Trend Micro

TIPPINGPOINT® SECURITY MANAGEMENT SYSTEM

Centralized management with integrated security policy, response, and visibility

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 inventory and health status for TippingPoint devices. The TippingPoint SMS provides a scalable, policy-based operational model, and enables straightforward management of large-scale TippingPoint deployments.

A significant component of TippingPoint SMS is the dashboard. It provides at-a-glance monitoring and launch capabilities into targeted management applications, and an overview of current performance for all TippingPoint devices in the network, including notifications of updates and potential issues that may need attention. Customers are also able to customize the SMS dashboard to their specific needs using a dashboard palette of drag-and-drop configurable gadgets that are categorized by health and status, task status, inspection event, event rate, security, reputation, application, and user.

TippingPoint Security Management System Dashboard

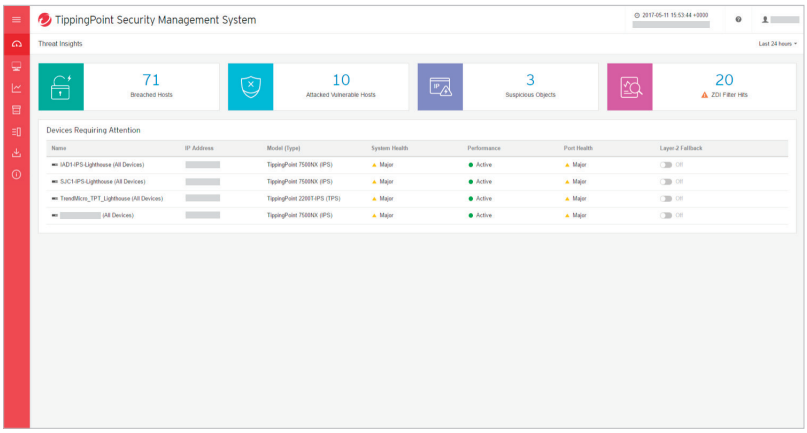
Key Features

- Global security device configuration and monitoring
- Flexible network security policy management shared across TippingPoint devices
- SMS Threat Insights prioritizes incident response measures and provides visibility into correlated threat data
- Simplify and automate advanced and external actions with Active Responder
- Centralized security feed management for Digital Vaccine® and Threat Digital Vaccine (ThreatDV) service
- Manage URL reputation feed with support for enforcement of user-provided malicious URL entries with full API management
- Enterprise Vulnerability Remediation (eVR) maps vulnerabilities to Digital Vaccine threat intelligence and remediates discovered vulnerabilities with a virtual patch
- Detect and block network traffic bi-directionally based on geographic region or country
- 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
- Active Directory (AD) integration provides network user context and reporting
- Visualization of all network traffic when combined with latest generation TippingPoint solutions
- Advanced reporting and trend analysis of security events and network usage
- Integrate with SIEM, breach detection, and other third-party security solutions

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 assists security professionals by prioritizing incident response measures for breaches or potential vulnerabilities. The portal provides views and actionable data on:



Breached hosts: Correlates breached host information from TippingPoint and the 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.

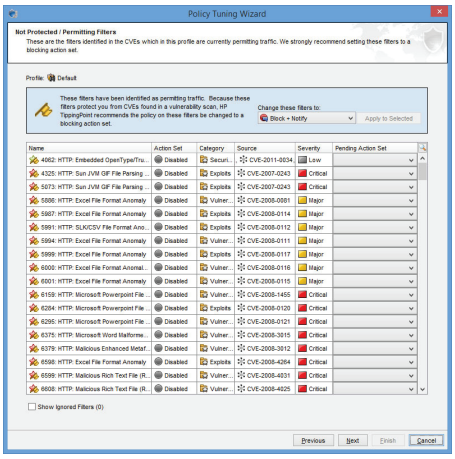
Attacked vulnerable hosts: Integrates with third-party vulnerability scanners (Rapid7, Tenable, and Qualys) to prioritize Digital Vaccine® (DV) filters based on actual vulnerabilities in a unique environment, which gives users the ability to quickly enable filters they may have been previously unaware of.

Suspicious objects: Incident response integration between 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 threat, turning unknown, potential threats into known threats. These suspicious objects can then be viewed in SMS Threat Insights to ensure users are protected.

ZDI filter hits: Undisclosed threats are vulnerabilities that are not publicly known outside of Trend Micro and the impacted software vendor that could be potential zero-day threats. The TippingPoint Digital Vaccine® Labs (DVLabs) team, working together with the Zero Day Initiative (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 displays filters that trigger on what may be the most impactful threats, gives security response teams visibility into the high-priority, undisclosed zero-day filters protecting vulnerabilities in their environment, and helps prioritize events that may require immediate action.

ADVANCED THREAT ANALYSIS

TippingPoint solutions are able to automatically block known and undisclosed vulnerabilities from the network. Through added forensics capabilities, the TippingPoint device can automatically forward unknown or suspicious indicators of compromise (IOCs) to SMS Threat Insights. It can then confirm if IOCs are malicious through the Deep Discovery Analyzer for in-depth sandbox analysis and remediation, all 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 adjusted automatically as threats arise.

DIGITAL VACCINE® AND THREATDV DISTRIBUTION

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

AUTOMATED EVENT ACTIONS

Included with the TippingPoint SMS is an automated response system called Active Responder 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 removal from the network.

ENTERPRISE VULNERABILITY REMEDIATION (EVR)

With Enterprise Vulnerability Remediation (eVR), customers can import vulnerability data from VA/VM vendors including Qualys, Rapid7 and Tenable, map CVEs to Digital Vaccine 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.

ACTIVE DIRECTORY INTEGRATION

TippingPoint SMS can provide visibility, enhanced context, and reporting on the traffic of a particular user through Active Directory (AD) integration. The user name, domain, machine, and user group are all tracked and available for forensics, reporting, and filtering results (e.g., 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 and other suspicious and malicious network traffic.

DEVICE CONFIGURATION AND MONITORING

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 SMSs 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.

Powered by XGen™ security

Trend Micro TippingPoint solutions are powered by XGen™ security, a smart, optimized and connected security approach

A LEADER

IN GARTNER 2017 IDPS MAGIC QUADRANT

SMS TECHNICAL SPECIFICATIONS

Physical Appliance Specifications

Features	TIPPINGPOINT SECURITY MANAGEMENT SYSTEM H3 APPLIANCE	TIPPINGPOINT SECURITY MANAGEMENT SYSTEM H3 XL APPLIANCE
Physical characteristics		
Dimensions	43.47 x 69.85 x 4.32 cm (17.11 x 27.5 x 1.7 in.)	44.55 x 67.94 x 8.73 cm (17.54 x 26.75 x 3.44 in.)
Form factor	1U rack mount	2U rack mount
Weight	16.78 kg (36.99 lb)	23.6 kg (51.5 lb)
Memory, processor, and storage	2x Intel® Xeon® E5-2620 v3 (2.4 GHz/6-core/15 MB/85 W) 64 GB RAM 600 GB storage (2 x 600 GB disks, RAID 1)	2x Intel Xeon E5-2690 v3 (2.6 GHz/12-core/30 MB/135 W) 96 GB RAM 1.8 TB storage (6 x 600 GB, RAID 1+0)
Environment		
Operating Temperature	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)
Electrical Characteristics		
Voltage	100 to 120 VAC, 200 to 240 VAC	100 to 120 VAC, 200 to 240 VAC
Frequency	50/60 Hz	50/60 Hz
Current	2.78 A (100 V) to 1.15 A (240 V)	4.58 A (100 V) to 1.88 A (240 V)
Power Supply	Redundant 500 W (Hot swappable)	Redundant 800 W (Hot swappable)
Capacity		
	200 million historical events	600 million historical events
		Provides additional processing and storage recommended for deployments larger than 150 devices
Lights-out management support	HPE iLO 4 support with a dedicated 10/100/1000BASE-T RJ45 iLO port	HPE iLO 4 support with a dedicated 10/100/1000BASE-T RJ45 iLO port

Virtual Appliance Specifications

Features	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	200 million historical events

TREND MICRO™

Securing Your Journey to the Cloud