Trend Micro™

TIPPINGPOINT™ THREAT PROTECTION SYSTEM FAMILY

Real-time detection, enforcement, and remediation without compromising security or performance

Organizations today are in the constant shadow of evolving and sophisticated cyber threats. In some cases, these threats are not only more complex than those of the past, but they are also targeted and rely on newly discovered vulnerabilities or exploits. In other cases, threats take advantage of older vulnerabilities that you thought were long forgotten. Safeguarding your network assets and data from such threats requires detailed visibility into all your network layers and resources. It requires comprehensive, up-to-date security intelligence, and a dynamic approach that uses awareness and automation to adapt to new threats, new vulnerabilities, and everyday network changes.

These vastly different threats require a multi-pronged approach to security. Organizations need robust security solutions at the edge of and inside their networks to prevent malicious attacks from getting to critical resources. They also need comprehensive threat intelligence to protect against known, unknown, and undisclosed vulnerabilities.

Trend Micro TippingPoint Threat Protection System (TPS) is a powerful network security platform that offers comprehensive threat protection against known and undisclosed vulnerabilities with high accuracy. TPS provides industry-leading coverage across different threat vectors from advanced threats like malware and phishing with extreme flexibility and high performance. The TPS uses a combination of technologies, including deep packet inspection, threat reputation, URL reputation, and advanced malware analysis on a flow-by-flow basis—to detect and prevent attacks on the network. The TPS enables enterprises to take a proactive approach to security, providing comprehensive contextual awareness and deeper analysis of network traffic. This complete contextual awareness, combined with the threat intelligence from Trend Micro™ TippingPoint™ Digital Vaccine® Labs (DVLabs) provides the visibility and agility necessary to keep pace with today's dynamic, evolving enterprise and data center networks.

> "Trend Micro™ Deep Discovery™ was a no brainer. It outperformed all competitors and was well-respected by Gartner™. When Trend Micro purchased TippingPoint, we knew we had the best of both worlds."
>
> Frank Bunton,
> Vice President and CISO,
> MedImpact

MedImpact

KEY FEATURES

TippingPoint Threat Protection Extended to the Cloud: Trend Micro™ Cloud Network Protection, powered by Trend Micro TippingPoint, is a powerful inline security solution that allows enterprises to extend their existing TippingPoint network protection to their hybrid cloud environments. Offering comprehensive threat protection—including virtual patching, shielding against vulnerabilities, blocking exploits, and defending against known and zero-day attacks with high accuracy—it provides industry-leading coverages across multiple threat vectors. Apply your TippingPoint security controls and policies to your cloud environments via your existing Security Management System (SMS).

On-Box SSL Inspection: Sophisticated and targeted attacks are increasingly using encryption to evade detection. TPS reduces security blind spots created by encrypted traffic with on-box SSL inspection.

Performance Scalability: The increase in data center consolidation and proliferation of cloud environments requires security solutions that can scale as network demands increase. TPS delivers unprecedented security and performance for high-capacity networks with a scalable deployment model that includes the industry's first 40 Gbps Next-Generation Intrusion Prevention System (NGIPS) in a 1U form factor with the ability to scale up to 120 Gbps aggregate in a 3U form factor.

Flexible Licensing Model: Easily scale performance and security requirements with pay-as-you-grow approach and flexible licenses that can be reassigned across TPS deployments without changing network infrastructure.

Real-Time Machine Learning: Many security threats are short-lived and constantly evolving, at times limiting the effectiveness of traditional signature and hash-based detection mechanisms. TPS uses statistical models developed with machine learning techniques deliver the ability to detect and mitigate threats in real time.

Enterprise Vulnerability Remediation (eVR): Quickly remediate vulnerabilities by integrating third-party vulnerability assessments with the TippingPoint product portfolio. Customers can pull in information from various vulnerability management and incident response vendors (Rapid7, Qualys®, Tenable), map Common Vulnerabilities and Exposures (CVEs) to TippingPoint Digital Vaccine® filters and take action accordingly.

Advanced Threat Analysis: Extend protection from unknown threats through integration with Trend Micro™ Deep Discovery™ Analyzer. TPS pre-filters known threats, forwards potential threats for automated sandbox analysis, and remediates in real time upon confirmation of malicious content.

High Availability: Ideal for inline deployment, TPS has multiple fault-tolerant features including hot swappable power supplies, watchdog timers to continuously monitor security and management engines, built-in inspection bypass, and zero power high availability (ZPHA). In addition, TPS can be provisioned using redundant links in a transparent active-active or active-passive high availability (HA) mode.

Integrated Advanced Threat Prevention: TPS integrates with Trend Micro™ Deep Discovery™ advanced threat detection solutions, rated as a "Recommended" breach detection system by NSS Labs[1].

Asymmetric Traffic Inspection: Traffic asymmetry is widespread and pervasive throughout enterprise and data center networks. Enterprises must overcome challenges from both flow and routing asymmetry to be able to fully protect their networks. TPS by default inspects all types of traffic, including asymmetric traffic, and applies security policies to ensure comprehensive protection.

Agility and Flexibility: TPS embraces software-defined network protection by deploying IPS as a service. TPS also protects virtualized applications from within your virtualized infrastructure (VMware®, KVM).

Best-in-Class Threat Intelligence: Digital Vaccine Labs (DVLabs) provide cutting-edge threat analysis and security filters that cover an entire vulnerability to protect against all potential attack permutations, not just specific exploits. In addition to DVLabs, exclusive access to vulnerability information from the Zero Day Initiative (ZDI) protects customers from undisclosed and zero-day threats. ZDI is the largest vendor-agnostic bug bounty program, with more than 1,450 vulnerabilities published in 2018 with Trend Micro TippingPoint customers were protected an average of 62 days ahead of a vulnerability being patched by affected vendors.

Virtual Patching: Provides a powerful and scalable frontline defense mechanism that protects networks from known threats and relies on vulnerability-based filters to provide an effective barrier from all attempts to exploit a particular vulnerability at the network level rather than the end-user level. This helps enterprises gain control of their patch management strategy with pre-emptive coverage between the discovery of a vulnerability and the availability of a patch, as well as added protection for legacy, out-of-support software.

Support for a Broad Set of Traffic Types: TPS platform supports a wide variety of traffic types and protocols. It provides uncompromising IPv6/v4 simultaneous payload inspection and support for related tunneling variants (4in6, 6in4, and 6in6). It also supports inspection of IPv6/v4 traffic with VLAN and MPLS tags, mobile IPv4 traffic, GRE and GTP (GPRS tunneling), and jumbo frames. This breadth of coverage gives IT and security administrators the flexibility to deploy its protection wherever it is needed.

Centralized Management: The TippingPoint Security Management System (SMS) delivers a unified policy and element management graphical user interface that provides a single mechanism for monitoring operational information, editing network security policies, configuring elements, and deploying network security policy across the entire infrastructure whether it is physical or virtual.

Key Benefits

Pre-emptive threat prevention

TPS deployed inline has the ability to inspect and block all directions of traffic (inbound, outbound, and lateral) in real time to protect against known, unknown, and undisclosed vulnerabilities.

Threat insight and prioritization

Visibility and insight is crucial to making the best security policy decisions. TPS delivers complete visibility across your network and provides the insight and context needed to measure and drive threat prioritization.

Real-time enforcement and remediation

Defend the network from the edge, to the data center, and to the cloud with real-time, inline enforcement and automated remediation of vulnerable systems. TPS achieves a new level of inline, real-time protection, providing proactive network security for today's and tomorrow's real-world network traffic and data centers. The Threat Suppression Engine (TSE) architecture performs high-speed inline deep packet traffic inspection, and the purpose-built appliance's modular design enables the convergence of additional security services.

Operational simplicity

With flexible deployment options that are easy to set up and manage through a centralized management interface, TPS provides immediate and ongoing threat protection with out-of-the-box recommended settings.

1 https://resources.trendmicro.com/2018-NSS-Labs-BDS-Report-Global.html

TPS TECHNICAL SPECIFICATIONS




Features	1100TX (TPNN0321)	5500TX (TPNN0322)	8200TX (TPNN0090)	8400TX (TPNN0091)
Supported IPS Inspection Throughput	250 Mbps/500 Mbps/1 Gbps	1 Gbps/2 Gbps/3 Gbps/5 Gbps	3/5/10/15/20/30/40 Gbps	
SSL Inspection (2K keys with ECDHE-RSA-AES256-GCM-SHA384)	Not available	Up to 3.5 Gbps (capped by IPS inspection throughput)	Up to 8 Gbps (capped by IPS inspection throughput)	
New SSL Connections per Second	Not available	2,700	5,500	
Latency	<40 microseconds			
Concurrent Sessions	15,000,000	30,000,000	120,000,000	
New Connections per Second	140,000	420,000	650,000	
MTBF (Mean Time Between Failures)	93,177 hours @ 25°C ambient	75,660 hours @ 25°C ambient	88,706 hours @ 25°C ambient	
Form Factor	1RU, 19"		1U	2U
Weight	14.5 lbs (6.58 Kg)	17.5 lbs (7.94 Kg)	32 lbs (max including IOMs) 29 lbs (w/ blank IOMs)	50 lbs (max including IOMs) 41.5 lbs (w/ blank IOMs)
Dimensions (W x D x H)	18.54" (W) x 17.90" (D) x 1.73" (H) 47.09 cm x 45.47 cm x 4.40 cm		16.78" (W) x 17.3" (D) x 1.72" (H) 42.62 cm x 45.00 cm x 4.40 cm	16.77" (W) x 18.70" (D) x 3.46" (H) 42.60 cm x 47.50 cm x 8.80 cm
Management Ports	1 GbE RJ45, 115200 8N1 serial RJ45		One out-of-band 10/100/1000 RJ-45 one RJ-45 serial	
Management Interface	One out-of-band 10/100/1000 RJ-45 one RJ-45 serial		Security Management System (SMS), local web console, command-line, SNMPv2c, SNMPv3 (Trend Micro™ TippingPoint™ MIB available)	
Network Connectivity	Up to 12x 1 GbE copper, up to 12x 1 GbE SFP, up to 8x 10 GbE SFP+, up to 2x 40 GbE QSFP+	Up to 20x 1 GbE RJ45, up to 20x 1 GbE SFP, up to 16x 10 GbE SFP+, up to 4x 40 GbE QSFP+	2x IOM slots, mix/match: 6-segment 1 GE copper 6-segment 1 GE SFP 4-segment 10 GE SFP+ 1-segment 40 GE QSFP+ 1-segment 40 GE QSFP+ bypass 4-segment 1 GE copper bypass 2-segment 1 GE SR/LR fiber bypass 2-segment 10 GE SR/LR fiber bypass	4x IOM slots, mix/match: 6-segment 1 GE copper IOM 6-segment 1 GE SFP IOM 4-segment 10 GE SFP+ 1-segment 40 GE QSFP+ 1-segment 40 GE QSFP+ bypass 4-segment 1 GE copper bypass 2-segment 1 GE SR/LR fiber bypass 2-segment 10 GE SR/LR fiber bypass
On-Box Storage	8 GB internal CFAST / 8 GB external 1.8" SSD	32 GB Internal CFAST / 32 GB External 1.8" SSD	32 GB hot-swappable 1.8" SSD module	
Voltage	100-240 VAC, 50-60 Hz		100 to 240 VAC/-40 to -60 VDC	
Current (Max. Fused Power)	4-2 A		12/6 amps AC, 24/16 amps DC	
Max Power Consumption	250 W (853 BTU/hour)	220W (751 BTU/hour)	750 W (2,557BTU/hour)	
Power Supply	Single field replaceable	Dual/ redundant hot-swappable/field replaceable	Dual/redundant hot-swappable	
Operating Temperature	32°F to 104°F (0°C to 40°C)			
Operating Relative Humidity	5% to 95% non-condensing			
Non-Operating/Storage Temperature	-4°F to 158°F (-20°C to 70°C)			
Non-Operating/Storage Relative Humidity	5% to 95% non-condensing			
Altitude	Up to 10,000 feet above MSL (3,048 m)			
Safety	UL 60950-1, IEC 60950-1EN 60950-1,CSA 22.2 60950-1RoHS compliance			
EMC	Class A, FCC, VCCI, KC EN55022, CISPR 22, EN55024 CISPR 24, EN61000-3-2 EN61000-3-3, CE marking			

CLOUD NETWORK IPS TECHNICAL SPECIFICATIONS

AWS® Instance Type	C5.2xlarge	C5.9xlarge and F1.2xlarge
IPS Inspection Throughput	2.5 Gbps	Up to 10 Gbps*
Latency	<100 microseconds	
Concurrent Connections	7.5M	12M
New Connections Per Second	75,000	100,000

*AWS infrastructure may restrict sustained throughput rates to lower amounts. This is specific to the EC2 instance type. For more information please contact AWS. Note: We test using our recommended default policy with representative traffic mixes. Your deployment may vary–infrastructure changes, policy, or changes from the representative traffic mix may impact your results. Additionally, your EC2 instance type may enforce sustained throughput restrictions

vTPS TECHNICAL SPECIFICATIONS

Features	vTPS Standard	
Supported IPS Inspection Throughput	250 Mbps/500 Mbps/1 Gbps/2 Gbps	
SSL Inspection	NA	Yes
Number of Logical Cores	2 or 3	4
Memory	8 GB	16 GB
Disk Space	16 GB	
IPS Concurrent Connections	1,000,000	
New Connections per Second	Up to 120 K VMware® up to 60K KVM	
Virtual Platform Support	VMWare ESXi 5.5, 6.0, 6.5, 6.7 (NSX is not required for transparent inspection and enforcement) & KVM – Redhat Enterprise Linux® 6, 7	
Network Drivers	VMware- VMNet3 KVM- virtIO	
Number of Network Segments	1	
Number of Virtual Segments	No limit	
Dedicated Management vNIC	Yes	

TIPPINGPOINT I/O MODULES

TippingPoint IO Module Description	Product SKU
TippingPoint IO Module: 6-segment Gig-T	TPNN0059
TippingPoint IO Module: 6-segment GbE SFP	TPNN0068
TippingPoint IO Module: 4-segment 10 GbE SFP+	TPNN0060
TippingPoint IO Module: 1-segment 40 GbE QSFP+	TPNN0069
TippingPoint IO Module: 4-segment Gig-T Bypass	TPNN0070
TippingPoint IO Module: 2-segment 1 G Fiber SR Bypass	TPNN0071
TippingPoint IO Module: 2-segment 1 G Fiber LR Bypass	TPNN0072
TippingPoint IO Module: 2-segment 10 G Fiber SR Bypass	TPNN0073
TippingPoint IO Module: 2-segment 10 G Fiber LR Bypass	TPNN0074
TippingPoint IO Module: 1-segment 40GbE LR4 Bypass	TPNM0132
TippingPoint IO Module: 1-segment 40GbE SR4 Bypass	TPNM0131

For details about what personal information we collect and why, please see our Privacy Notice on our website at: https://www.trendmicro.com/privacy

Securing Your Connected World