Proofpoint CASB による アダプティブ アクセス コントロール

人それぞれに適したアクセスとデータの管理でクラウドアプリを保護する

課題

- クラウドアカウントの乗っ取り
- クラウドアプリに対する危険なアクセス
- データ損失とコンプライアンス

主な機能

- IDと役割を基にしたアクセス制御で不正アクセスを阻止
- デバイスを基にしたアクセス/データ制御でコンプライアンスリスクを低減
- リアルタイムのデータ漏えい対策で機密ファイルを保護
- クラウドに迅速にデプロイ

製品

- Proofpoint CASB
- Proofpoint SaaS Isolation

クラウドを利用して、リモートから働くことができる分散型の職場環境に移行する企業が急増しています。そしてこのような環境を狙うサイバー攻撃も増加しています。場所や勤務時間が固定されていた従来型のワークスタイルから、よりフレキシブルで柔軟な形態に変わったことで、攻撃の対象もネットワーク境界からユーザー、ユーザーがアクセスするデータ、システム、リソースに変化しています。

このように進化を続ける環境では、クラウドアプリへのアクセスを保護し、データの損失を防ぎ、コンプライアンスを維持することが重要になります。

自宅やリモートで働く従業員は、当然ながら会社のネットワークの中にいるわけではなく会社のネットワークセキュリティでは保護されていません。また、その多くは管理されていないデバイスで仕事をしています。機密データを含むファイルが個人所有のデバイスにダウンロードされる可能性もあります。このため、組織は以前にもましてサイバー攻撃を受けやすい状態になっています。認証情報が盗まれた場合、アカウントが乗っ取られ、データが外部に漏えいする可能性があります。また、ビジネスメール詐欺（BEC）などのフィッシング攻撃を受ける可能性もあります。

こうしたリスクは現実のものであり、重大な被害をもたらします。Proofpoint CASBは、このようなリスクの回避に役立つソリューションです。短時間で導入することができ、Microsoft 365（Office 365）、G Suite、Zoom、Box、Salesforce、Workdayなどを保護できます。

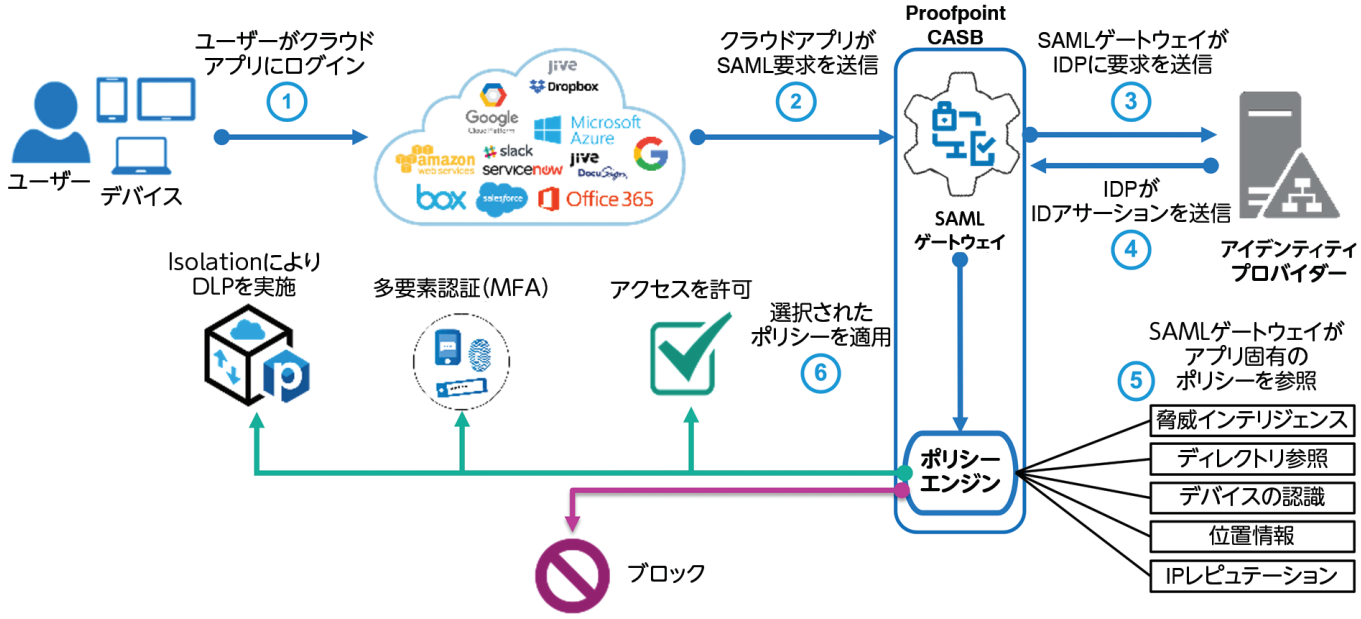

図1：アダプティブアクセスコントロールのアーキテクチャ

PROOFPOINTを選ぶ理由

- 人それぞれに適したPeople-Centricのセキュリティ制御により、サイバー攻撃で狙われやすいユーザーや特権ユーザー、攻撃にひっかかりやすいユーザーなどのVery Attacked People™を可視化
- リスク、コンテキスト、ユーザーの役割に基づくきめ細かいポリシー管理
- 実践で役立つ脅威インテリジェンス（IPレピュテーション、高リスクの不審なログイン）
- 数時間で導入可能なエージェントレスの強固なソリューション

人それぞれに適したセキュリティを施すアダプティブなアクセスコントロールをCASBに実装することにより、リスク、コンテキスト、役割に応じたリアルタイムのセキュリティ対策を実施できます。危険な場所やネットワークからのアクセス、既知の攻撃者からのアクセスは自動的にブロックされます。高度な認証、管理対象デバイスのポリシールール、VPNを介したアクセスなど、ユーザーのリスクや権限に応じてリスクベースの管理を行うことができます。

すべてのユーザーを同じ方法で保護する静的なセキュリティ / コンプライアンス対策と異なり、CASB対応のアクセスコントロールは柔軟な管理が可能です。リスクの低いユーザーに過度な負担をかけることなく、適切な規模のセキュリティ / コンプライアンス管理を行うことができます。

クラウド脅威対策

ユーザーアカウントの認証情報は組織に侵入するための鍵になります。クラウドアカウントの認証情報さえあれば、サイバー犯罪者は組織の内外で攻撃を開始することができます。

人それぞれに適したセキュリティを施すアダプティブアクセスコントロールでは、既知の攻撃者に関する脅威インテリジェンスを使用して、不審なログインをブロックし、アカウントの乗っ取りを防ぎます。CASBではさらに、コンテキストデータを使用してユーザーの身元を確認し、不正アクセスを未然に防ぎます。コンテキストデータとして次の情報を使用します。

- ユーザーの位置情報
- デバイス
- ネットワーク
- ログイン時間

これらのリスク指標を使用してアクセス制御ポリシーを定義することで、会社のアプリケーションへの侵入を防ぐことができます。

よく利用されるポリシー

クラウドベースの脅威を阻止するためによく利用されるCASBポリシーは次のとおりです。

高リスクの不審なログインをブロックする

攻撃者のシグネチャがProofpointに登録されている場合、CASBのアダプティブアクセスコントロールを使用して、危険度の高い不審なログインを防ぐことができます。Proofpointは、数千万のアカウントに対する不審なログインを追跡し、クラウドの脅威がどのようなものかよく理解しています。たとえば、CASBが不審なログインを検出したときに、最も攻撃を受けやすいユーザーアカウントへのアクセスをブロックできます。

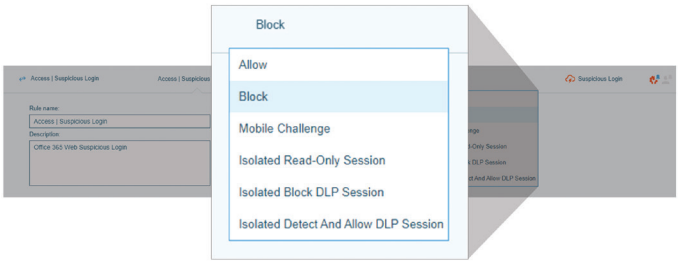

図2：不審なログインをブロックするCASBルールの例

危険な国やネットワークからのアクセスをブロックする

自社の拠点がなく、攻撃元となっている国をブラックリストに追加できます。また、Proofpointから提供されるIPレピュテーションに基づいて、攻撃者が身元を隠すために使用するTor、プロキシ、仮想プライベート ネットワーク（VPN）などの危険なネットワークからのアクセスをブロックしたり、このようなアクセスに対して多要素認証（MFA）を要求できます。

PEOPLE-CENTRICなアクセス

セキュリティとコンプライアンスの要件を満たすには、承認済みアプリと会社のデータに対するアクセスを保護する必要があります。オンサイトの従業員だけが対象ではありません。従業員がリモートからアクセスすることもあります。従業員だけでなく、コントラクターやパートナー、サプライヤーがアクセスすることもあります。クラウドにはどこからでもアクセスできるため、ユーザーの役割と権限、アプリとデータの機密性に応じてポリシーセットを作成しなければなりません。現在では「人」が新しい境界となっています。この境界を保護するには、ユーザーエクスペリエンスを十分に考慮する必要があります。Proofpointを使用すると、Very Attacked People™（VAP）であるユーザー / グループや、価値の高いデータ、システム、リソースに対してアクセス権限を持つユーザー / グループにアダプティブなアクセスコントロールを行うことができます。

VAP（Very Attacked People™）とは?

人に個性があるのと同様、ユーザーがサイバー攻撃者にもたらす価値や雇用主に与えるリスクは人によって異なります。

またデジタル上の習慣や弱点も人によって異なります。ユーザーは多様な手法の、様々なレベルの攻撃の標的となっており、仕事上の連絡先や、データ、システム、リソースへのアクセス権限が狙われています。

ユーザーの全体的なリスクは脆弱性、攻撃、特権という3つのファクターで決まります。

V：Vulnerability（脆弱性）ユーザーが管理対象外のデバイスを使用している場合があります。VPNやZTNAを使用せず、信頼されていないネットワークからアクセスすることもあります。また、フィッシングメールを開いたり、危険なリンクをクリックする可能性もあります。

A:Attack（攻撃）サイバー攻撃で最も狙われるのがユーザーです。ユーザーは無差別な攻撃を受けることもあれば、標的型の攻撃を受けることもあります。

P：Privilege（特権）重要なデータ、システム、リソースへのアクセスは特定のユーザーに限定されていますが、その定義が曖昧になっていることもあります。たとえば、重要な会社のデータに対するアクセス権のないアシスタントに、経営陣宛てのメール、連絡先、予定表の閲覧を許可していることがあります。このような情報はBEC攻撃で有益なデータとなります。

VAPとは、これらの要素の組み合わせでリスクが高くなる人物を意味します。

すべての人がVIPではありませんが、誰もがVAPになる可能性があります。

よく利用されるポリシー

個々のユーザーの脆弱性、攻撃プロフィール、権限に基づいてアクセスを管理するため、次のCASBポリシーがよく利用されています。

VAPにMFAを実施する

危険な状態のユーザーに対するセキュリティを強化できます。たとえば、Proofpointの People-Centric 脅威インテリジェンスでVAPと特定されたユーザーが重要なアプリにアクセスを試みたときに、アクセスをブロックしたり、認証情報を求めることができます。

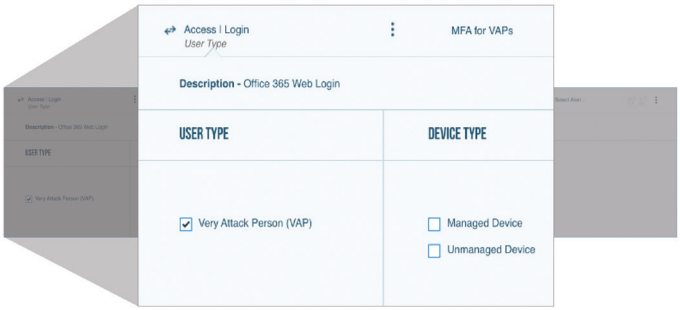

図3：VAPがWebのMicrosoft 365にアクセスする際に使用できるデバイスを制御するCASBポリシールール

重要なアプリの特権ユーザーに仮想プライベート ネットワーク（VPN）経由でのアクセスを強制する

会社のVPNやProofpoint Metaなどのゼロ トラスト ネットワーク アクセス（ZTNA）を使用しない限り、特権ユーザーでも重要なアプリにアクセスできないようにします。自社の企業ネットワークとVPNのIP範囲を定義できます。

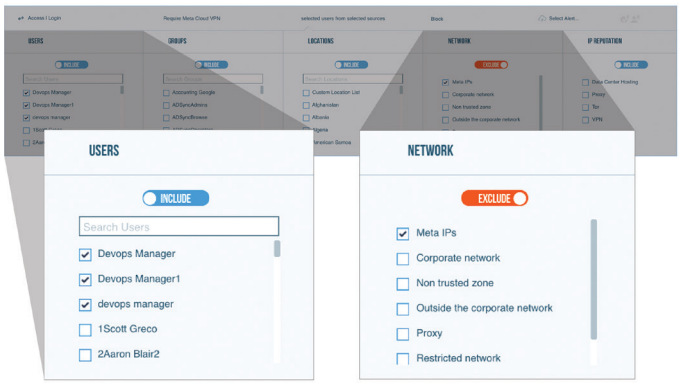

図4：管理者や他の特権ユーザーのリモートアクセスにVPNまたはZTNAを要求するCASBルールの例

デバイスを基にした制御でリアルタイムの情報漏えい対策を実現

管理対象外のデバイスで最大のリスクは、不完全なデバイスセキュリティです。従業員が管理対象外のデバイスから安全でないネットワークを介して会社のデータにアクセスしていると、情報漏えいやデータ消失のリスクが高まります。このような情報へのアクセス、共有、保存に使用されるアプリのセキュリティ対策が万全でなければ、組織の外部に情報が簡単に流出してしまいます。

CASB対応のアダプティブアクセスコントロールを使用すると、使用するデバイスや場所に関係なく、ユーザーはクラウドアプリに安全にアクセスすることができます。CASBでは次のことを行うことができます。

- デバイスの証明書を検出
- デバイスにデータセキュリティポリシーを作成
- Proofpoint SaaS Isolationとの連携でリアルタイムの管理を実施

分離された安全なブラウザー内でアプリケーションを読み取り専用モードで使用することをユーザーに許可できます。また、DLPに違反するファイルのアップロード/ダウンロードを阻止できます。

多くの企業では、従業員が日常的にクラウドで重要なコンテンツを共有しています。クラウド上には従業員や顧客の情報、ソースコード、数式など、さまざまな情報が保存されています。データ侵害やコンプライアンス違反を事前に検知し、防ぐことが重要になります。まず、情報漏えい対策（DLP）スキャンをリアルタイムで実行できる、リスクを考慮したデータセキュリティが必要です。また、重要なコンテンツのクラウドへのアップロード、個人所有デバイスへのダウンロードをブロックする機能も必要です。

よく利用されるポリシー

デバイスを保護するためによく利用されるCASBポリシーは次のとおりです。

信頼できるネットワーク上にない管理対象外のデバイスに読み取り専用アクセスを許可する

従業員が個人所有のデバイスからMicrosoft 365、Salesforce、Atlassianなどの承認済みアプリケーションを利用し、会社のデータにアクセスするようになると、会社のデータに対して新たなリスクが生じます。

個人所有デバイスでデータのダウンロードや同期が行われると、情報は保護された環境外に移動することになります。デバイスが盗まれればデータを失う結果になります。

では、コラボレーションツールにアクセスするデバイスを制限せず、データのダウンロードは会社支給の管理対象デバイスにのみ許可する方法はないのでしょうか。CASBを使用すれば、分離された安全なブラウザセッションに管理対象外のデバイスを誘導し、ファイルのアップロードとダウンロードを許可しないポリシーを簡単に作成できます。

企業ネットワークに接続している場合でも、管理対象外デバイスのDLP違反を防ぐ

データ侵害の半数以上は、攻撃者や悪意ある内部関係者による攻撃で発生しています。ユーザーが企業ネットワークまたはVPNに接続している場合、外部からサイバー攻撃を受けるリスクは低くなります。この場合、管理対象外デバイスで機密データを含まないファイルのダウンロードは許可し、機密情報を含むファイルの転送はブロックするのが良い方法でしょう。

CASBを使用すると、ユーザーを分離されたセッションに誘導し、すべてのファイル転送に企業のDLPポリシーを適用できます。DLP違反が検出されると、転送はブロックされます。

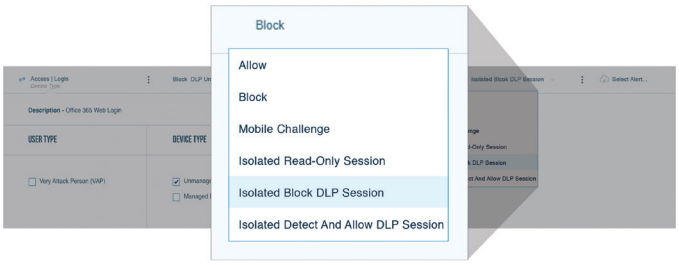

図5：管理対象外のデバイスで機密データのダウンロードをブロックするCASBルールの例

クラウドへの迅速なデプロイ

CASBのアダプティブアクセスコントロールは、クラウドアプリのログインをProofpointのSAMLゲートウェイにリダイレクトします。このゲートウェイは、サービスプロバイダーとアイデンティティプロバイダー間のフェデレーション認証を仲介します。これは、アイデンティティプロバイダーのインラインにデプロイされます。

アプリケーションから見ると、SAMLゲートウェイはアイデンティティプロバイダーのように見えます。実際のアイデンティティプロバイダー（ユーザーディレクトリを保持し、ユーザーのライフライクルを管理しているプロバイダー）から見ると、SAMLはサービスプロバイダーのように見えます。

ユーザーのプロビジョニングやその他のアイデンティティワークフローの管理機能は、IDとアクセス管理ソリューションによって行われます。SAMLゲートウェイは、ルールエンジンの評価に基づいて、MFA、セッション保護、リアルタイムDLPなどの複数のアクセス制御アクションをサポートします。

フォワードプロキシやリバースプロキシを使用する方法と比べると、ProofpointのSAMLゲートウェイでリアルタイムのアカウント制御とDLPを行う場合、次のようなアーキテクチャ上のメリットがあります。

- **デバイスを選ばない：**ユーザーが使用するデバイスが会社所有か個人所有かにかかわらず、企業ネットワークの内外から行われるアプリへのアクセスを保護できます。
- **IT部門が承認したアプリに対応：**SAML 2.0をサポートし、アイデンティティプロバイダーによって連携しているクラウドアプリであれば、SAMLゲートウェイはIT部門が承認したすべてのアプリをサポートします。
- **エンドポイントエージェントが不要：**SAMLゲートウェイは、アイデンティティ プロバイダーのように機能し、ログイントランザクションを検査します。トラフィックをルーティングするエンドポイントは不要です。ユーザーのデバイスのライフサイクルを管理する必要がないため、価値実現までの時間を短縮できます。
- **ポリシードリブン：**アダプティブアクセスコントロールでは、脅威、DLP、アプリの制御に対して柔軟なフローを設定できます。これらのオプションを使用することで、リスクと信頼のバランスを取ることができます。
- **強固でスケーラブル：**SAMLゲートウェイは、ネットワークトラフィックの検査を行う際にURLリライトやターミネーションなどの技術に依存しません。ログイントランザクションのみを検査するため、遅延が少なくなります。このため、クラウドアプリを壊すリスクはなく、どのクラウドアプリにも対応できます。
- **ユーザーのプライバシーを保護：**他のインラインソリューションと異なり、SAMLゲートウェイはすべてのデータを検証するわけではありません。また、ユーザーの認証情報を可視化することもありません。データ漏えい対策のため、ユーザーがブラウザー分離にリダイレクトされた場合、ファイル転送のみが検査されます。ポリシー違反にならない限り、データを保存することもありません。このため、ユーザーと組織のデータプライバシーが保護されます。Proofpoint CASBはエージェントレスでクラウドベースのため、ハードウェアの追加も必要なく、導入も短期間で済みます。Proofpointのプロフェッショナル サービスにより、ほとんどの組織はクラウドアクセスとデータの制御を数時間で実装しています。

製品

Proofpoint Cloud App Security Broker（CASB）

Proofpoint CASB は、Microsoft 365、Google G Suite、Box などのアプリケーションを保護します。クラウドアカウントの侵害、データの行き過ぎた共有、クラウドのコンプライアンスリスクから保護します。このソリューションは、アダプティブ コントロールによりクラウドアプリへのアクセスを保護します。CASBの機能は次のとおりです。

- People-Centricのアプローチで脅威を可視化
- 自動レスポンス機能
- DLPによる包括的なデータセキュリティ
- クラウドアプリとサードパーティアプリのガバナンス

エージェントレスなアーキテクチャにより、価値実現までの時間を大幅に短縮し、リアルタイムでポリシーを適用します。このパワフルな分析を用いると、組織にとって最も重要なリスク要因をベースにして、サードパーティアドオンアプリやユーザーに適切なアクセス権を割り当てられるようになります。

Proofpoint SaaS Isolation

SaaS Isolationは、Proofpoint CASBのアドオン オプションです。ブラウザー セッションをセキュアなコンテナに分離し、クラウド上のアプリやデータに対するユーザーのアクセスを保護します。このソリューションは、危険なユーザーや動作からファイルのアップロードとダウンロードを保護します。ファイル転送にクラウドDLPポリシーをリアルタイムに適用し、機密データの窃盗や消失を防ぎます。これにより、危険なクラウドの使用で発生するセキュリティ、生産性、プライバシーの問題を解決することができます。SaaS Isolationは、エージェントレスアーキテクチャを採用しているため、IT部門が承認したどのアプリケーションにも使用できます。また、デプロイ、管理、サポートを簡単に行うことができます。