DATASHEET

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, and up-to-date security intelligence and a dynamic approach that uses awareness and automation to adapt to new threats, new vulnerabilities, and every day 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 t® 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, malware, and phishing, etc., 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 to provide comprehensive contextual awareness and deeper analysis of network traffic. This complete contextual awareness, combined with the threat intelligence from Digital Vaccine® Labs (DVLabs) provides the visibility and agility necessary to keep pace with today's dynamic, evolving enterprise and data center networks.

> "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

KEY FEATURES

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 40Gbps NGIPS in a 1U form factor with the ability to scale up to 120Gbps 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 to 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 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 in-line 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 the most effective and "recommended" breach detection system by NSS Labs.

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: Trend Micro™ TippingPoint® Digital Vaccine® Labs (DVLabs) provides 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 700 vulnerabilities published in 2016. In 2016, Trend Micro TippingPoint customers were protected an average of 57 days ahead of a vulnerability being patched by affected vendors.

Virtual Patching: 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 its physical or virtual.

Key Benefits

Pre-emptive threat prevention

TPS deployed in-line 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 in-line, 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 in-line 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 setup and manage through a centralized management interface, TPS provides immediate and ongoing threat protection with out-of-the-box recommended settings.

TPS TECHNICAL SPECIFICATIONS

   

Features	440T (TPNN0291)	2200T (TPNN0292)	8200TX (TPNN0090)	8400TX (TPNN0091)
Supported IPS Inspection Throughput	250Mbps/500Mbps/ 1Gbps	1Gbps/2Gbps	3/5/10/15/20/30/40 Gbps	3/5/10/15/20/30/40 Gbps
SSL Inspection	Not Available	500Mbps	2Gbps(2K keys SHA256)	2Gbps(2K keys SHA256)
Latency	<100 microseconds	<100 microseconds	<40 microseconds	<40 microseconds
Security Contexts	750,000	2,500,000	10,000,000	10,000,000
Concurrent Sessions	1,000,000	10,000,000	120,000,000	120,000,000
New Connections per second	70,000	115,000	650,000	650,000
Form Factor	1U	2U	1U	2U
Weight	15.28 lbs. (6.93Kg)	26.26 lbs. (11.91Kg)	32lbs (Max including IOMs) 29lbs (w/ blank IOMs)	50lbs (Max including IOMs) 41.5 lbs (w/ blank IOMs)
Dimensions (W x D x H)	16.78 in.(W) x 17.3 in.(D) x 1.72 in.(H) 42.62 cm x 45.00 cm x 4.40cm	16.77 in. (W) x 18.70 in.(D) x 3.46 in.(H) 42.60 cm x 47.50 cm x 8.80 cm	16.78 in.(W) x 17.3 in.(D) x 1.72 in.(H) 42.62 cm x 45.00 cm x 4.40cm	16.77 in. (W) x 18.70 in.(D) x 3.46 in.(H) 42.60 cm x 47.50 cm x 8.80 cm
Management Ports	One out-of-band 10/100/1000 RJ-45 One RJ-45 serial Manageable			
Management Interface	Security Management System(SMS), Local Web Console , Command-line, SNMPv2c, SNMPv3(TippingPoint MIB available)			
Network Connectivity	Eight 10/100/1000 RJ-45 ports and integrated bypass support One 10/100/1000 RJ-45 high availability ports	Eight 10/100/1000 RJ-45 ports with integrated bypass support 8 x 1G SFP 4 x 10G SFP+ One 10/100/1000 RJ-45 High Availability ports Support for external ZPHA for SFP/SFP+	2x IOM Slots, Mix/Match: 6-Segment 1GE Copper 6-Segment 1GE SFP 4-Segment 10GE SFP+ 1-Segment 40GE QSFP+ 4-Segment 1GE Copper Bypass 2-Segment 1GE SR/LR Fiber Bypass 2-Segment 10GE SR/LR Fiber Bypass	4x IOM Slots, Mix/Match: 6-Segment 1GE Copper 6-Segment 1GE SFP 4-Segment 10GE SFP+ 1-Segment 40GE QSFP+ 4-Segment 1GE Copper Bypass 2-Segment 1GE SR/LR Fiber Bypass 2-Segment 10GE SR/LR Fiber Bypass
On-box Storage	8GB Hot-Swappable CFast Drive		32GB 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 A	12/6 Amps AC, 24/16Amps DC	
Max power consumption	250W(853 BTU/hour)	493W(1,682 BTU/hour)	750W(2,557BTU/hour)	
Power supply	Single fixed	Dual/redundant hot-swappable	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 (3,048m)			
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			

vTPS TECHNICAL SPECIFICATIONS

Features	vTPS Standard	
Supported IPS Inspection Throughput	250Mbps/500Mbps /1Gbps	250Mbps/500Mbps /1Gbps
SSL Inspection	NA	Yes
Number of logical cores	2 or 3	4
Memory	8GB	16GB
Disk Space	16GB	16GB
IPS Concurrent connections	1,000,000	
New connections per second	Up to 120K VMware; Up to 60K KVM	
Virtual Platform Support	VMWare ESXi 5.5, 6.0,6.5 (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 10GbE SFP+	TPNN0060
TippingPoint IO Module: 1-segment 40GbE QSFP+	TPNN0069
TippingPoint IO Module: 4-segment Gig-T Bypass	TPNN0070
TippingPoint IO Module: 2-segment 1G Fiber SR Bypass	TPNN0071
TippingPoint IO Module: 2-segment 1G Fiber LR Bypass	TPNN0072
TippingPoint IO Module: 2-segment 10G Fiber SR Bypass	TPNN0073
TippingPoint IO Module: 2-segment 10G Fiber LR Bypass	TPNN0074

Securing Your Connected World

©2018 by Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. For more information, visit www.trendmicro.com.
[DS01_TPS_Family_181109US]