標的型攻撃の狙い目はエンドポイント

～EDRはモバイルワークやテレワークにも有効なセキュリティー～

標的型などのサイバー攻撃は、エンドポイント（ユーザーが使う端末やサーバーなど）が攻撃者の狙う標的となります。対処が遅れればそれだけ被害は甚大になりかねません。エンドポイントを監視し、異常を検知したら瞬時に端末を遮断して、「攻撃の証拠を保存」し、全社的な対応を促すEDRは、被害を最小限に食い止める対策として注目されています。EDRがなぜ注目されるのか、EDRの特徴について説明します。

防御一辺倒では守れない、巧妙化するサイバー攻撃

年々巧妙化が進む標的型攻撃。警察庁の調査によれば、2017年の標的型攻撃メールの件数は前年の約1.5倍に増加し、過去最多の6027件に上りました。これもあくまで認知した件数に過ぎません。潜在的な攻撃はこれを大きく上回ることが容易に想像できます。

標的型攻撃のやっかいなところはいくつかあります。まず既存のエンドポイントセキュリティー製品では検知が難しい「未知のマルウェア」を用いるケースが多いことです。また最近では、OSが備える正規のツールを悪用したり、スクリプトを実行して侵入する「ファイルレス攻撃」が増加しており、検証対象のファイルが、すでに確認済みのマルウェアと一致するかデータベース（シグネチャー）を用いて判断するエンドポイントセキュリティー製品ではますます検出が困難になっています。

そこで近年、セキュリティー対策のアプローチに根本的な変化が必要だという考え方が広がってきました。米国立標準技術研究所（NIST）の「サイバーセキュリティーフレームワーク」や経済産業省の「サイバーセキュリティ経営ガイドライン」などがその例で、防御一辺倒ではなく、侵害がありうることを前提として検知、対処といった事後対応にも取り組むよう求めています。この流れのなかで急速に注目されているソリューションが「EDR」（Endpoint Detection and Response）なのです。

「侵入を前提とした対策」に取り組む現場が直面する課題

2017年、猛威を振るったランサムウェアが典型例ですが、ニュースで問題を知り、自社システム内での調査に取り組もうとして、作業の難しさを感じた人は少なくないでしょう。本社だけでなく支店や海外拠点も含めて、攻撃に悪用される恐れのある脆弱（ぜいじゃく）性が残った端末、すでに感染している恐れのある端末を洗い出す作業は困難で、時間もかかります。時には、台帳の情報とは異なり、いつの間にか社内ネットワークに加わった「幽霊端末」が見つかることもあり、こうした情報システム部の管理下にない端末こそ、マルウェア感染の原因になりやすいとされています。

組織内のパソコンがマルウェアに感染していることが判明したら、困難な作業が待っています。まず、内部での被害拡大を防ぐには、速やかにネットワークから遮断します。有線ネットワークだけの時代ならば「LANケーブルを抜いてください」で済んだかもしれませんが、多くのパソコンがワイヤレスでも接続されている現状では、設定画面を操作して設定変更しなければなりません。

標的型攻撃の狙い目はエンドポイント

さらに会社として再発防止を期するには、パソコン内のデータとネットワーク側のログを突き合わせて調査し、「いつ、何がきっかけでマルウェアに感染したか」を把握する作業を実施します。そして、パソコン側にデータが残っていたとしても、プロキシーサーバーやゲートウェイ、ファイアウォールの膨大なログと、エンドポイント側のログを突き合わせ、感染の引き金を突き止めるには、少なからぬ時間とノウハウが必要となります。しかし、感染力の高いマルウェアを相手にしている場合は、時間との勝負です。速やかに解析して対処しなければ、被害は拡大する一方です。

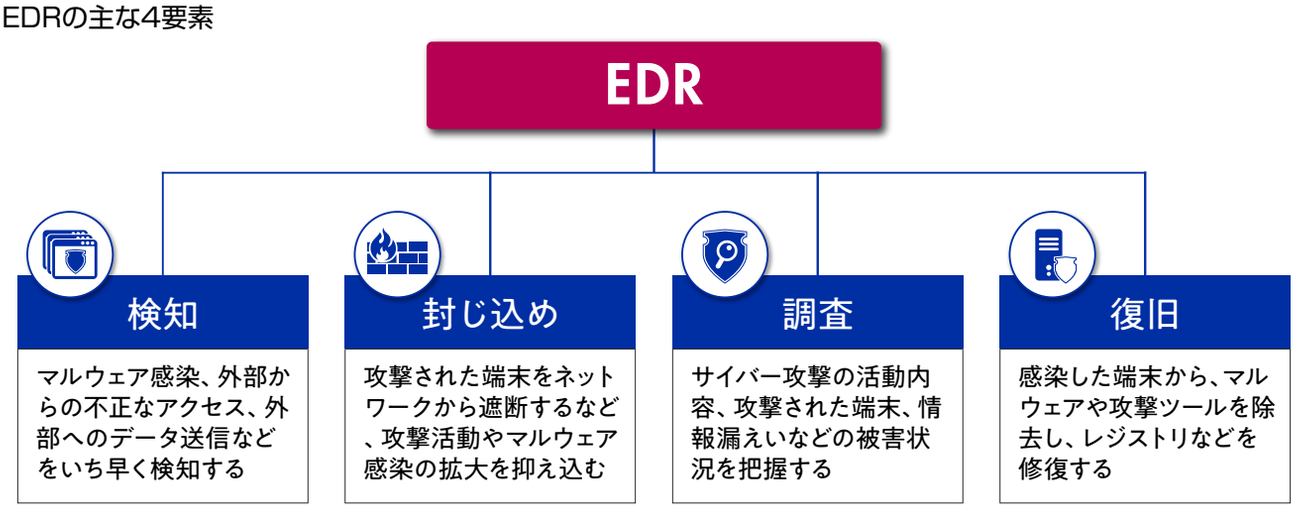
このように、いざ侵入を前提とした対策を実現しようとすると、セキュリティー運用の現場はさまざまな問題に直面することになり、この部分を支援するソリューションこそがEDRなのです。

ログの収集と遠隔制御で効率的な事後対策を実現するEDR

侵入前提の対策を実現する第1歩は、社内ネットワークに存在する端末がどのような状態に置かれているかを把握することです。そして、マルウェア感染のような異常が発生したら、いち早くその状況を検知し、エンドポイントから収集したログをもとに何が起きたか、顧客情報など重要なデータが社外に持ち出されていないかといった被害状況を確認する必要があります。EDRは文字通り脅威の検出と対応に特化した製品で、こうしたプロセスに役立つ機能を備えています。

ちなみにEDRという言葉を生み出したガートナーでは、主に「検知」「封じ込め」「調査」「復旧」という4機能を備えたものを「EDR製品」と定義しています。マルウェア感染からの「防御」よりも、防御の網をすり抜けて感染してしまった場合の一連の対応をスピーディーに行うものという位置付けです。なかには、防御と一体化した形で提供されている製品もあり、基本的にはエンドポイントにエージェントをインストールして利用されています。

図1：EDRの主な4要素



EDRの主要な機能は以下の通りです。

ログの保存・収集＝検知と調査の支援

エンドポイントに導入されたEDRのエージェントは、パソコン内でいつ、どんなファイルが実行され、どんなプロセスが起動したか、どんなネットワーク通信が発生し、レジストリ情報にどんな変更があったのかなどのログ情報を収集し、サーバー側に送信します。サーバー側はこれらの情報を集約・解析します。これによって、マルウェア感染などが発生しても、いち早くその兆候をつかんで、「具体的にどの端末が脅威にさらされているか」をピンポイントで把握できるのです。

さらに、その端末から外部にデータが送信されていないか、深刻な情報流出が起こっていないかを確認できるうえ、時系列をさかのぼっての調査も可能です。従来ならば、専門的な調査結果を待たねばならなかったセキュリティーインシデントの調査作業（フォレンジック）も、ある程度社内で進められます。

被害の最小化＝封じ込めと復旧の支援

EDR製品の多くは、管理コンソールから端末の情報を確認できるだけでなく、さまざまな遠隔操作が可能です。例えば、マルウェア本体のプロセスを停止させたり、隔離された検疫システムのみにアクセスを許可し、それ以外のネットワークから切断するなどの操作もできます。これにより、社内の他の端末にマルウェアが拡散するのを防げるのはもちろん、パソコン本体やサーバーに保存されていた重要なデータが社外に送信されるような深刻な事態も防止できます。

また製品によっては管理コンソールから、感染したパソコンをリモートで操作し、感染したマルウェアや攻撃ツールを除去し、書き換えられたレジストリなどをもとに戻すことも可能です。

攻撃の「鎖」を各ステップで断つEDR

では、EDRがどのように動作するかを、標的型攻撃対策を例に見てみましょう。

標的型攻撃は単純なものではなく、複数のプロセスに分けて展開されます。ロッキード・マーティンが提唱した、いわゆる「サイバーキルチェーン」と呼ばれるもので、偵察、武器化、デリバリー（配送）、エクスプロイト（攻撃）、インストール、遠隔操作と侵入拡大、目的の達成（情報の持ち出し）という複数の段階を経て実行されることが多くあります。一度侵入に成功したら、さらに別のマルウェアをダウンロードし、管理者アカウント情報を探るなどして社内システムで横展開を図りつつ、侵害範囲をひそかに広げていき、重要なデータを見つけたら外部に送信します。気付いたときには後の祭りなのです。

従来のセキュリティー対策の多くは、デリバリーやエクスプロイトをいかに防ぐかという点にフォーカスしてきました。

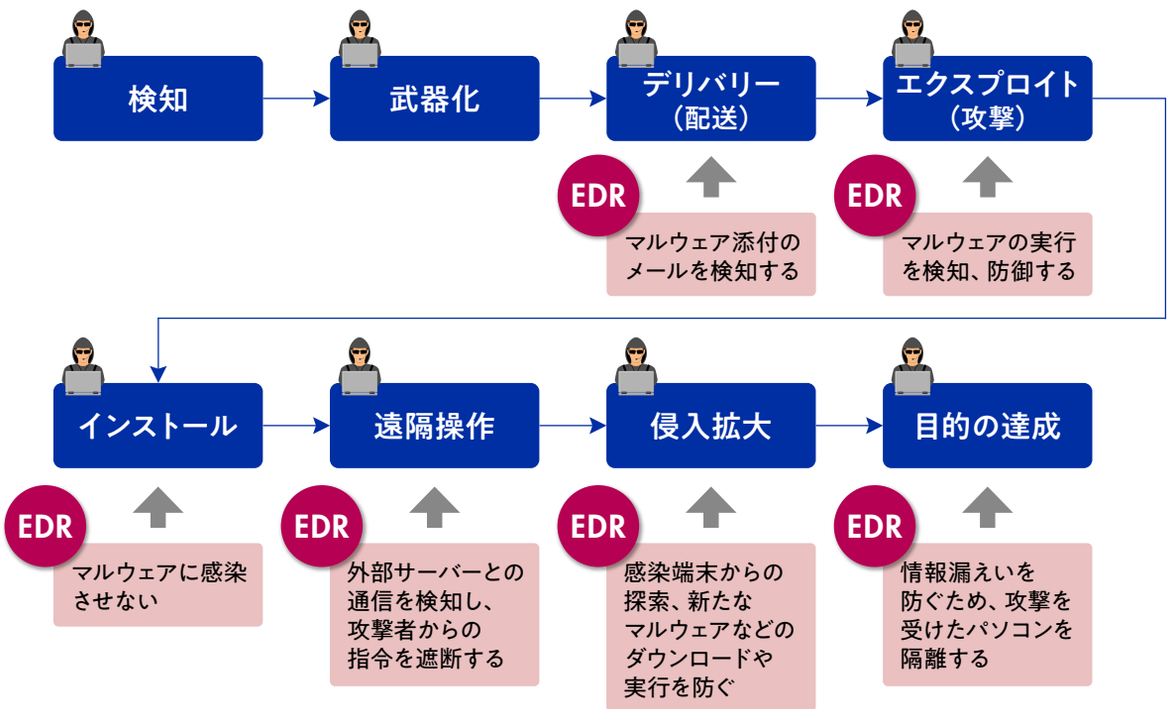
これに対しEDRは、既存のセキュリティー製品とも連携しながら、デリバリーから目的の達成に至るまで、サイバーキルチェーンの各段階で不審な動きを見つけ出し、被害拡大を防ぐ機能を提供するのです。

まず、防御をかいくぐってパソコンに何らかのマルウェアがインストールされたとしても、不審なプログラムが起動されたり、外部のサーバーと通信して遠隔制御を試みるような動きがあれば、EDRが検知して警告します。特にリスクの高い挙動と判断した場合には、管理コンソールから当該端末をネットワークから遮断し、それ以上の拡散行動を防ぎます。たとえ攻撃者が目立たない行動を心がけ、内部の他の端末に感染を広げようとしても、権限昇格などの動きを見つけたら警告し、食い止める仕組みです。

同時に、感染端末から収集したログを解析し、「個人情報の流出のような深刻な事態は起きていないか」「もし流出しているなら、どのデータが被害に遭ったのか、何名分なのか」といった詳細な情報を調査できます。そこで得た不審なファイルや通信先IPアドレスの情報を他のセキュリティー製品と共有することで、2次被害の防止に役立てられます。

たとえ標的型攻撃のターゲットになり、あの手この手で最初の侵入を許しても、それ以上の侵害は許さず、致命的な事態に至る前に食い止められるのです。

図2：標的型攻撃へのEDRの対応



既存の対策を補い、エンドポイントを守るEDR

これまで多くの企業が、さまざまなセキュリティー製品を導入し、組織内外の境界となる「ゲートウェイ」での防御に力を注いできました。しかし防御重視のアプローチでは、既知の脅威に効果的に対処することはできても、未知の脅威にはすり抜けられることもあり、致命的な事態を完全に食い止めるのは困難です。

これに対しEDRでは、攻撃者が狙う「エンドポイント」の状況を可視化し、詳細な情報を把握できます。仮に境界での防御をかいくぐられたとしても、その次のステップで確実に侵害を食い止めることができるのです。万一、情報流出が起こったとしても、「何が原因で、どのような影響があったのか、そして再発防止策は何か」を速やかに明確にし、説明責任を果たせるようになります。

また近年では、働き方改革の一貫として、モバイルワーク、リモートワークに取り組む企業が増えています。この結果、企業ネットワークの「境界」が曖昧になり、ゲートウェイ製品だけではカバーしきれない状況が生まれています。エンドポイント上でエージェントとして動作するEDRは、端末が出張先や自宅にあっても効果を発揮します。

昨今、企業において情報漏えい事件・事故が発生した際に、報道で大きく取り上げられることが増えました。一方で脅威の巧妙さは増すばかりです。企業では、マルウェアに侵入された場合も想定し、いかに早期に発見して対処し、情報漏えいの被害拡大を防ぐかが求められています。また原因が究明できず、説明責任を果たせなければ、企業にとっては社会的信用、顧客からの信頼を失うことにつながりかねません。こうしたことも考え合わせると、従来の対策を補い、致命的な事態を防ぐ対策として、EDRによるセキュリティー強化を真剣に検討すべき時期を迎えているといえるでしょう。

【制作／コンテンツブレイン】

NTTコムウェア株式会社
URL：http://www.nttcom.co.jp/
WEB掲載：2018.5