Proofpoint Shadow

リアルタイムに、権限昇格とラテラルムーブメントを阻止

主なメリット

- 攻撃者の早期検知と包括的な脅威調査を実現します
- 高精度のアラートを提供することで、SOCにおける誤検知を低減します
- エージェントレステクノロジーは、IT部門の少しの関与だけで簡単に導入することができます
- IT環境の変化に応じて動的に調整することで、継続的な防御を提供します
- 100万を超えるエンドポイントのネットワークで拡張性を実証済みです
- シグネチャやアノマリベースの脅威検知で対応できないリスクに対応します。

サイバー攻撃の90%以上は、リスクのあるアイデンティティが関係しています。攻撃者は、システムへの直接侵入ではなく、特権アイデンティティを標的とすることに戦略を変化させています。この変化は、ランサムウェア攻撃やデータ侵害による被害の急増につながっています。脆弱なアイデンティティに焦点を合わせることで、攻撃者は攻撃のタイムラインを数か月から数日、場合によっては数時間に短縮することができます。

この課題をプルーフポイントが解決します。プルーフポイントの強力な Proofpoint Shadow ソリューションは、エンドポイント環境に罠を張り巡らせることによって、検知の困難な攻撃者によるラテラルムーブメントを検知することができます。Proofpoint ITD (Identity Threat Defense) プラットフォームの構成要素である Shadow は、エンドポイントの正規の経路のように見せかけたデセプションを配置することで、攻撃者を決定論的な手法で捕捉します。

他のツールとは異なり、Shadow はシグネチャーや挙動に基づく分析に依存しません。また、脆弱性を悪用される可能性のあるエージェントやハニーポットも使用しません。それらの仕組みを使わなくても、Shadow のエージェントレスアーキテクチャでは、攻撃者に気づかれることなく侵入を検知することができます。Shadow は、Microsoft、Mandiant、米国防総省、Cisco など、世界トップクラスのセキュリティ組織との160回以上のレッドチーム演習において、防御に成功してきました。

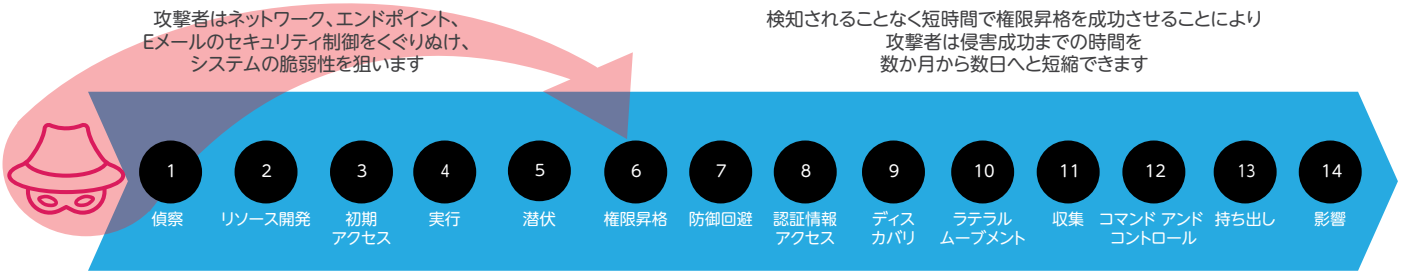

図1: 攻撃者は現在、攻撃チェーンにおける主要な経路として、脆弱なアイデンティティに焦点を合わせています。

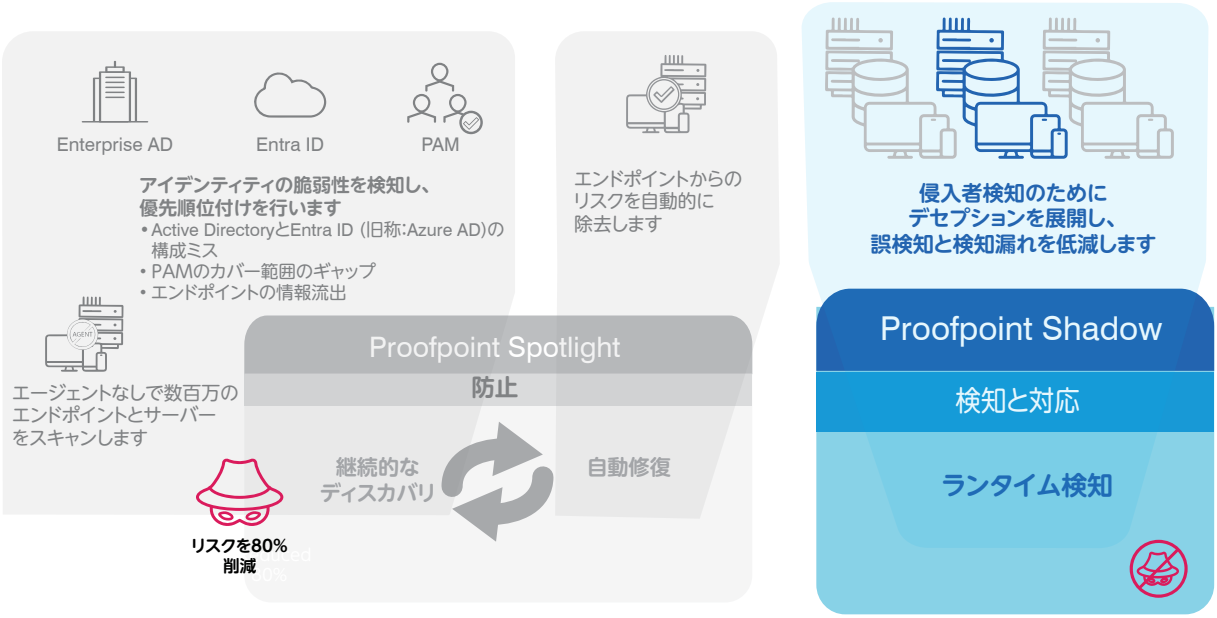

図2: Proofpoint ITD (Identity Threat Defense) プラットフォームの構成要素である Proofpoint Shadow は、ネットワーク内での攻撃者のラテラルムーブメントを検知して警告する罠を張り巡らせます。

確率論的検知から決定論的検知への移行

脅威を検知するには、様々な方法があります。例えば、実行ファイルの特殊なパターンやシグネチャを探すことに加えて、潜在的な攻撃者の行動に基づいてログ等を分析する方法もあります。しかしながら、従来のツールでは、攻撃者が特権昇格したり、検知されずネットワーク内でラテラルムーブメントを行うような深刻な攻撃は、多くの場合捕捉することができません。この侵入の検知に失敗すると、攻撃者にアカウントを乗っ取られたり、ランサムウェアをばらまかれたり、データを盗まれるなどの被害に繋がります。セキュリティチームがこのような攻撃に対して先手を打つには、より高度で信頼性の高いアプローチが必要です。

Shadowは決定論的なアプローチを提供します。ネットワーク内の広範囲にデセプションを配置することにより、攻撃者の初期侵入から目的を遂行するまでの一連のアクティビティを追跡することができます。それらのデセプションは、企業のエンドポイントの深部に隠されています。それらは、攻撃者が探している実際のファイル、RDPセッション、データベース接続、Eメール、スクリプトなどのように見え、なおかつ動作します。攻撃者がそのいずれかに手を出すと、Shadowはフォレンジックを利用したリアルタイムアラートをセキュリティチームに送信します。チームはこの情報をもとにインテリジェントな選択を行い、攻撃を食い止めてビジネスに被害が及ばないように保護することができます。

エージェントレスの検知と保護

Shadowの独自のエージェントレスで身元を隠すバイナリアプローチは、IT管理者とセキュリティチームの双方にとって助けとなります。インテリジェントな自動化と軽いリソース使用量により、ITへの影響は最小限に抑えられます。ソフトウェアエージェントに依存するセキュリティツールとは異なり、攻撃者はShadowをオフにしたり回避したりすることはできません。

75以上のデセプション手法

Shadowは75以上のアクティブなデセプション手法を駆使します。フェイクのファイルやファイル共有、データベース接続、FTPやRDP/SSH接続、ブラウザの履歴やURL、Windows認証情報、ネットワークセッション、Eメール、スクリプト、さらには過去のTeamsのチャットさえも作成し、それらは攻撃者の目には価値ある本物のように映りますが、実際には隠された「仕掛け線」として機能します。これらの手法は連動して、環境の内外を問わずどこから侵害の試みが開始されても、攻撃者をその攻撃の最中に捕捉できます。

Shadowを使えば、セキュリティチームは、本物そっくりにカスタマイズされた何百ものフェイクのWordファイルやExcelファイルを自動作成することができます。それには会社のロゴやレターヘッドさえ入れることができます。文書内のフェイクデータは、攻撃者がそれを使用してさらにアクセスを得ようとした場合には、セキュリティ管理者にアラームを出すようになっています。

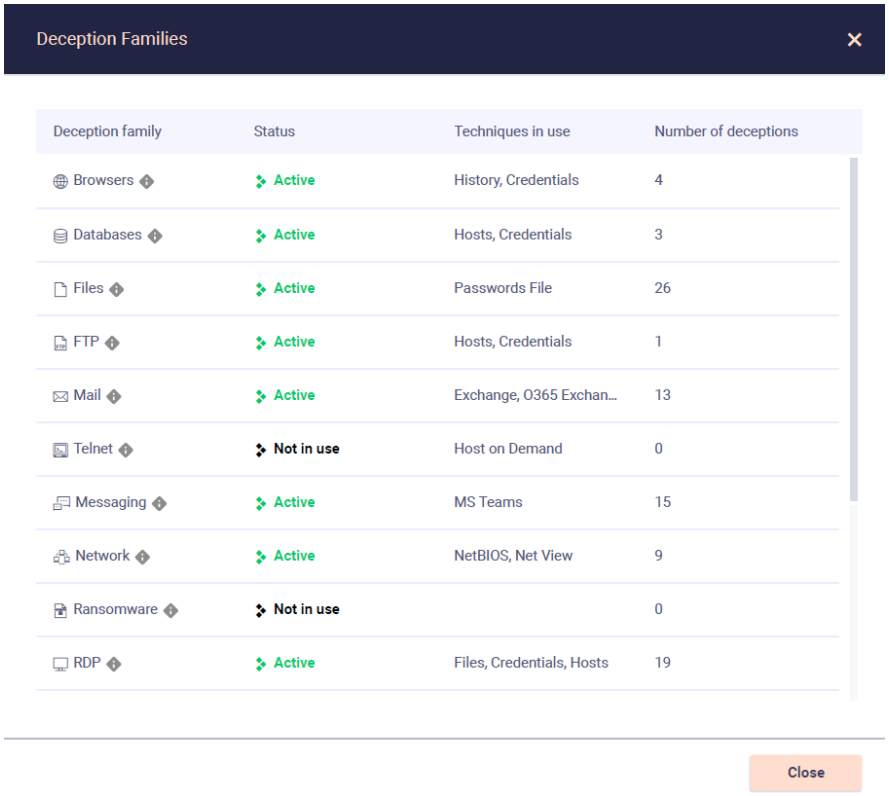

図3: Proofpoint Shadowユーザーインターフェース。

各エンドポイントにカスタマイズされた自動デセプション

Shadowのインテリジェントな自動化システムは、攻撃者の目にはリアルな迫真のデセプションを作成します。簡単に導入して拡張でき、セキュリティチームに余分な負荷をかけることもありません。Shadowによってエンドポイントの状況を分析し、各マシンに合わせたデセプションを設計し、それをワンクリックでデプロイできます。このソリューションはさらに、時間の経過とともにデセプションを調整して管理するという継続的なプロセスにも対応します。

攻撃者の観点からのビュー

Shadowの管理コンソールは、攻撃者のアクティビティに関する豊富なフォレンジックを提供します。セキュリティチームは、攻撃者が重要なアセットからどれほどの距離にいるかという重要なデータを得ることができます。また、攻撃者がデセプションの罠に掛かったときに何をしていたかをすべて時系列で表示することもできます。これにより、デセプションが攻撃者の視点からはどのように見えているのかをセキュリティ アナリストは把握できます。

詳細はこちら

詳細は、proofpoint.com/jpでご確認ください。