Proofpoint Cloud App Security Broker IaaS Protection

クラウドサービスの設定ミスを識別し、IaaS ストレージ内の機密データを保護

課題

- 設定ミス
- 不明なリソースと IaaS アカウント
- データ損失とコンプライアンス
- クラウドアカウントの乗っ取り

主な機能

- 複数のベンダー、アカウント、地域にまたがる IaaS リソースを一元管理し、マルチクラウドのセキュリティとコンプライアンス準拠を容易にする
- 公開されているベースラインから逸脱したセキュリティ設定のミスを特定
- ユーザーの行動を監視および分析し、未承認のログインや管理アクティビティを検知して阻止
- IaaS ストレージ内の機密データを保護
- 未承認の IaaS アカウントを発見して管理
- クラウドに迅速にデプロイ

製品

- Proofpoint Cloud App Security Broker（以下、Proofpoint CASB）
- Proofpoint CASB IaaS Protection

クラウドの採用は増加しています。より高いアジリティ、順応性、拡張性を求めてビジネスや IT チームが SaaS アプリを導入するように、DevOps チームもまた同様に、新しいアプリケーションとサービスをクラウド インフラ上で開発するために IaaS を導入しようとしています。

組織は、1 つまたは複数のクラウドサービス上に数十から数百もの IaaS アカウントを持ち、そこでさまざまな作業をおこなっていることがあります。また、データプライバシー規制により、世界の別の地域にあるクラウドリポジトリにデータを保管しなければならないことがあります。クラウドセキュリティのギャップが可視化できていないと、IaaS のセキュリティとコンプライアンスを維持することは困難です。さらに、アカウント侵害などのクラウド脅威や、スキルや人員の不足などによって状況はさらに複雑化します。

顧客による設定ミス、管理ミス、間違いが大規模なセキュリティ侵害につながることがあります。これらを見落とすと、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) などのクラウドサービスへの攻撃に繋がります。セキュリティ / リスク管理責任者は、こういったリスクを識別し、リスクを低減する必要性に迫られています。IaaS アカウント、リソース、クラウドストレージ内の機密データ（顧客や患者の記録など）は確実に保護しなければなりません。

Proofpoint CASB IaaS Protectionは、IaaS 環境を保護しコンプライアンスを維持するために以下を提供します。

- IaaS ディスカバリ
- クラウド セキュリティ ポスチャ マネジメント (CSPM)
- データセキュリティ
- 脅威対策
- アダプティブ アクセス コントロール

Proofpoint CASB IaaS Protection は Proofpoint CASB のアドオン機能です。

IaaS 環境での設定ミスを識別

Proofoint CASB IaaS Protection は、マルチクラウド環境のセキュリティ体制管理を支援します。これは Proofpoint CASB 機能の1つで、IaaS サービスの公開ベースラインに合致しない構成や設定（多要素認証を行っていない「root」ユーザーアカウントなど）を発見します。Proofoint CASB IaaS Protection は、次の4つのセキュリティ ベースラインを基に、仮想マシン、ストレージ、ネットワーク、アクセス制御の設定を評価します。

- CIS Foundations
- PCI DSS
- ISO 27001
- SOC TSP

セキュリティリスクとなる設定ミスを発見した場合は、それを修正するためのベストプラクティスを提供します。

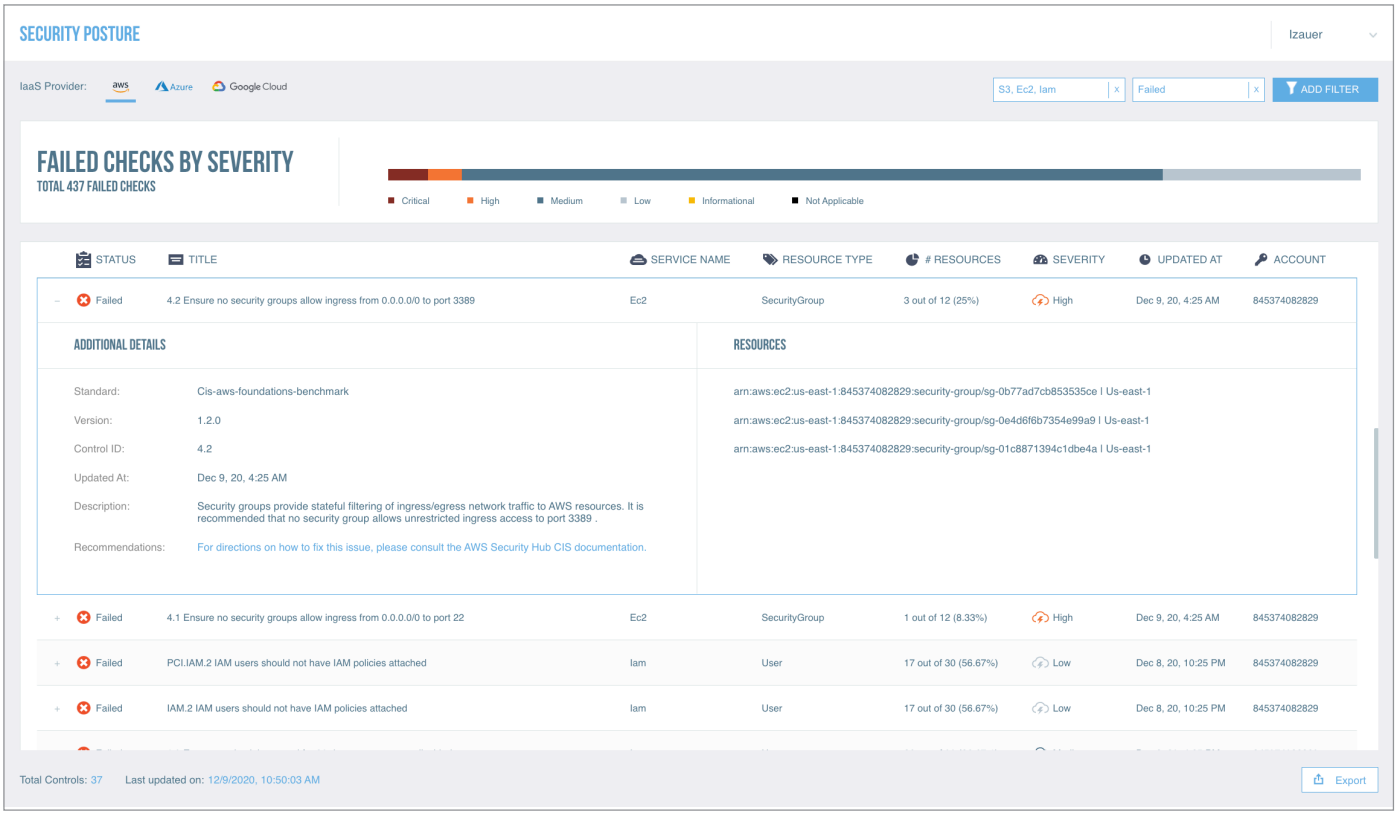

図1：設定ミス、セキュリティ ベースラインの達成方法、基準に満たないリソースのリストを表示するセキュリティ ポスチャ ダッシュボード

特権ユーザーのアクティビティを監視し制御

SaaS アプリケーションとは異なり、IaaS ユーザーのほとんどは DevOps エンジニアやソフトウェア開発者などの特権ユーザーで、仮想マシンやクラウドストレージなどの IaaS リソースをデプロイ、削除、構成することができます。また、管理者権限の割り当ても行えます。特権ユーザーのアクティビティを監視することは非常に重要です。

IaaS Protection を装備する Proofpoint CASB では、People-Centric なポリシーを設定できます（図 2）。これらのポリシーは豊富なコンテキストを用いて、未承認の特権ユーザーのアクティビティにアラートを出します。このコンテキスト情報には、ユーザーリスク、ロケーション、デバイス、ネットワーク、また、ユーザーがアクセスしようとしているクラウドアプリも含まれます。たとえば、ブロック対象リスト内の国からバケットアクセス権限が変更される、などという管理アクティビティを阻止することができます。

図 2：特権ユーザー アクティビティ用のポリシー ルール テンプレート

あらゆる IaaS リソースを発見

Proofpoint CASB では、複数のクラウドと地域に渡って IaaS のセキュリティとコンプライアンスを一元管理できます。また、SaaS アプリおよび、複数の IaaS ベンダー、アカウント、地域に存在する IaaS リソースを可視化します（図3）。

リソース作成の傾向を可視化し、リソースの過剰な作成や削除などといった異常アクションの発見に役立てます。また、発見したリソースをタイプや地域別で掘り下げて調べ、アカウントが規制やベストプラクティスに沿って作成されているかを確認できます。たとえば、多国籍または欧州の組織では、GDPR 違反を防止するため、EU 外にデプロイされたバケットがないかを監視します。

プロビジョニングされていない IaaS アカウントの発見

Proofpoint CASB はシャドー IT（IT 部門が承認や文書化していない IaaS アカウントを含む）を可視化します（図4）。ネットワーク トラフィック ログの監査も可能になります。自社ネットワークでアクセスされたクラウド アプリと IaaS アカウント（IT 部門にて承認済み、文書化されていない、プライベート用の可能性のある IaaS アカウントを含む）を可視化します。未承認アカウントの監査をする際は、CASB コンソールでステータスをトラッキングできます。たとえば、企業合併により取得された、文書化されていないアカウントが見つかった場合、規制に準拠するようにセキュリティ ベンチマークに基づいてプロビジョニングすることができます。

図3：リソースの傾向、ロケーション、タイプを表示する IaaS ディスカバリ ダッシュボード

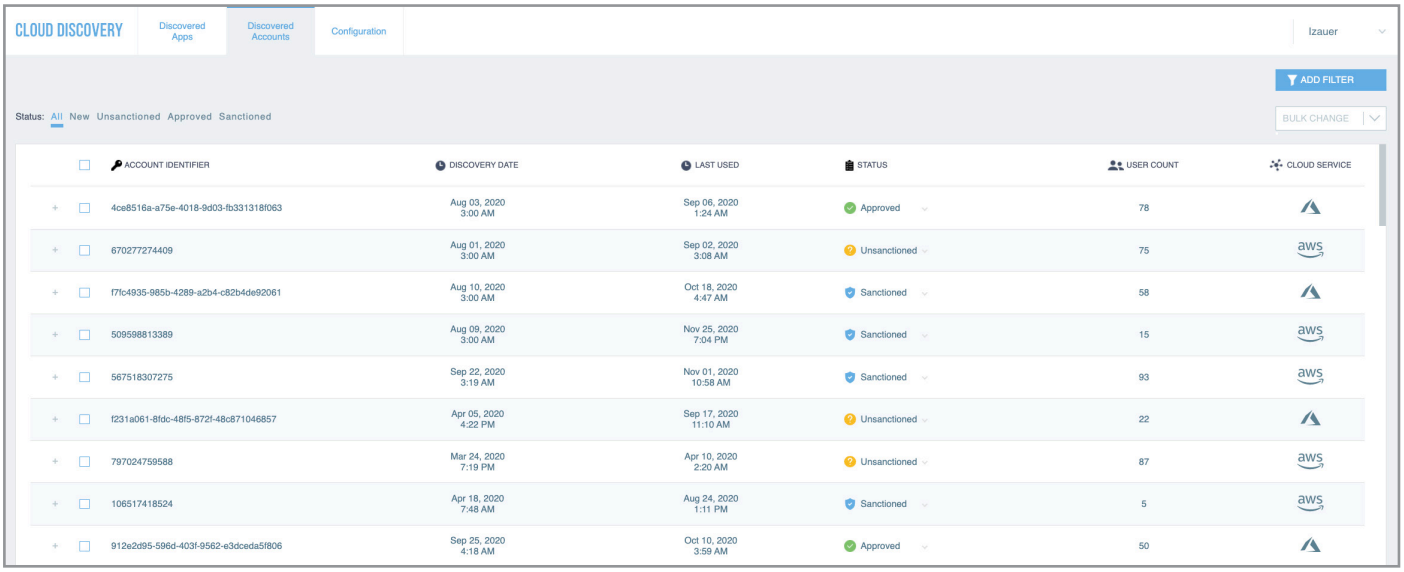

図4：自社ネットワーク上で発見された IaaS アカウントのステータスを示すダッシュボード

クラウドストレージ内の機密データの保護

IaaS Protection を装備した Proofpoint CASB は、AWS S3 バケットや Azure Storage Blob コンテナなどといったクラウド ストレージ リポジトリ内の機密データを特定し分類します。また、以下も可能にします。

- ファイルアクティビティを監視して DLP の違反を発見
- バケットとコンテナを監視して、過度の共有がされていないか確認
- DLP クラシファイア（他の Proofpoint DLP 製品と共有される、ビルトインのスマート識別子、ディクショナリ、ルール、テンプレートなど）を用いてデータ セキュリティ ポリシーを構築

このアウトオブボックスのクラシファイアは難しい設定なく、すぐに利用することができ、クラウドストレージに保存された規制対象データを発見して保護するまでの時間を短縮できます。また、コンプライアンス維持にも役立ちます。Proofpoint CASB は Proofpoint Enterprise DLP の一部として、SaaS アプリ、IaaS バケット、メール、エンドポイントで、一貫した DLP ポリシーを展開します。また、これら複数のチャネルで発生する DLP インシデントを 1 つのコンソールで集中管理します。複数のチャネルのコンテンツ、行動、および脅威テレメトリーを組み合わせて、DLP アラートの原因となったユーザーが、侵害を受けているのか、悪意があるのか、または過失であるのかを把握します。

Proofpoint CASB DLP の機能には以下が含まれます。

- 240 のビルトインのクラシファイアは PCI、PII、PHI および GDPR の諸規制をカバー
- ディクショナリと近接マッチングで DLP の検知機能を向上
- 正確なデータマッチング（EDM）によって、カスタム辞書または識別子を自動アップロードして組織固有の情報（アカウント番号や、データベース内のその他の構造化データを含む）を検知
- 文書のフィンガープリントを作成し、非構造化コンテンツ内の機密データ
  （数式、ソースコード、フォーム、契約、その他の知的財産等）を検知
- 300 種類のファイルタイプと、新しいカスタムまたは占有ファイルタイプに対応するファイルタイプ プロファイラーをサポート

柔軟なルールテンプレートを用いて、コンテンツ、ユーザーの行動、脅威対策ポリシーを構築でき（図 5）、データがどのように共有され、アップロードされ、ダウンロードされるかという方法を制御できます。またコンプライアンス維持のため、バケットの共有権限を自動的に減らすこともできます。たとえば、ブロック対象リスト内の国からのバケットの過剰共有を監視して削除できます。

DLP インシデントの調査も簡単になります。不審なログインや設定ミスのあるバケットを、DLP インシデントに関連付けできるようになります。また、レポート用にイベントとアラートをフィルタリングでき、アラートの受信登録をするとコンプライアンス状況の監視もできます。

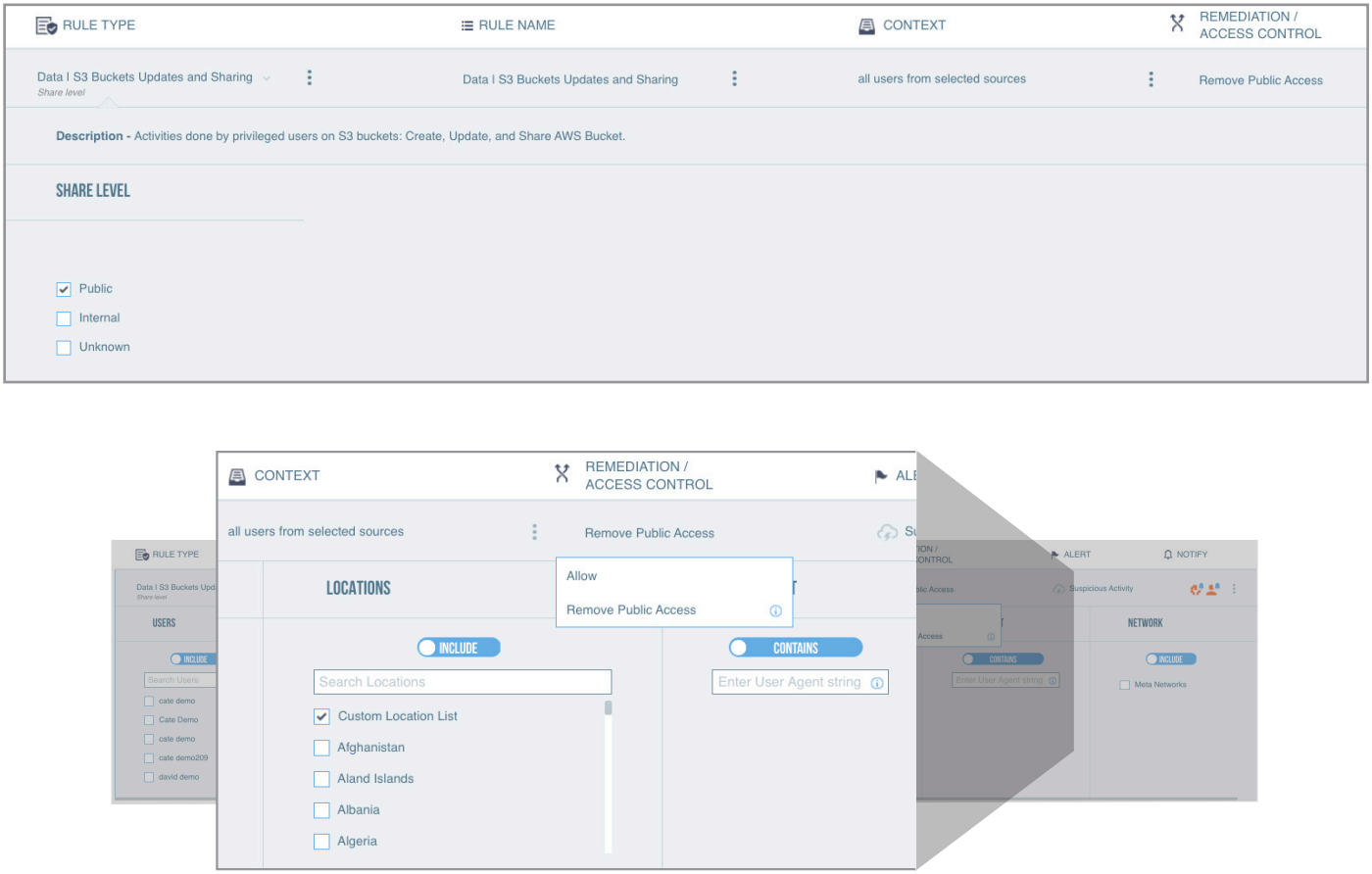

図 5：バケット / コンテナの共有権限を監視するポリシー ルール テンプレート

アダプティブ アクセス コントロールと脅威対策

IaaS 管理コンソールは Web ベースのアプリケーションで、クラウドリソースの作成と管理に用いられます。このツールは影響力が大きいため、このツールへのアクセスには監視と制御が必要です。また、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。これにより、以下を提供します。

- 高リスクな地域やネットワーク、また既知の攻撃者からのアクセスをブロックするポリシーを設定し、IaaS 環境を保護できます。
- 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。

Proofpoint CASB は、Proofpoint Nexus Threat Graph から得られる攻撃経路（クラウド、メールなど）についての脅威インテリジェンスを、ユーザー毎のコンテキストデータと組み合わせます。このデータを機械学習に取り込み、ユーザーの行動を分析し、さまざまなクラウドサービスやテナントに渡って異常を検知します。これにより以下が可能になります。

- クラウドアカウント侵害を検知
- 過去のアクティビティやアラート（フェデレーションする IaaS サービスへの不審なアクセスなど）を調査

詳細

詳細は proofpoint.com/jp でご確認ください。

Proofpoint | プルーフポイントについて

Proofpoint, Inc.（NASDAQ:PFPT）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 1000の過半数を超える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。