SOPHOS

エンドポイントセキュリティ バイヤーズガイド

サイバー脅威が複雑化する中、適切なエンドポイントソリューションを特定して導入することが、多くの企業で重要な課題になっています。しかし、エンドポイントセキュリティ市場には多くのソリューションが溢れており、各社はマーケティング目的の裏付けのない主張を展開しているため、十分な情報に基づいて最適なソリューションを選択することは容易ではありません。

このガイドでは、エンドポイントプロテクションソリューションの主な機能と、現在の高度な脅威から保護するために求められる能力について説明します。このような知見を得ることで、エンドポイントソリューション選びで優れた決断が可能になり、自社のセキュリティを向上できるようになるはずです。

ソフォス ホワイトペーパー 2023 年 10 月

セキュリティ脅威の現状

ソフォスが 14 カ国の IT 部門やサイバーセキュリティ部門のリーダー 3,000 人を対象に行った新しい調査から、サイバーセキュリティの戦いにおいて攻撃者と防御側のスピードが異なっていることが明らかになりました。防御側ではいくつもの課題が山積している一方で、攻撃者は加速度的に攻撃を進化させています。

サイバー犯罪者の経済圏の進化

この数年の脅威環境における最も大きな変化の 1 つは、サイバー犯罪者の経済圏に、犯罪を助長するサービスのネットワークが加わり、運用に関する専門的なアプローチが確立されており、サイバー犯罪が 1 つの産業になったことです。

テクノロジー企業は製品を「サービスとして」提供するようになりましたが、サイバー犯罪のエコシステムも同じようにサービスへと移行しています。これにより、サイバー犯罪に加担することが非常に容易になり、サイバー攻撃者は多くの攻撃を迅速化し、その影響力を増大させています。

その結果、サイバー攻撃者は多様で高度な攻撃を大規模に実行できるようになりました。94% の組織が過去 1 年間に 1 回サイバー攻撃を受けています。最も多く報告された攻撃はランサムウェアでしたが、組織はその他にも以下のようなさまざまな脅威を経験しています。[1]

27% 悪意のあるメール	27% フィッシング (標的型攻撃を含む)	26% データの外部への流出 (攻撃者による)
24% オンライン恐喝	24% ビジネスメール詐欺 (BEC)	21% モバイルマルウェア
18% クリプトマイナー	24% サービス拒否 (DDoS)	14% ワイパー型マルウェア

詳細については、「サイバーセキュリティの現状 2023 年版：サイバー攻撃者が防御側組織のビジネスに及ぼす影響」を参照してください。

後を絶たないランサムウェア攻撃の被害

3 分の 2 (66%) の組織が昨年ランサムウェア攻撃の被害を受けたと回答しています。

2020	2021	2022	2023
51%	37%	66%	66%

過去 1 年間にランサムウェア攻撃を受けましたか？
はい。 回答者数 = 3000 人 (2023 年)、5,600 人 (2022 年)、5,400 人 (2021 年)、5,000 人 (2020 年)

2023 年に報告された攻撃の割合は 2022 年と同水準でしたが、ランサムウェア攻撃を受けてデータが暗号化された割合は過去 4 年間で最も高い水準にあり、4 分の 3 以上 (76%) の攻撃でデータの暗号化に成功しています。

また、ランサムウェアの被害額もかつてないほど高額になっており、組織が影響を復旧するために必要となる平均費用は 182 万ドルと報告されており、2022 年の 140 万ドルから増加しています。[2]

ソフォスが毎年公開しているランサムウェアの調査レポート「ランサムウェアの現状 2023 年版」を参照して、攻撃の頻度、費用、根本原因など、2023 年に組織が直面した現実をご確認ください。

1 サイバーセキュリティの現状 2023 年版：サイバー攻撃者が防御側組織のビジネスに及ぼす影響」- 14 か国の IT/ サイバーセキュリティを担当するリーダー 3,000 人を対象に 2023 年 1 月と 2 月に独自に実施された独自調査から得られた知見。

2「ランサムウェアの現状 2023 年版」、ソフォス - 14 か国の IT/ サイバーセキュリティリーダー 3,000 人を対象として 2023 年 1 ～ 3 月に実施された独自調査から得られた知見。

従来のやり方ではセキュリティの成果が低下

近年、多くの組織のビジネス環境が変化しました。エンドユーザーは、オフィスに出社することもあれば、リモートで仕事をすることもあります。また、顧客やパートナーのオフィスに行くこともあるでしょう。企業データはオンプレミスだけに保存されているわけではありません。オンプレミス、クラウド、エンドユーザーのデバイスに存在しており、さまざまな場所で働く従業員のニーズに対応するためにローカルやリモートからアクセスできるようになっています。その結果、従来型のサイバーセキュリティのアプローチを使用し続けても、十分な成果を得られないことが多くあります。

IT セキュリティチームは、通常、次のような問題を抱えています。

- **スキルの不足 -** スキルのある IT 従業員を採用することは依然として困難です。多くの従業員の経験が不足しており、セキュリティアラートが本当の脅威を示しているかどうかを判断することができません。
- **余りにもノイズが多い -** さまざまなシステムから発行されるアラートが多すぎるため、オペレータは調査が必要なシグナルやアラートの優先順位を付けることができず、攻撃の指標を見逃す可能性があります。
- **データのサイロ化 -** 導入した特定のテクノロジーから脅威のシグナルやアラートが提供されますが、相関されないため、IT チームは全体像を把握できず、悪意のあるアラートやインシデントを迅速に修正できません。
- **統合されていない –** セキュリティツール間が相互に統合されていない、また、より広範な IT インフラストラクチャと統合されていないため、複雑さが増加しています。
- **手動のプロセス –**IT チームは、発生している問題を把握するために、イベント、ログ、情報の関連付けに貴重な時間を費やしています。この作業に時間を取られるため、攻撃の特定と対応が遅れることがあります。
- **受け身の対応 -** 上記のような問題があるため、多くの IT チームは攻撃者の後手に回っており、攻撃チェーンの早期の段階で脅威を食い止めることができず、脅威による影響を受けた後にしか対応できなくなっています。
- **緊急の対応に追われる -** 脅威を防ぐための日々の作業に追われて、長期的にセキュリティを強化するための戦略にまで手が回らなくなっています。IT チームが緊急対応に追われているときには、インシデントの根本原因を特定したり、攻撃や実行した対応を正確に記録できないことも多くあります。このような状況が続くと、構造的な問題を解決することは困難になります。
- **分散するデータ -** ユーザーとデバイスは企業のオフィスだけではなく、さまざまな場所に分散しています。そのため、ユーザーと同じように、データもオンプレミス、クラウド、デバイス、あらゆる場所に分散しており、ローカルまたはリモートアクセスソリューションからアクセスされています。

これらの多くの課題に対処する 1 つの方法は、最高クラスのエンドポイントプロテクションソリューションを導入することです。

エンドポイントプロテクションの基本機能

優れたエンドポイントセキュリティソリューションは、柔軟に利用でき、攻撃に合わせて組織を防御できなければなりません。最新のエンドポイントセキュリティソリューションは、最低限、予防を重視する以下のようなアプローチを採用している必要があります。

脅威にさらされる危険性を軽減 - 悪意のあるコンテンツと Web ベースの脅威をブロックし、アプリケーション、Web サイト、周辺機器などへのアクセスを制御します。

悪意のあるアクティビティをブロック - 悪意のあるコードやランサムウェアが目的を達成するために使用する手法を防止し、特定のアクティビティを識別し、実際に影響を受ける前に脅威を阻止します。

攻撃の変化に合わせて自動的に対応できる防御 - 組織は、脅威に自動的に対応でき、変化する攻撃者の行動に合わせて防御できるようにする必要があります。このような防御体制によって、攻撃者にとっての障害を作り出すだけでなく、攻撃者がネットワークに存在していることをチームに通知して、チームが対応するための貴重な時間を得ることが可能になります。

自社あるいはマネージドサービスの脅威ハンティングを強化 - 高品質のシグナルにセキュリティ情報を追加して強化して、脅威の検出と対応を劇的に加速できます。優れた情報を多く取り入れることができれば、より迅速に問題を解決できます。

セキュリティの最適な成果を実現する

ここまでは、エンドポイントプロテクションソリューションに求められる機能の概要を説明しましたが、これらのソリューションが組織にどのようなメリットをもたらすかについて、広い視点で考えることも不可欠です。強力なエンドポイントプロテクションは、セキュリティの優れた成果をもたらすように機能しなければなりません。

サイバーリスクの削減

強力なエンドポイントプロテクションは、サイバーリスクを低減し、膨大なサイバー脅威から組織を保護します。

予防重視のアプローチ

攻撃を早期に防止できれば、後で処理すべきことは少なくなります。優れたエンドポイントプロテクションは、コンピュータ、ラップトップ、モバイルデバイス、サーバーを標的とするサイバー脅威や攻撃を防御するために、いくつもの保護レイヤーを使用します。エンドポイントプロテクションは、これらのデバイスとデータを、マルウェア、ウイルス、ランサムウェア、その他の悪意のある攻撃から保護します。

セキュリティ対策のずれやミスを特定

セキュリティ対策は、さまざまな理由で、時間とともに変化します。独立した調査会社が実施した最近の調査では、セキュリティツールの設定ミスが、2023 年に IT 管理者が認識しているセキュリティリスクのトップに挙げられています。[3]

常にセキュリティ対策を評価でき、設定を最適化できるエンドポイントセキュリティソリューションを見つけてください。これらが自動化されているアプローチであれば、強力なセキュリティ体制を実現し、サイバーリスクを低減し、手動の作業という頭痛の種を軽減できます。

管理の合理化

管理コンソールが一元化されていれば、IT 管理者はすべてのエンドポイントのセキュリティ設定、ポリシー、除外、脅威アラートを 1 カ所から監視および管理できます。これにより、セキュリティ管理が簡素化され、設定ミスのリスクが軽減され、一貫した保護を保証できます。一元的に管理されるコンソールの中には、セキュリティ対策の「状態」を自動的にチェックし、危険にさらす可能性のあるアクティビティやポリシーの変更にフラグを立てるなど、一歩進んだ機能を提供しているものもあります。

検出と対応の迅速化

お客様の環境に攻撃者が侵入しているときは、一刻を争います。予防重視のアプローチを採用した高品質のエンドポイントプロテクションは、ノイズを減らし、精度の高いアラートを提供します。これらのアラートを調査するためには、EDR (Endpoint Detection and Response) および XDR (Extended Detection and Response) のテクノロジーを使用できます。

さらに、人工知能 (AI) や脅威インテリジェンスを活用し、検出された脅威を調査する優先順位を自動的に決定するソリューションもあります。これらのソリューションは、チームが貴重な時間をどの問題に集中すべきかを明確に示し、アナリストによる脅威対応を加速させます。

IT チームの効率性の向上

64% の企業が、IT チームがサイバー攻撃に対する緊急対応に費やす時間を減らし、より多くの時間を戦略的な問題に費やことを望んでいます。[4] 自動化されており、使いやすいエンドポイントプロテクションであれば、IT チームはこの目標を実現できます。

優れたエンドポイントソリューションは、多くの脅威が影響を及ぼす前に自動的にブロックし、クリーンアップします。これにより、IT 部門のリソースが解放され、ビジネス関連の取り組みに優先的にリソースを割り当てることができるようになります。XDR のようなテクノロジーは、アラート疲れを軽減し、企業にとって重要なプロジェクトに多くの時間を割り当てることができるようにします。

IT チームの効率性が向上すれば、最終的には、受け身型から、脅威による影響を事前に防止するプロアクティブなサイバーセキュリティに移行できます。これらのチームは、脅威による影響を修正するのに長時間をかけてるのではなく、脅威の検出に時間をかけることが可能であり、サイバーリスクを軽減できます。

3 サイバーセキュリティの現状 2023 年版：サイバー攻撃者が防御側組織のビジネスに及ぼす影響」- 14 か国の IT/ サイバーセキュリティを担当するリーダー 3,000 人を対象に 2023 年 1 月と 2 月に独自に実施された独自調査から得られた知見。

4 サイバーセキュリティの現状 2023 年版：サイバー攻撃者が防御側組織のビジネスに及ぼす影響」- 14 か国の IT/ サイバーセキュリティを担当するリーダー 3,000 人を対象に 2023 年 1 月と 2 月に独自に実施された独自調査から得られた知見。

サイバーセキュリティの ROI (投資効果) の向上

強力なサイバーセキュリティによって、大規模なセキュリティインシデントによる財務上および業務上の影響から組織を保護することが可能になります。

この時には、優れたエンドポイントプロテクションへの投資が鍵になります。脅威を予防できれば、攻撃による影響を修復するよりもはるかにコストは安くなります。強力なエンドポイントプロテクションは、脅威の大部分を侵入する前にブロックするため、攻撃を受けて対応するコストを負担する可能性も低くなります。

さらに、最高クラスのエンドポイントプロテクションソリューションは、これまでに投資したセキュリティ製品と統合および連携させることができ、保護能力を拡張し、複雑さを緩和し、既存のプロテクションテクノロジー (メール、ファイアウォール、ネットワーク、アイデンティティ、クラウドなど) がより優れた成果を発揮させるようにできます。

これらはすべて、サイバーセキュリティの ROI (投資効果) を向上させ、総所有コストを削減させます。

サイバー保険の等級の最適化

サイバー保険の保険料は近年大幅に上昇し、保険契約の申し込みも複雑化し時間がかかるようになりました。保険会社はサイバーセキュリティ対策の強化を求めています。実際、昨年保険に加入した組織の 95% が、自社のサイバーセキュリティ防御の体制が保険の等級に直接影響したと回答しています。[5].

保険の等級を最も有利にする鍵は、サイバーリスクを最小化することです。継続的なセキュリティサービスの実施や主要な検出および対応ツールなど、防御力を強化する投資を行うことで、サイバー保険への加入や等級に関するいくつもの利点を得ることができます。

1. サイバー保険に加入しやすくなる (サイバー保険への加入条件を満たしやすくなる)
2. 保険料を低く抑え、条件を改善できる
3. 保険金請求の可能性を軽減できるため、保険料が低くなる
4. 保険金を請求しなければならないときに、保険金が支払われないリスクを削減する

最高クラスのエンドポイントプロテクションテクノロジーは、検出と対応の機能の橋渡しとしての役割を果たします。検討しているベンダーがこれらの機能を提供していることを確認してください。エンドポイントの検出と対応 (EDR) 機能を導入することは現在、多くのサイバー保険会社で保険加入の前提条件となっており、この機能を導入していない組織は通常、保険を契約することが困難になっています。

検出と対応を最適化し、サイバーインシデントの発生リスクを最小化するサービスは、サイバー保険会社にとって重要な「評価基準」になっています。特に MDR (Managed Detection and Response) サービスを利用する組織は、リスクレベルが最も低くなることから、保険会社から最も優先度の高い顧客と見なされることが多くなります。

つまり、エンドポイントプロテクションソリューションから、既存の製品やサードパーティのセキュリティコントロールと統合でき、24 時間 365 日のフルマネージドの脅威ハンティング、検出、インシデント対応サービスにシームレスにアップグレードできるようにしているベンダーを検討することが重要です。

5 サイバー保険導入における最前線のサイバー防御の重要な役割 - ソフォス

エンドポイントセキュリティの評価：確認すべき 10 のポイント

ここまでは、最高クラスのエンドポイントセキュリティソリューションに求められる機能や要素について説明してきました。ここからは、候補となったベンダーに確認するべき質問を以下に示します。

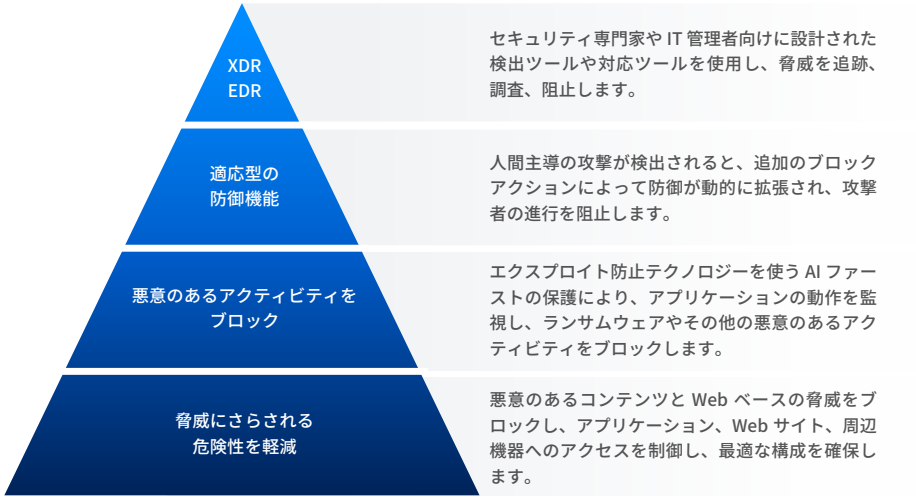
1. 製品は予防を重視した多層防御のアプローチを取っていますか？それとも検出を重視したアプローチを取っていますか？テクノロジーの中核を成すのは具体的にどの機能ですか？
2. セキュリティ対策のギャップやミスを検出して自動的に修正する機能はありますか？リスクを増大させるポリシー設定の変更を明確に伝えることはできますか？
3. その製品は自動的に脅威に対応しますか？脅威の除去とインシデント対応を自動的に実行できますか？
4. ハンズオンキーボード攻撃が検出されたときに、自動的に対応する防御機能を備えていますか？
5. 製品に強力なランサムウェア対策とエクスプロイト対策機能はありますか？これらの機能はデフォルトで有効になっていますか？これらの能力は、自社環境で機能させる前に起動して訓練する必要はありますか？
6. 製品を管理するために必要なコンソールの数はいくつですか？コンソールはクラウドでホスティングされますか、それともオンプレミスにインストールする必要がありますか？
7. 同じ管理コンソールとエンドポイント / サーバーの同じエージェントを使用して、製品を EDR/XDR にシームレスに移行できますか？
8. XDR の機能は、ネイティブおよびサードパーティのセキュリティ管理機能のアラートを統合して取り込み、環境の全体像を把握できますか？
9. 製品は、既存の製品やサードパーティのセキュリティコントロールと統合でき、24 時間 365 日のフルマネージドの脅威ハンティング、検出、インシデント対応サービスにシームレスにアップグレードできるようにしていますか？
10. ベンダーは、エンドポイントセキュリティへのアプローチを検証する第三者テスト機関、アナリスト、顧客の評価を公開していますか？

ソフォスのアプローチ

ソフォスのエンドポイントプロテクションのアプローチを見ていきましょう。ソフォスのエンドポイントセキュリティソリューションである Sophos Intercept X は、高度な攻撃に対する比類のない防御機能を提供し、洗練されたさまざまなテクノロジーを採用して、お客様のシステムに影響が及ぶ前に、広範な脅威を阻止します。強力な EDR および XDR ツールにより、組織は疑わしいアクティビティや攻撃の兆候を追跡、調査し、対応できます。

予防重視のアプローチ

Sophos Endpoint は、1 つのセキュリティテクノロジーに依存することなく、すべてのエンドポイントを保護するための包括的なアプローチを採用しています。できるだけ多くの脅威を早い段階で阻止することで、人手による調査や対処が必要なインシデントを減らし、リソースが限られている IT チームの負担を減らすことができます。



脅威にさらされる危険性を軽減

Sophos Endpoint は、お客様が脅威にさらされる危険性を軽減し、攻撃者が企業環境に侵入する機会を減らします。悪意のある Web コンテンツや Web ベースの脅威をブロックし、アプリケーション、Web サイト、周辺機器へのアクセスを制御します。

Web ベースの脅威をブロックし、Web アクセスを制御

Web ベースの脅威はさまざまです。多くの組織は、フィッシングや悪意のある Web サイト、その他の Web ベースの脅威から、オフィスで勤務するユーザーを保護するために次世代ファイアウォールを使用しています。これらのファイアウォールは、オフィスネットワークにあるエンドポイントを保護しますが、エンドポイントは自宅、外出先、カフェなど、ファイアウォールで保護できない場所で使用されることもあります。

Sophos Endpoint は、ファイル、Web ページ、IP アドレスを分析することにより、フィッシングサイトや悪意のある Web サイトへのアクセスをブロックします。エンドポイントがどこで利用されていても、常に脅威から保護することが可能です。

さらに、SophosLabs と Sophos MDR チームは、新たな脅威からソフォスのお客様を保護するために、リアルタイムの脅威インテリジェンスを提供しています。

Web、周辺機器、アプリケーションの制御

ソフォスの製品は、エンドポイントでの活動を制限できます。このようなコントロール機能は、通常、組織が定めている使用ポリシーと一緒に使用されます。

最初に、特定のカテゴリの Web サイト (ギャンブルやソーシャルメディアなど) へのアクセスを監視 / ブロックします。Sophos Endpoint では、特定のカテゴリの Web サイトを監視し、ブロックできます。

また、リムーバブルメディアやその他の周辺機器へのアクセスを制御することで、攻撃対象領域をさらに縮小できます。ユーザーがプリンターや USB ストレージデバイスを取り付けたり、USB ポートからスマートフォンを充電したりする場合を考えてみましょう。そのような操作を許可していますか？このコントロール機能は、悪意のあるコードがエンドポイントに侵入するのを阻止するだけでなく、企業データの外部への流出を阻止するのにも役立ちます。

使用を許可するアプリケーションのカテゴリも検討する必要があります。アプリケーションコントロールでは、業務用のデバイスで実行されるアプリケーションやブラウザプラグインをブロックできます。データの外部への流出を防ぐために、クラウドストレージの OneDrive や Google Drive のようなアプリケーションの使用について検討する必要があります。また、トレントプログラムや TOR ブラウザなどについても検討し、エンドポイントでそれらの使用を許可すべきかどうかを検討します。Web ブラウザのプラグインも多岐にわたります。多くは合法的であり、業務のために活用できますが、そうでないプラグインも存在します。

悪意のあるアクティビティをブロック

次の防御レイヤーでは、人工知能、挙動分析、ランサムウェア対策、エクスプロイト対策、その他のテクノロジーを使用して、脅威が拡大する前に迅速に阻止します。

ソフォスは、AI によって実行可能ファイルを分類するなど、保護機能に AI を積極的に採用しています。何百万もの問題のない実行ファイルと悪意のある実行ファイルについて訓練したモデルを利用しています。このモデルは、悪意のある実行可能ファイルをプロパティに基づいて迅速かつ効果的に識別することができ、シグネチャを必要としません。

ランサムウェア対策

Sophos Endpoint には、暗号化の兆候を中心に検出する高度なランサムウェア対策テクノロジーが搭載されています。このアプローチでは、新しい亜種やこれまでに検出されていないランサムウェアも阻止できます。ファイルの内容を検査して、サーバーにあるファイルを暗号化するネットワーク上で実行されている暗号化とランサムウェアを検出します。ランサムウェアによって暗号化されたファイルは、サイズやファイルの種類に関係なく、自動的に安全な状態にロールバックされ、ビジネスの生産性への影響を最小限に抑えます。また、一部のランサムウェア攻撃で使用されている暗号化の手法からマスターブートレコード (MBR) を保護しまし。

エクスプロイト対策

エクスプロイト対策テクノロジーは、攻撃者によるデバイスの侵害、認証情報の盗取、マルウェアの配信に使用される動作や手法を阻止します。ソフォスは、すべてのアプリケーションに対して、新しいオンデバイスエクスプロイト対策アプローチを大規模に導入しています。ソフォスは、Microsoft Windows で提供される基本的な保護機能に、事前に構成および調整された少なくとも 60 個のソフォス独自のエクスプロイト対策機能を追加しています。これらの機能はそのまますぐに使用できます。これにより、攻撃チェーン全体で使用される手法を阻止することで、ファイルレス攻撃やゼロデイ攻撃から組織を保護します。

適応型の防御機能

これらの適応型の防御は、攻撃の状況に合わせて自動的に防御をステップアップするセキュリティ業界初の取り組みです。Sophos Endpoint は、通常業務で使用されることがある一般的な操作であっても、攻撃に転用される危険性がある場合はブロックします。攻撃者がレッドフラグを立てたり悪意のあるコードを使用したりせずに、攻撃を進行させ足掛かりを築いている可能性のある場合に、この機能によって動的に対応して阻止します。

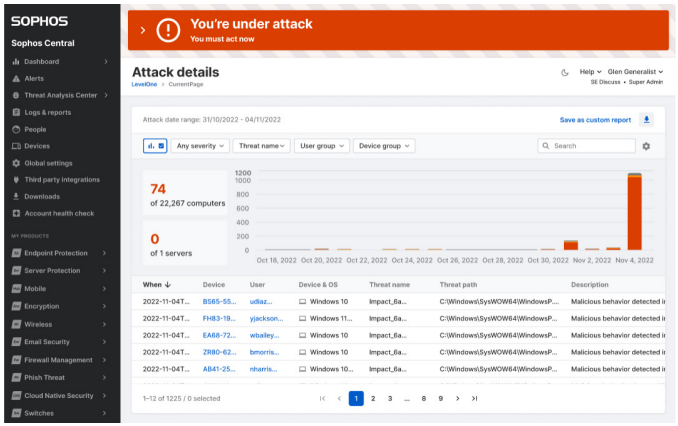
	振る舞い検知	適応型攻撃防御	Critical Attack Warning (重大な攻撃の警告)
範囲	個々のデバイス	個々のデバイス	個々のデバイス
特長	アクティブアドバーサリによる攻撃の初期段階を阻止する挙動検出エンジン	保護の感度 (レベル) を高めて被害を防止します	即時のインシデント対応が必要な攻撃を顧客に警告
トリガー	動作検出ルール	ハッキングツールセットの検出	組織レベルの相関関係やしきい値などの、影響の大きいアクティブアドバーサリの指標
アナロジー	「シールドオン！」	「シールドアップ！」	「レッドアラート！」

適応型攻撃防御

適応型攻撃防御は、「ハンズオンキーボード」攻撃が検出された場合に、エンドポイントの防御レベルを動的に強化します。これにより、攻撃者が追加の操作を実行する能力が失われ、攻撃を妨害して封じ込めると同時に、対応するための貴重な時間を確保できます。

Critical Attack Warning (重大な攻撃の警告)

Critical Attack Warning は、環境内の複数のエンドポイントまたはサーバーで攻撃者による活動が検出され、深刻な影響をもたらす攻撃を示す指標が見つかった場合に、重大な攻撃が環境全体で進行していることを警告します。これは攻撃を受けていることを示す、深刻な状況 (レッドアラート) です。自動化されたテクノロジーが状況を通知し、攻撃のコンテキストや詳細を提供します。これらの脅威に対しては、Sophos XDR を使用して自社で対応することも、パートナーや Sophos Incident Response チームに支援を要請することもできます。



サイバーセキュリティの総所有コストの削減

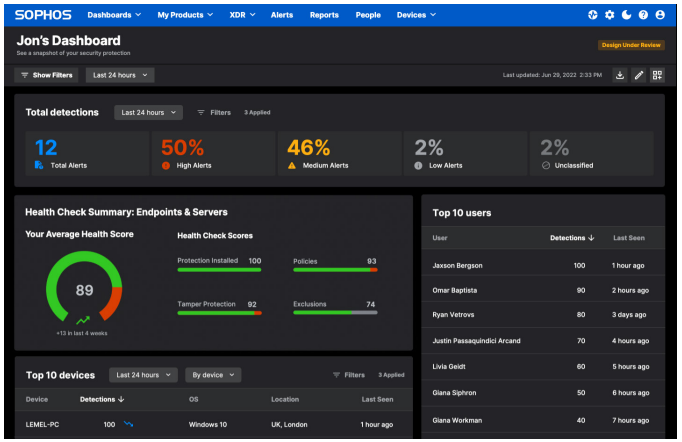
多くの組織の IT チームやセキュリティチームには余裕がありません。Sophos Endpoint は、作業の自動化を進めて、スタッフの時間と労力を節減できるようにすることを重視しています。IT チームやセキュリティチームの作業を自動化、削減、除去できれば、これらのチームは他のビジネスイニシアチブに注力できるようになります。

Sophos Central は、Sophos Endpoint を含むソフォス製品 (エンドポイント、サーバー、モバイルデバイス、ファイアウォール、スイッチ、アクセスポイント、メール、クラウド) を管理するクラウドベースの管理プラットフォームを提供します。ポリシーの作成と管理、検出した脅威とアラートの表示、潜在的な脅威の調査と修復、他のさまざまなソフォス製品のアクションで 1 箇所から実行できます。

ソフォスが推奨する保護テクノロジーはデフォルトで有効になっており、簡単に設定でき、複雑な調整をすることなくすぐに最強の保護設定を利用できます。必要な場合には、詳細にコントロールすることもできます。

セキュリティ対策のずれやミスの特定

組織のセキュリティ対策は、時間が経過すると、時代に沿わなくなり、最適な構成ではなくなることもあります。ポリシー、除外、およびその他の要因が適切に構成されていない、セキュリティ体制にリスクが生じます。ソフォスのアカウントの状態チェックは、セキュリティ対策のずれとリスクの高い設定ミスを特定し、ワンクリックで問題を修正できるようにします。

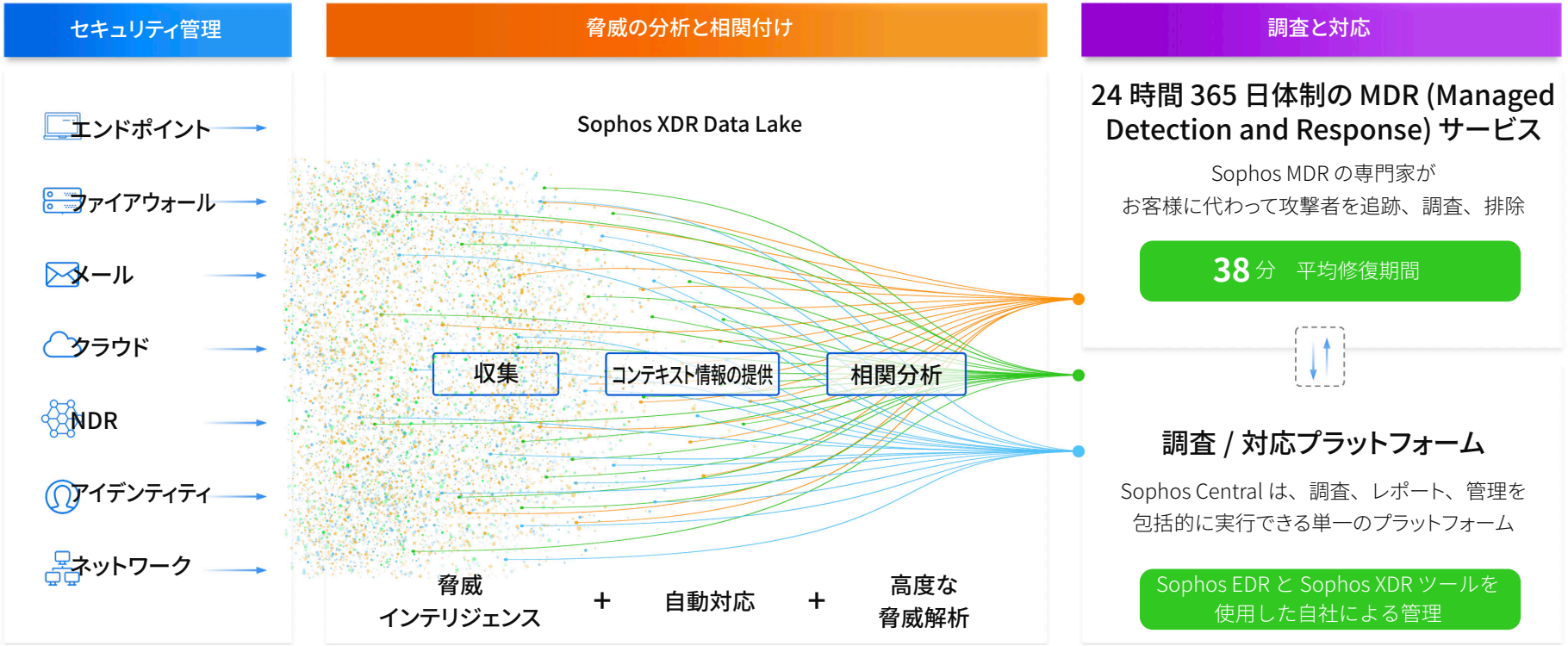


Synchronized Security

ソフォスは互いに連携したソリューションを提供します。Sophos Endpoint は、Sophos Firewall、Sophos ZTNA、およびその他の製品とステータスおよびセキュリティ状態の情報を共有して、脅威とアプリケーションの使用状況をさらに可視化します。Synchronized Security は、クリーンアップの実行中に侵害されたデバイスを自動的に隔離し、脅威が無力化されるとネットワークアクセスを自動的に復旧します。これらが管理者の介入なしで実現できます。

検出と対応の加速：EDR, XDR and MDR

予防を重視するソフォスのアプローチは、脅威の影響を受ける前に可能な限り多くの脅威を自動的にブロックしてクリーンアップします。そのため、IT およびセキュリティチームが後で調査が必要となる脅威の検出が少なくなります。



予防、検出、対応に対するソフォスのアプローチ。

Sophos EDR (Endpoint Detection and Response)

ソフォスは、強力な検出機能と対応機能を Sophos Endpoint の堅牢な予防重視のアプローチに統合することで、エンドポイントとサーバー全体で攻撃が疑われるアクティビティを検出および調査して、対応します。AI を活用した分析により、検出した脅威に優先順位が付けられ、自社のチームは、本当に重要な脅威に時間と労力を集中させることができます。セキュリティ担当者はリモートからデバイスにアクセスし、問題の調査、ソフトウェアのインストールとアンインストール、問題の修復を行うことができます。

Sophos XDR (Extended Detection and Response)

Sophos XDR は、包括的な脅威の検出と対応機能を求める企業のために開発されており、セキュリティ環境全体にわたって攻撃が疑われるアクティビティを検出および調査して、対応できます。このツールは、セキュリティアナリストがセキュリティアナリストのために設計しています。ソフォス独自のセキュリティコントロールとサードパーティのセキュリティコントロールのテレメトリを統合でき、検出と対応を加速する業界唯一のセキュリティ運用ツールです。

Sophos Managed Detection and Response (MDR)

脅威の検出と対応を管理するリソースが自社にない企業は、経験豊富な脅威ハンターとインシデント対応担当者から構成される精鋭チームが 24 時間 365 日提供するサービスである Sophos MDR を利用できます。Sophos MDR は、ソフォス製品とサードパーティのセキュリティ製品の両方から提供されるテレメトリを活用し、最も巧妙で複雑な脅威も検出して無効化します。

Sophos XDR と Sophos MDR は、メール、ファイアウォール、ネットワーク、アイデンティティ、クラウドなど、これまでに投資しているテクノロジーと統合でき、既存の投資の ROI をさらに高めることが可能になります。

Sophos XDR と MDR の統合。

ソフォス製品を選ぶ理由

ソフォスは、MDR、インシデント対応、および組織のサイバー攻撃への対処を支援するエンドポイント、ネットワーク、メール、クラウドセキュリティテクノロジーなど、高度なサイバーセキュリティソリューションを提供する世界的なリーダーであり、革新的な多くの製品を提供しています。ソフォスは、最大手のサイバーセキュリティ専門プロバイダーの 1 つであり、全世界で 55 万以上の組織と 1 億人以上のユーザーを、アクティブな攻撃者、ランサムウェア、フィッシング、マルウェアなどから保護しています。脅威の状況を詳細に可視化することで、比類のない脅威インテリジェンスを提供し、ソフォスの製品およびサービスの防御能力を向上させています。

独立機関によるテスト

実績のある第三者機関によるテストは、企業が導入するテクノロジーやセキュリティ製品を検討するときの重要な判断材料になります。しかし、攻撃の量と複雑さが増す中で、組織の実際の環境に即したテストでなければ正確な評価は得られません。

SE Labs 社

SE Labs は、サイバー犯罪者やペンテスターが現在使用している攻撃ツールや戦術、手法、手順 (TTP) をシミュレーションしてテストしている、業界でも希少なセキュリティテスト機関です。

SE Labs が公開した最新のエンドポイントセキュリティのレポート (2023 年 7 月～ 9 月) では、ソフォスは全体として AAA の評価を獲得し、再び業界最高の保護機能として評価されました。エンタープライズ部門と SMB 部門の両方で、ソフォスは「Protection Accuracy」、「Legitimate Accuracy」、および「Total Accuracy」の 3 つ分野で 100% の評価を獲得しました。SE Labs の 2023 年 第 3 四半期のレポートはこちらからご覧いただけます：

Endpoint Security: Enterprise | Endpoint Security: Small Business

AV-Test 社

Windows - 企業向けエンドポイントプロテクションの最優秀製品アワード (2023 年 5 月～ 6 月) macOS - 企業向け macOS エンドポイントプロテクションの認定製品 (2023 年 3 月)

MITRE Engenuity ATT&CK 評価テスト

Turla による攻撃手法を利用した 2023 年の MITRE Engenuity ATT&CK 評価テストにおけるソフォス製品の結果 Sophos Intercept X with XDR は、143 件の攻撃サブステップの 141 件を検出し、評価対象の攻撃の 99% を検出しました。また、Sophos Intercept X with XDR は、サイバー攻撃の内容、方法、目的について豊富なコンテキストをセキュリティチームに提供する能力を実証し、ATT&CK 評価のサブステップの 98% において豊富な分析結果を記録しました。

MITRE Engenuity ATT&CK 評価テストは、実環境における攻撃シナリオを取り入れた入念な構成、結果の透明性、および参加者情報の豊富さにより、世界で最も高く評価されている独立系のセキュリティテスト 1 つです。

受賞歴とアナリストレポート

ガートナー社

- ✓ 14 年連続で Gartner Magic Quadrant のエンドポイントプラットフォーム部門でリーダーに位置づけ
- ✓ エンドポイントプロテクションプラットフォーム (EPP) 部門における Gartner® Voice of the Customer Peer Insights ™ レポート (2022 年および 2023 年) で Customers' Choice に選定

G2

- ✓ 総合リーダー (Overall Leader) | エンドポイントプロテクション製品：2023 春および 2023 年秋の Grid Reports
- ✓ 総合リーダー | EDR：2023 春および 2023 年秋の Grid Reports
- ✓ 総合リーダー | XDR：2023 年秋の Grid Report
- ✓ 総合リーダーおよび最高ソリューション | XDR：2023 年春の Grid Report

Omdia

- ✓ 総合リーダー (Overall Leader) | 2022 年 11 月 包括的な XDR (Extended Detection and Response) プラットフォーム

CRN Tech Innovators Awards

- ✓ Sophos Intercept X が最高のエンドポイントプロテクションに選定される

ChannelPro Readers' Choice Awards

- ✓ Sophos Intercept X が Best Endpoint Security Vendor の Gold Winner を受賞

お客様の声

★★★★★

「Sophos Endpoint Protection の最大の特長は、高度な脅威対策にあります。ソフォスは、機械学習、挙動分析、シグネチャベースの検出など、高度な技術を組み合わせて悪意のある脅威を検出およびブロックします。

ソフトウェア開発者 | 金融業界 (銀行以外) Gartner Peer Insights でレビューの全文を読む

★★★★★

「単一のソリューションでサイバーセキュリティの高度な脅威を防ぐことができます」

ネットワーク管理者 | 教育業界 Gartner Peer Insights でレビューの全文を読む

★★★★★

「ソフォスのエンドポイントプロテクションを使用していますが、とても満足しています。攻撃対象領域を軽減し、攻撃が組織のネットワークに拡散するのを防止します。ランサムウェア対策とディープラーニング AI により、システムに影響を与える前に攻撃を阻止します。」

ICT セキュリティオフィス | 放送メディア業界 G2 でレビューの全文を読む

★★★★★

「ソフォスのエンドポイントソリューションは非常に使いやすく強力です。」

IT オペレーションマネージャー | 中堅企業 | G2 でレビューの全文を読む

★★★★★

「Sophos Endpoint は、攻撃者が悪用する可能性がある脆弱性を軽減し、顧客のシステムがサイバー攻撃者から保護されているという安心感をもたらします。」

システム管理、バックアップ、リカバリ担当マネージャー | エンタープライズ企業 | G2 でレビューの全文を読む

結論

サイバーセキュリティ環境は目まぐるしく変化しています。攻撃者は防御を回避するために常に技術を進化させており、セキュリティベンダーや組織はこれらの進化に対応しなければなりません。

そのためには、予防を重視するアプローチを取り入れているセキュリティツールを使用することが重要です。これらのツールは、攻撃の変化に自動的に対応できるようにし、攻撃をブロックまたは遅延させ、対応するための時間を得ることができるようにします。

一方で、エンドポイントセキュリティソリューションに求められる機能や、最も必要としているセキュリティの成果を適切に理解しておくと、十分な情報に基づいて適切な製品を購入できるようになります。現在の攻撃から組織を保護する最適な防御策を提供している製品を選ぶ必要があります。

ソフォスは、現在そして進化を続ける脅威から組織を保護します。ソフォスのソリューションは、組織が可能な限り最高のセキュリティ成果を達成できるように支援します。ソフォス製品の詳細について、ぜひお問い合わせください。

Sophos Endpoint の詳細と、高度な攻撃に対する比類のない保護機能については、**Sophos.com/endpoint** を参照してください。

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2024-01-15 JA-WP (PC)

SOPHOS