proofpoint®

Proofpoint Information

ソリューション アーキテクチャ

Protect people. Defend data.

Proofpoint Information Protection ソリューション コンポーネント

Proofpoint Information Protectionは、一連のAI活用テクノロジーの集合体であるProofpoint Nexusをベースに構築されています。これらのテクノロジーは、さまざまなチャネルにおいて、機密データを特定し、情報漏えいを防止し、内部脅威を封じ込めるよう設計されています。Nexusは、高度な言語モデルや振る舞い分析を用いて、ユーザーが意図的に、または誤って、機密データを共有してしまった可能性がある状況を検知します。許可されていないユーザーがデータにアクセスする、またはデータを移動するといった、異常な行動を特定することもできます。

このソリューションはまた、リスクのあるアクティビティをリアルタイムで阻止または修復できる自動ポリシーにより、きめ細かい制御を提供します。データのアクセスや動きをユーザーの行動と関連付けることで、Nexusは、メール、エンドポイント、クラウド アプリケーションにおいて個人を特定できる情報（PII）、ペイメント カード インダストリー（PCI）データ、その他の機密コンテンツといった、機密データを保護する上で役立ちます。

さらに、Nexusは、高度なAIを用いて管理と分析を統合することで、Proofpoint Data Loss Prevention (DLP)の機能を強化します。これにより、セキュリティチームは、データのアクセスと動きを監視し、GDPRやHIPAAなどのプライバシー規制に準拠できます。また、組織は特定のニーズに合わせてポリシーを調整することもできます。これにより、重要な業務を中断することなく、的を絞った保護を確保できます。

Proofpoint Information Protectionは複数の製品で構成されています。右に記載されている製品のほとんど（Adaptive Email DLP以外）はこのソリューションと統合しています。

Proofpoint ITM (Insider Threat Management)およびProofpoint Endpoint DLP は、内部関係者の悪意、不注意、または無自覚から生じる情報漏えいやブランドの風評被害から守ります。プルーフポイントはユーザー アクティビティとデータの動きを関連付けます。これにより、ユーザーリスクの特定、内部関係者によるデータ侵害の検知、インシデント レスポンスの迅速化が可能になります。また、USBメモリ、クラウド上の同期フォルダ、印刷などによるデータの持ち出しを阻止することもできます。ITMもEndpoint DLPも共通の軽量なエンドポイント エージェントを提供するため、一般的なユーザーやリスクのあるユーザー、そして高リスクのユーザーを柔軟に監視できます。

Proofpoint Cloud DLP（インラインDLPを含む）は、「人」を中心としたデータセキュリティとクラウドアプリのガバナンスを提供します。機密データを保護し、OAuthアプリを管理します。また、プライバシーやデータセキュリティの法律に準拠する上でも役立ちます。このマルチモードCASBは、BYOD（個人所有機器の持ち込み）向けのDLPなど、APIとプロキシベースの両方のデプロイモデルに対応しています。

Proofpoint Email DLPにより、メールによる機密情報の漏えいを防ぐことができます。また、PCI、PII、GDPR、SOX、HIPAAといった規制要件に対して、規格に沿った設定不要のポリシーで準拠できます。AIを活用した分類を含むカスタム ディクショナリを作成し、組織独自のデータを識別し、保護することもできます。Proofpoint Email DLPは容易に導入することが可能です。既存のメールセキュリティ システムの一機能としてセットアップできます。また、企業全体のDLPプログラムに統合することもできます。

Proofpoint Adaptive Email DLP は、振る舞いAIを使用し、従業員の通常のメール送信行動、信頼関係、機密データの操作方法などを学習します。続いて、各メールを分析し、異常な行動を検知すれば、潜在的な情報漏えいインシデントについて管理者に通知します。リアルタイムの警告をユーザーに提供し、メールによる機密データの漏えいを防ぎます。現時点で、Proofpoint Adaptive Email DLPはProofpoint Information Protectionプラットフォームに統合されていないため、本書では取り上げません。

環境において

Proofpoint Information Protectionは100% SaaSベースで提供します。バックエンドの分析アプリケーションは、視覚表現、異常検知、ビッグデータのクエリ、機械支援型のレビューやケース管理など、統合された管理とレポートの機能を提供します。また、セキュリティポスチャ、セキュリティ動向、コンプライアンス リスクをリアルタイムで監視できるダッシュボードも提供します。このソリューションは、経営幹部への報告に使用できるメトリクスを用いたレポート機能をサポートしています。

Enterprise DLP論理アーキテクチャ

Proofpoint Enterprise DLPソリューションは、セキュリティ管理者に、自社環境において機密データを保護し、効果的にインシデントを調査するツールを提供します。これにより、組織のデータ侵害リスクを大幅に減らすことができます。

インシデント管理の観点から、DLPソリューションの主な目的は、単一画面で、フォレンジックログ分析にかかる時間を短縮させ、調査とインシデント修復を迅速化し、全体的に少ない労力でより効率的に作業ができるようにすることです。

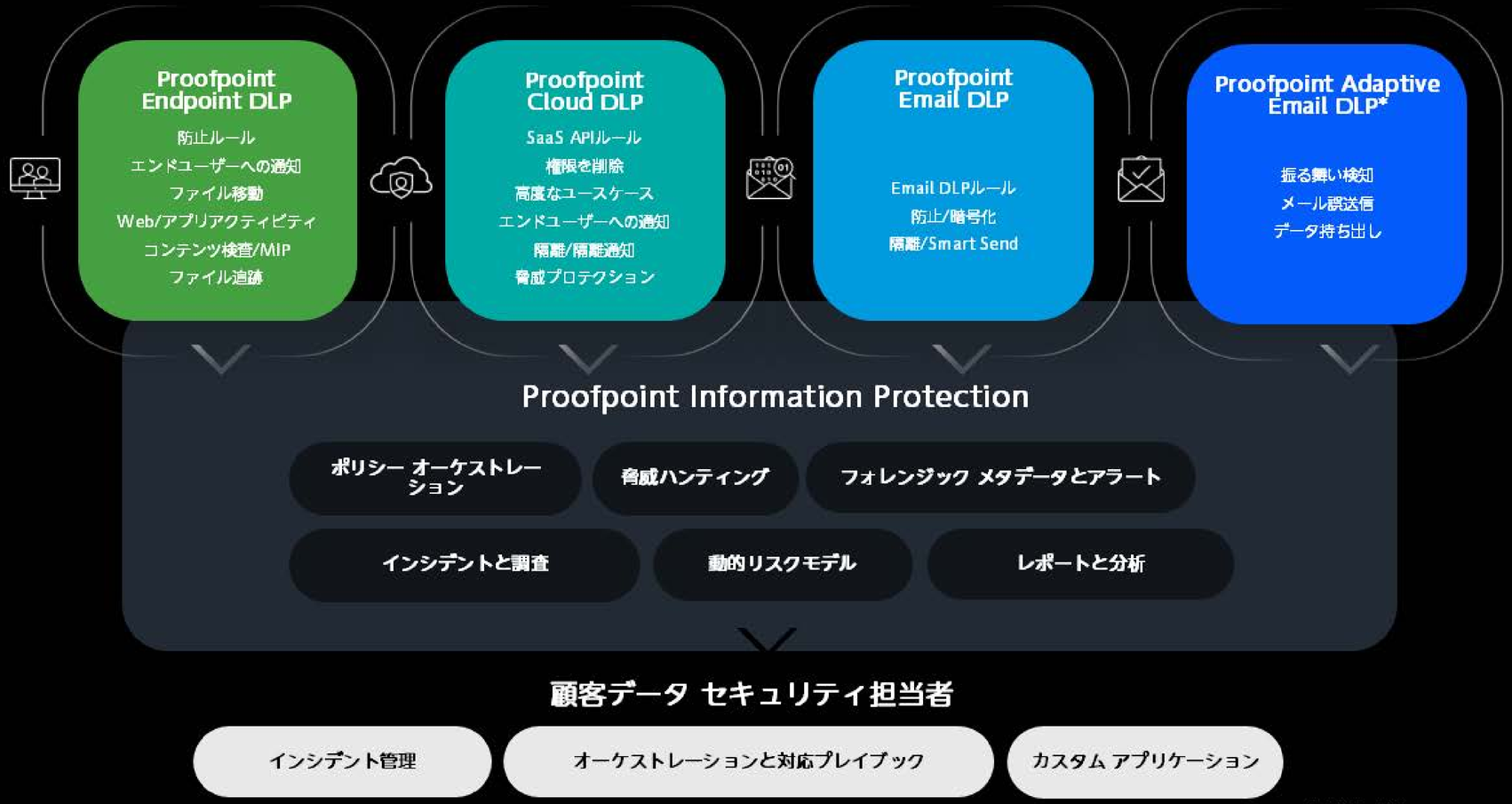
複数の異なる検知コンポーネントが統合ソリューションで連携しています。ソリューション アーキテクチャとは、その構成だけでなく、製品導入のルールやポリシーも示すものです。また、DLP プログラムにおける組織のリスクや事業上の課題も明確にします。

これにより、企業の情報に関連した、特定のアクティビティに対する可視性と制御を提供するために、組織固有のルールを作成することができます。セキュリティ インシデント アナリストへのアラート提供や、チャネル内自動修復の調整のためにDLPルールを作成できます。ルールをきめ細かく設定できるため、柔軟な対応機能により、重要な事業活動が妨げられることはありません。

また、重要なインシデントや高リスクのアクティビティは、特定、収集、エクスポート、担当チームとの共有が簡単です。これにより、インシデント管理にかかる負担や費用を削減し、チームは、情報漏えいによる被害から、組織とユーザーを効果的に保護することができます。

Enterprise DLPリファレンスアーキテクチャ

以下の図は、DLPソリューションのコンポーネント間のアクティビティと通信の流れを示したものです。



*将来的に統合

ドキュメント#:1207-005-08-01

Proofpoint Information Protectionの統合分析

エンドポイント、クラウド、メールにおけるInformation Protectionの統合分析アーキテクチャ

アラート管理、調査、対応をサポートする統合分析

統合アラート マネージャーは、ソリューションにより収集されたすべてのイベントのデータ分析とレポートを提供します。また、アラートワークフローを管理することもできます。このデータ分析機能を通じて、脅威ハンティングの探索、異常検出、機械支援アラートのトリアージなど、多くの高度なユースケースが提供されます。

分析アプリケーションでは特定の検知ルールを設定できます。そして、これらのルールによって発動されるアラートは、セキュリティ インシデント アナリストがトリアージできます。違反があれば、メールまたはアウトバウンドWebhookイベントが、SIEM/SOARまたはインスタント メッセージ システムといった、サードパーティ レシーバー アプリケーションに送信され、アラートの詳細が確認できます。

Splunkやその他のSIEMベンダーは、Proofpoint Information Protectionと統合でき、内部脅威、ラテラルムーブメント、データ持ち出しに関する情報が一目でわかります。これにより、関係するユーザーを迅速に特定したり、その他のイベントソースに対し、詳細を関連付けることができます。

プルーフポイントのプラットフォームはServiceNowとも統合でき、データの持ち出しやコンプライアンス違反があれば通知できます。続いてServiceNowは、顧客にアラートを提供し、アラートに基づいて新しいチケットやワークフローを作成できます。ServiceNowとの統合により、DLPにおいて調査と対応はより速くなります。

ドキュメント#:1207-005-08-01

プラットフォームのアクセスとプライバシーの制御

プルーフポイントの従業員は、お客様からデータを共有されない限り、お客様のデータにアクセスすることはありません。お客様よりアクセスが許可された場合、プルーフポイントの従業員またはお客様の従業員がProofpoint User Centerを使用してシステムにログインすることがあります。または、一時的なユーザーとして、ペルソナを使用してアクセスが割り当てられる場合があります。

高度な権限をもつ管理者アカウントの使用に関してアラートをセットアップする必要があります。セキュアに保つために、このアカウントのパスワードを変更する必要があります。パスワードはエスクローに保管することも、それぞれの担当者が保持しておくこともできます。

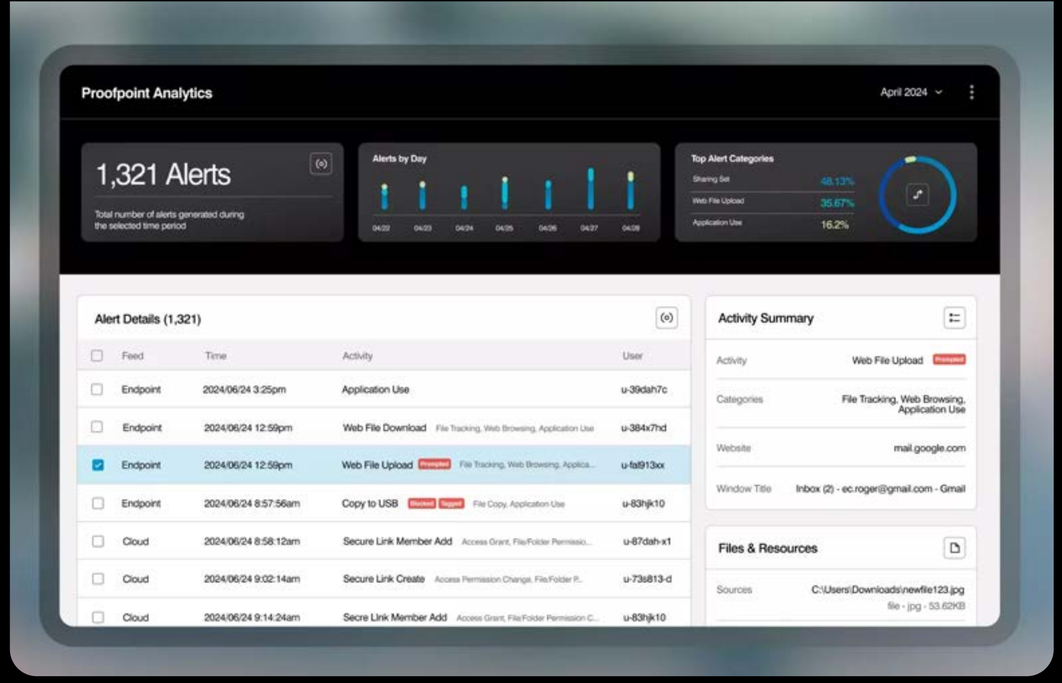
SAMLまたはOAuth2.0を使用し、シングル サインオン（SOO）やマルチファクタ認証（MFA）など、クラウドベースの認証方法を統合することを強くおすすめします。複数のアイデンティティ プロバイダーを組み合わせることも可能です。

Proofpoint Information Protectionプラットフォームの[Administration（管理）] > [Account Settings（アカウント設定）]に移動し、必要な設定に応じて、アイデンティティ プロバイダーを構成する必要があります。Information Protectionプラットフォームと連携させるために、アイデンティティ プロバイダーを構成する必要もあります。

管理者アカウントは、プラットフォーム内のすべての設定とデータへの、匿名化されていない完全なアクセス権を有します。そのため、認証情報を保護し、極秘として扱う必要があります。追加のローカル管理アカウントは、製品テストにおいて、[Administration（管理）] > [User Management（ユーザー管理）]から作成することができます。各アカウントには、必要に応じて固有のアクセスポリシーを割り当てることができます。しかし、ほとんどの場合、管理ユーザーをさらに追加した場合、そのユーザーが利用できる制御や管理作業へのアクセスを制限する必要があります。

Proofpoint Information Protectionは、プライバシー バイ デザインの原則の下に構築されています。知る必要がある人のみが機密データとユーザーを特定できる情報にアクセスできます。プルーフポイントは、米国、欧州、オーストリア、カナダ（2024年末）、日本（エンドポイント データのみ）で地域別データセンターを使用しています。これにより、データを地理的に分離できます。そのため、米国のレルムは、米国のデータを米国のデータセンターに送信し管理するように設定できます。きめ細かいアクセスポリシーにより、管理者は、アクセスを割り当てることができるため、米国で働くセキュリティ アナリストには米国のデータのみが表示されます。

Proofpoint Information Protectionでは、システム管理者は、フォレンジックデータ（PII、PHI、PCI）を、コンソール内で隠したり、ユーザーのアイデンティティを表示させないよう構成することもでき、アナリストのバイアスを取り除くことができます。ユーザー名、ホスト名、IPアドレス、位置情報、ファイル名を匿名化できます。調査を進めていくうちにユーザーのアイデンティティを明らかにする必要があれば、セキュリティ アナリストは、権限をもつ管理者に匿名化の解除を要求することができます。



Webコンソールアクセス

管理者とアナリストは、サポートされているブラウザを使用してプラットフォームにアクセスできます。ポリシーとルールの管理、アラートの確認、インシデントの直接修復、収集したデータセットの分析、捕捉されたユーザー アクティビティに基づいたレポートの確認を行うことができます。

分離されたサブ組織を管理する場合、組織は多くの場合、プルーフポイントのプラットフォーム上の複数のサブテナントにアクセスできます。

プラットフォームの通知

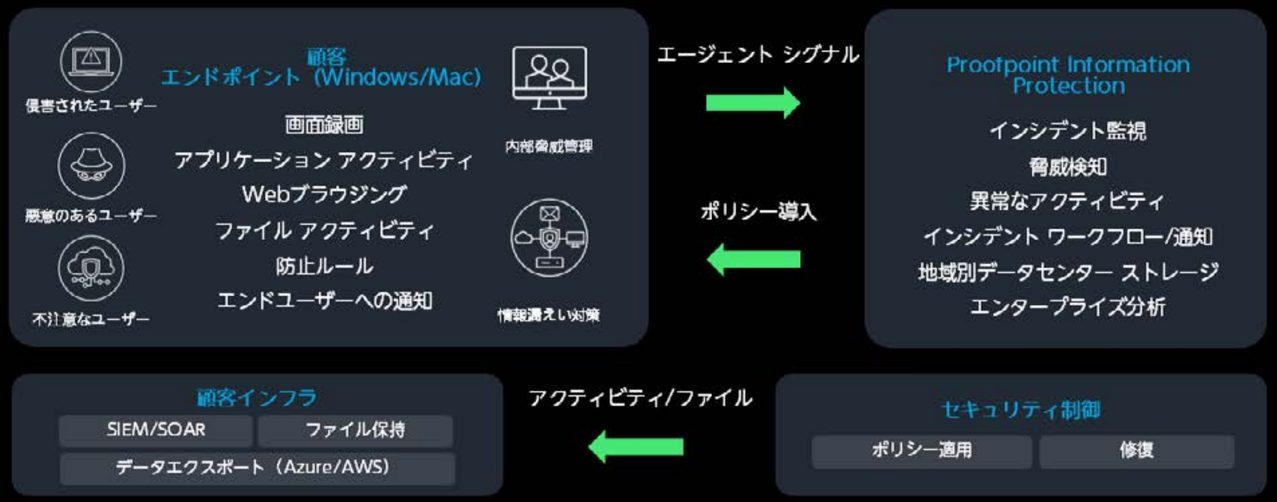
アラートは、プルーフポイントのプラットフォーム内で監視と処理が可能です。または、内部のインシデント管理手順に従って外部で行うこともできます。Proofpoint Information Protectionプラットフォームによって生成されたアラートを受け取る、メールアドレスを確認する必要があります。外部システム（SIEM、SOAR、ITSM）もまた、アラートを受信するよう構成できます。

外部アプリケーション

外部アプリケーションは、REST API経由でプルーフポイントのプラットフォームにアクセスできます。

Proofpoint Endpoint DLP/ITMリファンレンスアーキテクチャ

DLPとITMの単一のエージェントは、データを収集し、プラットフォームにアップロードしながら、
DLPポリシーを適用します。



DLP/ITMエンドポイント エージェント構成

Proofpoint Endpoint DLPエージェントは、サポートされているバージョンのWindowsまたはmacOS上で実行している、顧客のエンドポイントにインストールできます。エージェントを本場環境にインストールするには、人がいない環境で、企業標準のリモート ソフトウェア インストール ツールを使用する必要があります。

インストール後、エージェントは、ユーザー アクティビティを表すメタデータを記録します。明示的なルールは必要ありません。メタデータはInformation Protectionプラットフォームによってセキュアにアップロードされ、処理されます。エージェントの管理と構成を行うには、プラットフォームの[Administration（管理）] > [Endpoints（エンドポイント）]アプリケーションを使用します。

プルーフポイントのエンドポイント エージェントはサイレントインストールが可能です。各エージェントは、ユーザーメモリ空間で実行されます。必要なリソースは最小限で、アップデートは自動的に行われます。インストールやアップグレードの後も再起動する必要はありません。エージェントと既存のエンドポイント セキュリティの間でコンフリクトが生じたり、他のアプリケーションに障害が発生したり、パフォーマンスが低下したりすることはありません。

インストールされたエージェントとITMサーバーは、HTTPSプロトコル経由で非同期で通信します。DLPエージェントは、TLS暗号化を使用してプルーフポイントのクラウドサービスと通信します。接続に関するファイアウォール要件については、プルーフポイントのオンライン ドキュメンテーション ポータル（要ログイン）をご覧ください。

動的プロキシ経由で接続する必要のあるエージェントは、オペレーティング システム レベルで定義されたプロキシ設定を使用します。オペレーティング システムは、（ユーザーアカウントではなく）システムアカウント内で実行するアプリケーションの動的プロキシを使用する構成にする必要があります。静的プロキシの使用もまたサポートされています。この設定は、エージェントがインストールされると構成されます。

アンチウイルスやEDRのソフトウェアの中には、オンデマンドで実行可能ファイルのスキャンを実行し、デフォルトでこれらの通信の処理を保留にする、またはブロックするものがあります。安定した機能性を確保するために、プルーフポイントによるプロセスは、他のセキュリティツールによる調査から除外する必要があります。プルーフポイントでは、プルーフポイントのツールにおいて特定のアプリケーションをアロウリストに追加する必要はないと考えています。これは、プルーフポイントのエージェントはユーザーモードで動作する軽量アプローチは採用しているため、カーネルモードで動作する エンドポイント エージェントの動作に設計上、干渉するとは考えにくいためです。

セーフリストに追加するWindowsエンドポイント エージェント コンポーネント

プルーフポイントのファイルをEDRまたはアンチウイルス システムの影響を受けないようセーフリストに追加する方法については、オンラインドキュメント**「ITM / Endpoint DLP Excluding Processes from Antivirus Software」ガイドを参照してください。**

注：macOSで通知を表示する、またはスクリーンショットを収集するには、モバイルconfigファイルをデプロイすることで、プライバシー設定がプルーフポイントのプロセスに付与されるようにする必要があります。このプロセスの詳細については、オンライン ドキュメント「Mac Agent System Preferences - Security & Privacy Settings」をご覧ください。

プルーフポイントのエンドポイント エージェントは２種類のプロキシをサポートしています。動的プロキシの場合は、オペレーティング システム レベルでPAC自動構成ファイルを使用します。静的プロキシの場合は、インストール時にホスト名とポートを入力します。エージェントが使用するデフォルトの認証情報を設定するには、インストール時にドメイン、ユーザー名、および/またはパスワードの項目を入力します。

エージェントの更新

SaaSプラットフォームとして、プルーフポイントは、新機能を迅速にエージェントに展開できます。プルーフポイントでは、リリーススケジュールに対応できない顧客向けに、エージェントの長期サポート（LTS）バージョンも用意しています。しかし、一般的に、サポートされる最新のリリースでエージェントをお使いいただくことをおすすめしています。

エージェントを最新の状態に維持するために、設定済みの更新ポリシーに基づいた、自動更新サービスの使用をおすすめします。管理者がエージェントの更新を決めると、ターゲットリリースと条件を定義するポリシーを更新する、または作成してアップグレードに適用します。エージェントのアップデーターは、エンドポイントで処理を行い、正しいバージョンが自動的にダウンロードされ、インストールされるようにします。

ルート証明書

インストールされるエンドポイントには有効なルート証明書が必要です。プルーフポイントは有効なルート証明書でエージェントに署名し、顧客がプルーフポイントによるものであることを認識できるようにします。この証明書は、有効なルート証明書に応じて異なり、年間の有効期限があります。

エージェントヘルス監視

エラーや前回のチェックイン時間といった、エージェントヘルス情報は、プラットフォームのEndpoint Catalogueで確認できます。Windowsエージェントは自己修復に優れ、エージェントに障害が発生した、または終了した場合に再起動する監視サービス（ITクラウドサービス）が備わっています。 Macエージェントのロガープロセスも同様に起動されます。エージェントに強制終了や中断が発生すると、プログラムがエージェントを再起動します。

エージェントの強化

エンドポイント上のエージェントの構成ファイルやログファイルは完全に暗号化できます。

インストール時に、セキュリティキーを追加してエージェントがアンインストールされたり、プロセスの名前が変更されたりしないよう、さらに強化することもできます。

エンドポイント レルムの構成

エージェントレルムは、ストレージの地理的情報やデータ保持期間に基づいて、エージェントを分離します。

エンドポイントの防止ルールは、階層型エージェントポリシーにより導入されます。ユーザーへの警告やブロックといったアクションを実行します。同時に、エージェントのログのメタデータは、ユーザーのアプリケーション アクティビティに関するシグナルを提供します。これらのログは、分析プラットフォームに送信され、処理が行われます。オプションでスクリーンショットが利用できます。

処理されたデータは、選択したエージェントレルム設定に応じて、選択した地域別AWSデータセンター（現在、米国、EU、アジア太平洋、日本、カナダ）に保存されます。

エージェントポリシー設定

エージェントポリシーは、プルーフポイントのエージェントが捕捉するものを定義します。これらはエージェントレルムに割り当てられます。これにより、設定を構成し、同時に複数のレルムのエンドポイントに適用することができます。

複数のエージェントポリシーを１つのエージェントレルムに割り当てることができます。複数のポリシーを割り当てる場合、優先順位を決めることができます。これにより、どの設定をどのエージェントに適用するかを定義できます。この順序指定により、エージェントポリシーごとに、どの設定が有効にされ、使用されるかを決めることができます。

エンドポイントの防止とエンドユーザーへの通知

DLPまたは内部リスクプログラムの基本は、データ侵害のリスクを低減できるようエンドユーザーの振る舞いを改めさせることです。DLPルールを管理対象エンドポイントに導入すれば、ポリシー違反に対し、エンドユーザーをブロックしたり、警告したりできます。行動に影響を与え、これによりデータ侵害のリスクを低減できます。

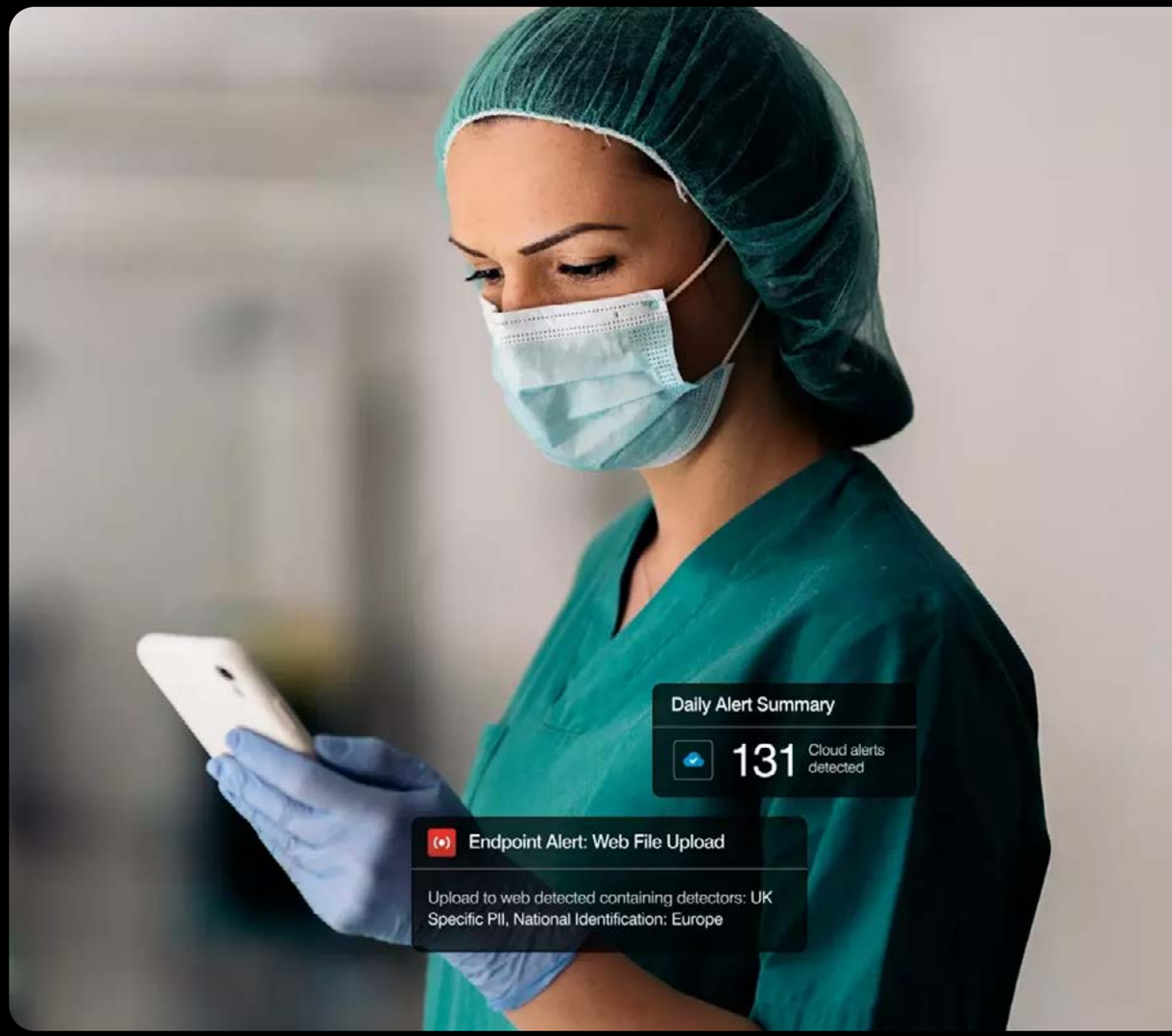
DLPルールは、企業の機密情報の持ち出しが起こりそうな状況において、エンドユーザーの行動を変えることを目的としています。最初に、一般的なアプローチは、アラートや調査で確認できるアクティビティ メタデータにより、ユーザーが何をしているかを監視することです。セキュリティチームは、アラートを確認しながら、組織の優先事項やインシデント検知プロセスに沿ってルールを調整していきます。

調整を終え次第、ルールを導入できます。その後、ポリシーに従っていないエンドユーザーは、操作を実行できず、ブロックされたというメッセージを受け取ります。操作を実行するには、メッセージ内で提示される「正当な理由」リストから１つを選択する必要があります。

通常、エンドユーザーへの通知には、どのポリシーに違反したのかを示す説明が記載されます。通知には、企業の公式ロゴや、組織のセキュリティポリシーについて記したWebページへのリンクを含めることもできます。使用できる企業ロゴ画像のサイズは56K未満です（MIMEタイプのimage/*）。

ユーザーは、操作がブロックされた際にすべきこと、またはこのような中断に対する苦情を申し立てる方法が確認できます。DLPプログラムの必要性にについて説明した、企業のセキュリティ イントラネット ページへのリンクを含めるのも良いでしょう。

検知ルールは、プルーフポイントの分析アプリケーションでアラートを生成し、インシデント対応担当者はこれらを管理できます。担当者は、エンドポイントのデバイスで選択したユーザーアクティビティにより生成された、収集メタデータを確認します。メタデータは、スクリーンショットの頻度や解像度など、エージェントポリシーの設定に従って、エージェントにより記録されます。これは、管理コンソールで管理されます。



Proofpoint Cloud DLPの構成

Proofpoint Cloud DLPはエージェントレスのアーキテクチャをサポートしています。クラウドAPIを使用して重要なクラウド アプリケーションを保護します。また、BYODデバイスにインラインDLPを提供し、ユーザーが認証を経てクラウド アプリケーションにアクセスしたデバイスに対しブラウザ分離を使用します。

Proofpoint Cloud DLPは、組織のプライマリ クラウドサービスや許可されたSaaS/IaaSアプリケーションにそれぞれのAPI経由で接続します。これは、クラウド セキュリティ インシデントの修復など、ほぼリアルタイムで双方向の機能を提供します。

Proofpoint Cloud DLPは非常にパワフルで、Proofpoint Endpoint DLPが使用するものと同じDLP Detectorスタックで修復を提供します。

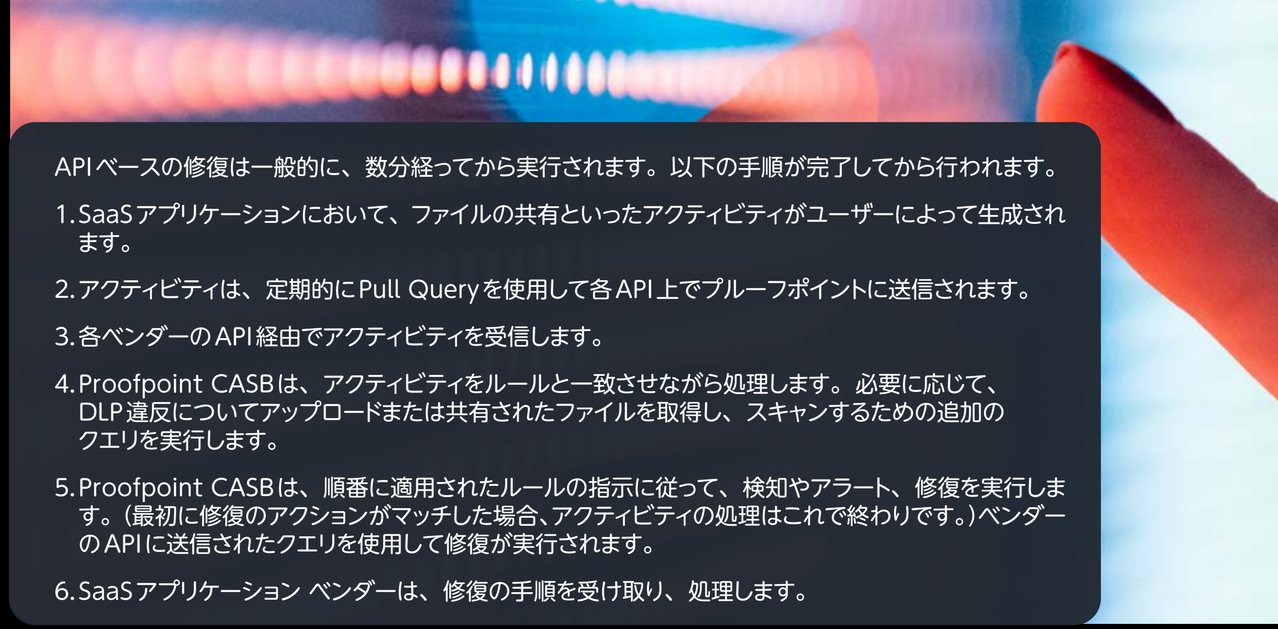
Proofpoint CASB Adaptive Access Controlsは、Proofpoint Cloud DLPのパワーを、さまざまな高度なリアルタイム ユースケースに広げます。例えば、非管理対象デバイスの認識とブロックや、クラウド アイデンティティ プロバイダーとのSAML/OIDC統合による高リスクの場所からのアクセスの認識とブロックがあります。

Proofpoint SaaS Isolationとの統合を利用して、ブラウザベースのファイルのアップロードやダウンロードに対し、よりきめ細かいDLPコントロールを使用できます。これは、エージェントなしで可能です。そのため、BYOデバイスでのDLPに最適です。また、Proofpoint Okta APIコネクタは、SAML統合を簡素化します。Oktaとのフェデレーションが構成されたアプリケーションに自動的にアダプティブ コントロールを適用できます。

追加の手順として、AzureやAWSといった、IaaSサービスは、DLP監視用に構成できます。プルーフポイントでは、これらのAPIについては個別に請求されます。

最初に、選択したエンタープライズ クラウド アプリケーションのベンダー APIは、セキュリティ監視のためにProofpoint Cloud DLPに接続されます。

Proofpoint Cloud DLPで特定のルールを作成し、クラウドサービスにおいて企業DLPポリシーの違反を特定し、修復することができます。また、自動ガバナンスルールをサードパーティ OAuthアプリケーションに適用することもできます。Microsoft 365やGoogle Workspaceといった、主要なSaaSサービスや組織のサービスへのシステムやデータのアクセスを維持できます。



APIベースの修復は一般的に、数分経ってから実行されます。以下の手順が完了してから行われます。

1. SaaSアプリケーションにおいて、ファイルの共有といったアクティビティがユーザーによって生成されます。
2. アクティビティは、定期的にPull Queryを使用して各API上でプルーフポイントに送信されます。
3. 各ベンダーのAPI経由でアクティビティを受信します。
4. Proofpoint CASBは、アクティビティをルールと一致させながら処理します。必要に応じて、DLP違反についてアップロードまたは共有されたファイルを取得し、スキャンするための追加のクエリを実行します。
5. Proofpoint CASBは、順番に適用されたルールの指示に従って、検知やアラート、修復を実行します。（最初に修復のアクションがマッチした場合、アクティビティの処理はこれで終わりです。）ベンダーのAPIに送信されたクエリを使用して修復が実行されます。
6. SaaSアプリケーション ベンダーは、修復の手順を受け取り、処理します。

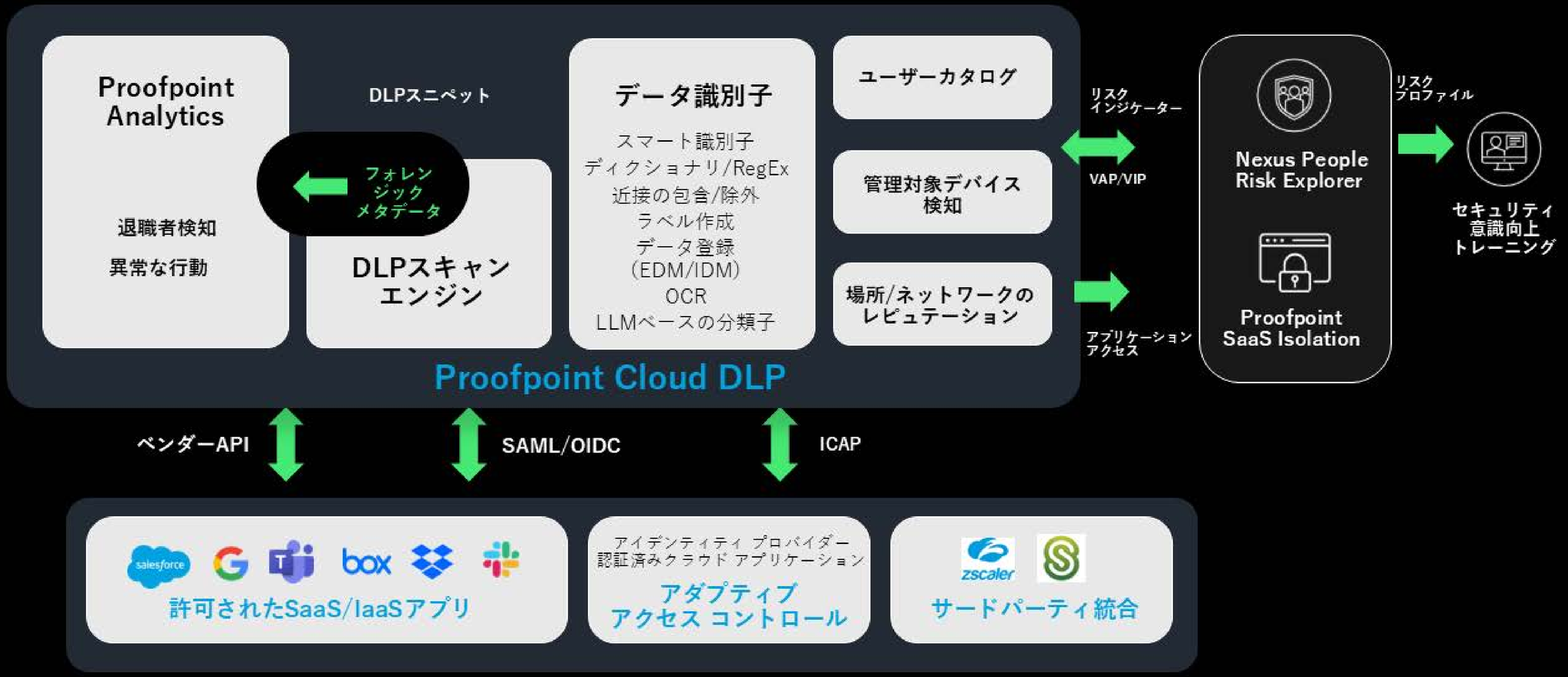
Proofpoint CASB Adaptive Access Controlsにより、サポートされているアプリケーションは、エージェント不要でインラインで制御可能です。アイデンティティ プロバイダーとのSAML 2.0またはOIDC統合により、Proofpoint Cloud DLPを使用して追加の保護を認証済みアプリケーションに適用できます。

Proofpoint CASB Adaptive Access Controlsをセットアップするには、ユーザーログイン要求を、アイデンティティ プロバイダーで認証される前にプルーフポイントにリルートする必要があります。続いて、一定の条件に基づいてのみ、許可された企業のクラウド アプリケーションへのアクセスを許可するルールがプルーフポイントによって適用できます。

ポリシーは、ユーザーが非管理対象のデバイス、オフィス ソース ネットワークのEgressレンジ外、リスクのある場所または高リスク要素からSaaSアプリケーションにアクセスしているかといった、パラメータに基づいて設定できます。Proofpoint SaaS Isolationとの追加の統合を利用して、ブラウザベースのクラウド アプリケーションのアクセスに対し、よりきめ細かいコントロールを使用できます。これにより、エージェント不要で、プルーフポイントのDLPスタックとのリアルタイムの統合が可能です。

DLPをさらに統合し、クロスチャネルの情報漏えい可視化を提供するために、プルーフポイントは、ZscalerやCitrix ShareFileとのICAP統合もサポートしています。統合するには、サードパーティ アプリケーションのICAPクライアントに対し、プラットフォームでこのチャネルにDLP Detectorセットを構成した後、そのトラフィックをDLPサービスに送信して設定します。

Proofpoint Cloud DLP参照アーキテクチャ



ドキュメント#:1207-005-08-01

Proofpoint Email DLPの構成

Proofpoint Email DLPは、プラットフォームによって提供されたインライン メール ゲートウェイを使用してアウトバウンドのメールを処理します。このゲートウェイは、アウトバウンドのメール アーキテクチャに統合されています。

プルーフポイントは、アウトバウンドのProofpoint Email DLPをテストしている場合でも、これを本番環境に組み込む場合でも、既存のメールアーキテクチャに基づいて、インフラとシステムを構成する方法についてアドバイスします。

アウトバウンドのメールゲートウェイにすでにプルーフポイントを使用している場合、Proofpoint Email DLPは、Regulatory Compliance モジュールにライセンスを適用するだけで、プルーフポイントの既存のメールゲートウェイで直接有効にされます。メールフローが変更されることはありません。SPF、DMARC、IPウォームアップへの影響はありません。

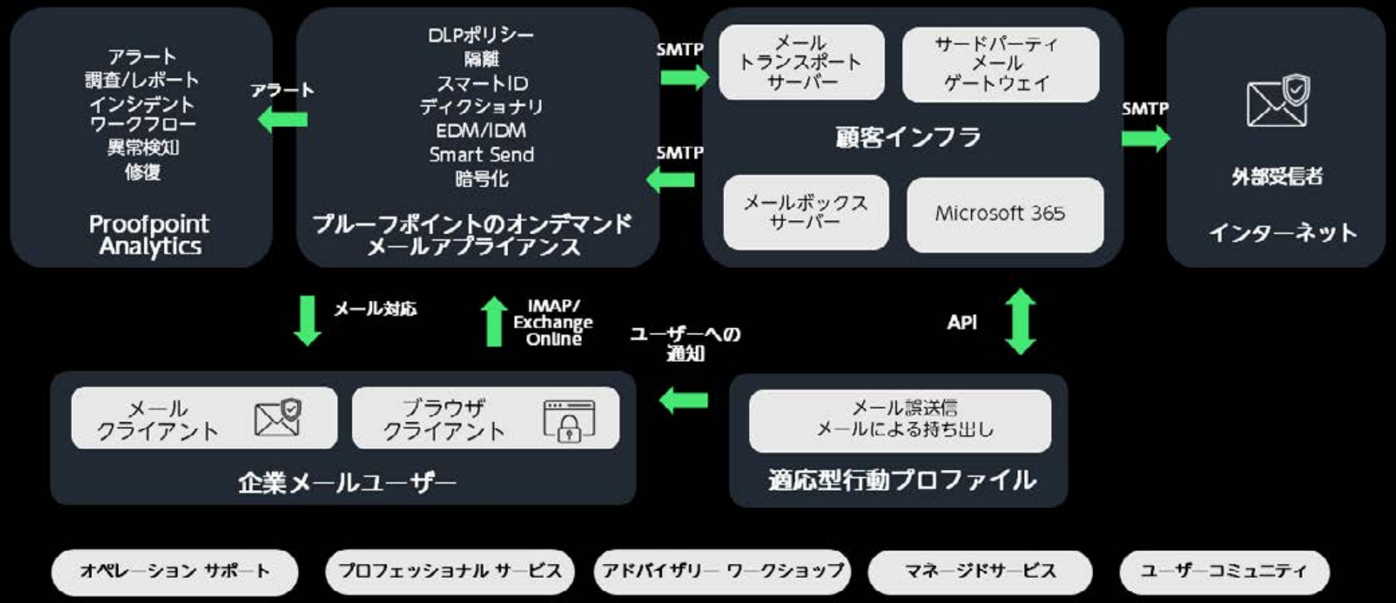
Email DLPが有効になったら、レポート、エンフォースメント、エンドユーザーへの通知ややり取りなど、DLPの全機能を評価できます。

プルーフポイントをメール処理フローの最後のホップとして使用しない場合、プルーフポイントのクラウドベースのメールゲートウェイは、追加のSMTPホップとしてアウトバウンドのメールインフラに統合されます。これは、インフラがさらに変更されるのを避けるために、既存のメールゲートウェイの前に挿入するのが理想です。

アウトバウンドのメールサービスが統合されたら、レポート、エンフォースメント、エンドユーザーへの通知ややり取りなど、DLPの全機能を使用できるようになります。

Proofpoint Email DLP参照アーキテクチャ

Email DLPコンポーネントが企業のメールユーザーと相互に関係し、通信する仕組み



ディザスタリカバリ(DR)

プルーフポイントは、プルーフポイントのプラットフォーム内でディザスタリカバリを完全に管理し、運用します。プルーフポイントのサービスのいずれかにおいて、業務の中断が発生すれば、プルーフポイントは、ディザスタリカバリ計画を実装します。これには、状況に関する定期的な更新情報レポートが含まれます。レポートには、イベントの概要説明、顧客への影響、通常のオペレーションの復旧予定時期が含まれます。プルーフポイントの事業継続性プログラムのドキュメントには、ビジネスプロセスがどのように復元されるかに関する説明が含まれます。計画は、少なくとも1年に1回見直され、机上での演習が毎年行われます。詳細は、プルーフポイントでのSOC 2 Type 1リクエストとして要求可能です。

プルーフポイントのクラウドサービスがネットワーク上でアクセスできなくなっても、既存のDLP防止ルールのエンフォースメントに影響はありません。すべてのDLP防止ルールは、マシンポリシーによりエージェントに直接適用されます。これらのルールは適用するために、サーバーと通信する必要はありません。

この期間において防止ルールが管理者により変更された場合、マシンは、プルーフポイントのサービスとの接続が確立されてからのみ、変更を受け取ります。これは、10分ごとに確認されます。

検知について、接続が失われると、エージェントは、エージェンレルムやエージェントポリシーの設定で定義され、選択したイベントを保存します。これらは管理コンソールで管理されます。デバイスがアプリケーションとの通信を再確立すると、選択したイベントのメタデータがアップロードされます。

データの機密度

機密データ識別子に基づいたDLPルールを作成することで、一貫した、包括的な方法でセキュリティ制御を適用できます。

データ機密度は、データグループが開示された場合に、組織に与える悪影響の度合いによって定義されます。影響には、顧客からの信頼の喪失、利害関係者からの信用の喪失、直接の金銭的被害、規制機関による罰金があります。

Cloud DLPとEndpoint DLPのDLP Detector

ここで取り上げるProofpoint DLP Detectorは、Cloud DLPとEndpoint DLPのルールにのみ適用されます。 Endpoint DLPでコンテンツスキャンを使用する場合、以下の手順を実行する必要があります。

- インストール時に、エンドポイント エージェントは、コンテンツ スキャン コンポーネントが有効になっている必要があります。または、このコンポーネントで更新する必要があります。
- エンドポイント コンテンツ スキャンは、次の選択可能なエンドポイント アクティビティについて、エージェントレルムに対し有効にする必要があります：Webファイルアップロード、Webファイル同期、USBメモリへのコピー、Webファイルダウンロード、ドキュメント開封、印刷、クリップボードからのテキストの貼り付け、ネットワーク ドライブへのコピー。
- コンテンツスキャンにDLP Detectorセットを使用する場合、ディテクターをエージェントレルム構成に追加し、エンドポイントのエージェントにデプロイする必要があります。

デプロイが完了したディテクターは、検知や防止のルールで使用できます。エージェントに導入される防止ルールのロジックには、エンドポイントのエンフォースメント（正当な理由またはブロック）や機密データディテクターが含まれます。

Proofpoint Cloud DLPに接続されたクラウド アプリケーションにおいて、ポリシーエンジンは、DLPアプリケーションで構成されてから短時間でDLP Detectorを使用できるようになります。Cloud DLPのルールは、プラットフォーム内でアラートを提供するよう構成できます。ただし、書き込みモードでは、Cloud DLPアプリケーションのルールを使用して、SaaSアプリケーション（APIまたはインライン）の接続タイプに基づいて、修復アクションを実行できます。Cloud DLPルールは、DLP違反をロジックに組み込むことができます。このルールのプロパティは、DLPアプリケーション ディテクターに自動的に同期されます。オンボーディング済みのエンタープライズSaaSアプリケーションのすべてのクラウドアクティビティは、分析アプリケーションに取り込まれます。構成済みCloud DLPアラートは、コンソールで表示されます。修復アクションは、アラートから直接管理し、確認できます。

Proofpoint DLPは移動中の機密データと使用中のデータを認識します。これには以下の３つの方法があります。

1. **視覚的な秘密度ラベル（Microsoft Information Protection）が付与されたファイル**

   Microsoftラベルを使用するデータ分類プログラムを使用している場合、プルーフポイントは、Microsoftの秘密度（MIP）のテナントIDとラベルを識別できます。識別された後はルールに従って処理できます。

2. **Proofpoint DLP Detectorの定義に一致するコンテンツを含むファイル**

   Proofpoint DLP Detectorは、事前に作成されたスマート識別子、設定不要またはカスタムのディクショナリ キーワード、分類子などを使用して機密コンテンツを特定します。

3. **メタデータ（ファイル名、パス、ファイル拡張子、Trueファイルタイプ、ドキュメント プロパティ）などのコンテキストとなるマーカーのあるファイル、または追跡されたURLからのファイル**

   Endpoint DLPでは、サポートされているブラウザを使用してエンドポイントにダウンロードされたファイルは、自動的に追跡されます。コピー、移動、削除、名前変更といった、デバイス上でファイルに行われたすべてのアクティビティは追跡されます。ファイルが特定のEgressチャネル経由でマシンから送信された場合は、これ以上追跡されません。追跡されたファイルのすべてのアクティビティはエージェントにより捕捉され、ファイルのタイムラインで履歴を確認できます。

   そのため、追跡されるファイルは常に、ブラウザがこのファイルの場所を特定するために使用するURLからのものであり、このURLは、トラッキング オリジン リソースURLと呼ばれます。これは、機密のWebサービスから提供されたファイルに対する行動を監視し、制御するための検知と防止のルールのために、エンドポイント エージェントによって使用できます。

Email DLPのDLP Detector

Email DLPのDLPルールは、Proofpoint Email Security (PPS/PoD)ソリューションで構成する必要があります。しかし、このプロセスは、本書の対象外となるため、ここでは取り上げません。

Proofpoint Email Securityソリューションの規制コンプライアンス モジュールは、必要なスキャンを実行する、Email DLPルールに基づいて必要なアラートのログを作成する、チャネル内処理アクションを実行するために構成されます。修復には、メッセージを処理するためにローカル隔離フォルダに移動する、メッセージを暗号化する、メールでエンドユーザーに対応する、メッセージを送信する、メッセージを承認する前に確認するようユーザーに求めるスマート応答をユーザーに送信するといった機能が含まれます。

Email DLPポリシーに違反したすべてのアクティビティは、アラート内で確認できます。これには、管理者により直接ダウンロードと確認が可能なメールの詳細が含まれます。

DLP識別子、ディテクター、セット

プルーフポイントのディテクター表現は、独自の構文で書かれています。構文には、スマートID、ディクショナリ、近接包含/除外、EDM、IDMデータセットの5つの条件タイプに対する任意のブーリアンの組み合わせが含まれます。処理の順序は、括弧()で示されます。追跡されるURLは、ファイルが指定の場所からブラウザでダウンロードされると、エージェントで確認できる特定のURL（リスト）です。

カスタム ディクショナリは、ファイル内の潜在的な機密データを特定する、DLP Detectorによって使用される顧客固有の用語リストです。ファイルがスキャンされると、ディテクターは、有効なディクショナリにおいてすべての用語に対しすべての単語とフレーズを比較します。

カスタムスマートIDは、プラットフォームにより深く統合されており、プルーフポイントのエンジニアリングによって管理されます。一部のケースでは、値にチェックサムを実行するためにスマートIDを作成する必要がある場合があります。例えば、顧客固有のポイントカード番号や正規表現やコードを使用するアルゴリズムです。

最初の導入作業には、機密データマーカーの洗練化と調整が多くを占めます。これにより、誤検知アラートの発生率を下げ、精度を高めることができます。

コンテンツスキャン ディテクターは、追加されたディクショナリやスマートIDに基づいて機密データの一致条件を示します。

ディテクターセットには、エンドポイント エージェントによって使用されるDLP Detectorが含まれます。これらはエージェントレルムの構成設定に含め、導入する必要があります。

コンテンツ調査のその他の高度な機能には以下が含まれます。

- 画像を処理してテキストを抽出し、DLP分析を行うOCR(光学式文字認識）
- 構造化された表形式データの多層カラム一致により、高精度の検知を行うEDM (Exact Data Match)
- 構造化されていないファイルのアップロードや、Egressチャネル経由で送信されたファイルの類似分析を行う、IDM(Index Data Match、ドキュメント フィンガープリンティング)

現在、リソースの制約により、これらの高度な機能はエンドポイントのエージェントで利用できませんが、Cloud DLPとEmail DLPで利用可能です（スキャンプロセスがクラウドで行われる場合）。

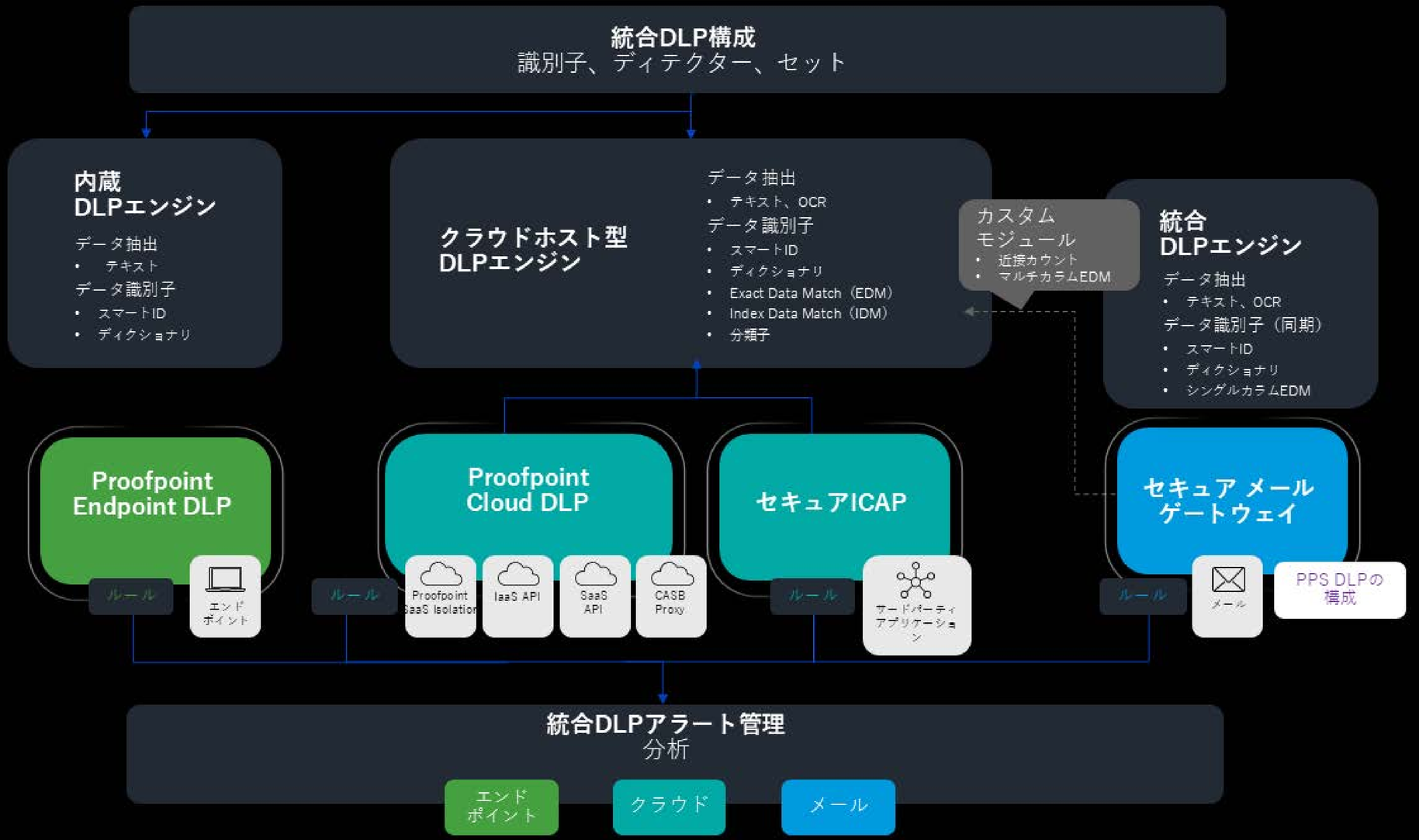
オフラインアーカイブ/データエクスポート

プルーフポイントのデータエクスポート機能により、データをセキュアにプルーフポイント外で複製できます。エクスポートするデータを指定します。これにはアクティビティ データ、アラート、イベントが含まれます。エクスポートされたデータの保持制限はありません。エクスポートされると、データを操作して分析や関連付けを行うことができます。

データは、プルーフポイント アプリケーションから独立した、お客様が所有するAWS S3/Azureバケットに複製できます。複製後、SIEMやデータレイクなど、その他の分析ツールに取り込むことができます。

エクスポートデータは、エクスポートを開始した時刻から15分前のものです。エクスポートは15分ごとに実行されます。

DLPチャネルによるデータ抽出と識別子



ドキュメント#:1207-005-08-01

proofpoint®

詳細はこちら：http://proofpoint.com/jp

Proofpoint, Inc.は、サイバーセキュリティのグローバル リーディング カンパニーです。組織の最大の資産でもあり、同時に最大のリスクともなりえる「人」を守ることに焦点をあてています。プルーフポイントは、クラウドベースの統合ソリューションによって、世界中の企業が標的型攻撃などのサイバー攻撃からデータを守り、そしてそれぞれのユーザーがサイバー攻撃に対してさらに強力な対処能力を持てるよう支援しています。また、Fortune 100 の 87% の企業などさまざまな規模の企業が、プルーフポイントのソリューションを利用しており、メールやクラウド、ソーシャルメディア、Web関連のセキュリティのリスクおよびコンプライアンスのリスクを低減するよう支援しています。詳細は www.proofpoint.com/jp にてご確認ください。