Trend Micro™ TIPPINGPOINT™ TXE SERIES

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

Your organization is 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 risks involves 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. Your organization benefits from robust security solutions at the edge of, and inside, your networks. This prevents malicious attacks from getting to critical resources. Comprehensive threat intelligence protects your environment against known, unknown, and undisclosed vulnerabilities.

Trend Micro™ TippingPoint™ Threat Protection System (TPS) is a powerful network security platform that delivers comprehensive threat protection against known and undisclosed vulnerabilities with high accuracy. TippingPoint TPS provides your organization with industry-leading coverage across different threat vectors with extreme flexibility and high performance, keeping you resilient against advanced threats like malware and phishing. The TippingPoint 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 your network. The TippingPoint TPS enables your teams to take a proactive approach to security, providing you with comprehensive contextual awareness and deeper analysis of network traffic. This complete contextual awareness, combined with the threat intelligence from Trend Micro™ TippingPoint™ Digital Vaccine™ (DV) Threat Intelligence provides the visibility and agility necessary to keep pace with today's dynamic, evolving enterprise and data center networks.

Key Features

TippingPoint Threat Protection Extended to the Cloud: Trend Micro™ Cloud Network Protection, powered by TippingPoint, is a robust, inline security solution that allows your enterprise to extend your existing TippingPoint network protection to your 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—you get industry-leading coverage 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. TippingPoint TPS reduces your 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. TippingPoint TPS delivers unprecedented security and performance for your high-capacity networks. This includes a scalable deployment model, featuring the industry's first 100 Gbps next-generation intrusion prevention system (NGIPS) in a 1U form factor—with the ability to scale up to 0.5 Tbps (500 Gbps) aggregate in a 5U form factor.

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

Gartner

Ranked #1 in Gartner IDPS Market Share worldwide @ 23.5% share

Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q20 and 2020, Christian Canales, Naresh Singh, Joe Skorupa, Gartner (March 2021)

OMDIA

Brought to you by Informa Tech

Leader in global vulnerability research and discovery since 2007

> 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

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. TippingPoint TPS uses statistical models, developed with machine learning techniques, so you can detect and mitigate threats in real time.

Enterprise Vulnerability Remediation (eVR): Quickly remediate vulnerabilities by integrating third-party vulnerability assessments with the TippingPoint solution portfolio. Your team can pull in information from various vulnerability management and incident response vendors (Rapid7, Qualys, Tenable) to map Common Vulnerabilities and Exposures (CVE) to TippingPoint DV filters and act accordingly.

Advanced Threat Analysis: Extend protection from unknown threats through integration with Trend Micro™ Deep Discovery™ Analyzer. TippingPoint 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, TippingPoint TPS provides you with 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, you can provision TippingPoint TPS using redundant links in a transparent active-active or active-passive high availability (HA) mode.

Integrated Advanced Threat Prevention: TippingPoint TPS integrates with Deep Discovery™ advanced threat detection solutions.

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

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

Best-in-Class Threat Intelligence: Trend Micro™ Research 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, you have exclusive access to vulnerability information from our Trend Micro™ Zero Day Initiative™ (ZDI)—for advanced zero-day threat protection. The ZDI is the largest vendor-agnostic bug bounty program. With more than 1,604 vulnerabilities published in 2020, TippingPoint customers are protected an average of 102 days ahead of a vulnerability being patched by the affected vendors.

Virtual Patching: Leverage a powerful and scalable frontline defense mechanism that protects your network from known threats. Vulnerability-based filters provides your team with an effective barrier from all attempts to exploit a particular vulnerability at the network level—rather than the end-user level. This helps you gain control of your 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: The TippingPoint 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 your IT and security administrators the flexibility to deploy protection wherever it is needed.

Centralized Management: The Trend Micro™ TippingPoint™ Security Management System (SMS) delivers a unified policy and element management graphical user interface. This provides you with a single mechanism for monitoring operational information, editing network security policies, configuring elements, and deploying network security policy across your entire infrastructure, whether physical or virtual.

Key Benefits

Pre-emptive threat prevention

TippingPoint TPS, deployed inline, inspects and blocks all directions of traffic (inbound, outbound, and lateral) in real time, protecting your environment against known, unknown, and undisclosed vulnerabilities.

Threat insight and prioritization

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

Real-time enforcement and remediation

Defend your network from the edge to the data center and the cloud with real-time, inline enforcement and automated remediation of vulnerable systems.

TippingPoint TPS achieves a new level of inline, real-time protection, so you have 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, you're given immediate and ongoing threat protection with out-of-the-box recommended settings.

Technical Specifications

Trend Micro offers these performance numbers as an example of expected performance using recommended settings, in a conservatively configured testing lab environment. Customers are encouraged to complete proof-of-concept testing at their own site to confirm the TippingPoint TPS (Threat Protection System) capabilities meet individual requirements[1].

PERFORMANCE SPECIFICATIONS					
9200TXE	Single Appliance	Two-Unit Stack	Three-Unit Stack	Four-Unit Stack	Five-Unit Stack
Inspection Throughput[2]	100Gbps	200Gbps	295Gbps	390Gbps	485Gbps
New Connections Per Second	1M	2M	3M	4M	5M
Max Concurrent Connections	300M	600M	900M	1,200M	1,500M
Latency	<60 microseconds				
TLS Inspection Throughput[3]	25Gbps	N/A[4]			
New TLS Connections Per Second	10,000	N/A			
Max TLS Concurrent Connections	250,000	N/A			
Max imported TLS/SSL Certificates	1,000	N/A			

PHYSICAL SPECIFICATIONS	
Model	9200TXE
Dimensions	18.54" W x 34.10" D x 1.73" H (1RU)
Weight	42lbs (w/ Blank IOMs)
Voltage	100VAC ~ 240VAC, -40VDC ~ -60VDC
Max Fused Power	1500W @110VAC, 2000W @220VAC
Max Power Consumption	1300W w/ 2x 100GbE IOMs
Power Supplies	2x hot swappable, 1 + 1 redundant 1500W/110VAC, 2000W/220VAC
Fans	7x hot swappable
Mounting	19-inch-wide rack
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 Humidity	5% to 95% non-condensing
EMC	Class A, FCC, VCCI, CE Marking EN55032:2014/A11:2020, CISPR: 2015; EN55035:2017/A11:2020, CISPR 35: 2015; EN61000-3-2:2014; EN61000-3-3:2013/A1:2019
Safety	IEC 60950-1:2005, AMD1:2009, AMD2:2013; IEC62368-1:2014
Altitude	Up to 6,500 feet above MSL (2000m)
Mean Time Between Failure (MTBF)	64,589 Hours @ 25C

CONNECTIVITY SPECIFICATIONS			
Model	9200TXE		
Network I/O Modules	Up to 2 Modules from list below		
Management I/O Ports	1GbE Copper or SFP28 RJ-45 Serial		
Stacking I/O Ports	Dual QSFP28-DD		
NETWORK I/O MODULES			
Standard	**Ports**	**Port Speed**	**Part Number**
6-Segment 25GbE SFP28	SFP28/SFP+/SFP	25/10/1Gbps	TPNN0370
4-Segment 100GbE QSFP28	QSFP28/QSFP+	100/40Gbps	TPNN0371
Bypass	**Ports**	**Port Speed**	**Part Number**
4-Segment 25GbE Fiber SR	Multi-mode Fiber (LC Type)	25Gbps	TPNN0374
4-Segment 25GbE Fiber LR	Single-mode Fiber (LC Type)	25Gbps	TPNN0375
2-Segment 100GbE Fiber SR4	Multi-mode Fiber (MPO Type)	100Gbps	TPNN0372
2-Segment 100GbE Fiber LR4	Single-mode Fiber (LC Type)	100Gbps	TPNN0373

[1] Performance tests are run in a lab-based environment with DUT configured using recommended settings. Actual performance may differ in a production network.

[2] Average latency for all packet sizes.

[3] Average packet size of 1024 bytes, 2048bit key with ECDHE-RSA-AES256-GCM-SHA384 cipher.

[4] The initial release of the 9200TXE will not support TLS decryption in a Stacking Configuration