Forcepoint Web Security

FORCEPOINT'S CLOUD AND ON-PREMISES WEB SECURITY

貴社のビジネスとそのデータは常に攻撃を受けています。従来のセキュリティソリューションでは、もはや十分な保護が得られません。事実、攻撃者は貴社をデータの損失や訴訟の危険にさらす可能性があります。高度な脅威、暗号化ランサムウェア、エクスプロイトキットからネットワークとデータを保護することは、ますます危険にさらされているモバイルおよびクラウド接続のデジタル世界でビジネスを存続させるために不可欠です。

カスタマイズ可能な展開オプション

企業は、これらの種類の脅威が発生したとき防御するために、相互に通信するカスタマイズ可能なソリューションを必要としています。 Forcepoint Web Securityは、組織のニーズに合わせてWeb保護パッケージを調整するのに役立つ複数の展開オプションとモジュールにより、高度な脅威とデータの盗難に対するリアルタイムの保護を提供します。

Forcepoint Web Securityは、コンテンツを意識した防御とクラウドアプリの検出と監視を通じて強力な保護を提供し、社内ユーザーとモバイルユーザーの両方にとって機密データへのリスクを軽減します。

何よりも、Forcepoint Webセキュリティは他のForcepointソリューションと簡単に統合可能で、単一の一貫したセキュリティ管理により、最小のセキュリティチームでもインバウンドおよびアウトバウンドの脅威から保護することができます。

Forcepoint Web Security

高度な脅威防御のための リアルタイム分析

Forcepoint Web Securityは、Forcepoint ACE予測分析との複合スコアリングプロセスを使用して、８つの防御評価領域を介してアンチウイルス防御で行えることをはるかに超えています。 複数のリアルタイムコンテンツエンジンが、Webページ全体のコンテンツ、アクティブなスクリプト、Webリンク、コンテキストプロファイル、ファイル、および実行可能ファイルを分析します。

フォレンジックデータへの簡単なダッシュボードアクセス

Forcepoint Web Securityの高度な脅威ダッシュボードは、誰が攻撃を受けたのか、どのデータが標的にされたのか、データの意図されたエンドポイント、そして攻撃の実行方法についてのフォレンジックレポートを提供します。 セキュリティインシデントには、可能な限りデータ盗難のキャプチャが含まれます。 防御はインバウンドおよびアウトバウンド通信を分析します。

統合されたデータ盗難防止

業界最先端の統合型データ盗難防御（オプション）は、データ盗難の試みを検出して傍受し、データ損失防止（DLP）に関する規制遵守を提供します。 これらの機能の例には、カスタム暗号化されたアップロードの検出、パスワードファイルデータの盗難、低速データ漏洩（Drip-DLP）、画像内のテキストの光学式文字認識OCR（光学式文字認識）、および地理的位置の認識が含まれます。

統合されたサンドボックス

統合されたサンドボックスサービスを使用してマルウェアの行動を自動的に分析することで、貴社の資産をより適切に保護する方法を学びましょう。

クラウドアプリケーションの発見、監視と制御

組織内で使用されているクラウドアプリケーションを発見し、認可されていないクラウドアプリケーションやサービスに送信することでユーザーがデータを危険にさらすことを防ぎます。 インライン（プロキシ）統合を使用して、クラウドアプリケーション用の完全なCloud Access SecurityBroker（CASB）機能を簡単に追加します。

強化された保護モジュール

Hybrid Cloud Deployment	Webプライベートクラウド用の物理アプライアンスまたは仮想アプライアンスとしてForcepoint Web Securityをデプロイします。 どちらを選択しても、リモートユーザー保護のためのForcepointのグローバルクラウドインフラストラクチャでさらに拡張できます。保護とポリシーの適用をリモートユーザーに拡張する
WEB DLP	**データ盗難に対するアウトバウンド保護を強化するための、強力で状況に応じたDLPエンジンを追加する** Forcepoint Web DLPはデータ盗難に対する封じ込め防御を提供し、007,1以上の事前定義されたポリシーとテンプレートへの規制遵守を可能にします。 また、低速データ漏洩に対するDrip-DLP、画像ファイル内のデータファイルの盗難に対する光学式文字認識（OCR）、犯罪的に暗号化されたファイルを検出するためのカスタム暗号化検出などの業界最先端の保護も含まれます。
Cloud Sandbox	**マルウェアファイルの自動および手動分析のためのビヘイビアサンドボックスを統合する** 仮想環境で疑わしいファイルを分析し、単純なファイル実行よりもはるかに深く見て、高度なマルウェアから最高レベルの保護を提供します。悪意のあるファイルが検出されると、詳細なフォレンジックレポートが自動的に提供されます。
Mobile Security	**iOSおよびAndroidユーザーにポリシーと保護を拡張する** 既存のセキュリティポリシーをモバイルデバイスに拡張し、それらを高度な脅威、モバイル攻撃、なりますなどから保護します。Forcepoint Mobile Securityはモバイルデバイスマネージャと同様に保護します。
Cloud Access Security Broker (CASB)	**既存の機能を補完するためCASBの全機能を拡張し使用されているクラウドアプリケーションを可視化** これらの完全なCASB機能は、インライン（プロキシ）展開用のクラウドアプリケーションを制御するために使用でき、Webセキュリティゲートウェイから簡単に拡張できます。

Forcepointソリューションの背後にある力

Forcepoint ACE

Forcepoint ACEは、複合リスクスコアリングおよび予測分析を使用して、Web、Eメール、データ、およびモバイルのセキュリティに対するリアルタイムのインラインコンテキスト防御を提供します。

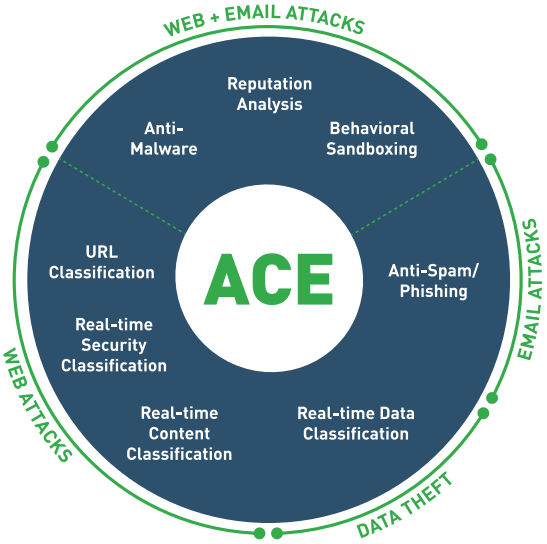
利用可能な最も効果的なセキュリティを提供するため。 業界をリードするデータ盗難防止のためのデータ対応防御を備えたインバウンドトラフィックとアウトバウンドトラフィックを分析して封じ込めを行います。 リアルタイムセキュリティ、データおよびコンテンツ分析のための分類エンジン - 長年の研究開発の結果 - ACEは、従来のアンチウイルスエンジンよりも多くの脅威を毎日検出することができます。（htt://psecuritylabs.forcepoint.COMで毎日更新され確認できます。） ACEは、すべてのForcepointソリューションの背後にある主要な防御策であり、Forcepoint ThreatSeekerIntelligence Cloudによってサポートされています。

Forcepoint ThreatSeeker Intelligence

Forcepoint Security Labsが管理するForcepoint ThreatSeeker Intelligenceは、すべてのForcepointセキュリティ製品に中核的な集合的なセキュリティインテリジェンスを提供します。Facebookからの入力を含め、9億以上のエンドポイントを統合し、Forcepoint ACEのセキュリティ防御により、1日あたり最大50億のリクエストを分析します。この広範なセキュリティの脅威に対する認識により、Forcepoint ThreatSeeker Intelligenceは、高度な脅威、マルウェア、フィッシング攻撃、ルアーおよび詐欺をブロックするリアルタイムのセキュリティアップデートを提供することができますし、最新のWeb評価もまた提供できます。Forcepoint ThreatSeeker Intelligenceは、サイズと、一括入力を分析するためのACEリアルタイム防御の使用において比類のないものです。(Webセキュリティにアップグレードすると、Forcepoint ThreatSeeker IntelligenceがWebの脅威やデータの盗難に対する危険を減らすのに役立ちます。）

統合的アーキテクチャ

クラス最高のセキュリティと統一されたアーキテクチャを備えたForcepointは、Forcepoint ACEによるリアルタイムのインライン防御により、ポイントオブクリックによる保護を提供します。ACEの比類のないリアルタイム防御は、Forcepoint ThreatSeeker IntelligenceとForcepoint Security Labsの研究者の専門知識によって支えられています。強力な結果は、単一のユーザーインターフェースと統一されたセキュリティインテリジェンスを持つアーキテクチャです。



単一の統一されたアーキテクチャ

- 徹底的な検査をサポートするために利用可能な10,000の分析法。
- 予測セキュリティエンジンは、いくつかの動きを先取りしています。
- インラインオペレーションは脅威を監視するだけでなく、**ブロック**します。

その他の機能

- **Remote User Protection.** Hybrid Cloudの展開により、1つのコンソールとポリシーで企業、支店、およびリモートユーザーを管理できます。
- **Flexible SSL Inspection.** きめ細かいSSL検査機能により、プライバシーと規制要件を維持しながらHTTPSトラフィックを監視できます。
- **API for Threat Intelligence.** 発行されたAPIを取り込むと、Webセキュリティがよりスマートになります。業界または地域固有の脅威インテリジェンスを取り入れ、セキュリティ管理の自動化を可能にします。
- **Application and Protocol Control.** ネットワークエージェントは、セキュリティ体制を強化するために、何百ものプロトコルとアプリケーションを細かく制御します。
- **Flexible Reporting.** 4つのカスタマイズ可能なダッシュボード、およびを超える事前定義済みのカスタマイズ可能なレポートにより、読みやすいビジネスおよび技術情報、さらに脅威レベルなどに関する貴重な洞察が得られます。
- **Multiple Deployment Options** クラウド、ハイブリッド、またはオンプレミスアプライアンス（仮想または物理）から展開可能です。
- **Proxy-Less EndpointProtection.** 私たちのソリューションは、どこでも、どんなネットワークでも働くユーザーを保護します。 アプリケーションは、通常プロキシベースのクラウドソリューションで問題を引き起こすような環境でも機能し続けます。
- **IntegratedDLPIncidentRiskRanking.**業界初のセキュリティ分析機能により、DLP調査のコストを削減し、効率を高めます。
- **Expanded Internet Access for Roaming Users.** 従業員が会社の所在地と社外の所在地から接続するときに異なるポリシーを適用する（ビデオストリーミングは自宅では許可され、登録された企業の場所にいるときにブロックされます）。
- **Cloud App Control.** 承認されていないクラウドアプリケーションの使用をブロックする一方で、組織に承認されているとみなされるものの使用を許可します。 インライン（プロキシ）展開モードでクラウドアプリケーションを制御するためのWebセキュリティソリューションに対応するための完全なCASB機能を簡単に追加できます。
- **Web Security Cloud Migration tools.** Forcepointの主要オンプレミスアプライアンスから業界で最も安全なクラウド、Forcepoint Web Security Cloudへのアップグレード。

ABOUT FORCEPOINT

Forcepointは、最も重要なこと、つまり重要なデータやシステムと対話するときの人々の行動に焦点を合わせることによって、サイバーセキュリティを変革しています。 サイバーセキュリティに対するこの人間中心のアプローチにより、従業員は通常のユーザーの行動のリズムと組織内外でのデータの流れを理解することによって革新することができます。 Forcepointの行動ベースのソリューションは、リアルタイムでリスクに適応し、統合セキュリティプラットフォームを介して提供され、ネットワークユーザーとクラウドアクセスを保護し、機密データが企業ネットワークから流出するのを防ぎ、インサイダーによる侵害を排除します。 テキサス州オースティンに本拠を置くForcepointは、150カ国以上の何千もの企業および政府機関の顧客のHuman Pointを保護します。

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