

ホワイトペーパー

Synchronized Security™ の解説

SOPHOS

Synchronized Security

Synchronized Security ™ は、ソフォスの業界をリードする AI ネイティブなサイバーセキュリティ防御システムである Sophos Fusion の中核を成しています。これは、ソフォス製品とサードパーティ製品を問わず、接続されたすべての制御ポイントから得られる脅威に関する洞察を、脅威への一元的な対応へとつなげる結合組織としての役割を果たします。

Gartner は「Tech FutureSight: Protect the Global Attack Surface With an Autonomous Cyber Defense System」[1] の中で、「組織は、サイバーセキュリティツールのさまざまな要素を連携させ、リスクや脅威にプロアクティブかつリアクティブにマシンスピードで対応するためのインテリジェントな統合レイヤーを必要としている」と指摘しています。Synchronized Security は、Sophos Fusion でこの統合レイヤーを実現する上で重要な役割を果たします。

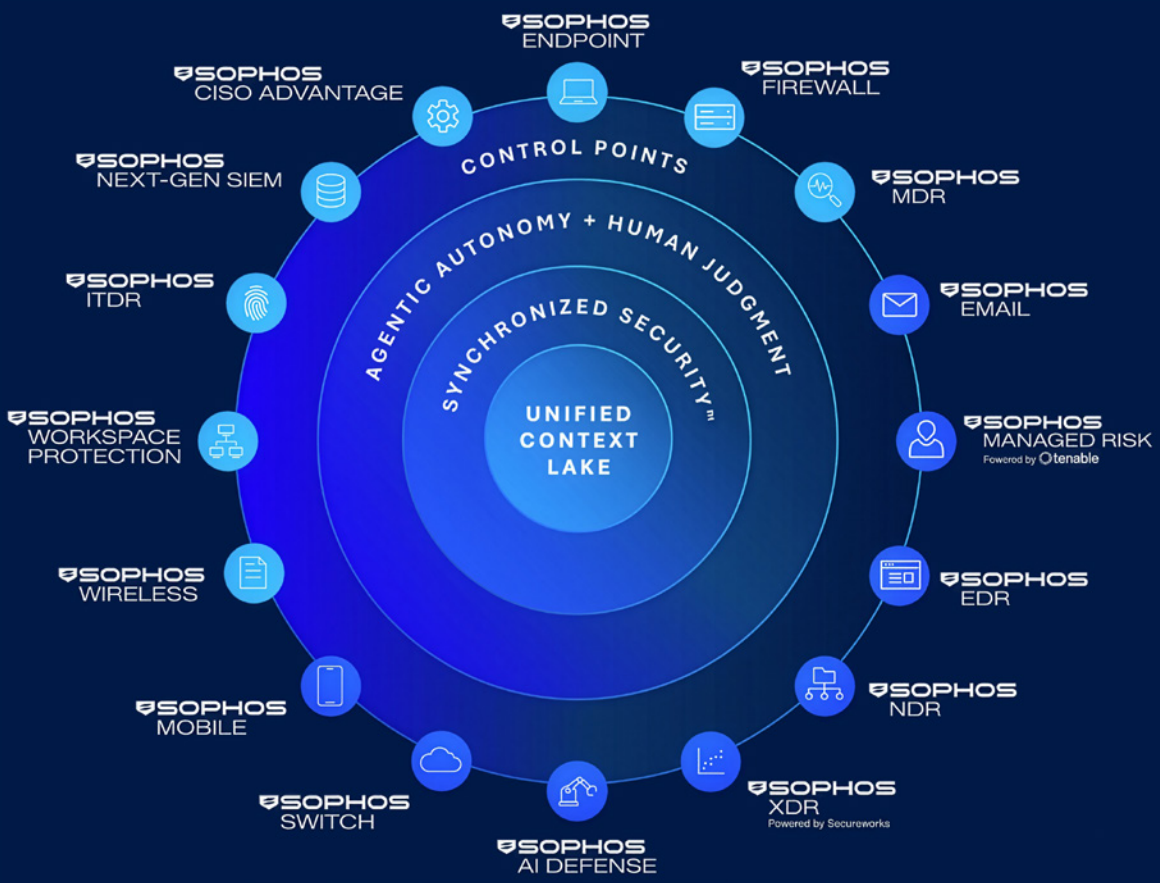
このガイドでは、Synchronized Security の仕組みやそのメリット、そして組織がそのメリットをどのように活用できるかについて説明します。

1 Tech FutureSight:Protect the Global Attack Surface With an Autonomous Cyber Defense System, Neil MacDonald, 12 December 2025.GARTNER は、Gartner, Inc. およびその関連会社の商標です。



概要：

- Synchronized Security は Sophos Fusion 防御システムの中核的な要素であり、追加のモジュールやライセンス、追加コンポーネントを購入する必要なく自動的に含まれます。
- Synchronized Security は、接続された制御ポイント全体で脅威に連携して対応することを可能にします。開始するには、Sophos Fusion 内で 2 つ以上の制御ポイントが連携している必要があります。
- Synchronized Security は、ソフォスとソフォス以外の制御ポイントの両方で機能します。個々の顧客環境で実行される対応アクションは、Sophos Fusion に接続されているセキュリティ管理と、顧客が各制御ポイントに許可している自律的なアクションの範囲によって異なります。
- Sophos XDR は Synchronized Security の中核を成し、顧客環境全体から収集したシグナルを単一の攻撃チェーンとして関連付け、ソフォスの防御システム全体で自動または人による対応アクションを実行できるようにします。
- ソフォスのソリューションは、Sophos XDR がなくても連携して動作でき、Synchronized Security による連携のメリットをさらに広げることができます。
- Synchronized Security は、ソフォスが 2015 年から提供を開始したものです。それ以降、基盤となる機能を実環境で検証し、発展させてきました。



連携した対応が重要な理由

セキュリティツールは、これまで特定の 1 つの役割に特化して構築されてきました。エンドポイントエージェントは、自身が実行されるデバイス (デスクトップ、ノート PC、サーバーなど) を保護します。ファイアウォールは、ネットワークを通過する通信を監視します。メールサービスは、受信トレイに届くメールを制御します。それぞれが自らの役割には優れている一方で、各ツールの外部で発生している問題を把握することはできません。

攻撃者は、こうした状況を古くから理解しています。現代の侵入は、単一の場所での単一の出来事ではありません。侵入は、アイデンティティ、メール、エンドポイント、ネットワークを横断するように設計されています。これらの領域間にはギャップであり、攻撃者はそのギャップを悪用しています。

そのため、セキュリティチームを管理している方であれば誰でも体験したことがある結果が生まれています。個々のセキュリティソリューションは、それぞれの担当領域の異常しか識別できず、それらの異常は一見すると無関係に見えます。それぞれ単独では、十分に対処できるように見えます。被害が発生するまで、それらの異常が同一の攻撃によるものだと認識できるだけの時間も、状況を把握するための情報もありません。

AI によって、このギャップはさらに広がっています。攻撃は今や、これまで業界が経験したことのない規模と、マシンスピードで実行されています。しかし、多くの防御は依然として人間の速度で行われており、アナリストが複数のコンソールを行き来しながら、手作業で情報を関連付けています。

セキュリティ環境に別の製品を追加しても、このギャップは埋まりません。組織はすでに導入している製品を連携させることを検討すべきです。Sophos Fusion においてこの連携を担っているのが、Synchronized Security です。



Synchronized Security の機能

連携によって、脅威への対応の速度、規模、範囲が変わり、攻撃の結果も変わります。エンドポイント、ネットワーク、その他のセキュリティ対策が連携して動作すれば、封じ込めは数秒で実行されます。誰かが異常に気づいてから対応するのを待つ必要はありません。侵害されたエンドポイントは瞬時に隔離され、脅威のラテラルムーブメントや、機密データへの到達、常駐化を阻止します。さらに、対応が自動化されているため、人員が手薄になりがちな夜間や週末でも機能します。

連携によって、攻撃者が悪用するギャップも埋めることができます。これまでアラートを発行するだけだったサードパーティの制御ポイントも、防御に積極的に貢献するようになります。既存のセキュリティ投資が孤立することなく、連携した対応の一部として機能するようになります。

セキュリティチームの運用にも、すぐに効果が現れます。定型的な封じ込めは、アナリストの介入なしに実行されます。人による調査が必要な場合も、アナリストは複数のコンソールを切り替えて手作業で情報をつなぎ合わせるのではなく、複数のレイヤーにまたがる情報があらかじめ集約された状態から調査を開始できます。

同じ連携基盤によって、防御体制を容易に証明できるようになります。複数のレイヤーにまたがる情報が保持され、連携した対応によって、何が確認され、どのような対応が行われたのかを一貫した記録として残すことができます。このようなセキュリティ対策に対する説明は、監査人、規制当局、保険会社から求められています。防御を強化するアーキテクチャは、顧客がその防御を証明する能力も高めます。

接続する制御ポイントの範囲が広がるほど、防御も強化されます。Sophos Fusion に接続する新たな制御ポイントが増えるたびに、統合されたコンテキストレイクに追加のシグナルが取り込まれ、対応できる場所も増えていきます。それでも、運用負担がそれに応じて増えることはありません。対応する範囲が広がっても、作業が増えるわけではありません。

マネージドサービスプロバイダーは、ソフォス製品とサードパーティの制御ポイントが混在する環境を含め、すべての顧客環境で同じ連携を一貫して適用できます。封じ込めの自動化により、手作業によるトリアージや修復対応の負担を軽減できます。

Synchronized Security の仕組み

Synchronized Security はテレメトリから始まります。接続されたすべての制御ポイントは、発生した問題を統合されたコンテキストレイクに報告します。エンドポイント、ファイアウォール、メール、クラウド、ネットワーク、アイデンティティ、および生産性ツールがすべて同じコンテキストレイクに問題を送信します。サードパーティの制御ポイントも、ソフォスの制御ポイントと同様に問題を報告します。情報が集約されるまでキューで待機することも、後から調整するための二次的なデータストアも必要ありません。

Sophos XDR は共有された全体像を解釈し、通常ならアナリストが手作業で行う作業を実行します。関連するイベントを結び付け、発生しているアラートを個別ではなく、1 つの攻撃チェーンとしてまとめます。重要なのは、情報を関連付けることです。1 つの制御ポイントから見えるのは、常に攻撃の一部分にすぎないからです。

すべての情報を関連付けた後に、対応アクションが制御ポイントに送り返されます。Sophos XDR は、そのための仕組みとして、SOAR による自動化、プレイブック、ケース管理、そして幅広い対応アクションを提供します。その大半は、人の介入なしに自動的に実行されます。人間による判断が必要な場合は、社内のアナリストが Sophos XDR を使って、Sophos MDR のアナリストと同じように、手動でアクションを実行できます。

サードパーティの制御ポイントとの双方向連携により、Sophos Fusion は統合を通じてデータを取得して送信できます。例：

- ソフォス以外のファイアウォールからテレメトリを取り込み、そのファイアウォールにブロック対象の IP アドレスを送り返すことができます。
- ServiceNow と統合すると、ケースを開き、情報を更新し、閉じることができます。
- Sophos Firewall のアクティブな脅威対応は、サードパーティの脅威フィードに対する API 経由の対応によって、侵害されたデバイスや不正なデバイスをネットワークから遮断します。

ソフォスの制御ポイントは、Sophos XDR を介さずに相互に直接対応できる点も特徴です。組み込みのセキュリティハートビートは、Sophos Endpoint から他のソフォスの制御ポイントへデバイスのセキュリティ状態を伝達します。緑のステータスは正常、黄色のステータスは潜在的に侵害されている可能性があることを、赤のステータスは侵害されていることを示します。

他のソフォスの制御ポイントは、デバイスのセキュリティ状態に基づいて動作するように構築されています。制御ポイントを同じ Sophos Fusion アカウントに接続すれば、基本的な対応アクションを利用するための追加設定は必要ありません。ファイアウォールルールによってインターネットアクセスを制限したり、Sophos Workspace Protection のポリシーを適用したりするなど、デバイスのセキュリティ状態を利用する機能は、適用する前に顧客が設定します。

収集

相関分析

対応

Sophos Fusion がテレメトリを収集し、Sophos XDR がコンテキストを構築し、自動化された対応アクションが制御ポイントに対応を送り返します。

1 つの機能で、複数の連携を実現

2015 年に世界で初めて Synchronized Security ™ がリリースされて以来、10 年以上にわたり拡張されてきました。 制御ポイント間の連携の深さは、顧客環境に導入されている制御ポイントの組み合わせによって異なります。

ソフォスの制御ポイント間では、最初から連携して動作するように設計されているため、最も深いレベルの連携が実現します。サードパーティの制御ポイントは Sophos Fusion の統合を通じて接続され、実行できる対応アクションは、他社が提供する機能によって異なります。

連携の深さは、顧客が各制御ポイントに対して Sophos Fusion にどこまでの操作を許可するかによっても異なります。その選択は顧客に委ねられており、そのような選択肢があること自体が重要で、欠点ではありません。多くの組織に、感染したエンドポイントを承認を得ずにネットワークから切り離すべきかと尋ねれば、「はい」という答えが返ってくるでしょう。一方、システムが自律的にファイアウォールポリシーを書き換えてリスクを縮小すべきかと尋ねれば、答えは分かれます。

ファイアウォールは、この判断の難しさを端的に示す例です。結局のところ、侵害されたエンドポイントをブロックすることも、ファイアウォールルールを変更することにほかなりません。多くの組織がファイアウォール設定の自動変更に慎重になるのも無理はなく、変更管理のプロセスが設けられているのには、正当な理由があります。

顧客は独自の自動化処理やプレイブックを作成し、ソフォスが提供するものと併用できます。Sophos Endpoint を利用している顧客は、侵害されたデバイスを Fortinet のファイアウォールでどのように扱うかを自ら決定できます。これには、ファイアウォールの動作だけでなく、その設定方法も含まれます。いったん定義すると、通常の連携対応と同じように、Sophos Fusion 内で自動処理が実行されるようになります。

Synchronized Security の実行

連携がどのように機能するのかは、具体例を見るとより分かりやすくなります。以下のユースケースは、別々の機能を列挙したものではなく、同じ機能が異なるレベルの連携で動作する例を示しています。

ソフォス製品間の連携

Sophos Endpoint がエンドポイントまたはサーバーで脅威を検知すると、そのデバイスのセキュリティハートビートのセキュリティ状態を赤に設定します。新しいステータスは、セキュリティハートビートを介して、接続されている他のソフォスの制御ポイントと自動的に共有されます。これに続いて、複数の対応が自動的に実行されます。

- Sophos Endpoint は、ランサムウェアによる暗号化のブロックおよびロールバックや、アクティブアドバーサリーを抑制するためのより高度な対策の展開などにより、脅威の修復を試みます。
- Sophos Firewall は、デバイスのインターネットアクセスを制限し、コマンド＆コントロールサーバーへのいかなる接続も遮断し、正常なデバイスに到達するのを防ぎます。
- Sophos Wireless、Sophos Switch、および Sophos Workspace Protection は、デバイスのネットワークリソースへのアクセスを制限し、侵害の影響をさらに限定します。
- 正常なエンドポイントには赤のセキュリティ状態が通知され、影響を受けたデバイスからのネットワーク接続要求を拒否します。

同じ仕組みによって、感染が明確ではない問題も検知できます。大量のスパムやフィッシングメールを送信しているエンドポイントまたはサーバーは、赤のセキュリティ状態に設定されます。Sophos Endpoint は、これまで特定されていなかった悪意のあるユーザーやアプリケーションを検知し、Sophos Email は、メッセージが受信トレイに届く前にブロックします。

エンドポイントやサーバーは、必要な修復対応に応じて、数秒から数日間にわたってセキュリティ状態が赤のままになることがあります。問題が解消されると、デバイスのセキュリティ状態は緑に戻り、システム全体でアクセスが自動的に復旧します。

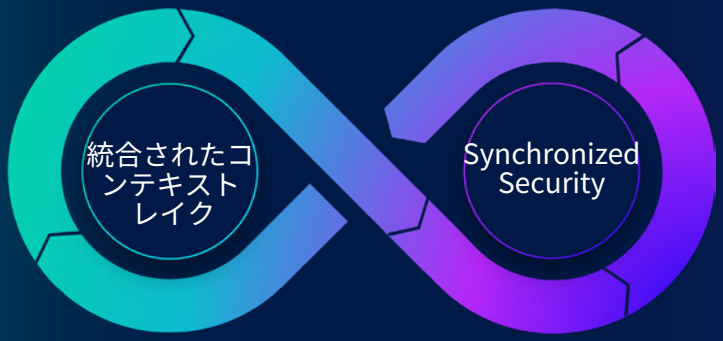
その価値が最も明確になるのは、人が監視していないときです。金曜の深夜にサーバーが侵害された場合でも、数秒でネットワークから切り離されるため、攻撃者に週末にネットワーク内を移動される時間を与えずに済みます。

シナリオ

Sophos Endpoint が脅威を検知すると、デバイスのセキュリティハートビートの状態が赤に設定されます。新しいステータスは、接続されているすべてのソフォスの制御ポイントと自動的に共有されます。 エンドポイントの脅威が取り除かれると、同じサイクルに従ってアクセスが復旧します。

シグナル

SOPHOS ENDPOINT
脅威を検知



連携対応

SOPHOS FIREWALL
ネットワーク接続を遮断し、ネットワークアクセスを制限します。

SOPHOS WIRELESS

SOPHOS SWITCH

SOPHOS WORKSPACE PROTECTION
デバイスのネットワークリソースへのアクセスを制限

SOPHOS ENDPOINT
正常なエンドポイントはネットワーク通信を拒否

Sophos Endpoint とサードパーティファイアウォール

連携はソフォスの制御ポイントに限定されません。Sophos Endpoint と Fortinet のファイアウォールを併用している顧客は、侵害されたデバイスをトリガーとして、Fortinet のファイアウォールで対応アクションを実行できます。顧客は、その対応内容と対応の範囲を自ら定義できるため、自動化を自社の変更管理の範囲内に収めることができます。Sophos XDR の自動化機能とプレイブック (SOAR) 機能が、Sophos Fusion の Fortinet 連携と連携して、これを実現します。



Microsoft のテクノロジーとテレメトリ

ほぼすべての組織が Microsoft のテクノロジーを利用しており、アイデンティティはランサムウェア攻撃の主要な攻撃経路となっています。盗まれたセッショントークンや侵害されたアカウントは、攻撃者に正規の侵入経路を与えます。アカウント自体が侵害されたままであれば、エンドポイントをどれだけ封じ込めても効果はありません。修復対応を完了するには、対応を Microsoft 環境にまで広げる必要があります。

アカウントのロックが、その最も分かりやすい例です。Sophos Fusion は、侵害された Microsoft アカウントをロックして攻撃者を締め出し、その後アカウントが再び安全に使用できるようになったらロックを解除できます。アカウントも他の制御ポイントと同様に、システムが認識して対応できる対象として扱われます。管理者が後から別途対応する必要はありません。

この統合は双方向です。Microsoft のさまざまなソースのテレメトリが、ソフォスの制御ポイントと同じ統合されたコンテキストレイクに取り込まれます。その中には、Microsoft Entra ID や Microsoft Graph Security などが含まれます。つまり、Microsoft からのシグナルによってソフォスの制御ポイントで対応を実行することも、ソフォスのシグナルによって Microsoft 環境で対応を実行することも容易に行えます。Microsoft で検知された不審なサインインをきっかけに、ソフォスで保護されているエンドポイントを隔離できます。しかも、どちらか一方を相手の監視対象として個別に設定する必要はありません。

有線および無線のネットワークエッジ

スイッチやアクセスポイントは、セキュリティ防御の一部とはあまり考えられていません。これらはトラフィックを転送し、ユーザーの接続を維持するために導入されるインフラであり、多くの組織がそのように扱っています。しかし、これらはすべてのデバイスがネットワークに接続する地点に位置しており、そのため、侵害されたデバイスや不正なデバイスを最も早い段階で遮断することが可能となります。

Sophos Fusion では、Sophos Switch およびソフォスワイヤレスアクセスポイントが制御ポイントとして機能します。これらは接続デバイスに関する情報を提供し、より広範なシステムが検知した情報に基づいて対応を行うことができます。管理者は、新たに接続されたデバイスや未承認のデバイス、想定外の SSID に接続しているクライアント、あるいは誤ったスイッチポートに接続されたデバイスを特定できます。

Sophos Firewall の Synchronized Security 機能であるアクティブな脅威対応は、そのコンテキストを行動に変えることができます。統合されたコンテキストレイクのテレメトリを利用して、不審なデバイスがネットワークの内部へ進む前に、有線または無線のアクセスレイヤーでブロックできます。顧客はアクティブな脅威対応を有効にするかどうかを選択でき、アクセスレイヤーでの自動ブロックを許可するかどうかを自ら決定できます。

サードパーティのネットワークデバイスも、先ほど説明したサードパーティファイアウォールと同じ仕組みで連携します。



Sophos AI Defense によるシャドー AI 利用の検知

連携の対象は、マルウェアや侵入だけではありません。Sophos AI Defense は Sophos Fusion の制御ポイントであり、組織全体で AI がどのように利用されるかを管理します。これは、さまざまなソフォス製品から送られる AI アクティビティのテレメトリを、他のすべてのシグナルとともに統合されたコンテキストレイク上で解析し、Sophos EDR、Sophos XDR、Sophos MDR で確認できる情報として提供します。Sophos AI Defense は、AI の利用状況に関する詳細な情報を可視化するよう設計されており、その情報が統合されたコンテキストレイクに取り込まれると、他のすべての情報と同じ Synchronized Security の仕組みによって処理されます。

シャドー AI は、この仕組みが必要な理由を示す好例です。ある従業員が、誰も把握していない AI ツールの利用を始め、そこにソースコードや顧客記録を貼り付けるケースを考えてみましょう。ブラウザは貼り付けられたデータを認識し、エンドポイントはそのアプリケーションを認識し、ファイアウォールは、まったく管理されていない可能性のあるデバイスから AI サービスへの通信を認識します。しかし、どの制御ポイントからも全体像を把握できないため、そのツールは発見されないままになります。

Sophos AI Defense は、それらのシグナルを集約し、コンテキストに応じて評価することで、セキュリティアナリストが何が起こったのかを理解するために必要な証拠を提供します。ユーザーのアイデンティティや権限、行動、データの露出状況、ユーザーと AI モデルの場所などのテレメトリを組み合わせることで、適切な利用と、管理されていない、過剰な権限が付与された、またはポリシーに違反するアクティビティを区別します。

判定された問題への対応は、制御ポイントで適用されます。

- Sophos Workspace Protection は、コピーやペースト、アップロード、ダウンロード、スクリーンショットを含むブラウザを制御します。
- Sophos Endpoint は、ユーザーグループやデバイスの種類にわたって、AI アプリケーションや Web サイトへのアクセスを制限します。
- Sophos Firewall は、管理対象外のデバイスやブラウザ以外のアクティビティを含め、ネットワークレイヤーで AI サービスへの通信を制御します。
- ソフォス製品は、プロンプト、アップロード、AI とのやり取りをリアルタイムで検査し、ースコード、顧客情報、財務データが社外に流出するのを防ぎます。
- 管理者は、Sophos Fusion から環境全体で特定の AI ツールをブロックできます。

ポリシーの適用だけでは終わりません。ポリシー違反や未承認のエージェントの動作は、他の問題が検知された場合と同じように、Sophos EDR、Sophos XDR、Sophos MDR のワークフローで検知され、アイデンティティ、エンドポイント、ネットワークの脅威に対してすでに使用されている自動化機能やプレイブックによって対応されます。連携がどの程度まで及ぶかは、どの制御ポイントが Sophos Fusion に接続されているかによって異なります。

82%

組織の 82% が、環境内に未知の AI ツールやワークフローを発見しています。[2]

2 Cloud Security Alliance、エンタープライズ環境におけるシャドー AI エージェントの問題、2025 年

脅威対応にとどまらない連携

ソフォスの制御ポイント間の連携は、脅威の判定結果を共有するだけにとどまりません。制御ポイントは別の制御ポイントに直接問い合わせ、その回答に基づいて対応できます。Sophos Endpoint で保護されたエンドポイントやサーバーは、ネットワークトラフィックについて、Sophos Firewall では把握できない情報の大半をすでに把握しています。ポート上の通信からその背後で使用されているアプリケーションを特定すること、セッションの背後にいるユーザーを特定すること、そしてデバイスにアクセスを許可してよい状態かどうかを判断することの 3 つのやり取りから、こうした連携によって何が可能になるのかが分かります。

Synchronized Application Control

通常とは異なるポートで、分類されていない接続を検知した場合を考えてみましょう。ファイアウォールだけで検査すると、見えるのはパケットの流れと、わずかな情報だけです。Sophos Firewall は、Sophos Endpoint に対して、そのポートで送受信しているアプリケーションを尋ね、どのアプリケーションが処理しているかという回答を得ることができます。顧客はその回答に基づいてアプリケーションを許可またはブロックすることができます。時間の経過とともに、ネットワーク上で何が稼働しているのかについても正確に把握できるようになります。通常、その実態は誰もが想定している以上に多様です。

IP アドレスではなく、アイデンティティ

ユーザーのアイデンティティは同じように機能します。Sophos Endpoint は認証済みユーザーの情報を Sophos Firewall に渡すため、変動するユーザー名や IP アドレスではなく、ユーザーとそのアイデンティティに基づいてポリシーを設定できます。これにより、管理者が本来なら手作業で維持する必要がある対応関係の管理が不要になり、時間の経過とともに実態とずれていくこともありません。

正常なデバイスのみが接続される

アクセスの判断にもメリットがあります。従来の VPN では、デバイスが正常な状態かどうかを確認することはできず、認証情報だけに基づいてエンドポイントのアクセスを許可します。しかし、Sophos Workspace Protection は、アクセスを許可する前に Sophos Endpoint でデバイスの状態を確認するため、侵害されたエンドポイントがネットワーク上のアプリケーションやデータにアクセスすることはありません。

このような制御ポイント間のやり取りは、あらかじめ決められたものだけではありません。こうした高度な連携が可能なのは、ソフォスが各製品を連携して動作するように開発し、時間をかけてその機能を拡充してきたためです。現在、ソフォスの制御ポイント間で共有される情報は、10 年前と比べて大幅に充実しています。

これらはいずれも、最初から脅威対応を目的としたものではありません。しかし、脅威対応と無関係のまま終わることはほとんどありません。誰も説明できないアプリケーションや、本来サインインすべきでないユーザーの存在は、最初は普通の運用上の一部に過ぎませんが、やがて問題として浮上します。ネットワークの運用を容易にする可視性によって、新たな脅威も発見しやすくなります。

ハイブリッド環境全体にわたる協調的な対応

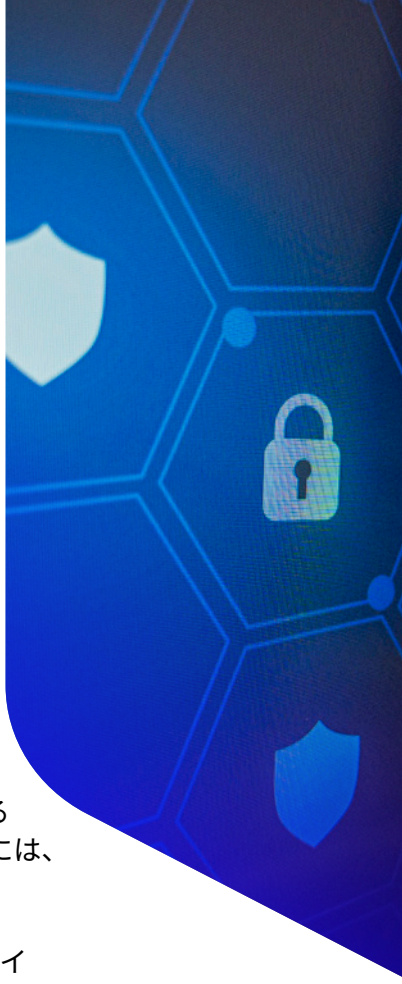
Sophos MDR によるこの実例は、Synchronized Security が実際にどのように機能するのかを示しています。影響を受けた組織は Sophos MDR の顧客で、Sophos Endpoint と Sophos Email に加えて、Microsoft Entra ID、Microsoft Graph Security、Fortinet のファイアウォールを利用していました。また、別のネットワークでは Sophos Firewall も利用していました。それらの各制御ポイントが同じ統合されたコンテキストレイクに情報を提供していました。

- 攻撃者は、AI を利用して作成した誘い文句から攻撃を開始し、正規のサイトにホストされたフィッシングページを使用しました。ユーザーはクリックしてパスワードを入力しました。
- この攻撃キットは認証情報ではなく、ライブセッションのトークンを窃取しました。これにより、攻撃者は多要素認証を回避し、パスワードリセットを無効にしました。
- 攻撃者は既知の攻撃者インフラからサインインし、特定のサプライヤーからのメールをすべて隠す目立たない受信トレイのルールを作成しました。これは、送金詐欺につながる準備でした。
- Sophos Endpoint、2 つの Microsoft ソリューション、そして Fortinet のファイアウォールの合計 4 つの制御ポイントがそれぞれ不審な兆候を検知しました。どのシグナルも、それ単独では対応を開始するほど重大なものではありませんでした。
- 専用に設計されたソフォスの検知機能が作動し、個々のシグナルから 1 つの攻撃チェーンが浮かび上がりました。
- サインインはブロックされ、セッションは取り消され、エンドポイントは正常に隔離されました。悪意のある IP アドレスは、Fortinet のファイアウォールが収集したテレメトリを使用して、Sophos Firewall でブロックされました。

その後、人間の担当者がケースを終了しました。アナリストは、受信トレイルールが特定のサプライヤーを指定していることを確認し、これが送金詐欺の準備であると判断しました。



Synchronized Security を有効にする方法



Synchronized Security は、製品でも SKU でもアドオンでもなく、追加でライセンスを取得する必要もありません。Sophos Fusion 内で 2 つ以上の制御ポイントが連携して動作すると、制御ポイントがソフォス製品かどうかを問わず、Synchronized Security を自動的に利用できるようになります。

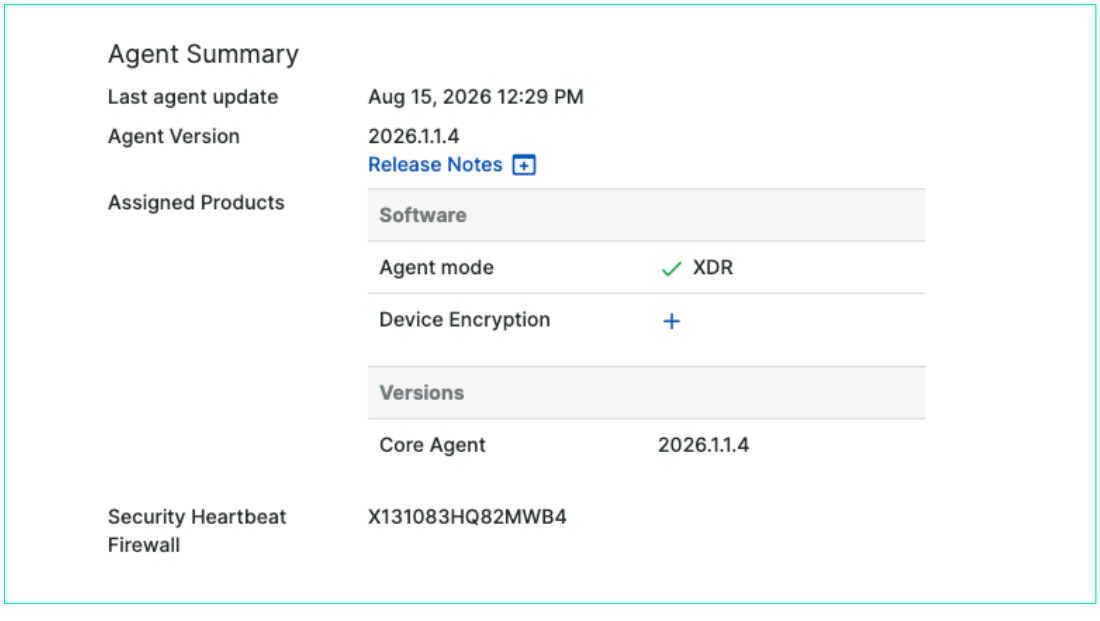
同じ Sophos Fusion アカウントで管理される Sophos Endpoint と Sophos Firewall の組み合わせは、一般的な出発点となります。両方がそのアカウントに接続されると、追加の設定なしでそれらの間の連携が有効になります。セキュリティ状態をファイアウォールルールや Sophos Workspace Protection ポリシーの一部として利用するなど、デバイスの状態に基づくユースケースは、顧客が設定します。

Sophos Fusion はソフォス製品と 500 以上のサードパーティ統合に対応しており、これらの制御ポイントを統合して連携できます。しかし、利用可能な自動応答レベルは制御ポイントによって異なります。たとえば、ソフォスの制御ポイントにおけるアクティブな脅威対応は、デフォルトでオフになっており、この機能を使用するためには、顧客がオンにする必要があります。

ソフォスは、Synchronized Security を介して自動的に実行される自動化処理やプレイブックを提供しており、幅広いユースケースに対応しています。デフォルトの自動化が自社の環境に適さない場合は、前述のように、顧客が独自の自動化処理を追加できます。

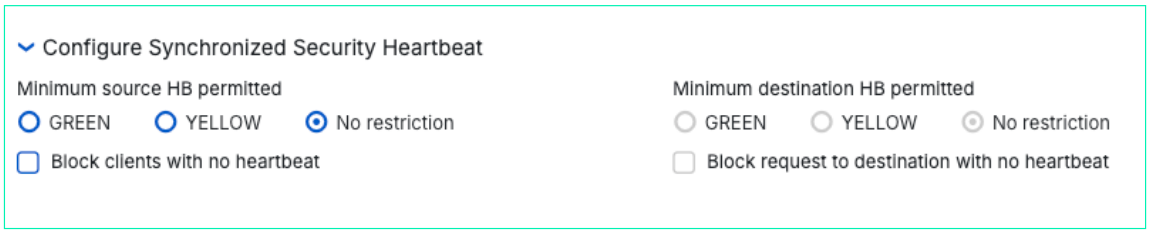
Sophos Endpoint と Sophos Firewall の連携

Sophos Endpoint がファイアウォールと連携していることを確認するには、Sophos Fusion で「コンピュータのサマリー」を開きます。この画面に、そのエンドポイントのセキュリティハートビートを受信している Sophos Firewall のシリアル番号が表示されます。



Synchronized Security を利用した Sophos Firewall ポリシー

ファイアウォールルールでは、デバイスによるインターネットへのアクセスを許可する前に、緑のセキュリティ状態を必須条件として設定することもできます。その場合、保護されていないデバイス (Sophos Endpoint が実行されていないデバイス) は接続できず、セキュリティ状態に問題があるデバイスも同様に接続できません。



まとめ

問題は、セキュリティツールが不足していることではありません。問題は、組織がすでに導入しているツールがそれぞれ個別に動作しており、攻撃者がそのツール間のギャップを突くように攻撃手法を構築してきたことです。Synchronized Security によって、セキュリティツールを統合された連携型の防御として機能させることができます。

Sophos Fusion で 2 つ以上の制御ポイントを運用しているなら、Synchronized Security はすでに機能しています。制御ポイントをさらに接続すれば、その効果はより広範囲に及びます。すでに導入しているソフォス以外のツールも、単に報告するだけではなく、対応に組み込まれます。

どこまで自動化するかは、顧客自身で決められます。自社の変更管理プロセスを無視するような連携では意味がないため、自動化の範囲は、制御ポイントごとに顧客自身で設定できます。

これが、ソフォスのサイバー防御システムがもたらす実践的な価値です。その価値とは、製品を増やすことではありません。すでに利用している製品が連携し、AI によって加速する攻撃が製品間を移動するよりも迅速に、マシンスピードで対応できるようにすることです。

詳細については、
www.sophos.com/
synchronizedsecurity
をご覧ください。

ソフォス株式会社営業部
Email：sales@sophos.co.jp

© Copyright 2026.Sophos Ltd.All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos は、Sophos Ltd. の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。