これからのセキュリティ対策は「事後」がカギ

複数社の事前検証で見えてきた、トレンドマイクロ Apex One の実力

» 企業活動を脅かすサイバー攻撃。その手口はますます巧妙化し、攻撃者による企業ネットワークへの不正侵入やエンドユーザーPC のウイルス感染被害などが頻発している

目次

必要性が高まる「脅威に侵入されたあと」の対処

企業活動を脅かすサイバー攻撃。その手口はますます巧妙化し、攻撃者による企業ネットワークへの不正侵入やエンドユーザーPC のウイルス感染被害などが頻発している。

例えば、ファイルレス攻撃などの新たな手法では、企業の内部ネットワークへ侵入したのち、正規のユーザー権限や社内システムなどを乗っ取って不正行為を行うため、被害に気付くことが難しい。とはいえ、不正侵入、不正操作で機密情報が社外に流出すれば企業の責任は免れない。経営に影響を及ぼす可能性もあるだろう。

情報セキュリティ対策の見直しが急務になる中、この 7 月にリリースされた製品が注目を集めている。それが、法人向けエンドポイントセキュリティ「ウイルスバスター コーポレートエディション」（以下、ウイルスバスター Corp.）の後継となる新製品「Trend Micro Apex One」（以下、Apex One）だ（図 1）。

図 1　●Trend Micro Apex One の防御アプローチ

ウイルスバスター Corp.が提供してきた「事前予防」の機能を強化したほか、新たに「事後対処」の機能を追加。簡単・迅速なインシデント対応を支援する統合ソリューションとなっている

かねてウイルスバスター Corp.が提供してきた、攻撃の侵入を未然に防ぐ（事前予防／EPP：Endpoint Protection Platform）機能を強化したほか、仮に脅威に侵入されても被害状況を可視化してインシデント対応を支援する（事後対処／EDR：Endpoint Detection and Response）各種機能を新たに実装。両方を 1 製品内でシームレスに統合することで、エンドポイントセキュ

リティの統合プラットフォームとして機能する。これまで手薄になりがちだった EDR の仕組みを、ウイルスバスター Corp.のバージョンアップで簡単に導入できる点が、注目を集める最大の理由といえるだろう。

一方、EDR においては、対策を単発で終わらせず、改善に向けた運用サイクルを継続的に回すことが重要になる。そこで現在は、複数の企業が事前検証を実施しているという。今回はその内容を紹介しながら、Apex One の実力を確認したい。

EPP・EDR の統合製品である点が大きなメリットに

そもそも EDR には、脅威が侵入した際にネットワーク内の感染端末を表示して被害の範囲を可視化したり、システムログから感染原因と思しきプロセスを抽出し、侵入経路を明らかにしたりするといったことが含まれる。

トレンドマイクロ株式会社
エンタープライズ SE 本部
セールスエンジニアリング部
エンドポイントセキュリティチーム
シニアソリューションアーキテクト
大森 華子氏

「数年前にランサムウエアの WannaCry が猛威を振るいました。その際、既存のエンドポイント対策で『WannaCry の検知はできたが、組織全体の影響範囲の可視化や収束対応に苦労した』というお客様の声が多くありました。また同時に、GDPR（EU 一般データ保護規則）のような法規制やグループ企業の親会社からの要請により、インシデント発生時の原因特定や解析、報告が必須になっている企業も増えています。これらの状況を背景に EDR の考え方が注目され始め、今では多くの企業がセキュリティ強化に向けて欠かせないアプローチの 1 つと考えています」とトレンドマイクロの大森 華子氏は説明する。

EDR 単体の製品を導入した場合、そのままでは既存の EPP 製品との十分な連携ができないため、個別に運用作業が発生する。例えば、EPP と EDR を異なるベンダー製品で行う場合、検知した脅威の名称の突合せが必要となる。これではセキュリティ対策全体の工数が増えてしまうため、実運用に載せることは難しかった。

「その点、1 つの製品である Apex One ならシンプルな管理が行えるため心配は無用です。製品コンセプトに基づき、十分な性能や機能が発揮できるよう、導入前にはお客様環境での検証を行うことをお勧めしています」と大森氏は語る。

情報の量と分かりやすさ、管理画面の UI が高評価

それでは事前検証の結果を見ていこう。

ある企業では他社の EDR 製品を含めて検証を行ってきたが、中には提供される情報が多過ぎて、何に対してどう対応すればよいか判断が難しい製品もあったという。Apex One では最初に被害端末を可視化し、影響範囲を絞り込む。そして、侵入経路を視覚的に分かりやすく管理画面に表示するので、起こっている事態が容易に把握できる点が評価されたという（図 2）。

図 2　●侵入経路を視覚的に分かりやすくした、Apex One の管理画面

脅威の侵入経路をビジュアルで分かりやすく表示するため、迅速かつ的確な対応が容易に行える

（ca91-1[.]winshipway[.]com はトレンドマイクロ製品の動作試験用ドメイン）

「もちろん裏では情報を網羅的に取得していますが、そのまま表示するだけでは利便性が低下し、重要アラートの見落としなどを招いてしまいます。当社の知見に基づき、必要十分な情報を精査して表示することで、お客様の会社のシナリオに即した運用ができました」と同社の中村 俊一氏は話す。

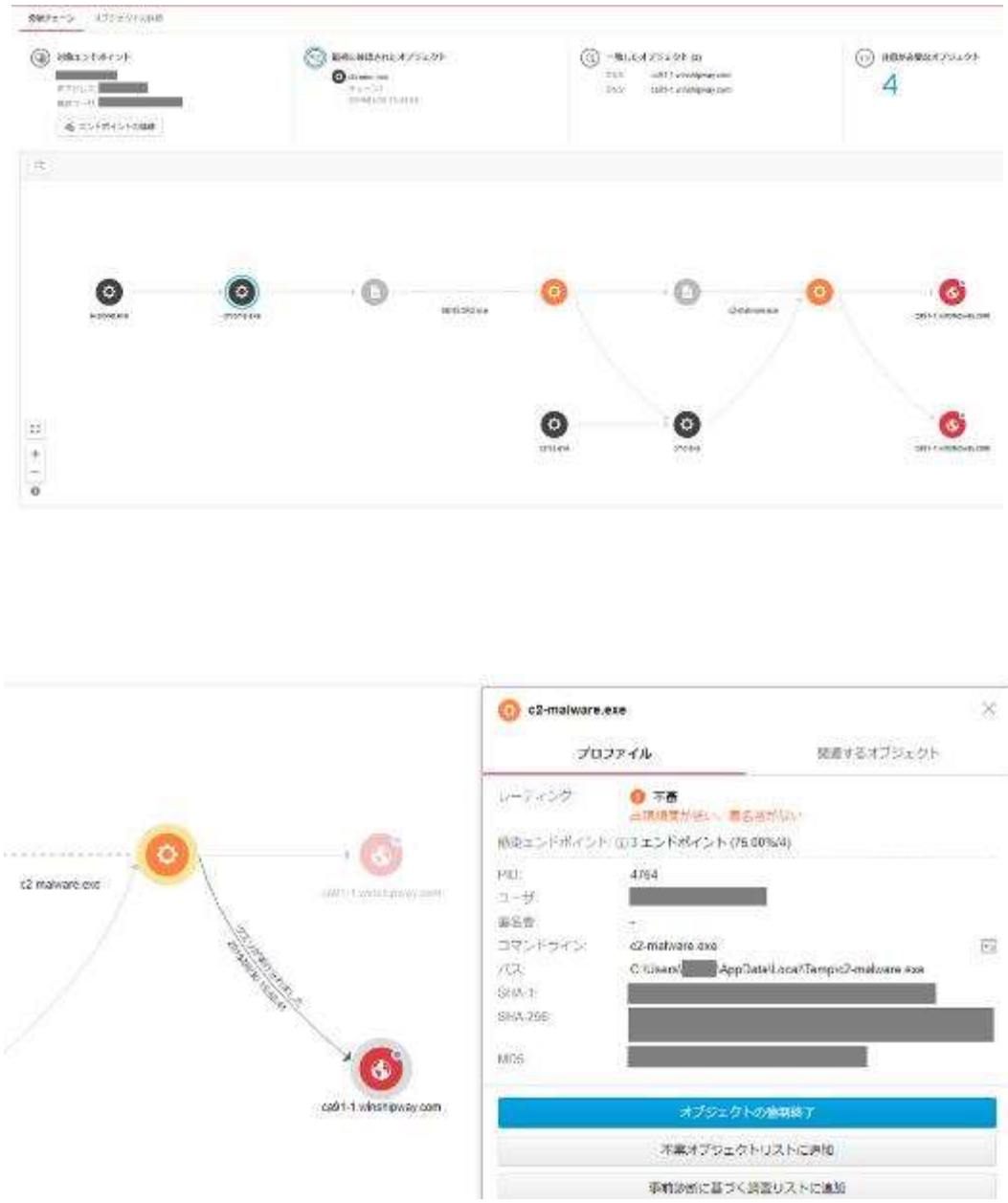
トレンドマイクロ株式会社
エンタープライズ SE 本部
セールスエンジニアリング部
エンドポイントセキュリティチーム
ソリューションアーキテクト
中村 俊一氏

また、多くのグループ会社を抱える別の企業では、グループ各社のセキュリティ対策強化を課題としていた。本社は高度な対策環境を整えてきたが、グループ各社の対策レベルはまちまちで、そこがセキュリティホールになる懸念を抱いていたのだ。

そこでこの企業は、あるグループ会社で発見した脅威を Apex One の EDR で解析し、シグネチャを作成してグループ全社に配布する方式を検討。このサイクルを回すことで、グループ全社の対策レベルを向上しようと考えた。

「Apex One では、EDR で見つけた脅威の情報をブラックリスト化して EPP のシグネチャとしてフィードバックすることで、同じ脅威の侵入を未然に防ぐことが可能です。こうした脅威情報を事前予防に回す作業も、Apex One は管理画面のクリック操作で簡単に実行できます。検証を通じて、EPP と EDR が 1 製品に統合されているメリットを実感していただくことができました」と中村氏は強調する（図 3）。

図 3　●原因特定と対処のシームレスな連動が可能



侵入経路や脅威の種類などを調査・分析（上）した結果は、すぐに EPP による対策へフィードバックされる（下）。これは統合製品の強みといえる

ファイルレス攻撃の対応など EPP の機能も確認

さらに、これまで管理が難しかった持ち出し PC の対策強化に期待する企業もある。

ある製造業の企業では、ウイルス対策が脆弱な海外拠点や海外出張に持ち出す PC の保護、および帰国後の社内システムへの感染を防ぐ方法を求めていた。ネットワーク環境が整備されていない地域への出張などではパターンファイルの更新が遅れがち。また、USB メモリーでのデータ受け渡しも発生しやすく、ウイルス感染リスクが高まるからだ。実際、帰国後の PC からは、これまで必ずといっていいほど数個のウイルスが発見されていたという。

「Apex One は、外部との中継点にエッジリレーサーバーを導入することにより、持ち出し PC に対しても EDR による侵入プロセスの特定・可視化が行える上、感染 PC をネットワークから隔離し、被害の拡大を防ぐことも可能です。こうした機能は、製造業のような多くの海外拠点を構えるお客様に高く評価されています」（中村氏）

また、強化された EPP の機能も評価されている。例えば、機械学習技術を用いたウイルス検索技術により、パターンファイルに依存せず、日々増加する亜種ウイルスなどにも対応が可能だ。事前検証を行った企業からは、「EPP の機能が強力で、なかなか EDR の検証に進めない」といった声もあったといい、これは検証環境ならではのうれしい悩みといったところだろう。

ウイルスバスター Corp.を利用中の企業の IT 担当者、セキュリティ担当者にとって、負荷なく EDR 機能を導入できる Apex One は、まさしく“持ってこい”の製品といえる。事前検証を含め、導入に向けた検討をしてみて損はないはずだ。

※本コンテンツは、日経 xTECH ACTIVE に掲載された記事広告を再構成したものです

TREND MICRO

トレンドマイクロ株式会社

www.trendmicro.com

東京本社
〒151-0053 東京都渋谷区代々木 2-1-1
新宿マインズタワー
TEL.03-5334-3601（法人お問い合わせ窓口）
FAX.03-5334-3639

名古屋営業所
〒460-0002 愛知県名古屋市中区丸の内 3-22-24
名古屋桜通ビル 7F
TEL.052-955-1221　FAX.052-963-6332

大阪営業所
〒532-0003 大阪府大阪市淀川区宮原 3-4-30
ニッセイ新大阪ビル 13F
TEL.06-6350-0330　FAX.06-6350-0591

福岡営業所
〒812-001 1 福岡県福岡市博多区博多駅前 2-3-7
シティ 21 ビル 7F
TEL.092-471-0562　FAX.092-471-0563