Proofpoint Spotlight

アイデンティティの脆弱性を攻撃者が悪用する前に、自動的に検知、優先順位付け、修復

主なメリット

- 攻撃チェーンの複数の段階でのアイデンティティリスクの検出
- Active Directory、Entra ID（旧称: Azure AD）、PAM、エンドポイント、LAPSにおいてアイデンティティを可視化
- エンドポイントで見つけ出すことができるアイデンティティ脆弱性についての優先順位付きリストを自動的に取得
- 「シャドウアドミン」などの脆弱性を手動または自動で修復
- ドメインとトラストエンタープライズマップにより、子会社や新たに取得した企業のリスクを可視化
- アイデンティティのセキュリティ態勢を強化するための長期的なリスクトレンドに関するインテリジェントなレポート

認証情報の窃取と悪用は蔓延しており、増大する懸念となっています。攻撃者はその焦点を、システムベースの脅威からアイデンティティを標的とした攻撃へと移行させています。攻撃者はそのような攻撃を数時間から数分で完了させることができます。侵害やマルウェアの痕跡を残すことはありません。

特権アカウント管理（PAM）や多要素認証（MFA）を実施しているにもかかわらず、企業のエンドポイントの6分の1で、引き続き脆弱なアイデンティティがあることが確認されています。これらはサイバー攻撃者にとって主要な標的です。ランサムウェアなどの標的型脅威は、その達成手段として特権アイデンティティに焦点を合わせています。

Proofpoint Spotlightは、アイデンティティが悪用されるリスクを低減するのに役立ちます。このソリューションは、Proofpoint ITD (Identity Threat Defense) プラットフォームの構成要素です。アイデンティティの脆弱性を継続的かつ包括的に検知し、その脅威を自動的に修復します。Spotlightは、本格的な侵害へと発展する前にアイデンティティの脅威に対処します。

セキュリティアラートへの対応は、ビジネスへの影響を防ぐことが目的ですが、そのアラート数が増えるにつれてノイズの量も増え、セキュリティチームはその見分けに時間を割かなければなりません。この問題を解決する為、国防に関わっていたエンジニアが脆弱性への対応タスクに対して優先順位を付けるSpotlightを開発しました。

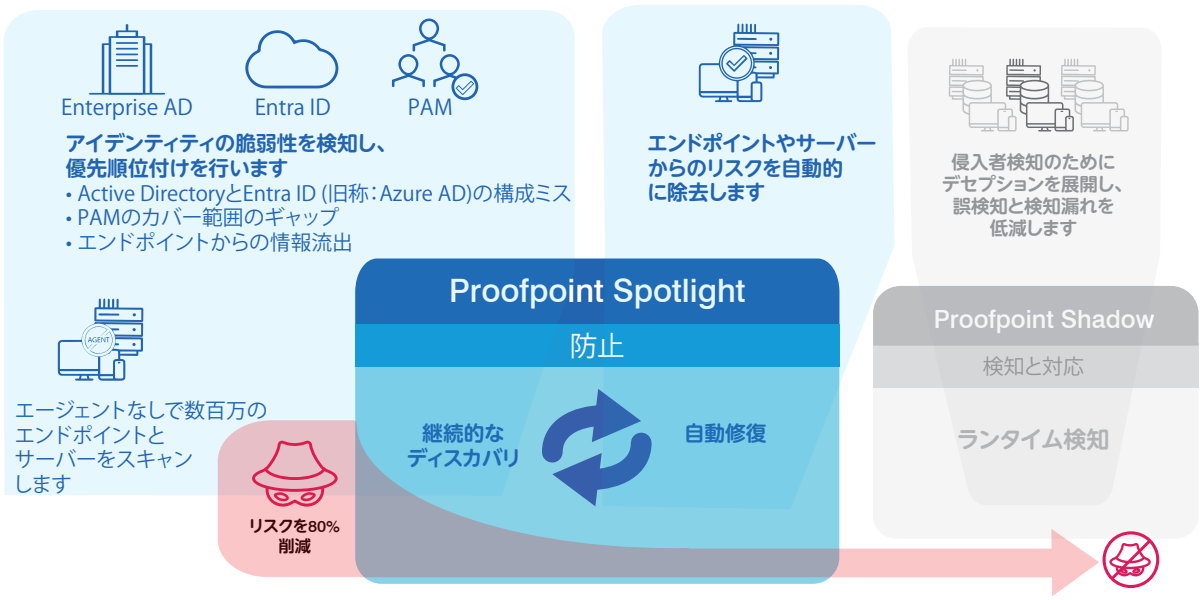

図1: Proofpoint Identity Threat Defenseの構成要素であるProofpoint Spotlightは、特権アイデンティティの脆弱性とポリシー違反を継続的に検知して修復します。

攻撃者が特権アイデンティティを悪用する方法

攻撃者はまずホストを侵害しますが、通常はそれが最終標的ではありません。ほとんどの攻撃では、攻撃者は特権を昇格しようとします。検知されずに最終目標に到達するために、環境内でラテラルムーブメントを実行します。Bloodhound、Cobalt Strike、Mimikatz、ADFindなどのツールを使い、特権認証情報を素早く悪用し、自らの存在を隠します。

当社の調査では、90%以上の組織が過去1年間にアイデンティティ関連の侵害を経験しています。ランサムウェア攻撃は記録的なレベルに達しています。この増大には多くの理由があります。その1つは、アイデンティティとアクセスの管理システムのデプロイが非常に複雑だということです。アイデンティティも絶えず変化しています。組織は環境のギャップについての完全な可視性を得ることができません。

さらに以下のような理由もあります。

- サービスアカウント、ローカル管理者、特権ドメインの認証情報のPAM設定や管理が不十分または不適切である
- 過剰な特権を持つ「シャドウアドミン」アカウントを意図せず作成している
- RDPセッションの終了が適切でない
- エンドポイントに認証情報やクラウドアクセス トークンをキャッシュするユーザーアプリケーションがある（ブラウザ、SSH、FTP、PuTTY、データベースなどを含む）

実際にあった攻撃の例：保険会社が受けた攻撃

攻撃者は、クレデンシャル スタッフィング攻撃によって、リモートデスクトッププロトコル（RDP）を介してネットワークにアクセスしました。攻撃者は、窃取した認証情報を最初のアクセスに使用しました。

そこから攻撃者はドメイン管理者へと特権を昇格させました。重要なデータは暗号化されてしまい、一部は流出しました。この組織は攻撃から回復するために4000万ドルの身代金を支払いました。

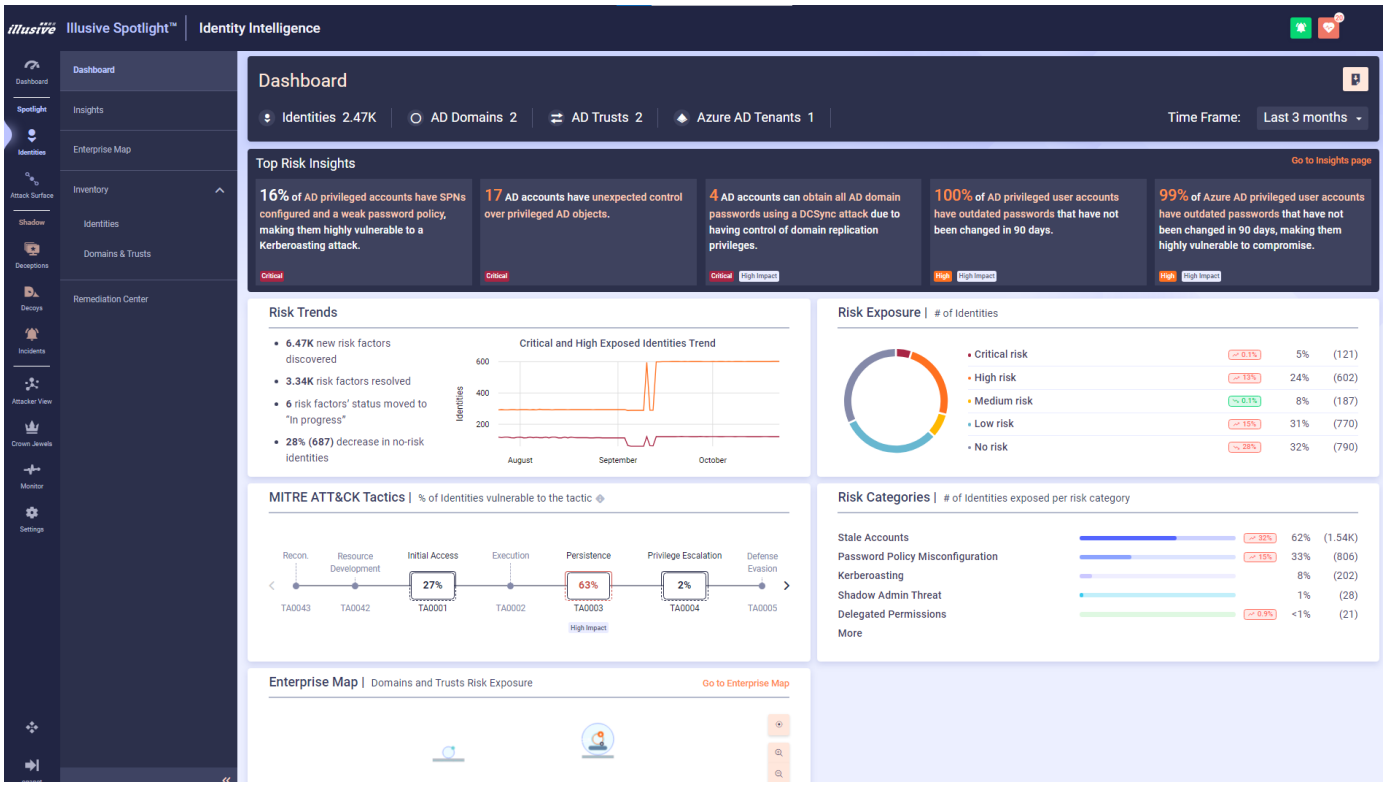

図2: Proofpoint Spotlight アイデンティティ リスク ダッシュボード。

脆弱なアイデンティティの発見、優先順位付け、修正

Spotlightは、アイデンティティセキュリティポリシーと実際の環境とのギャップを明らかにします。以下のシステムをスキャンし、現在のアイデンティティの脆弱性を完全に可視化して、優先順位付けを行います。

- **ディレクトリ構造。** Active DirectoryとEntra ID（旧称：Azure AD）
- **PAMソリューション。** CyberArkとDelinea Centrify
- **エンドポイント。** クライアントとサーバー

Proofpoint Spotlightは、重大な侵害に発展しかねない犯罪の遂行に攻撃者が必要とするアイデンティティの脆弱性を取り除くことで、攻撃を阻止します。

詳細はこちら

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.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 75% 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。