FORCEPOINT

FORCEPOINT Next Generation Firewall (NGFW)

Enterprise SD-WAN meets the #1 in network security

ForcepointのNGFWに切り替えたお客様より、サイバー攻撃の86%の低下、53%のネットワーク総費用の削減、および70%のインシデント対応時間の短縮*が報告されています。

Forcepoint Next Generation Firewall（NGFW）は、高速で柔軟なネットワーキング（SD-WANおよびLAN）と業界をリードするセキュリティを組み合わせて、進化し続ける多様なエンタープライズネットワーク全体でユーザーと使用されるデータの接続と保護を実現します。Forcepoint NGFWは、物理システム、仮想システム、およびクラウドシステムにわたって一貫したセキュリィ、パフォーマンス、および運用を提供します。 ハイベイラビリティとスケーラビリティ、および360度の可視性を備えた集中管理をゼロから構築できるよう設計されています。

エンタープライズ向け「Always-On」SD-WANコネクティビティ

今日の企業は、完全に回復力のあるネットワークセキュリティソリューションを求めています。Forcepoint NGFWは、あらゆるレベルで高いスケーラビリティと可用性を備えています。

- **アクティブ - アクティブ、混合クラスタリング**異なるバージョンを実行している異なるモデルによる最大16ノードを一度に一緒にクラスタ化できます。これにより、優れたネットワークパフォーマンスと回復力が提供され、詳細なパケット検査やVPNなどのセキュリティを実現します。

- **シームレスなポリシー更新とソフトウェアアップグハード** 業界をリードするForcepointの可用性により、サービスを中断することなく、ポリシーの更新およびソフトウェアのアップグレードをームレスにクラスタにプッシュすることができます。

- **SD-WANネットワーククラスタリング** 高可用性の適用範囲をネットワークおよびVPN接続に拡張します。MPLSのような高価な専用線を補完または交換するために、ローカルブロードバンド接続を有効活用する機能をノンストップなセキュリティで実現します。

セキュリティニーズの変化に対応

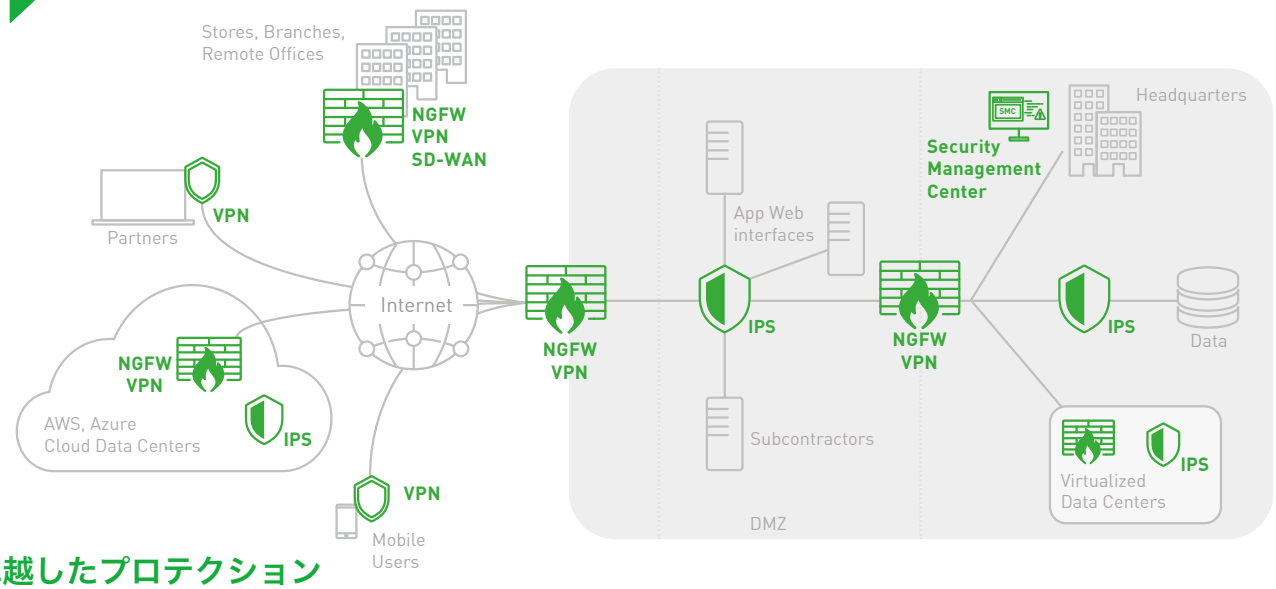
統合されたソフトウェアコアにより、は、動的なビジネス環境において、ファイアウォールVPNからIPS、レイヤ2ファイアウォールと、複数のセキュリティ機能を処理できます。また単一のコンソールからあらゆる管理をさまざまな方法で展開できます（物理、仮想、クラウドアプライアンスなど）。

Forcepointは、各接続に対してアクセス制御と詳細検査を独自に調整して、高いパフォーマンスとセキュリティを提供します。きめ細かいアプリケーション制御、侵入防御システム（IPS）防御、組み込みの非公開プライベートネットワーク（）制御、およびミッションクリティカルなアプリケーションプロキシを、効率的に拡張可能で高いスケーラビリティを持った設計がなされています。Forcepointの強力な回避防止技術は、検査前およびすべてのプロトコルレイヤでネットワークトラフィックをデコードおよび正規化して、最も先進的な攻撃方法を明らかにし、ブロックします。

巧みなデータ侵害攻撃を阻止

大規模なデータ侵害は、あらゆる業界の企業や組織を悩ませ続けていますが、今ではForcepointのアプリケーションレイヤーエクスフリトレーションプロテクション機能で反撃可能です。 Forcepoint NGFWは、きめ細かいエンドポイントコンテキストデータに基づいて、PC、ラップトップ、サーバー、ファイル共有、およびその他のエンドポイントデバイス上の特定のアプリ ケーションから発生するネットワークトラフィックを選択的かつ自動的にホワイトリストまたはブラックリストに追加します。 許可されていないプログラム、Webアプリケーション、ユーザー、および通信チャネルを介してエンドポイントから機密データが漏洩することを防止することは、従来のファイアウォールを超えるものです。

* "Quantifying the Operational and Security Results of Switching to Forcepoint NGFW", R. Ayoub & M. Marden, IDC Research, May 2017.



多数の展開オプションを持つ1つのプラットフォームで -
すべて単一のコンソールから管理

卓越したプロテクション

攻撃者は、ネットワーク、アプリケーション、データセンター、エンドポイントへの侵入を実行するエキスパートです。一旦内部に侵入すると、知的財産、顧客情報、その他の機密データを盗み、企業やその評判に回復不能な損害を与えることとなります。

最新の攻撃手法は、脆弱性の悪用の単純な伝達共有を超えて移動しながら、多くのよく知られた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を回避することができます。

巧みな回避手法(Evasions)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。回避によって、何年もブロックされてきた古い攻撃でさえも内部システムを危険にさらすために再パッケージ化することができます。

Forcepoint NGFWは異なるアプローチを取ります。業界をリードするセキュリティエンジンは、3つのステージすべてに対応しています。

ネットワーク防御の目的：回避策を打破、脆弱性の悪用を検出しマルウェアを阻止する事です。既存のファイアウォールの背後に透過的に導入することで、中断することなく保護を追加することも、オールインワンセキュリティのためのフル機能のNGFWとして導入することもできます。

さらに、Forcepoint NGFWは急激に変化する世界で貴社のビジネスとユーザーを安全に保つため、HTTPS Web接続を含む暗号化されたトラフィックの高速復号化をきめ細かいプライバシー制御と組み合わせて提供します。 特定のエンドポイントアプリケーションからのアクセスを制限してデバイスをロックダウンしたり、脆弱なソフトウェアの使用を防ぐこともできます。

ビジネスにおける成果

- ブランチ、クラウド、データセンターの迅速な展開
- ダウンタイムの短縮
- 中断することなくセキュリティを強化
- セキュリティ侵害の最小化
- 新しい脆弱性への露出が少なく、ITチームは新しいパッチを展開する準備が可能となる
- ITネットワークインフラストラクチャとセキュリティの総保有費用を削減

主な機能

- エンタープライズ規模でのSD-WAN接続
- 組み込みIPSと回避防御
- デバイスの高可用性クラスタリングとネットワーク自動化された、ダウンタイムゼロでのアップデート
- ポリシー駆動型集中管理
- 実用的でインタラクティブな360°の可視性
- ミッションクリティカルなアプリケーションのためのSidewinderセキュリティプロキシ
- Human-centricなユーザーとエンドポイントのコンテキスト
- きめ細かいプライバシー制御を備えた高性能復号化
- クライアントアプリケーションとバージョンによるホワイトリスト/ブラックリスト
- CASBとWebセキュリティの統合
- マルウェア対策サンドボックス機能
- 物理、AWS、Azure、VMwareへ展開可能な統合ソフトウェア

Forcepoint Next Generation Firewall (NGFW) 仕様

プラットフォーム	
物理アプライアンス	Multiple hardware appliance options, ranging from branch office to data center installations
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
エンドポイント	Endpoint Context Agent (ECA), VPN Client
仮想コンテキスト	Up to 250
集中管理	Enterprise-level centralized management system with log analysis, monitoring and reporting capabilities **See the Forcepoint Security Management Center datasheet for details.**
FIREWALL機能	
ディープパケット インスペクション	Multi-Layer Traffic Normalization/Full-Steam Deep Inspection, Anti-Evasion Defense, Dynamic Context Detection, Protocol-Specific Traffic Handling/Inspection, Granular Decryption of SSL/TLS Traffic, Vulnerability Exploit Detection, Custom Fingerprinting, Reconnaissance, Anti-Botnet, Correlation, Traffic Recording, DoS/DDoS Protection, Blocking Methods, Automatic Updates
ユーザー識別	Internal user database, Native LDAP, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, Client Certificates
高可用性	▸ Active-active/active-standby firewall clustering up to 16 nodes ▸ SD-WAN ▸ Stateful failover (including VPN connections) ▸ Server load balancing ▸ Link aggregation (802.3ad) ▸ Link failure detection
IPアドレスアサインメント	▸ IPv4 static, DHCP, PPPoA, PPPoE, IPv6 static, SLAAC, DHCPv6 ▸ Services: DHCP Server for IPv4 and DHCP relay for IPv4 and IPv6
ルーティング	▸ Static IPv4 and IPv6 routes, policy-based routing, static multicast routing ▸ Dynamic routing: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, IGMP proxy ▸ Application-aware routing
IPv6	Dual stack IPv4/IPv6, ICMPv6, DNSv6, NAT, Full NGFW features
プロキシリダイレクト	HTTP, HTTPS, FTP, SMTP protocols redirection to Forcepoint or third party Content Inspection Service (CIS) on premise and Cloud
地理的プロテクション	Dynamically updated source/destination country or continent
IPアドレスリスト	Predefined IP categories or using custom or imported IP address lists
URLフィルタリング (Separate Subscription)	Custom or imported URL lists

Forcepoint Next Generation Firewall (NGFW) 仕様

エンドポイント アプリケーション	Application name and version
ネットワーク アプリケーション	7400+ network and cloud applications
Sidewinderセキュリティプロキシ	TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS
SD-WAN	
プロトコル	IPsec and TLS
サイト-to-サイトVPN	▸ Policy- and route-based VPN ▸ Hub and spoke, full mesh, partial mesh, Hybrid topologies ▸ Dynamic selection of multiple ISP Links ▸ Load sharing, active/standby, link aggregation ▸ Live monitoring and reporting on ISPs link quality (Delay, jitter, packet loss)
リモートアクセス	▸ Forcepoint VPN client for Microsoft Windows, Android, and Mac OS ▸ Any standard IPsec client ▸ High availability with automatic failover ▸ Client security checks ▸ Access to TLS VPN portal
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
ファイルリピュテーション	High speed cloud based Malware reputation checking and blocking
Anti-Virus	Local antivirus 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

*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