

Forcepoint ONE Web Security

データ損失やマルウェア攻撃を防ぎ、生産性を維持

ユースケース

- ▶ 従業員にWebへの迅速かつ安全なアクセスを提供
- ▶ 許容可能な使用ポリシーを適用
- ▶ 認可されていないWebサイトへの機密データのアップロードをブロック
- ▶ ユーザビリティを損なうことなく、マルウェアがユーザーデバイスに侵入するのを防止
- ▶ シャドーITの発見と管理
- ▶ ユーザーのプライベートデータが企業にさらされるのを防止

ソリューション

- ▶ 統合DLPと高度な脅威対策を備えた高速なWebセキュリティ
- ▶ ユーザーグループ、デバイスタイプ、ユーザーの場所、Webサイトカテゴリ、Webサイトのリスクスコアなどに基づいて粒度の細かいZero Trustアクセスとデータ制御を実施
- ▶ 分散アーキテクチャにより、高稼働率プラットフォーム上のボトルネックを排除
- ▶ 内蔵のRemote Browser Isolation (RBI) が、分類されていないサイトや新たに登録されたサイトでの安全な閲覧と、これらのサイトからの安全なダウンロードを確保

結果

- ▶ 生産性を向上させ、あらゆる場所からのシームレスかつ安全なWebの閲覧を実現
- ▶ クラウド内の機密データの制御とマルウェアの阻止によりリスクを低減
- ▶ セキュリティ運用を簡素化することでコストを削減

Webには良い面も悪い面もあります。ほとんどの人は、仕事をする上で情報を得るためにWebに依存していますが、Webは、データの流出、人事ポリシー違反、生産性の低下、マルウェア感染などのリスクを生じさせる場所でもあります。GenAIによりこの危険性はさらに増えています。生産性の大幅な向上を確保できる一方で、組織をより多くのリスクにさらすからです。しかし、適切なガードレールがあれば、AIで得られる生産性の向上のメリットを活用しながら、同時に機密データを安全に保ち、適切な使用を確保することができます。データと人員の安全を保つことができなかった場合の影響が日増しに大きくなる中、Web上でのインタラクションの保護は、現代の組織にとって戦略的な要件となります。

従業員にWebへの迅速かつ安全なアクセスを提供

ほとんどの最新のWebセキュリティソリューションは、オンプレミスまたはクラウドのいずれであれ、一元化されたデータセンターを経由するように、すべてのWebトラフィックのルートを強制的に切り替えるため、遅延が発生し、最新のWebアプリケーションにとっては大幅の干渉となります。クラウドアーキテクチャは、必要に応じてスケールアップ・拡張するように設計されていますが、多くのSWGベンダーには、この非常に高度に分散化されたクラウドプレゼンスが欠けています。これとは対照的に、Forcepoint ONEは分散アーキテクチャであり、世界中に300以上のポイントオブプレゼンス (PoP) を持つ非常に復旧性の高いクラウドアーキテクチャを提供するだけでなく、顧客にさらなる柔軟性を提供する代替オプションも用意されています。デバイス上のエージェントは、混雑するPoPを解消し、パフォーマンスに左右されるWebコンテンツやアプリケーションにおいて、競合他社のSecure Web Gatewayに比べて最大2倍のスループットを提供できます。このオプションは、ユーザーのデバイス上でローカルにセキュリティポリシーを適用し、ユーザーとWebサイト間でトラフィックを直接交換できるようにします。

リスクの高いWebサイトで許容可能な使用ポリシー (AUP) 制御を実施

Webは気を散らす場所になることもあり、会社のビジネスのために常に使用されるとは限りません。Forcepoint ONEのWeb制御では、ブロック、確認ページの使用、クォータ時間の使用、多要素認証のプロンプト、許可を実行でき、RBIを使用してトラフィックを分離することも可能です。ユーザーグループ、デバイスのセキュリティ姿勢、場所に基づいてアクセスを管理できます。これにより、組織はシャドーITによるGenAIサイトの利用をブロックするための制御を簡単に実施できます。例えば、企業が認可したリソースに誘導するブロックページを使用したコードを生成したり、他のタイプのAIサイトを識別するための粒度の細かい設定を行い、会話やマルチメディアを生成するAIサイトへのアクセスを許可しつつ、それらのサイトに投稿できるデータに関するガードレールを適用することができます。

認可されていないWebサイトへの機密データのアップロードをブロック

当社のセキュリティエンジンにより、規制されたデータや知的財産が個人ファイルストレージ、ソーシャルメディア、個人の電子メールアカウント、またはGenAIサイトに送信されることを防ぐことができます。使いやすいコントロールを使用して、機密データのファイルへのアップロードやテキスト投稿をスキャンしてブロックすることができます。オプションで、お客様はForcepoint ONE Data Securityから高度なDLPポリシーを継承し、業界をリードする高度なデータセキュリティソリューションで拡張することができます。

ユーザビリティを損なうことなく、マルウェアがユーザーデバイスに侵入するのを防止

Forcepoint ONE Web Securityサービスは、Webサイトのカテゴリブロック、ダウンロードされたファイルのインラインスキャン、Remote Browser IsolationなどのZero Trustベースの高度な脅威対策など、Webを媒介とするマルウェアに対する複数の保護手段を提供します。Forcepoint RBIにより、汚染されたサイトやダウンロードされたファイルも、安全かつ効率的に使用できます。

シャドーITの発見と管理

Web Security Serviceは、推奨される企業アプリケーションの代わりに使用されるWebサイトを識別するために動作します。これらの「シャドーIT」サイトは自動的に収集され、Cloud Appsダッシュボードに表示されます。

ユーザーのプライベートデータが企業にさらされるのを防止

従業員のプライバシーを保護するために、組織は銀行、医療、保険データなど、個人識別情報 (PII) とともに使用されることの多い特定のWebサイトで送受信されるトラフィックの復号化と検査を防ぐことができます。

Forcepoint ONE Web Securityが稼働時間、生産性、パフォーマンスを最大化

Web Security Serviceは、300を超えるポイントオブプレゼンス (PoP)、グローバルなアクセス可能性、99.999%の稼働率が実証された、当社の高度なクラウドプラットフォームであるForcepoint ONEの一部であり、Webアクセスを保護し、ユーザーの生産性を維持します。Forcepoint ONEにはCASB、SWG、ZTNAが統合されており、企業SaaS、Web、プライベートアプリケーションへのアクセスを保護し、セキュリティを簡素化します。

現実世界のWebセキュリティを簡素化

Forcepoint ONEクラウドプラットフォームは、クラウドセキュリティを実装するための「簡単なボタン」を提供します。管理者は、1つのコンソールから、Forcepoint RBIを使用してZero TrustのWebアクセスを適用するなど、あらゆるサイトでのファイルのダウンロードとアップロードをリアルタイムで管理できます。



在宅勤務をしているビジネスアナリストのクリスが仕事を始めるときに、Web Security Serviceがどのようにすべてを簡素化するか見てみましょう。

クリスは、会社関連調査のためにreddit.comを参照します。	クリスはreddit.com/r/technologyを訪問し、マルウェアに関する最近の投稿を調査します。SWGコンテンツポリシーはディレクトリのレベルで詳細に設定することができます。このReddit内のスレッドは仕事に関連しているとみなされ、クリスはアクセスできるようになります。
r/technologyのスレッド内で、クリスは誤って不適切なページへのリンクをクリックしました。	クリスのForcepoint ONE管理者は、r/technologyなどのディレクトリへのアクセスを許可するSWGコンテンツポリシーを作成していますが、不適切なReddit内のスレッドやページへのアクセスはブロックしています。SWGによってクリスのエラーは防止され、新しいページはブロックされます。
クリスは会社のラップトップ上で、顧客PIIが含まれる機密性のあるスプレッドシートで作業を開始しましたが、個人のラップトップ上で作業を続けたいと考えました。そこで、ファイルを個人のクラウドストレージにアップロードし、個人のラップトップにダウンロードしようとした。	ビジネスデータの損失を防ぐために、同社のForcepoint ONE管理者は、機密顧客情報 (PII) の個人的なファイル共有WebサイトへのアップロードをブロックするSWGコンテンツポリシーを作成しています。クリスのアップロードの試みはブロックされ、アップロードがブロックされた理由を説明するメッセージがポップアップ表示されます。

Web、クラウド、プライベートアプリケーション向けの統合セキュリティソリューションの一部

Webセキュリティに加えて、Forcepoint ONEクラウドセキュリティプラットフォームは、あらゆる企業SaaSテナントとプライベートアプリケーションのビジネス情報へのアクセスを保護します。

- **クラウド (SaaSおよびIaaS):** CASBは、インターネット接続されたデバイス上の最新のブラウザから、SAML2とサードパーティIDプロバイダ (IDP) との統合をサポートするパブリックWebアプリケーションに、コンテキストに応じたアクセス制御、Data Loss Prevention (DLP)、およびマルウェア保護を適用します。よく利用されるIaaSやSaaS内にある保存データも、機密データやマルウェアがないかスキャンして、修復することができます。Forcepoint ONE Data Securityと統合し、SSEチャネルを通じて高度なDLPポリシーを適用します。
- **プライベートアプリケーション:** ZTNAは、VPNに関連する複雑さやリスクなしに、プライベートアプリケーションへのアクセスを保護し、簡素化します。他のForcepoint ONEソリューションと同様に、ZTNAは、コンテキストに応じたアクセス制御、DLP、マルウェア保護をすべてのプライベートWebアプリケーションに適用します。
- **追加機能:** CDRでRBIの基本レベルを拡大し、未知のサイトや新たに登録されたサイト以外もカバーするようにしてWeb脅威からの完全な保護を実現したり、Advanced Malware Detection and Protectionを追加して、エンタープライズクラスのマルウェアサンドボックス化と分析を実現することができます。

詳細については、Forcepoint ONEソリューション概要をご覧ください。



あらゆるデバイスからクラウドアプリケーション内のデータを保護する準備はできましたか？

デモから始めましょう。

forcepoint.com/contact