Trend Micro™

TippingPoint™ Security Management System

Centralized management with integrated security policy, response, and visibility

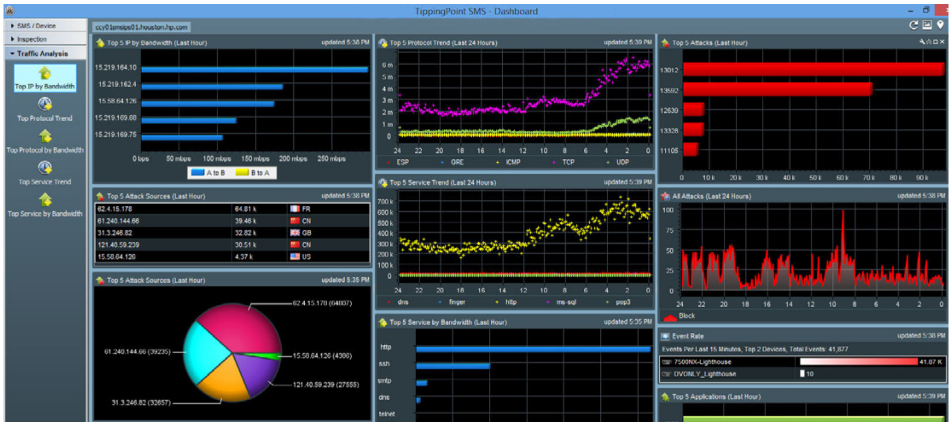
Trend Micro™ TippingPoint™ Security Management System (SMS) provides a scalable, policy-based operational model and enables straightforward management of large-scale Trend Micro™ TippingPoint™ deployments.

TippingPoint SMS enables:

- Big-picture analysis with trending reports
- Correlation and real-time graphs on traffic statistics
- Filtered attacks
- Network hosts and services
- Inventory and health status for TippingPoint devices

A significant component of TippingPoint SMS is the dashboard. It provides at-a-glance monitoring and launch capabilities into targeted management applications.

It also presents an overview of current performance for all TippingPoint devices in the network, including notifications of updates and potential issues that may need attention. Customers can customize the TippingPoint SMS dashboard to their specific needs by using a dashboard palette of drag-and-drop configurable gadgets that are categorized by health and task status, inspection event, event rate, security, reputation, application, and user.



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

Events Per Last 15 Minutes, Top 2 Devices, Total Events: 41,877

7500NX-Lighthouse	41.87 K
DVONLY_Lighthouse	10

TippingPoint SMS Dashboard

Key Features

- Global security device configuration and monitoring.
- Flexible network security policy management shared across TippingPoint devices.
- SMS Threat Insights, prioritizing incident response measures and providing visibility into correlated threat data.
- The ability to simplify and automate advanced and external actions with Active Responder.
- Centralized security feed management for Trend Micro™ Digital Vaccine™ (DV) and Trend Micro™ Threat Digital Vaccine (ThreatDV) services.
- The ability to manage URL reputation feed, with support for enforcement of user-provided malicious URL entries with full API management.
- Enterprise Vulnerability Remediation (eVR), to map vulnerabilities to Trend Micro™ Digital Vaccine™ Threat Intelligence and remediate discovered vulnerabilities with a virtual patch.
- The ability to detect and block network traffic bi-directionally based on geographic region or country.
- The ability to submit potential threats identified by TippingPoint to a sandbox for advanced threat analysis and automated blocking.
- Centralized certificate repository for the SMS and managed TippingPoint devices with on-box SSL inspection enabled.

Continuing on page 2...

Threat Visibility and Prioritization

SMS Threat Insights is an aggregation portal that takes events from TippingPoint devices, vulnerability scanners, and sandboxing solutions, and displays them in one place to prioritize, automate, and consolidate network threat information.

This allows multiple security groups to have a common framework for discussion and resolution. By correlating and automating threat data from multiple security tools, SMS Threat Insights assist security professionals by prioritizing incident response measures for breaches or potential vulnerabilities. The portal provides views and actionable data on:

Breached hosts

Information is correlated from TippingPoint and Trend Micro™ Deep Discovery™ Analyzer (sandbox) to help prioritize events for response. Security professionals can isolate, seek out, and quarantine users on the network who appear to be infected or acting suspiciously.

Attacked vulnerable hosts

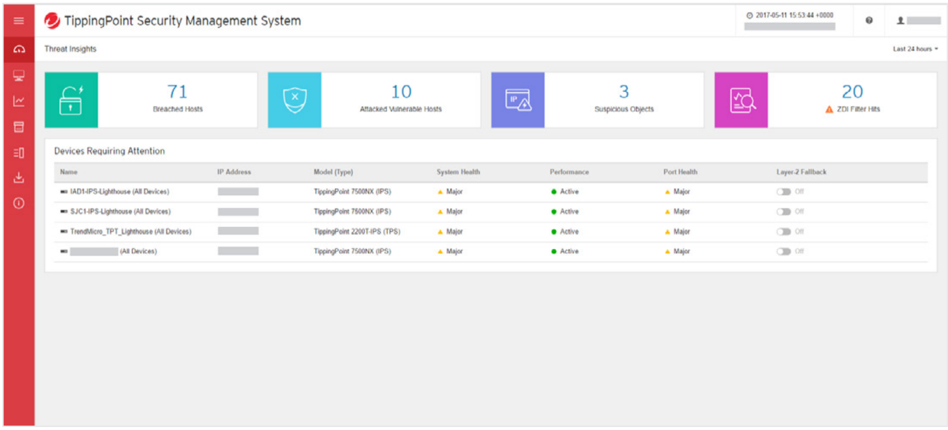
Integrated with third-party vulnerability scanners (Rapid7, Tenable, and Qualys) to prioritize Trend Micro DV filters based on actual vulnerabilities in a unique environment. This gives users the ability to quickly enable filters in which they may have been previously unaware.

Suspicious objects

Incident response is integrated between Trend Micro™ Deep Discovery™ and TippingPoint via the SMS. By automatically submitting identified potential threats (like URLs) from TippingPoint to the Deep Discovery sandbox, it isolates and investigates the risk, converting unknown, potential threats into known threats. These suspicious objects can then be viewed in SMS Threat Insights to ensure that users are protected.

Trend Micro™ Zero Day Initiative™ (ZDI) filter hits

Undisclosed threats are vulnerabilities that are unknown to the public—outside of Trend and the impacted software vendor—that could potentially be zero-day threats. The Trend Micro Forward-Looking Threat Research (FTR) team, in collaboration with ZDI, provides preemptive protection from undisclosed and zero-day threats through exclusive access to vulnerability information. In most cases, this preemptive protection is available before a vulnerability is disclosed or exploited. SMS Threat Insights display filters that trigger on the potentially most impactful threats to give security response teams visibility into the high-priority, undisclosed zero-day filters protecting vulnerabilities in their environment and help prioritize events that may require immediate action.



Devices Requiring Attention

Name	IP Address	Model (Type)	System Health	Performance	Port Health	Layer-2 Fallback
IAD1-IPS-Lighthouse (All Devices)	[redacted]	TippingPoint 7500NX (IPS)	▲ Major	● Active	▲ Major	Off
SJC1-IPS-Lighthouse (All Devices)	[redacted]	TippingPoint 7500NX (IPS)	▲ Major	● Active	▲ Major	Off
TrendMicro_TPT_Lighthouse (All Devices)	[redacted]	TippingPoint 2200T-IPS (TPS)	▲ Major	● Active	▲ Major	Off
[redacted] (All Devices)	[redacted]	TippingPoint 7500NX (IPS)	▲ Major	● Active	▲ Major	Off

Key Features

- Active Directory (AD) integration for prioritized network user context and reporting.
- Visualization of all network traffic when combined with the latest generation of TippingPoint solutions.
- Advanced reporting and Trend Micro analysis of security events and network usage.
- The ability to integrate with SIEM, breach detection, and other third-party security solutions.

Advanced Threat Analysis

TippingPoint solutions can automatically block known and undisclosed vulnerabilities from the network. Through added forensic capabilities, the TippingPoint solution can automatically forward unknown or suspicious indicators of compromise (IoC) to SMS Threat Insights. It can then confirm if IoCs are malicious through Deep Discovery Analyzer for in-depth sandbox analysis and remediation without changing policy or altering network infrastructure.

Advanced Policy Definition

Policies can be defined based on physical segments, virtual local area network (VLAN), IP range, and direction. Security policies can be easily changed to fit the rhythm of business operations and be automatically adjusted as threats arise.

Digital Vaccine and Threat Digital Vaccine (ThreatDV) Distribution

The TippingPoint Threat Management Center (TMC) distributes filter updates through weekly DV packages to protect systems against known and zero-day threats. The TippingPoint SMS can be configured to automatically check for, download, and distribute filter updates to TippingPoint devices.

Automated Event Actions

Included with the TippingPoint SMS is Active Responder, an automated response system that allows users to specify an action in response to a security event. This can range from directing a user to a self-remediation site, generating a trouble ticket, or if the event is severe enough, moving them to a secure VLAN or removing them from the network.

Enterprise Vulnerability Remediation (eVR)

With eVR, customers can import vulnerability data from vulnerability assessment and vulnerability management (VA/VM) vendors (including Qualys, Rapid7, and Tenable), map common vulnerability exposures (CVEs) to DV filters, and take immediate action based on the enhanced threat intelligence to increase their security coverage.

Geo/Location Filtering

TippingPoint SMS can be configured to detect and block network traffic based on a computer's IP address and host name within a geographic region or country.

Customers can establish an action set associated with geographic filters to minimize or eliminate communications with potentially risky systems.

Microsoft Active Directory (AD) Integration

TippingPoint SMS can provide visibility, enhanced context, and reporting on the traffic of a particular user through AD integration. The username, domain, machine, and user group are all tracked and available for forensics, reporting, and filtering results (for example, see all attacks targeted to machine X or from user Y). Administrators can also see the IP history of a particular AD user or the user history for a particular IP.

Comprehensive Network Traffic Visualization

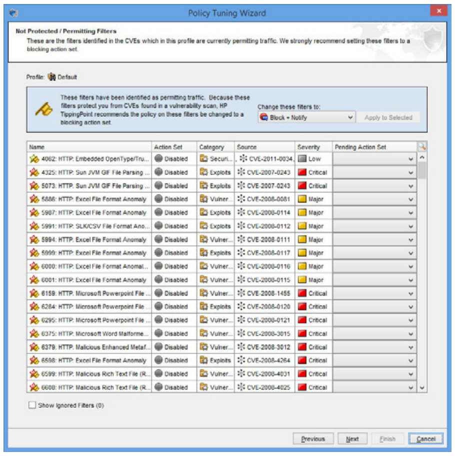
TippingPoint solutions can support the export of network flow data statistics for visualization and analysis. With TippingPoint SMS, statistics and flow data summaries can be viewed and analyzed to optimize performance and help identify compromised hosts as well as other suspicious and malicious network traffic.

OMDIA

Leader in global vulnerability research and discovery since 2007.

Gartner

Ranked #1 in Gartner IDPS Market Share worldwide @ 23.5% share for 2020[1]



Policy Tuning Wizard

Not Protected / Permitting Filters

These are the filters identified in the CVEs which in this profile are currently permitting traffic. We strongly recommend setting these filters to a blocking action set.

Profile: Default

These filters have been identified as permitting traffic. Because these filters protect you from CVEs found in a vulnerability scan, HP TippingPoint recommends the policy on these filters be changed to a blocking action set.

Change these filters to: Block + Notify

Name	Action Set	Category	Source	Severity	Pending Action Set
4062: HTTP: Embedded OpenType/Tru...	Disabled	Securi...	, CVE-2011-0034,	Low	
4325: HTTP: Sun JVM GIF File Parsing ...	Disabled	Exploits	CVE-2007-0243	Critical	
5073: HTTP: Sun JVM GIF File Parsing ...	Disabled	Exploits	CVE-2007-0243	Critical	
5886: HTTP: Excel File Format Anomaly	Disabled	Vulner...	CVE-2008-0081	Major	
5987: HTTP: Excel File Format Anomaly	Disabled	Exploits	CVE-2008-0114	Major	
5991: HTTP: SLK/CSV File Format Ano...	Disabled	Exploits	CVE-2008-0112	Major	
5994: HTTP: Excel File Format Anomaly	Disabled	Vulner...	CVE-2008-0111	Major	
5999: HTTP: Excel File Format Anomaly	Disabled	Exploits	CVE-2008-0117	Major	
6000: HTTP: Excel File Format Anomal...	Disabled	Vulner...	CVE-2008-0116	Major	
6001: HTTP: Excel File Format Anomaly	Disabled	Vulner...	CVE-2008-0115	Major	
6159: HTTP: Microsoft Powerpoint File ...	Disabled	Vulner...	CVE-2008-1455	Critical	
6284: HTTP: Microsoft Powerpoint File ...	Disabled	Exploits	CVE-2008-0120	Critical	
6295: HTTP: Microsoft Powerpoint File ...	Disabled	Vulner...	CVE-2008-0121	Critical	
6375: HTTP: Microsoft Word Malforme...	Disabled	Vulner...	CVE-2008-3015	Critical	
6379: HTTP: Malicious Enhanced Metaf...	Disabled	Vulner...	CVE-2008-3012	Critical	
6598: HTTP: Excel File Format Anomaly	Disabled	Exploits	CVE-2008-4264	Critical	
6599: HTTP: Malicious Rich Text File (R...	Disabled	Vulner...	CVE-2008-4031	Critical	
6608: HTTP: Malicious Rich Text File (R...	Disabled	Vulner...	CVE-2008-4025	Critical	

☐ Show Ignored Filters (0)

Device Configuration and Monitoring

TippingPoint SMS management can scale up to hundreds of devices or drill down deep into the internal workings of TippingPoint devices. In addition, a single client can operate across multiple TippingPoint SMSes for even greater scalability. Network parameters, as well as TippingPoint device and filter behaviors, can be viewed, assessed, and tuned from one interface.

Third-Party Integration

TippingPoint SMS integrates with several third-party security solutions using APIs to enhance a layered approach to security. These APIs can be used to integrate with existing security tools to enhance response and control across the network. Customers can gain visibility into their network to make informed decisions and take immediate action on any potential threats to infrastructure or data. TippingPoint SMS can integrate with leading SIEM, VA/VM, breach detection, and other complementary security solutions.

SMS Technical Specifications

Physical Appliance Specifications

	TIPPINGPOINT SMS H4 APPLIANCE		TIPPINGPOINT SMS H4 XL APPLIANCE	
Physical Characteristics				
Manufacturer	Dell	HPE	Dell	HPE
Dimensions	48.18 x 74.39 x 4.27 cm (18.97 x 29.29 x 1.68 in.)	45.46 x 70.69 x 4.29 cm (17.11 x 27.83 x 1.69 in.)	48.18 x 74.39 x 4.27 cm (18.97 x 29.29 x 1.68 in.)	45.46 x 70.69 x 4.29 cm (17.11 x 27.83 x 1.69 in.)
Form Factor	1U rack mount		1U rack mount	
Weight	21.9 kg (48.3 lb)	37.0 lb	21.9 kg (48.3 lb)	37.0 lb
Memory and Storage	64 GB RAM, 800 GB storage (2 x 800 GB disks, RAID 1)		96 GB RAM, 2.4 TB storage (6 x 800 GB disks, RAID 1+0)	
Environment				
Operating Temperature	10 to 35°C (50 to 95°F)		10 to 35°C (50 to 95°F)	
Electrical Characteristics				
Power Supply	Redundant 495 W (hot swappable)	Redundant 500 W (hot swappable)	Redundant 750 W (hot swappable)	Redundant 800 W (hot swappable)
Voltage	100 to 120 VAC or 200 to 240 VAC		100 to 120 VAC or 200 to 240 VAC	
Frequency	50/60 Hz		50/60 Hz	
MAX Power Consumption	281 W (2.6 A @ 110 VAC, 1.2 A @ 240 VAC)	279 W (2.6 A @ 110 VAC, 1.2 A @ 240 VAC)	413 W (3.8 A @ 110 VAC, 1.7 A @ 240 VAC)	401 W (3.7 A @ 110 VAC, 1.7 A @ 240 VAC)
Capacity				
	200 million historical events		600 million historical events	
			Provides additional processing and storage recommended for deployments larger than 150 devices	
OOB Remote Management	Dell iDRAC9 enterprise w/ GbE RJ45	HPE iLO 5 advanced w/ GbE RJ45	Dell iDRAC9 enterprise w/ GbE RJ45	HPE iLO 5 advanced w/ GbE RJ45

Virtual Appliance Specifications

	TIPPINGPOINT VSMS ENTERPRISE VIRTUAL APPLIANCE
Hypervisor Support	VMware ESX/ESXi v5.5 update 1 or later KVM
Resources	300 GB of disk space (min); 2 virtual CPUs 12 GB of memory (min); 2 virtual NICs
Capacity	100 million historical events

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

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