

Forcepoint ONE：オールインワンのクラウドプラットフォームでハイブリッドワーカーのセキュリティをシンプルに

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化および制御。
- 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コンテンツへのアクセスを制御。
- 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

- コンソールからエンドポイントエージェントまで、すべてのアプリに共通するポリシーセットの管理を実現する単一の統合プラットフォーム。
- 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ーカー (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（詳細は2ページを参照）。

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それぞれ単一のポリシーセット、コンソール、エージェント（エージェントレス対応）に統合。
- 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ゼンス (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。

複雑なポイントソリューションがもたらすリスク

セキュリティの複雑化は留まるところを知りません。従業員の75%がリモート勤務になれば、自宅とオフィスの境界線は曖昧になります。Webサイト、クラウドアプリ、プライベートアプリなど、現在データはあらゆる場所に存在します。

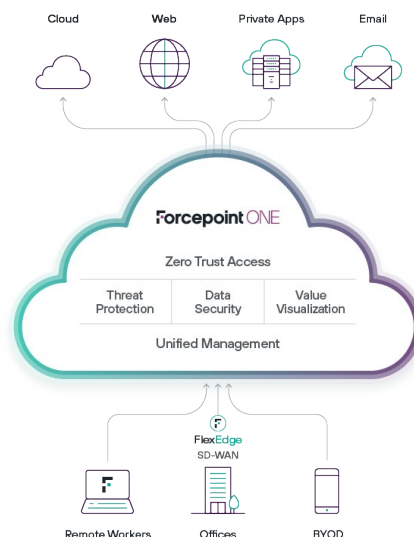
アンマネージドデバイスやBYODを使用するリモート勤務の従業員、パートナー、請負業者は、御社を脆弱にします。デバイスは古い機能を用いて速度の遅いVPNに接続しています。コラボレーションやコミュニケーション目的で使用する業務用アプリにもリスクが潜みます。サイバー犯罪者や国家は御社のデータを狙っており、あらゆる手口を使って侵入を試みています。

よりシンプルなアプローチが必要となります。

Forcepoint ONEがセキュリティをシンプルに

Forcepoint ONEは、セキュリティを簡素化するオールインワンのクラウドプラットフォームです。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ーカー (CASB)、ゼロトラストネットワークアクセス (ZTNA) などの重要なセキュリティサービスを統合した当社は、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) を迅速に導入することが可能です。

断片的な製品の時代は終わりを迎えました。当社は、単一のプラットフォーム、コンソール、エージェントなど、多くのソリューションを提供します。マネージドアプリ/アンマネージドアプリとすべてのデバイスにおいて、単一のセキュリティポリシーセットで可視化およびアクセス制御、データ保護を実現します。





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。

- **Web、クラウド、プライベートアプリへのアクセスに対応した統合ゲートウェイ** – SWG、CASB、ZTNAを一元管理する業務用アプリに対するIDベースのアクセス制御。
- **クラウドおよびプライベートアプリ用エージェントレスBYODセキュリティ** – 機密データを保護しながら、個人デバイスでプライベートな業務用Webアプリを安全に使用。
- すべてのゲートウェイでデータの損失や流出を防ぎ、ハッカーの侵入を阻止する**脅威に対する高度な保護とデータセキュリティの統合**。
- **グローバルアクセスによるダイナミックなスケーラビリティ** – 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99.99%のアップタイムを提供。

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

- **Web** : SWGは、リスクとカテゴリに基づきあらゆるウェブサイトとのやりとりを監視および制御し、マルウェアのダウンロードまたは個人の共有ファイルや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SWGは、あらゆる場所のマネージドデバイスに対して利用規約を施行します。
- **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。
- **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。

単一のポリシーセットによるシンプル化

- **単一の管理コンソール**で構成および監視、報告を実行。
- **単一のログインポリシーセット**でユーザーの場所、デバイスの種類、デバイスポスチャ、ユーザーの行動、ユーザーグループに基づきWeb、クラウド、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、アカウントの乗っ取り防止に役立ちます。
- **単一のDLPポリシーセット**機密データのダウンロード/アップロード、管理対象SaaSアプリ/プライベートアプリ/ウェブサイトのマルウェア、および管理対象SaaSとIaaSに格納されたデータを制御します。
- WindowsおよびMacOS用**統合オンデバイスエージェント**でSWG、CASB、ZTNAをサポートし、非ブラウザ型のクライアントアプリとシャドーITを制御。
- **統合解析と値の視覚化**一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。
- **ゼロトラストコンテンツの非武装化と再構築 (CDR)** : 文書に埋め込まれたマルウェアを除去し、ユーザーが開く前にファイルを再作成します。

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**。
- **Webセキュリティエディション**では、クラウドおよびプライベートアプリのサポートを後から追加できます。
- **すべてのサブスクリプション**には、クラウドの一元管理、データ損失防止機能を備えた統合ポリシー、統合エンドポイントエージェント経由の自動アクセス、包括的なレポートが含まれます。

forcepoint.com/contact