Forcepoint ONE

Web Security データシート

主な利点:

- 99.999%の稼働率SLA
- 300以上の拠点と分散SWGアーキテクチャによるスマートなステアリングとにより、レイテンシを最小限に抑え、スループットを最大化
- 複数のリアルタイムコンテンツエンジンで、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、コンテクストプロファイル、ファイル、実行可能ファイルを分析し、究極の保護を実現
- SCIMプロビジョニングにより、ユーザーのオンボーディングが加速
- 移動中データのスキャンにより、ユーザーの場所に関係なく、ユーザーとWebアプリケーション間のマルウェアやデータ流出をブロック
- CDRを備えたRBIにより、不明なWebサイトと、これらのWebサイトからダウンロードしたファイルを安全に使用可能
- WebサイトへのアクセスをURLディレクトリレベルまで制御
- ユーザーがSWG機能を迂回または無効化するのを阻止

Forcepoint ONE Web Securityは、生成AIサイトのような新たなテクノロジーに対する詳細な制御を含め、あらゆるWebサイトの使用に対してガードレールを提供します。企業ポリシーの適用を簡素化し、生産性を向上させて新技術を活用しながら、機密データの露出やマルウェアからのリスクを軽減します。

Forcepoint ONE Web Securityアーキテクチャ

Forcepoint ONEは分散型施行アーキテクチャを使用しているため、組織は変化するビジネス要件を満たすために柔軟に対応できます。Forcepoint ONE Web Securityでは、サイトや支店向けのクラウドベースのフォワードプロキシ、または管理対象デバイス向けの独自のエージェントベースプロキシのいずれかを使用してポリシーを適用することができます。クラウドベースのプロキシにより、組織は、ゲストや管理対象外デバイスを使用するユーザーを含めたサイトのすべてのユーザー、そして管理対象デバイスを使用するリモートユーザーに対して、Zero Trust Web Accessを提供することができます。各拠点では、GREまたはIPSECトンネルを使用してクラウド内のForcepoint ONE Web Securityプラットフォームにwebトラフィックを転送することができ、拠点でForcepoint FlexEdge Secure SD-WANを使用している場合は、「EasyConnect」を使用してサイトをForcepoint ONEクラウドプラットフォームに自動的に接続することができます。ポリシーマネージャーにより、サイト全体で使用できるネットワークごとのポリシーを簡単に適用できます。たとえば、組織は、Zero Trust Web Access向けのオプションのForcepoint RBIサービスを使用してゲストのインターネットアクセスが隔離されるように設定し、このゲスト用WI-FIポリシーをすべての場所に簡単に適用することができます。このオプションは、公共または顧客向けWI-FIにアクセスできる支店やサイトに最適です。Forcepointは、エージェントベースのWebセキュリティを使用して、管理対象デバイスを利用するリモートワーカーにも理想的なソリューションを提供します。

エージェントベースのWebセキュリティでは、PACファイルを使用してトラフィックをクラウドプロキシに誘導したり、Webパフォーマンスを可能な限り向上させるためにローカルにポリシーを適用したりすることができます。エージェントベースの適用により、ユーザーと会社のデータは、ユーザーが自宅、現場、オフィスのどこにいるのであれ、安全に保護されます。設計上、Web Securityエージェントは Forcepoint ONEテナント管理者の承認なしに、ユーザーが停止またはアンインストールすることはできないため、ユーザーがこの機能を回避するのは容易ではありません。

Forcepoint ONEの分散アーキテクチャは、主要な人口密集地で300以上のPOP（Point of Presence）を提供します。これは、デバイス上のエージェントがForcepoint ONEバックプレーンと通信する必要がある場合、またはサイトトラフィックがクラウドプロキシに誘導される場合に、世界中で低遅延が得られることを意味します。第二に、エージェントベースのWebセキュリティはデバイス上から実行することができます。つまり、図1に示すように、エージェントベースのWebセキュリティを使用する場合、Forcepoint ONEバックプレーンを通過する必要があるトラフィックはほぼなくなります。

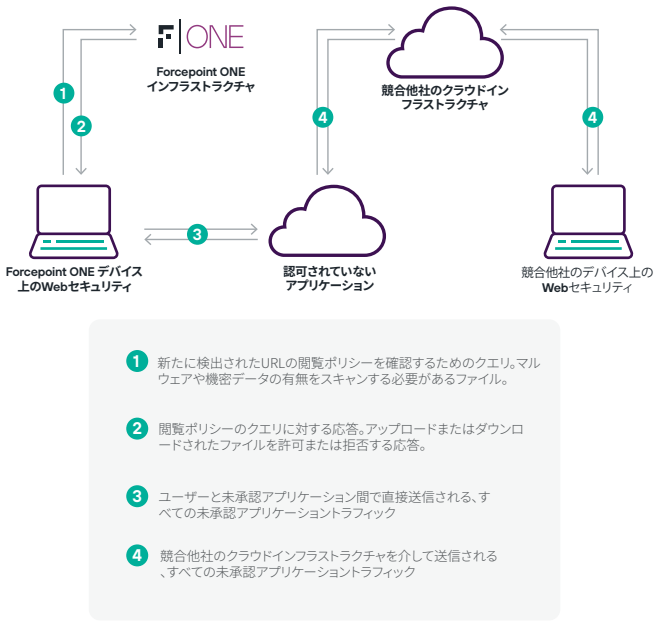

図1: Forcepoint ONE Web Securityトラフィックのルーティングと競合他社の比較

図に示すように、左側にあるForcepoint ONEオンデバイスWebセキュリティは、最近アクセスしていないWebサイトにアクセスして、アクセス制限を決定する場合と、マルウェアや機密データがないかスキャンする必要があるファイルやその他のデータをアップロードまたはダウンロードするの場合の2つの状況では、Forcepoint ONEバックプレーンとのみ通信する必要があります:

これと比較して、右側にある他のベンダーのオンデバイスSWGでは、トラフィックを検査し転送するために、すべてのWebトラフィックをベンダーのクラウドバックプレーン経由で送信する必要があります。このように、すべてのWebトラフィックが他のベンダーのクラウドインフラストラクチャ経由でルーティングされると、最大50%の有効スループットが失われるため、低帯域幅の地域にいるユーザーに生産性上の問題が発生します。ほとんどのユーザーにとって、ファイルのアップロードとダウンロードはインターネットトラフィック全体からみるとほんの一部にすぎないため、Forcepoint ONE Web Securityは通常、利用可能なインターネット帯域幅全体の約95%のスループットをサポートしながら、遅延を削減し、より多くのユーザーをサポートすることができます。

Forcepoint ONE Web Securityの機能

詳細なコンテンツカテゴリとポリシーオプション

リアルタイムでカテゴリ別に分類するため、すべてのWebトラフィックを非常に詳細なWebカテゴリごとに簡単に管理することができます。たとえば、すべてのGenAIサイトを同じように扱うのではなく、複数のカテゴリに分けることで、コードを生成するためのサイトへのアクセスを制限しながら、画像や会話を生成するためのサイトへのアクセスを増やすことができます。それと同時に、機密データを安全に保つためのガードレールを適用することができます。

リアルタイムスキャン

Forcepoint ONE Web Securityは、パフォーマンスを犠牲にせずに、トラフィックコンテンツをリアルタイムで検査し、非常に効率的かつ正確にWebコンテンツを分類およびスキャンします。これにより、組織は業界トップの脅威対策や使いやすいデータセキュリティなど、ニーズに合わせてWebアクセスと使用制御を簡単に適用できます。新しいWebコンテンツが検出されると、セキュリティスキャンエンジンがMLを活用してゼロデイ脅威を特定し、アクセスをブロックします。Forcepoint ONE Web Securityは、高い評価を得ているDNSチェックやIPだけにとどまらず、既知のマルウェアと同じ様に新規マルウェアからの効果的な保護も提供することで、リアルタイムでリスクを軽減し、あらゆる場所にいるユーザーに確実に高速なパフォーマンスを提供します。

コンテンツ検査（DLPとマルウェア）

Forcepoint ONE Web Securityは、暗号化されたWebトラフィックを検査し、当社のデータ検査および分類エンジンを使用して機密データの損失をブロックします。複雑な設定をすることなくPCI、PHI、PII制御をすぐに適用して、ボタンをクリックするだけでパスワード情報や暗号化されたファイルを制御することができます。管理者は必要に応じて、カスタムパターン、フレーズ、辞書、正規表現を作成することもできます。さらに、Forcepoint ONE Data Securityと統合させることで、高度なDLPポリシーをForcepoint ONE Web Securityに直接継承できます。

RBIの要点

今日では、新しいツールや新しいサイトにアクセスして業務をおこなう必要があることが多々ありますが、このようなアクセス先が信頼できないWebの部分となることが多くなっています。このような場所でこそ、Webアクセスに対するゼロトラストアプローチが必要となります。Forcepoint ONE Web Securityには、脅威をホストしている可能性のある「未知の」サイトや新しく登録されたサイトへの安全なアクセスを可能にする、最低限レベルのRemote Browser Isolation（RBI、リモートブラウザ分離）が付属しています。RBIは、隔離された安全なクラウド環境でWebトラフィックをレンダリングし、セッションはエンドユーザーにストリーミングされるため、Webページ上のものがユーザーのデバイスに触れることはなく、セッションの終了時にブラウザとそれをホスティングするvmは単純に削除されます。

分析ダッシュボード

Web生産性ダッシュボードには、リクエストされた上位カテゴリ、リクエスト別になった上位フィルタリングアクション、ブロックされたリクエストの上位グループ、ブロックされたリクエストの上位ユーザー、上位ソーシャルWebチャンネル、および上位ソーシャルWebアクティビティなど、Webトラフィックデータがグラフで表示されます。脅威ダッシュボードは、セキュリティイベント、脅威タイプ、送信元と送信先別になったセキュリティリスクがあるエリア、上位セキュリティリスクのあるサイトが表示され、帯域幅ダッシュボードには、Webカテゴリ別になった帯域幅使用状況、上位接続IP、上位ループ、サイト、上位ユーザーが表示されます。

クラウドアプリケーションダッシュボードは、クラウドアプリケーションの使用状況と関連するリスクに関する情報が表示されます。これには、リスクレベル別にランク付けされ、クラウドアプリケーション、帯域幅、またはユーザー別にリストされたクラウドアプリケーションの表示が含まれます。その他のグラフには、ヒット数および帯域幅別になった上位クラウドアプリケーション、カテゴリ別の上位クラウドアプリケーション、リスクレベル別の上位クラウドアプリケーション、上位クラウドアプリケーションユーザー、およびカテゴリ別のクラウドアプリケーションアクティビティなどが表示されます。帯域幅ダッシュボードには、Webカテゴリ、接続IP、上位グループ、ユーザー、サイトごとの帯域幅使用状況が表示されます。また、Data Securityダッシュボードには、コンテンツタイプ、ソースおよび重要度、上位ドメイン、Webカテゴリ別になった、DLPインシデントが経時的に表示されます。

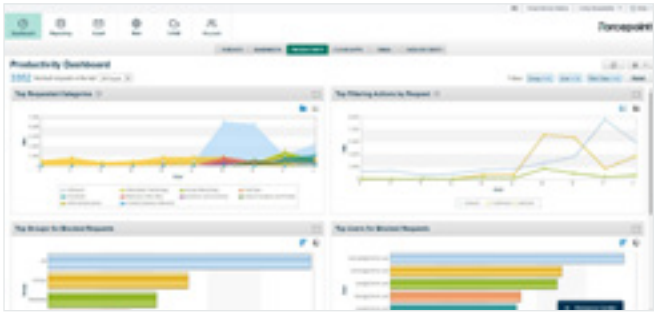

図2：生産性ダッシュボード

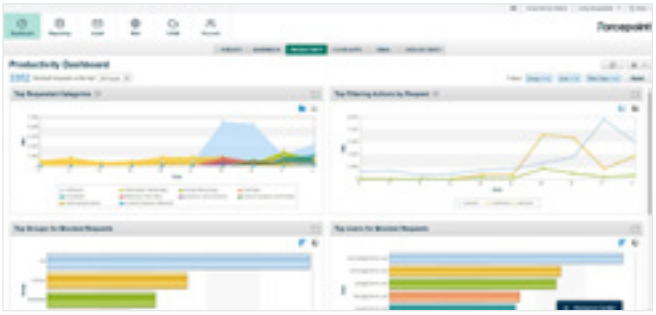

図3：脅威ダッシュボード

Webセキュリティ迂回を防止

ユーザーは、Forcepoint ONEテナント管理者に要請しない限り、WindowsまたはMacOSデバイス上のWebセキュリティプロセスを強制終了させたり、Web Securityを搭載したデバイス上のエージェントをアンインストールしたりすることはできません。

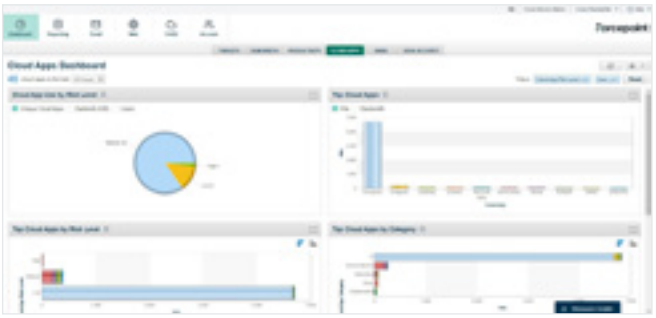

図4：クラウドアプリケーションダッシュボード

Forcepoint ONE Web Securityの機能と利点

機能		利点
Web制御機能		
粒度の細かいWebアクセス制御	→	企業Webおよびクラウドアプリケーションの使用を細かく制御可能
粒度の細かいソーシャルメディア制御	→	ソーシャルメディアの使用を制限し、メール、ゲーム、チャット、投稿、写真のアップロードなどのセクションを区別します
接続に基づくポリシーの切り替え/コンテキスト認識型のポリシー切り替え	→	ユーザーの接続方法と接続場所に基づいてポリシーを自動的に調整
生産性制御/クオータ	→	営業時間内にあらゆるWebカテゴリに対してクォータを実施し生産性を維持
シングルサインオン	→	OktaやPing IdentityなどのSSOプロバイダと統合し、より強力なIDベースのアクセス制御を実施
データ保護機能		
クラウドアプリケーションの可視化	→	クラウドアプリケーションダッシュボードは、企業全体で使用されているすべての認可済みおよび未認可のクラウドアプリケーションを可視化します。
認可されていないクラウドアプリケーションのブロック	→	Webアクセス制御を使用して、未認可のクラウドアプリケーションへのアクセスを制限します。
基準コンプライアンスDLP	→	PII、PHI、PCI、パスワードファイル、カスタム暗号化ファイルなどの機密情報がWebチャネルを介して送信されないように保護します（オンプレミスおよびハイブリッドの場合は、Web DLPモジュールを介して提供されるか、フルDLPスイートに統合されています）。
Forcepoint ONE Data Securityを統合	→	高度なデータ分類子とDLPポリシーを継承し、ボタンをクリックするだけでWebチャネルで使用できます
脅威防止機能		
プロキシ（SSL）	→	すべてのWebトラフィックのインライン検査でセキュリティ有効性を最大化
リアルタイムでセキュリティを分類	→	多くの種類の分析を採用し、動的コンテンツの背後に隠れている悪意のあるコードを識別します
リアルタイムでコンテンツを分類	→	あらゆるWebページのWebコンテンツを130種類以上のカテゴリに分類し、粒度の細かいアクセスフィルタリングを実現
アンチウイルス、アンチマルウェア	→	最新のバイナリおよびスクリプトベースの脅威を事前にブロックする最先端のマルウェア保護を適用
ヒューリスティック分析	→	以前に遭遇したことのないマルウェアを識別し、保護します
評判分析	→	評判データベースは、トラフィックが信頼できないサイトにリダイレクトされるのを防ぎます
URLデータベース	→	既知のURLを分類し、関連付けられたサイトとリダイレクトに基づいて新しいURLを評価
行動ファイルサンドボックス	→	高度なマルウェア検知が究極のセキュリティレイヤーを追加し、ファイルに巧妙に隠されたゼロデイ脅威に対する保護を確保
Remote Browser Isolation	→	ソリューションがブロックすべきリスクの高いサイトを検出した場合でも、業務上アクセスを許可する必要がある場合は、リスクの高いセッションをRemote Browser Isolation経由で処理し、アクセスを許可しながらセキュリティを確保します
ファイルタイプによるブロック（受信）	→	ポリシー内のファイルタイプに基づいて受信ファイルをブロックできます
クラウドアプリケーションリスクデータベース	→	企業全体で使用されているクラウドアプリケーションのリスクレベルを特定
ThreatSeeker Global Threat Intelligence	→	世界中に展開されているForcepoint製品から脅威情報を集約し、脅威のテレメトリをすべてのForcepointセキュリティソリューションに提供