TREND MICRO™

Machine Learning Masters

Go Beyond Next-Gen

POWERED BY XGen™ SECURITY

Stuart Lambert
Head of Public Sector Sales
stuart_lambert@trendmicro.co.uk

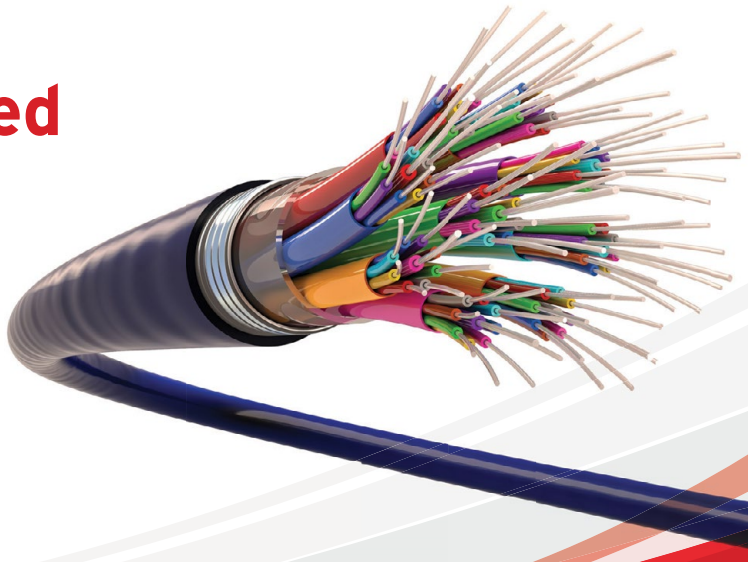
Bharat Mistry
Principal Security Strategist
bharat_mistry@trendmicro.co.uk

www.trendmicro.co.uk/xgen

TREND MICRO

POWERED BY XGen SECURITY

Detect and prevent breaches at wire speed



Your enterprise is in the crosshairs of the increasingly complex array of ransomware, advanced threats, targeted attacks, vulnerabilities, and exploits.

Only complete visibility into all network traffic and activity will keep your network security ahead of today's purpose-built attacks which bypass traditional controls, exploit network vulnerabilities, and either ransom or steal sensitive data, communications, and intellectual property.

Trend Micro Network Defence detects and prevents breaches at wire speed anywhere on your network to protect your critical data and reputation.

NSS LABS RECOMMENDED

Proven capability

Trend Micro TippingPoint:
"Recommended" Next-Generation Intrusion Prevention System and 99.6% security effectiveness.

Trend Micro Deep Discovery:
"Recommended" Breach Detection System 4 years in a row and 100% detection rate

Industry leading threat intelligence

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

Please get in touch:
Bharat Mistry, Principal Security Strategist
Bharat_mistry@trendmicro.co.uk

www.trendmicro.co.uk/xgen-cyber

HERE'S HOW MACHINE LEARNING WORKS BEST IN IDENTIFYING SECURITY THREATS

Machine learning (ML) appears to have suddenly emerged in security, and almost as quickly it has assumed the mantle of a new "next-generation" tool to tackle cybercrime. In fact, the story is a little more nuanced than that.

Some well-established security companies, including Trend Micro, have worked with machine learning for more than a decade. Until recently, they tended not to discuss this work openly, mainly because of understandable concerns that the technology, applied on its own, flagged too many false positives.

More recently, two things have happened, and I believe they are correlated. One is the rise of ransomware like CryptoLocker around 2014. The other is the emergence of next-generation security vendors who promote machine learning as the "new" control companies must have in order to tackle advanced threats. Many organisations working with established security companies will, in fact, have been applying machine learning in their solutions for many years.

Ransomware changed the game because it made timing a critical part of malware detection. Other types of malware might try to steal intellectual property or start a spambot. Catching them an hour or so after first infection – having vastly minimised the chance of false positives first – may have been an acceptable trade-off. With ransomware, however, there is no room for manoeuvre. The moment it encrypts files and locks victims out of their data, it starts to cause financial damage and business disruption. Catching it at 'time zero' is critical.

Around the same time as ransomware started becoming prominent, 'next-generation' vendors began actively promoting machine learning in their endpoint security products. It makes sense to harness artificial systems to recognise malware in a climate where threats are multiplying faster than ever. But getting this right, and minimising false positive errors in the process, is not trivial.

The fact is, machine learning is ideal for tackling those critical 'time zero' issues like ransomware, but it still leaves the possibility of false positives. Machine learning is best used after other security methods have been applied – and further meta data about the context of the file has been collected. Machine learning is excellent for processing files where the context suggests that they are more suspicious such as those files that arrive via email, downloads or infected USB sticks. Other security layers, a dynamic whitelist and context can be used to make sure that the machine learning is given minimal opportunity to mistakenly flag good files as false positives.

The volume of good and bad files to scan is increasing exponentially. Clearly, we need to augment our current systems of detection to cope with this level of activity. Historically, malware detection has looked in the rear-view mirror. The industry needed a virus sample before it could develop an antidote. But many malware samples we get today are unique. For example, a new instance of the Cerber ransomware is created every 15 seconds. It tells us how profitable ransomware must be, that cybercriminals think this is worth the effort. The thing is, we have seen a similar effect at work with benevolent software too. The growth of DevOps and the cloud model means that new versions of legitimate software such as Google or Dropbox updates appear on an almost hourly basis.

Driving by looking backwards is impossible when the terrain changes so fast. We need machine learning, and ultimately, artificial intelligence, to change that paradigm by protecting against threats we have not yet seen.

The more extreme marketing hype around machine learning would have you believe that its amazing formulas give no false positives; that machine learning is a magic black box that provides all the security you need in a single layer. Our take is that machine learning is very useful when it interoperates carefully with other layers to mitigate risks like false positives, or to enhance whitelists.

Our product set uses XGen security, which is Trend Micro's blended approach of defence techniques that includes – but is not limited to – machine learning. When scanning files, the toolset applies traditional techniques to identify known good and known malicious files. Further pruning is done using the context of the files and meta data about the files leaving a small subset of files. We process these remaining suspicious files with machine learning, so we only apply it to a subset of the total number of files.

Gartner has validated our approach, placing Trend Micro highest and furthest in the leader's quadrant for "ability to execute" and "completeness of vision" in its 2017 Magic Quadrant for Endpoint Protection Platforms.

I am a huge advocate for machine learning, but no one solution will solve all security problems — it never has. We have seen some cybercriminals already experimenting with modifying programs to beat machine learning. That is another reason why a defence-in-depth approach ensures that nothing malicious gets missed. A multi-layered approach is far more effective at providing a defensive posture which is hard to attack.

Jonathan Oliver
Senior Data Scientist and Director, Trend Micro

"The moment ransomware encrypts files and locks victims out of their data, it starts to cause financial damage and business disruption. Catching it at 'time zero' is critical"

TREND MICRO NAMED A LEADER AGAIN IN GARTNER MAGIC QUADRANT FOR ENDPOINT PROTECTION PLATFORMS

The endpoint security market is dynamic, with new entrants and ongoing innovation for improving threat detection and response. In the midst of all this market energy we are pleased to be named a Leader in Gartner's 2018 Magic Quadrant for Endpoint Protection Platforms (EPP)[1]. Trend Micro has been recognized as a leader since this Magic Quadrant started back in 2002 (first called Enterprise Antivirus).

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (January 2018)

Since the early days of the Gartner Magic Quadrant for this category, there have been successive waves of innovation. Back in 2002, integrated firewalls captured the market's (and Gartner's) attention. Over the years, we've seen technologies, such as full disk encryption, data loss prevention (DLP), behavioral detection, application control, and more recently, machine learning, as effective new ways to protect endpoints, detect threats and give security teams peace of mind. Trend Micro has consistently been part of these innovation waves.

It's clear that the market is excited about Endpoint Detection & Response (EDR). There are two drivers for this, and we are committed to delivering effective solutions in both areas:

BETTER DETECTION AND AUTOMATED RESPONSE:

EDR's investigative capabilities are useful, but the only way it's manageable is if automated threat detection is effective and accurate, followed by rapid automated neutralization (quarantine, isolation, rollback of damaged files, etc.). Trend Micro has a powerful capability set that is built into our core **EPP** agent, including behavioral detection methods and two powerful machine learning engines (one at pre-execution time, and one working at runtime to help spot stealthier ransomware and file-less threats). Today, very few vendors are using machine learning for runtime detection. In the last two years, Trend Micro has detected and intercepted 1.7 billion ransomware threats,[2] using its cross-generational blend of techniques, a reason why we consistently perform well in independent third-party testing.

INVESTIGATION

After successful detection and response, after a missed detection, or for hunting purposes, EDR's investigative capabilities bring a lot of value. Trend Micro **Endpoint Sensor** delivers strong investigative capabilities to complement the detection and response functionality of our core endpoint solution. (And, we'll be packaging the investigative features into the endpoint agent during 2018 to simplify deployment).

The downside of EDR's investigative capability is that it typically requires an analyst with specialized skills to operate it from day to day. Many organizations don't have the resources to staff these positions, so we expect a strong future for Managed Detection and Response (MDR) where the investigation and hunting skills can be delivered via SaaS offering.

We're committed to continuing to work hard for our global customer base, delivering effective threat detection and response, and investigation capability that fits our customers' requirements. And we know that to earn our position in the Leaders' Quadrant, we need to continue executing well on our product quality and service delivery.

There is always noise in the market, and the last couple of years have been especially deafening, with new VC investments in the industry, and ransomware being driven by a viable business model. Enterprises face a challenge when trying to assess solutions, with marketing from vendors all sounding the same. Gartner's framework and analysis helps cut through the noise. What else can customers use to help frame their decisions? Two words: independent testing. While it's great for vendors to talk about cutting-edge techniques, enterprises want to know if the techniques actually work. Trend Micro supports steady improvements to the transparency and methodology of independent third-party testing. We urge the vendor community and customers to continue investing in testing approaches that address the #1 customer pain: threat detection.

For additional information on Gartner's Magic Quadrant for Endpoint Protection Platforms, please visit:
https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html

[1] Gartner, "Magic Quadrant for Endpoint Protection Platforms," Ian McShane, Avivah Litan, Eric Ouellet, Prateek Bhajanka; 24 January 2018.
[2] Source: TrendLabs, Jan 2017

TREND MICRO™

Securing Your Connected World

Enterprise Security

SOLUTIONS OVERVIEW

Constant IT change is the new normal for organizations and businesses; changes that are empowering us with better and more efficient use of their most important asset – information. However, three important trends in today's evolving IT landscape are also creating some of the most pressing challenges for enterprises:

Cloud and Virtualization: The growing use of cloud-based and virtualized computing drives dramatic efficiency and operational gains. But how do you evolve security strategies to fit these environments to ensure performance is not sacrificed and security gaps are not created?

Complex Networks: The enterprise boundary is gone, with networks extending far beyond the traditional LANs and WANs. Wifi, remote access, branch offices, and the cloud are giving enterprises more flexibility and productivity. Today there are more points to protect than ever, so how do you evolve your network security to go beyond perimeter defenses and also detect lateral movement within networks?

Consumerization: The explosion of endpoints is boosting productivity– giving flexibility and mobility to users like never before, but with the introduction of multiple devices and cloud-based applications such as Dropbox™ and Gmail at work, how do you re-think traditional defenses?

As technology changes, security technology has to evolve to keep up with threats. New environments require new ways of thinking about security to ensure there are no vulnerabilities and that performance is not compromised. Threat actors constantly look for ways to penetrate these new environments, while creating more sophisticated threats.

The Sophistication of Cyber Threats

In the early days, the threat landscape was black and white – requiring the ability to quickly and efficiently determine the known good and known bad. Classic techniques like anti-malware and content filtering were sufficient to detect and block known bad files, URLs, and spam. These highly efficient techniques remain critical for eliminating the high volume of known bad threats still active today. Since there is an increase in stealthier and more sophisticated unknown threats, the 'grey' areas like targeted attacks, zero-day exploits, ransomware, and business email compromise, require more advanced threat defense techniques.

While some "next gen" offerings rely solely on one technique like behavioral analysis or machine learning, we believe that when it comes to defending your organization against the full range of known and unknown threats, there is no silver bullet. Your enterprise needs trusted solutions that can help solve multiple concerns.

Trend Micro XGen™ security

Trend Micro solutions are powered by **XGen™ security** that is:

- **Smart:** Protects against the full range of known and unknown threats using a cross-generational blend of threat defense techniques that applies the right technique at the right time, and is powered by global threat intelligence
- **Optimized:** Delivers security solutions to protect users, networks, and hybrid cloud environments – all designed specifically for and tightly integrated with leading platforms and applications, like VMware, Amazon Web Services (AWS), Microsoft® Azure™, Google Cloud, Office365, and more
- **Connected:** Speeds time to response with automatic sharing of threat intelligence across security layers and centralized visibility and control

XGen™ security uses proven techniques to quickly identify **known** good or bad data, freeing advanced techniques to more quickly and accurately identify **unknown** threats. This identification in rapid succession with right-time technology regardless of location and device across a connected system, maximizes both visibility and performance. This core set of techniques powers each of the Trend Micro solutions, in a way that is optimized for each layer of security: hybrid clouds, networks, and user environments.

Maximum Security with Minimum Impact

Trend Micro offers a truly smart, optimized, and connected threat defense – all powered by XGen™ security. The cross-generational blend of threat defense techniques protects against the ever-changing threat landscape, providing maximum security with minimum impact.

HYBRID CLOUD SECURITY

Comprehensive server security provides adaptive protection for systems and applications across physical, virtual, cloud, and hybrid cloud deployments. Data center operators and architects can control operating costs while improving performance with security optimized for VMware® virtual environments. Cloud architects can meet shared security requirements when deploying sensitive applications to the cloud. Our elastic security enables the full benefit of the cloud's agility and cost savings on the leading cloud service providers' platforms, including Amazon Web Services (AWS) and Microsoft® Azure™.

- **Trend Micro™ Deep Security™**, available as software, as a service, or through the AWS and Azure marketplaces, provides comprehensive server and virtual desktop protection for physical, virtual, cloud, and hybrid deployments. Centrally managed through an intuitive dashboard, Deep Security includes anti-malware with web reputation, network security through intrusion prevention (IPS) and firewall, and system security through integrity monitoring and log inspection.
  - **Trend Micro Deep Security as a Service** is a cloud-hosted solution designed specifically for customers using AWS, Azure, Google Cloud, and VMware vCloud® Air™.

NETWORK DEFENSE AGAINST TARGETED ATTACKS

The Trend Micro Network Defense is a family of security solutions that enable you to rapidly detect, analyze, and respond to targeted attacks and advanced threats.

- **Trend Micro™ Deep Discovery™** is an advanced threat protection platform that enables you to detect, analyze, and respond to stealthy, targeted attacks. It uses specialized detection engines, custom sandboxing and global threat intelligence from the Trend Micro™ Smart Protection Network™ to defend against attacks that are invisible to standard security products. Deep Discovery uniquely detects and identifies evasive threats in real time, then provides the in-depth analysis and relevant actionable intelligence that will protect your organization from attack.
- **TippingPoint Next-Generation Intrusion Prevention System and Advanced Threat Protection**

  Proven wire-speed Next-Generation Intrusion Prevention System proactively detects and prevents vulnerabilities, network exploits, and delivers identity and application awareness to enable contextual visibility and enforcement.

  Integrated network-wide breach detection identifies targeted attacks and advanced threats, including proactive threat prevention through integration with the TippingPoint Next-Generation Intrusion Prevention System, Trend Micro, and third-party security investments.

ANALYSTS, CUSTOMERS, AND TEST LABS AGREE: TREND MICRO LEADS IN ENTERPRISE SECURITY

Hybrid Cloud Security

IDC *Analyze the Future*

Trend Micro is the global market leader in server security[1]

[1] IDC, Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind, #US41867116, November 2016

Network Defense

NSS LABS RECOMMENDED
RECOMMENDED
Breach Detection System
3 YEARS IN A ROW
99.8% Detection Rate

NSS Labs, Breach Detection Systems Test Report 2016 – Trend Micro Deep Discovery Inspector

"The best working technology is the one that's most transparent to users. Deep Discovery has been remarkably robust, even while handling a huge volume of traffic."

David Shipley, Head of Technology Management, University of New Brunswick

TippingPoint

NSS LABS RECOMMENDED
TippingPoint
RECOMMENDED
Next-Generation IPS
99.5% Security Effectiveness

USER PROTECTION

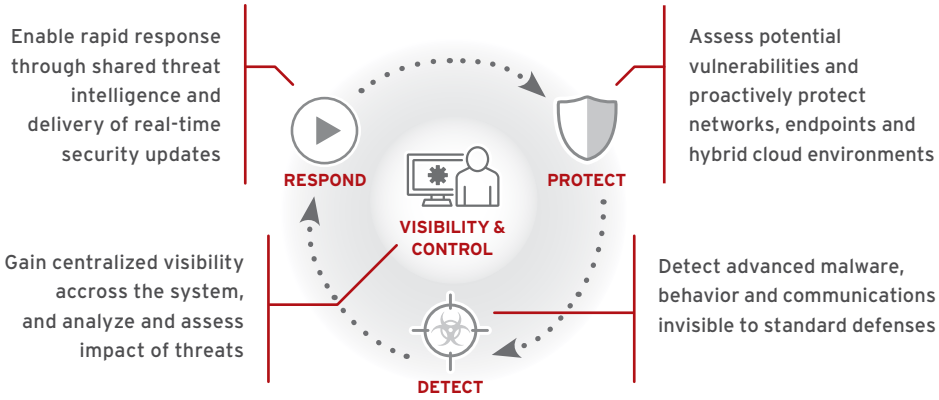
Our interconnected suite of security protects your users no matter where they are going or what they are doing. Core to the suites is endpoint security that infuses high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across any user activity.

- **Trend Micro™ Smart Protection Complete** is a software suite that delivers the best protection at multiple layers, supports flexible on-premises, cloud and hybrid deployment models, and lets you manage users across multiple threat vectors from a single pane of glass with a complete view of your security. Includes endpoint security, mobile security, secure web gateway, email and collaboration security, integrated data loss prevention, and centralized management.
- **Trend Micro™ Smart Protection for Endpoints** is a software suite that protects virtual and physical desktops with multiple layers of threat and data security across devices and applications. Features cloud flexibility and user-centric visibility supported by a full range of endpoint security, integrated data loss prevention, and centralized management.

CONNECTED THREAT DEFENSE

Trend Micro Connected Threat Defense—a layered approach to security that gives you a better way to quickly protect, detect, and respond to new threats that are targeting you, while improving your visibility and control across your organization at the same time.

Connected Threat Defense: Better, Faster Protection



User Protection

Gartner has positioned Trend Micro as a Leader in the Magic Quadrant for Endpoint Protection Platforms since 2002.[2]

2 - Gartner "Magic Quadrant for Endpoint Protection Platforms," by Eric Ouellet, Ian McShane, January 2017

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Trend Micro named a leader in The Forrester Wave™: Endpoint Security Suites, Q4 2016

FORRESTER WAVE LEADER 2016 Endpoint Security Suites

"In the last few years, we've really moved the needle on security. Trend Micro increases our competence and lets our customers see us as a trusted partner."

William Crank, Chief Information Security Officer, Medhost

CENTRALIZED MANAGEMENT AND REPORTING

Simplify administration, improve security intelligence, and lower security management costs with an integrated, centrally managed security framework.

- **Trend Micro™ Control Manager™** software provides a central platform to manage the configuration, policies, and operation of Trend Micro enterprise security products.

SUPPORT SERVICES

Trend Micro provides a wide assortment of support services to help ensure that you get the most value from your security investment. Two levels of technical support are available.

- **Standard Support** includes all regular product updates and upgrades, along with highly responsive, expert telephone support during regular business hours, and 24x7 telephone support for critical issues.
- **Premium Support** provides you with a named Customer Service Manager who will be your on-going contact to assist you with urgent issues and provide expert guidance designed to elevate your security posture.

www.trendmicro.com/enterprise

TREND MICRO™

Securing Your Journey to the Cloud

Trend Micro Inc., 225 E John Carpenter Freeway,
Suite 1500, Irving, Texas 75062
Phone: (817) 569-8900 Toll-free: (888) 762-8736

SOLUTION BRIEF

Trend Micro

HYBRID CLOUD SECURITY

Secure virtual, cloud, physical, and hybrid environments easily and effectively

INTRODUCTION

As you take advantage of the operational and economic benefits of virtualization and the cloud, it's critical to secure your virtualized data centers, cloud deployments, and hybrid environments effectively. If you neglect any aspect of security, you leave gaps that open the door to web threats and serious data breaches. And, to meet data privacy and compliance regulations, you will need to demonstrate that you have the appropriate security, regardless of your computing environment.

Trend Micro Hybrid Cloud Security solutions protect applications and data and prevent business disruptions, while helping to ensure regulatory compliance. Whether you are focused on securing physical or virtual environments, cloud instances, or web applications, Trend Micro provides the advanced server security you need for virtual, cloud, and physical servers via the Trend Micro™ Deep Security™ platform.

Trend Micro is the **#1 provider of server security for physical, virtual, and cloud environments**[1]— combining the most complete set of security capabilities with automated management to dramatically reduce both risk and cost.

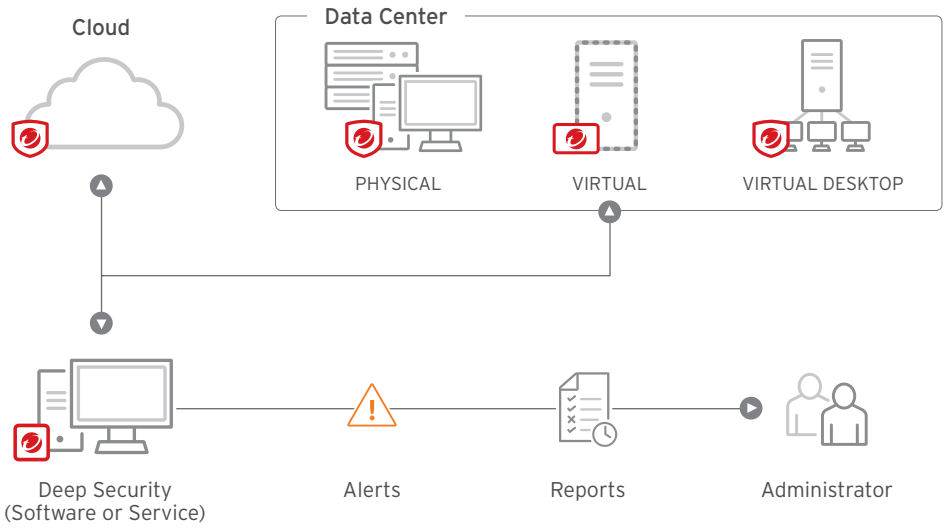
[1] IDC, Worldwide Endpoint Security Market Shares: Success of Midsize Vendors, #US40546915, Figure 5, Dec 2015

Why Trend Micro for hybrid cloud security?

- Secures physical, virtual, and cloud environments with one comprehensive solution
- Provides the most complete set of security capabilities available from the global market share leader in server security
- Saves resources/reduces costs with automated policy and lifecycle management with optimized security
- Available as software or as-a-service with central management across hybrid environments

DEEP SECURITY

With a single, comprehensive security solution, deployment and management are much faster and easier as you transition from physical and virtual environments to the cloud. Centralized management and vulnerability shielding help you save time and resources. Furthermore, our deep integration with VMWare optimizes virtual server performance without compromising on security.



Deep Security Agent
Deep Security Manager
Deep Security Virtual Appliance

> "Deep Security has been a very good fit in our data center and provides excellent protection for our virtualized servers and desktops and our continually changing environment. I love it."
>
> **Orinzal Williams**
> Executive Director
> United Way of Atlanta
> Georgia, US

TREND MICRO HYBRID CLOUD SECURITY SOLUTIONS

PROVEN VIRTUALIZATION SECURITY

Optimized security for the modern data center helps data center operators and architects control operating costs while improving performance with security optimized for virtual environments. Decrease risk, costs, and save time with automatic policy management, hypervisor-based security and central management.

ELASTIC CLOUD SECURITY

Automated security for the Cloud helps cloud architects meet shared security responsibility when deploying sensitive applications to the cloud. It provides elastic security for dynamic workflows running in Amazon Web Services (AWS), Microsoft Azure, and VMware vCloud Air.

> "I did the Deep Security deployment myself—it was less than a day for the roll out across 100 virtual machines. Overnight, I saw our memory resource utilization go down by 27 percent."
>
> **Nick Casagrande**
> Director of IT
> Southern Waste Systems LLC
> Florida, US

OPTIMIZED SECURITY FOR THE MODERN DATA CENTER

Trend Micro's market-leading security protects virtual desktops and servers, cloud, and hybrid architectures against zero-day malware and other threats while minimizing operational impact from resource inefficiencies and emergency patching.

Provisions full security capabilities automatically in the data center

To reap the benefits of virtualization and be efficient, a security solution built for virtual environments must be automated as part of the data center provisioning process. Trend Micro not only ensures physical servers and virtual machines (VMs) are protected the moment they are provisioned, it also recommends and applies only the policies that are relevant. Deep Security fits dynamic environments, by following VMs as they are brought up and down.

Deep Security's capabilities include:

- Anti-malware with web reputation to protect against constant malware attacks
- Network security, including intrusion detection and protection (IDS/IPS) to shield unpatched vulnerabilities, as well as a stateful firewall to provide a customizable perimeter around each server
- System security, including file and system integrity monitoring for compliance, as well as log inspection to identify and report important security events

Optimizes data center resources

Deep Security takes a better approach with hypervisor-based security. It is deployed at the hypervisor level so there is no need to install and manage a separate agent on every VM. This also means that individual servers and VMs are not cluttered with signature libraries and detection engines, which leads to tremendous improvements in management, network usage, speed of scans, host-wide CPU and memory usage, input/output operations per second (IOPS), and overall storage.

This central architecture also makes it possible to have a scan cache. The scan cache eliminates duplication in scanning across similar VMs, which can dramatically improve performance. Full scans complete up to 20 times faster, real-time scanning up to five times faster, and even faster logins for VDI.

To further simplify provisioning, Trend Micro solutions take advantage of the latest VMware platform innovations. Our tight integration with VMware allows automatic protection of new virtual machines as they are brought up, while automatically provisioning appropriate security policy and ensuring no security gaps.

This hypervisor-based approach is continued in the new NSX platform from VMware to ensure these performance advantages are preserved as organizations begin to migrate to the new architecture.

Manages security efficiently, even while transitioning to new environments

Managing security is easy with a single dashboard that allows continuous monitoring of multiple controls across physical, virtual, and cloud environments. Robust reporting and alerting help you focus on what's important so you can quickly identify issues and respond accordingly. Easy integration with other systems, such as SIEM, help incorporate security management as part of other data center operations. All controls are managed through a single virtual appliance so there is no need to manually keep agents up to date—an especially difficult task when rapidly scaling your operations. The dashboard includes information from cloud environments such as Amazon Web Services (AWS), Microsoft Azure, and VMware vCloud Air, making it painless to manage all your servers, regardless of location, from one central tool.

Achieves cost-effective compliance

Major compliance requirements for PCI DSS 3.1, as well as HIPAA, NIST, and SSAE 16 are addressed with:

- **Detailed, auditable reports** that document prevented vulnerabilities, detected attacks, and policy compliance status
- **Reduced preparation time and effort** required to support audits through centralized security controls and consolidated reporting
- **Support for internal compliance initiatives** to increase visibility of internal network activity
- **Proven technology** certified to Common Criteria EAL4+

Future proof your VMware investment with NSX

Organizations currently using VMware, and considering migrating to NSX, can take advantage of Trend Micro's unique ability to provide a single security solution to manage both current and future deployments. Trend Micro's modern data center security supports NSX with a comprehensive security platform designed to provide server, application, and data security across physical, virtual, and cloud servers.

AUTOMATED SECURITY FOR THE CLOUD

Cloud adoption is accelerating rapidly, driven by the cost savings, agility, and other advantages it offers. As you transition to the cloud, you must take care to ensure that you implement adequate security under the shared security responsibility model, and that your security solution meets internal and regulatory compliance rules.

Trend Micro Deep Security is optimized for leading cloud service providers (CSPs) including AWS, Microsoft Azure, and VMware vCloud Air. Deep Security makes using leading orchestration tools like Chef, Puppet, Salt, and Opworks easy, providing automated generation of policy scripts that enable security to be managed as part of cloud operations.

Prevents data breaches and business disruptions

Already selected by thousands of global customers to protect millions of servers, Trend Micro's market leading security capabilities help organizations to:

- Defend against network and application threats, leveraging proven host-based network security controls like Intrusion Detection & Protection (IDS/IPS)
- Protect against vulnerabilities, instantly shielding vulnerable applications and servers with a 'virtual patch' until a workload can be replaced
- Keep malware of workloads, ensuring that servers and applications are protected
- Identify suspicious changes on servers, including registry settings, system folders, and application files that shouldn't change

Reduces operational costs

Trend Micro provides advanced server security for cloud instances while simultaneously managing security on virtual and physical servers in the data center.

The integrated administrative console gives you a single, up-to-date view of the security posture for your entire cloud environment, reducing time and resource costs by making security management more efficient. Automated vulnerability shielding prevents the disruption of emergency patching.

In addition, Deep Security's tight integration with both AWS and Azure allows specific customizable policy templates to be applied based on instance metadata, ensuring the right policies are applied to the right servers automatically.

Achieves cost-effective compliance

Major compliance requirements for PCI DSS 3.1, as well as HIPAA, NIST, and SSAE 16 are addressed with:

- **Detailed, auditable reports** that document prevented vulnerabilities, detected attacks, and policy compliance status
- **Reduced preparation time and effort** required to support audits through centralized security controls and consolidated reporting
- **Support of internal compliance initiatives** to increase visibility of internal network activity
- **Proven technology** certified to Common Criteria EAL4+
- **Comprehensive set of tools** to eliminate need for multiple vendors

To learn more about our cloud and data center security solutions or to take a test drive, visit trendmicro.com/hybridcloud

> "Businesses face ever-growing and ever-changing threats on the Internet. By blocking threats, Deep Security protects the online experiences of our customers. This upholds our reputation and theirs."

Todd Redfoot
Chief Information Security Officer (CISO) at Go Daddy

TREND MICRO™

Securing Your Journey to the Cloud

Now available on aws marketplace Windows Azure Marketplace

Trend Micro™

SMART PROTECTION COMPLETE

Maximum Trend Micro™ XGen™ endpoint security from your proven security partner

Traditional security solutions can't keep up with today's threats. Turning to multiple point products to address the myriad of challenges only increases complexity, slows your users, and may leave gaps in your security. To further complicate matters, you're moving to the cloud and need flexible security deployment options that will adapt as your needs change. You need multidimensional security that consolidates your view across all layers of protection and all deployment models.

Trend Micro™ Smart Protection Complete is a connected suite of security capabilities that protects your users no matter where they go or what they do. This modern security delivers the best protection at multiple layers: endpoint, application, and network, which work together to stop threats across your organization. Core to the suite is XGen™ endpoint security that infuses high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across any user activity. Plus, you can evolve your protection along with your business using flexible on-premises, cloud, and hybrid deployment models that fit your IT environment today and tomorrow. Administrative overhead is minimized with central management across multiple threat vectors from a single "pane of glass," giving you complete visibility of the security of your environment.

Multiple layers of connected threat protection

This comprehensive suite integrates security across protection layers with flexible cloud deployment, simplified licensing, and central management for network-wide visibility and control of threats and data. The following layers of security are included in this suite:

- **ENDPOINT SECURITY.** XGen™ endpoint security synthesizes machine learning with other techniques for maximum protection. Secure user activity on physical and virtual desktops, laptops, or mobile devices with threat and data protection, application control, vulnerability protection, and encryption.
- **MOBILE SECURITY.** Secure, track, monitor, and manage your employees' mobile devices and company data with mobile security that balances consumerization with IT control.
- **EMAIL AND COLLABORATION SECURITY.** Get superior protection against spam, phishing, malware, and targeted attacks at the mail server, gateway, and for cloud-based applications like Office 365.
- **WEB SECURITY.** Protect your users' web activity on any device in any location. They gain secure access to the latest web and social media applications, and you get complete visibility and control of employee web usage in a cloud-based SaaS or on-site secure web gateway solution.
- **CENTRALIZED SECURITY MANAGEMENT.** Manage multiple layers of connected threat and data protection for complete, user-centric visibility across the entire threat life cycle.

Protection Points

- Endpoints
- Smartphones and tablets
- USB and removable drives
- Mail servers
- File servers
- Messaging gateway
- Web gateway
- Collaboration portals
- IM servers
- Cloud email and file sharing

Threat and Data Protection

- Ransomware
- Unknown malware
- Targeted attacks
- Endpoint firewall and host intrusion prevention
- Vulnerability shielding
- Application control
- Inappropriate content
- Phishing attacks
- Spam and bots
- Spyware and rootkits
- Virus and Trojan malware
- Web threats

Data Protection and Compliance

- Compliance risks
- Lost devices
- Accidental data loss
- Data theft

Key Benefits

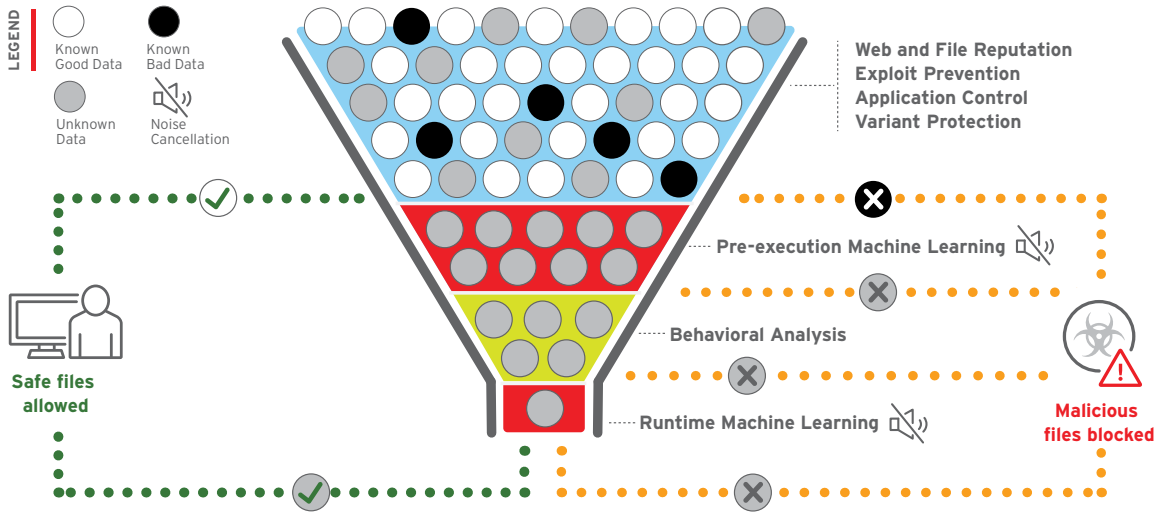
- Regain control of your end-user IT environment by centralizing threat and data protection across security layers
- Stops ransomware from encrypting your endpoints
- Block zero-day malware with signature-less techniques
- Enable your users to securely work from the platforms they find most productive
- Protect data with no increase in management or client footprint
- Minimize risks with any mix of real-time, proactive cloud-based security
- Reduce management complexity and overall costs

ADVANTAGES

Maximum Protection

XGen™ endpoint security

Infuses high-fidelity machine learning with other detection techniques for the broadest protection against ransomware and advanced attacks



- Progressively filters out threats using the most efficient technique for maximum detection without false positives.
- Blends signature-less techniques including machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good-file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking.
- High-fidelity machine learning uses both pre-execution and run-time analysis, unlike other machine learning vendors who only use one technique.
- Deploys noise cancellation techniques like census and whitelist checking at each layer to reduce false positives.
- Leverages Trend Micro's 11 years of experience using machine learning in spam filtering and website analysis.

Data Protection

- Safeguards data with full disk, file, and folder encryption to keep data private.
- Device control to prevent information from moving to where it doesn't belong, such as USB memory sticks or cloud storage.
- Mobile security secures your employees' mobile devices and company data with mobile device management (MDM) and data protection.
- Integrated, template-based Data Loss Prevention (DLP) to protect sensitive data across endpoint, web, email, and SaaS apps.

Email and Web Protection

- Consistently top rated email security stops targeted email attacks, spam, phishing, ransomware, and unknown malware from impacting your business.
- Stops threats before they reach users with advanced detection techniques including document exploit detection and sandbox malware analysis.
- Security for the email server, gateway, collaboration portal, instant messaging, and cloud-based applications such as Office 365.
- Secure web gateway protects users from web-borne threats and provides granular control and visibility of web usage.

Connect Threat Defense

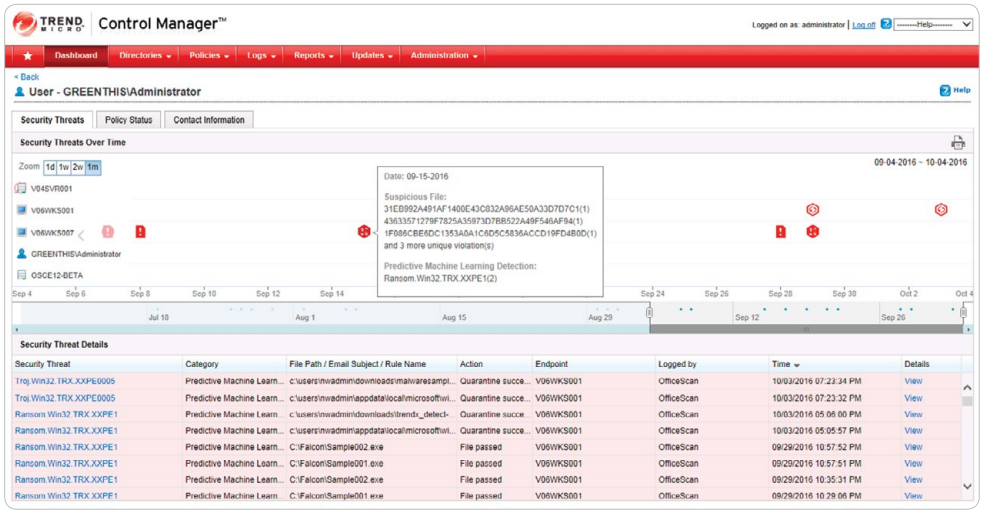
- Instantly share information on suspicious network activity and files with other security layers to stop subsequent attacks.
- Reduce time to protect against emerging and targeted attacks.

Minimum Impact

Data Protection

High performance and accurate detection:

- Lightweight and optimized security uses the right detection technique at the right time to ensure minimal impact on devices and network.
- Multiple methods and checks against false positives reduce IT help desk calls.



Central management and visibility:

- Comprehensive central view of user security lets you quickly and efficiently analyze data and threats across the whole solution.
- User-centric visibility across both cloud and on-premises allows you to easily understand how threats are affecting a particular user across multiple systems.
- Automatic sharing of threat intelligence across security layers enables protection from emerging threats across the whole organization.
- Customizable dashboards to fit different administration responsibilities.

Flexible management and licensing:

- Flexibility to deploy endpoint security the way that best supports your changing business models—on-premises, in the cloud.
- Mix and match cloud or on-premises products without a change to the commercial agreement.

Outstanding support

- 24x7 support means that if a problem arises, Trend Micro is there to resolve it quickly.

Proven Security Partner

Trend Micro has a history of constantly innovating to provide the most effective and efficient security technologies.
We are always looking ahead to develop the technology needed to fight tomorrow's ever changing threats.

- Over 25 years of security innovation
- Protects over 155 million endpoints
- Trusted by 45 of the top 50 global corporations
- A Leader since 2002 in the Gartner Magic Quadrant for Endpoint Protection Platforms and placed furthest to the right in "Completeness of Vision" for 2016

TREND MICRO SMART PROTECTION COMPLETE

Build a solid security foundation across your network for complete end-user protection with broad platform support that provides security for heterogeneous environments and protection for your unique network configuration.

SUITE COMPONENTS

MULTILAYERED PROTECTION	PLATFORM COVERAGE	ADVANTAGE
Central Management		
Control Manager	Software: Windows	Centrally manages security
Endpoint Security		
OfficeScan	Software: Windows, Apple Macintosh	Proactive threat protection infused with machine learning for physical and virtual Windows clients. An expandable plug-in architecture that is deployed and managed from a single console.
Vulnerability Protection	Software: Windows	Shield against vulnerabilities in operating systems and client applications with a network-level Host Intrusion Prevention System (HIPS).
Endpoint Application Control	Software: Windows	Safeguard your data and machines against unauthorized access and user error, and lock down endpoints to prevent unwanted and unknown applications from being executed. Dynamic whitelisting and system lockdown.
Endpoint Encryption	PCs, laptops, CDs, DVDs, and USB	Secure data stored on PCs, laptops, CDs, DVDs, and USB drives with full disk, folder, file, and removable media encryption with multi-OS key management and policies.
Worry-Free Services	Cloud-based SaaS	Proactive SaaS managed threat protection for Windows, Mac, and Android clients.
Server Protect	Windows/Netware, Linux	Keeps malware out of file servers.
Mobile Security		
Mobile Security	iOS, Android, Blackberry, Symbian, and Windows Mobile	Mobile Device Management (MDM), data security, mobile antimalware and web security, and application management.
Email and Collaboration Security		
Hosted Email Security	Cloud-based SaaS: protects email traffic to cloud or on-premises email systems	Continuously updated protection stops spam and viruses before the network.
Cloud App Security	Cloud-based SaaS: Office 365 email, SharePoint Online, Box for Business, Dropbox for Business, Google Drive	Strengthens Office 365 security with sandbox malware analysis and data loss prevention. Protects file sharing from malware and compliance risks.
InterScan Messaging Security	• Software Virtual Appliance: VMware, Hyper-V, Software Appliance • Software: Windows, Linux	Safeguards the email gateway from spam and other email threats.
ScanMail Suite for Microsoft Exchange	Software: Windows	Blocks spam, malware, and other email threats at the mail server.
ScanMail Suite for IBM Domino	• Software: Windows, Linux for x86, IBM AIX, IBM i5 OS, Sun • Solaris™, Linux on IBM® zSeries, IBM z/OS	Blocks spam, malware, and other email threats at the mail server.
PortalProtect for Microsoft SharePoint	Software: Windows on SharePoint server	Secure your collaborations in SharePoint against malware, web threats, and compliance risks.
IM Security for Microsoft Lync	Software: Windows on Lync server	Safeguard IM communications against malware, web threats, and compliance risks.
Secure Web Gateway		
InterScan Web Security	• Software Virtual Appliance: VMware, Hyper-V, Software Appliance • Cloud-based SaaS	Secure your users' web activity. Features leading anti-malware and real-time web reputation. Provides complete visibility and control with granular application control, flexible URL filtering, and comprehensive reporting.
Integrated Data Protection		
Data Loss Prevention	Integrated across endpoints, email and collaboration, and secure web gateway	Enforces DLP policies across the enterprise using simple and customizable templates.

TREND MICRO™

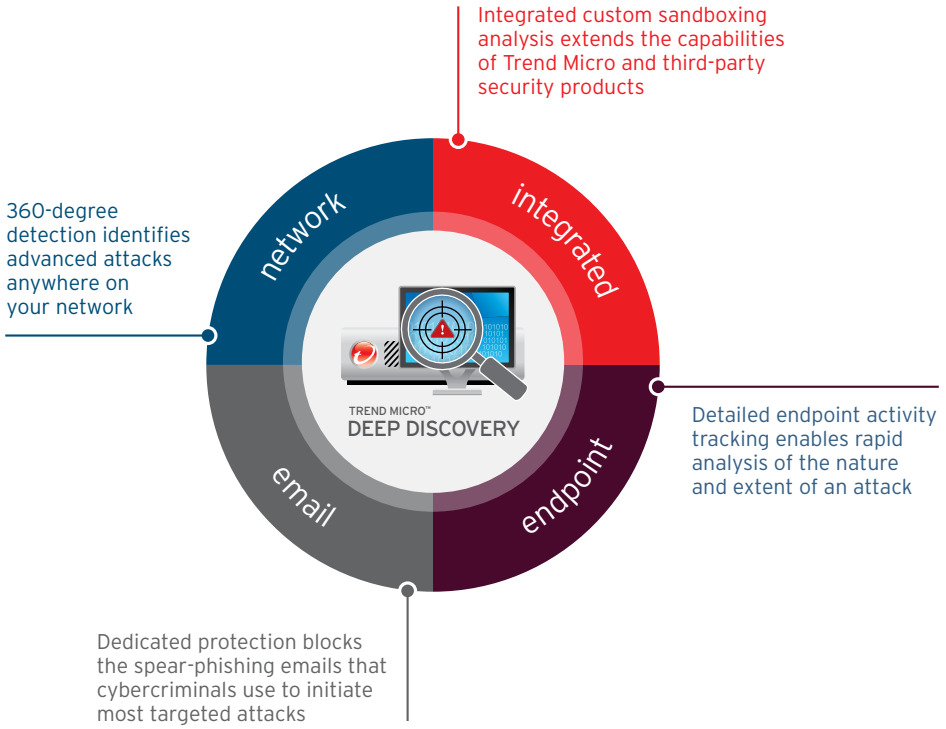
Securing Your Journey to the Cloud

Trend Micro™

DEEP DISCOVERY

Advanced Threat Protection Against Targeted Attacks

Trend Micro Deep Discovery is an advanced threat protection platform that enables you to detect, analyze, and respond to today's stealthy, targeted attacks. Using specialized detection engines, custom sandboxing, and global threat intelligence from the Trend Micro™ Smart Protection Network™, Deep Discovery defends against attacks that are invisible to standard security products. Deployed individually or as an integrated solution, Deep Discovery solutions for network, email, endpoint, and integrated protection provide advanced threat protection where it matters most to your organization.



Key Benefits

Protection Against Attacks
Unique threat detection technologies discover attacks before the damage is done.

A Single Platform. A Range of Solutions
Deploy advanced threat protection where it matters most to your organization.

Intelligence for a Rapid Response
Deep Discovery and global threat intelligence drive a rapid and effective response.

The Trend Micro Custom Defense

Unite your entire security infrastructure into a real-time defense against targeted attacks. Deep Discovery detection and intelligence sharing is the foundation of the Custom Defense, enabling you to rapidly detect, analyze, and respond to your attackers.

NSS Labs RECOMMENDED
Trend Micro™ Deep Discovery
TOP SCORE
in breach detection
NSS Labs 2014 Breach Detection Tests

THE DEEP DISCOVERY PLATFORM: KEY FEATURES

Advanced Threat Detection
Identifies attacks anywhere on your network using specialized detection engines, correlation rules, and custom sandboxing.

Custom Sandboxing
Uses virtual environments that precisely match your system configurations to detect the threats that target your organization.

Smart Protection Network Intelligence
Leverages real-time, cloud-based security intelligence for threat detection and in-depth attack investigation.

Custom Defense Integration
Shares IOC detection intelligence with other Trend Micro and third-party security products to stop further attacks.

NETWORK ATTACK DETECTION

Defend against attacks invisible to standard security solutions

TREND MICRO™ DEEP DISCOVERY INSPECTOR is a network appliance that monitors traffic across all ports and more than 80 protocols and applications. Using specialized detection engines and custom sandboxing, it identifies the malware, C&C, and activities signaling an attempted attack. Detection intelligence aids your rapid response and is automatically shared with your other security products to block further attack.

EMAIL ATTACK PROTECTION

Stop the spear-phishing attacks that lead to a data breach

TREND MICRO™ DEEP DISCOVERY EMAIL INSPECTOR is an email security appliance that uses advanced malware detection techniques and custom sandboxing to identify and block the spear-phishing emails that are the initial phase of most targeted attacks. It adds a transparent email inspection layer that discovers malicious content, attachments, and URL links that pass unnoticed through standard email security.

ENDPOINT ATTACK DETECTION

Investigate and respond to attacks with endpoint and server intelligence

TREND MICRO™ DEEP DISCOVERY ENDPOINT SENSOR is a context-aware endpoint security monitor that records and reports detailed system activities to allow threat analysts to rapidly assess the nature and extent of an attack. Indicators of compromise (IOC) intelligence from Deep Discovery and other sources can be used to search endpoints to verify infiltrations and discover the full context and timeline of an attack.

INTEGRATED ATTACK PROTECTION

Improve the threat protection of your existing security investments

TREND MICRO™ DEEP DISCOVERY ANALYZER is an open custom sandbox analysis server that enhances the malware detection capabilities of all your security products. The Analyzer supports out-of-the-box integration with many Trend Micro products, manual sample submission, and an open Web Services interface to allow any product or process to submit samples and obtain results.

CENTRALIZED MANAGEMENT AND INVESTIGATION

Assess, prioritize, and investigate attacks with Trend Micro or SIEM systems

TREND MICRO CONTROL MANAGER provides centralized views, threat investigation, and reporting across Inspector units, as well as central management functions for all Deep Discovery and Trend Micro products. Most Deep Discovery products also integrate with popular SIEM solutions, including HP ArcSight, IBM QRadar, and Splunk.

TREND MICRO™

Trend Micro

TACKLING UNKNOWN THREATS USING MACHINE LEARNING WITH NEXT-GENERATION INTRUSION PREVENTION

Combating dynamic threats

Modern threats are evanescent, incredibly short lived and ever changing. Signature-based detection, even using regular expressions, cannot identify a wide range of current threats. It is not the right toolset, as signatures would have to be developed, monitored, and updated for specific instances of a wide variety of threats. Even still, these signatures would often be outdated as soon as they are released because of the dynamic nature of modern threats. Statistical models effectively close these security gaps.

The ability to evaluate security filters that represent statistical models of malicious network data will greatly improve the security effectiveness of technologies like Next-Generation Intrusion Prevention Systems (NGIPS). IT security managers are faced with a series of challenges: increasingly sophisticated threats, riskier user behavior and a lack of visibility across their security systems.

The following use cases address some of the security gaps that cannot be solved by traditional signature-based detection solutions: malicious HTML content including JavaScript, malicious files, and malicious Adobe objects including Flash and PDF. Statistical models can be used to identify all of these, in-line, in real time.

EXPLOIT KITS AND OTHER MALICIOUS OBFUSCATED HTML

Live Stack testing from NSS Labs makes use of a number of exploit kits, which account for over 80% of Live Stack testing misses. These exploit kits deliver malicious obfuscated HTML, with code objects encoded in some manner within the HTML document to be decoded by later JavaScript or VBScript evaluation. Delivering protection against exploit kits, which are designed to evade detection by regular expressions, provides a substantial increase in security effectiveness to these prevalent and growing threats[1].

MALICIOUS OBFUSCATED JAVASCRIPT

JavaScript is increasingly used to deliver malicious content, including attacks that use JavaScript alone to accomplish malicious actions[2]. These scripts are obfuscated in order to evade detection by signatures or regular expressions. Statistical models can identify malicious obfuscated JavaScript, and close this gap. This is similar to the detection of obfuscated HTML, but focuses on malicious obfuscated JavaScript. This can apply to importation of JavaScript files and not just to HTML documents <script> elements.

MALICIOUS FLASH OBJECTS

One of the largest gaps in security effectiveness in the NGIPS is the lack of coverage in identifying malicious Flash objects. Malicious Flash objects and PDF files are widely used in attacks[3]. Many of the vulnerabilities disclosed to the Zero Day Initiative (ZDI) bug bounty program are within Adobe products. External research indicates that static analysis can detect malicious Flash files. Where static analysis is successful, statistical models can be applied.

MALICIOUS PDF FILES

Another large gap in security effectiveness in the NGIPS is the lack of coverage in identifying malicious PDF files. External research indicates that static analysis can detect malicious PDFs. Because malicious PDFs often incorporate malicious Flash objects or obfuscated JavaScript, completing 2.2 Malicious Obfuscated Javascript and 2.3 Malicious Flash

References:

1. **https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf**

2. **http://www.computerworld.com/article/3018972/security/ransom32-first-of-its-kind-javascript-based-ransomware-spotted-in-the-wild.html**

3. **http://www.computerworld.com/article/2521020/security0/rogue-pdfs-account-for-80--of-all-exploits--says-researcher.html**

above is prerequisite to this effort.

https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/malicious_pdfs.pdf?la=en.pdf?dl=true

http://www.diva-portal.se/smash/get/diva2:653114/FULLTEXT01.pdf

MALICIOUS PORTABLE EXECUTABLE (PE) FILES

Polymorphic malware results in over one million new malware samples per day[4]. Using PE headers alone, statistical models can predict whether an executable is malicious with greater than 95% accuracy[5]. Internal research from Trend Micro's TippingPoint DVLabs team has verified that creation of statistical models that identify malicious PE files is straightforward and effective.

CUSTOM PACKED FILES

Over 75% of malware executables are packed[6]. Regular expression filters can block files packed with off the shelf packing utilities, but malware authors are increasingly using custom polymorphic packers to evade detection. Custom packed files can be detected by measuring the compressibility of the files (ibid). While compressibility will not be directly used because of the latency it would introduce, related complexity measures such as entropy may be used. This approach is simpler and more direct using a model based on PE imports because it relies on very few features, and possibly just one.

USING MACHINE LEARNING TO ADDRESS UNKNOWN THREATS WITH NGIPS

Across many industries machine learning techniques are being quickly adopted; however, Trend Micro is the first to leverage this capability to detect and eliminate some of the threats mentioned above in-line at wire speed through the TippingPoint Next-Generation Intrusion Prevention System (NGIPS) and Threat Protection System (TPS).7 Our revolutionary approach powered by XGen™ security provides an additional measure of security on top of traditional signature-based approaches to intrusion prevention.

The following illustration details a very simplistic representation of machine learning capabilities using the

Trend Micro TippingPoint solutions.

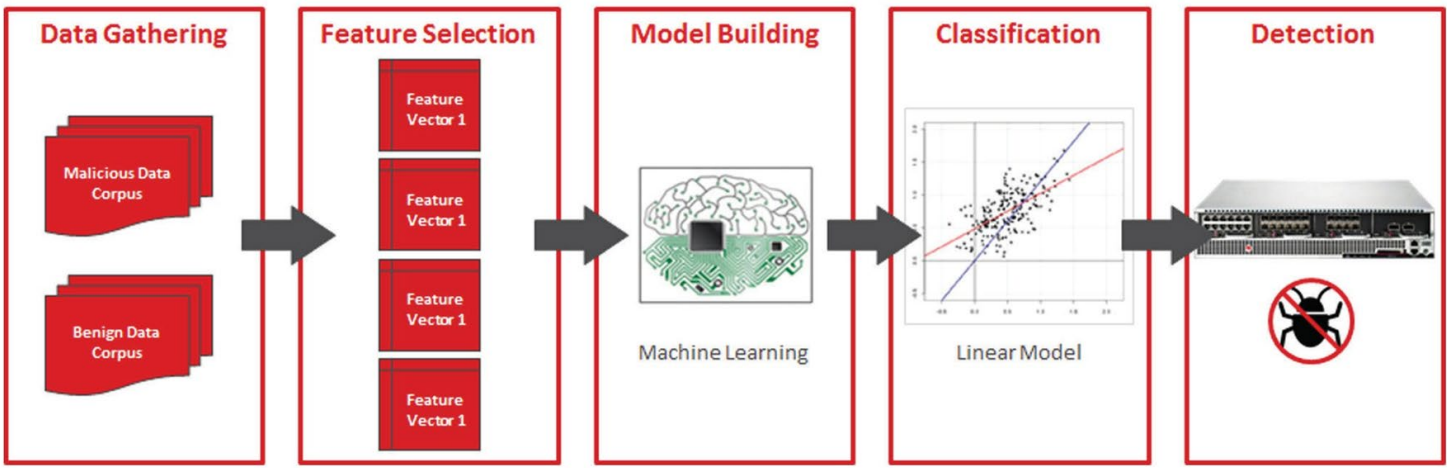


Illustration: Basics of machine learning and application to the TippingPoint **NGIPS and TPS**

4 http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

5 https://arxiv.org/ftp/arxiv/papers/1308/1308.2831.pdf

6 http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

7 http://www.trendmicro.com/us/business/network-security/intrusion-prevention-system/

Digital Vaccine® (DV) filter packages used by the TippingPoint NGIPS and TPS are a strong mechanism to detect network-based malicious activity, exploitation of vulnerabilities, and unwanted application use. However, as the TippingPoint solutions block these critical attacks more effectively, exploit kit authors adjusted their tactics to evade traditional signature-based techniques such as pattern-matching regular expressions. They now obfuscate content, including packing/compression, script obfuscation, encryption and much more. This makes classic detection mechanisms extremely difficult, often requiring multiple signatures and in many cases, only detecting a subset of the malicious content.

This is where machine learning and statistical data modeling become so effective. At a high level, machine learning works by training a machine by extracting "feature vectors" from a dataset of benign and malicious examples in order to compute a mathematical model. This model is evaluated against network traffic and, in the case of the TippingPoint solutions, can make a real-time decision about whether the content appears to be benign or malicious. If the content is determined to be malicious, the TippingPoint solutions block the content from entering the network. DV filters developed using the mathematical models operate without affecting network performance and without introducing a high amount of false positives.

Trend Micro TippingPoint also uses machine learning to detect Domain Generation Algorithms (DGAs) used in many malware families (e.g. Conficker) to randomly generate domain names in order to contact their command and control (CnC) servers. TippingPoint Threat DV DGA filters include classifiers, developed using machine learning techniques across a significant DNS datasheet, that can detect families of DGAs using a combination of syntactical rules and logistic regression with over 95% accuracy. DGA filters are also in place to catch many types of malware whose domain names cannot be encompassed by a regular expression that would not generate a large number of false positives.

Powered by XGen™ security

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

A LEADER

IN GARTNER 2018 IDPS MAGIC QUADRANT

TREND MICRO™

Securing Your Connected World

NOTES

NOTES

About Trend Micro

As a global leader in cloud security, Trend Micro develops security solutions that make the world safe for businesses and consumers to exchange digital information. With more than 25 years of experience, we deliver top-ranked security that fits our customers' needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments.