Trend Micro

TIPPINGPOINT® THREAT PROTECTION SYSTEM

Comprehensive network security through actionable security intelligence

The threat landscape continues to evolve both in sophistication and in technology. This means a new security system that is both effective and flexible is needed due to the dynamic nature of the landscape—one that allows you to tailor your security to meet the needs of your network. Selecting a network security platform is a critical decision because it serves as the foundation for advanced network security capabilities now, and in the future. And, given the backdrop of the changing threat landscape, the importance of network security continues to increase, making it a difficult task.

Trend Micro TippingPoint Threat Protection System (TPS) is a powerful network security platform that offers comprehensive threat protection shielding against vulnerabilities, blocking exploits and defending against known and zero-day attacks with high accuracy. It provides industry-leading coverage across the different threat vectors from advanced threats, malware, and phishing, etc., with extreme flexibility and high performance. The TPS uses a combination of technologies, like deep packet inspection, threat 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 networks.

Key Benefits

Neutralize known and unknown malware: Discovers and actively blocks attempts from both known and unknown malware

Unparalleled visibility: Monitor all types of traffic including encrypted traffic to detect and mitigate attacks

Network reliability: Deployed in-line on a purpose built hardware with features designed to deliver high performance under attack

Industry leading threat intelligence: Leverage the leading research team for up-to-date threat coverage for your organizations assets

Comprehensive security solution: Single vendor solution covering network security, advanced threat, and end user protection

KEY FEATURES

On-box SSL

Provides enterprises with the ability to reduce the security blind spots created by encrypted traffic

Machine learning to stop exploit kits in real-time

Statistical models developed with machine learning techniques deliver the ability to detect and mitigate exploit kits in real-time on the TPS

Enterprise vulnerability remediation (eVR)

Enables customers to pull in information from various vulnerability management and incidence response vendors, map Common Vulnerabilities and Exposures (CVEs) to TippingPoint Digital Vaccine filters and take action accordingly

High availability

TPS has multiple fault tolerant features making it ideal for in-line deployment, including hot swappable power supplies, built-in inspection bypass, and zero power high availability (ZPHA)

Integrated protection

The TPS family of products integrates with TippingPoint Advanced Threat Protection, which rates as the most effective "Recommended" breach detection system by NSS Labs[1], to detect and block targeted attacks and advanced threats

Agility and flexibility

TippingPoint TPS is designed to follow your network wherever it moves, whether it's hardware or virtualization

Operational simplicity

TippingPoint Security Management System provides a single point of management for policy and device management

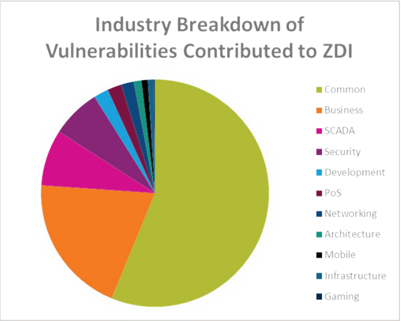
Virtual patching

A powerful and scalable frontline defense mechanism that protects from known threats and relies on the vulnerability-based filters to provide an effective barrier from all attempts to exploit a particular vulnerability

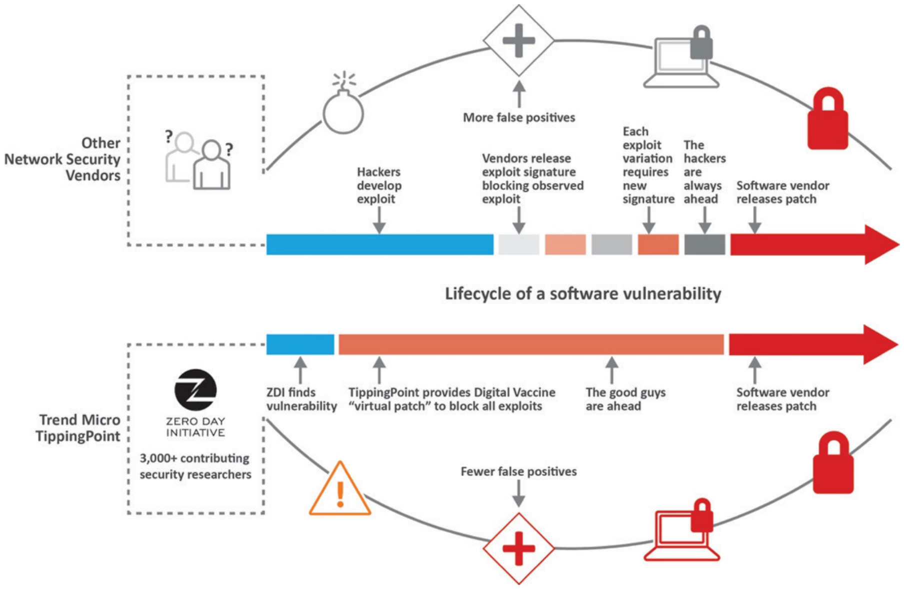
SECURITY EFFECTIVENESS

One of the most critical challenges for security teams is proactively managing the threat landscape without compromising their network's integrity. With the evolving threat landscape, the network security platform must implement a proactive threat framework to respond to zero-day threats. TPS transforms this arduous process into one that relies on proactive threat intelligence combined with an easy-to-use policy framework and out-of-the-box recommended settings. Automatic updates provide immediate and ongoing threat protection with minimal manual effort.

Another aspect of measuring security effectiveness is the time-to-respond for organizations. This metric is often impacted not only based on the how quickly they can discover new threats, but also what actions they can undertake to protect their organization from those threats. This is where TippingPoint's DVLabs and Zero Day Initiative (ZDI) teams play a key role. They focus on advanced research dedicated to understanding, anticipating, and resolving emerging and continuing threats. Through DVLabs internal research efforts and ZDI, TippingPoint delivers continuously updated security coverage to customers, in terms of filters addressing both zero-day vulnerabilities and known vulnerabilities. They also often deliver exploits months in advance, providing critical coverage for security teams.



SOFTWARE VULNERABILITY LIFECYCLE



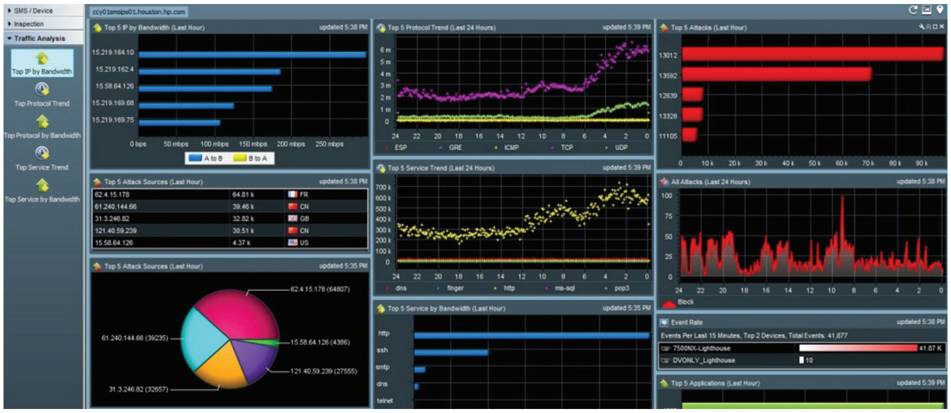
TippingPoint ZDI has the most verified vulnerabilities in 2014 with 317

- Frost & Sullivan 2014 Public Vulnerability Research Market

ZDI published 653 vulnerabilities in 2015

OPERATIONAL SIMPLICITY

There has been an endless proliferation of security vendors and tools from SIEM, IDS, IPS, firewalls, and many other appliances. This is another critical challenge facing security teams– effectively managing their network security deployments. Securing network and data assets within the perimeter, core, or data centers and in hybrid networks (physical and virtual appliances) requires a management framework that spans across multiple boundaries. TippingPoint Security Management System (SMS) appliance provides a single, unified management interface and a global vision and security policy control for large-scale deployments. It delivers robust management functionality and flexible physical and virtual deployment options. Trend Micro TippingPoint Security Management System (SMS) enables "big picture" analysis with trending reports, correlation and real-time graphs on traffic statistics, filtered attacks, network hosts and services, and TippingPoint Next-Generation Intrusion Prevention System (IPS) and Threat Protection System (TPS) inventory and health. The TippingPoint SMS provides a scalable, policy-based operational model and enables straightforward management of large-scale IPS and TPS deployments.



Top 5 Attack Sources (Last Hour) updated 5:38 PM

62.4.15.178	64.81 k	FR
61.240.144.66	39.46 k	CN
31.3.246.82	32.82 k	GB
121.40.59.239	30.51 k	CN
15.58.64.126	4.37 k	US

SMS / Device
Inspection
Traffic Analysis
Top IP by Bandwidth
Top Protocol Trend
Top Protocol by Bandwidth
Top Service Trend
Top Service by Bandwidth
ccy01smsips01.houston.hp.com
Top 5 IP by Bandwidth (Last Hour) updated 5:38 PM
15.219.164.10
15.219.162.4
15.58.64.126
15.219.169.68
15.219.169.75
0 bps 50 mbps 100 mbps 150 mbps 200 mbps 250 mbps
A to B
B to A
Top 5 Protocol Trend (Last 24 Hours) updated 5:39 PM
6 m 5 m 4 m 3 m 2 m 1 m 0
24 22 20 18 16 14 12 10 8 6 4 2 0
ESP GRE ICMP TCP UDP
Top 5 Attacks (Last Hour)
13012
13592
12639
13328
11105
0 10 k 20 k 30 k 40 k 50 k 60 k 70 k 80 k 90 k
Top 5 Service Trend (Last 24 Hours) updated 5:39 PM
700 k 600 k 500 k 400 k 300 k 200 k 100 k 0
dns finger http ms-sql pop3
All Attacks (Last 24 Hours) updated 5:38 PM
100 75 50 25 0
Block
Top 5 Attack Sources (Last Hour) updated 5:35 PM
62.4.15.178 (64807)
61.240.144.66 (39235)
15.58.64.126 (4386)
121.40.59.239 (27555)
31.3.246.82 (32657)
Top 5 Service by Bandwidth (Last Hour) updated 5:35 PM
http
ssh
smtp
dns
telnet
Event Rate updated 5:38 PM
Events Per Last 15 Minutes, Top 2 Devices, Total Events: 41,877
7500NX-Lighthouse 41.87 K
DVONLY_Lighthouse 10
Top 5 Applications (Last Hour) updated 5:39 PM

TippingPoint Security Management System Dashboard

MANAGING THE BLIND SPOTS: ENCRYPTED TRAFFIC

SSL encryption is the cornerstone technology that makes the Internet secure. Email, e-commerce, voice-over-IP, online banking, remote health, and countless other services are kept secure with SSL. Sophisticated and targeted attacks are increasingly using encryption to evade detection by the intrusion prevention systems; this poses a huge challenge for enterprises. In fact, over 25-35 percent[2] of all internet traffic in typical organization is SSL traffic and is projected to increase by roughly 20 percent every year. This leaves a huge gap in the security posture of organizations. TippingPoint TPS eliminates the SSL blind spot by inspecting encrypted SSL traffic on the same box without compromising network performance, using the same management and graphical interface. This makes the administration of the solution simple, and minimizes IT configuration and management demands. Policy-based control provides the ability to determine which SSL encrypted flows should be decrypted for inspection purposes and which should not. It also helps in reducing SSL management and costs by consolidating private key storage and SSL certificate management.

Key Benefits

- On-box SSL eliminates the need for a dedicated SSL appliance (one less appliance in the network to manage)
- SSL enabled to deliver high performance
- Supports 1K, 2K, 4K keys

Features	2200T 1Gbps	2200T 2Gbps
IPS + SSL Throughput	500 Mbps + 500 Mbps	1.5 Gbps + 500 Mbps
Concurrent Sessions	40,000	40,000
New Connections per second	1,200	1,200
Security Contexts	40,000	40,000
Supported Cipher Suites	1k, 2k, 4k	

FLEXIBLE, AGILE, AND ELASTICALLY SCALABLE NETWORK SECURITY

As demands shift from physical to virtual network segments, you need security systems that are physical and virtual to provide flexible and strong protection. The TippingPoint Virtual Threat Protection System (vTPS) provides IPS protection in a virtual form factor to give you the flexibility you need to protect your mixed, physical, and virtual network environment. TPS and vTPS share the same management system to make managing your mixed environment even easier. Share policies and settings across both environments for the most comprehensive protection.

[1] - NSS Breach Detection System Test Report-2015

[2] - https://nsslabs.com/reports/ssl-performance-problems

VIRTUAL THREAT PROTECTION SYSTEM

Performance tests may vary based on CPU architecture and other factors.

Features	TippingPoint vTPS Standard Virtual Appliance
Virtual Platform Support	VMWare ESXi 5.5, 6.0
	NSX is not required for transparent inspection and enforcement
	KVM – Redhat Enterprise Linux 6, 7
Network Drivers	VMWare – VMXNet3
	KVM – virtIO
Number of logical cores	3 or 4
Memory required	8 GB
Disk space required	16GB
Virtual Appliance Specifications	
Performance	Includes 500Mbps inspection license
IPS Concurrent connections	1,000,000
New connections per second	Up to 120K VMware Up to 60K KVM
Number of network segments	1
Number of virtual segments	No limit
Management port	Yes
Management port	Yes

THREAT PROTECTION SYSTEM TECHNICAL SPECIFICATIONS

Features	Threat Protection System 440T TPNN0002	Threat Protection System 2200T TPNN0005
IPS Inspection Throughput	500Mps Upgradeable to 1Gbps	1 Gbps upgradeable to 2 Gbps
SSL Inspection	Not Available	Available
Latency	<100 microseconds	<100 microseconds
Security Contexts	750,000	2,500,000
Concurrent Sessions	7,500,000	10,000,000
New Connections per second	70,000	115,000
Form Factor	1U	2U
Weight	15.28 lbs. (6.93Kg)	26.26 lbs. (11.91Kg)
Dimensions (Wxdxh)	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 console Manageable via Security Management System(SMS), LSM HTTPS web interface, Command-line, TippingPoint MIB	
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+
On-box Storage	8 GB solid state replaceable CFast flash drive	
Voltage	100-240 VAC, 50-60 Hz	
Current (max. fused power)	4-2 A	12-6 A
Max power consumption	250W(853 BTU/hour)	493W(1,682 BTU/hour)
Power supply	Single fixed	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 60950-1 EN 60950-1,CSA 22.2 60950-1 RoHS Compliance	
EMC	Class A, FCC, VCCI, KC EN55022, CISPR 22, EN55024 CISPR 24, EN61000-3-2 EN61000-3-3, CE Marking	

*Test methodology: RFC2544 with 0 drop UDP packets for throughput and latency for all packet sizes

TREND MICRO™

Securing Your Journey to the Cloud