A Trend Micro White Paper | **June 2020**

Trend Micro™ Vulnerability Protection Overview

» This document outlines the process behind IDS/IPS rule creation and answers common questions about vulnerability coverage with Trend Micro Cloud One™ – Workload Security and Trend Micro™ Deep Security™ software.

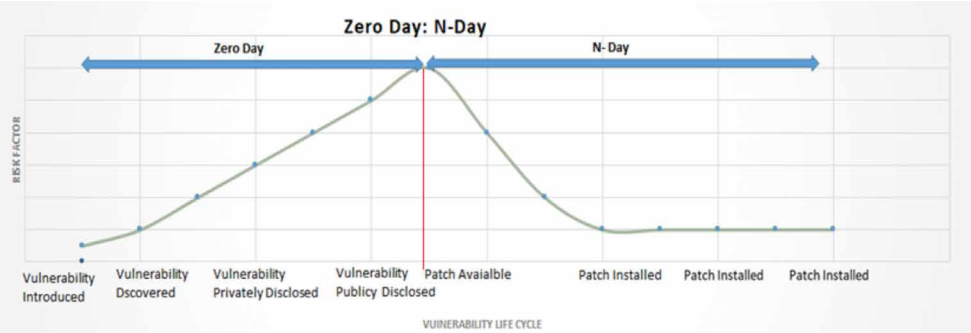
PURPOSE OF THIS WHITE PAPER

Trend Micro Research investigates vulnerabilities, new technologies, threats, and helps to provide detection/protection via various security controls within Trend Micro™ Deep Security™ software and Trend Micro Cloud One™ – Workload Security. This document explains the process of monitoring vulnerabilities and threats, the creation of intrusion detection and prevention system (IDS/IPS) rules, the frequency of rule updates, and the quality assurance of the rules. It also includes critical information on vulnerability coverage for various operating systems and applications protected by Trend Micro, including end-of-support systems like Microsoft® Windows® Server 2008 and Microsoft® Windows® Server 2003.

VULNERABILITY LIFE CYCLE

Vulnerabilities are broken down into two categories, based on the timeline.

- Zero-day: Vulnerability discovered to vulnerability patch available.
- N-day: Vulnerability patch available to patch installed in the OS/application.



Trend Micro Research provides the IPS rules for zero-day and N-day vulnerabilities, utilizing insights from Trend Micro™ Zero Day Initiative™, and focuses on the fastest turnaround time possible in every given situation.

RULE DEVELOPMENT PROCESS

The rule development process is divided into various stages:

1. Monitoring for vulnerabilities and emerging threats
2. Vulnerability research and IPS rule development
3. Recommendation rule development
4. Quality assurance and delivery of IPS rules to customers

Monitoring for Vulnerabilities and Emerging Threats

The rule development process begins with monitoring for the latest vulnerabilities and threats. Trend Micro Research monitors threats 24/7 from various sources, including:

- *ZDI*, owned by Trend Micro
- Partnership programs with software vendors, such as Microsoft® and Adobe® via Microsoft® Active Protections Program (MAPP)
- The Trend Micro Research team provides malware and telemetry information from customers (through the *Trend Micro™ Smart Protection Network™*), honeypots, and other sources.
- Vendor advisories
- Public information

VULNERABILITY RESEARCH AND IPS RULE DEVELOPMENT

Development Criteria

There are hundreds of vulnerabilities reported every week in various applications and operating systems. Vulnerability research and rule creation starts with carefully triaging and prioritizing these vulnerabilities, focusing on software commonly used in enterprise networks. This includes operating systems, such as Microsoft® Windows®, Linux®, UNIX®, as well as web/applications servers and enterprise software, including web browsers.

The IDS/IPS provided by Trend Micro is very similar to a network IDS/IPS system, however, it is applied at the host for more granular and specific security coverage. Trend Micro IPS primarily provides protection for remote vulnerabilities and exploits. This means that particular attention is paid to vulnerabilities that can be exploited over the network from a remote attacking computer. This includes protecting against newer threats like ransomware, where generic protection can be applied at the server and application layer, along with specific ransomware rules to detect and stop ransomware attacks.

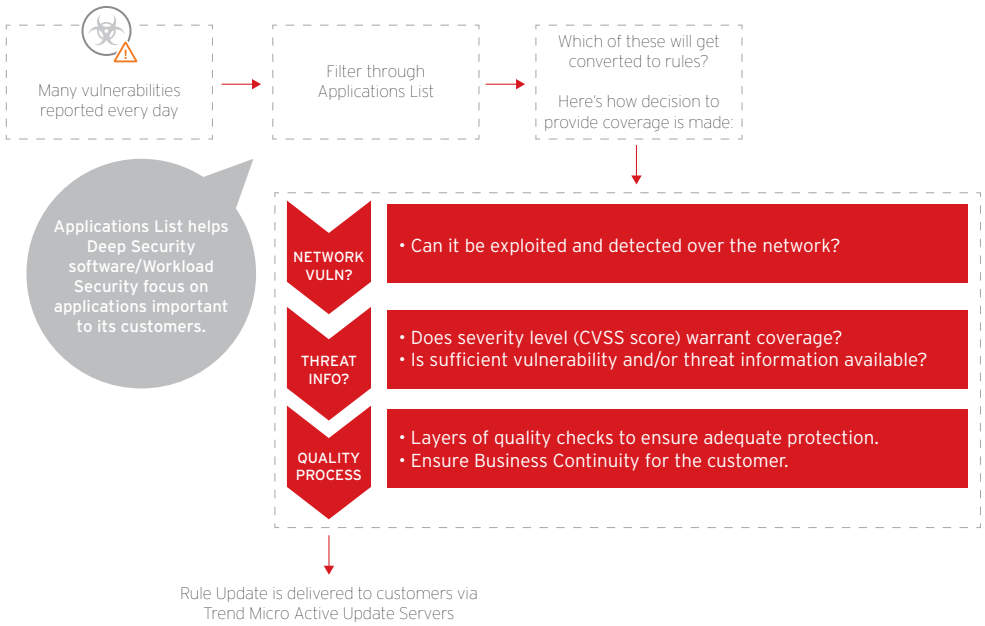
In order to determine where coverage is possible, the following criteria is used:

1. Is the vulnerability in enterprise software that many of our customers depend on and for which Trend Micro is in a position to protect?
2. Is it possible to detect the vulnerability by deep packet inspection (DPI)? If not using DPI, we determine the possibility of detection and protection using other security controls, like Application Control, Integrity Monitoring, or Log Inspection.
3. Is there a sufficient amount of vulnerability information available to be able to develop an intrusion prevention rule for the vulnerability?
4. Is the vulnerability severity level significant enough to warrant coverage? Typically, protection is provided only when the CVSS score is 5.0 or higher, however, we do review these on an individual basis in order to make a final coverage determination.

One of the biggest challenges preventing Trend Micro (and all network security products) from delivering protection for a specific vulnerability is simply the lack of adequate, actionable information. This lack of information makes it difficult to write rules with the confidence that the rule will block a particular attack and not impact day-to-day business outcomes.

The following illustration depicts the process described above.

IDS/IPS Rule Creation Criteria



Rule Development and Unit Testing

Developing a rule is similar to writing a small software program. First, all available threat information is analyzed to determine whether or not a rule can be created. Once it has been determined that it is possible and meets our stated criteria, a rigorous process is followed from start to finish, ensuring the overall quality and functionality of the released product.

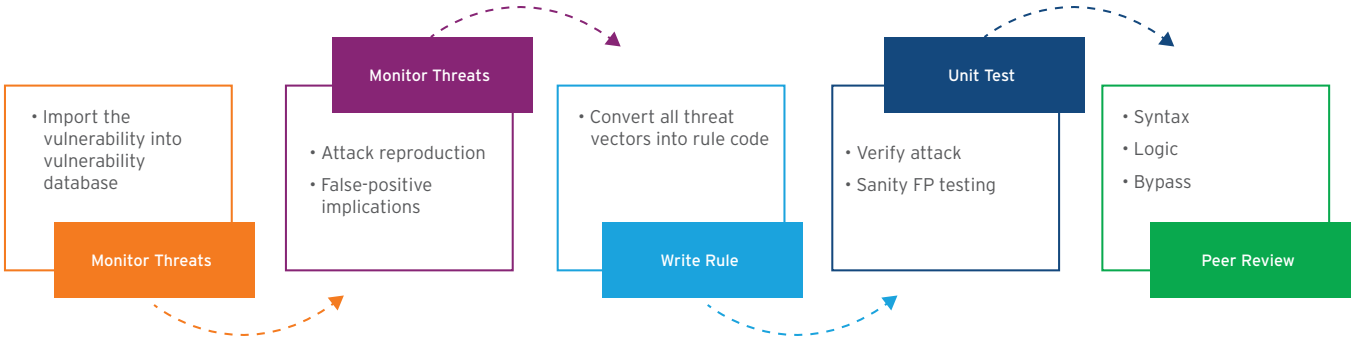
The triaged/selected vulnerabilities are imported into a tracking system and pushed into the research queue. The research team then selects vulnerabilities from the top of the research queue and collects all relevant threat information that will be used to develop an IDS/IPS rule.

An IDS/IPS rule is very different from an antivirus signature. It is not just a pattern, but a series of checks that look deep into the protocol, checking for very specific fields and structures in a protocol and/or file. This is why very clear actionable information is required to write an IDS/IPS rule.

Once an IDS/IPS rule is developed, it is subjected to various tests to ensure that it covers all aspects of the vulnerability, including tests for potential false-negative and false-positive conditions. A false negative is when a rule does not detect certain attack conditions and a false positive is when a rule identifies legitimate traffic as an attack. Both false negatives and false positives can have negative business impact, so the tests are required to ensure the highest quality rule is developed. These tests are carried out by the developer of the rule and a member of the quality assurance team.

After unit testing is completed, the rule undergoes a peer review process.

The figure below summarizes the IDS/IPS rule development process:



IDS/IPS Rule Development Process

Recommendation Rules

Trend Micro Research also creates rules for the "Recommendation Scan" feature from Trend Micro. In addition to the development of the specific rule, most IDS/IPS rules have a corresponding recommendation rule that identifies vulnerable software. This allows a recommendation scan to ensure that the IDS/IPS rule is deployed on the appropriate systems within a customer's environment and not deployed on systems where it is not required. This is a key difference between Trend Micro's host-based IPS and other host-based and network-based IPS approaches. The rules applied can be specific to a given system and the recommendation scan makes it easy to identify which rules should be applied to a given system. Recommendation rules are verified against real applications and patches, in most cases, as a part of the rule development process.

INTEGRATION TESTING

Once the entire process is finished, the completed rule is included in an overall update with other rules scheduled for later release. At this point, all rules are vigorously run through integration tests to ensure that the entire update works as expected within product and simulated customer environments.

This testing includes:

- **False-positive tests:** With any IDS/IPS product, false positives are a significant concern. We work to prevent these by running the rules through terabytes of "good traffic". Good traffic has been generated based on thousands of test cases collected from customer environments.
- **Regression tests:** This testing ensures that the rule doesn't have any impact on existing rules. We accomplish this by replaying attacks against all rules that could be possibly impacted and making sure the rules prevent those attacks.
- **Performance tests:** The rules are subjected to network performance tests, using industry standard tools to ensure any potential performance impact is minimal and well within reason.
- **Staging tests**: This testing ensures that the rule updates work fine with all supported versions.
- **Soak tests:** A rule update is released to an internal production operational environment within Trend Micro to ensure that the rule update does not have any negative operational impact.
- **Security update tests:** Before a rule update is released to customers, our team ensures that the update is posted and there are no issues importing them into the product.

DELIVERY TO CUSTOMERS

Once this comprehensive process is complete, the rules package is delivered and made available to customers globally. In situations where there is known exploitation or presence of an exploit is known, for example Bluekeep, Drupalgeddon, ShellShock, and Heartbleed vulnerabilities, this is typically done within a few hours of the vulnerability being disclosed publicly.

The following table provides a summary of the software categories Trend Micro has provided protection for over the course of many years.

	Before 2019 (approx.)	Vulnerabilities covered in 2019 (approx.)	Total
Platforms	**1,077**	**314**	**1,391**
Microsoft® Windows® OS and Core Services	672	135	807
Non-Windows OS and Core Services	405	179	584
Server Applications	2,998	297	3,295
Web Servers	158	7	165
Application Servers	1,126	85	1,211
Web Console/Management Interfaces	172	10	182
Database Servers	95	3	98
DHCP, FTP, DNS Servers	95	3	98
Mail Server	104	7	111
Directory Server/Services	77	0	77
HP® Products	190	15	205
IBM® Products	31	0	31
Oracle® Application	88	1	89
Backup Software	150	0	150
News/Media Streaming	12	0	12
PPTP Server	1	0	1
Kubernetes®	2	1	3
Miscellaneous	406	153	559
Anti-Spam Server	8	0	8
Other Applications (best effort)	283	12	295
Desktop Applications	**5,039**	**496**	**5,535**
Browsers	1,487	96	1,583
DHCP, DNS, FTP Clients	99	1	100

PDF Readers	1,062	314	1,376
Browser Plugins and Media Players	1,158	11	1,169
Dependent Libraries	25	2	27
Microsoft 365®	402	21	423
Other Microsoft Products	202	33	235
Others (best effort)	604	18	622
Application Control Rules	**84**		
File Sharing Software/P2P	24		
Miscellaneous	12		
Instant Messaging	16		
Email Clients/Protocols	8		
Remote Administration Tools	13		
Web Browsers	7		
Web Media	4		

FREQUENCY AND TIMING OF TREND MICRO RULE UPDATES

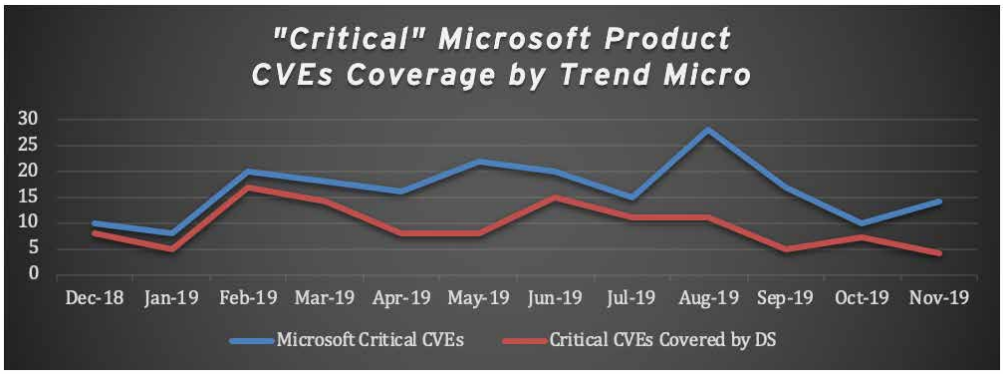
Development and delivery of IDS/IPS rules is completed in priority order. In addition to the criteria discussed above, the determination is also based on active exploitation, the presence of known exploits, and the exploit surface for the vulnerability.

While every effort is made to cover as many vulnerabilities and threats as quickly as possible, it is simply not feasible to provide a timeline to when a rule for a particular vulnerability may be made available. Zero-day vulnerabilities take top priority with Microsoft's "Patch Tuesday", also reviewed extensively for coverage potential. If vital details, such as a "proof of concept" (PoC) or vulnerability specifics, are not available, it will prevent a potential solution from being considered until Trend Micro can obtain the necessary information for review.

When adequate information is available and the vulnerability meets our creation criteria, the following table provides an estimated timeframe for when a solution could be made available.

Criteria	Typical Timeframe
Actively Exploited Vulnerabilities/Zero-Day Vulnerabilities	4 - 24 hrs
Microsoft Patch Tuesday	Immediately after Microsoft ships their patches
CVSS 9.0 - 10.0	Within 7 days
CVSS 7.0 - 9.0	Within 14 days
All Other Vulnerabilities	Best effort

Every month, we ship dozens of new rules and at least four rule updates. Out of band rule updates are required when more threat information is available, or to fix any discovered issues. *The following graph summarizes the number rules shipped for Microsoft environments over the past two years.*



In order to give a view of the volume of vulnerabilities covered and rules delivered, the table below is a high-level view of protection provided by Trend Micro:

	2015	2016	2017	2018	2019
Vulnerabilities Addressed	787	755	795	1057	964
Updated Rules	600+	426	488	813	558
Zero-Days Addressed	9	25	15	17	6

PROTECTION FOR END-OF-SUPPORT OPERATING SYSTEMS AND APPLICATIONS

Providing security for current and end-of-support (EOS) systems is one of many advantages of using Trend Micro to protect enterprise workloads. Host-based IDS/IPS helps in detecting and preventing threats before the malicious network packets reach your applications and is extremely valuable for systems that are EOS and no longer have vendor supplied patches available. It helps you protect against new vulnerabilities that are uncovered in these platforms and applications, as well as discover when malicious changes occur on your systems.

Vulnerable systems can quickly be assessed using the built-in recommendation scan feature to see what vulnerabilities are present. For example, today, Trend Micro detects and includes **316 specific rules that can be applied to a Windows Server 2003 system**. What's important to note, is that since Windows Server 2003 went EOS in July 2015, Trend Micro has added **over 100 rules** to protect against new vulnerabilities that can be exploited.

A good example of a critical vulnerability is MS15-011 (CVE-2015-008), which was discovered before the operating system went EOS, but was not fixed. Trend Micro can detect the presence of the vulnerability and protect against any attack that might happen over the network–specific to this issue.

Trend Micro protection for **Microsoft® Windows XP, Microsoft® Windows® 2000 Server,** and **Windows Server 2003** will be provided until the **end of 2020**. This will allow organizations to make a secure transition to a new platform, including transitioning to the cloud.

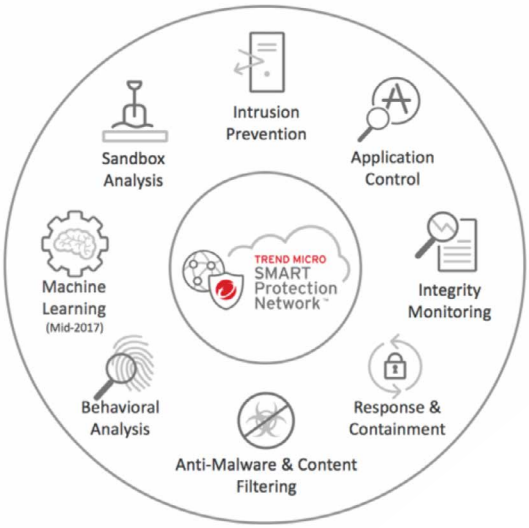
TREND MICRO: SECURING HYBRID CLOUD WORKLOADS

As organizations identify and plan for migration of systems to new environments, Trend Micro can play a significant role in addressing many of the critical security requirements. Ranked #1 in Hybrid Cloud Workload Security Market Share[1], Trend Micro streamlines operations through its ability to secure workloads across physical, virtual, cloud, and container environments. Available as software, service (PCI DSS level one certified), or via the AWS and Microsoft® Azure™ marketplaces, Trend Micro can help organizations streamline the purchasing and implementation of the essential security elements recommended by the Center for Internet Security. With proven API-level integration with VMware®, AWS, and Azure, Trend Micro provides full visibility across the hybrid cloud and includes the ability to automate security aligned with DevOps approaches.

Powered by XGen™, both Deep Security and Workload Security (SaaS-based) include a cross-generational blend of security controls for protecting servers, virtual machines, cloud workloads, and containers, including:

[1] *Worldwide Software Defined Compute Workload Security Market Shares, 2018*
[2] *The Forrester Wave™: Cloud Workload Security, Q4 2019*

- Network security to enable virtual patching, network attack prevention, and lateral movement prevention through IDS/IPS and a host-based firewall.
- Anti-malware that includes file reputation, variant protection, machine learning, behavioral analysis, and web reputation to protect vulnerable systems from the latest in threats.
- System security enables the lockdown of systems, discovery of unplanned or malicious changes to the registry and key system files, and discovering anomalies in critical log files through application control, integrity monitoring and log inspection.



Trend Micro helps to protect workloads across the data center and cloud with multiple security capabilities delivered through a single agent, enabling you to:

- Defend against threats and protect against vulnerabilities using proven IPS to instantly shield vulnerable applications, containers, and servers with a "virtual patch" until it can be patched (or until transition from an EOS operating system).
- Detect and block lateral movement across the enterprise, stopping the spread of threats, like ransomware, while also detecting command and control (C&C) that would indicate an impending threat.
- Keep malware off workloads, ensuring that servers and applications are protected and unusual or suspicious behavior from attacks, like ransomware, are neutralized.
- Lockdown servers with application control, making sure that only authorized applications can run.
- Identify suspicious changes on servers with integrity monitoring, including flagging changes to things like registry settings, system folders, and application files that shouldn't change—when they do.
- Accelerate compliance with key frameworks like the SANS/CIS Critical Security Controls, as well as key regulations like the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA), delivering multiple security controls, central control, and easy reporting in a single product.

CONCLUSION

With thousands of customers and millions of workloads/servers protected, Trend Micro solutions are designed for the hybrid cloud. We provide a cross-generational blend of threat defense techniques optimized for securing physical, virtual, cloud, and container workloads. Delivering protection from advanced attacks and multiple capabilities in a single platform that allows for vendor consolidation, Trend Micro solves real-world problems and simplifies operations without compromising security. Ranked #1 in market share by IDC and Named a leader in the Forrester Wave™ for Cloud Workload Security, Q4 2019[2], we believe you can feel confident in choosing Trend Micro to protect your hybrid cloud deployments.

Find out more about Trend Micro hybrid cloud security solutions at *www.trendmicro.com/hybridcloud*.

TREND MICRO™
Securing Your Connected World

Trend Micro, a global leader in cybersecurity, helps make the world safe for exchanging digital information. Leveraging over 30 years of security expertise, global threat research, and continuous innovation, Trend Micro enables resilience for businesses, governments, and consumers with connected solutions across cloud workloads, endpoints, email, IIoT, and networks.

With over 6,700 employees in 65 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. www.trendmicro.com

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1408.257.2003

[WP00_Vulnerability_Protection_Overview_200602US]