これからの NGAV が進む道とは

サイバー攻撃は増加の一途をたどっており、エンドポイントの数は増え続け、攻撃者が企業の機密データにアクセスできる機会はますます増加しています。数多くの企業はいまだに、シグネチャベースの従来のアンチウイルス ツールでこうしたエンドポイントを保護しています。残念ながら、従来のアンチウイルスでは、もっと言えば「次世代アンチウイルス」とうたわれるそれらの後継手法でさえも、企業を脆弱性から完全に守ることはできません。現代の攻撃者は、シグネチャを使わないファイルレス手法を数多く考案しています。最新型マルウェアの作成と悪用もかなり効率化されており、作成されてから 24 時間未満のものがほとんどです。本書では、このような脅威を阻止するために、セキュリティ チームが従来のエンドポイント セキュリティ手法をいかに進化させられるかについて解説していきます。

サイバーセキュリティ市場は、洗練された高度な攻撃を特定できるツールを求める声に応え続けてきました。企業が被害の状況を調査し、根本原因を追跡・特定して、被害を受けたエンドポイントを修復できるようなツールです。こうしたツールは「NGAV (Next-Gen AntiVirus: 次世代アンチウイルス)」、「EPP (Endpoint Protection Platform: エンドポイント プロテクション プラットフォーム)」、「EDR (Endpoint Detection and Response: エンドポイント ディテクション & レスポンス)」と呼ばれる技術に分類されますが、それぞれに含まれる機能の多くは重複しています。このような現状では、企業が何に投資すればよいのか判断が難しくなります。さらに問題なのは、これらの手法のうち、企業が求めるような成果が実証されている手法は 1 つもないという点です。実際 Ponemon Institute の調査では、エンドポイントの脆弱性をすべて軽減しデータ侵害を回避するには、時間とリソースが十分でないと感じている企業は 67% にも達しています [1]。また、一般的な EDR 製品は最初の攻撃ベクトルのわずか 26% しか検出できていないという SANS Institute のテスト結果もあります [2]。EPP の保護が不十分で EDR が攻撃を検出できないということであれば、レスポンスを実施しようがありません。

本書では、企業のエンドポイントを最先端の攻撃から守るために欠かせない機能を具体的に見ていきます。さらに、SecOps ワークフローの最適化とセキュリティ成果の最大化を現在と将来にわたってもたらしてくれる、これらの機能の拡張性に優れた導入戦略についても考えていきたいと思います。

強力な防御は、今も昔もセキュリティの基本

攻撃者がますます巧妙になり、潜在的な脆弱性を抱えたエンドポイントの数が増え、その多様化も進む中、脅威を 100% ブロックすることは不可能かもしれません。まして無害のアクティビティをブロックしない、および業務オペレーションを長期間中断させないという条件であれば、これは完全に不可能です。

しかしそれでも、一貫性のある統合型防御を構築することなしには、どんな検出も対応も無駄に終わるということは理解されなければなりません。EDR がすばらしい性能を発揮しても、攻撃を検出するのは被害が顕在化した後になります。検出が攻撃の後というのは、SecOps は常に受け身でいることを余儀なくされるということです。最初に被害を把握し、次に攻撃の把握と評価のための運用コストを精査し、リソースを投じて被害軽減を図るのは、一番後回しになります。EDR はエアバッグを作動させる衝突検出センサーのようなものです。確かにエアバッグで人命は助かりますが、そもそも衝突を避けるに越したことはありません。セキュリティに置き換えると、自動車衝突の回避・阻止機能に相当するセキュリティ技術を導入することで、防御第一の体制を実現できます。強力な防御体制を構築する第一歩として、組織が採用している脅威対処の方法を見直しましょう。

エンドポイント防御の 3 大要件

攻撃者が情報窃取やランサムウェア実行などの目標を達成するには、「攻撃のライフサイクル」と呼ばれる一連のイベントを完了する必要があります。ほぼすべての攻撃の成功はエンドポイントに侵入できるかどうかにかかっており、大部分の組織がエンドポイント防御策を講じているものの、感染例はいまだ後を絶ちません。

現在、最先端の攻撃者の多くが、アプリケーション脆弱性を標的とする攻撃 (エクスプロイト) と、悪意のあるファイル (マルウェア、ランサムウェア) を展開する攻撃という、2 つの基本的な攻撃手法を組み合わせています。これらの手法は個別でも組み合わせても使用できますが、それぞれには次のような根本的な違いがあります。

- **エクスプロイト**: 技術を駆使し、オペレーティング システムのコードやアプリケーション コードの脆弱性を通じてアクセス権を奪取することです。
- **マルウェア**: 感染、探索、窃取など、攻撃者の意図どおりの活動を実行するファイルまたはコードです。
- **ランサムウェア**: マルウェアの一種で、価値のあるファイルやデータを人質に身代金を要求します。通常、人質は暗号化され、攻撃者が復号キーを持っています。

このようなマルウェアとエクスプロイトの根本的な違いをふまえ、両方に対する効果的な防御策を講じる必要があります。そのためには、防御策に次のような機能を含めることが必要です。

1. マルウェア分析

脅威を取り巻く環境は現在ますます複雑化しており、最先端の企業環境を狙う脅威の多様化、大量化、先鋭化と相まって、効果的な脅威防御はますます困難になっています。既知の悪意あるコンテンツを識別するだけでなく、未知のマルウェアやエクスプロイトを検出しなければならないことも、問題をさらに難しくしています。

ターゲティング能力と回避能力を備えた巧妙な脅威に対処するには、エンドポイント防御と共有の脅威インテリジェンスを連携させ、学習と進化が可能な防御体制を確立する必要があります。IDC Research の調査によれば、セキュリティ体制強化の優先項目または最優先項目として、セキュリティ担当者の 39% が共有型脅威インテリジェンスの導入を検討しています [3]。クラウドベースの脅威インテリジェンスとエンドポイント防御を連携させれば、詳細な分析によって未知の潜在的な脅威を迅速に検出できるようになります。エンドポイントでの機械学習を実現することで、瞬時のファイル評価による不審な特徴の特定、詳細な動的分析の実行、必要に応じたベア メタル サンドボックスでの隔離を通して、回避性能を向上させたマルウェアでさえも阻止できるようになるでしょう。

2. ランサムウェア防御

ランサムウェアは真新しい存在ではありませんが、WannaCry、Petya/NotPetya、TrickBot などの大規模な攻撃は、最新のランサムウェアに対して従来の防御策がもはや効力を失ったことを教えてくれました。攻撃者の手腕は進化し続けており、マルウェアを利用することで、巧妙な手口、自動化のしくみ、ターゲティング能力、回避能力をますます洗練させています。

ランサムウェアを防御するには、一連の機能からなる「多層防御 (Defense in Depth)」をエンドポイントに実装し、攻撃ライフサイクルのさまざまな段階に対応したランサムウェアの検出と無

1.「Challenging State of Vulnerability Management Today: Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture (脆弱性管理の最新課題 : リソース、リスク、可視性のギャップがもたらすサイバーセキュリティの弱体化)」(Balbix, Inc.、Ponemon Institute、2018 年 7月) https://www.balbix.com/app/uploads/Ponemon-Survey-Vuln-Management-.pdf
2.「Endpoint Protection and Response: A SANS Survey (エンドポイント プロテクション & レスポンスに関する SANS 調査)」(SANS Institute、2018 年 6 月 12日) https://www.sans.org/reading-room/whitepapers/analyst/membership/38460
3.「Bridging Security Gaps with Network-to-Endpoint Integration (ネットワーク エンドポイント統合によるセキュリティ ギャップの解消)」(IDC Research、Konstantin Rychkov 氏、Duncan Brown 氏、2018 年 10月) https://www.paloaltonetworks.com/resources/whitepapers/bridging-security-gaps-with-network-to-endpoint-integration

効化を実行する必要があります。たとえば WannaCry の場合、カーネル権限をユーザー レベルに昇格する試みを検出し、この攻撃を無効化するエクスプロイト防御が第 1 段階となります。これに失敗した場合、親プロセスを検出し、親プロセスによる子プロセスの生成を阻止する、子プロセス制御を発動します。いずれの手法でも脅威を検出できなかった場合は、エージェントがローカル分析と機械学習を利用して、既知の WannaCry の特性を特定できる必要があります。

WastedLocker: マルウェアとエクスプロイトの融合

WastedLockerに代表されるランサムウェアは、エクスプロイトとマルウェアを融合し、搭載された数多くの最新機能を駆使してエンドポイント防御をかいくぐり、その目的を達成します。WastedLockerの利用によるこれまでの要求額は数百万ドルにも達します。WastedLockerランサムウェアでは、まず偽のソフトウェア更新によってユーザーをだまし、悪意のあるコードをWebサイトからダウンロードさせます。このコードによってカスタムのCobalt Strikeローダーが標的のシステムに配信され、WastedLockerが読み込まれます。次にWastedLockerは被害者のネットワーク上を横方向に移動します。システム管理ユーティリティを1つ以上使用することによって自身を確実に実行しながら、最終的にペイロードを配信します。

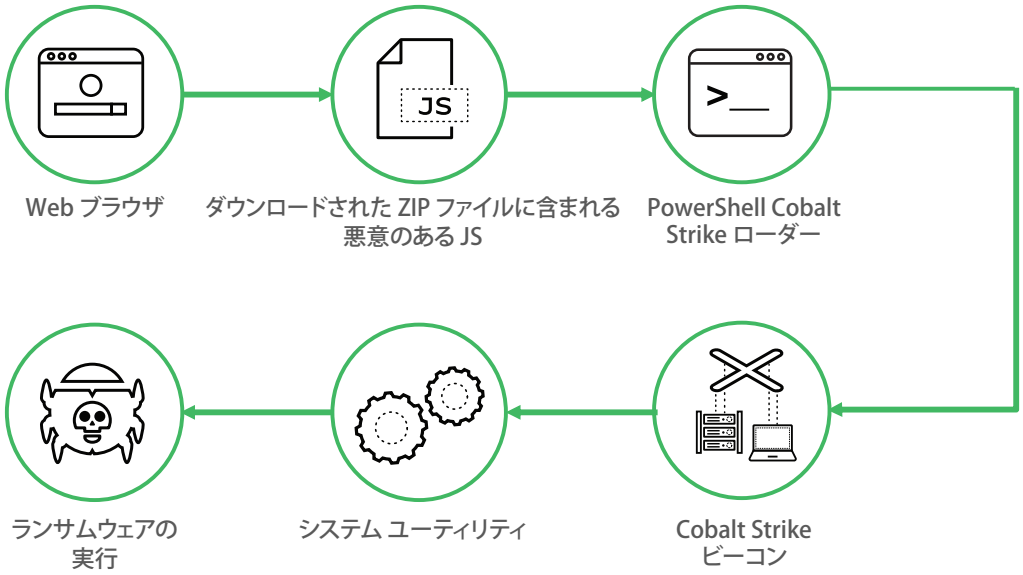

図 1: WastedLocker の攻撃シーケンス (簡略図)

3. エクスプロイト防御

ソフトウェアの新しい脆弱性とエクスプロイトは毎年数千件単位で発見されています。ソフトウェア ベンダーにはソフトウェア パッチのきめ細かな配布が求められ、あらゆる組織のシステム管理者やセキュリティ管理者にとって、パッチ管理は必須の仕事です。パッチを適用する最大の理由は、脆弱性エクスプロイトに対処することです。

エクスプロイト技術を理解する

高度な脅威の多くは、一見無害なデータ ファイルに悪意あるコードを潜り込ませるしくみになっています。これらのファイルを開くと、ファイル閲覧用ネイティブ アプリケーションが抱えるパッチ未適用の脆弱性を悪用して、悪意のあるコードが実行されます。エクスプロイトされているアプリケーションは IT セキュリティポリシーによって許可されているため、この種の攻撃は、アプリケーション許可リストによる統制を回避します。

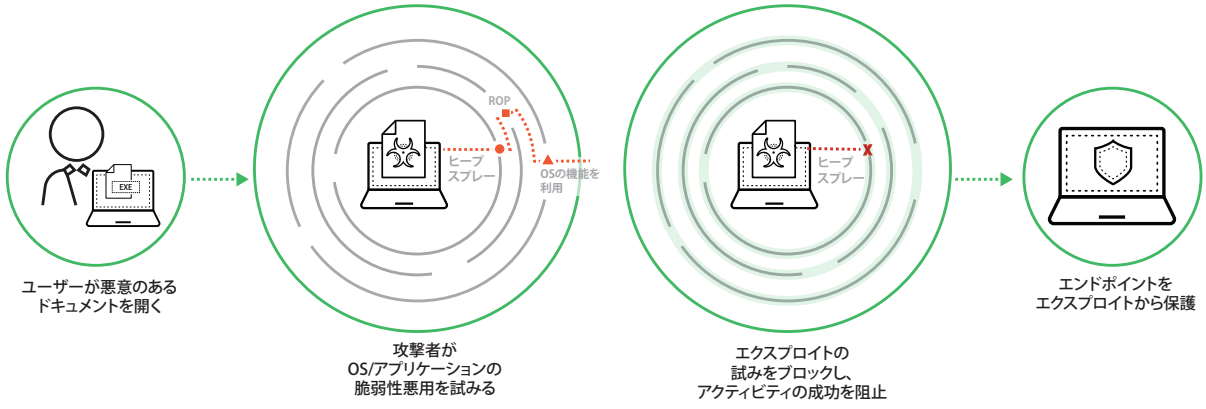

図 2: エクスプロイト自体ではなく、エクスプロイト技術に注目する

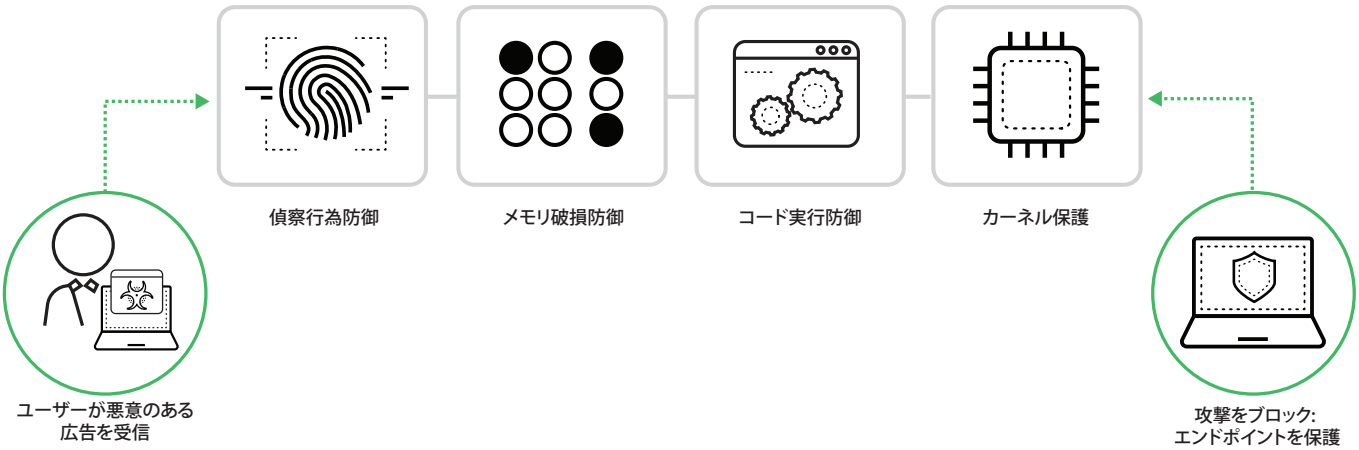

図 3: さまざまなエクスプロイト防御手法

数千もの種類があるエクスプロイトですが、実は数千種類すべてがほんの一握りの主要技術を利用しており、この共通部分にはほとんど変化がありません。つまりどのようなエクスプロイトでも、エクスプロイトがどれだけ複雑でも、攻撃者が目的を完遂するには、ゴールに向けて迷路を 1 マスずつ進むように、これら一連の主要技術を順番に実行する必要があります。

エクスプロイト防御では、あらゆるエクスプロイトが共通して使用する主要技術に焦点を当て、これらを無効化することで、パッチ適用済みかどうかに関係なくアプリケーションの脆弱性を悪用できないようにします。このアプローチは異種混在環境において特に欠かせません。たとえば多様なクラウド ワークロードを実行する環境では、物理エンドポイント制御によって仮想環境に予期しない混乱がもたらされる可能性があります。

未来を任せられるエンドポイント セキュリティ戦略を

強力な防御策に注力することは非常に大切ですが、最先端の攻撃者に対抗するにはそれだけでは不十分です。エンドポイント プロテクション ソリューションによってセキュリティ侵害の 98% をブロックできたとしても、残された 2% は、ディテクション & レスポンスによって発見し緩和しなければなりません。

このようなディテクション & レスポンス機能には、エンドポイント外をカバーすることが求められます。攻撃者はエンドポイントにとどまっているわけではないため、セキュリティ ツールにも同様の拡張が必要なのです。この点に対応できていなかったのが EDR で、リソースに限りがあるセキュリティ チームが悪意あるアクティビティの痕跡を何時間もかけて追跡しても、得られた情報はファイアウォールその他の適用ポイントでアクティビティがブロックされたことだけ、ということになりがちでした。そこでお勧めするのは、エンドポイント プロテクション & ディテクションの機能を、包括的な XDR (eXtended Detection and Response: 拡張型ディテクション & レスポンス) プラットフォームを構成する機能群として導入することです。XDR では、一元管理されたデータ ストリームに機械学習を適用し、さまざまなデータ ソースの情報をもとに攻撃を完全に可視化し、さまざまな適用ポイントを連携させながら防御策を講じることができます。XDR なら、どんな NGAV や EDR よりも射程の広い防御機能を実現し、巧妙化し続ける攻撃者と現在と将来にわたって戦うセキュリティ チームに必要な、全方位的な可視性と強力な分析機能を提供できます。

Forrester Consulting が 2020 年に実施した調査によれば、現在導入されているさまざまなセキュリティ ツールが適切に連携されているという組織はわずか 49% しかありません。彼らは、適切なデータを収集し分析に適した形式に整えるために膨大な時間を費やしているだけでなく、具体的なイベントに紐付けられるユーザー、デバイス、プロセス、アプリケーションを判断するために、複数のソースから自らデータを収集しなければならない場合さえあります。このプロセスを XDR なら自動化できます。データ ソースの違いを越えて関連性の高いアラートを結び付けセキュリティ インシデントを導き出す「アラート ステッチング」により、アナリストが日々目の当たりにする何の関係性も持たないアラートの量を大幅に減らすことができます。

アラートの量が削減されれば、セキュリティ チームの機動力は飛躍的に増加します。最先端の XDR ソリューションは、エンドポイント プロテクション / ディテクション / レスポンスを最小フットプリントでシームレスに連携し、シグネチャに依存しない防御、クラウドベースの管理インターフェイス、幅広いデータ収集に基づくイベントとアラートの記録を提供して、セキュリティ適用領域の空白をなくします。これによってセキュリティ オペレーション チームが必要とする可視化が実現されることで、エンドポイント管理を犠牲にすることなく防御第一の体制を構築できるようになります。

今後の NGAV 投資では、XDR こそ唯一の選択肢

未来のセキュリティ オペレーションに、連携性のないツールや手動のプロセスを稼働させる余地はありません。高度化を続ける脅威、充実する一方のツールを阻止するには、自動化、ビッグデータ、機械学習をより一層インテリジェントかつ綿密に活用する必要があり、新機能をすばやく包括的に展開できる統合型ツールキットも欠かせません。これからのエンドポイント セキュリティ投資は、マルウェア防御性能とエンドポイント エージェントのフットプリントだけで決めるのではなく、セキュリティ オペレーションのワークフローにどれくらいの効率化が見込めるかという、組織全体のセキュリティチーム体制に致命的な影響を及ぼす観点を考慮しなければなりません。

今後の新たなセキュリティ投資では、常に次の点を検討する必要があります。

- プロテクション / ディテクション / レスポンスのコントロールが AI と機械学習によって連携されており、セキュリティの空白を自動的に埋められるかどうか。
- コントロールが統合されており、SecOps、エンドポイントやネットワークの管理者、IR チーム間がシームレスにコミュニケーションできるか。
- セキュリティ アラートの数を削減し、質を高められるか。

- エンドポイント、ネットワーク、クラウドにわたるインフラストラクチャ全体を包括的に可視化し、検出と対応にかかる時間を短縮し、最終的に攻撃の滞在時間を短縮できるか。

XDR は、これらすべての条件を満たす唯一のエンドポイント セキュリティ ソリューションです。XDR は、ネットワーク、エンドポイント、クラウドの豊富なデータを分析と結び付け、迅速なアラートのトリアージとインシデント対応によって、各脅威の全体像と根本原因を自動的に示します。これにより、トリアージから脅威ハンティングに至るセキュリティ オペレーションの全段階を担うアナリストの負担が、時間と労力の両面で軽減されます。また、適用ポイントとの緊密な統合によって SecOps による脅威対応が迅速化されます。さらに SecOps は脅威対応から得た情報を使って防御策を最適化し、将来の脅威防御に備えられるため、次回の対応はさらに高速化されます。さらにもう 1 つ、セキュリティ アナリストの脅威対応に必要な知識とスキルのハードルが下がり、結果的にセキュリティ オペレーションのコストを削減できるというメリットもあります。

おわりに

プロテクション / ディテクション / レスポンスを連携する防御第一のアプローチを採用し、「攻撃そのもの」から「攻撃の手法」へと SecOps チームの意識を変えることで、セキュリティの空白、過剰なアラート、オペレーションの分断、攻撃の長時間の滞在という、組織が抱える 4 つの根本課題を解決できます。

今後のエンドポイント セキュリティへの投資は、「防御の連携」、「アラートの数を削減する」、「軽量なエンドポイント エージェントによる検出と対応を実現する」、「SecOps、エンドポイント管理、IR を高度な因果関係チェーンで連携する」、「エンドポイント、ネットワーク、クラウドにわたるインフラストラクチャ全体を包括的に可視化し、検出と対応にかかる時間を短縮し、最終的に攻撃の滞在時間を短縮する」という一連の目標を念頭に検討することをお勧めします。

paloalto NETWORKS

〒 100-0011

東京都千代田区内幸町 2 丁目 1 番 6 号
日比谷パークフロント 15 階

電話番号 : 03-6205-8061

www.paloaltonetworks.jp