Smart, Optimized, Connected

Navigating the evolving threat landscape with a more complete approach to network security

>> A Trend Micro white paper
Contents

How targeted attacks are changing the network security landscape ........................................... 2
  Responding to increasingly complex threats ................................................................................. 4

Smart: A cross-generational approach to network security ......................................................... 5
  Security fueled by market-leading global threat intelligence ..................................................... 6
  Detection techniques that comprise a smart network defense ................................................... 7

Optimized: Full integration with other security solutions ............................................................. 11

Connected: Seamless sharing of threat intelligence ................................................................. 12
  Centralized visibility and control ................................................................................................. 14

Trend Micro: An innovator in network security ............................................................................ 14
HOW TARGETED ATTACKS ARE CHANGING THE NETWORK SECURITY LANDSCAPE

It used to be that cybercriminals would blindly cast a wide net, sending millions of fraudulent emails in the hope that a few people would be tricked into handing over their personal or financial information. As organizations evolved their security infrastructures and the average user became more aware of how and how not to behave online, cybercriminals looking to make a profit soon realized they could no longer rely on crude, random attacks. Today, targeted attacks are the weapon of choice: a far more lucrative tactic that uses malware purpose-built to bypass defenses and penetrate the network of a single organization.

Single-target attacks are not ‘one size fits all’ — they require specialized knowledge and detailed information on the target. They are the result of advance reconnaissance, research and testing, all with the goal of finding the best way to circumvent an organization’s security measures and exploit the vulnerabilities in its software, systems and users. In many cases, this means utilizing a specific user’s personal information (such as their interests, known associates or familiar email addresses) to entice them to follow an email-embedded link, open a weaponized attachment or visit a fake website that can immediately download malicious code. After compromising the user’s system, the code can then spread silently and laterally throughout the enterprise’s network.

This tailored approach makes each targeted attack unique, using unexpected combinations of applications, devices, protocols, ports, command-and-control communications\(^1\), encrypted malware, and zero-day exploits to achieve its objectives. Targeted attacks are also dynamic, able to change their behavior and digital ‘appearance’ during the course of an attack, making it even more difficult for traditional anti-malware defenses to detect them.

It’s not a surprise, then, that many enterprises have already been compromised by targeted malware — and they likely don’t even know it.

---

\(^1\) Command-and-control servers can be used to remotely send malicious commands to a botnet or compromised network of computers. The term originated from the military concept of a commanding officer directing control to his/her forces.

Has your organization been hit?

Of the 264 enterprise networks analyzed during proofs of concept conducted by Trend Micro in 2015–16, we found that:

- 80% had experienced a network-based attack or exploit
- 90% had active command-and-control activity on their network
- 65% had been infected by zero-day or unknown malware
- 17% were being actively breached
Responding to increasingly complex threats
Research sponsored by Trend Micro suggests that 58 percent of surveyed organizations have discovered malware in their networks that went undetected by traditional security solutions. Most of the surveyed organizations also felt certain that other malware was still running undetected on their servers, mobile devices and PCs.²

Even though they know they have been compromised, resource constraints make it impossible for organizations to investigate every possible threat – and even if they could, it is becoming increasingly difficult to definitively determine what is bad and what is good among the traffic passing over their networks. On top of that, with the emergence of targeted ransomware, the time an enterprise has to detect and stop an attack has been reduced to mere seconds: most systems can be encrypted in less than a minute and the time from delivery to open is, on average, just 111 seconds.

With today’s enterprises in the crosshairs of a massive volume and variety of increasingly complex attacks, traditional security measures on their own are not enough. New security capabilities are needed to create an effective defense against these advanced threats, including the ability to monitor network traffic for malicious behavior, rapidly identify and block ‘known bad’ entities as they pass through the network (i.e., before they have a chance to be delivered to a user’s device), and analyze and respond to suspicious payloads.

In addition to the known and unknown threats, enterprises also need to be able to protect themselves against undisclosed threats: unpatched vulnerabilities that are known only by one particular security vendor (typically through its ‘bug bounty’ program) and the affected software vendor. Undisclosed vulnerabilities are considered unknown by all other security vendors and malware writers – and may exist for months before a patch becomes available.

To meet all these requirements, enterprises must employ an approach to network security that is smart, optimized and connected. Such an approach is embodied in Trend Micro’s Network Defense solution powered by XGen™ security, which leverages a unique blend of cross-generational threat protection techniques and market-leading global threat intelligence to detect and mitigate targeted attacks.

SMART: A CROSS-GENERATIONAL APPROACH TO NETWORK SECURITY

No one security technique can possibly protect against every threat, especially with attackers now able to dynamically alter the nature of their attacks to evade detection (whether by changing IP addresses, for example, or by using polymorphic malware that automatically changes form each time it executes). The ability to identify and prevent a broad range of network activity, suspicious payloads and attacker behavior is more important than ever – and the best way to achieve maximum protection is through a multi-layered approach to security that uses a variety of cross-generational techniques to analyze, identify and respond to threats.

![Diagram of network security layers](image)

**Figure 1. Delivering more efficient network security with multi-layered threat protection**

XGen™ security protects against the full range of known, unknown and undisclosed threats by leveraging multiple advanced threat-defense techniques, all working together and building on each other’s strengths to catch the highest possible percentage of malicious elements with minimal false positives. If a malicious file happens to slip through one layer of security, it is
backed up by the capabilities of several more layers of defense, each relying on a different style of protection and detection.

This smarter approach to security also ensures the right technique will be applied at the right time. For instance, Trend Micro’s Network Defense solutions use proven techniques such as network content inspection, intrusion prevention, early zero-day protection, and web and URL filtering to quickly identify known good and known bad data. This frees up the more advanced (and resource-intensive) techniques, such as customized sandboxing and machine learning, to focus on accurately identifying and mitigating any unknown threats in the network. Should a potentially malicious payload make it all the way to the bottom of the ‘funnel’ (as illustrated above), it will have gone through the most extensive analysis possible to ascertain whether it is malicious or not.

**Security fueled by market-leading global threat intelligence**

A cross-generational approach that employs a number of different detection and protection techniques is only half of what makes XGen™ security truly smart. For even greater efficiency and accuracy, those techniques are powered by global, cloud-based threat intelligence from the Trend Micro™ Smart Protection Network™, which continuously mines data from around the world to ensure a constant stream of information on known good and known bad files, applications and URLs.

Using the data collected from its millions of global sensors, the Smart Protection Network first checks anomalies (such as attachments and executable attached code) and newly born domains against reputation management databases and internal Trend Micro threat lists. Next, big-data analytics are applied to threat candidates to determine any suspicious patterns or behaviors – and stamp out an attack before it can infiltrate an organization’s network.

The Smart Protection Network consists of:

- A global network consisting of hundreds of millions of sensors to collect more threat information in more places – 16 billion threat queries daily – including data on files, IP addresses, URLs, mobile apps, operating system vulnerabilities and more
- Global threat intelligence that analyzes hundreds of terabytes of data on a daily basis, drawing from a database of nearly one billion known good files to identify 500,000 new, unique threats each day
- Proactive cloud-based protection to block threats across all of our customers’ networks – as many as 250 million each day – and minimize risk

Through the Smart Protection Network, the solutions powered by XGen™ security can constantly adapt to protect against future attacks, evolving to identify and defeat new ransomware and other unknown threats by automatically sharing threat intelligence among the various security layers.

---

*Smart, Optimized, Connected*
Detection techniques that comprise a smart network defense

XGen™ security applies a blend of cross-generational threat-detection techniques to not only provide the best possible protection against the latest advanced attacks but also to provide the most optimized and connected threat defense. Some of the various detection techniques used by Trend Micro’s Network Defense solutions are described on the following pages.

Network content inspection

Before launching a targeted attack, attackers will typically conduct advance reconnaissance on an enterprise’s network, application and communication protocols to identify the best ways to evade the existing security defenses. The attack will then be tailored to take advantage of the least expected and least monitored points of vulnerability.

In addition, attackers do not use a predictable or predefined subset of network ports. Instead, they exploit an evolving variety of the 65,000+ available network ports to launch and manage their attacks – and as conditions change, they can readily change ports to remain elusive. Any unmonitored port is essentially an unpolicing thoroughfare for an attacker.

For this reason, enterprises need to be able to monitor all inbound, outbound and internal network traffic – as well as any and all devices that are connected to their networks – for suspicious behavior and malicious activity. This lets them rapidly identify and block known bad files and external threats, malicious URLs, outbound communications with command-and-control servers, and more.
The Network Content Inspection Engine — the module at the heart of Trend Micro’s advanced threat-protection platform — monitors all traffic that passes through the network layer, including the headers of and data within network packets, to identify ransomware, targeted attacks and advanced threats anywhere on the network. This monitoring takes place across both physical and virtual network segments as well as all network ports and more than 100 network protocols. By recombining and inspecting files from the different packets within the various network flows (such as torrents, instant messaging and peer-to-peer file sharing), the Network Content Inspection Engine ensures these files are consistent with relevant network protocols and application behaviors, using that information to decide whether they should pass through, be blocked or be redirected.

Intrusion prevention

An intrusion prevention system blocks network-based exploits of known vulnerabilities in popular applications and operating systems. Trend Micro’s TippingPoint Next-Generation Intrusion Prevention System (NGIPS) uses technologies such as deep packet inspection and threat reputation to detect and prevent intrusion by attackers in-line and in real-time.

Early zero-day protection

Between the time an undisclosed threat is discovered and the software vendor releases a patch to address it, companies are at risk. One of the key contributors to the Smart Protection Network is the Zero Day Initiative (ZDI), the leading organization for global vulnerability research and discovery. Through exclusive access to the vulnerability data collected through the ZDI, Trend Micro is able to provide early zero-day coverage for its customers by developing Digital Vaccine® filters for undisclosed vulnerabilities and making them available to NGIPS systems, helping to keep their networks safe ahead of an available patch.

Filtering and reputation

File and web reputation blocks users from accessing compromised or malicious websites by tracking the credibility of web pages and domains. It checks the reputation of each file (including metadata such as prevalence, age and geo-location) against an extensive database in the cloud before permitting user access.

A wide range of advanced detection capabilities

Some additional techniques used by Trend Micro include:

- **Lateral movement detection** - Monitors suspicious traffic moving inbound, outbound and laterally across the network (specifically, between servers). If the traffic is confirmed to be malicious, an NGIPS can then terminate the threat and block all future similar traffic movement.

- **Command-and-control blocking** - Identifies and shuts down endpoint traffic (over any port) that is attempting to connect to or contact a known command-and-control server (such as botnet or targeted attack behaviors).

- **Variant protection** - Looks for obfuscated or polymorphic malware by using fragments of previously seen malware to detect patterns and commonalities among variants.
Mobile application reputation, meanwhile, protects against malicious mobile apps – such as those that have been decompiled and repackaged with harmful code – by comparing resource usage, privacy violations and other behaviors against the known app hashes that have been collected and scanned into the cloud-based Trend Micro Mobile App Reputation Service threat database.

Network content correlation
Fast, easy access to correlated and relevant threat intelligence is also critical to an effective defense. The real-time correlation of events happening in the network with the threat insights available from existing log information, software, gateways and other security solutions makes it possible to analyze all of the facts about the content passing over an organization's network.

For Trend Micro, this means taking local threat intelligence gathered by its range of security products and correlating it with the global threat intelligence in the Smart Protection Network. Drawing on the latest data science techniques, the Smart Protection Network rapidly and accurately collates this massive amount of threat intelligence, and then uses predictive analytics to provide immediate and automatic protection from the multitude of threats.

One of the more important functions of the Smart Protection Network is its ability to learn from its previous actions: patterns of newly identified threats and attack behaviors are maintained in its database, often for years, for use in future analysis. Trends associated with customer type, geolocation, industry and other metadata are identified and included in this historical information.

The Network Content Correlation Engine is the program module that implements the rules or policies for content correlation used by Trend Micro's advanced threat-protection platform. These rules are regularly updated by Trend Micro after analyzing the patterns and trends exhibited by new and modified viruses and malware.

Behavioral analysis
The Network Content Correlation Engine also takes into consideration behavioral analysis, looking for suspicious or unusual behavior as an item interacts with an organization's operating systems, application and scripts – even if that particular item isn't on a blacklist. Consider, for example, a user's machine that is trying to respond to DNS requests or initiate PsExec commands when it has never done so before. While those actions are not necessarily malicious, they may indicate the presence of malware, prompting them to be flagged for further analysis and alerting should they reoccur.

Machine learning
Trend Micro's TippingPoint NGIPS is the first standalone NGIPS to apply machine learning statistical models to feature vectors extracted from network data on the wire to make a real-
time decision on whether network traffic is malicious or benign. This approach helps to better detect advanced malware behavior and communications that are invisible to standard defenses. TippingPoint NGIPS also applies machine learning techniques to detect and block known and unknown malware families that use domain generation algorithms to generate domain names for infected hosts attempting to contact their command-and-control servers.

Customized sandboxing

Perhaps the most deterministic of the ‘smart’ security techniques is customized sandboxing. A sandbox is technology that enables any file (especially those of unknown origin) to be unpacked, tested and examined in a safe, isolated virtual environment before it has a chance to run on a live system. While this process typically happens on an automated basis (based on configurable analysis policies), incident response personnel can also manually submit malware samples for analysis, helping reduce incident investigation times.

Using extensive detection and anti-evasion techniques, the sandbox can effectively identify ransomware, advanced malware, zero-day exploits, and multi-stage downloads resulting from malicious payloads or URLs. To further improve detection rates, the sandbox is also fully customizable, using virtual images to precisely emulate an enterprise’s specific operating system configurations, drivers, installed applications and language versions.

Given that targeted attacks are tailored to an enterprise’s specific computing environment, this customizability is critical. Consider the fact that most other vendors’ sandboxes will test a suspicious file only in a standard image of Windows with English language settings. If a piece of malware is set to execute only in an operating system environment using Portuguese, as an example, the generic English sandbox won’t catch it. Trend Micro’s sandboxes, on the other hand, are not limited to a checklist of standard products and operating system versions, meaning they will be able to identify and mitigate that particular malware before it can execute in its target setting.

Trend Micro’s sandboxes can also use a ‘live mode’ to increase their overall detection rate, allowing for additional information to be gathered on suspicious objects while also making it possible to demonstrate multi-stage threats that would bypass most other sandbox technologies. Live mode connects the internal sandbox to an external internet connection to monitor communications in and out of the sandbox.
OPTIMIZED: FULL INTEGRATION WITH OTHER SECURITY SOLUTIONS

Every network is different — and enterprises can’t be expected to forklift out all of their existing security solutions just to make way for XGen™ security. That’s why the Trend Micro solutions powered by XGen™ security are specifically designed for tight integration and interoperability with the platforms and applications they may already have in place, effectively uniting an enterprise’s entire security infrastructure into a better defense against targeted attacks.

Third-party security technologies that work with Trend Micro’s Network Defense solutions include:

- Security information and event management (SIEM)
- Vulnerability assessment and management
- Application security
- Next-generation firewalls
- Breach detection
- SSL visibility and enforcement
- Software-defined networking and the cloud
- Network packet brokers
- Incident response automation

Trend Micro’s advanced threat-protection platform uses open APIs that allow its malware detection engines and sandboxing capabilities to be seamlessly integrated into any other Trend Micro or third-party security solution. This means, for example, it can automatically provide updates on identified threats to next-generation firewalls, allowing any detected malware and command-and-control information to be quickly shared between security products. It also integrates with leading encryption appliance vendors to ensure network traffic can be monitored and inspected even when it is encrypted.

Trend Micro’s TippingPoint NGIPS, meanwhile, can work closely with leading vulnerability assessment and management solutions to optimize an organization’s security coverage. Vulnerability scans can be imported and mapped to Digital Vaccine filters to quickly remediate vulnerable assets and systems. Policy adjustment recommendations are then delivered and tuned against the organization’s specific security infrastructure, ultimately reducing administration time and unnecessary notifications while providing a more complete, ‘big picture’ view into its overall security posture.
Trend Micro threat data can even be shared with popular SIEM solutions, allowing data to be quickly correlated from multiple sources for faster and more efficient threat response.

This high level of integration and optimization with other vendors’ products helps Trend Micro customers improve the value of their security investments. It means they can easily enhance the capabilities of the products they already have in place while still benefiting from Trend Micro solutions and expertise – without having to rip and replace their entire security infrastructure.

CONNECTED: SEAMLESS SHARING OF THREAT INTELLIGENCE

Organizations must be in a position to manage risk before, during and after an attack. This requires more than just a multi-layered approach to security – it requires the techniques comprising that approach to connect and communicate seamlessly with each other, sharing threat intelligence across every security layer of the entire enterprise network to accelerate response times and adapt to new threats.

This kind of architecture is referred to by Trend Micro as Connected Threat Defense – and it involves a constant cycle of protecting against, detecting and responding to threats.

![Figure 3. Trend Micro connected threat defense framework](image)

Organizations must be able to protect themselves from as many threats as possible. This starts with having a good understanding of the potential threats they face and the vulnerabilities in their networks that could be exploited. Despite the fact that a very large percentage of threats can be prevented through proactive protection techniques, there will always be some advanced threats that sneak through the defenses. Organizations therefore
require a number of advanced detection techniques, supported by rapid and automated response to any detected threats.

For the best possible security posture, there must be connections between each stage in this cycle. Multiple techniques can be used at the same time to detect and respond to different kinds of threats at the server, network and user levels – and it is critical that all of these layers of security are able to talk to each other. The connected threat defense framework ensures the intelligence collected by the tools and techniques applied in one stage is automatically shared with those used in the other stages for faster and even automated reporting and remediation of new and unknown threats.

The more security layers an enterprise has to consider (if it needs to protect thousands of users and their endpoints in addition to its networks and servers, for example), the greater the need for this kind of connected approach.

Figure 4. The link between security layers and connected threat defense

Trend Micro's advanced threat-protection platform serves as the foundation of our connected threat defense framework. In its sandbox environment, the behavior of an unknown piece of malware can be safely observed to confirm whether a file is definitively good or bad. Should the malware send command-and-control traffic to a dozen IP addresses around the world upon execution, for instance, those addresses can be shared with all other connected Trend Micro products so they can all block communications to those addresses going forward.
Centralized visibility and control

Organizations also need visibility across their environment and repertoire of security techniques, using analytics to fully assess the risk and impact of an attack. Through its connected threat defense framework, Trend Micro is able to provide a single console/dashboard for strong centralized visibility and control, delivering a complete view of threat activity across multiple layers of protection, with user-centric threat timelines and forensic tools to simplify threat investigation as well as day-to-day security management. This high level of visibility across users and systems improves an enterprise’s understanding of threats, response time and productivity of its IT resources.

TREND MICRO: AN INNOVATOR IN NETWORK SECURITY

With tailor-made targeted attacks becoming the norm, traditional security solutions are no longer enough to protect the networks of today's enterprises. A new breed of security capabilities is needed to effectively monitor network traffic for malicious behavior, rapidly identify and block ‘known bad’ entities, and analyze and respond to suspicious payloads.

Based on nearly three decades of experience in the security industry, Trend Micro recommends that all organizations adopt a smart, optimized and connected approach to network security – one that utilizes a variety of cross-generational threat protection techniques (and can apply the right technique at the right time), with seamless integration and interconnections between security products to enable the sharing of real-time threat intelligence for improved detection accuracy and a greater level of protection.

With XGen™ security, Trend Micro is the first vendor to provide enterprises with a truly smart, optimized and connected approach to network security. Continuously adapting to the evolving threat and IT landscape to deliver market-leading endpoint, cloud and network security solutions, Trend Micro was also the first major security vendor to:

- Detect and block attacks in-line and in real-time by embedding machine learning techniques in its NGIPS
- Provide file and web reputation protection to all of its customers from the cloud

A recognized leader in security

Trend Micro is a:

- Recommended vendor for Next-Generation Intrusion Prevention Systems (NSS Labs, 2016)
- Recommended vendor for breach detection systems for three consecutive years (NSS Labs, 2016)
- Leader in the 2017 Gartner Magic Quadrant for Intrusion Detection and Prevention Systems
- Leader in 2016 Forrester Wave for Advanced Malware Analysis
- The leader in global vulnerability research and discovery (Zero Day Initiative) since 2007 by Frost & Sullivan
• Offer an NGIPS that delivers up to 100 Gbps inspection throughput with low latency for data centers and high-performance enterprise networks

Drawing on this extensive history of innovation, Trend Micro’s Network Defense solutions, powered by XGen™ security, are helping enterprises efficiently and effectively protect themselves against the existing threats that continue in circulation while being proactive in identifying new, unknown threats – all without sacrificing performance and visibility across the multiple solutions they may have in place throughout their security infrastructure.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.