FORCEPOINT

FORCEPOINT
Intrusion Prevention System

Forcepointは、データセンター、オフィス、支店、クラウドにわたる分散型エンタープライズネットワークを保護するための、業界最高レベルのセキュリティ*侵入防御システム（IPS）を提供しています。

*NSS Labs NGIPS Test 2017

Forcepointのネットワークセキュリティソリューションは、業界で最も安全な侵入防止システムを提供します。 独立系テストで最高の評価を得ているForcepointのIPSは、スタンドアロンのレイヤ2 IPSデバイスとして、または物理、仮想、およびクラウド環境のフル機能のレイヤ次世代ファイアウォール（NGFW）の一部として展開できます。 攻撃者がエンタープライズネットワーク内に侵入して拡散するために使用する回避技術、悪用、およびマルウェアを阻止します。

有効性とスピードのためのユニークなアーキテクチャ

Forcepointは、単純なパケット検査を超えた、動的なストリームベースの検査アプローチを採用しています。 これは実際のペイロードを再構築して検査し、カモフラージュのエクスプロイトやマルウェアを回避するための回避技術を打破します。

さらに、高速できめ細かい復号化により、SLT / LSSトラフィック内に隠れようとする攻撃のマスクを解除できます。 Forcepointは各ペイロードストリームを分析して、プロトコルのさまざまな層をデコードして、異常または不正なプロトコル設定、メタデータ、およびヘッダーを解析します。

解析後、Forcepointは高度な技術を駆使して、さまざまな種類のシステムの脆弱性に対するエクスプロイトの兆候がないかどうかを確認します。 冗長なパターンベースのシグネチャメカニズムとは異なり、Forcepointのより洗練されたアプローチは、そのような攻撃を単一の簡潔なシグネチャで識別することを可能にします。 シグネチャは、各プロトコルコンテキストに合わせて調整された高速のDeterministic Finite-Automata（DFA）を使用して照合されるため、CPUリソースにほとんど影響を与えずに新しいシグネチャを組み込むことができます。

攻撃者の先を行く継続的なアップデート

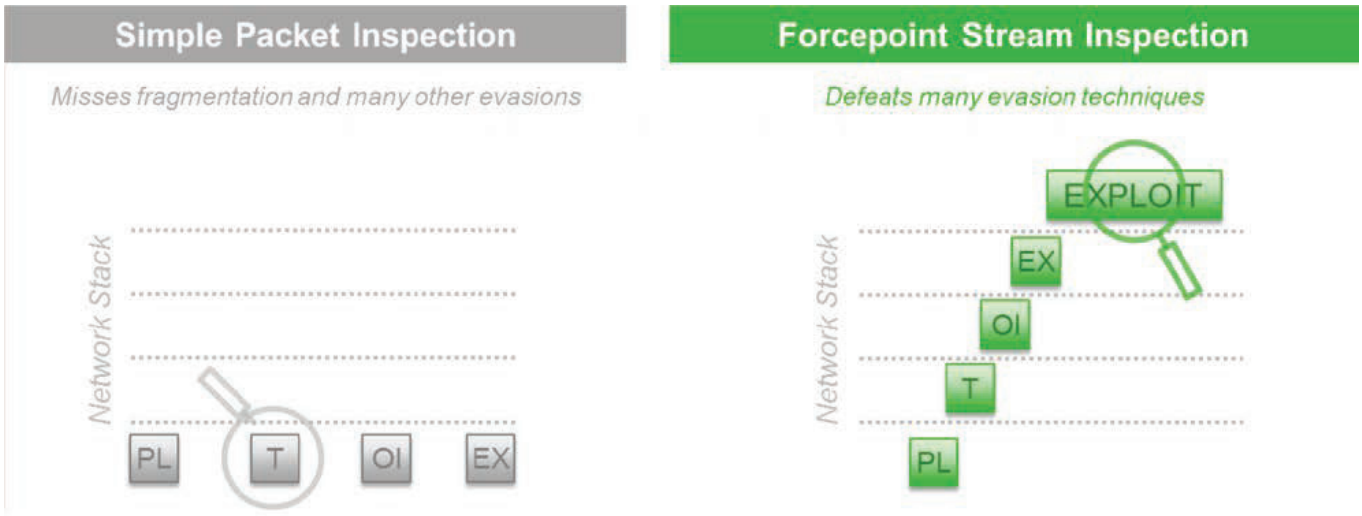
Forcepointのグローバルリサーチチームは、脅威インテリジェンスフィード、多種多様なソースからの脆弱性レポート、およびエクスプロイトと脆弱性を分析するためのさまざまなテストシステムを絶えず調べています。 新しいフィンガープリントは、必要に応じて当社のクラウドサービスを通じて公開され、Forcepointネットワークセキュリティシステムによって自動的にダウンロードされます。 この予防的なアプローチにより、ITチームは時間に余裕を持つことができ、まず公開されたパッチを分析して、即座の不正アクセスを恐れずに修復作業を実施することができます。

ゼロデイと不要なコンテンツをストップ

Forcepointのネットワークセキュリティ製品は、未知の攻撃や望ましくないコンテンツに対する多層の防御機能も提供します。 送信されたファイルは厳格なレピュテーションとマルウェアスキャンを通過し、ゼロデイ攻撃のような新たな脅威は当社の高度なサンドボックス技術で発見されます。 Forcepointは、WEBサイトとコンテンツの分類とフィルタリングのパイオニアです。 IPSデバイスとファイアウォールを使用することで、組織は職場の規制をより容易に遵守し、個人データへの暴露を制限し、ユーザーが危険なコンテンツを含むWEBサイトにアクセスするのを防ぐことができます。

Fail-Openの弾力性

Forcepointのアプライアンスは、IPSやNGFWの電源が切れた場合でもトラフィックを実行し続けるフェールオープンインターフェイスなど、さまざまなモジュラーネットワークカードをサポートしています。



FORCEPOINT は高速エクスプロイト指紋によるフルストリーム再構成を結合する

ビジネス継続のためのプロテクション

攻撃者は、毎日、企業ネットワーク、アプリケーション、データセンター、およびエンドポイントへの侵入を学習、実践しています。 侵入すると、知的財産、顧客情報、およびその他の機密データを盗み出して、企業や評判に回復不能な損害を与える可能性があります。

インターネット攻撃は、単に脆弱性の悪用を拡散し拡大します。多くの有名ベンダーのファイアウォールを含む、従来のセキュリティネットワークデバイスによる検出できない新しい手法が使用されることが増えています。

これらの回避手法は、エクスプロイトやマルウェアを偽装するために複数のレベルで機能し、従来のシグネチャベースのパケット検査からは見えません。この回避技術によって、何年もブロックされてきた古い攻撃でさえも、突然内部システムを危険にさらすために使用される可能性があります。

orcepointは異なるアプローチを取ります。 業界をリードするIPSエンジンは、回避技術の阻止、脆弱性の悪用の検出、およびマルウェアの阻止の3段階のネットワーク防御すべてに対応するように設計されています。 既存のファイアウォールの後ろに透過的に配置して、中断することなく、またはオールインワンセキュリティとしてのフル機能のNGFWとして導入することも可能です。

すべてのForcepointネットワークセキュリティ製品は継続的に更新され、一元管理されており、ネットワーク全体でシームレスにセキュリティポリシーとダッシュボードを共有できます。Forcepointを使用すると、データセンター、オフィスネットワーク、ブランチオフィス、またはクラウド環境全体にわたって、信頼性の高い、一貫性のある効率的なビジネスの安全性を維持できます。

ビジネスの成果

- 侵害の減少
- 運用を中断することなくセキュリティを強化
- ITチームが新しいパッチを展開する準備をしている間の新しい脆弱性への露出減少
- ブランチ、クラウド、データセンターの安全な展開
- セキュリティとネットワークインフラストラクチャのTCOを削減

主な機能

- レイヤ2 IPSまたはレイヤ3 NGFWの一部としての展開
- 実際のペイロードを調べるストリーム検査
- 反回避防御(evasion defenses)のパイオニア
- きめ細かいプライバシー制御を使用した高速復号化
- プロトコル異常と誤用の検出
- 高速DFAによる攻撃とマルウェアの検出
- サービス拒否(DOS)検出
- ボット対策
- クラウドまたはオンプレミスアプライアンスを介したゼロデイサンドボックス
- 業界最先端のURLフィルタリング
- フェールオープンネットワークインターフェース
- 展開間の統一された機能とパフォーマンス
- ポリシーベースの集中管理
- ダウンタイムなしの迅速なアップデート

Forcepoint Intrusion Prevention System (IPS) の仕様

サポートされているプラットフォーム	
アプライアンス	Multiple series of modular appliances for deployment in data centers, at network edges, and in branches
クラウドインフラ	Amazon Web Services, Microsoft Azure
仮想アプライアンス	x86 64-bit based systems; VMware ESXi, VMware NSX, Microsoft Hyper-V, and KVM virtualized environment
展開モード	Standalone IPS (layer 2, with optional fail-open network interface modules), part of NGFW (layer 3)
仮想コンテキスト	Virtualization to separate logical contexts with separate interfaces and policies

インスペクション	
多層トラフィック正規化/フルストリームディープインスペクション	• Reconstructs and analyzes actual payloads to assure integrity of data streams • Discards duplicate lower-level segments that could lead to ambiguities when reassembled
Anti-Evasion防御	Stops out-of-order fragments, overlapping segments, protocol manipulation, obfuscation, encoding tricks
動的コンテキスト検出	Protocol, application, file type
プロトコル固有のトラフィック処理/検査	Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IP-in-IP, IPv6 encapsulation, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC Classic, OPC UA, Oracle SQL Net ,POP3, POP3S, RSH, RSTP, SIP, SMTP, SSH, SunRPC, NBT, SCCP, SMB, SMB2, SIP, TCP Proxy, TFTP, Integrated inspection with Sidewinder Security Proxies
SSL / TLSトラフィックの詳細な復号化	• High-performance decryption of HTTPS client and server streams • Policy-driven controls to protect users' privacy and limit organizations' exposure to personal data • TLS certificate validity checks and certificate domain name-based exemption list
脆弱性エクスプロイトの検出	• Protocol-independent, any TCP/UDP protocol with evasion and anomaly logging • Virtual patching for both client and server CVE vulnerabilities • Sophisticated fingerprint approach eliminates need for many signatures • High-speed deterministic finite automata (DFA) matching engine handles new fingerprints quickly • Continual update of fingerprints from Forcepoint
カスタムフィンガープリント	• Protocol-independent fingerprint matching • Regular expression-based fingerprint language with support for custom applications
偵察検知	TCP/UDP/ICMP scan, stealth, and slow scan detection in IPv4 and IPv6
ボットネット対策	• Decryption-based detection and message length sequence analysis • Automatically updated URL categorization to block or warn users away from botnet sites
相関分析	Local correlation, log server correlation
DoS/DDoS 防御	• SYN/UDP flood detection with concurrent connection limiting, interface-based log compression • Protection against slow HTTP request methods, half-open connection limit. • Separation of Control Plane and Data Plane
ブロッキング方法	Direct blocking, connection reset, blacklisting (local and distributed), HTML response, HTTP redirect
トラフィックレコーディング	Automatic traffic recordings/excerpts from misuse situations
自動アップデート	• Continual dynamic updates through Forcepoint Security Management Center (SMC) • Updates virtual patching and provides detection and prevention for emerging threats

Forcepoint Intrusion Prevention System (IPS) の仕様

高度なマルウェア検出とファイル制御	
プロトコル	FTP, HTTP, HTTPS, POP3, IMAP, SMTP
ファイルフィルタリング	Policy-based file filtering with efficient down-selection process. Over 200 supported file types in 19 file categories
ファイルレピュテーション	High speed cloud-based malware reputation checking and blocking.
ファイルAVスキャン	Local anti-virus scan engine*
ゼロデイサンドボックス	Forcepoint Advanced Malware Detection available both as cloud and on-premise service, same as used by Forcepoint Web Security, Forcepoint Email Security and Forcepoint CASB

URLフィルタリング	
URLカテゴライズ	Powered by Forcepoint ThreatSeeker Intelligence, same as used by Forcepoint Web Security and Forcepoint Email Security
自動アップデート	Continually updated as new sites are analyzed
カテゴリベースアクセスポリシーの執行	Forcepoint NGFW URL Filtering available as an add-on subscription

管理とモニタリング	
マネジメントインタフェース	Enterprise-level centralized management system with log analysis, monitoring and reporting capabilities (see Forcepoint Security Management Center datasheet for details)
SNMPモニタリング	SNMPv1, SNMPv2c, and SNMPv3
トラフィックキャプチャ	Console tcpdump, remote capture through Forcepoint Security Management Center
高セキュリティ管理コミュニケーション	256-bit security strength in engine-management communication
セキュリティ認証	Common Criteria Network Devices Protection Profile with Extended Package Stateful Traffic Filter Firewall, FIPS 140-2 crypto certificate, CSPN by ANSSI, (First Level Security Certification USGv6)

*110/115アプライアンスではローカルのマルウェア対策スキャンは利用できません。

お問合せ先
ForcepointJapan株式会社
〒105-0003　東京都港区西新橋1-2-9　日比谷セントラルビル14階
Tel:03-5532-5602
Email: Japan@forcepoint.com
Web: www.forcepointcom/ja