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

ソリューション

- 統合DLPと高度な脅威対策を備えたクラウドアプリケーションセキュリティ
- 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できるようにします
- 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

今日の新しいワークモデルでは、ユーザーがどこにいても、どこからでもビジネス データに高速かつ制御されたアクセスができることを求めています。つまり、ユーザーは Microsoft 365、Google Workspace、Slack、Jira、Salesforce などのクラウド アプリのデータに、あらゆるデバイスや場所からアクセスできる必要があります。平均的な企業で 250 を超える SaaS アプリが存在すると、可視性と制御が簡単に管理不能になる可能性があります。

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、Zero Trustアクセスを実装しており、基幹業務にかかわるクラウドアプリケーションを従業員の個人デバイス（BYOD）やパートナーや請負業者の管理対象外デバイスから安全に利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、BitdefenderとTrellixのマルウェアエンジンを使用して、ユーザーとSaaSアプリ間で移動中のデータ中のマルウェアを検出し阻止します。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

Forcepoint ONE CASBはシャドーITを明るみに出し、複数の属性を分析することで、認可されていない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使用状況をより深く理解し、必要なセキュリティ制御を実施することができます。CASBは、Forcepoint ONEセキュアウェブゲートウェイのネットワークログまたはテレメトリを使用して、使用中の管理対象外SaaSアプリケーションを検知します。これにより、SaaSアプリケーションに、その認可状況にかかわらず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に維持します。

Forcepoint ONEのCASBが稼働率、可用性、生産性を最大化

CASBは、300を超えるプレゼンス（PoP）、グローバルアクセス性を備えたハイパースケラーベースのクラウドプラットフォームであるForcepoint ONEの一部です。また、CASBは、クラウドアプリケーションをシームレスに保護しつつ99.99%の稼働率を達成し、ユーザーの生産性を維持しています。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、クラウドアプリ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、パフォーマンスが低下し、遅延に敏感なSlackのよう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

現実世界のクラウドセキュリティをシンプルに

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、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、クラウドアプリケーションにアップロードされている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して、認可されていないアプリケーションへのファイルのアップロードを阻止することもできます。

ウェブ、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

CASBに加えて、Forcepoint ONEオールインワンプラットフォームは、あらゆるウェブサイトやプライベートアプリのビジネス情報へのアクセスを保証します。

- → **ウェブ：** SWGはリスクとカテゴリーに基づき、あらゆるウェブサイトとのやり取りを監視・制御し、マルウェアのダウンロードや個人のファイル共有や電子メールアカウントへの機密データのアップロードを阻止します。オンデバイスSWGは、あらゆる管理対象デバイスで許容可能な使用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に関連する複雑化やリスクなしに、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。
- → **クラウドプロバイダー** のリクスのある設定をスキャンするなどの追加機能、必要に応じて、クラウドセキュリティ対策管理（CSPM）およびSaaSセキュリティ対策管理（SSPM）など。

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