TREND MICRO™

Trend Micro

TIPPINGPOINT® NEXT-GENERATION INTRUSION PREVENTION SYSTEM NX SERIES

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 to adapt 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 an increasingly difficult task.

Trend Micro TippingPoint Next-Generation Intrusion Prevention System (NGIPS) achieves a new level of in-line, real-time protection, providing proactive network security for today and tomorrow's real-world network traffic and data centers. The NX series NGIPS's next-generation architecture adds significant capacity for deep packet traffic inspection, and its modular software design enables the addition of valuable network protection services to its proven intrusion prevention solution. It provides industry-leading coverage across the different threat vectors. The NX series 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. It 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) and Zero Day Initiative (ZDI) provides the visibility and agility necessary to keep pace with today's dynamic, evolving enterprise networks.

KEY FEATURES

Highest port density: The NX series supports market-leading segments across multiple configurations with up to 24 segments of 1GE, 16 segments of 10GE or 4 segments of 40GE

Virtual patching: A powerful and scalable frontline defense mechanism to protect from known threats, relying on the vulnerability-based filters to provide an effective barrier to all attempts to exploit a particular vulnerability

Enterprise vulnerability remediation: 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

Integrated protection: The NX series of products integrates with TippingPoint Advanced Threat Protection; rated as the most effective recommended breach detection system by NSS labs, to detect and block targeted attacks and advanced threats[1]

1 - NSS Breach Detection System Test Report-2015

Key Benefits

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

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

Industry-leading threat intelligence: Leverage the leading research teams of Zero Day Initiative (ZDI) and Digital Vaccine® Labs (DVLabs) for up-to-date threat coverage for your organizations assets

Operational simplicity: TippingPoint Security Management System provides a single point of management for policy and device management
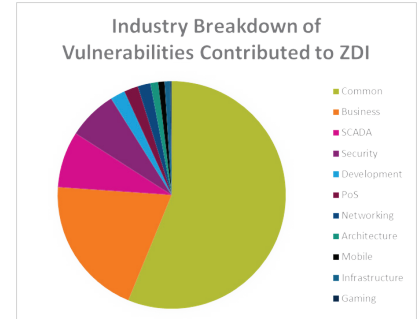
NSSLABS
RECOMMENDED

TippingPoint
RECOMMENDED
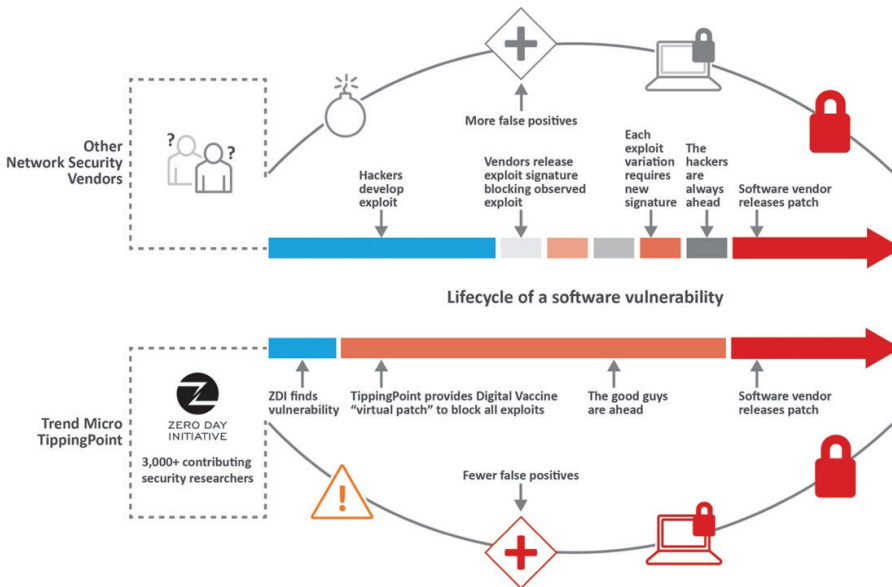Next-Generation IPS

99.5% Security Effectiveness

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 NX Series NGIPS transforms this extremely 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 with automatic updates, it provides 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 how quickly new threats can be discovered, but also what actions they can take to protect their organization from those threats. This is where TippingPoint's Digital Vaccine (DVLabs) team and Zero Day Initiative (ZDI) 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 constantly updated security coverage to customers. The security coverage filters address zero-day vulnerabilities, known vulnerabilities, and exploits often months in advance—providing critical coverage for security teams.

Industry Breakdown of Vulnerabilities Contributed to ZDI

- Common
- Business
- SCADA
- Security
- Development
- PoS
- Networking
- Architecture
- Mobile
- Infrastructure
- Gaming

SOFTWARE VULNERABILITY LIFECYCLE

Lifecycle of a software vulnerability

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

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 a robust management functionality and flexible physical and virtual deployment options.

TippingPoint Security Management System Dashboard

TIPPINGPOINT NX SERIES TECHNICAL SPECIFICATIONS

Features	2600NX	5200NX	6200NX	7100NX	7500NX
IPS Inspection Throughput	3 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps
Security Contexts	2,600,000	2,600,000	4,000,000	5,000,000	5,000,000
Concurrent Sessions	30 Million	30 Million	60 Million	60 Million	60 Million
New Connections per second	300,000	300,000	450,000	450,000	450,000
Latency	<40 microseconds				
Form Factor	2U				
Weight	42 lbs. (19.1Kg)				
Dimensions (WxDxH)	16.8 in. (W) x 21.75 in. (D) x 3.5 in. (H) 42.78 cm x 55.25 cm x 8.89 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	Every NX chassis supports up to 4 hot-swappable I/O modules; With the NX chassis populated with 4 of the SFP+ NX I/O modules, you can achieve inspection of up to 16 segments of 10GE, or a combination of 1GE, 10GE, and 40GE segments				
Voltage	100-240 VAC				
Current (max. fused power)	12-6 A				
Max power consumption	750W(2559 BTU/hour)				
Power supply	Dual 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 ft.(3,048m)				
Safety	UL 60950-1; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; EN/IEC 60825-1; ROHS Compliance				
EMC	FCC Class A; VCCI Class A; EN 55022 Class A; CISPR 22 Class A; CNS 13438 Class A				

TREND MICRO™

Securing Your Journey to the Cloud