Trend Micro™

TIPPINGPOINT® THREAT PROTECTION SYSTEM PRODUKTFAMILIE

Echtzeiterkennung, Durchsetzung und Problembehebung ohne Kompromisse bei Sicherheit oder Leistung

Unternehmen und Organisationen sind heutzutage permanent mit raffinierten Cyberbedrohungen konfrontiert, die zudem ständig weiterentwickelt werden. In einigen Fällen sind diese Bedrohungen nicht nur komplexer als in der Vergangenheit, sondern werden auch gezielt angewandt und basieren auf neu entdeckten Sicherheitslücken oder Exploits. Es kommt jedoch auch vor, dass Bedrohungen ältere, längst vergessen geglaubte Sicherheitslücken ausnutzen. Um Netzwerkressourcen und Daten vor solchen Bedrohungen schützen zu können, benötigen Unternehmen einen detaillierten Einblick in alle Netzwerkschichten und Ressourcen. Des Weiteren sind umfassende und aktuelle Sicherheitsinformationen sowie ein dynamischer Ansatz erforderlich, der sich durch Automation und Kontextbewusstsein an neue Bedrohungen, neue Schwachstellen und alltägliche Veränderungen im Netzwerk anpassen kann.

Der Umgang mit diesen ganz unterschiedlichen Bedrohungen erfordert einen breit gefächerten Sicherheitsansatz. Unternehmen benötigen umfassende Sicherheitslösungen sowohl innerhalb ihrer Netzwerke als auch an deren Schnittstellen nach außen, um zu verhindern, dass schädliche Angriffe wichtige Ressourcen erreichen. Umfassende Bedrohungsinformationen sind zum Schutz vor bekannten, unbekannten und nicht offengelegten Schwachstellen ebenfalls unabdingbar.

Trend Micro™ TippingPoint® Threat Protection System (TPS) ist eine leistungsfähige Netzwerksicherheitsplattform. Sie bietet einen umfassenden Bedrohungsschutz mit hoher Genauigkeit gegen bekannte und nicht offengelegte Sicherheitslücken. TPS bietet branchenführende Abdeckung über verschiedene Bedrohungsvektoren von komplexen Bedrohungen, Malware und Phishing usw. hinweg, mit maximaler Flexibilität und hoher Leistung. TPS nutzt eine Kombination von Technologien wie Deep Packet Inspection, Bedrohungsreputation, URL-Reputation und modernste Malware-Analysen auf Flow-by-Flow-Basis, um Angriffe auf das Netzwerk zu erkennen und zu verhindern. Die Plattform ermöglicht Unternehmen einen proaktiven Sicherheitsansatz, mit dem ein umfassendes Kontextbewusstsein sowie eine tiefergehende Analyse des Netzwerkverkehrs gewährleistet wird. Dieses komplette Kontextbewusstsein bietet in Verbindung mit den Bedrohungsinformationen von Digital Vaccine® Labs (DVLabs) die nötige Sichtbarkeit und Flexibilität, um mit den heutigen dynamischen, sich entwickelnden Netzwerken in Unternehmen und Rechenzentren Schritt zu halten.

„Die Entscheidung für Deep Discovery war ganz klar. Die Lösung übertraf hinsichtlich der Leistung alle Mitbewerber und wurde auch von Gartner als renommiertes Produkt gewertet. Als TippingPoint dann von Trend Micro akquiriert wurde, wussten wir: Jetzt haben wir das Beste beider Welten.“

Frank Bunton,
Vice President und CISO,
MedImpact

MedImpact

HAUPTFUNKTIONEN

On-Box-SSL-Überprüfung: Ausgefeilte und zielgerichtete Angriffe nutzen in zunehmendem Maße Verschlüsselung, um einer Erkennung zu entgehen. Durch den Einsatz von On-Box-SSL-Überprüfung reduziert TPS die Sicherheits-Blindspots, die durch verschlüsselten Datenverkehr erzeugt werden.

Skalierbarkeit der Leistung: Durch die zunehmende Konsolidierung von Rechenzentren und das starke Wachstum von Cloud-Umgebungen werden skalierbare Sicherheitslösungen benötigt, die an steigende Netzwerkanforderungen angepasst werden können. TPS bietet hervorragende Sicherheit und Leistung für Hochleistungsnetzwerke. Das skalierbare Bereitstellungsmodell von TPS umfasst eine Brancheninnovation – ein NGIPS mit 40 Gbit/s in einem 1U-Formfaktor, das auf insgesamt bis zu 120 Gbit/s in einem 3U-Formfaktor skaliert werden kann.

Flexibles Lizenzierungsmodell: Problemlose Skalierbarkeit von Leistung und Sicherheitsanforderungen mit einem Pay-as-you-grow-Ansatz und flexiblen Lizenzen, die in TPS-Bereitstellungen neu zugewiesen werden können, ohne dass die Netzwerkinfrastruktur verändert werden muss.

Machine Learning in Echtzeit: Viele Sicherheitsbedrohungen sind kurzlebig und werden ständig weiterentwickelt, was manchmal die Effektivität von herkömmlichen, auf Signaturen und Hash-Werten basierenden Erkennungsmechanismen einschränken kann. TPS verwendet statistische Modelle, die mit Machine Learning entwickelt wurden, wodurch Bedrohungen in Echtzeit erkannt und eingedämmt werden können.

Enterprise Vulnerability Remediation (eVR): Durch Integration von Schwachstellenbewertungen von Dritten in die TippingPoint Produktfamilie können Sicherheitslücken schnell geschlossen werden. Kunden können Informationen von verschiedenen Anbietern für Schwachstellenmanagement und Incident Response (Rapid7, Qualys, Tenable) sammeln, den TippingPoint Digital Vaccine®-Filtern die Common Vulnerabilities and Exposures (CVEs) zuordnen und entsprechend geeignete Maßnahmen ergreifen.

Komplexe Bedrohungsanalyse: Erweiterter Schutz vor unbekannten Bedrohungen durch Integration in Deep Discovery™ Analyzer. TPS filtert bekannte Bedrohungen vor, leitet potenzielle Bedrohungen zur automatischen Analyse an eine Sandbox weiter und führt bei Bestätigung des Verdachts auf schädliche Inhalte eine Bedrohungsbeseitigung in Echtzeit durch.

Hohe Verfügbarkeit: TPS verfügt über mehrere fehlertolerante Funktionen, darunter Hot-Swap-fähige Stromversorgungen, Watchdog-Timer zur kontinuierlichen Überwachung von Sicherheits- und Verwaltungs-Engines, integrierte Bypass-Unterstützung und Zero Power High Availability (ZPHA) – ideal für die Inline-Bereitstellung. Zudem kann TPS unter Verwendung von redundanten Links in einem transparenten Hochverfügbarkeitsmodus (Active-Active oder Active-Passive) bereitgestellt werden.

Integrated Advanced Threat Prevention: TPS kann in die fortschrittlichen Bedrohungserkennungslösungen von Trend Micro™ Deep Discovery™ integriert werden, die von NSS Labs als effektivstes Breach Detection System empfohlen werden.

Überprüfung von asymmetrischem Datenverkehr: Asymmetrischer Datenverkehr ist in Unternehmensnetzwerken und Rechenzentren weit verbreitet. Unternehmen müssen die Herausforderungen der Asymmetrie sowohl im Datenfluss als auch im Routing meistern, um ihre Netzwerke vollständig schützen zu können. TPS überprüft standardmäßig alle Arten von Datenverkehr, auch den asymmetrischen, und wendet Sicherheitsrichtlinien für umfassenden Schutz an.

Agilität und Flexibilität: TPS unterstützt den softwaredefinierten Netzwerkschutz durch Bereitstellung von IPS als Service. TPS schützt auch virtualisierte Anwendungen innerhalb einer virtualisierten Infrastruktur (VMware, KVM).

Branchenführende Bedrohungsanalysen: Trend Micro™ TippingPoint® Digital Vaccine® Labs (DVLabs) bietet modernste Bedrohungsanalysen und Sicherheitsfilter, die eine Sicherheitslücke komplett abdecken und vor allen möglichen Angriffsvariationen – nicht nur vor bestimmten Exploits – schützen. Unsere Kunden profitieren jedoch nicht nur von DVLabs, sondern haben auch exklusiven Zugriff auf Schwachstelleninformationen der Zero Day Initiative (ZDI) zum Schutz vor nicht offengelegten Bedrohungen und Zero-Day-Bedrohungen. ZDI ist das größte herstellerunabhängige Bug-Bounty-Programm und veröffentlichte im Jahr 2016 700 Schwachstellen. Trend Micro TippingPoint Kunden waren im selben Jahr durchschnittlich 57 Tage lang geschützt, bevor die Schwachstellen von den jeweiligen Herstellern behoben wurden.

Virtuelles Patching: Virtuelles Patching liefert einen leistungsfähigen und skalierbaren Abwehrmechanismus, der Netzwerke vor bekannten Bedrohungen schützt. Dabei werden auf Schwachstellen basierende Filter verwendet, um alle Versuche, eine bestimmte Sicherheitslücke auf der Netzwerkebene (im Gegensatz zur Endbenutzerebene) auszunutzen, effektiv zu blockieren. Dies hilft Unternehmen, die Kontrolle über ihre Patch-Management-Strategie zu übernehmen. Dazu wird der Zeitraum zwischen der Entdeckung einer Sicherheitslücke und der Verfügbarkeit eines Patchs vorbeugend abgedeckt. Außerdem bietet das System zusätzlichen Schutz für ältere Out-of-Support-Software.

Support für verschiedenste Arten von Datenverkehr: Die TPS-Plattform unterstützt viele verschiedene Arten von Datenverkehr und zahlreiche Protokolle. Sie bietet simultane Payload-Prüfungen für IPv6/v4 ohne Kompromisse und unterstützt verwandte Tunneling-Varianten (4in6, 6in4 und 6in6). Außerdem unterstützt das System die Überprüfung von IPv6/v4-Datenverkehr mit VLAN- und MPLS-Tags sowie von mobilem IPv4-Datenverkehr, GRE und GTP (GPRS-Tunneling) und Jumbo-Frames. Diese umfangreiche Abdeckung gibt IT- und Sicherheitsadministratoren die Flexibilität, Schutz immer dort bereitzustellen, wo er benötigt wird.

Zentrale Verwaltung: Das TippingPoint Security Management System (SMS) bietet eine grafische Anwenderoberfläche für einheitliche Richtlinien- und Elementverwaltung. Diese Oberfläche stellt einen einzigen Mechanismus zur Überwachung von operativen Informationen, zur Bearbeitung von Netzwerksicherheitsrichtlinien, zur Konfiguration von Elementen und zur Bereitstellung von Netzwerksicherheitsrichtlinien in der gesamten Infrastruktur zur Verfügung, unabhängig davon, ob diese physisch oder virtuell ist.

Entscheidende Vorteile

Präventive Gefahrenabwehr

Beim Inline-Einsatz von TPS kann das System Datenverkehr in allen Richtungen (eingehend, ausgehend und lateral) in Echtzeit überprüfen und blockieren und das Netzwerk so vor bekannten, unbekannten und nicht offengelegten Sicherheitslücken schützen.

Informationen über und Priorisierung von Bedrohungen

Einblick und Transparenz sind für die Gestaltung von optimalen Sicherheitsrichtlinien von grundlegender Bedeutung. TPS bietet vollständige Transparenz für das gesamte Netzwerk und liefert die erforderlichen Informationen und den Kontext, um die Priorisierung von Bedrohungen zu messen und voranzutreiben.

Durchsetzung und Problembehebung in Echtzeit

Verteidigen Sie das Netzwerk vom Rand bis hin zum Rechenzentrum und zur Cloud mit Inline-Durchsetzung in Echtzeit und automatisierter Behebung anfälliger Systeme. TPS erreicht Inline-Echtzeitschutz auf einer neuen Ebene. Das System bietet proaktive Netzwerksicherheit für den realen Netzwerkverkehr und die Rechenzentren von heute und morgen. Die Threat Suppression Engine (TSE)-Architektur bietet eine äußerst schnelle Inline-Überprüfung von Datenpaketen (Deep Packet Inspection), und das modulare Design der speziell zu diesem Zweck entwickelten Appliance ermöglicht die Konvergenz mit zusätzlichen Sicherheitsdiensten.

Einfache Verwaltung

Durch flexible Bereitstellungsoptionen, die über eine zentrale Verwaltungsoberfläche einfach eingerichtet und verwaltet werden können, bietet TPS sofortigen und andauernden Bedrohungsschutz mit vorinstallierten empfohlenen Einstellungen.

TPS – TECHNISCHE DATEN

Funktionen	440T (TPNN0291)	2200T (TPNN0292)	8200TX (TPNN0090)	8400TX (TPNN0091)
Unterstützter IPS-Überprüfungsdurchsatz	250 Mbit/s/ 500 Mbit/s/1 Gbit/s	1 Gbit/s/2 Gbit/s	3/5/10/15/20/30/40 Gbit/s	3/5/10/15/20/30/40 Gbit/s
SSL-Überprüfung	Nicht verfügbar	500 Mbit/s	2 Gbit/s (2K-Schlüssel SHA-256)	2 Gbit/s (2K-Schlüssel SHA-256)
Latenz	< 100 Mikrosekunden	< 100 Mikrosekunden	< 40 Mikrosekunden	< 40 Mikrosekunden
Sicherheitskontexte	750.000	2.500.000	10.000.000	10.000.000
Gleichzeitige Sitzungen	1.000.000	10.000.000	120.000.000	120.000.000
Neue Verbindungen pro Sekunde	70.000	115.000	650.000	650.000
Formfaktor	1U	2U	1U	2U
Gewicht	6,93 kg (15,28 Pfund)	11,91 kg (26,26 Pfund)	14,5 kg (max. einschließlich IOMs) 13,2 kg (mit leeren IOMs)	22,7 kg (max. einschließlich IOMs) 18,8 kg (mit leeren IOMs)
Abmessungen (B x T x H)	16,78 Zoll (B) x 17,3 Zoll (T) x 1,72 Zoll (H) 42,62 cm x 45,00 cm x 4,40 cm	16,77 Zoll (B) x 18,70 Zoll (T) x 3,46 Zoll (H) 42,60 cm x 47,50 cm x 8,80 cm	16,78 Zoll (B) x 17,3 Zoll (T) x 1,72 Zoll (H) 42,62 cm x 45,00 cm x 4,40 cm	16,77 Zoll (B) x 18,70 Zoll (T) x 3,46 Zoll (H) 42,60 cm x 47,50 cm x 8,80 cm
Verwaltungsports	1 Out-of-Band-RJ-45 (10/100/1000), 1 RJ-45 seriell, verwaltbar			
Verwaltungsoberfläche	Security Management System (SMS), lokale Webkonsole, Befehlszeile, SNMPv2c, SNMPv3 (TippingPoint MIB verfügbar)			
Netzwerkkonnektivität	8 RJ-45-Anschlüsse (10/100/1000) mit integrierter Bypass-Unterstützung 1 RJ-45-Hochverfügbarkeitsanschluss (10/100/1000)	8 RJ-45-Anschlüsse (10/100/1000) mit integrierter Bypass-Unterstützung, 8 x 1G SFP 4 x 10G SFP+ 1 RJ-45-Hochverfügbarkeitsanschluss (10/100/1000), Unterstützung für externe ZPHA für SFP/SFP+	2x IOM-Steckplätze, Mix/Match: 6-Segment 1GE Kupfer 6-Segment 1GE SFP 4-Segment 10GE SFP+ 1-Segment 40GE QSFP+ 4-Segment 1GE Kupfer-Bypass 2-Segment 1GE SR/LR Glasfaser-Bypass 2-Segment 10GE SR/LR Glasfaser-Bypass	4x IOM-Steckplätze, Mix/Match: 6-Segment 1GE Kupfer 6-Segment 1GE SFP 4-Segment 10GE SFP+ 1-Segment 40GE QSFP+ 4-Segment 1GE Kupfer-Bypass 2-Segment 1GE SR/LR Glasfaser-Bypass 2-Segment 10GE SR/LR Glasfaser-Bypass
On-Box-Speicher	8-GB-CFast-Laufwerk (Hot-Swap-fähig)		32-GB-1,8-Zoll-SSD-Modul (Hot-Swap-fähig)	
Spannung	100 bis 240 VAC, 50 bis 60 Hz		100 bis 240 VAC / -40 bis -60 VDC	
Strom (max. abgesichert)	4-2 A	12-6 A	12/6 Ampere AC, 24/16 Ampere DC	
Max. Leistungsaufnahme	250 W (853 BTU/Stunde)	493 W (1682 BTU/Stunde)	750 W (2557 BTU/Stunde)	
Stromversorgung	Einzeln, fest	Dual/redundant, Hot-Swap-fähig	Dual/redundant, Hot-Swap-fähig	
Betriebstemperatur	0 °C bis 40 °C (32 °F bis 104 °F)			
Relative Luftfeuchtigkeit bei Betrieb	5 % bis 95 % nicht kondensierend			
Betriebsfremd/ Lagertemperatur	-20 °C bis 70 °C			
Betriebsfremd/Lagerung relative Feuchtigkeit	5 % bis 95 % nicht kondensierend			
Höhenlage	Bis zu 3.048 m			
Sicherheit	UL 60950-1, IEC 60950-1, EN 60950-1, CSA 22.2 60950-1, ROHS-Konformität			
EMC	Klasse A, FCC, VCCI, KC, EN55022, CISPR 22, EN55024 CISPR 24, EN61000-3-2, EN61000-3-3, CE-Kennzeichnung			

vTPS – TECHNISCHE DATEN

Funktionen	vTPS Standard	
Unterstützter IPS-Überprüfungsdurchsatz	250 Mbit/s/500 Mbit/s/ 1 Gbit/s	250 Mbit/s/500 Mbit/s/ 1 Gbit/s
SSL-Überprüfung	–	Ja
Anzahl der logischen Kerne	2 oder 3	4
Arbeitsspeicher	8 GB	16 GB
Festplattenspeicher	16 GB	16 GB
IPS – gleichzeitige Verbindungen	1.000.000	
Neue Verbindungen pro Sekunde	Bis zu 120 K VMware, bis zu 60 K KVM	
Unterstützung für virtuelle Plattformen	VMWare ESXi 5.5, 6.0,6.5 (NSX ist für transparente Überprüfung und Durchsetzung nicht erforderlich) und KVM – Redhat Enterprise Linux 6, 7	
Netzwerktreiber	VMWare – VMNet3; KVM – virtIO	
Anzahl der Netzwerksegmente	1	
Anzahl der virtuellen Segmente	Keine Obergrenze	
Dediziertes Verwaltungs-vNIC	Ja	

TIPPINGPOINT E/A-MODULE

TippingPoint-E/A-Module – Beschreibung	Produkt-SKU
TippingPoint-E/A-Modul: 6-Segment Gig-T	TPNN0059
TippingPoint-E/A-Modul: 6-Segment GbE SFP	TPNN0068
TippingPoint-E/A-Modul: 4-Segment 10GbE SFP+	TPNN0060
TippingPoint-E/A-Modul: 1-Segment 40GbE QSFP+	TPNN0069
TippingPoint-E/A-Modul: 4-Segment Gig-T Bypass	TPNN0070
TippingPoint-E/A-Modul: 2-Segment 1G Glasfaser SR Bypass	TPNN0071
TippingPoint-E/A-Modul: 2-Segment 1G Glasfaser LR Bypass	TPNN0072
TippingPoint-E/A-Modul: 2-Segment 10G Glasfaser SR Bypass	TPNN0073
TippingPoint-E/A-Modul: 2-Segment 10G Glasfaser LR Bypass	TPNN0074

TREND MICRO™

Securing Your Connected World