エンドポイントを保護して
どんな場所からでも働ける
環境をつくる

目次

概要

多くの人が自宅やさまざまな場所で働くようになっている中、脅威は進化と拡大を続けており、より巧妙な攻撃や回避技術が使われることで、従来のネットワーク境界の外にいる人への攻撃が容易になっています。Forrester の最近の報告によると、74% の組織がテレワークの脆弱性を狙ったサイバー攻撃の被害に遭い、ビジネスに影響を与えたと回答しています [1]。ランサムウェアは、現在多くの企業が直面しているサイバー犯罪の中で最も恐ろしい形態の一つであり、今後もなくなることはないでしょう。FortiGuard Labs によると、2021 年 6 月のランサムウェアの週の平均の活動が、1 年前の水準の 10.7 倍に増加したと報告されています [2]。また、「ランサムウェア調査レポート」によると、ランサムウェアの標的になったことがあると回答した企業は 67% で、半数近くが複数回にわたり標的にされたと回答しています [3]。

最近のマルウェアは、さまざまな方法でシステムにアクセスできるようになっています。クリックによるアクセスが一般的ですが、中にはクリックなしでアクセスすることもあります。アクセスすると、攻撃者はマルウェアを拡散して、ネットワークを移動するエンドポイントを介してあらゆるネットワークに足掛かりを得ようとします。攻撃はきわめて広範に及ぶため、企業は備えが必要です。特にランサムウェアに直面している場合、攻撃前、攻撃中、攻撃後の問題に対処できるように戦略を構築しておく必要があります。多くの成長企業では、インシデントレスポンス計画がすでにセキュリティ戦略に組み込まれています。これにより、組織は従業員が自宅や空港などあらゆる場所にいても潜在的なインシデントのリスクや範囲を軽減し、移動するエンドポイントを保護する対策を講じることができます。

67% の企業が「ランサムウェアの標的になったことがある」と回答し、半数近くが「複数回にわたって標的にされた」と返答 [4]

はじめに

攻撃が増加する中、トロイの木馬からファイルレススクリプトまで、さまざまな手法で多様なベクターを組み合わせた攻撃が行われる傾向にあります。多くの場合、従業員は自宅や会社でフィッシング詐欺を識別できずに安全でないサイトを閲覧し、ソーシャルメディアで時間を費やし、音楽やビデオをダウンロードしています。このように、本来攻撃対象になっていないデバイスでもあらゆるところで感染してしまう可能性があります。

さらに、攻撃者は時間をかけて特定の職務内容を偵察し、従業員が大規模ネットワークに再接続したときにネットワークへ侵入します。一度侵入すると何週間にもわたって環境内に潜伏し、マップを作成し、セキュリティ制御を回避することもあります。こうした時間が攻撃者にとって、ランサムウェアのペイロードを投下したり、データの流出方法を見つけたり、その情報を人質に取る機会になってしまいます。攻撃者が長く潜伏するほど、最終的な損害も大きくなります。企業としては、重要なシステムを可能な限り迅速に保護したり復旧したりできるように包括的な予防、検知、レスポンス、復旧の戦略を整える必要があります。

インシデント前の戦略

エンドポイントは、ランサムウェアなどほとんどの攻撃における最終目的地とされるため、強力なエンドポイントセキュリティが不可欠です。このプロセスでは、各エンドポイントの攻撃対象領域を減らすことから始めます。そのためには、不要なポートや周辺機器を閉じ、システムにインストールされている脆弱なアプリケーションからの通信を制御し、脆弱性が悪用されないよう防御し、この安全な設定を維持する必要があります。

そして、脅威インテリジェンスと機械学習（ML）を組み合わせた堅牢な静的分析を使用することが重要です。分析はデバイスに追加されたすべてのコードに対して行いますが、すべてのランタイムアクティビティに対する動的な振る舞いベースの検査で脅威を検知して分析を補う必要があります。手動によるアラートのトリアージやレスポンスを待たずに、リアルタイムでアクションを実行し、進行中の攻撃を阻止できることが不可欠です。

また多くの場合、企業ではエンドポイントセキュリティだけでなく、データバックアップの頻度、場所、セキュリティに対する基本的な変更も必要になります。デジタルサプライチェーン上にセキュリティ上の不備があったり、在宅勤務する従業員がいる場合、あらゆるところから攻撃を受けるリスクが差し迫っています。SASE（セキュアアクセスサービスエッジ）、ネットワーク外デバイスの保護、ゼロトラストネットワークアクセス（ZTNA）、ネットワークセグメンテーション戦略などのクラウドベースのセキュリティソリューションでは、ポリシーやコンテキストに基づき、アプリケーションやリソースへのアクセスが制限されます。そして組織のセキュリティを確保する上で、最終的には人的要素がテクノロジーと同様に重要になります。従業員に新しいソーシャルエンジニアリング戦術を継続的に学習してもらい、検出内容やレスポンス方法を把握させることが不可欠です。

ランサムウェアからの保護

ランサムウェアは過去 10 年以上にわたり、最も多用され高度に進化したマルウェアの 1 つです。2022 年以降も攻撃者は組織への侵入方法を探り続けていくことでしょう。エンドポイントが接続するネットワークが多いほど攻撃対象としては魅力的なものになります。

こうした日常の現実に対して、エンドポイントセキュリティでは、システムにおいて悪意のある暗号化が行われていないか継続的に監視したり、ファイルアクセス監視（FAM）やファイル整合性監視（FIM）を使用したりする必要があります。エンドポイントセキュリティソリューションの目的は、マルウェアによる実行を最小限に抑えることです。

URL フィルタリング

Web は今日の急速に進化する高度な攻撃を行うための最重要な攻撃経路の 1 つであり続けています。攻撃には、ランサムウェア、フィッシング、コマンド & コントロール（C2）バックドアなどがあります。暗号化により、Web からの攻撃の多くは直接エンドポイントに到達することになります。また、ファイアウォールやエンドポイントセキュリティなど、さまざまなセキュリティ製品を通じて優れたテクノロジーにアクセスできるにもかかわらず、企業は利用ポリシーの実行に苦労しており、何もできないことが多くなっています。

エンドポイントセキュリティを介した URL フィルタリングでは、既知の悪意のあるサイトおよび C2 サーバーへのアクセスをブロックすることができます。このアクションにより、フィッシング攻撃、クレデンシャルハーベスティング、ランサムウェア、その他多くのマルウェアやビーコンがエンドポイントにインストールされ、データが盗み出されたり、大規模ボットネットや暗号化プールの一部としてデバイスが組み込まれ（クリプトジャッキング）たりすることを阻止できます。

2022 年以降も攻撃者は企業や組織への侵入方法を探り続けていくことでしょう。エンドポイントが接続するネットワークが多いほど攻撃対象としては魅力的なものになります。

継続的な監視戦略

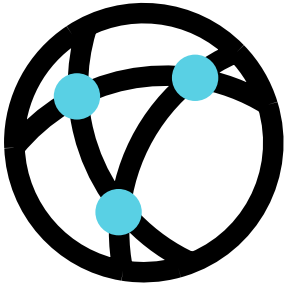
Aberdeen が最近発表したレポートによると、従来のシグネチャベースのエンドポイント保護によるセキュリティ効果の基準値は 91.5% とされています（セキュリティ侵害リスクが 7.5% 残っています）。攻撃対象領域を 4.7% 縮小した場合、この効果が 96% まで向上したことも報告されています。さらに、振る舞いベースのエンドポイントセキュリティにより、効果は 99.6%（または 0.4% のリスクエクスポージャー）まで向上すると見込まれています [5]。

あらゆる保護措置に関しては、組織が有するセキュリティオペレーションセンター（SOC）が 8×5（1 日 8 時間、週 5 日）や 24×7（24 時間 365 日）対応の場合でも、エンドポイントセキュリティベンダーやマネージドセキュリティサービスパートナーとサービス契約を結ぶことにより、時間外の対応やエスカレーションサポートが受けられるようになります。これらのサービスでは、アラートや疑わしい脅威の監視に重点を置き、予防的な脅威ハンティング（セキュリティ侵害指標の検出、潜在的な脆弱性のあるプログラムや不正プログラムの特定、フォレンジックアーティファクトの取得や分析など）をはじめとするインシデントの対応者に対しては、ガイダンスや次のステップが提供されます。イベントが分析されると、インシデント通知により、脅威に関する内容とレビューや改善手順に関する推奨事項が示されます。

インシデントレスポンス

エンドポイントセキュリティにどれほど利点があっても、ソリューションや階層型のソリューションセットは完璧ではありません。攻撃者はどういうわけかくぐり抜けてしまうものです。ランサムウェアや他の攻撃が実行される前にブロックすることが重要であればあるほど、攻撃による損害が発生しないように計画したり、損害を減災または回復できるように予防したりすることが重要になります。セキュリティインシデントが発見された場合、封じ込めが適切に行われていても、潜在的な損害を最小限に抑えるためには迅速なレスポンスが不可欠です。脅威を効果的に軽減するには、専門的なスキル、ツール、繰り返し可能なプロセスが必要です。これにより、状況を見定めて、脅威の拡大を阻止しながらオペレーションを回復させる方法を判断することができるようになります。

堅牢なエンドポイントセキュリティプラットフォームは、場所に縛られない働き方を求める世界中の人々にとって、最初で最後の防御線である必要があります。現在、最新のプラットフォームでは、未承認のファイル暗号化や C2 サーバー接続など、悪意のあるアクションが発生したときに自動検知され、あらかじめ用意された対策に従って脅威を排除し、エンドポイントを修復できることが求められています。第 1 世代の EDR（エンドポイントの脅威検知とレスポンス）ツールは、人工知能（AI）や ML アルゴリズム基づいて攻撃に対処できるすばらしいものでした。しかしながら、アラートが殺到した場合の SOC スタッフのへの負担は大きく、極度の疲労を引き起こしました。インシデントレスポンスをプレイブックとしてカスタマイズ設計できれば、手動による修復の必要がなくなります。



堅牢なエンドポイントセキュリティプラットフォームが、どんな場所からでも働ける環境において最初で最後の防御線である必要性が求められます。

終わりに

プライベートな場所と会社の間の壁は、COVID-19 のパンデミックの間に著しく蝕まれ、企業ネットワークへの大きな足掛かりを敵に与えてしまっています。テレワークでは、企業のファイアウォール内で守られていたデスクトップ PC が自宅のノート PC に変わり、企業の境界の外で動作することになったことで、攻撃対象領域が大幅に広がりました。従業員が出張する際にも、多くのデバイスがこのように使用され、公共のアクセスポイントから企業リソースにアクセスすることも少なくありません。さらに、企業ネットワークにアクセスするデバイスを使用して企業のファイアウォール外で Web サイトを閲覧することで、アクセスしたリソースが悪意のあるコンテンツにさらされる可能性もあります。

企業には、最初で最後の防御線となるエンドポイントセキュリティプラットフォームが必要です。また、人やエンドポイントでの通信を悪意のあるサイトや C2 サーバーなどへの接続から保護しながら、世界で最も攻撃的で巧妙に設計された形式の攻撃に対処できることが求められています。そして、マルウェアが実行される前にほぼすべてをブロックし、エンドポイントの問題があれば修復する必要があります。

[1] 「Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work」、Forrester、2021 年 9 月（英語）：https://www.tenable.com/analyst-research/forrester-cyber-risk-report-2021

[2] 「フォーティネットグローバル脅威レポート 2021 年上半期版」、FortiGuard Labs、フォーティネット、2021 年 8 月：https://www.fortinet.com/jp/demand/gated/TR-21H1

[3] 「2021 年ランサムウェア調査レポート」、フォーティネット、2021 年 11 月：https://www.fortinet.com/jp/demand/gated/ransom-survey-2021

[4] 同上

[5] 「Quantifying the Risk Reduction of Evolving Endpoint Security Technologies,」、Aberdeen Strategy and Research、2021 年 7 月（英語）：
https://fusecommunity.fortinet.com/groups/community-home/events/event-description?CalendarEventKey=57651ee2-f725-4005-aaf7-767497e853aa

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

EB-Protecting-Endpoints-WFA-202203-R1