データシート

Trend Micro

TippingPoint™ Threat Protection System Family

セキュリティやパフォーマンスを損なわずに、リアルタイムに検出、適用、保護

今日の組織は、進化する巧妙なサイバー脅威の危険に常にさらされています。このような脅威の中には、過去の脅威よりも複雑さを増しただけでなく、新たに見つかる脆弱性やエクスプロイトを標的にしたり、利用したりするものがあります。忘れ去られたと思われていた、かなり昔の脆弱性を利用する脅威もあります。このような脅威からネットワークに繋がる資産とデータを守るには、ネットワークレイヤとリソース全体に対する詳細な可視化が必要です。それには、包括的で最新のセキュリティインテリジェンスと、新たな脅威や新たな脆弱性、日々のネットワーク変更に合わせて認識し、自動化する動的アプローチが求められます。

このような多種多様な脅威に対応するには、多方面からのセキュリティアプローチが必要です。組織は、不正な攻撃が重要なリソースに到達するのを防ぐため、ネットワークの境界や内部に配置する、強固なセキュリティソリューションを求めています。また、既知、未知、未公開の脆弱性を防御する包括的な脅威インテリジェンスも求めています。

TippingPoint Threat Protection System (TPS) は、既知および未公開の脆弱性に対して精度の高い包括的な脅威対策を提供する、強力なネットワークセキュリティプラットフォームです。TPSは、不正プログラムやフィッシングなど、多岐にわたる経路から侵入する高度な脅威に、きわめて高度な柔軟性と優れたパフォーマンスで対処する業界をリードする製品です。TPSは、ディープパケットインスペクション、脅威レピュテーション、URLレピュテーション、高度な不正プログラム解析などの技術をフローごとに組み合わせて、ネットワーク上の攻撃を検出し、ブロックします。
TPSにより、企業はセキュリティに対するプロアクティブなアプローチを取れるようになり、ネットワークトラフィックに関する総合的なコンテキスト認識とより深い分析が可能になります。この総合的なコンテキスト認識は、Trend Micro Researchの脅威インテリジェンス (Trend Micro™ TippingPoint™ Digital Vaccine™) との組み合わせにより、今日の絶えず変化し進化する企業ネットワークやデータセンターネットワークに遅れを取らないようにするために不可欠な可視性と俊敏性をもたらします。

NetSec OPEN Certified

優れたパフォーマンスと、100%のセキュリティ機能の有効性の高さにより、NetSecOpenの認定を取得

OMDIA

Brought to you by Informa Tech

2007年以降、脆弱性に関するグローバルな調査と発見のリーダー

主な機能

オンボックスSSLインスペクション: 暗号化を使用して検出を回避する、巧妙な標的型攻撃が増えています。TPSは、オンボックスSSLインスペクションにより、暗号化されたトラフィックによるセキュリティの見落としを削減します。

パフォーマンスの拡張性: データセンター統合の拡大とクラウド環境の急増による、ネットワークに対するニーズの増加に対応できるセキュリティソリューションが求められています。TPSは、大容量ネットワーク向けの卓越したセキュリティとパフォーマンスを、拡張性の高い導入モデルを利用して提供します。TXシリーズでは、 1Uフォームファクタ40Gbpsの検査スループットを実現し、台数をスタックすることにより合計120Gbpsまで拡張可能となります。

柔軟なライセンスモデル: 従量料金制の柔軟なライセンスにより、 ネットワークインフラストラクチャを変更することなくTPSの導入環境全体で再割り当てが可能になり、パフォーマンスとセキュリティの要件を容易に拡張できます。

リアルタイムの機械学習: セキュリティ脅威の多くは、短い時間で絶えず進化しており、従来のシグネチャベースやハッシュベースの検出メカニズムでは、効果が限定される場合があります。TPSは、機械学習技術により開発された統計モデルを活用し、リアルタイムで脅威を検出し、軽減する能力を提供します。

脆弱性リスクの回避 (eVR): サードパーティの脆弱性診断とTippingPoint製品ポートフォリオを統合し、 脆弱性を迅速に保護します。お客さまは、脆弱性管理やインシデント対応のさまざまなベンダ (Rapid7、 Qualys®、Tenable) が提供する情報を取り込み、CVE (Common Vulnerabilities and Exposures) をTippingPoint Digital Vaccineフィルタにマッピングして、適切な対策を取ることができます。

高度な脅威分析: Deep Discovery Analyzerとの連携により、未知の脅威から幅広く保護します。TPSは既知の脅威を事前にフィルタリングし、潜在的な脅威を自動でサンドボックス分析の対象として転送します。また、不正なコンテンツを確認すると、リアルタイムで遮断します。

高可用性: TPSはインライン型の配置に適しており、ホットスワップ対応の電力ユニット、セキュリティエンジンと管理エンジンを絶えず監視するウォッチドッグタイマ、組み込みの検査バイパス、Zero Power High Availability (ZPHA) など、複数のフォールトトレランス機能を備えています。さらに、アクティブ-アクティブまたはアクティブ-パッシブの透過的な高可用性 (HA) モードで冗長リンクを使用して、TPSを配置することができます。

高度な脅威予防対策と連携: TPSは高度な脅威検知ソリューションである、 Deep Discoveryと連携します。

非対称トラフィック検査: トラフィックの非対称性は、企業ネットワークやデータセンターネットワーク全体に拡がっています。企業は、フローおよびルーティング両方の非対称性による課題を克服し、ネットワーク全体を完全に保護する必要があります。TPSは、非対称トラフィックを含む、すべての種類のトラフィックを検査するよう初期設定されており、セキュリティポリシーを適用して包括的に保護します。

迅速な展開と柔軟性: TPSはIPSをサービスとして配置することで、 ソフトウェア定義型のネットワーク保護を提供します。 またTPSはお客様の仮想インフラ(VMWare、 KVM)から仮想化されたアプリケーションを保護することも可能です。

クラス最高の脅威インテリジェンス: Trend Micro Researchによる最先端の脅威分析とセキュリティフィルタの提供を通じて、すべての脆弱性に対応し、特定のエクスプロイトだけでなく、すべての潜在的な攻撃の組み合わせから保護します。Trend Micro Researchに加えて、Zero Day Initiative (ZDI)から提供される脆弱性情報への専用アクセスにより、 ゼロデイ脅威からお客さまを保護します。 ZDIは、ベンダに依存しない最大のバグ発見報酬プログラムであり、 2021年には1,604件以上の脆弱性を公開。 TPSのお客さまは、 影響を受けたベンダの脆弱性のパッチの提供に対して、 平均で102日先行して保護を受けることができています。

仮想パッチ: 強力で拡張性の高い最先端の防御メカニズムを提供して既知の脅威からネットワークを保護します。また、脆弱性ベースのフィルタを活用して、特定の脆弱性を悪用しようとするすべての試みをエンドユーザレベルではなくネットワークレベルで効果的にブロックします。これにより、脆弱性の発見とパッチ入手の差を先取りして埋めるとともに、古いサポート対象外のソフトウェアも防御することで、 企業のパッチ管理戦略を強化できます。

幅広いタイプのトラフィックへのサポート: TPSプラットフォームは、幅広いタイプのトラフィックとプロトコルをサポートします。徹底したIPv6/v4同時ペイロード検査を実施し、関連するトンネリング型 (4in6、 6in4、6in6) をサポートします。VLANタグおよびMPLSタグ付きのIPv6/v4トラフィック、モバイルIPv4トラフィック、GREおよびGTP (GPRSトンネリング)、ジャンボフレームの検査もサポートします。このような幅広い対応により、IT管理者やセキュリティ管理者は、必要な場所に柔軟に保護を導入できます。

集中管理: TippingPoint Security Management System (SMS) は、ポリシーと要素を管理する統合されたグラフィカルユーザインターフェースを提供します。また、運用の監視、ネットワーク情報の監視、 ネットワークセキュリティポリシーの編集、要素の設定、およびネットワークセキュリティポリシーの導入を行います。物理か仮想かを問わず、インフラストラクチャ全体に単一のメカニズムをもたらします。

主な利点

予防的な脅威対策

インラインに配置されるTPSは、すべての方向のトラフィック (インバウンド、アウトバウンド、水平方向) をリアルタイムで検査およびブロックし、既知、未知、未公開の脆弱性を保護します。

脅威の見極めと優先度付け

脅威を可視化し見極めることは、最適なセキュリティポリシーの決定に重要です。TPSは、ネットワーク全体を可視化し、脅威の優先順位を計算して設定するのに必要なインサイト(見極め)とコンテキストを提供します。

リアルタイムの適用と修復

ネットワークからデータセンターおよび組織のネットワークの境界線、 クラウドに至るまで、インラインでのリアルタイムの適用と自動修復によって脆弱なシステムを保護します。TPSは、新しいレベルのリアルタイムのインライン保護を実現し、現在および将来にわたり、実際のネットワークトラフィックとデータセンターにプロアクティブなネットワークセキュリティを提供します。Threat Suppression Engine (TSE) のアーキテクチャにより、インラインの高速ディープパケットインスペクションが実行され、専用アプライアンスのモジュール設計により、追加セキュリティサービスの集約も可能になります。

運用の簡素化

TPSは、一元化された管理インタフェースで設定と管理が容易にできる柔軟な導入オプションを備えており、すぐに使用可能な推奨設定により、迅速かつ継続的に脅威対策を実現します。

Threat Protection System TXシリーズの技術仕様 *1

	1100TX (TPNN0321)	5500TX (TPNN0322)	8200TX (TPNN0090)	8400TX (TPNN0091)
インスペクションスループット *2	250 / 500 Mbps / 1 Gbps	1 / 2 / 3 / 5 Gbps	3 / 5 / 10 / 15 / 20 / 30 / 40 Gbps	
同時接続セッション数	15,000,000	30,000,000	120,000,000	
1秒当たりの新規接続数	100,000	400,000	650,000	
SSLインスペクション (2K keys、ECDHE-RSA-AES256-GCM- SHA384)	提供なし	最大3.5 Gbps (インスペクションスループットにより制限)	最大8 Gbps (インスペクションスループットにより制限)	
1秒当たりの新規SSL接続数	提供なし	3,500	7,000	
SSL同時接続セッション数	提供なし	80,000	100,000	
レイテンシ	100マイクロ秒未満	60マイクロ秒未満	40マイクロ秒未満	
MTBF(室温25℃における平均故障間隔)	93,177時間	75,660時間	88,706時間	
フォームファクタ	19インチ1U			19インチ2U
重量	6.58Kg	7.94Kg	14.53Kg	22.70Kg
外形寸法 (W x D x H)	47.09 cm (W) x 45.47 cm (D) x 4.40 cm (H)		42.62 cm (W) x 45.00 cm (D) x 4.40 cm (H)	42.60 cm (W) x 47.50 cm (D) x 8.80 cm (H)
管理ポート	1 GbE RJ45 / 115200 8N1 シリアルRJ45			
管理インタフェース	セキュリティ管理システム(SMS) / Local Security Manager(LSM) / コマンドラインインタフェース(CLI)			
I/Oモジュールスロット数	1	2		4
使用可能最大セグメント数	6	10	12	24
オンボックスストレージ	8 GB 1.8インチSSD	32 GB 1.8インチSSD		
電源	100-240 VAC、50-60 Hz		100 ～ 240 VAC / -40 ～ -60 VDC	
電力 (最大ヒューズ電力)	4-2Aアンペア		12/6アンペアAC、24/16アンペアDC	
最大消費電力	250 W (853BTU / 時間)	220 W (751BTU / 時間)	750 W (2,557BTU / 時間)	
電源ユニット	単一	二重化、冗長ホットスワップ対応		
動作温度	0° C ～ 40° C			
動作相対湿度	5% ～ 95% (非結露)			
非動作時/保存温度	-20° C ～ 70° C			
非動作時/保存相対湿度	5% ～ 95% (非結露)			
高度	平均海面からの最高高度10,000フィート (3,048 m)			
安全性・規格	UL 60950-1、IEC 60950-1 EN 60950-1、CSA 22.2 60950-1 RoHS準拠			
EMC	Class A、FCC、VCCI、KC EN55022、CISPR 22、EN55024 CISPR 24、EN61000-3-2 EN61000-3-3、CE Marking			

Threat Protection System I /O モジュール

TX用 I/O モジュール	製品SKU
TippingPoint IO Module: 6-segment Gig-T Rev B	TPNN0196
TippingPoint IO Module: 6-segment GbE SFP	TPNN0068
TippingPoint IO Module: 4-segment 10GbE SFP+	TPNN0060
TippingPoint IO Module: 4-segment Gig-T Bypass	TPNN0070
TippingPoint IO Module: 2-segment 1G Fiber SR Bypass	TPNN0071
TippingPoint IO Module: 2-segment 1G Fiber LR Bypass	TPNN0072
TippingPoint IO Module: 2-segment 10G Fiber SR Bypass	TPNN0073
TippingPoint IO Module: 2-segment 10G Fiber LR Bypass	TPNN0074
TippingPoint IO Module: 1-segment 40GbE QSFP+	TPNN0069
TippingPoint IO Module: 1-segment 40GbE SR4 Bypass	TPNM0131
TippingPoint IO Module: 1-segment 40GbE LR4 Bypass	TPNM0132

vTPS 技術仕様

特長	vTPS Standard	vTPS Performance
インスペクションスループット	250 / 500 Mbps / 1 / 2 Gbps	
同時接続数	10,000,000(VMware)、1,000,000(KVM)	
1 秒当たりの新規接続数	120,000 (VMware)、60,000 (KVM)	
SSL インスペクション	提供なし	1Gbps(VMware)
1 秒当たりの新規SSL接続数	提供なし	1500 (Vmware)、900 (KVM)
SSL 同時接続セッション数	提供なし	6500 (Vmware、KVM)
論理コア数	2 または3	4
メモリ	8 GB	16 GB
ディスク容量	16 GB	
仮想プラットフォームのサポート	VMware ESXi 5.5、6.0、6.5、6.7 (NSX は透過性検査と適用には不要) およびKVM- Redhat Enterprise Linux® 6、7	
ネットワークドライバ	VMware- VMNet3 KVM- virtIO	
ネットワークセグメント数	1	
仮想セグメント数	無制限	
専用管理vNIC	あり	

*1：パフォーマンステストは推奨設定を使用したラボ環境による実測値です。実際のパフォーマンスは実稼働ネットワークにおいて異なる場合があります。お客様はご自身の実環境での実証テストで確認を実施することをお勧めします。

*2：すべてのパケットサイズの平均遅延。

*3：平均パケットサイズ 1024 バイト、ECDHE-RSA-AES256-GCM-SHA384 暗号による 2048 ビットキー。

*4：9200TXE の初期リリースでは、スタッキング構成での TLS 復号化はサポートされません。

*5：最大速度に合わせたSFPモジュールをご利用ください。

弊社における個人情報の収集の詳細については、弊社Web サイトの「Privacy Notice」(以下URL) をご覧ください。

https://www.trendmicro.com/ja_jp/about/legal.html

Securing Your Connected World

TREND MICRO、Securing Your Connected World 、Deep Discovery および、ZERO DAY INITIATIVE はトレンドマイクロ株式会社の登録商標です。
本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。
記載内容は2025年11月現在のものです。
内容は予告なしに変更になる場合がございます。
Copyright @ 2023 Trend Micro Incorporated. All rights reserved.