A Trend Micro White Paper | **May 2018**

GO BEYOND NEXT-GEN IPS

» How Trend Micro™ XGen™ network security delivers smart, optimized and connected enterprise threat prevention

In a constantly evolving network security landscape, the decade-old next-generation intrusion prevention system (next-gen IPS) suddenly doesn't look "next-gen" any more. This white paper explains why enterprises can no longer solely rely on a next-gen IPS to protect their networks. It also explores how Trend Micro can help enterprises go beyond next-gen IPS with XGen™ network security: an approach that offers smarter protection optimized for today's hybrid environments and is connected with a broad range of security solutions to deliver a greater level of defense in depth.

CONTENTS

When "next-gen" becomes out of date 3

Trend Micro goes beyond next-gen IPS 3

Smarter protection 4

Protection against undisclosed vulnerabilities 4

Custom sandbox analysis 5

Lateral movement detection 5

Machine learning 5

Optimized for today's dynamic environment 5

High-Performance hardware 5

Host-Based intrusion prevention for the cloud 5

Industrial IoT traffic protection 6

Automated and connected 6

Connected threat defense 6

Visibility and prioritization 7

Actionable threat intelligence 7

'X' marks the spot 8

WHEN “NEXT-GEN” BECOMES OUT OF DATE

Organizations of all kinds have relied on next-gen IPS to detect and block threats at wire speed, making decisions on whether traffic is malicious or benign in-line and in real time. But with the first next-gen IPS arriving on the scene more than a decade ago, at what point does “next generation” become “current generation” — or even “last generation”?

That moment may have already arrived. There are four key reasons why the typical next-gen IPS is no longer enough to protect the enterprise network:

1. The network is everywhere.
A next-gen IPS is built for physical, on-premises networks. However, with more data going to more places — data centers, branch offices and, most importantly, the cloud — the traditional ‘boundary’ of the enterprise network has eroded to the point that that strategy of relying solely on perimeter-based defenses has become unsustainable.

2. More endpoints means more exposure to risk.
This expanded network also includes a growing number of Internet of Things (IoT) and industrial IoT (IIoT) devices for inventory management, fleet management and other applications. It’s difficult to apply endpoint security to these devices, making it necessary to protect them at the network level — a challenge when it is unclear where the enterprise network ends.

At the same time, employees want to use their preferred applications, devices and services — not necessarily those favored by the enterprise. This ‘consumerization’ of IT makes it increasingly difficult for enterprise IT resources to maintain control over user activities. It also provides hackers with a lot more entry points (which are often unprotected) through which they can breach and establish a foothold within the enterprise network.

3. The threats facing enterprises are more complex.
On its own, the typical next-gen IPS has proven largely ineffective against many of the most advanced threats, which are using sophisticated evasion techniques to bypass even the best defenses along the network’s edge. According to data gathered during 330 real-world Trend Micro proof-of-concept deployments in 2016–17, nearly every organization (97 percent) had malware and 90 percent had active command-and-control traffic in their networks.

As most attacks are now multi-vector, no single safeguard can possibly deliver 100-percent effectiveness. This is especially true at the perimeter, where security is often sacrificed for performance. And if the enterprise is not monitoring traffic moving laterally across its network, threats can hide for several months before being detected.

4. Security teams are stretched thin.
Although enterprise IT budgets have grown, security budgets have not. Which means, while enterprises are purchasing more devices and infrastructure, they don’t have the resources to protect them. They lack enough qualified staff to deal with new threats as they arise — and with skills in short supply, security teams struggle to stay on top of threats they already face. And with the standard next-gen IPS lacking any sort of integration with other security tools to provide network-wide visibility into threats or automated response measures, the end result is a slow, siloed response by overtaxed and understaffed security teams.

Trend Micro goes beyond next-gen IPS

Enterprises wanting to defend against the full range of threats need to look beyond their next-gen IPS. Trend Micro XGen™ network security approach provides a blend of cross-generational advanced threat prevention tools and techniques to ensure the right security technology can be applied at the right place and the right time to stop known, unknown and undisclosed threats.

With XGen™ network security, enterprises benefit from smarter protection that is optimized for today’s hybrid environments — automated and connected with a wide range of security products and industry-leading threat intelligence to deliver a more thorough, layered approach to security.

SMARTER PROTECTION

Because 90 percent of malware targets existing vulnerabilities, the filters found in a next-gen IPS are invaluable when it comes to rapidly detecting, analyzing and protecting against *known* threats like WannaCry ransomware. Trend Micro TippingPoint® solution, for example, ships with recommended settings for its filters that cover a broad range of existing vulnerabilities.

But in the face of unknown and undisclosed threats, a smarter, more comprehensive approach is required. Trend Micro XGen™ network security leverages a broad range of advanced detection and protection techniques, including custom sandbox analysis, lateral movement detection and machine learning — all backed by world leading threat and vulnerability research. In doing so, it offers enterprises a much faster time to protection against threats of all kinds.

Protection against undisclosed vulnerabilities

Trend Micro XGen™ network security products are powered by the vulnerability research and threat analysis of Trend Micro research, which includes the Zero Day Initiative (ZDI): the largest vendor-agnostic bug bounty program in the world.

The ZDI rewards independent security researchers for identifying and disclosing vulnerabilities in operating systems and software before they can be exploited. Through the ZDI, Trend Micro gains exclusive insights into the latest threats — then works closely with software vendors to ensure fast, timely patching of vulnerabilities before they become known "in the wild".

Between the time an undisclosed threat is discovered and when the vendor releases a patch for it, enterprises are at risk. That's why Trend Micro researchers take what has been learned by the ZDI to quickly develop and distribute security filters that cover an entire vulnerability (not just specific exploits), ensuring Trend Micro customers are protected well before the vendor's patch is made available — with filters distributed an average of 72 days ahead of the vendor patch in 2017.

The ZDI has been the leading global organization in vulnerability research and discovery since 2007. It is a top provider of vulnerabilities to organizations like Adobe, Microsoft and the U.S. Industrial Control Systems Cyber Emergency Response Team — and it discovered 66.3 percent of all verified vulnerabilities in 2017, more than any other bug bounty program combined. Without the ZDI, many vulnerabilities would continue to remain behind closed doors or be sold to the black market and used for nefarious purposes

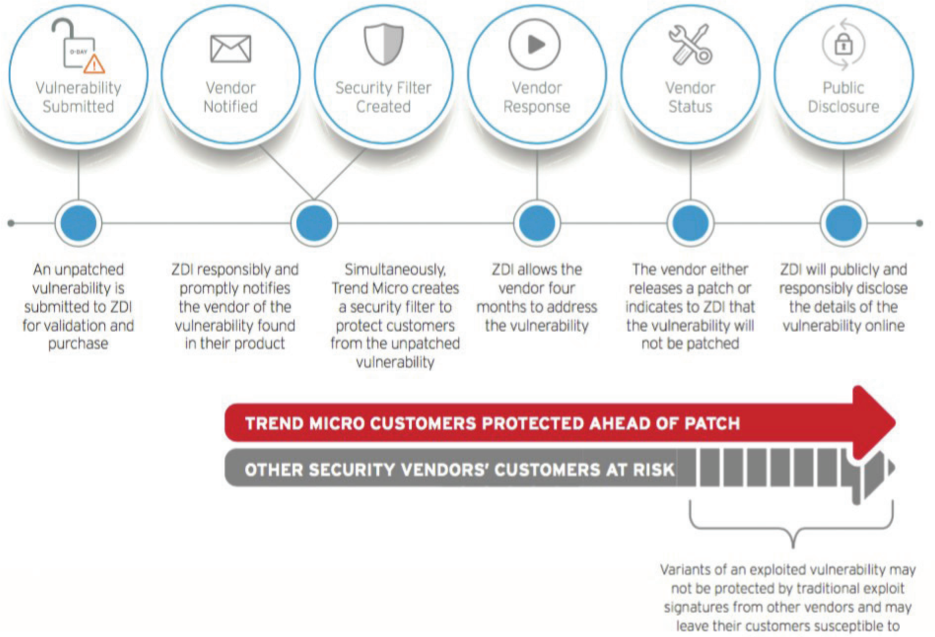
0-DAY
Vulnerability Submitted
Vendor Notified
Security Filter Created
Vendor Response
Vendor Status
Public Disclosure
An unpatched vulnerability is submitted to ZDI for validation and purchase
ZDI responsibly and promptly notifies the vendor of the vulnerability found in their product
Simultaneously, Trend Micro creates a security filter to protect customers from the unpatched vulnerability
ZDI allows the vendor four months to address the vulnerability
The vendor either releases a patch or indicates to ZDI that the vulnerability will not be patched
ZDI will publicly and responsibly disclose the details of the vulnerability online
TREND MICRO CUSTOMERS PROTECTED AHEAD OF PATCH
OTHER SECURITY VENDORS' CUSTOMERS AT RISK
Variants of an exploited vulnerability may not be protected by traditional exploit signatures from other vendors and may leave their customers susceptible to future attack

Figure 1. ZDI bug bounty program helps deliver faster time to protection

Three kinds of threats

Known threats — These are known to the public and security tools. They are added to reputation databases, addressed by physical and virtual patches, have security pattern files written for them, or have exploit filters created to block them. Even though they are known, many still get through via unpatched systems and software. The 2003 SQL Slammer worm, for example, infected 75,000 victims in 10 minutes even though a patch had been released six months earlier.

Unknown threats — These have never been seen before and are usually created to specifically target a single individual or enterprise. They are customized to evade conventional defenses and remain hidden while stealing or encrypting data, often using multiple attack vectors such as emails, links, downloads and lateral movement to open back doors into the network.

Undisclosed threats — A hybrid between known and unknown threats, these are usually known by some security researchers and the affected software vendors, but not the public. Until the software is patched, enterprises are at risk of threat actors exploiting them to gain access or launch attacks. The 2014 POODLE attack, for example, took advantage of a vulnerability in SSL 3.0 that was discovered by threat researchers more than five months before it was first exploited.

[1] Frost & Sullivan, February 2018. *Analysis of the Global Public Vulnerability Research Market, 2017.*

Custom sandbox analysis

Any potential threats or incidents of compromise are sent automatically to a custom sandbox for detonation and analysis. This sandbox uses a precisely tuned virtual image that replicates an organization's real system configurations, drivers, operating systems, installed applications and language versions — tricking malware into executing itself fully and exposing behaviors such as multi-stage downloads and command-and-control communications. This allows security administrators to safely investigate how the malware might compromise systems on the network and determine the severity of the threat so they can prioritize accordingly.

Lateral movement detection

Advanced threats like crypto-ransomware use sophisticated evasion techniques to bypass even the best defenses along the network's edge. Once a threat gets inside the network — perhaps through an unsecured protocol or unprotected device — perimeter-focused security cannot see it and is unaware of its existence, meaning the threat can move laterally across the network with little chance of detection.

Trend Micro's solution keeps an eye on not only the traffic moving in and out of the network, but also the 'east–west' traffic moving across it. By monitoring every port and more than 100 protocols, Trend Micro's solutions provide 360-degree visibility to help prevent undetected malware from spreading within the network and freely accessing critical servers.

Machine learning

With patented machine learning techniques, XGen™ network security solutions go beyond simple whitelists and blacklists, constantly analyzing traffic characteristics to predict whether something will be malicious or not. Statistical models are applied to feature vectors extracted from network data on the wire, with minimal impact on network performance, allowing for real-time decisions to immediately block traffic that emulates both known or unknown malware family characteristics.

Trend Micro TippingPoint solution was the first standalone next-gen IPS to use machine learning to detect and block threats in-line and in real time. Continuous machine learning analysis following malware execution in the custom sandbox also helps improve the enterprise's overall security effectiveness.

OPTIMIZED FOR TODAY'S DYNAMIC ENVIRONMENT

Being able to leverage the latest and most advanced threat detection and prevention techniques is just part of the XGen™ equation. To deliver the best possible results for today's enterprises, Trend Micro solutions are also fully optimized to meet the requirements of hybrid on-premises and cloud IT environments.

High-Performance hardware

As data volumes continue to grow and enterprises consolidate their data centers to cut IT costs, network performance has become a top priority — often at the expense of security. For example, if a next-gen IPS introduces high levels of latency, it can lead to unacceptable response times for end users, affecting transaction speeds, backup times and more. Enterprises need a way to effectively secure their networks without jeopardizing performance. Designed specifically for today's high-capacity enterprise networks and consolidated data centers, Trend Micro TippingPoint solution provides unparalleled performance in a compact physical footprint. It delivers high-speed inspection throughput up to 120 Gbps in a 3U stack form factor with very low latency — less than 40 microseconds — to meet the most demanding performance requirements across all directions of traffic.

Host-Based intrusion prevention for the cloud

Many enterprises are exposed to risk due to a lack of consistent security policies across their on-premises networks and the cloud, often relying solely on the security provided by their cloud providers. But cloud security must be a **shared responsibility between the cloud provider and the enterprise**. While the service provider takes care of the infrastructure of the cloud, it is not responsible for securing the data and applications stored in the cloud. With XGen™ network security, enterprises can secure their cloud environments — and take responsibility for everything in those environments — with a scalable solution that is tightly integrated with a wide range of major cloud and container platforms, including Amazon Web Services, Microsoft Azure, VMware, Google Cloud Platform, IBM Cloud and Docker.

This high level of integration makes it easy for enterprises to apply a broad range of security processes and controls to the cloud, such as application control and integrity monitoring, which are purpose-built and optimized for their specific cloud environments. It also makes it possible to automatically scale protection as more cloud workloads are turned up, without any gaps in coverage. As well as, allowing for shared intelligence to be applied across multiple Trend Micro solutions.

IIoT traffic protection

The majority of IIoT devices were not designed with security in mind. In particular, the supervisory control and data acquisition (SCADA) systems at the heart of much of the world's critical infrastructure — such as power generation and distribution systems — are decades old and were never intended to access public-facing networks. As the number of IIoT endpoints on the network continues to grow, the insecure designs and poor authentication/authorization methods specific to these devices can compromise critical data.

Since endpoint security is difficult or even impossible to implement on these devices (which are too valuable to replace but too old to secure), the network itself is the first and often only line of defense. Trend Micro solutions leverage a library of more than 300 IoT vulnerability rules, enabling them to detect and block specific traffic protocols and software vulnerabilities unique to IIoT devices and environments at the network level.

Dedicated IIoT research

Trend Micro is actively investing in research on IoT/IIoT vulnerabilities, looking at how these devices and the processes they use could be exploited. Areas of research include the vulnerabilities in robotic manufacturing equipment and medical devices, and how attackers can hijack the communication protocols used by drones. Active research is also being done on consumer IoT devices, such as kitchen appliances and smart TVs.

For example, Trend Micro solutions provide comprehensive coverage for all of the standard protocols used by SCADA systems, including DNP3, ICS, Modbus and ICCP. Custom security intelligence can also be developed according to user activities that are unique to a particular SCADA environment (e.g., setting policies to block attempts to raise the temperature of a particular power reactor beyond a certain threshold).

AUTOMATED AND CONNECTED

Finally, Trend Micro is improving network protection through a more integrated and connected approach to network security: one that enables fast and automated protection powered by the real-time sharing of and centralized visibility into the latest threat intelligence and insights.

Connected threat defense

It's one thing to deploy a layered approach to network security. Although, if that involves a number of disparate solutions that can't actually 'talk' to each other, enterprises aren't getting maximum value from their security investments. Regardless of whether they're focused primarily on enterprise networks, endpoints or cloud environments, Trend Micro solutions seamlessly integrate and connect with each other, sharing threat data and intelligence in real time. They also connect with a number of complementary third-party security and incident response tools through open, vendor-agnostic application programming interfaces (APIs) — enabling a much greater degree of automation and coordination among the enterprise's security policies.

At the highest level, this integrated approach means that if a malicious file is found by one security solution, information about it can be quickly and automatically sent to everyone else, to ensure that threat can be blocked going forward. Threat information is also shared with Trend Micro Smart Protection Network™, to update all Trend Micro customers so they can be protected against that same threat.

For example, here's how this approach might handle a suspicious URL or file. When an unknown or suspicious threat is detected as it enters or crosses the network, a copy of that threat is sent to the custom sandbox, where it is detonated and analyzed to determine if it is malicious or not. The threat intelligence obtained through that process (including IP addresses, DNS names, URLs and SHA1 hash values) is sent to the TippingPoint Security Management System (SMS), which automatically sets and distributes policies telling the next-gen IPS and other security solutions to automatically block any current and future breaches or lateral movement by that threat.

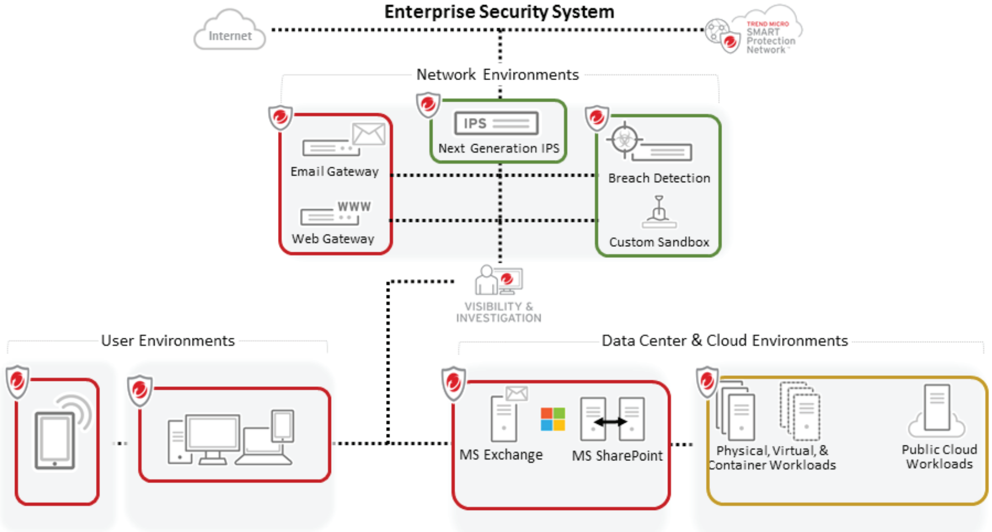

Figure 2. Faster time to protection with Trend Micro Connected Threat Defense

Visibility and prioritization

By aggregating security data from multiple security tools, Trend Micro gives security administrators greater insight into the volume and severity of threats faced by their networks, allowing them to make more informed decisions about potential threats to their infrastructure or data.

Simplified dashboards provide centralized visibility into event and threat data correlated across the network. It can show how many times a specific filter has been fired, for example, or how many users were affected by a specific threat. This enables 'big picture' analysis of traffic statistics and filtered attacks, and provides an at-a-glance overview of critical threats affecting the network to help security administrators prioritize incident response measures.

Trend Micro also delivers an automated response system that allows administrators to specify actions and policies for deployment in response to various security events. This gives them the ability to provide the same level of protection across the entire network, along with the confidence that there are no gaps in the policy updates being pushed out across their deployment.

Actionable threat intelligence

Data and research are essential to keeping enterprises protected against the complex and varied threats they face — and will continue to face. Threat actors never stop and are constantly changing the way they target and attack people and businesses around the world. That's why Trend Micro has invested heavily in its security research capabilities.

Trend Micro research

Beyond the Zero Day Initiative described earlier, the researchers at Trend Micro examine a broad range of areas within the threat and computing landscapes. They continually analyze new malware, malicious URLs and command-and-control locations that could be potentially used in attacks. To help enterprises minimize the risk of being breached (and also how to detect and remediate breaches that have occurred), researchers look at the entire attack chain lifecycle to better understand how hackers are evolving their tools, tactics and procedures. Research is also being conducted on artificial intelligence, machine learning, IoT/IIoT and more.

Trend Micro researchers have investigated many of the world's underground cybercommunities to identify the newest tools and techniques used by attackers and have established active partnerships with law enforcement agencies and cybersecurity organizations (e.g., Interpol, FBI) to assist with investigations and help bring cybercriminals to justice.

Sharing research with the world

The intelligence gathered by Trend Micro about the latest threats and vulnerabilities is shared with customers, partners and the security industry as a whole. Trend Micro regularly issues alerts, blogs and reports that include guidance on how to protect systems or networks that are under attack. And when there are major threats that can have broad repercussions (such as 2017's WannaCry ransomware), Trend Micro will provide free tools to help organizations protect themselves whether they are a Trend Micro customer or not.

Smart Protection Network

Trend Micro Smart Protection Network collects, identifies and delivers the latest security intelligence to Trend Micro products to ensure they can adapt to and defend against current and emerging threats. Continuously mining data from around the world on known good and known bad files, applications and URLs, the Smart Protection Network serves as a massive information source for understanding threat behaviors and driving innovation in Trend Micro technologies.

The Smart Protection Network consists of:

- A global network of hundreds of millions of sensors to collect more threat information in more places — three trillion threat queries each year — including data on files, IPs, URLs, mobile apps, operating system vulnerabilities and more
- Global threat intelligence that analyzes terabytes of data on a daily basis, drawing from a database of nearly one billion known good files to identify 250,000 new, unique threats each day
- Proactive cloud-based protection for half a million businesses around the world, blocking more than 65 billion threats yearly

X' MARKS THE SPOT

In a rapidly changing IT environment, a next-gen IPS alone is no longer enough to meet the complex security needs of today's dynamic enterprise environments. The network boundary now extends well beyond the enterprise perimeter. The growing number of endpoints exposes the enterprise to increasingly sophisticated malware that can remain undetected in the network for months at a time. And enterprise security teams are stretched thin, struggling to stay ahead of the threats they already know about, let alone any new ones that may arise.

Addressing these challenges requires a smart, optimized and connected approach to network security. Drawing on Trend Micro's three decades of experience protecting enterprises against cyber threats, as well as its extensive history of research and innovation, the integrated, cross-generational security solutions that make up the XGen™ approach can provide the intelligence, automation and visibility into inbound, outbound and lateral traffic that enterprises need to defend against the most complex known, unknown and undisclosed threats.

A recognized leader in security

Trend Micro is a:

- Recommended vendor for next-generation intrusion prevention systems (NSS Labs, 2017)
- Recommended vendor for breach detection systems for four consecutive years (NSS Labs, 2017)
- Leader in the 2018 Gartner Magic Quadrant for Intrusion Detection and Prevention Systems
- Leader in Global Vulnerability Research and Discovery since 2007 (Frost & Sullivan)
- Recommended vendor for data center intrusion prevention systems (NSS Labs, 2018)

TREND MICRO™

Securing Your Journey to the Cloud

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1 408.257.2003