White Paper

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 Cloud One™ – Workload Security and Trend Micro™ Deep Security™ software. 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 (EOS) systems like Microsoft® Windows® Server 2012, Server 2012 R2 and Microsoft® Windows® Server 2008 and older.

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, utilising insights from Trend Micro™ Zero Day Initiative™ (ZDI) 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

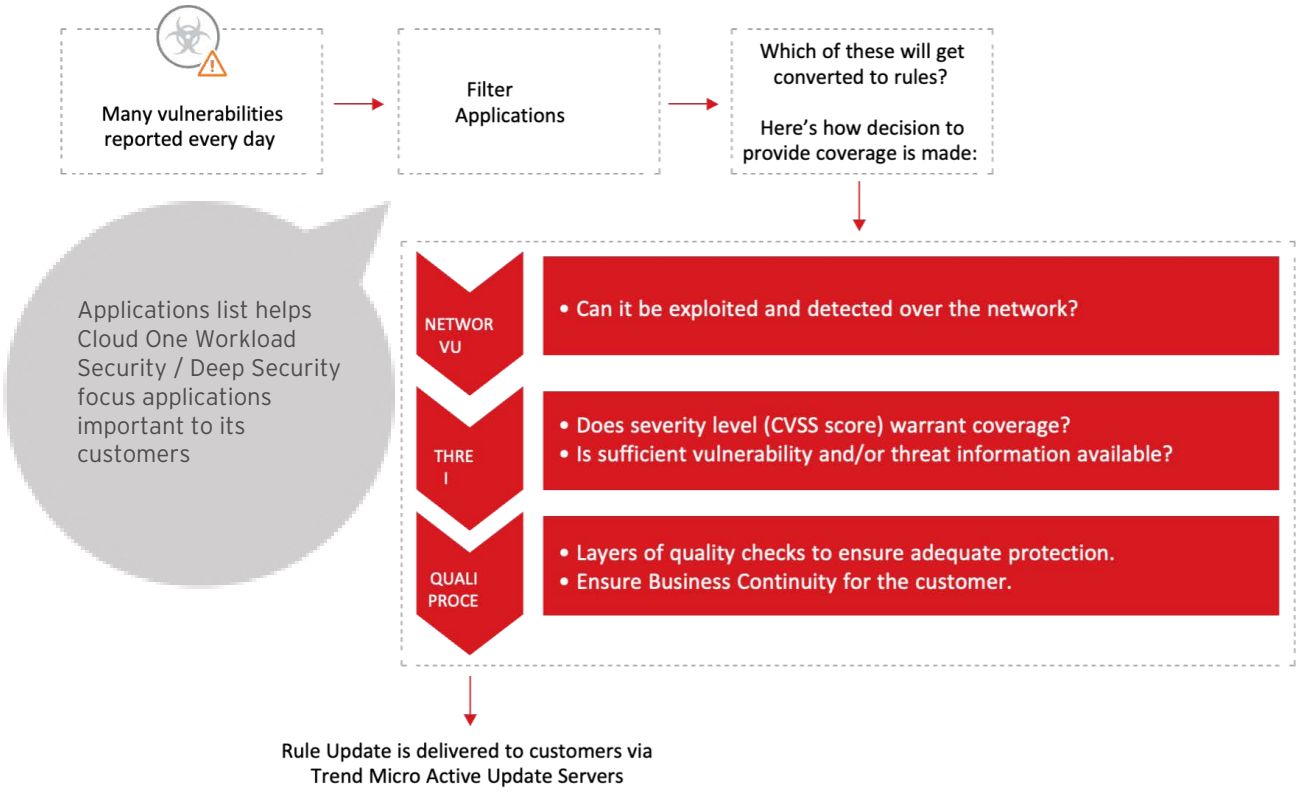
VULNERABILITY RESEARCH AND IPS RULE DEVELOPMENT

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 prioritising 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.

To determine where coverage is possible, the following criteria is use:

1. Is the vulnerability in enterprise software that many of our customers depend on and for which Trend Micro can protect?
2. Is it possible to detect the vulnerability by deep packet inspection (DPI)? If not using DPI, we determine the possibilty of detection and protection using other security controls, like Application Control, Integrity Monitoring, or Log Inspection.
3. Is there enough 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 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



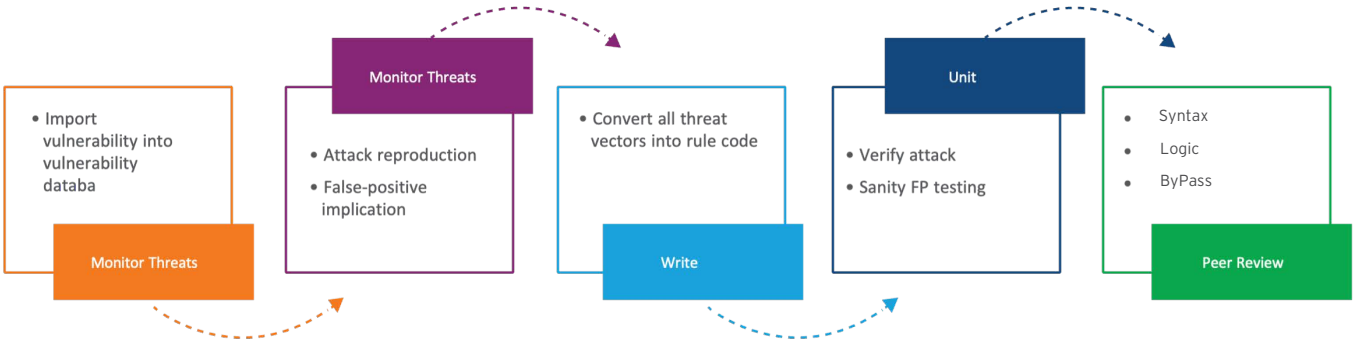
Rule Development & Unit Testing
Developing a rule is like writing a small software program. First, all available threat information is analysed to determine whether a rule can be created. Once it has been determined that it is possible and meets our stated criteria, a rigorous process is followed from 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. Therefore, 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, Eternal Blue, 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 Trend Micro has provided protection for over the course of many years.

	Vulnerabilities Before 2020 (approx.)	*Vulnerabilities Since 2020 (approx.)*	Total
	4138	1636	5774
Windows Core*	68	43	**111**
Server Application	947	1281	**2228**
Desktop Application	3049	283	**3332**
Client Application	61	19	**80**
Linux	13	10	**23**

**Windows is no longer an operating system for only PCs, laptops, and tablets. Windows Core OS is a stripped-down version of Windows that can be adapted to run on a wide variety of devices with minimal work*

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.

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.

	2023 *	2022	2021	2020	Pre-2020	TOTAL
Vulnerabilities Addressed	13	1070	661	483	3962	6,189

**Data to March 2023*

PROTECTION FOR END OF SUPPORT OPERATING SYSTEMS AND APPLICATIONS

Providing security for current and 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. Since Jan 2020, when Windows Server 2008 went EOS, we have released 197 VP rules/filters to address on-going vulnerabilities (of which 78 are critical severity). The vast majority have not seen a corresponding update or release from Microsoft. An example of a critical vulnerability is MS15-011 (CVE-2015-008), which was discovered before Windows Server 2003 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 Server 2012 will be provided until such time that our customers no longer need to be protected. This will allow organisations to make a secure transition to a new platform, including transitioning to the cloud with minimal impact to their business.

SECURING THE HYBRID CLOUD

Being a cloud-first company is fast becoming the norm. An estimated 85% of organisations are aiming to embrace a cloud-first principle by 2025. (Source Gartner) But transformation doesn't happen overnight, it takes time and during the transition organisations will have a mix of technologies that can be complex for teams to secure as risks are uncovered. From hybrid, multi-cloud to cloud native applications (CNAPP) trying to piece together views from various security tools is creating visibility silos leading to hidden gaps in coverage, leaving organisations vulnerable. Trend Micro Cloud One™ secures you journey from virtual machines to cloud native while embracing the organisational silos. By integrating with Trend Micro Vision One ™, Trend's XDR and MDR platform, we can provide visibility across entire attack /surface to protect their business.

Our customers gain visibility & control with security designed for the cloud and can identify threats in minutes, protecting their business reputation and ensuring data compliance.

Trend Micro streamlines operations through our Cloud One security services platform, delivering the broadest and deepest cloud security offering in one solution, enabling you to secure your cloud infrastructure with clarity and simplicity.

By considering your cloud projects and objectives holistically, Cloud One can provide powerful security, while you leverage all the benefits and efficiencies the cloud offers your business. Comprised of multiple services designed to meet specific cloud security needs, Cloud One gives you the flexibility to solve your challenges today, and the innovation to evolve with your cloud services in the future. You no longer must find point products to meet the unique requirements of your infrastructure or work with the processes you've already implemented. With a comprehensive set of services, designed specifically for the cloud, Cloud One secures the different parts of your environment within one simple platform. With support for all major cloud platforms, and solutions that integrate directly into your DevOps processes and toolchain, Trend Micro Cloud One is designed to provide the flexibility you need without slowing down your business or application delivery. Available as software as a service via the AWS and Microsoft Azure marketplaces, Trend Micro can help organisations streamline the purchasing implementation of the essential security elements recommended by the Center for Internet Security.

With thousands of customers and millions of workloads/servers protected, Trend Micro solutions are designed for the hybrid cloud. 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 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.