アンラボ・セキュリティレター

Press Ahn

2023.5　Vol.113

V3、MDS、EDR 統合セキュリティ

V3、MDS、EDR 統合セキュリティ

デジタル転換の加速化、非対面サービスの日常化でネットワーク接続接点が増加し、侵害事故に対する懸念も広がっている。多くの企業が様々な最新セキュリティソリューションを導入しているが、これは運用や管理の不備による新たなセキュリティホール（hole）を引き起こす。徐々に知能化される脅威に対する正確な検知と能動的な対応、効率的なセキュリティソリューションの運用・管理のため、セキュリティソリューション間の連携はもはや選択ではなく必須である。

アンラボは、製品と製品、製品とサービスを有機的に連動させ、統合セキュリティを実現している。3月号ではアンラボの統合オファリングに関して詳しく紹介した。今回は、アンラボの主要エンドポイントおよびネットワークセキュリティ製品である AhnLab V3 と MDS、EDR それぞれの特徴と相互連携性を調べる。

製品別の機能および特徴

これら 3つの製品間の関連性を説明する前に、各製品の主要機能と特徴から簡単に紹介する。

1) AhnLab V3

AhnLab V3 は、コンピュータセキュリティのためのワクチンプログラムで、アンラボの代表的なエンドポイントセキュリティ製品である。V3 はシグネチャ（Signature）方式を使用し、既知の脅威を素早く検知・遮断する。このシグネチャ方式とは、ファイルの表面、つまり外形データを分析して正常ファイルと不正ファイルそれぞれの固有の特徴を抽出する技法である。

また、V3 は 1,500以上の不正行為パターンを検知し、既知の脅威に対応する。ただし、伝統的なシグネチャ、ルールベースの診断ではランサムウェア、ファイルレス（Fileless）攻撃などを含む新たな脅威および未知の脅威の検知には限界がある。これに対し、V3 は「デコイ（Decoy）ファイル診断」、「隔離スキャン」、「ランサムウェアセキュリティフォルダ」機能を通じてランサムウェアに対応す

る。また、「プロセスメモリ診断」および「AMSI（Anti Malware Scan Interface）」診断により、マグニバー（Magniber）のようなファイルレス形態で流布されるマルウェアを検知・遮断することができる。

2) AhnLab MDS

AhnLab MDS（Malware Defense System）は、持続的標的型攻撃（APT）に対応するネットワークサンドボックスソリューションである。ネットワーク、PC、メールサーバー前面、ネットワーク連携区間などファイルが存在するすべての領域でファイルをスキャンする。ネットワークに流入した疑わしいファイルを隔離された仮想 VM 環境で実行し、行為分析を通じて悪性かどうかを確認する。これにより、ゼロデイ（Zero Day）攻撃、ランサムウェア、脆弱性攻撃、APT など多様なセキュリティ脅威を効果的に検知して対応することで、内部システムのマルウェア感染を事前に防止する。

MDS はデータ DB とマシンラーニング（ML）、人工知能（AI）を活用して脅威を正確かつ迅速に検知し、対応する。また、これらの技術に基づいてフィッシングおよび詐欺メールに含まれる URL リンクを分析して悪性かどうかを判断する MTA（Mail Transfer Agent）機能を提供する。さらに、MDS エージェント（Agent）を通じてファイル実行を保留し、VM 迂回型マルウェア対応技術にも対応する。

V3 との違いは、V3 も動的スキャン機能を提供するが、インストールされた端末のリソースを一部活用して悪性診断を行うため、限定的なスキャンのみ可能である。MDS の場合、高性能アプライアンス内のサンドボックス環境で多数のエンジンをベースに様々な運用環境を実現し、動的スキャンを行う。これにより、MDS は文書ファイルを実行・操作して隠された不正行為を見つけたり、未知の脅威に対する検知が可能なだけでなく、アンチウイルスソリューションに対する迂回動作をするランサムウェアも診断できる。

3) AhnLab EDR

AhnLab EDR（Endpoint Detection & Response）は、独自開発した行為ベースの分析エンジンをもとにエンドポイント脅威を検知・対応するソリューションであり、PC および複数のデバイスで発生するすべての行為をモニタリングする。エンドポイントを狙う未知の脅威の潜伏期間の最小化、潜在的被害および再発防止を目的とする。

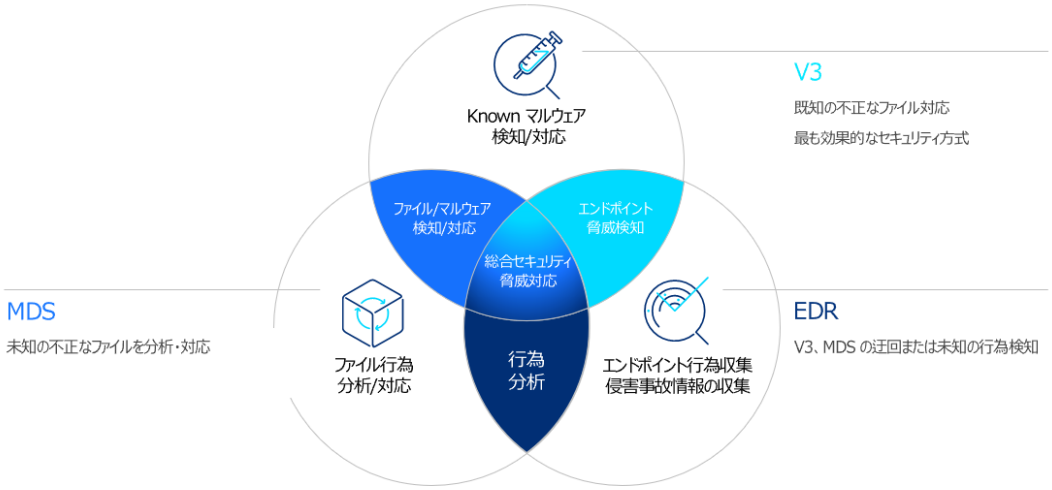
EDR は、すべてのエンドポイントの行為情報収集、関連性および攻撃段階別多次元分析、幅広いエンドポイントの可視性ベースの一歩進んだ脅威対応、連続的なモニタリングおよび統合セキュリティ管理機能を重点的に提供する。また、アンラボの専門技術力が凝縮された専用コンソール「EDR Analyzer」を提供することで、ユーザーが検知・分析、対応の観点から脅威を正確に認知して条件を設定できる運用の利便性も提供する。

また、EDR は検知タイプ別に脅威を分類し、脅威の認知から分析、対応まで迅速なワークフローに対応する。AhnLab EPP、AhnLab MDS など多様なソリューションと連動して脅威対応力を最大化し、顧客企業の環境に最適化されたエンドポイントセキュリティ運用が可能である。

究極的には、EDR を活用すると脅威を能動的に追跡することができ、顧客企業は事前予防および再発防止システムをより容易に構築できる。

製品間の連携・セキュリティによる統合セキュリティの実現

AhnLab V3 と MDS、EDR いずれもエンドポイントとネットワークセキュリティ領域で優れた性能を誇る。そして、これらの製品を連携して使用する場合、各製品の限界を補完し、シグネチャベースの遮断からサンドボックス動的分析、行為検知・対応など全方位的なセキュリティ力を確保することができる。



[図 1] V3、MDS、EDR 統合セキュリティ

例えば、V3 をインストールしたサーバーに MDS と EDR を追加すると、エージェントに不正ファイルの削除、システム隔離、告知事項の伝達などの対応コマンドを出し、ML およびビッグデータベースの脅威検知機能を通じて APT 攻撃など未知の脅威を効果的に検知 & 対応できる。また、ユーザーにファイルの実行から終了までの行為を詳細に分析した結果レポートを提供し、ウイルストータル(Virus Total) 連動を通じて悪性判断の有無を効果的に判断できるようにする。

このようなシステムで、MDS はネットワークトラフィックからファイルを抽出・収集し、ワクチンより先にファイル分析を行う。実行および非実行ファイルをサンドボックス仮想環境で稼働させ、行為を分析して悪性かどうかを判断し、未スキャンファイルに対しては実行を保留し、脅威行為を事前に遮断する。また、スパムメールソリューションとの連動によりメール本文の添付ファイルを分析するなどメールスキャンを実施し、フィッシングや詐欺による被害を最小限に抑える。このほか、文書スキャンのための専用エンジンを搭載しており、文書を悪用した攻撃も防止する。

EDR は未知の脅威だけでなく、V3 と MDS を迂回する攻撃も遮断する。エンドポイントで発生するすべてのプロセスおよびファイル、ネットワーク、レジストリ、システム行為を収集し、アンラボのノウハウとマイターアタック (MITRE ATT&CK) フレームワークを利用した検知パターンおよびルール (Rule) で脅威をモニタリングして検知する。顧客企業の環境に合った IoC、YARA、行為ルールの生成による脅威の検知・対応も可能である。

さらに、EDR は V3、MDS と有機的な連動を通じて追加的な分析が可能である。V3 でマルウェアと診断された情報に基づいて EDR が流入経路など詳細分析情報を提供し、今後発生する可能性のある同様の脅威を先制的に防げるようにする。EDR で収集された様々なプロセス / ファイル情報をサンドボックスで分析しようとする場合、MDS を通じて分析結果を確認して脅威に対する追加の証跡を確認することができる。

まとめると、V3、MDS、EDR は各セキュリティ領域で果たす役割が少しずつ異なる。これらの役割は入国審査に例えられる。例えば、V3 はシグネチャとパターンに基づいてマルウェアを素早く検知し、問題となるファイルや URL などを遮断・削除・治療して事前に対応するという点で、ブラックリスト (Blacklist) に基づいて入国者を審査するパスポートチェックと同じだと言える。パスポートチェック後、手荷物および携帯品に対して安全保障上の危害物品と輸出入禁止品目を精密にスキャンする X 線検査は、MDS がサンドボックス技術に基づき未知の脅威を正確に検知する機能と似ている。入国審査の最後の関門である防犯カメラ検査の段階で入国者の動線と動きを監視するように、EDR はエンドポイントで脅威の可能性があるすべての行為をモニタリング・検知し、脅威を追跡して分析する。

[図 2] V3、MDS、EDR の役割の比較

企業や機関でも入国審査の手続きのように段階別に徹底したセキュリティシステムの構築が必要である。ワクチン、サンドボックス、EDR につながる統合セキュリティシステムを構築すれば、複雑なシステム環境を徹底的に保護し、より強力なセキュリティ態勢を確立するのに役立つだろう。

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)