Trend Micro™

SOLUTIONS TIPPINGPOINT THREAT PROTECTION SYSTEM (TPS)

Détection en temps réel des menaces et remédiation, sans peser sur la sécurité, ni les performances

Les entreprises actuelles sont sous la menace permanente de cybermenaces sophistiquées et en évolution. Nombre de ces menaces ont gagné en complexité et tirent parti de vulnérabilités et exploits nouvellement identifiés. Dans d'autres cas, les menaces exploitent d'anciennes vulnérabilités parfois oubliées. Protéger vos ressources réseau et vos données contre de telles menaces exige une visibilité précise au cœur de vos couches et ressources réseau. Il devient nécessaire d'opter pour une veille riche et actualisée contre les menaces, ainsi que des fonctions d'automatisation pour lutter contre les nouvelles menaces et vulnérabilités, mais aussi s'adapter aux évolutions quotidiennes du réseau.

Ces menaces très différentes impliquent d'aborder la sécurité selon différents angles. Les entreprises ont besoin de solutions de sécurité robustes au cœur et en périphérie de leurs réseaux pour empêcher les attaques de se propager jusqu'aux ressources critiques. D'autre part, une veille efficace sur les menaces s'impose pour se protéger des menaces connues, inconnues et non-divulguées.

Trend Micro™ TippingPoint™ Threat Protection System (TPS) est une plateforme de sécurité réseau qui déploie une protection intégrale et précise contre les vulnérabilités. TPS sécurise ainsi différents vecteurs d'attaque contre les menaces avancées, les malware et le phishing, de manière flexible et performante. TPS associe différentes technologies pour détecter et prévenir les attaques sur le réseau : deep packet inspection, réputation des menaces, réputation d'URL et analyse antimalware. La solution incite à une approche proactive à la sécurité qui favorise une prise en compte du contexte et une analyse plus poussée du trafic réseau. Cette approche contextuelle, associée aux services de Trend Micro™ TippingPoint™ Digital Vaccine® Labs (DVLabs), offre la visibilité et l'agilité nécessaires pour protéger les réseaux d'entreprise et les data centers dynamiques actuels.

> “Trend Micro™ Deep Discovery™ se veut particulièrement simple. La solution surperforme ses concurrents et est reconnue par Gartner. Lorsque Trend Micro a racheté TippingPoint, nous savions que nous aurions accès au meilleur de deux mondes.”
>
> Frank Bunton,
> Vice President and CISO,
> MedImpact

MedImpact

FONCTIONNALITÉS CLÉS

La protection de TippingPoint étendue au Cloud : Trend Micro™ Cloud Network Protection, optimisé par Trend Micro™ TippingPoint™ est une solution de sécurité robuste qui permet aux entreprises d'apporter la protection réseau existante de TippingPoint aux environnements Cloud hybrides. Avec une protection totale contre les menaces (Virtual Patching, protection contre les vulnérabilités, neutralisation des exploits et défense contre les attaques connues et Zero-Day), la solution sécurise de multiples vecteurs d'attaque de manière optimale. Les fonctions et règles de sécurité de TippingPoint s'appliquent à vos environnements Cloud via votre système actuel de gestion de la sécurité.

Inspection SSL intégrée : les attaques sophistiquées et ciblées exploitent de plus en plus le chiffrement pour se rendre furtives. Les solutions TippingPoint réduisent les zones d'ombre créées par le trafic chiffré grâce à une inspection du trafic SSL.

Évolutivité des performances : la consolidation des data centers et le développement des environnements Cloud nécessitent des solutions de sécurité évolutives, adaptées aux exigences croissantes des réseaux. Avec un niveau de sécurité et des performances optimales pour les réseaux de grande envergure, les solutions TippingPoint proposent un modèle de déploiement évolutif avec le premier système nouvelle-génération de prévention des intrusions (NGIPS) au format 1U et doté de performances de 40 Gbps (évolutives jusqu'à 120 Gbps au format 3U).

Flexibilité du modèle de licence : faites évoluer vos niveaux de performances et de sécurité avec un modèle de tarification à l'utilisation et des licences flexibles qui peuvent être appliquées aux solutions TippingPoint sans modifier l'infrastructure réseau.

Machine Learning en temps réel : de nombreuses cyber-menaces ont une durée de vie limitée et évoluent constamment, limitant ainsi l'efficacité des solutions de détection traditionnelles basées sur des signatures et hash. TPS utilise des modèles statistiques basés sur le Machine Learning pour détecter et neutraliser les menaces en temps réel.

EVR (Enterprise Vulnerability Remediation) : restaurez rapidement les vulnérabilités en intégrant les évaluations de vulnérabilités réalisées par des tiers à vos produits TippingPoint. Obtenez des informations auprès de différents fournisseurs proposant des solutions de gestion des vulnérabilités et de prise en charge d'incidents (Rapid7, Qualys, Tenable), mappez les vulnérabilités de la base CVE avec les filtres TippingPoint Digital Vaccine® et décidez de manière éclairée.

Analyse avancée des menaces : renforcez la protection contre les menaces inconnues grâce à une intégration avec Deep Discovery™ Analyzer. Les solutions TippingPoint pré-filtrent les menaces connues, soumettent les menaces potentielles à une analyse automatisée en sandbox et restaurent les contenus malveillants le cas échéant.

Haute disponibilité : TippingPoint dispose de plusieurs fonctionnalités avec tolérance aux pannes (blocs d'alimentation remplaçables à chaud, surveillance constante des moteurs de gestion et de sécurité, bypass d'inspection et fonction ZPHA - Zero Power High Availability). De plus, la solution peut bénéficier de liens redondants dans un mode haute disponibilité (HA) actif-actif ou actif-passif transparent.

Prévention intégrée contre les menaces : les produits TippingPoint s'interfacent avec Trend Micro™ Deep Discovery™, reconnu par le NSS Labs comme le système de détection des intrusions le plus performant du marché.

Inspection asymétrique du trafic : les enjeux d'asymétrie du trafic sont courants au sein des réseaux d'entreprise et de data center. TippingPoint inspecte tous les types de trafic par défaut, y compris le trafic asymétrique, et applique des politiques de sécurité adéquates pour une protection complète. Les entreprises doivent relever les défis liés au trafic et au routage asymétrique afin de protéger leurs réseaux. Par défaut, TPS inspecte tous les types de trafic, y compris le trafic asymétrique, et applique les règles de sécurité pour garantir une protection intégrale.

Agilité et flexibilité : TPS déploie le système IPS en tant que service, proposant ainsi une protection réseau de type "Software Defined". TPS protège également les applications virtualisées depuis votre infrastructure (VMware® et KVM).

Veille optimale sur les menaces : pour protéger efficacement les entreprises contre tous les profils attaque, et pas seulement des exploits spécifiques, les Digital Vaccine® Labs proposent des analyses des menaces et des filtres de sécurité. D'autre part, les clients accèdent en exclusivité aux informations sur les vulnérabilités de Zero Day Initiative (ZDI) et se protègent ainsi contre les menaces Zero-Day non divulguées. ZDI est le premier programme indépendant de récompense à la recherche de vulnérabilités, avec 700 vulnérabilités divulguées en 2016. En 2016, les clients de Trend Micro TippingPoint ont été protégés en moyenne 57 jours avant qu'une vulnérabilité ne soit patchée par son éditeur.

Virtual Patching : le Virtual Patching est un mécanisme de défense de premier niveau, puissant et évolutif qui protège les réseaux contre les menaces connues. Il tire parti de filtres pour contrer l'exploitation d'une vulnérabilité spécifique. Les entreprises gèrent ainsi leur stratégie de patchs de manière pertinente et se protègent entre le moment où une vulnérabilité est identifiée et la date de disponibilité d'un patch. La protection des logiciels obsolètes, en fin de support est également assurée.

Prise en charge d'un large éventail de types de trafic : la plateforme TPS prend en charge de multiples profils de trafic et de protocoles réseau. Les solutions inspectent simultanément les charges IPv6/v4, ainsi que les variantes de tunnel (4in6, 6in4 et 6in6). Elle assure également l'inspection du trafic IPv6/v4 encapsulé au travers de VLAN et de MPLS, le trafic IPv4 mobile, GRE et GTP (tunneling GPRS), ainsi que les Jumbo frames. Ce vaste périmètre fonctionnel offre aux administrateurs IT et de sécurité la flexibilité nécessaire pour déployer la protection partout où elle est nécessaire.

Gestion centralisée : le système de gestion de la sécurité (SMS) de TippingPoint offre une interface utilisateur unifiée pour gérer les règles et les éléments. Cette interface permet de surveiller les informations opérationnelles, de modifier les règles de sécurité réseau, de configurer les éléments et de déployer des règles de sécurité réseau sur l'ensemble de l'infrastructure physique ou virtualisée.

Avantages clés

Prévention proactive des menaces

Déployé de manière transparente (mode inline), TippingPoint inspecte en temps réel et bloque, si nécessaire, le trafic réseau entrant, sortant et interne pour protéger les entreprises contre les vulnérabilités connues, inconnues et non divulguées.

Visibilité et hiérarchisation des menaces

La visibilité est essentielle à la prise de décision en matière de sécurité. TippingPoint offre une visibilité complète de votre réseau et fournit les informations contextuelles nécessaires pour hiérarchiser les menaces..

Application de la sécurité en temps réel et remédiation

Protégez votre réseau, de sa périphérie au data center et jusqu'au Cloud, via une application transparente et temps-réel de la sécurité et une remédiation automatisée des systèmes vulnérables. TippingPoint offre un niveau de protection optimal, avec une sécurité proactive pour le trafic réseau et les data centers actuels et futurs. L'architecture du moteur TSE (Threat Suppression Engine) assure une inspection performante et en profondeur des flux de paquets. Sa conception modulaire permet la convergence de services de sécurité additionnels.

Simplicité opérationnelle

Avec des options de déploiement flexibles, faciles à configurer et à gérer via une interface centralisée, TippingPoint fournit une protection immédiate et continue contre les menaces à l'aide de paramètres recommandés prêts à l'emploi.

SPÉCIFICATIONS TECHNIQUES DE TPS

Fonctionnalités	440T (TPNN0291)	2200T (TPNN0292)	8200TX (TPNN0090)	8400TX (TPNN0091)
Débit d'inspection du système IPS	250 Mbps/500 Mbps/ 1 Gbps	1 Gbps/2 Gbps	3/5/10/15/20/30/40 Gbps	3/5/10/15/20/30/40 Gbps
Inspection SSL	Non disponible	500 Mbps	2 Gbps (clés 2K SHA 256)	2 Gbps (clés 2K SHA 256)
Latence	< 100 microsecondes	< 100 microsecondes	< 40 microsecondes	< 40 microsecondes
Sessions simultanées	1 000 000	10 000 000	120 000 000	120 000 000
Nouvelles connexions par seconde	70 000	115 000	650 000	650 000
MTBF (Mean Time Between Failures)	39 694 heures @ 25°C ambiant	34 837 heures @ 25°C ambiant	88 706 heures @ 25°C ambiant	88 706 heures @ 25°C ambiant
Format	1U	2U	1U	2U
Poids	6,93 Kg	11,91 Kg	14,51 Kg (max. avec modules E/S), 13.15 Kg (avec modules E/S vides)	22,67 Kg (max. avec modules E/S), 18,82 Kg (avec modules E/S vides)
Dimensions (L x P x H)	42,62 cm x 45,00 cm x 4,40cm	42,60 cm x 47,50 cm x 8,80 cm	42,62 cm x 45,00 cm x 4,40 cm	42,60 cm x 47,50 cm x 8,80 cm
Ports de gestion	Port de gestion « out of band » RJ45 10/100/1000			
Gestion des interfaces	SMS (système de gestion de la sécurité), Console Web locale, CLI (interface de ligne de commande) SNMPv2c, SNMPv3 (disponibilité TippingPoint MIB)			
Connectivité réseau	8 ports RJ-45 10/100/1000 avec bypass Un port haute-disponibilité RJ-45 10/100/1000	8 ports RJ-45 10/100/1000 avec bypass 8 ports SFP 1G 4 ports SFP+ 10G Un port haute-disponibilité RJ-45 10/100/1000 avec ZPHA externe pour SFP/SFP+	2 slots pour module E/S, avec possibilité d'associer 6-segment 1 GE cuivre 6-segment 1 GE SFP 4-segment 10 GE SFP+ 1-segment 40 GE SFP+ 2-segment 1 GE cuivre bypass 2-segment 1 GE fibre SR/LR bypass 2-segment 10 GE fibre SR/LR bypass	4 slots pour module E/S. Associations possibles : 6-segment 1 GE cuivre IOM 6-segment 1 GE SFP bypass 4-segment 10 GE SFP+ 1-segment 40 GE QSFP+ 4-segment 1 GE cuivre bypass 2-segment 1 GE fibre SR/LR bypass 2-segment 10 GE fibre SR/LR bypass
Stockage embarqué	DD CFast 8 Go remplaçable à chaud		Module SSD 32Go 1,8" remplaçable à chaud	
Tension	100-240 VAC 50/-60 Hz		100 à 240 VAC/-40 à -60 VDC	
Courant (max. et protégé par fusible)	4-2 A	12-6 A	12/6 Amps AC, 24/16 Amps DC	
Consommation max. en puissance	250 W (853 BTU/heure)	493 W (1 682 BTU/heure)	750 W (2 557 BTU/heure)	
Alimentation électrique	Simple	Double/redondant remplaçable à chaud	Double/redondant remplaçable à chaud	
Température de fonctionnement	0°C à 40°C			
Humidité relative de fonctionnement	5% à 95% sans condensation			
Température de stockage hors service	-20°C à 70°C			
Humidité relative hors service de stockage	5% à 95% sans condensation			
Altitude	Jusqu'à 3 048 m			
Sécurité	Compliance UL 60950-1, IEC 60950-1EN 60950-1,CSA 22.2 60950-1RoHS			
EMC	Class A, FCC, VCCI, KC EN55022, CISPR 22, EN55024 CISPR 24, EN61000-3-2 EN61000-3-3, marquage CE			

SPÉCIFICATIONS TECHNIQUES CLOUD NETWORK IPS

Fonctionnalités	Cloud Network Protection
Type d'instance AWS	C5.2xlarge
Performances de l'IPS	Jusqu'à 3,5 Gbps
Latence	<100 microsecondes
Sessions simultanées	7,5 M
Nouvelles connexions par seconde	75 000

* Test de performance, les valeurs réelles peuvent varier.

Spécifications techniques vTPS

Fonctionnalités	vTPS Standard	
Débit d'inspection de l'IPS	250 Mbps/500 Mbps/ 1 Gbps/2 Gbps	250 Mbps/500 Mbps/ 1 Gbps/2 Gbps
Inspection SSL	Non disponible	Oui
Nombre de cœurs logiques	2 ou 3	4
Mémoire	8 Go	16 Go
Espace disque dur :	16 Go	16 Go
Sessions simultanées IPS	1 000 000	
Nouvelles connexions par seconde	Jusqu'à 120 K pour VMware Jusqu'à 60 K pour KVM	
Compatibilité plateforme virtuelle	VMWare ESXi 5.5, 6.0,6.5 (NSX non requis pour l'inspection et l'application transparentes) & KVM – Redhat Enterprise Linux® 6, 7	
Pilote réseau	VMWare- VMNet3; KVM- virtIO	
Nombre de segments réseau	1	
Nombre de segments virtuels	Pas de limite	
Gestion dédiée vNIC	Oui	

MODULES E/S TIPPINGPOINT

Description du module E/S TippingPoint	Référence produit
Module E/S TippingPoint 6-segment Gig-T	TPNN0059
Module E/S TippingPoint 6-segment GbE SFP	TPNN0068
Module E/S TippingPoint 4-segment 10GbE SFP+	TPNN0060
Module E/S TippingPoint 1-segment 10GbE SFP+	TPNN0069
Module E/S TippingPoint 4-segment Gig-T Bypass	TPNN0070
Module E/S TippingPoint 2-segment 1G Fiber SR Bypass	TPNN0071
Module E/S TippingPoint 2-segment 1G Fiber SR Bypass	TPNN0072
Module E/S TippingPoint 2-segment 10G Fiber SR Bypass	TPNN0073
Module E/S TippingPoint 2-segment 10G Fiber LR Bypass	TPNN0074

TREND MICRO™

Securing Your Connected World

Pour toute information sur les données personnelles que nous recueillons et les raisons de ce recueil, merci de consulter notre charte de confidentialité sur : https://www.trendmicro.com/privacy