

FireCloud Internet Access



場所を問わないエンタープライズグレードのプロテクション

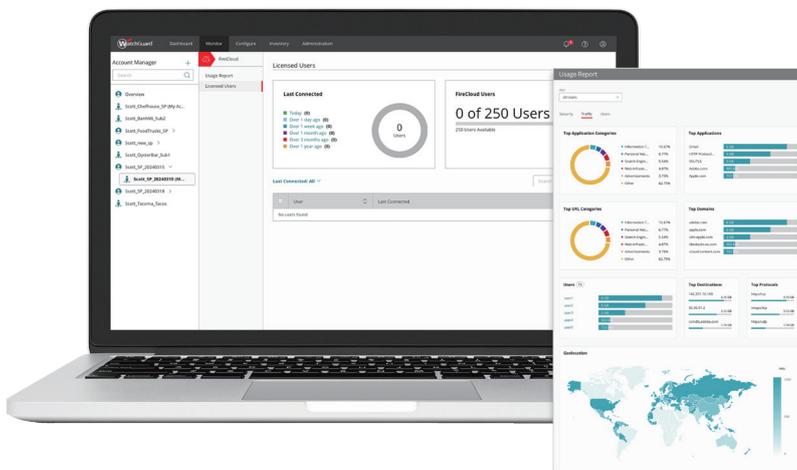
今日の職場は、従来のオフィス形態から進化を遂げ、従業員は遠隔地や自宅から効率的に仕事をするようになってきました。このような柔軟性の高い環境はビジネスに貢献しますが、同時に従来のネットワークの境界を曖昧にし、セキュリティ上の大きな課題にもつながっています。FireCloud Internet Accessは、ユーザーの生産性を維持しながら、こうしたセキュリティの問題に取り組むために設計されたクラウドベースのセキュリティソリューションです。FireCloud Internet Accessは、SASE（セキュアアクセスサービスエッジ）ソリューションの重要なコンポーネントであり、インターネットやクラウドアプリケーションへのリモートユーザーアクセスを世界中のどこからでも管理し、セキュリティを確保するという重要な課題に対応しています。

ネットワーク境界を越える強力なセキュリティ

従来の境界セキュリティソリューションは、あらゆる組織を保護するために不可欠ですが、リモートワーカーが増加しているのに対して、既存のツールは複雑な脅威の情勢に対処できず、リモートユーザーのセキュリティを強化するソリューションが必要とされています。ユーザーは勤務地を問わず、オフィスで働く組織のユーザーと同等レベルの保護を受けて然るべきです。

FireCloud Internet Accessは、オンプレミスのセキュリティサービスを世界中のリモートワーカーに拡張するクラウドベースのセキュリティソリューションです。URLフィルタリング、侵入防止システム（IPS）、DNSセキュリティなど、オンプレミスで提供されている保護機能を含む堅牢なセキュリティと管理機能を提供し、安全でセキュアなWebおよびクラウドアプリケーションへのアクセスを実現します。

FireCloud Internet Accessを利用することで、マルウェア、フィッシング詐欺、その他のオンライン脅威からビジネスを保護し、柔軟にセキュリティの導入と拡張を可能にします。



FireCloud Internet Access の主な特長：

- セキュリティパフォーマンスの向上：**ファイアウォールのセキュリティポリシーと保護機能を素早くリモートワーカーにまで拡張し、シームレスなユーザーエクスペリエンスを実現します。
- 管理の合理化と効率化：**組織全体で一貫したセキュリティポリシーを適用することで、導入の簡素化、環境の強化、効率性の向上、そして攻撃リスクの低減を実現します。
- 包括的な脅威プロテクション：**侵入防止システムとマルウェア検知により、新たな脅威から組織を守ります。
- セキュアなインターネットアクセス：**従業員のリモートインターネットアクセスを管理し、コンプライアンスを高め、Webベースの攻撃を防御します。
- 集中管理：**クラウドベースの管理により、管理負荷の削減、アップデートやメンテナンスの自動化、セキュリティイベントのレポートの合理化を可能にします。

従業員向けのシームレスなグローバルセキュリティ

FireCloud Internet Access は、リモートワーカーのセキュリティを確保し、クラウドでホストされるアプリケーションを保護します。WatchGuard Cloud を通じてシームレスに管理される FireCloud Internet Access は、ファイアウォール・アズ・ア・サービス (FWaaS) とセキュア Web ゲートウェイ (SWG) 機能を統合し、堅牢なエンタープライズグレードのセキュリティを提供します。WatchGuard Cloud を利用することで、管理者はグローバル規模でセキュリティサービスとポリシーを容易に設定し、即座に世界中の PoP (ポイントオブプレゼンス) に反映させることができます。ユーザーは、どのデバイスでも FireCloud クライアントに認証情報を入力するだけでスムーズにアクセスし、接続先を問わず、安定したセキュリティを確保することができます。



ステートフルファイアウォール

ネットワークトラフィックの検査に加え、悪意のあるアクティビティをブロックし、機密データを保護します。また、侵入防止、マルウェア検知、URL フィルタリングなどの高度な機能も提供し、さまざまな脅威から組織を保護します。



侵入防止サービス (IPS)

悪意のあるトラフィックを特定してブロックし、潜在的な侵害からネットワークを保護することで、スパイウェア、SQL インジェクション、クロスサイトスクリプティングなどのネットワーク攻撃からリアルタイムで保護します。



アプリケーション制御

デバイス上で実行可能なアプリケーションをきめ細かく制御することで、不正なソフトウェアの実行や潜在的な侵害を防止し、ネットワークセキュリティを強化します。



WebBlocker

悪意のある Web サイトや不適切なコンテンツを防御することで、ネットワークの安全を守り、組織のセキュアで生産的なオンライン環境の維持に貢献します。



Gateway AntiVirus

送受信トラフィックにウイルス、マルウェア、その他の脅威がないかスキャンし、サイバー攻撃に対する包括的な保護を提供することで、機密データを保護し、ビジネスの継続性を確保します。



APT Blocker

AI と機械学習を活用して、高度な持続的脅威 (APT)、ゼロデイエクスプロイト、ランサムウェアなどの巧妙なサイバー脅威を特定し、ブロックします。



DNSWatch

クラウドベースの DNS セキュリティサービスを通じて、高度な脅威インテリジェンス、リアルタイム防御、DNS フィルタリングを提供し、ネットワークとユーザーを保護します。



WatchGuard Cloud

単一のインターフェイスから合理化された可視化、制御、リアルタイムの脅威モニタリング、ログとレポートデータの保持を実現し、ネットワークセキュリティ管理の簡素化、時間の節約を可能にし、一元管理プラットフォームを通じて情報に基づいた意思決定を支援します。

Fireboxのセキュリティ機能をリモートワーカーに拡大



ファイアウォール・アズ・ア・サービス (FWaaS)

- DNS フィルタリング
- ボットネット検知
- 侵入防止 (IPS)
- APT Blocker
- クラウドサンドボックス
- TLSインスペクション
- ジオロケーション防御
- Gateway AntiVirus (GAV)

セキュリティWebゲートウェイ(SWG)

- WebBlocker URLフィルタリング
- アプリケーション制御

ユーザー認証

- 接続マネージャ
- アイデンティティプロバイダ (IdP)

管理サービス

- 共通ポリシー／設定
- 容易な設定ウィザード
- IdP向けSAML連携またはローカルアカウント設定
- 一元プラットフォーム: ネットセキュリティ、アイデンティティ、エンドポイント