turning the unknown into known and shares the threat information with a host of security tools including TippingPoint.

Zero Day initiative – An independent organization of over 3,000 security researchers discovering vulnerabilities in operating systems and software used by business and individuals around the world before they can be exploited.

DVLabs – Provides cutting-edge threat analysis and security filters that cover an entire vulnerability providing preemptive threat protection against undisclosed vulnerabilities via the TippingPoint NGIPS.

TREND MICRO™

Securing Your Connected World