

Forcepoint ONE: クラウドプラットフォームがハイブリッドワーカーのためのセキュリティを簡素化

ユースケース

- ハイブリッドワーカーによるWeb、クラウド、プライベートアプリ上のデータのやりとりを可視および制御。
- マネージドデバイス/アンマネージドデバイスからアクセスする機密データの不正使用を防止。
- リスクの高いWebコンテンツやさまざまな種類のGenAIサイトへのアクセスを制御します。
- 複雑なVPNを利用しなくても、ビジネスリソースやプライベートアプリへの安全なリモート高速アクセスを提供。

ソリューション

- 単一の統合プラットフォームにより、すべてのビジネスアプリで一貫したセキュリティポリシーを管理できます。
- セキュアWebゲートウェイ (SWG)、クラウドアクセスセキュリティブロッカー (CASB)、ゼロトラストネットワークアクセス (ZTNA) を組み合わせることで、アクセスやデータを保護するオールインワンのクラウド型サービス。
- 攻撃者の侵入を阻止して機密データを保持する、脅威に対する高度な保護とデータセキュリティの統合。
- RBI、パブリッククラウドテナントのリスクのある構成をスキャンするCSPM、コンテンツ脅威を除去するCDRなどの追加機能。
- データタグ付けに利用できるForcepoint分類。

結果

- 簡素化 - Web、クラウド、プライベートアプリのセキュリティを統合プラットフォームに統合 (エージェントレスにも対応)。
- 最新化 - ゼロトラスト原則とSASEアーキテクチャおよびリモートブラウザ隔離、ダウンロードしたファイルのサニタイズなどの高度なセキュリティの組み合わせを実現。
- 場所の制限なし - 300以上のポイントオブプレzens (PoP) で、グローバルに利用可能。
- 信頼性 - 2015年以降、99.99%の検証済みアップタイムを提供。
- 高速化 - 分散配備と自動スケーリングにより問題が生じやすい箇所を排除。

データファーストのセキュリティ

セキュリティの複雑化がますます進む中、より良い方法はまだ残されています。ユーザーは、ウェブサイト、クラウドアプリケーション、プライベートアプリケーションなど、データがあらゆる場所に分散した状態で、様々なところから仕事をしています。

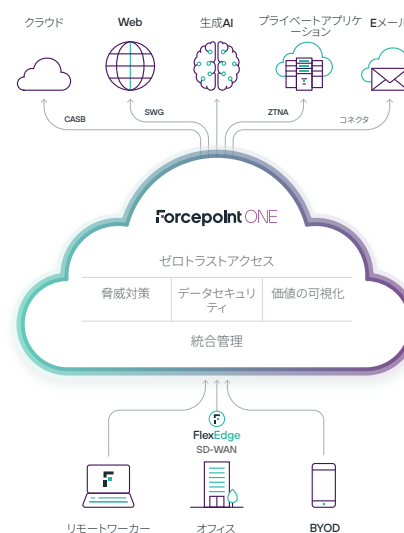
オフィス回帰への傾向とハイブリッドワーカーをサポートするには、データを中心に置く統合型セキュリティプラットフォームが必要不可欠です。セキュリティ制御は、一貫した可視性と制御を持ち、ウェブ、クラウド、プライベートアプリケーションへのアクセスへと拡張できる必要があります。そうすることで、組織のデータ流出を未然に防ぐことができます。

データファーストソリューションにより、あらゆる場所で作業するユーザーのためにビジネスデータをあらゆる場所で保護できます。

Forcepoint ONEがセキュリティをシンプルに

Forcepoint ONEは、セキュリティをシンプルにする統合クラウドプラットフォームです。SWG、CASB、ZTNAなどの重要なセキュリティサービスを統合しているため、ゼロトラストとセキュリティサービスエッジ (SSE、SASEのセキュリティコンポーネント) をすぐに導入できます。

さまざまなタイプのGenAIサイトへのアクセスを制御し、機密データを保護してマルウェアへの暴露を防ぐべく常にガードレールの役割を果たすため、GenAIなどの新たなテクノロジーを安全に導入し、生産性を最大限に高めることができます。





Forcepoint ONEが提供するクラウドネイティブなゼロトラスト機能には、以下のようなものがあります。

- **クラウドおよびプライベート アプリ向けのエージェントレス DLP セキュリティ。**機密データを安全に保ちながら、個人のデバイスからプライベート ビジネス Web アプリを安全に使用します
- **統合された高度な脅威保護とデータセキュリティ。**データの損失や流出を防止し、あらゆる場所で一貫性のある制御をすることでハッカーの侵入を阻止します。
- **クラウド、ウェブ、プライベートアプリアクセスのための統合ゲートウェイ。**SWG、CASB、ZTNAに向けた1つの場所で管理されるビジネスアプリケーションの認証ベースのアクセス制御。
- **グローバルアクセスによるダイナミックなスケラビリティ** - AWS上に構築された300のPoPは、勤務場所を問わず、高速で遅延の少ない接続と

Web、クラウド、プライベートアプリ向けの統合セキュリティ

- **クラウド:**CASBは、あらゆるデバイスから企業の SaaS アプリやデータへの粒度の細かなアクセスを実現します。CASBは、機密データのダウンロードをブロックし、マルウェアのアップロードをリアルタイムでブロックします。一般的なSaaSやIaaSの静止データに対してマルウェアや機密データの スキャンを行い、必要に応じて修復を行います。CASBは、シャドーITアプリを検出し、あらゆるマネージドデバイスからのアクセスを制御します。
- **Web:**SWGがリスクとカテゴリに基づいてあらゆる Webサイトとのやり取りを監視および制御し、マルウェアのダウンロードや、個人のファイル共有や電子メールアカウントへの機密データのアップロードをブロックします。当社のオンデバイスWebセキュリティが、あらゆる場所の管理対象デバイスに対して許容される使用ポリシーを適用します。
- **プライベートアプリ:**ZTNAは、VPN関連の複雑さやリスクに悩まされることなく、プライベートアプリケーションへのアクセスを保護し、簡素化できます。

脅威に対する高度な保護とデータセキュリティの統合

- **データ損失防止 (DLP)** : ファイルやテキストのアップロードとダウンロード時に機密データをスキャンし、必要に応じてブロック、追跡、暗号化、再編集を行います。
- **マルウェアスキャン** : ファイルのアップロードとダウンロード時にマルウェアをスキャンし、検出時にはブロックします。

統合された可視性と制御

- **統合管理スイート** から、SSEチャネル全体の構成、監視、レポート作成を実行できます。
- **ログインポリシー** で、ユーザーの場所、デバイスの種類、デバイスのセキュリティ体制、ユーザーの動作、ユーザーグループに基づいて、Web、クラウド、またはプライベートアプリケーションへのアクセスを制御。これらのパラメータは、アカウント乗っ取りを防止するのに役立ちます。
- **使いやすいDLPポリシー** で、管理対象SaaSアプリ、プライベートアプリ、Webサイトの機密データとマルウェア、さらに管理対象のSaaSおよびIaaSに保存されているデータのダウンロードとアップロードとを制御します。
- オンデバイスエージェント (WindowsおよびMacOS用) で、非ブラウザクライアントアプリやシャドウITコントロール用のSWG、CASB、ZTNAをサポートします。
- **統合解析と値の視覚化** - セキュリティリスクや全体の利用状況、オールインワンのクラウドセキュリティプラットフォームへの影響に関する素早い洞察を提供します。

必要に応じて追加機能を利用可能

- **クラウドセキュリティのポスチャマネジメント (CSPM)** : AWS、Azure、GCPのテナント設定をスキャンし、リスクの高い構成を手動および自動で修正します。
- **SaaSセキュリティのポスチャマネジメント (SSPM)** : Salesforce、ServiceNow、Office 365のテナント設定をスキャンし、リスクの高い構成を手動および自動で修正します。
- **リモートブラウザ分離 (RBI)** : クラウドホスト型VMでブラウザを実行することにより、ローカルデバイス上のウェブ感染型マルウェアからユーザーを保護します。
- **Forcepoint Classification** : AIを活用しタグ付け精度を高めるデータ分類を実行します。
- **AMDP** : 制御されたマルウェアのサンドボックス内でファイルの動作を分析し、隠れた悪意のあるコンテンツを特定します。

シンプルさを追求したサブスクリプション

ユーザーごとの年間契約も可能:

- Web、クラウド、プライベートアプリのセキュリティに対応した**オールインワンエディション**。
- **ウェブセキュリティエディション**には、無制限のクラウドアプリをサポートするWebゲートウェイおよびインラインCASB、さらにクラウドアプリ用のAPIサポートとプライベートアプリ用のサポートを後から追加するための、未分類および新規に登録されたサイト用のRBIエッセンスが含まれます。
- **ZTNA エディション**は、無制限の数のプライベートアプリケーションを保護します。
- **CASB エディション**は、無制限の数のクラウドアプリケーションをインラインで保護し、追加のアプリパックまたは専用のAPIポーリングノードを追加する機能を備えた3つのアプリケーション用のAPIを含みます。
- **すべてのサブスクリプション**には、一元的なクラウド管理、データ損失防止を備えたポリシー、エンドポイントエージェント経由の自動アクセス、および包括的なレポート機能が含まれています。

forcepoint.com/contact