IDC MarketScape

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment (Japanese)

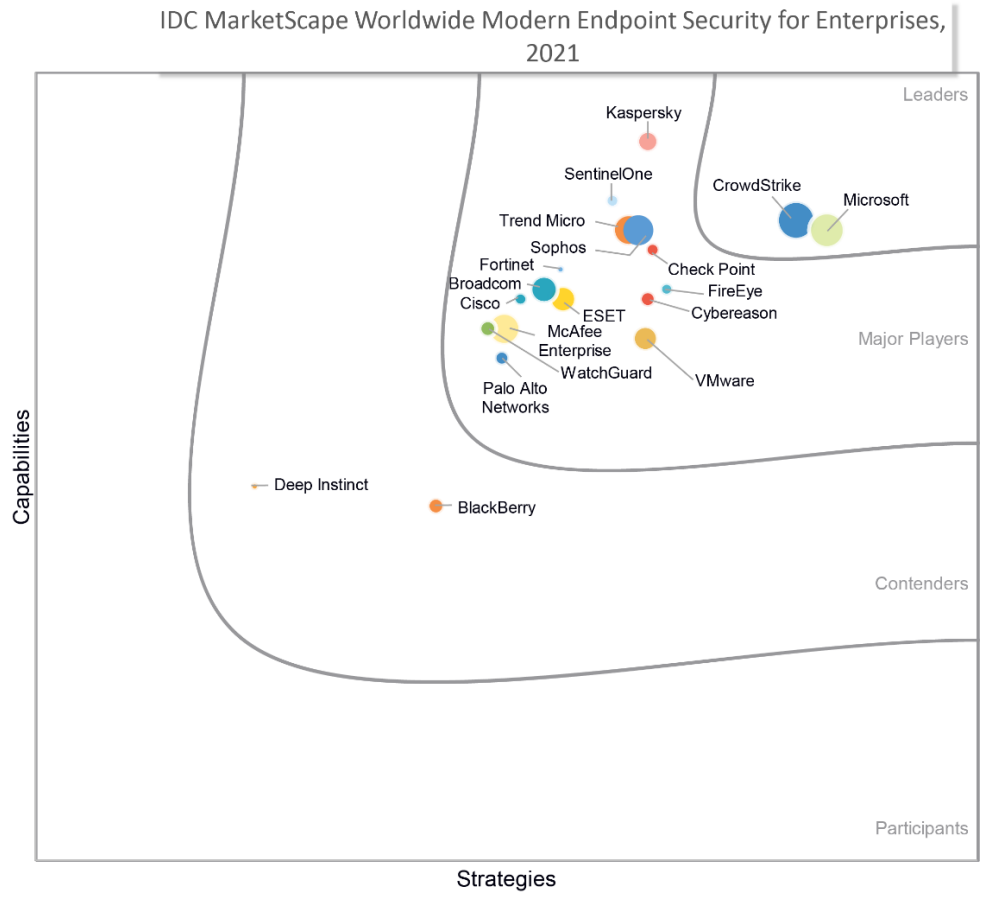
Michael Suby

THIS IDC MARKETSCAPE EXCERPT FEATURES ESET

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment



Source:IDC, 2021

調査概要

本 Excerpt の内容は、『*IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment*（IDC #US48306021、2021 年 11 月発行）』からの抜粋である。本 Excerpt には以下の項目の一部または全部が含まれる。IDC の見解、IDC MarketScape ベンダー選定の基準、提言、ベンダープロフィール概要、補遺、参考資料、Figure 1 も含まれる。

調査手法、市場定義、スコアリング基準の詳細については「補遺」のセクションを参照していただきたい。

なお、本調査レポートは、『I*DC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment*（IDC #US48306021e、2021 年 11 月発行）』の日本語翻訳版である。

IDC の見解

効果的なエンドポイントセキュリティ対策について、企業が本腰を入れることの重要性が、かつてないほど高まっている。その主な理由は、企業の IT フットプリント（IT への依存性、時間と場所を含む）が一気に広がったことである。新型コロナウイルス感染症（COVID-19）の感染拡大が契機となって、何百万人ものオフィスワーカーが働く場所を職場から在宅での勤務（WFH：Work From Home）に変更した。オフィスへの復帰が少しずつ進んでいるとはいえ、多くの企業でワークプレイス環境がパンデミック前の状態に戻ることはありそうもない。また、COVID-19 感染拡大の状況下において、クラウドアプリケーションの利用も急増している。ビジネスリーダーが、足元のニーズに対応することはもちろん、今後のデジタルトランスフォーメーション（DX）における競争力強化に向けた柔軟性を必要とした結果である。

従業員とアプリケーションの両方が同時期にオフプレミスに転換したことは、脅威アクター（threat actors：脅威をもたらす個人あるいはグループ、つまりサイバー攻撃者を指し、本調査レポートでは一貫して「脅威アクター」と表記する）に恩恵をもたらした。WFH の従業員が使う PC を標的とする機会が増えたためである。これらのデバイスは、オフィスを中心に考えた防御の境界の外部に存在するというだけでなく、企業管理の対象外にあるホームネットワークを介して、ほぼフルタイムで接続されており、ビジネス以外の目的での使用や、本人以外の家族メンバーが同じデバイスを使用する可能性も高まっている。根本的に、脅威アクターがリモートに置かれた PC に侵入する可能性は、従来の数倍にまで拡大している。さらに、これらのデバイスのユーザーは生産性を保つために、VPN（Virtual Private Network）を介してクラウドアプリケーション（カスタムおよび Software-as-a-Service）やオンプレミスアプリケーションへのアクセスが求められる。結果的に、PC が標的として狙われることが多くなった。それだけでなく、クラウドとオンプレミスのどちらのアプリケーションに対してもリモートでのアクセスが急速に増加したことから、ビジネスネットワークがフラット化、つまり均質化している。言い換えると、ネットワークのセグメンテーションを利用してセキュリティを維持するという従来のアプローチが、これまでほど有効とは言えないことを意味する。脅威アクターにとってさらに好都合なことに、最初に感染した PC から次の PC、そしてそれらの接続先にある IT システムに向けて標的を移す際に遭遇する障壁が、ことごとく低下している。

脅威アクターはエンドポイントに狙いを定めるだけではなく、活動に必要なノウハウも強化している。10 年ほど前は、エンドユーザーのデバイスからマルウェアを識別し除去するには、シグネチャベースのアンチウイルスソフトウェアで十分であると考えられていた。ところが時代は大きく変わった。脅威アクターはもはや、デバイスへマルウェアを「ドロップ」することだけに頼って攻撃を実行しているわけではない。正規のソフトウェアプログラム、ツール、ファイルを巧みに操作する傾向を強めている（いわば、遠隔だけでなく「LOTL：Living off the Land」と呼ばれる、検知／分析を回避するよう、PC などのデバイスに搭載されている機能を利用する攻撃手法）。その結果として、悪意のある振る舞いを識別することが、適切な防御にとって必須の要件となった。

ただし、悪質な振る舞いを識別するのは簡単なタスクではない。エンドユーザーデバイス（PC およびスマートフォン）が実行する処理の多様性、広範性、複雑性から、悪質な挙動と正当な挙動の区別が付けにくい。さらに、脅威アクターは自らの存在を隠蔽するため、一連のアクションのオーケストレーション（調和連携）を取り入れており、その一つひとつは一見したところ無害である。進行中の攻撃を発見しそれらを無力化するようスピーディかつ正確に対処するには、関連性のあるアクションの痕跡を組み合わせることが必要不可欠となった。

エンドポイントセキュリティの構築は極めて重要である。侵入前の防御（deterministic prevention）のための EPP（Endpoint Protection Platform）と、侵入後の対策（post-compromise reaction）のための EDR（Endpoint Detection and Response）を組み合わせた先進的エンドポイントセキュリティ（MES：Modern Endpoint Security）製品は、エンドポイントを狙った脅威への対抗を目的とするエンドポイントセキュリティが進化を遂げた最新の姿である。IDC の調査からは、先進的なエンドポイントセキュリティへの需要の増大が確認できる。

ただし、先進的エンドポイントセキュリティ（MES）製品は単独で存在するものではなく、相互補完的なセキュリティテクノロジーおよびセキュリティオペレーションの集合の一つの要素である。これらが連携して機能することによって、エンドポイントのセキュリティポスチャおよびビジネス機能の回復力が強化される。このような包括的な先進的エンドポイントセキュリティ（MES）という観点に立つと、企業は MES 製品が単独で提供するメリットに限定して評価を下すべきではない。セキュリティを強化し、セキュリティおよび IT オペレーションを拡張する、他のテクノロジーとの統合やワークフローの効率化についても検証する必要がある。これらのテクノロジーとしては、ハードウェアベースのデバイス完全性チェックと修復、エンドポイント／IT ハイジーン（衛生）管理、ファイルおよびデータのバックアップとリカバリー、EDR から XDR（eXtended Detection and Response）への進化がある。

IDC MarketScape ベンダー選定の基準

この調査に参加したのは、以下の基準を満たすベンダー各社である。

- エンドポイントで稼働する 1 つのソフトウェアエージェントから見たとき、そのベンダーの先進的エンドポイントセキュリティ（MES）製品が、EPP と EDR の両方を同時にサポートしている。
- 先進的エンドポイントセキュリティ（MES）製品がサポートするエンドユーザーのパーソナルコンピューティングデバイスプラットフォームには、少なくとも、Windows および macOS の最新バージョンが含まれる。
- ベンダーは、2019 年 1 月よりも前から、顧客向けに先進的エンドポイントセキュリティ（MES）製品の販売を開始している。
- 2020 年における EPP（アンチウイルス、または次世代アンチウイルスとも呼ばれる）、EDR、および先進的エンドポイントセキュリティ（MES）製品の民間企業および官公庁カスタマー向けの売上総額が（米国会計基準[GAAP]で）3,000 万ドル以上である。
- 2020 年の年末時点で、保護対象エンドポイント数 2,500 以上のカスタマーの割合が 5%を超えている。

IT バイヤーへの提言

脅威環境が多様化し、複雑化するなどしているのと同様、エンドポイントセキュリティ市場も進化している。

脅威環境はエンドポイントデバイスの「侵入後の対処」（compromising）に焦点を合わせる方向へ進化したように、本 IDC MarketScape に含まれる先進的エンドポイントセキュリティ（MES）のベンダー各社も進化した。そのため、企業のエンドポイントセキュリティ購買担当者は、自社の状況や要件に最も適したベンダーを幅広い選択肢の中から選ぶことができるようになった。IDC の

全般的なアドバイスは、戦略への適合性の観点からベンダーを評価することである。ベンダーとその MES 製品の選択は、単に現時点の脅威に対抗するためだけではない。明日になれば脅威は変化するからである。セキュリティオペレーションのコストや複雑性を軽減しながら、今後生じる可能性のある脅威に対しても対応可能なベンダーであるかどうかを基準に、長期的な観点から選択を行う必要がある。

具体的には、IDC は企業の MES バイヤー向けに以下のアドバイスを提供する。

- **まず焦点を合わせるべき MES の基本条件**
  - **保護の有効性**：IDC のバイヤー分析では、MES ベンダーの選択における企業の考慮事項のトップは、「今まで発生したことのない脅威や攻撃戦術に関するベンダーの調査や研究」が重要であるとしている。ただし、バイヤーは、ベンダーが調査や研究するだけでは満足せず、その結果を求めている。新しい形式の攻撃を自動的かつ確実にブロックすることほど、最良の結果はない。この意味で、保護の有効性に関する独立した評価は、有益な指針にはなるが、万能薬ではない。IDC は、POC（Proof of Concept：概念実証）実施することを推奨する。さらに、EPP に関する POC を恒常的な活動と位置づけることを推奨する。既存のベンダーが EPP 機能を進化させる一方で、新しいベンダーが「次世代」のアプローチを引っ提げて登場する状況の中、自社の環境における比較分析は、最良のリトマス試験紙となる。重大なセキュリティインシデントに見舞われた後で、より有効な MES 製品を探し始めるような事態は避けるためである。
  - **EDR の自動化**：バイヤーによるベンダー選択基準リストの 2 番目は、インシデント調査のスピードと容易性である。EPP による即時の防御を巧みに逃れ、エンドポイントに足場を築く攻撃が存在するのは、不幸な現実である。セキュリティチームは準備を整えておく必要がある。ただし、EDR 機能を備えるだけでは十分ではない。人間の関与が必要である。人が果たす役割を、調査プロセスではなく意思決定に集中させることが、脅威アクターの滞在時間とセキュリティ担当者の所要時間を短くする上で重要である。したがって、自動化は必要不可欠である。関連データの結合と相関付け、攻撃シーケンスの視覚化、リスク評価に応じたレスポンスの考案、選択したレスポンスの実行など、自動化にはさまざまな形式がある。さらに、企業が MES ベンダーを検討する際の重要な要因として、自動化された脅威ハンティングが挙げられている。ベンダーの自動化レベルや、セキュリティ担当者の立場から見た使いやすさを評価するには、POC（概念実証）を実施するのが最善の策である。
  - **デバイスのサポート**：MES 製品は、ソフトウェアエージェントによってサポートされているオペレーティングシステム（OS）を搭載したエンドポイントデバイスタイプに対してのみ、EPP および EDR 機能を提供する。当然のことながら、環境内に存在するデバイスタイプと OS プラットフォームのサポートについて確認しておく必要がある。本 IDC MarketScape の分析対象に含まれるベンダーはすべて、Windows および macOS の最新バージョンをサポートしている。ただし、攻撃を受けるデバイスタイプは Windows と Mac の PC だけではない。モバイルデバイス、物理および仮想サーバー、クラウドワークロードも標的になる。ベンダーのデータシートには、サポート対象のデバイスタイプと OS が記載されているが、機能の類似点や違いについてさらに詳しく調べ、そのベンダー製品が環境内のすべてのデバイスに対応し、統合管理を提供するかどうか確認することを、IDC は推奨する。
- **機能間の統合に関する検証**：エンドポイントセキュリティ機能とエンドポイント管理機能は、相互に関連している。パッチが適用されていない古いソフトウェアアプリケーションや古いバージョンの OS は、脅威アクターの標的となる。悪用された場合、セキュリティを補償するための次の 2 つのレイヤーとなるのが EPP および EDP である。企業には、専用のパッチ管理ソリューションがすでに存在している可能性が高い。この場合、時間の節約につながるワークフローの機能拡張や、迅速なリスク削減のため、ベンダー間の統合について検証する必要がある。さらに、製品スイートの一部としてパッチ管理を提供するベンダーが増えている。一連の機能セット（集合体）が企業 IT 資産のさまざまなニーズに対応する場合、これも適切な選択肢となる。加えて、パッチ管理はエンドポイントの攻撃

対象を削減し、結果的に悪用されにくくするための機能の一つである。その他の機能としては、デバイス制御、ファイアウォール管理、脆弱性評価、マイクロセグメンテーション、アプリケーションのブラックリスト／ホワイトリスト化、プロセスレベルの許可リストなどがある。MES ベンダーの検討に際して、ベンダーが提供するアタックサーフェス削減機能の集合と専用製品を比較することで、セキュリティポスチャの強化につながる有効な（場合によっては、より低コストを実現する）方法が明らかになる可能性がある。

- **XDR フレームワークの評価**：エンドポイントに影響を及ぼす攻撃を完全かつ迅速に把握するには、MES ソフトウェアのエージェントがエンドポイントから収集したテレメトリーだけでは不十分な場合がある。その他のソース（例：ネットワークセンサー、境界防御、電子メールおよび Web ゲートウェイ、クラウドアクセスセキュリティブローカー、アイデンティティ管理サービスなど）が、有益な補完情報をもたらす可能性がある。これらのソースの多くは、攻撃を緩和するためのレスポンスを適用したり、セキュリティポリシーを調整したりするための制御点でもある。非常に単純化した言い方をすれば、これは XDR（eXtended Detection and Response）の領域である。本 IDC MarketScape の分析対象に含まれるほとんどすべてのベンダーが、エンドポイント以外のセキュリティ製品ポートフォリオ、エコシステムパートナー、またはこれらの組み合せによって XDR フレームワークを提供している。MES 製品評価の一環として、ベンダーが提供している XDR の現状、今後の開発、セキュリティに対する付加価値、EDR から XDR への移行に必要な項目（例：追加費用、テクノロジーアップグレード、スタッフのトレーニングや補強）について評価する必要がある。
- **ランサムウェア対策および復旧オプションに関する確認**：ビジネスリーダーが最も懸念する問題は、ランサムウェアインシデントが起こった際の次の展開であるが、これは無理もないことである。IDC が 2021 年 7 月に実施したユーザー調査「*Future Enterprise Resiliency and Spending Survey, Wave 6*」では、過去 12 か月の間に 1 回以上のランサムウェアインシデントが発生した企業では、IT 意思決定者の 75%が、正常な状態に戻すには内部スタッフだけでは手に負えず、非常に多くのリソースが必要であったと回答している。ランサムウェアは他のマルウェアと同様、しばしばエンドポイントデバイスを通じてビジネスネットワークに侵入する。そのため、MES などのエンドポイントセキュリティ製品は、極めて重要な防衛線である。しかし、ランサムウェアが検知を潜り抜け、最終的に身代金の支払い可能性や金額を増加させるよう進化していったのと同じように、MES 製品もランサムウェアを検知し、その実行（例：データの流出、ファイルの暗号化）を防止して、他のエンドポイントや重要システムに伝播させないよう進化する必要がある。MES ベンダーのランサムウェア対策と、影響を受けたファイルおよびエンドポイント構成（例：レジストリーキーの変更など）を以前の正常な状態に戻すためのインシデント復旧オプションについて、ベンダーに問い合わせることを IDC は推奨する。その上で、自社の全体的なサイバーレジリエンシー計画の文脈に即して、これらの機能を評価する必要がある。
- **デバイスセキュリティ機能の組み込みに関する見通し**：何度も言うように、脅威アクターは攻撃の手法を絶えず進化させている。エンドポイントに侵入し乗っ取るための新しい手段を絶えず探っている。まだ主流にはなっていないが、攻撃者によってデバイスのファームウェアが危険にさらされることが、1 つの可能性として考えられる。この可能性が現実となってから対処するのではなく、ファームウェアの完全性を確認し修復するためのアプローチについて、MES ベンダーに問い合わせる必要がある。さらに、デバイスのチップベースの処理機能を活用する MES 機能の実行または補強についても問い合わせるべきである。最終的には、組み込みデバイスのセキュリティと、クラウドを利用した機能で補強したデバイス上のセキュリティソフトウェアとのコラボレーションが、エンドポイントセキュリティソリューションを測る物差しとなる。デバイスおよび MES 製品の購入に際して、セキュリティを最大化するような意思決定を行うには、組み込みデバイスのセキュリティ機能を活用するアプローチの現状および今後の計画について、MES ベンダーに問い合わせる必要がある。
- **マネージドサービスオプションの検討**：MES ベンダーは、EDR の自動化と簡素化に取り組んでおり、今後もそうすると予測されるが、EDR 機能を最大限利用するには、経験豊富なセキュリティ専門家が必要である。IDC は、MES ベンダーやチャネルパートナーが提供するマネージドサービスオプションを検討することを推奨する。サービスを巡るニー

ズは、契約レベル（例：オンデマンド形式のコラボレーションから、24 時間体制のアウトソーシングまで）や、実行するタスク（例：脅威モニタリング、脅威ハンティング、脅威レスポンス）によって異なる。そのため、現時点におけるニーズと予算に最も合致するというだけでなく、状況の変化に応じて調整できる柔軟性を備えたマネージドサービスを探す必要がある。

ベンダープロフィール（要約）

本セクションでは、IDC MarketScape の調査で得られた特定のベンダーに関する IDC の主な調査結果について簡単に説明する。付録に示す各基準を用いて、すべてのベンダーを評価したが、ここでは各ベンダーの強みと課題を要約する。

ESET

ESET（イーセット）は、企業向け先進的エンドポイントセキュリティ（MES）に関する 2021 年 IDC MarketScape で Major Players のカテゴリーに位置づけられている。

設立以来 35 年近い歴史があり、企業／商業用および消費者セグメントの両方に対応している ESET は、本 IDC MarketScape に含まれるベンダー中、最も長い歴史を持つベンダーの一つである。欧州で生まれた同社は、地域的な多様性を高めており、その企業顧客ベースは、エンドポイント数が 100 以下の企業から数千のエンドポイントを保有する大企業まで、均等な広がりを見せている。同社の歴史を通じて一貫しているのが、研究とテクノロジーを重視する企業文化と安定したリーダーシップである。

強み

非公開企業である ESET は、高い収益性を生かし、自社製品の進歩に直接貢献する分野（具体的にはソフトウェアの開発、脅威研究、脅威ハンティング）にその利益を再投資している。

ESET は西欧、中欧、東欧の幅広い顧客層に合わせ、各国の主要言語で顧客にサービスを提供している。欧州以外で重要なプレゼンスを有するその他の地域（北米、日本、中南米）では、直接またはパートナーを通じて、現地語によるサポートを提供している。

ESET は自社のエンドポイントセキュリティ製品の評価テストに意欲的であり、独立系 EPP 評価への ESET の参加はベンダー中でも上位に位置する。ESET Enterprise Inspector によって EDR 機能を発表したのが 2018 年であったため、EDR 評価への参加は他のベンダーほど早くはなかったが、それ以降、複数のテスト機関が実施する EDR 評価に積極的に参加している。

セキュリティ製品ポートフォリオに、電子メール、クラウド型ビジネスアプリケーション、クラウドアクセス、データ、アイデンティティを含む ESET は、ネイティブに統合された幅広い製品間プラットフォームソリューションを提供しており、他のベンダーと比べて相対的に充実した位置につけている。

ESET は、自社スタッフおよびパートナーを通じて MDR とマネージド脅威ハンティングサービスを提供し、顧客がスキル不足を解消できるように支援している。

前述のように、ESET はコンシューマー（消費者）セグメント向けセキュリティを提供している。コンシューマーセグメントで活動している他のベンダーと同様、ESET は独自に収集、分析した脅威データを有利に活用している。

課題

ESET にはほんの少し欠けている機能分野がある。たとえば ESET には、ランサムウェアによって侵害されたユーザーファイルや設定を攻撃前の状態に戻すためのロールバック修復機能がない。しかし、ESET が独自に開発した 2 つのテクノロジー、Network Attack Protection および Ransomware

Shield によるランサムウェア防御に重点を置いていることは明らかである。また、ESET のハードウェアベースのセキュリティ機能にも限界がある。ハードウェアベースとまったく同じわけではないが、アプリケーションレイヤー以下で動作する保護機能が、OS 起動前認証（プリブート認証）である。ESET は UEFI スキャンを標準機能として追加した。その UEFI Scanner は、デバイスの起動に先立って起動する可能性のある脅威をスキャンする。

アタックサーフェスの削減を目的とする ESET の機能集合は、この市場のいくつかのベンダーほど幅広く提供されているわけではない。ESET は、デバイス制御とホストファイアウォール管理を製品内部でネイティブに提供している。脆弱性評価とパッチ管理は、今のところネイティブやサードパーティによる統合を通じても、ESET のソリューションセットに含まれていない。

ESET の MES ビジネスは着実に成長しているが、世界規模で見ると、市場全体の伸びが ESET の成長を上回っている。ESET の競合リスクは、大規模な世界的ベンダーの POC への参加という面で ESET を締め出す可能性である。

ESET を検討すべき状況

既存の ESET エンドポイントセキュリティの顧客企業は、ESET の EDR 機能を試用すると共に、今後のロードマップ機能について検討すべきである。ESET の長年に渡る機能拡張の歴史から、同社と競合他社の間に機能的な差があったとしても、その差は縮まっていく可能性が大きい。また、前述のように ESET には、脅威検知のための有益なテレメトリーを提供し、ポリシー実施（予防および対応）のための追加コントロールポイントとなる、別の分野のセキュリティ製品がある。これは、より少ないベンダーでセキュリティスタックを統一したい企業や、脆弱性評価とパッチ管理にそれぞれ別のベンダーを利用しても構わない企業にとっては有利である。統合管理に関する評価では、一元的な管理と、それによるセキュリティスタッフの生産性向上への貢献に着目すべきである。管理者やアナリストの経験に加え、インテグレーションに関するベンダーの主張と実際の製品間インテグレーションの違いも、重要な問題である。さらに、ESET のパートナーエコシステムを自社のマルチベンダー環境と比較し、ベンダー間におけるテレメトリーの交換や、レスポンスのオーケストレーションが自社の要件を満たすかどうかを確認する必要がある。

補遺

IDC MarketScape Graph の見方

IDC は本調査の中で、企業の成功の可能性を測る主要な因子を、能力と戦略という 2 つのカテゴリーに分けて分析している。

Y 軸は、ベンダーの現在の能力とサービスメニュー、そして顧客のニーズにどの程度うまく合致しているかを反映している。この能力カテゴリーは、今日、この時点での企業および製品の能力に焦点を合わせている。このカテゴリーに基づき、IDC アナリストは、企業が選択した市場戦略を遂行する上で、こうした能力をどのように組み立て発揮しているかを分析する。

X 軸、言い換えると戦略軸上の位置は、ベンダーの将来戦略が 3〜5 年後の顧客ニーズに応えられる度合いを示す。この戦略カテゴリーは、製品／サービス、顧客セグメント、ビジネスに関するハイレベルの意思決定や仮説、そして今後 3〜5 年間の市場開拓計画に焦点を合わせている。

IDC MarketScape において各ベンダーを表すマーカーの大きさは、評価対象である市場セグメントにおけるそれぞれのベンダーの市場シェアを表す。

IDC Marketscape 調査方法

IDC MarketScape における評価基準の選択、重み付け、ベンダースコアは、市場やベンダーに関する十分な調査に基づいた IDC の判断によって設定されている。IDC アナリストは、標準的な特性の範囲を定め、その基準に基づき、市場のリーダーや関係者、エンドユーザーとの体系化された議論、サーベイ、インタビューを通して、ベンダーの評価を行っている。市場の重み付けは、ユ

ーザーインタビュー、バイヤー調査、IDC の各市場の専門アナリストで構成されるレビュー委員会のインプットに基づいて行われている。IDC のアナリストは、それぞれのベンダーの特徴や対応、能力について正確かつ一貫性のある評価を行うため、ベンダーの詳細なサーベイやインタビュー、公開情報、そしてエンドユーザーエクスペリエンスに基づき、各ベンダーのスコア、そして最終的には IDC MarketScape 上のポジショニングを算出している。

市場定義

先進的エンドポイントセキュリティ（MES）製品は、パーソナルコンピューティングデバイス（PCD、ワークステーションやラップトップなど）上に存在する、またはその内部で動作する悪意のあるコードや振る舞いを検知し、対応（例：ブロック、削除、隔離）を実行することによって、サイバー攻撃から PCD を保護する。先進的エンドポイントセキュリティ（MES）製品には、2 つの検知と対応メカニズムがある。これらは経過時間と人的な関与に基づいて区分される。EPP（Endpoint Protection Platform）は、検出判定を下し、リアルタイムかつ自律的に（すなわち、人間による関与を必要とせず）対応を開始する。EDR（Endpoint Detection and Response）は、EPP による検知を回避したサイバー攻撃に対する、第 2 段階の検知および対応である。EDR では、検出判定を取得して対応を開始するまでに、数分から数日を要する場合がある。検知と対応に必要な経過時間に影響する要因としては、サイバー攻撃の展開の速さ、攻撃ステップの手順、巧妙性や独自性がある。この経過時間の短縮には、自動化とあらかじめ定義されたワークフローが役立つ。最低でも検知の確認や対応の承認のため、一般には、セキュリティアナリスト（人間）による関与が必要である。

参考資料

関連調査

- *Top Technology Integration Opportunities for Unified Endpoint Management*（IDC #US48266821、2021 年 9 月発行）
- *Market Analysis Perspective: Worldwide Tier 2 SOC Analytics, 2021 – Where the Puck Is Going*（IDC #US47394921、2021 年 9 月発行）
- *Market Analysis Perspective: Worldwide Corporate Endpoint Security, 2021*（IDC #US48208121、2021 年 9 月発行）
- *IDC's 2021 Ransomware Study: Where You Are Matters!*（IDC #US48093721、2021 年 7 月発行）
- *Which Criteria Rank Highest in the Evaluation of Modern Endpoint Security Products?*（IDC #US48053021、2021 年 7 月発行）
- *Worldwide Corporate Endpoint Security Forecast, 2021-2025: On a Higher Growth Trajectory*（IDC #US47957021、2021 年 6 月発行）
- *Worldwide Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth*（IDC #US47768021、2021 年 6 月発行）
- *Insights from IDC's EDR and XDR 2020 Survey: Operational Challenges and Initiatives Are Abundant*（IDC #US47357921、2021 年 1 月発行）

Synopsis

本 IDC 調査レポートでは、IDC MarketScape モデルによるエンタープライズ向け先進的エンドポイントセキュリティ（MES）のベンダー評価を提供する。

IDC Security and Trust のリサーチバイスプレジデントである Michael Suby は、「先進的エンドポイントセキュリティ（MES）製品は、ポイントソリューションから、複数の機能を実行するセキュリティプラットフォームに進化している。このように進化した主な原因は、時間である。脅威アクターによってセキュリティ防御体制の脆弱性や弱点が発見および悪用されるペースが速まっている。逆に言うと、企業のセキュリティ専門家は一刻の猶予も許されない。脅威への対応に追われる現状から、脅威の先回りをする状態への変化を望むのであれば、広範囲の IT 資産全体に渡っ

て、より迅速かつ効率的なオペレーションが必要である。先進的エンドポイントセキュリティ（MES）製品が辿っている軌跡は非常に心強い。ベンダー各社は、まずエンドポイント保護とエンドポイント検知およびレスポンスを統合し、1つにまとまったリスク削減および侵入回避プラットフォームに、その他のセキュリティ機能やITハイジーン機能を組み込みつつある」と述べている。

IDC 社 概要

International Data Corporation（IDC）は、IT および通信分野に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。50 年にわたり、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。

現在、110 か国以上を対象として、1,100 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っています。

IDC は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com