

Proofpoint AEP (Active Exploits Protection)

実行前の初期段階でエクスプロイトを阻止



主なメリット

- ペイロードの実行やエンドポイントの侵害の前に、メールの入口でエクスプロイト活動を特定し、阻止することで、クラス最高の初期段階エクスプロイト保護を提供します。
- 実際に観察されたアクティブエクスプロイトに基づいて脆弱性に優先順位を付けます。
- パッチが展開される前に露出を減少させ、エクスプロイト駆動のマルウェアやコマンドアンド コントロール活動から保護します。
- 現在および過去の脅威コンテキストと、継続的に更新される脅威インテリジェンスにより、調査を加速します。
- AIおよびエージェント駆動のセキュリティワークフローに備えます。

概要

エクスプロイトの速度と規模が増加しています。新しい脆弱性が記録的な量で公開されており、攻撃者はそれらをより早く武器化しています。従来の脆弱性管理および露出管理ソリューションは、通常、深粒度スコアや理論的リスクに基づいて優先順位を付けますが、攻撃者が実際にどのような悪用を試みているかを捉える可視性を欠いています。

Proofpoint AEP (Active Exploits Protection)は、そのモデルを刷新します。

メールやネットワークのトラフィックを介したエクスプロイト配信の初期段階の可視性を活用することで、プルーフポイントは、ペイロードが実行される前に、組織が悪意のある活動を特定できるようサポートします。このソリューションは、実世界のエクスプロイトインテリジェンス、敵を意識した優先順位付け、即時保護機能を組み合わせて、セキュリティチームが最も重要なことに集中し、露出を早く減少させるのを助けます。その結果、攻撃チェーンの早い段階で攻撃を防ぐことを中心に構築された、よりプロアクティブなエクスプロイト防御アプローチが得られます。

ソリューション: 初期段階エクスプロイト インテリジェンスと即時保護

Proofpoint AEP (Active Exploits Protection)は、実世界のエクスプロイトインテリジェンスを実行可能な保護と優先応答に変換します。このソリューションは、攻撃者視点のエクスプロイトインテリジェンス、メールおよびネットワークベースの脅威検出、さらに運用統合を組み合わせることで、組織が実行前にエクスプロイト活動を特定し、阻止するのを支援します。

先進的な攻撃の多くの起点となる、メールから得られる初期段階のエクスプロイト可視性を活用することで、プルーフポイント は攻撃チェーンの最も早い段階でエクスプロイト配信の試みや実際の攻撃者の行動を特定できます。

この独自の脆弱性インテリジェンスとネットワークおよびエクスプロイト駆動の脅威に対する広範なカバレッジを活用することで、Proofpoint AEPは、アクティブなエクスプロイトに基づいて脆弱性の優先順位を付け、パッチ適用ウィンドウ中の露出を減少させ、実行可能な脅威インテリジェンスで調査を加速します。

理論的リスクよりもアクティブなエクスプロイトを優先する

ただCVSSスコアの高さに目を向けるのではなく、アクティブなエクスプロイトに関連する脆弱性に対する修復作業に注力する必要があります。

Proofpoint AEPは、グローバルなテレメトリソース全体で観察された攻撃者の行動とエクスプロイトインテリジェンスを関連付け、組織が即座に運用リスクをもたらす脆弱性を特定できるようにします。

この攻撃者視点のアプローチは、セキュリティチームが不要な情報を削減し、優先順位の精度を向上させ、最も悪用される可能性が高い脆弱性にリソースを集中するのに役立ちます。

主な機能は以下のとおりです。

- アクティブに悪用されているCVEに基づいてアセットのパッチ適用を優先する
- 緊急の脅威を低優先度のリスクから区別する
- リアルタイムのIPおよびドメインの評判フィードを含む明確で実行可能な脅威コンテキストでパッチの優先順位をガイドする
- 実際の攻撃者の活動に基づいて優先順位を見直すことで、運用上の焦点を改善する

パッチ適用中でも即時保護を実現

パッチ適用には時間がかかります。Proofpoint AEPにより、組織は、継続的に更新されるエクスプロイトインテリジェンスを提供し、メールおよびネットワークトラフィック全体で即時保護を可能にすることで、この期間において露出を減らすことができます。

高度な脅威に対するタイムリーで高精度な検出ロジックを提供します。

主な機能は以下のとおりです。

- 攻撃チェーンの早い段階での保護を改善するために設計された継続的に更新されるエクスプロイトインテリジェンス
- IDS、IPS、NGFW、および関連するセキュリティ制御のためのネットワークベースの検出ルール
- マルウェアのコールバック、ドロップパー、コマンド アンド コントロール、難読化、エクスプロイトキット関連の脅威および情報漏えいのための高精度なシグネチャ
- 変化する脅威状況に対応するための毎日のルール更新
- 主要なマルウェアファミリー、攻撃キャンペーン、およびネットワークベースの脅威ベクトルに対するカバレッジ
- SuricataおよびSnort対応のデプロイを含む、広く使用されているIDSおよびIPSフォーマットのサポート

マルウェアの配信

コマンド アンド コントロール通信

エクスプロイトキット

認証情報のフィッシング

攻撃の拡散

ランサムウェア、ボットネット

プロトコルとアプリケーションの異常

コインマイニング

分散型サービス拒否攻撃(DDoS)

監視制御およびデータ取得(SCADA)攻撃

グローバル脅威インテリジェンスでセキュリティツールを強化

Proofpoint AEP (Active Exploits Protection)は、ファイアウォール、IDS、IPS、NGFW、UTM、SIEM、認証システム、脅威ハンティング プラットフォーム、インシデント レスpons ワークフロー、カスタムセキュリティツールなど、幅広いセキュリティツールと統合される実用的なインテリジェンスを提供します。

このソリューションは、疑わしいおよび悪意のあるIPアドレス、ドメイン、マルウェア、シグネチャ、キャンペーン、および関連する攻撃活動に関する評判と脅威インテリジェンスを提供します。

主な機能は以下のとおりです。

- IP、ドメイン、マルウェアハッシュ、シグネチャ、およびメッセージテキストに関する現在および過去の脅威インテリジェンス
- 脅威カテゴリと信頼度スコアで整理されたIPおよびドメインの評判フィード
- 現在の活動を反映するための積極的なエイジングを伴う頻繁なフィード更新
- ピボット、詳細分析、調査のための検索可能なグローバル脅威データベース
- TXT、CSV、JSON、IDS、圧縮形式など、運用統合のための複数のフィード形式
- SIEM、TIP、インシデント レスpons、内部ツールのためのAPIベースの強化

検知の正確性を向上させ、ノイズを減少

Proofpoint AEPは、実世界の脅威観察、マルウェア分析、グローバルセンサーのフィードバック、および専用の脅威研究に基づいて構築されています。これにより、高精度の検出が可能になり、既存のネットワーク セキュリティツールにおける誤検知を減少させることができます。

主な機能は以下のとおりです。

- 観察された脅威に基づく研究主導の検出コンテンツ
- 実行後のネットワーク動作をキャプチャするマルウェアサンドボックス分析
- 検知精度を向上させる、グローバルセンサーのフィードバック
- アナリストのワークフローをサポートするシグネチャの説明、参照、ドキュメント
- 組織の優先事項に沿ったカテゴリベースのポリシー強制

AI駆動のワークフローで拡大

Proofpoint AEPIは、先進的なインテリジェンス駆動のセキュリティ オペレーションをサポートするように設計されています。将来の機能は、MCPおよびエージェントベースのワークフローを通じて脅威インテリジェンスへのアクセスを提供し、APIおよびAI駆動のユースケースを可能にすることが期待されています。

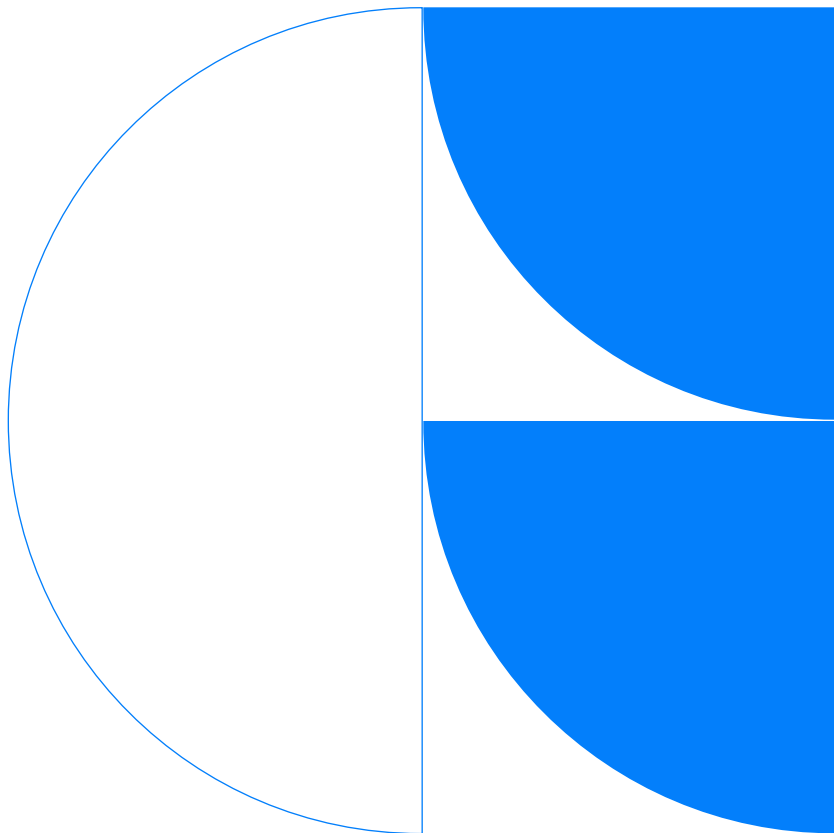
これらのワークフローは、チームが優先順位の高い脅威インテリジェンスを自動化されたセキュリティオペレーションに直接組み込むことを支援し、意思決定を加速し、手動トリアージを削減することを目的としています。

まとめ

Proofpoint AEP (Active Exploits Protection)は、メールから得られる最先端の初期段階エクスプロイト可視性、敵を意識したエクスプロイトインテリジェンス、および即時保護機能を組み合わせることで、組織が侵害される前にエクスプロイト駆動の攻撃を防ぐのを支援します。

脆弱性の重大性スコアや理論的な露出モデルにのみ依存するのではなく、Proofpoint AEPは、セキュリティチームが現実の世界で攻撃者が積極的に狙っているものに基づいて優先順位を付けることを可能にします。

優先順位付け、保護、調査を統合することで、Proofpoint AEPはセキュリティチームが重要なことに集中し、即座に保護し、迅速に調査するのを助けます。



Proofpoint, Inc.について

Proofpoint, Inc.は、人とエージェント中心のサイバーセキュリティのグローバルリーダーとして、人、データ、AIエージェントがメール、クラウド、コラボレーション ツールを介しておこなう接続を保護します。ブルーポイント社は、Fortune 100のうち80社以上、10,000社を超える大企業、そして数百万の中小規模組織に対し、脅威の阻止、情報漏えいの防止、人とAIのワークフロー全体にわたってレジリエンスの構築を支援する、信頼されるパートナーです。ブルーポイントのコラボレーションおよびデータセキュリティ プラットフォームは、あらゆる規模の組織がAIを安全かつ自信を持って活用しながら、人を保護して力を発揮できるよう支援します。

詳細については、www.proofpoint.com/jpをご覧ください。

ブルーポイントとつながる: [LinkedIn](#)

Proofpointは、米国および/またはその他の国におけるProofpoint, Inc.の登録商標または商標名です。記載されているその他すべての商標は、それぞれの所有者に帰属します。