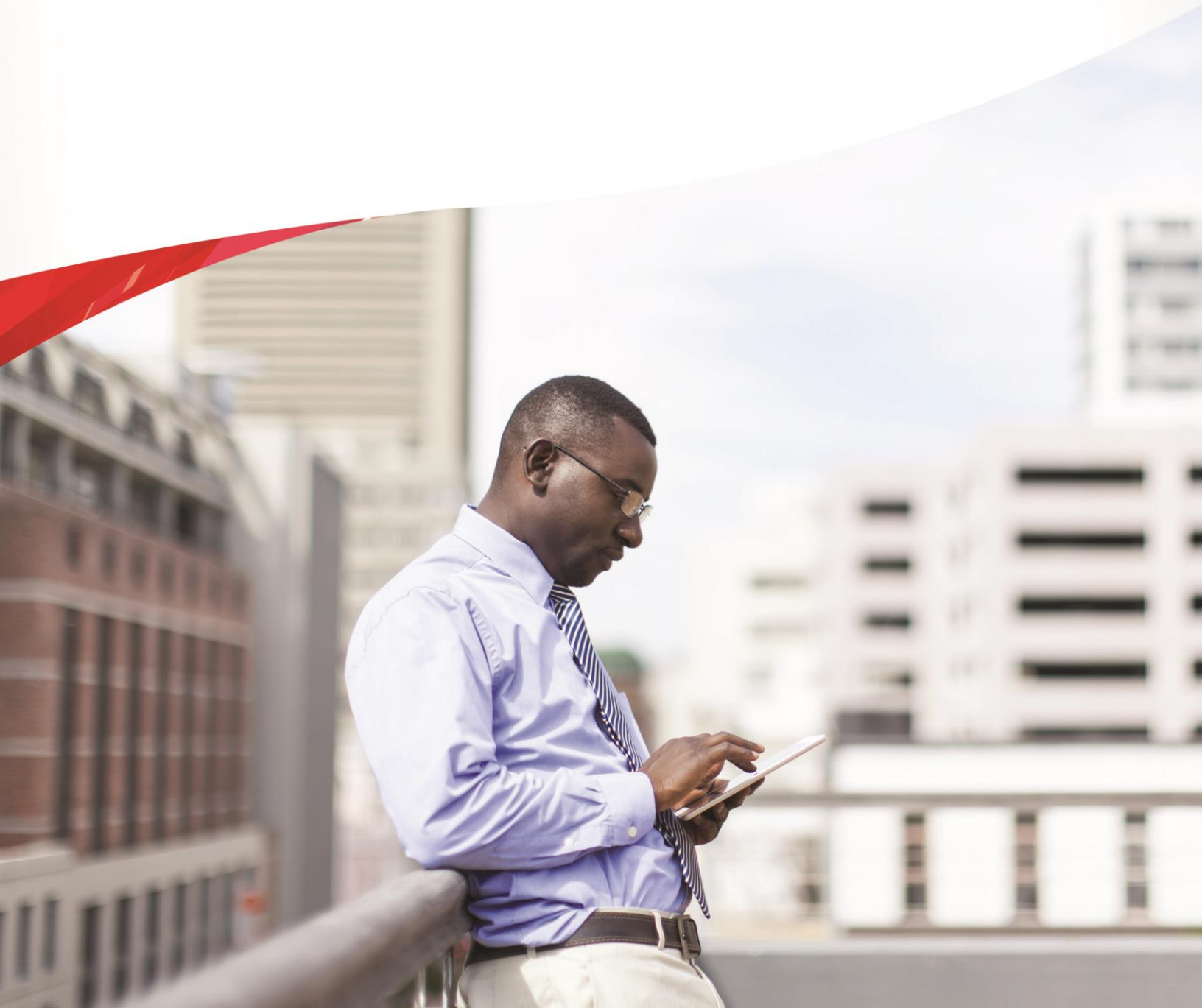
A Trend Micro White Paper | **October 2016**

There is no silver bullet

The strengths and weakness of today's threat-protection techniques—and why a multi-layered approach to endpoint security is a must

>> A Trend Micro technical white paper



The security landscape changed dramatically with the maturation of crypto-ransomware in 2014. Not only did this new type of malware bring about a more lucrative business model for attackers, it also spurred the adoption of many so-called 'next-gen' endpoint security techniques. While these techniques bring impressive new capabilities to the fight against malware, there is still no one 'silver bullet' that can stop every threat — meaning a blend of advanced techniques is required to achieve maximum protection.

This white paper takes a closer look at the advantages and disadvantages of many of today's threat-protection techniques, and outlines why organizations should employ a multi-layered, defense-in-depth approach to security. That approach is embodied in Trend Micro™ XGen™ endpoint security, which combines cross-generational threat protection with global threat intelligence to defend against and adapt to the latest threats.

CONTENTS

SHADES OF GRAY: MAKING SENSE OF THE CHANGING THREAT LANDSCAPE

The security landscape used to be black and white: traditional anti-virus signatures and web filtering protected against 'known bad' entities; whitelists and application control ensured users were exposed to only the 'known good' files.

But as the IT environment becomes more sophisticated, so do the threats faced by businesses of all sizes across every industry. As organizations transition to the cloud and adopt an ever-increasing number of mobile devices — and with their employees often using their own personal devices and cloud-based file-sharing services at work —

the possible attack surface has broadened beyond just on-premises infrastructure.
More concerning, however, is the way attackers are now looking at their 'work' as a business — and investing a considerable amount of money into evasion techniques that allow them to slip through the security measures put in place by most organizations.

The new business model for attackers

Security vendors have seen a fundamental shift in the commodity malware industry in recent years. One moment stands out in particular: the introduction of crypto-ransomware in 2013 (and its maturation as a viable method of attack the following year), which dramatically changed the business model for online attackers.

Consider the ways a malware infection can be monetized. An attacker can:

- Rent out infected servers to send spam, launch distributed denial of service (DDoS) attacks or mine for Bitcoins
- Steal money directly from the victim (e.g., through a banking trojan)
- Steal the victim's data or intellectual property
- Ransom the files on the victim's computer

Each approach has different costs, risks and potential rewards for the attacker. It takes a lot of infrastructure to control and maintain a botnet of infected servers — and the prices people are willing to pay for spambots and 'DDoS-for-hire' services are typically quite low. While stealing money directly from a person's bank account can lead to potentially high rewards, doing so requires a complex system of 'money mules' to launder that money. What's more, even getting to that point can be quite difficult, as most banks have comprehensive systems in place to detect any suspicious transactions and stop them before they go through. And when it comes to stealing intellectual property, attackers must first identify the value of the stolen data (if there even is any) and then be able to find a buyer for it, usually resulting in a long, drawn-out sales process.

In comparison, ransoming a computer and its files allows attackers to quickly realize a premium price per infection (most charge between $500 and $1,000 for decryption keys) and get paid immediately in Bitcoin, which can be anonymized using a Bitcoin scrambler to ensure the transaction can never be traced.

What is crypto-ransomware?

Crypto-ransomware is different from traditional malware in that its purpose is not to steal the victim's data. In fact, the data never leaves the victim's computer. Instead, the malware locks, encrypts or otherwise prevents access to the data and files located on the computer — unless the victim pays a ransom. Once the ransom has been paid, the attacker provides a decryption key that unlocks the data. If the ransom isn't paid on time, the price may go up — or the malware could even delete the encrypted files or post them publicly.

The fear of losing priceless data will push many victims to pay, especially businesses and institutions (such as hospitals) whose day-to-day productivity relies heavily on the availability of their data.

Crypto-ransomware is typically distributed via exploit kits, social engineering schemes and spam emails.

The evasion and detection arms race

Due to the fast and impressive return on investment of crypto-ransomware, attackers are able to re-invest their 'earnings' into new evasion techniques — which help them take in even more money so they can further strengthen their evasion capabilities.

Many attackers no longer rely on free (or very cheap) botnets, instead compromising or, in some cases, purchasing legitimate infrastructure from which to launch their attacks: data centers and ISPs that won't appear on any blacklists. In the past, the links in spam emails would have directed victims to dodgy websites likely to be caught by anti-spam filters; attackers now compromise legitimate web servers, which then redirect their victims' browsers to the malicious website.

Social engineering attacks are also on the rise, which see people tricked into handing over their confidential information through fake web pages that replicate the look and feel of banks, government agencies or utility companies, complete with CAPTCHA fields or obfuscated JavaScript to avoid detection.

Another concern is the use of polymorphic malware 'hash factories', which can automatically change the characteristics of their malware files on a regular basis — as quickly as every 15 seconds, in the case of the Cerber crypto-ransomware.[1] By constantly inserting new pieces of code into the malware to make variants of the file (usually a sequence of non-effective assembly instructions or arbitrary benign API functions), it becomes practically impossible for traditional, static, signature-based detection to keep pace.

Other new techniques for avoiding signature-based detection include splitting the crypto-ransomware's main malicious logic into many small sequences of instructions that are scattered across the entire malware binary, then connected together through unconditional jumps. There is also 'packed' malware, which includes a short piece of code and a long string of data. The code decompresses or decrypts the data into a new piece of code that is then executed — and that new code can be packed again and then decrypt itself to produce the actual malicious code.

By abusing legitimate web services and creating malware that can easily avoid detection, attackers have upended the traditional IT security paradigm. Suddenly, the systems and applications that have always been classified as known good don't look quite as secure anymore. The dividing line between black and white has been muddled — resulting in a constantly growing 'gray' area that is much harder to defend against.

Responding to the gray with multi-layered endpoint protection

In response to the proliferation of gray-area threats, security vendors have developed a number of so-called 'next-gen' threat-protection techniques in recent years: sandboxing, behavior monitoring and vulnerability shielding, to name a few. While these have all added impressive new security capabilities to the mix, it's important for enterprises of all sizes to recognize that no one next-gen technique can possibly protect against every threat.

As analysts such as Gartner's Neil MacDonald have been saying for years, a multi-layered, defense-in-depth approach to security is the best way to ensure maximum protection.[2] This means having many different security techniques working together and complementing each other to catch the highest possible percentage of malicious elements. If an organization relies on just one or two techniques for its security needs, there's a much greater likelihood something bad will slip through the cracks — with potentially devastating consequences.

Although new threat-protection techniques are typically available as individual point products when they first arrive on the market, most will eventually end up consolidated into an endpoint protection platform delivered by a single security vendor. As MacDonald points out on the Gartner blog, relying on a single vendor for endpoint security does not lead to a loss of defense-in-depth. Instead, an integrated endpoint protection platform can help organizations eliminate the gaps in security coverage and visibility that can occur when using a mix of different point products — all while achieving significant cost savings and operational simplification.[2]

[1] "Cerber ransomware morphing every 15 seconds." *SecurityWeek*, June 2016. Available from http://www.securityweek.com/cerber-ransomware-morphing-every-15-seconds.

[2] MacDonald, Neil. "Defense-in-depth doesn't mean spend-in-depth." *Gartner Blog Network*, March 2009. Available from: http://blogs.gartner.com/neil_macdonald/2009/03/04/defense-in-depth-doesnt-mean-spend-in-depth/.

PEELING BACK THE LAYERS OF DEFENSE-IN-DEPTH

Protection and detection techniques are always evolving: as threats become more sophisticated, new ways of defending against them continue to emerge. (Soon followed, of course, by new ways of evading detection.) For example, signature-based detection long ago evolved to include file reputation, making it possible to wipe away billions of known threats with very high performance. But in the face of more advanced and unknown threats, even that isn't enough — necessitating the development of the advanced security capabilities seen today.

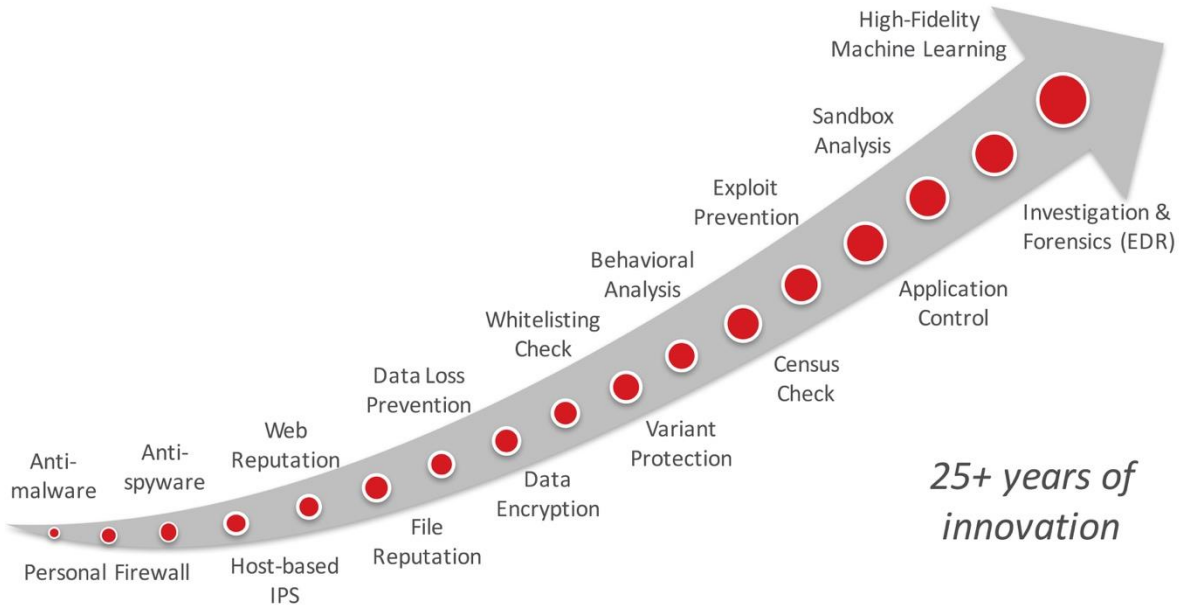


Figure 1. Evolution of endpoint security techniques

Every endpoint protection technology, including the latest advanced techniques, has its advantages and disadvantages. That's what makes the multi-layered approach so important. If a malicious file happens to get past one layer of security (because the web server behind the attack is not on a blacklist, for instance), it is backed up by the capabilities of several more layers of defense, each relying on a different style of protection and detection.

So what techniques should be part of a multi-layered endpoint protection platform?

Signature-based detection

Traditional signature-based anti-virus and anti-malware offer a high level of protection against known threats in a very computationally efficient way. (The process of matching files against a list of known malware signatures is far less CPU-intensive than the more advanced behavior-based detection techniques.) But with new variants of crypto-ransomware being released every minute, the usefulness of signature-based detection as a standalone security technique is waning. To provide any real value to an enterprise, it must be complemented by a wide range of other techniques.

Still, signature-based detection should be a part of a multi-layered security approach, including:

- **File and web reputation –** Blocks the execution of any files, URLs and websites that match the signature of a known malicious item, but has difficulties with unknown/unrecognized threats (such as polymorphic or packed malware) or attacks originating from a 'good' ISP or data center.
- **C&C blocking –** Examines and shuts down endpoint traffic (over any port) that is attempting to connect to or contact a known command-and-control (C&C) server.

Non-signature-based detection

These techniques defend against malware without requiring any previous knowledge of exact file signatures. Instead, they make determinations based on a file's characteristics and behavior. Some of the techniques to be included in a multi-layered security approach include the following:

Variant protection

Variant protection looks for obfuscated, polymorphic or variants of malware by using fragments of previously seen malware and detection algorithms.

Census check

The likelihood that a file is malicious can be determined in part by its prevalence and maturity (i.e., how often it has been seen over a given time period). Files that have never been detected are considered to be more suspicious. This technique has proven to be quite strong against malware hash factories.

Whitelisting check

To reduce false positives on endpoint detections, all files should be checked against a database of known and verified good files. (As an example, Trend Micro's certified safe software whitelist contains almost one billion known good files.)

Behavioral analysis

This technique examines an item as it is unpacked, looking for suspicious or unusual behavior in how it interacts with operating systems, applications and scripts — even if the item isn't on a blacklist. While crypto-ransomware can easily pass by traditional anti-virus (by being a freshly compiled executable), it will behave suspiciously as it loads into memory, triggering further action. As attackers are still finding it difficult to evade behavior-based detection, this technique is a must-have for any organization.

Behavioral analysis can take many forms, including:

- **Script protection –** Checks for malicious code or scripts within files attempting to execute on the endpoint (e.g., Office macros, scripts in PDF, PowerShell scripts).
- **Injection protection –** Blocks processes from injecting code where it shouldn't be (such as program libraries).
- **Suspicious action monitoring –** Examines an item as it is loading or running, looking for suspicious behavior in how it interacts with other processes.
- **Ransomware protection –** Looks for rapid obfuscation/encryption of files by an unknown process, then terminates that process and restores the encrypted files.

- **Memory inspection –** Evaluates processes running in memory, scanning them for malware (or fragments of recognizable malware) as an item is unpacked into memory. This ensures malware packer tools can't just obfuscate an older known piece of malware.
- **Browser exploit protection –** Uses emulation and algorithmic detection technology to protect against exploit code on web pages (e.g., exploits in Java and Flash).

STRENGTHS	WEAKNESSES
• Can catch items that get through signature-based blacklists • Can examine behavior of malicious documents in known good applications (e.g., PDFs) • May enable analysis in the network before malware reaches the endpoint	• Has a reputation for producing more false positives (especially if not paired with whitelists and file-reputation techniques) and, as a result, requiring more IT management than other detection methods, causing some organizations to disable this function in their endpoint protection platforms • Can be somewhat more CPU-intensive than other protection methods

Exploit prevention

While there are hundreds of thousands of malicious files out there, there aren't very many unique *exploits* that can be used to compromise a user's system. As such, it is often easier to focus on preventing the exploitation of specific application or OS-related vulnerabilities rather than blocking the files themselves. Also known as vulnerability shielding, exploit prevention techniques can include:

- **Host-based firewalls –** Protects endpoints on the network using stateful inspection and network virus scanning.
- **Exploit protection –** Monitors programs that demonstrate abnormal behavior associated with exploit attacks, and uses multiple heuristic analysis techniques to detect exploit code on web pages as users attempt to access them with their browsers.
- **Intrusion prevention –** Blocks network-based exploits of known vulnerabilities in popular applications and operating systems by using host-based intrusion prevention (HIPS) rules that provide a virtual patch.
- **Lateral movement detection –** Uses IDS/IPS signatures on network traffic at the endpoint solutions to detect and block the lateral movement (or spread) of malicious activity across servers, workstations and laptops.

STRENGTHS	WEAKNESSES
• Able to block unknown threats targeting known vulnerabilities in an OS or application • Helps when OS or application patches are not yet available or will never be (e.g., legacy OS) • Can detect malicious activity and attempts by malware to spread across an organization's network	• Can't block malware that doesn't exploit application or OS vulnerabilities • Intrusion prevention is generally less effective against zero-day application or OS vulnerabilities

Application control/whitelisting

This technique blocks the installation and execution of any executables that aren't known good applications or dynamic link libraries (DLLs). It essentially offers full control over which applications can and can't be used in an enterprise environment. While this tactic can be very effective, few organizations are willing to limit their users to only those applications found on a whitelist.

Because of the level of intervention required to manage this process, application control has traditionally been used only for servers or dedicated-function machines where applications aren't changed very often. However, the latest techniques are much more user-friendly, with automated rules and policies that give users the flexibility to install new applications as long as they meet specific criteria pre-established by their administrators. With these advances, application control can provide greater value in dynamic user environments (e.g., typical laptop and desktop setups).

STRENGTHS	WEAKNESSES
• Doesn't need to identify malware; blocks unknown apps instead • Vendors can supply whitelist from the cloud • Deterministic (i.e., it knows what it will stop) • Can be used for system lockdown • Can help with corporate policy on appropriate usage, category-based exclusions, etc.	• Only stops executables and will miss other malicious actions or vulnerability exploits (unless they launch a separate executable) • Some solutions require a locally defined whitelist, which can take time to produce • Vendors' whitelists may vary in completeness • Some solutions rely on vendor certificates to determine maliciousness (rather than the app's characteristics), making them vulnerable to 'code signing' compromise attacks

Investigation and forensics

Also known as endpoint detection and response (EDR), this technique records and reports on system-level activities in great detail, allowing for rapid analysis of the nature and extent of an attack. The information collected can provide valuable insight into how an infection propagates through a company's systems and can help determine the extent of data loss — all of which can be leveraged to make better detection and prevention decisions in the future. However, this is a purely *reactive* technique implemented after an attack has already occurred; it typically can't block any malware on its own. In addition, a high level of skill and training is required for IT teams to analyze and take action on the collected data in a useful way.

BRINGING A NEW LEVEL OF INTELLIGENCE TO SECURITY WITH MACHINE LEARNING

Machine learning represents the newest and most intriguing of the advanced security techniques. By constantly analyzing the attributes and characteristics of both known good and known bad files, machine learning algorithms can 'train' detection engines to adapt to the latest threats and be more efficient in blocking new unknown malicious items. It's a powerful technique that becomes even stronger with the rise of malware hash factories because the more malware is transformed, the more data these algorithms have available to analyze, leading to even better performance.

While many security vendors are hyping machine learning as a cutting-edge innovation (and often claiming it as a competitive differentiator), it's not an entirely new concept. Most vendors have been relying on machine learning as far back as 2005, when it was first used to train anti-spam engines. The technology has evolved continuously since then and can now be found 'under the hood' of a range of malware detection and prevention techniques, from spam detection to URL reputation and categorization, to detecting malicious social media accounts.

So why is machine learning getting the spotlight now? It ties back to the maturation of crypto-ransomware in 2014. Before then, enterprises were more concerned with business-critical false positives than missed detections.

Because it requires a lot of time and effort for an IT administrator to track down and analyze the source of a false positive (potentially leading to costly business disruptions), many companies simply put up with a certain number of malware infections. As machine learning had the reputation of producing high false positive rates (and still does, to some extent), security vendors employed the technique rather conservatively.

When attackers realized they could quickly and easily extort money directly from the owner of an infected computer (rather than using the infected computer for other means), the paradigm flipped: suddenly, a missed detection could create a much larger business disruption than a false positive. With their critical business data on the line, enterprises decided they would rather be safe than sorry.

Going beyond with high-fidelity machine learning

The most recent advancements in machine learning have focused on file-based threat detection across endpoints, servers and gateways. Rather than looking for a specific behavior or file signature, this type of machine learning involves extracting a file's features (essentially, its underlying 'DNA') and then using mathematical algorithms to determine/predict whether that file is malicious. This is typically expressed as a percentage based on if the file in question contains some or many of the characteristics of a known bad file.

The algorithms are trained and learn from data on existing verified good and bad files — and the more data the algorithms have to work with, the more accurate their predictions will be, especially when dealing with zero-day attacks. (Going forward, the real competitive differentiation between security vendors will be how well they are able to train their machine learning algorithms, determined by the reliability, timeliness and volume of their sources of known good and bad files.)

To provide a more robust level of malware protection, a new technique known as 'high-fidelity' machine learning can be used to extract and analyze a file's characteristics both *before* and *during* its execution. This allows for determinations to be made based on more than just a static snapshot of the file — machine learning can also detect files that reveal certain malicious characteristics only upon execution.

This two-tiered process that is central to high-fidelity machine learning also helps increase overall detection accuracy. During the pre-execution phase, machine learning can block malware before it has a chance to run. However, if the malware uses obfuscation methods such as packers or self-extracting archive techniques to avoid detection at this phase, there is a next step at which it can be caught by high-fidelity machine learning. On execution, malware reveals its true intentions — and the behavior it shows during runtime allows for more precise security features to be examined. (Even though it is much harder for malware to avoid detection during execution, there is a chance it could cause partial damage to an organization's systems and devices before its processes can be terminated.)

Leading the way in high-fidelity machine learning

Trend Micro was the first security vendor to infuse 'high fidelity' machine learning into its approach, analyzing files both before and during runtime, augmented by 'noise cancellation' techniques such as census and whitelist checking (against a database of nearly 1 billion good files) at each layer to reduce false positives.

To ensure the highest fidelity, Trend Micro's algorithms use only the features that will lead to the most accurate detection — without the performance impact or higher rates of false positives common to other vendors' machine learning technologies.

These algorithms are trained from the data collected by the Trend Micro Smart Protection Network, which uses a global network of hundreds of millions of sensors to capture and analyze terabytes of threat-related data on a daily basis.

High-fidelity machine learning is made even more efficient through the integration of 'noise cancellation' techniques such as census and whitelist checks, which help to greatly reduce the incidence of false positives (and, in turn, avoid the major headaches false positives can give to IT administrators).

STRENGTHS	WEAKNESSES
• Works well on unknown executable malware that is heavily manipulated and typically gets through traditional signature-based blacklists • Runtime machine learning an analyze behavioral features during execution • Can detect techniques that attempt to avoid sandboxes	• Can be somewhat more CPU-intensive than other protection methods • Generally weaker at detecting scripts and macros (e.g. in Office docs) • Has higher rates of false positives if not paired with census and whitelist checking and other layers of endpoint security • Can't see behavioral features during runtime if pre-execution machine learning is used on its own (as is the case with some vendors)

Using malware DNA to stop zero-day attacks

High-fidelity machine learning can be used to effectively analyze and compare the DNA (i.e., its core features and characteristics) of an unknown/zero-day file to that of a known crypto-ransomware file even when the file signatures don't match.

If the crypto-ransomware has been modified by a hash factory, for example, some elements of the new variant's underlying code will look very similar to those found in the code of the known version of the file (as illustrated by green boxes below). However, as everything else in the code will be different (red boxes), it is unlikely that traditional methods (such as file reputation or variant protection) will be able to match the variant to the known bad file.

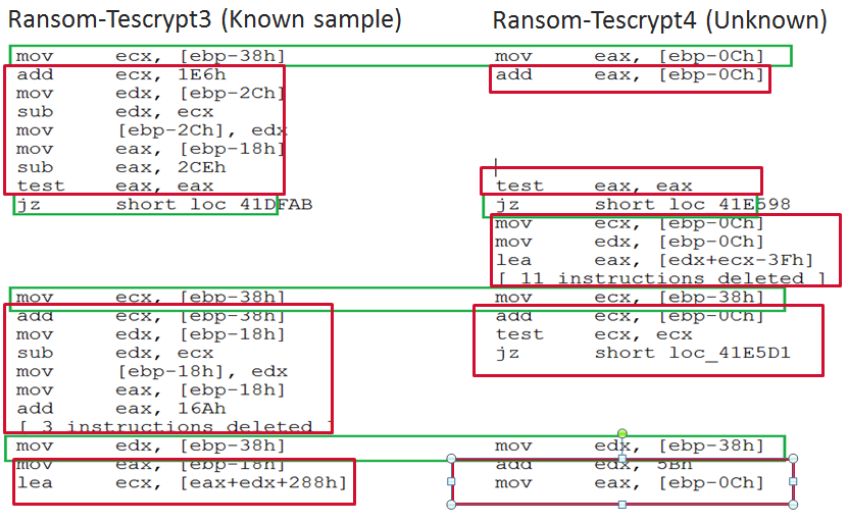


Figure 2. Limited code similarities between new and known malware variants

But by extracting and analyzing thousands (or even tens of thousands) of different features across the entire file, machine learning can pick out the many similarities to a known version of crypto-ransomware. By identifying these similarities in the malware's features — its DNA — the machine learning algorithms can confidently determine that the unknown file is crypto-ransomware.

There are a number of different ways machine learning can extract and observe the features that make up a piece of malware's DNA, including using its opcode and import table:

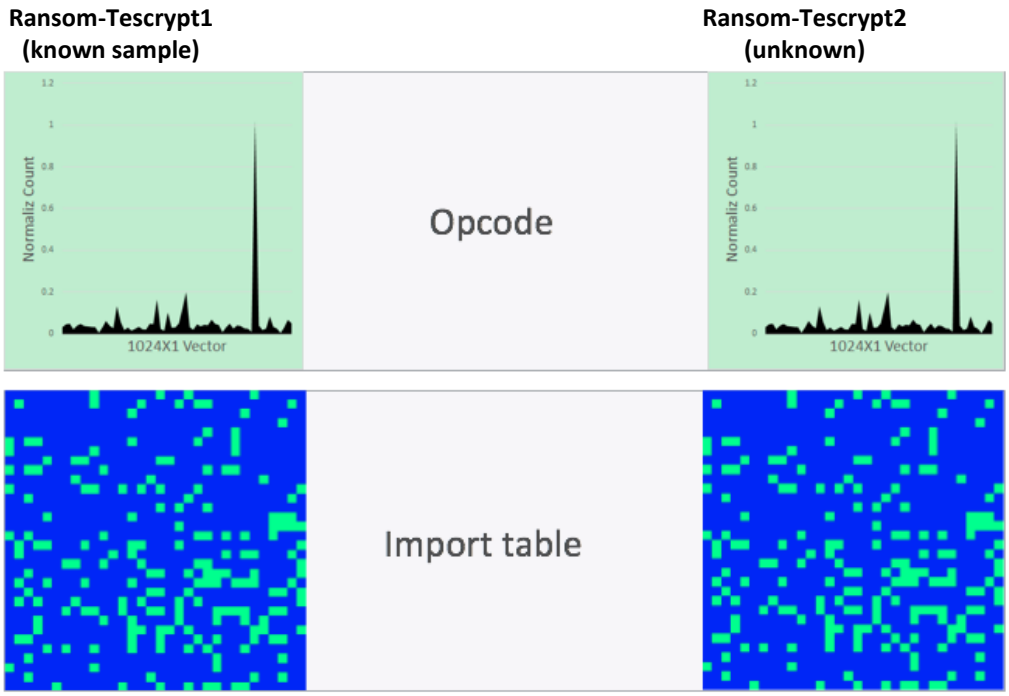


Figure 3. DNA similarities between new and unknown malware variants

A strong defense… for now

By looking closely at file features, advanced machine learning technology can correlate threat information and perform in-depth file analysis to more accurately predict emerging unknown security risks.

But it is *not* the final word in malware protection. Despite the claims of some vendors, it is not the 'silver bullet' that will put an end to malware once for and all. Like every other security technique discussed thus far, machine learning has its strengths as well as its weaknesses.

First, machine learning requires large volumes of data and significant amounts of processing power (and associated backend infrastructure) to complete in an effective and efficient way. In addition, as more and more vendors adopt and promote machine learning techniques, it is a certainty that the malware itself will change in response as attackers try to evade detection (just as spam did more than a decade ago to defeat the machine learning of that era). To pass through existing machine learning solutions, malware will likely start to leverage legitimate packing tools, use self-extracting archives and other installers, be written in other programming languages or formats.

By bringing a new level of intelligence to endpoint security, machine learning is a highly valuable tool in the fight against modern malware. But to defend against these new scenarios, it needs to be backed by comprehensive whitelists, malware family patterns and other carefully crafted detection techniques as part of a multi-layered, defense-in-depth approach to online security.

STRONGER TOGETHER: THE VALUE OF A MULTI-LAYERED APPROACH TO SECURITY

The key to the multi-layered approach to security is that every protection and detection technique, including machine learning, must work in concert, building on each other's strengths and providing the capabilities needed to compensate for their weaknesses.

More accurate detection at less cost

The primary reason to adopt a defense-in-depth approach to security is that it results in extremely high catch rates, including for crypto-ransomware. For the small number of malware that will slip through both the signature- and behavior-based detection techniques, nearly every malicious file will be caught deeper down the funnel by advanced machine learning processes.

In addition, multi-layered threat protection means fewer false positives and better system performance. As a much smaller set of unknown files will need to undergo machine learning techniques (which are both computationally intensive and known to produce more false positives), less strain is put on an organization's IT systems and resources.

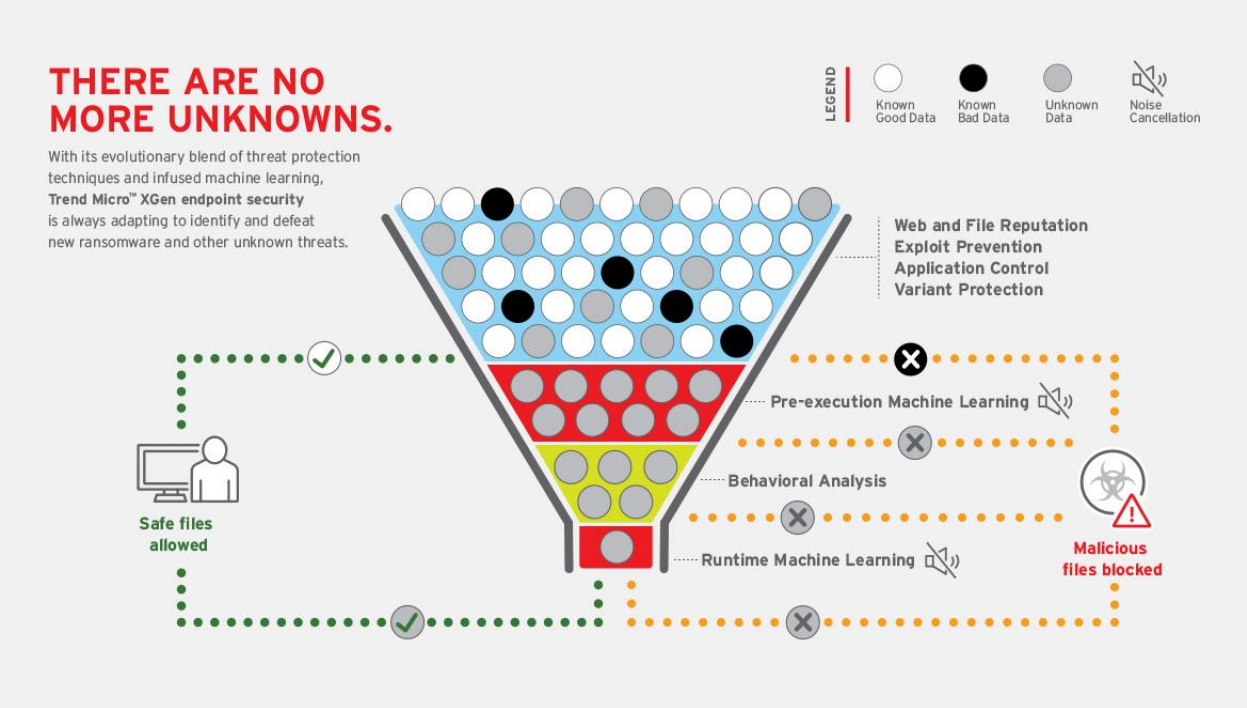


Figure 4. Delivering more efficient security with multi-layered threat protection

Sharing intelligence for faster, more adaptive security

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 seamlessly communicate with each other, sharing threat intelligence across the entire enterprise network to accelerate time to respond and adapt to new threats for more effective endpoint protection.

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.

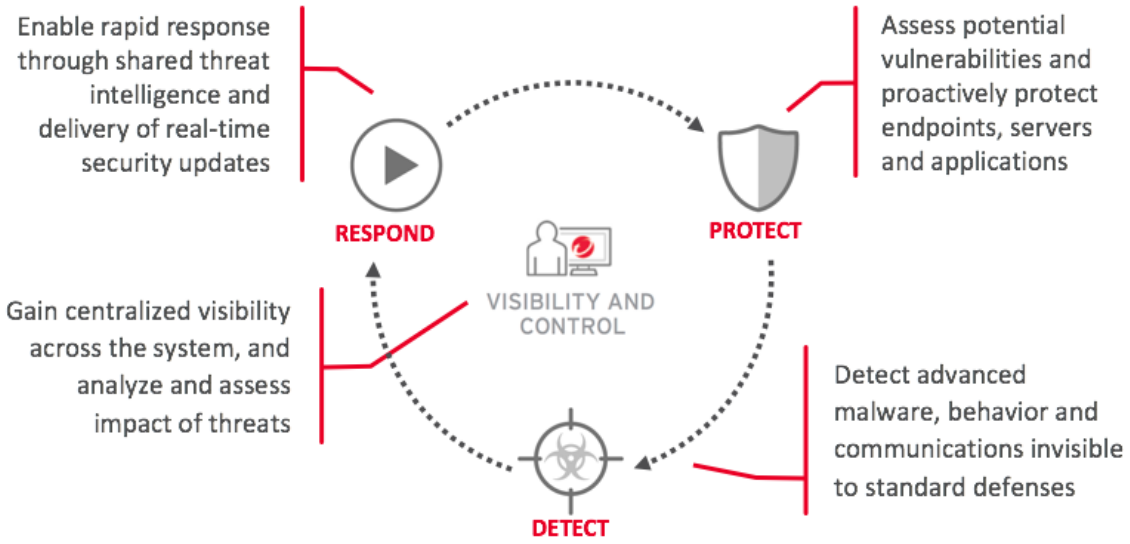


Figure 5. Trend Micro connected threat defense framework

Organizations need to be able to **protect** themselves from as many threats as possible from entering their environment. This starts with having a good understanding of the potential threats they face. Organizations should conduct a vulnerability assessment across the entire enterprise, taking an inventory of all endpoints, applications and servers — and fully understanding their vulnerabilities and exploits. With that insight, a range of capabilities can be deployed to proactively protect their endpoints, including antimalware file reputation, encryption, web filtering, intrusion prevention, host-based firewalls and more.

Despite the fact that a very large percentage of threats can be prevented with these techniques, there will always be some advanced threats that sneak through the defenses. For these, organizations require **detection** techniques like the ones discussed earlier in this paper, including behavioral analysis, machine learning, application control and lateral movement detection.

Rapid and automated **response** to detected threats is also critical. Where possible, security updates should be deployed automatically in real time, further enhancing protection.

Finally, organizations need to have visibility across their environment and security techniques, using analytics to fully assess the risk and impact of an attack.

TREND MICRO: AN INNOVATOR IN SECURITY

Drawing on more than 27 years of experience, Trend Micro is a proven leader in multi-layered, defense-in-depth security approaches, offering all organizations multiple protection and detection techniques to eliminate security gaps across any user activity and any endpoint. **Trend Micro™ XGen™ endpoint security** offers a unique blend of cross-generational threat protection techniques — encompassing the full spectrum of signature- and behavior-based techniques, including high-fidelity machine learning — to ensure the right technique is consistently applied at the right time.

To enable more efficient and accurate malware detection, XGen endpoint security is powered by global, cloud-based threat intelligence from the Trend Micro Smart Protection Network, which continuously mines data from around the world to ensure we have a constant stream of good and bad file information from which to train our machine learning algorithms. Through our commitment to connected threat defense, XGen endpoint security can constantly adapt to protect against future attacks, evolving to find new crypto-ransomware and other unknown threats (including zero-day attacks) by automatically sharing threat intelligence among the various security layers.

The Trend Micro Smart Protection Network consists of:

- A global network of hundreds of millions of sensors to collect more threat information in more places — 16 billion threat queries daily — 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 1 billion known good files to identify 500,000 new, unique threats each day
- Proactive cloud-based protection to block threats — as many as 250 million daily — and minimize risk

More than 27 years of innovation

Trend Micro was the first major vendor to integrate machine learning, signature-based detection and behavioral analysis into a unified, multi-layer approach to security. We were also the first to:

- Deliver connected threat defense across endpoints, email and web gateways with network breach detection and sandboxing
- Integrate security for Amazon Web Services and Microsoft Azure cloud environments
- Integrate virtualization security with VMware
- Deliver threat intelligence from the cloud

Trend Micro also provides a single console/dashboard across all endpoints and gateways — whether on-premises or in the cloud — for strong centralized visibility, with user-centric threat timelines and forensics tools to simplify threat investigation. Security and compliance are improved through the seamless sharing of intelligence across the layers of defense, centralized threat and data protection policy management capabilities, and integrated security management and analysis across multiple layers of protection to defend against advanced threats that exploit multiple attack vectors.

CONCLUSION

Crypto-ransomware had a profound impact on the security game, facilitating the development of advanced protection and detection techniques such as machine learning. But even the latest techniques aren't powerful enough to stop every threat on their own.

Based on nearly three decades of experience in the security industry, Trend Micro strongly recommends that all organizations adopt a multi-layered, defense-in-depth approach to online security. Rather than relying on just one or two of the so-called 'next-gen' techniques in isolation, a robust, multi-layered approach should involve a vast array of signature- and non-signature based security techniques — working together and sharing threat intelligence to improve detection accuracy and deliver a maximum level of protection.

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints.
With over 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.