Trend Micro

TIPPINGPOINT® VIRTUAL THREAT PROTECTION SYSTEM

Comprehensive network security for your physical and virtual environments

PLATFORM OVERVIEW

The threat landscape continues to evolve and so does your network infrastructure. As demands shift from physical to virtual network segments, you need security systems that are physical and virtual to provide flexible and strong protection at the same time. Enterprises need security solutions that are designed to protect both virtualized and physical environments, also known as heterogeneous or mixed environments. They also need a solution that can be managed, provisioned and licensed in an effective way to provide optimal protection, while maintaining a strong total cost of ownership (TCO). Protecting your heterogeneous environment with security solutions designed for physical environments can leave gaps in your protection. Your mixed environment requires a set of security solutions to protect both areas uniquely, managed through a single pane of glass.

Trend Micro TippingPoint Virtual Threat Protection System (vTPS) is a powerful network security platform that offers comprehensive threat protection against attacks. It blocks vulnerabilities and exploits, and defends against known and zero-day attacks with high accuracy. It provides industry-leading coverage across the different threat vectors from hackers, malware, and phishing with extreme flexibility and high performance. The vTPS uses a combination of technologies, including but not limited to, deep packet inspection, threat reputation, and advanced malware analysis on a flow-by-flow basis—to detect and prevent attacks on the network. The vTPS enables enterprises to take a proactive approach to security by providing 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

Proven in-line threat protection

Flexible
Embrace the software-defined network protection by deploying IPS as a service on your hardware.

Focused
Target network security policies precisely for the applications services and users on your network.

Control
Network-based security brought to the edge of every host, bringing visibility and control without impacting endpoints.

KEY FEATURES

Machine learning to stop exploit kits in real-time
Uses statistical models developed with machine learning techniques and delivers the ability to detect and mitigate exploit kits in real-time.

Block advanced threats
Integrates with TippingPoint Advanced Threat Protection to block targeted attacks and advanced persistent threats that may have slipped past existing defenses providing a defense in depth approach.

Enterprise vulnerability remediation (eVR)
Pulls in information from various vulnerability management and incidence response vendors, maps Common Vulnerabilities and Exposures (CVEs) to TippingPoint Digital Vaccine filters, and takes action accordingly.

Virtual patching
Powerful frontline defense mechanism that can be deployed in minutes to protect from known threats, relying on the vulnerability-based filter within vTPS, which blocks attempts to exploit a particular software flaw.

Agility and flexibility
Supports VMware, KVM, and OpenStack environments, allowing you to choose the virtual solution that best meets your requirements, regardless of the security that supports it.

Operational simplicity
TippingPoint Security Management System provides a single point of management for policy and device management across your physical or virtual network segments.

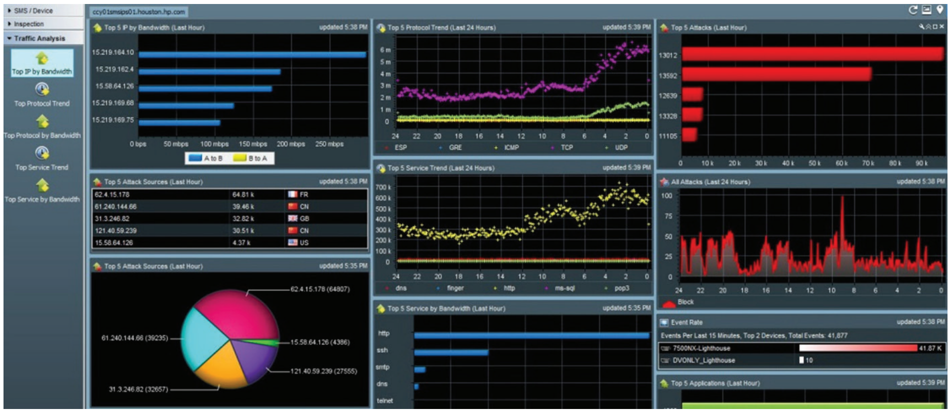
Budget minded TCO
Network independent architecture that doesn't require costly add-ons or products.

Flexible deployment scenarios

- Deploying IPS as a service in a consolidated set of virtualized infrastructure services at remote branches
- Offering an IPS service to protect virtualized applications from within your virtualized infrastructure
- Where IPS services are needed and custom hardware may not be an option
- Lab environments where virtual infrastructure can be quickly redeployed
- IPS services designed to be enforced at the network – no agent required

OPERATIONAL SIMPLICITY

One of the most critical challenges facing security teams is effectively managing their network security deployments. Securing network and data assets within the perimeter, core, or data centers and in hybrid networks, including both physical and virtual appliances, requires the management framework to span across multiple boundaries. TippingPoint Security Management System (SMS) appliance provides a 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.



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 Security Management System Dashboard

Integrated protection

The TPS family of products integrates with TippingPoint Advanced Threat Protection, the most effective recommended breach detection system by NSS Labs, to detect and block targeted attacks and advanced threats. Along with multiple scanning engines, Advanced Threat Detection will detonate and analyze these stealthy threats in a safe sandboxing environment. This allows the TPS and vTPS to block inbound and outbound command and control communication, lateral movement, and quarantine the infected hosts—ultimately preventing the spread of the attack.

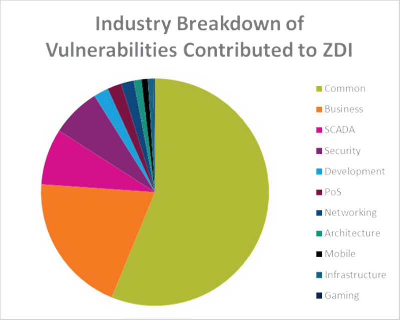
SECURITY EFFECTIVENESS

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.

TippingPoint Digital Vaccine (DVLabs) team and Zero Day Initiative (ZDI) focus on advanced research to secure enterprise networks, business-critical data, and application vulnerabilities, helping customers reduce their risk and enhance their security investment. ZDI continuously undertakes extensive research dedicated to understanding, anticipating, and resolving emerging and continuing malware threats. Through DVLabs internal research efforts and TippingPoint ZDI, TippingPoint delivers constantly updated security coverage to customers.

TippingPoint TPS transforms this difficult process into one which relies on proactive threat intelligence, an easy-to-use policy framework, and out-of-the-box recommended settings with automatic updates, and provides immediate and ongoing threat protection with little manual effort. TippingPoint incorporates the ability to correlate a variety of network topologies, threats, and reputation data. This helps security teams correlate the threat activity with the application usage to enable informed decisions.

ZERO DAY
INITIATIVE



Virtual Threat Protection System Performance tests may vary based on CPU architecture and other factors.	
	TippingPoint vTPS Standard Virtual Appliance TPNM0034
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

Securing Your Journey to the Cloud