アンラボ・セキュリティレター

Press Ahn

2018.5　Vol.53

EDR はセキュリティの未来となるか

次世代エンドポイントセキュリティ製品導入のための提言

EDR はセキュリティの未来となるか

最近セキュリティ分野で最も注目されるソリューションは EDR(Endpoint Detection & Response)だろう。EDR 市場に向けられる高い関心は、既存のソリューションでは不十分だった可視性(Visibility)と対応(Response)をより強化させたという期待感のためだ。EDR はこれらの期待を満足させるカギとなるか。それともただ一過性の流行に過ぎないのか。今回のコラムでは、EDRの登場に至る背景と市場のニーズ、そして 2018年リリース予定の「AhnLab EDR」と「AhnLab EPP」を紹介する。

インシデントとマルウェア脅威

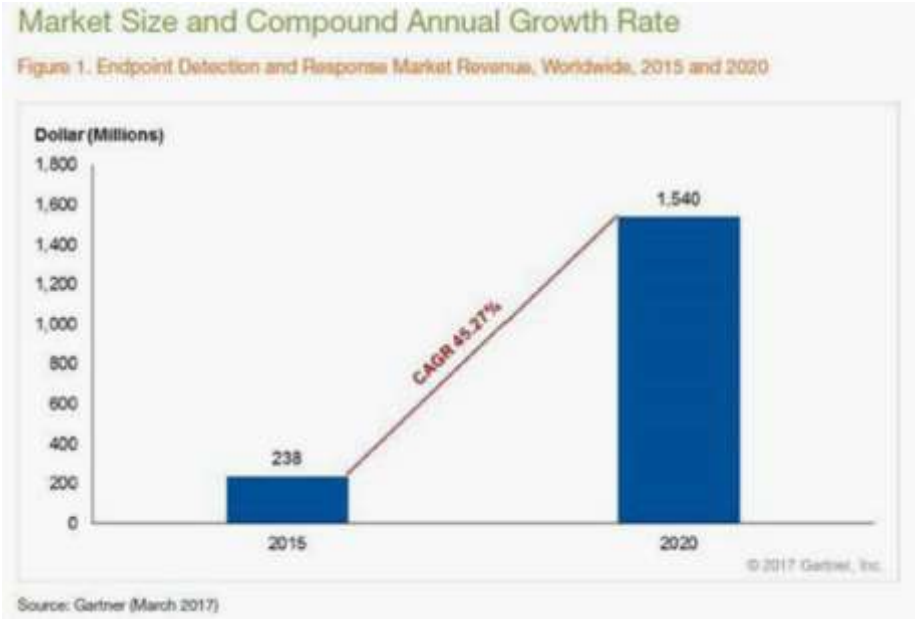
2017年にも深刻なインシデントが発生し、Equifax、Uber、Verizone などの名だたる企業が大規模な個人情報流出を経験している。また世界を震撼させた WannaCry、Petya、韓国のインターネットサービス業者を破産にまで追い込んだ Erebus などランサムウェアによる被害も続出した。
ほとんどはエンドポイントでマルウェアを使って進行され、これは最初のマルウェア「Brain」登場以降 30年余り続いてきたパターンだった。
攻撃者がマルウェアを使って攻撃を成功させている点では変わりないが、確かなのは検知を回避する技術が進化していることだ。エンドポイントの統合的な脅威管理・対応ソリューションが必要とされる理由がここにある。

セキュリティソリューションの限界と顧客のニーズ

エンドポイント領域における通常のセキュリティ対策としては、アンチウイルス、パッチ管理、デバイスコントロール、NAC 製品を配置することがあり、ネットワーク領域ではファイアウォール、侵入遮断システム(IPS)、DDoS 防御システム、Web ファイアウォール(WAF)を運用する企業が多い。それにもかかわらずマルウェアに感染してシステム中断やデータ流出のような被害が発生するのである。
攻撃者は上記の様々なソリューションの検知を回避して巧妙な攻撃を仕掛けてくる。パッチを適用しないアプリケーション、脆弱なサイト接続によって感染するケースが多発しているがネットワークセキュリティ製品の場合は、信頼されたアドレス、プロトコル、アプリケーションから侵入するマルウェアの遮断に限界がある。
比較的最新の製品で、ビヘイビアとデータをもとに分析する UEBA(User and Entity Behavior Analytics)とSIEM(Security Information and Event Management)も 完璧に脅威を遮断することはできない。UEBA はビヘイビアベースであり、SIEMのようなデータ収集サーバーが別途必要になってくる。SIEM の場合は連動されたセキュリティ製品からログを送信してもらう必要があり、別途セキュリティ製品に依存するしかない。

業界はこれまで導入したソリューションだけでは不十分だということを感じている。企業にとっては新型マルウェアなどの「未知の脅威」と、潜在的に有害な可能性を持つ「見えない脅威」への対応も必要で、被害が発生する前に検知・対応が可能でなければならない。

現在最も関心が高いソリューションは *EDR(Endpoint Detection and Response)*だ。グローバルリサーチ機関 *Gartner* は *EDR* の市場規模を *2015*年 *2*億*3800*ドルから、*2020*年*15*億ドルまで*(*年平均成長率*(CAGR) 45.27%)*成長すると予測している。また *2020*年までに大企業の *65%*以上と中堅企業の半分以下が完全な機能を持つ *EDR* に投資すると予想した。



[図1] EDR 世界市場規模及び成長予測 (*出典: Gartner)

EDR(Endpoint Detection and Response)とは

EDR は 2013年に Gartner がコラムで ETDR(Endpoint Threat Detection and Response 以降 EDR と呼ばれた)を紹介して初めて登場した。2014年からは市場と技術トレンド、主要ベンダーの動向を紹介する EDR マーケットガイドも毎年発行している。

Gartner は EDRを「エンドポイントレベルで継続的なモニタリングと対応を提供するセキュリティソリューション」と定義する。また ▲検知(Detect security incident)、▲分析(Investigate security incident)、▲エンドポイントのセキュリティコントロール(Contain the incident at the endpoint)、▲感染前の状態に復元(Remediate endpoint to a preinfection state)の 4つの機能を提供しなければならないと説明した。

EDR はエンドポイントで発生した多様な行為をどれだけ早く、どれだけ多く検知できるかが大事だが、検知された端末以外に被害はないか、またどんな端末が攻撃されたかなどエンドポイントレベルの被害範囲をトレースする可視性(Visibility)も提供しなければならない。さらに感染された端末を隔離またはネットワーク遮断、脆弱性を検知してパッチを適用するような対応(Response)機能も重要だ。これら動作の目的はセキュリティ脅威から被害を最小化することにある。現在多くのセキュリティ企業で EDR ソリューションをリリースし、アンラボ、シマンテック、トレンドマイクロのような Endpoint Protection Platform(EPP)企業は既存の製品に EDR モジュールを追加する形態で対応している。また次世代アンチウイルス(Next Generation Anti-Virus)会社や新規 EDR 会社なども市場を先取りしようと競争中だ。

EDR と EPP を合体させる

アンラボも下半期に EDR 製品をリリース予定だが、ポイントはアンラボの次世代エンドポイントセキュリティプラットホーム「AhnLab EPP」も一緒になっている点だ。最近エンドポイントの帰還と表現されるほどエンドポイントセキュリティに注目が集まっているが、アンラボは設立当時からエンドポイントセキュリティの重要性について強調してきた。

特に昨年 2017年には、エンドポイントセキュリティプラットホーム戦略「AhnLab SECURITY LADDERS」を発表し、エンドポイントセキュリティの革新が必要であることを提唱した。AhnLab SECURITY LADDERS とは、レガシー(Legacy)、適応(Adaptive)、検知(Detection)、顧客主導(Driven)、エンドポイント(Endpoint)、対応(Response)、サービス(Service)の頭文字をとった単語で「顧客がシンプルに適用できるセキュリティ」を意味する。アンラボは脅威への管理・対応を中心にしたプラットホーム観点にシフトし、検知と迅速な対応が可能となる「検知(Detection)-分析(Analysis)-対応(Response)」の構造を体系化した。

一般的な EPP はファイルベースマルウェアを防止するためにアプリケーションの悪意ある活動を検知・遮断してインシデントに対応する(必要な調査と駆除)エンドポイントセキュリティソリューションだが、AhnLab EPP(Endpoint Protection Platform)は、アンラボの多様なエンドポイントソリューションを有機的に統合連携して持続的に発生するセキュリティ脅威を検知・モニタリング・対応する次世代プラットホームである。

本製品はエージェント単体とシングルマネジメント(One Agent、Single Management)コンソールから総合的に運用できる点が最大の強みだ。

例えば V3 ユーザーなら AhnLab EDR ライセンスを追加すればエージェントを追加インストールすることなく AhnLab EPP から統合管理モニタリング対応が可能となる。管理コンソールからはパッチ管理ソリューション(AhnLab Patch Management)、脆弱性チェックソリューション、個人情報流出ファイル遮断ソリューション(AhnLab Privacy Management) などの製品を選択して適用することができる。

[図2] AhnLab EPP をベースにした EDR 構図

EDR ソリューションは膨大な量のデータを効率的に収集・保存・分析して複数のソリューションと連動する必要があるため、これらを反映したアーキテクチャを持つ新しいプラットホームが必要だ。アンラボが EDR を実現するために、そのプラットフォームとして誕生したのが AhnLab EPP なのである。現在 EDR 市場は EPP 市場とスピーディに融合されつつあり、次世代エンドポイントセキュリティ製品は今後の 3~5年でシングルマネジメントコンソールとエージェント単体の結合(Single integrated agent with single management consoles)にシフトされるだろう。

既存の EPP ベンダーは攻撃者をよりモニタリングしやすいように迅速に EDR 機能を取り入れ、EDR ベンダーは EPP ベンダーと競争するためより良い検知・対応機能を追加している。多くのセキュリティ企業が EDR 製品をリリースし、EDRがこそが「セキュリティの解決策」のごとく思われがちだが、EDR もセキュリティ脅威に対応するための一つのツールであることを忘れてはならない。EDR というツールをしっかりとコントロールする「人」と「プロセス」がなければ意味がない。

AhnLab EDR と AhnLab EPPがそれぞれどんな機能と特徴を持つか、相互連携を通じてどのような効果を出すのか。

詳細はプレスアン次号で続けて紹介する予定だ。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)