Forcepoint

ソリューション概要

Cloud Access Security Broker

あらゆるデバイスからアクセスできる、あらゆるクラウド アプリの安全なデータ

課題

- BYODから管理対象アプリケーションへのアクセスを保護し、制御
- 管理対象SaaSアプリケーションにおける機密データのアップロードとダウンロードを制御
- ビジネスデータファイルに隠されたマルウェアを阻止
- シャドーITの検出と管理

ソリューション

- 統合DLPと高度な脅威に対する保護によるSaaSアプリケーションのセキュリティ
- ユーザー、デバイス、場所に基づいた細かな**Zero Trust**アクセスとデータ制御
- ハイパースケーリング**AWS**プラットフォームが稼働時間を最大化し、遅延を最小化
- 管理対象デバイスと管理対象外のデバイスに**DLP**を適用

結果

- 生産性を向上させ、あらゆる場所で情報をシームレスに安全に利用
- 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
- 一ヶ所でポリシー設定を実施し、セキュリティオペレーションを簡素化することでコストを削減
- 情報を制御するための実証可能なプロセスでコンプライアンスを合理化

今日の新しい労働力モデルでは、ユーザーの場所にかかわらず、あらゆる場所にあるビジネスデータに高速かつ管理されたアクセスができることが求められます。つまり、あらゆる種類のデバイスや場所からMicrosoft 365、Google Workspace、Slack、Jira、SalesforceなどのSaaSアプリケーションのデータにアクセスする必要があるということです。平均的な企業では、250以上のSaaSアプリケーションが利用されているため、可視性の確保と管理が容易に手に負えなくなります。

BYODや管理対象外のデバイスからビジネスアプリケーションへのアクセスを保護

Forcepointはクラウドセキュリティを簡素化します。Forcepoint ONEのCASBセキュリティサービスは、ゼロトラストアクセスを実装し、ビジネスに不可欠なSaaSアプリケーションを従業員のパーソナルデバイス（BYOD）やパートナーや請負業者の管理されていないデバイスから安全に使用できるようにします。

管理対象SaaSアプリケーションにおける機密データのアップロードとダウンロードを制御

機密データを制御するために1つのセキュリティポリシーセットを提供し、従業員や請負業者がインターネットに接続する場所や方法に関係なく、業界最高のパフォーマンスを発揮します。識別子と場所に基づいて異なるポリシーを持つことで、きめ細かなZero Trust制御が可能です。モバイルデバイスからのこれらのアプリへのアクセスを管理することで、導入と生産性が向上します。機密データとマルウェアのインラインスキャンにより、すべてのSaaSアプリケーションでデータを安全に保ちます。企業アプリ内での機密データの共有方法をより確実に把握できます。また、組み込まれたData Loss Prevention (DLP)機能により、データ漏えいを阻止するためのポイント製品を必要としません。

ビジネスデータファイルに隠されたマルウェアを阻止

Forcepoint ONE CASBは、複数のサードパーティ製のマルウェア対策エンジンを使用して、ユーザーとSaaSアプリケーション間で使用中のデータに含まれるマルウェアを検出しブロックすることができます。また、一般的なSaaSおよびIaaSストレージ内のファイル内のマルウェアを検出して、それらのファイルを隔離することもできます。

シャドーITの検出と管理

Forcepoint ONE CASBはシャドーITを可視化し、複数の属性を分析することで、未承認のアプリケーションのリスクスコアを生成します。これにより、ITチームは組織内でのSaaSの使用状況をより深く理解し、必要なセキュリティ管理を実施することができます。CASBは、企業ファイアウォールやプロキシのネットワークログを使用して、使用中の管理されていないSaaSアプリケーションを検出し、承認済みおよび未承認のSaaSアプリケーションに一貫したセキュリティポリシーを適用し、ビジネスデータが使用される場所を問わず安全性を確保します。

稼働時間、可用性、生産性を最大限に高めるSaaSセキュリティソリューション

当社のCASBは、300以上のポイントプレゼンス（PoP）、グローバルなアクセス性、実証済みの99.99%の稼働率を備えたクラウドネイティブのハイパースケーラベースのアーキテクチャ上に構築されており、SaaSアプリケーションをシームレスに保護し、ユーザーの生産性を維持します。その他のソリューションは、ユーザーやユーザーがアクセスしているアプリケーションに近い場所ではなく、SaaSアプリケ ケーション間のネットワークトラフィックをプライベートデータセンターに迂回します。その結果、パフォーマンスの低下につながり、Slackのような遅延に敏感なアプリケーションが機能せず、従業員が高リスクの回避策を求める原因となります。

あらゆる場所で仕事をする人のため、
あらゆる場所でデータを保護

現実世界のクラウドセキュリティをシンプルに

管理者は、管理対象デバイスと非管理対象デバイス（BYODや請負業者、パートナーのコンピューターなど）のユーザーのアクセスと制御データを1つのコンソールから管理できます。

在宅勤務のビジネスアナリストであるクリス氏が勤務開始日を迎えたとき、CASBがクラウドセキュリティを簡単に実装する方法をご覧ください。

クリスは、企業が提供するラップトップからSalesforceアカウントにログインします。	Forcepoint ONEのCASBは、ビジネスアプリケーションへの接続を管理し、ユーザーはシームレスかつ安全にログオンできます。
クリスは、salesforce.comに直接アクセスするか、企業アプリケーションポータルを通じて閲覧します。	SalesforceはセッションをCASB（SAML経由）にリダイレクトし、デバイスの管理状況、位置、セキュリティ体制を分析します。CASBは、事前定義されたセキュリティポリシーに基づき、多要素認証によりクリスのアイデンティティを確認します。
クリスは管理対象アプリケーションアクセスを許可されます。	管理者ポリシーは、アプリケーションへの直接アクセス、制御されたアクセス、アクセス拒否も制御します。これはミリ秒単位で行われるため、従業員の生産性に影響を与えません。クリスのデバイスとアプリケーションからのすべてのトラフィックはCASBを通過します（リバースプロキシまたはフォワードプロキシを使用します）。
クリスは、Salesforce　ら収益予測をダウンロードすることにしました。	CASBは、アプリケーションからダウンロードしたファイルをスキャンし、マルウェアや機密データの検出を行います。結果とポリシーに応じて、マルウェアファイルをブロックし、機密データをブロック、追跡、または暗号化することができます。ポリシーが管理対象外のデバイスへの機密データのダウンロードを制限している場合、クリスは会社のラップトップを使用しているため、ダウンロードは許可されます。
機密データやマルウェアに汚染されたファイルを、クリスはSlack経由で転送しようとします。	CASBは、SaaSアプリケーションにアップロード中のファイルをチェックすることもできます。CASBはアップロードを自動的にブロックします。デバイス統合エージェントを使用することで未承認のアプリケーションへのファイルのアップロードをブロックすることもできます。

ForcepointのData Security Everywhereアプローチの一環

Forcepointの「Data Security Everywhere」ミッションは、組織がSaaS、Web、電子メール、ネットワーク、エンドポイント全体でデータを保護し、従業員は働く場所にかかわらず、あらゆる場所のデータにアクセスして安全に作業できるようになります。

業界をリードするDLP機能をSaaSアプリケーションに拡張

Forcepointでは、組織は既存のForcepoint DLPポリシーを活用してSaaSアプリケーションのデータを保護し、わずか数クリックで業界をリードするデータセキュリティをクラウドに拡張することができます。単一のコンソールから適用される統合DLPポリシーは、SaaSアプリケーションに一貫したエンタープライズクラスのデータセキュリティを提供し、データセキュリティ管理を簡素化し、侵害を最小限に抑え、コンプライアンスを効率化するのに役立ちます。この統合により、お客様は次のメリットを得ることができます。

→ 統合ポリシーとコンソールによる簡素化されたクラウドデータセキュリティ。

→ 150以上の地域を包括的にカバーしコンプライアンスをサポートするための、すぐに使える1,700の分類子とポリシーテンプレート。

→ 構成設定と価値を創造するまでの時間が数分で完了し、IT/セキュリティチームの生産性を向上。

→ 冗長で断片化されたセキュリティ製品を排除することで、大幅なコスト削減を実現。

詳細については、Forcepoint DLPパンフレットをご覧ください。

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

[FP-Forcepoint ONE CASB-Solution-Brief-JA] 09Dec2024