Datasheet

Trend Micro™ TippingPoint™ Security Management System (SMS)

Centralized management with integrated security policy, response, and visibility

TippingPoint SMS provides you with a scalable, policy-based operational model. Use it to enable straightforward management of your large-scale Trend Micro™ TippingPoint™ deployments.

TippingPoint SMS enables you to:

- Gain big-picture analysis with trending reports
- Leverage correlation and real-time graphs on traffic statistics
- Filter attacks
- Manage network hosts and services
- Analyze inventory and health status of TippingPoint devices

TippingPoint SMS dashboard

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

It also presents an overview of current performance for all TippingPoint devices on your network, including notifications of updates and potential issues that may need your attention. Customize the TippingPoint SMS dashboard to suit your needs via a palette of drag-and-drop configurable gadgets categorized by health and task status, inspection event, event rate, security, reputation, application, and user.

Figure 1: TippingPoint SMS dashboard

Key benefits

- Enable global security device configuration and monitoring
- Implement flexible network security policy management across TippingPoint devices
- Prioritize incident response measures and gain visibility into correlated threat data using Threat Insights
- Simplify and automate advanced and external actions with Active Responder
- Centralize security feed management for Trend Micro™ Digital Vaccine™ and Trend Micro™ Digital Vaccine™ Threat Intelligence (DVTI) services
- Manage your URL reputation feed and support enforcement of user-provided malicious URL entries with full API management
- Use Enterprise Vulnerability Remediation (eVR) to map vulnerabilities to DVTI and remediate discovered vulnerabilities with a virtual patch
- Detect and block network traffic bi-directionally based on geographic region or country

Threat visibility and prioritization

Leverage our Trend Vision One™ – Threat Insights aggregation portal to display events from TippingPoint devices, vulnerability scanners, and sandboxing solutions in one place. This helps you prioritize, automate, and consolidate your network threat information and equips multiple security groups with a common framework for discussion and resolution. By correlating and automating threat data from multiple security tools, Threat Insights assists helps you prioritize incident response measures for breaches or potential vulnerabilities.

Threat Insights 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. Isolate, seek out, and quarantine users on your network who appear to be infected or acting suspiciously.

Attacked vulnerable hosts

Integrate with third-party vulnerability scanners to prioritize Digital Vaccine filters based on actual vulnerabilities in a unique environment. This enables your users to quickly enable filters that they might not have known about before.

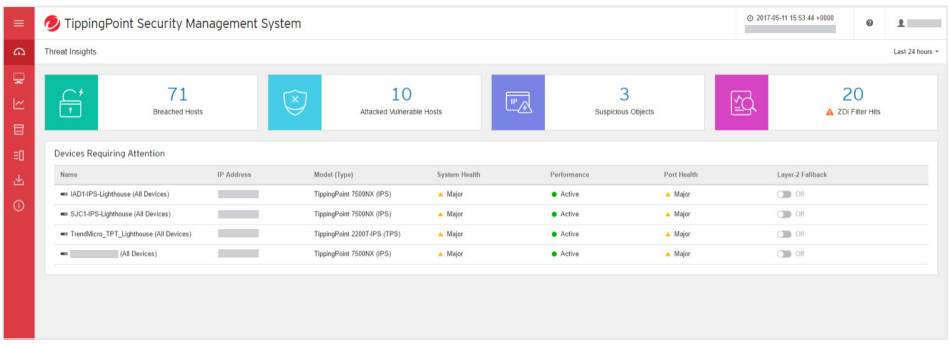
Suspicious objects

Incident response is integrated between Trend Micro™ – Deep Discovery™ and TippingPoint SMS. Automatically submit identified potential threats (such as URLs) from TippingPoint to the Deep Discovery sandbox to isolate and investigate risks. This also enables you to convert unknown, potential threats into known threats. These suspicious objects can then be viewed in Threat Insights to ensure your users are protected.

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

Undisclosed threats are vulnerabilities that are unknown to the public—outside of Trend Micro and the impacted software vendor—that could potentially be zero-day threats. The Trend™ Research team, in collaboration with ZDI, provides preemptive protection from undisclosed and zero-day threats with proactive insights on vulnerability information. In most cases, this preemptive protection is available before a vulnerability is disclosed or exploited. Threat Insights displays filters that trigger on the potentially most impactful threats, giving your security response teams visibility into the high-priority, undisclosed zero-day filters protecting vulnerabilities in their environment. This helps you prioritize events that may require immediate action.

Figure 2: Threat Insights overview



Additional benefits

- Submit potential threats identified by TippingPoint to a sandbox for advanced threat analysis and automated blocking
- Centralize your certificate repository for TippingPoint SMS and managed TippingPoint devices with on-box SSL inspection enabled
- Integrate Microsoft Active Directory (AD) for prioritized network user context and reporting
- Visualize all network traffic when combined with the latest TippingPoint solutions
- Leverage advanced reporting and analysis of security events and network usage
- Integrate with security information and event management (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, they can automatically forward unknown or suspicious indicators of compromise (IoC) to Threat Insights. Deep Discovery Analyzer can then confirm whether IoCs are malicious through in-depth sandbox analysis and remediation—all without changing your policy or network infrastructure.

Advanced policy definition

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

Digital Vaccine and DVTI distribution

The TippingPoint Threat Management Center (TMC) distributes filter updates through weekly Digital Vaccine 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. It can direct a user to a self-remediation site, generate a trouble ticket or, for severe events, move them to a secure VLAN or remove them from the network.

Enterprise vulnerability remediation (eVR)

With eVR, you 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 your security coverage.

Geographic and 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. 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, you can 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

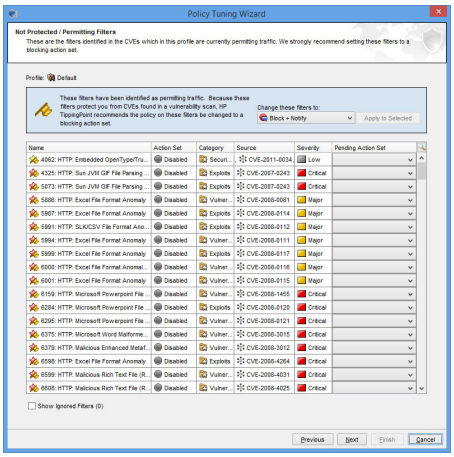
TippingPoint solutions can support the export of network flow data statistics for visualization and analysis. With TippingPoint SMS, your statistics and flow data summaries can be viewed and analyzed to optimize performance and help identify compromised hosts as well as other suspicious and malicious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

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

Leader in global vulnerability research and discovery since 2007

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

Figure 3: Policy tuning wizard



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 SMS instances for even greater scalability. Your network parameters—as well as your 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 your network. Gain visibility into your 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.

TippingPoint SMS technical specifications

Physical appliance specifications

Features	TippingPoint SMS H5 appliance	Tippingpoint SMS H5 XL appliance
Manufacturer	Dell	Dell
Dimensions	4.27 cm H x 48.22 cm W x 75.85 cm D (1.68" H x 18.97" W x 29.85" D)	4.27 cm H x 48.22 cm W x 75.85 cm D (1.68" H x 18.97" W x 29.85" D
Form factor	1U rack mount	1U rack mount
Weight	18.2 kg (40.1 lbs)	18.2 kg (40.1 lbs)
Memory and storage	64 GB RAM 800 GB storage (2 x 800 GB SSD, RAID 1)	128 GB RAM 2.4 TB storage (6 x 800 GB disks, RAID 10)
Operating temperature	10°C – 35°C (50°F – 95°F)	10°C – 35°C (50°F – 95°F)
Power supply	Dual 1100 W PSUs (1+1 redundant, hot-swappable)	Dual 1100 W PSUs (1+1 redundant, hot-swappable)
Voltage	100 VAC ~ 240 VAC	100 VAC ~ 240 VAC
Frequency	50/60 Hz	50/60 Hz
Maximum power consumption	476W	598W
Capacity	200 million historical events	600 million historical events
Additional processing		Provides additional processing and storage recommended for deployments larger than 150 devices
Ethernet management connectivity	Dual 1GbE RJ45 / Dual 25GbE SFP28	Dual 1GbE RJ45 / Dual 25GbE SFP28
Out-of-box remote management	Dell iDRAC9 Enterprise w/ GbE RJ45 DB9 serial / DB15 VGA + USB keyboard	Dell iDRAC9 Enterprise w/ GbE RJ45 DB9 serial / DB15 VGA + USB keyboard

	TippingPoint SMS enterprise virtual appliance
Hypervisor support	VMware ESX/ESXi v7.0 or 8.0 / KVM
Resources	Storage: 600 GB (recommended) Compute: 8 virtual CPUs Memory: 32 GB (minimum)
Capacity	100 million historical events