SOPHOS
Cybersecurity evolved.

Anywhere Organization の保護

あらゆる場所、あらゆるデバイス、あらゆるリソース

ソフォス ホワイトペーパー 2021年 2月

これからはリモートワークの時代: ガートナーによると、パンデミックが収束した後、リモートワークで働くことを考えている組織は 74% に上ります。同時に、従業員が仕事をするために必要なリソースも、複数の場所になります。例えば、オフィス内のサーバー、Office 365 や Salesforce などのクラウドベースアプリケーション、Amazon Web Services (AWS) や Microsoft Azure のプライベート/パブリッククラウド環境などです。

IT チームは、場所を問わず、すべてのユーザーとすべてのリソースを保護する必要があります。一方で、攻撃者は、仮想化が進む組織にあらゆる場面で侵入するための、より効果的で破壊的な方法を編み出し続けています。

ユーザーとリソースがどこにでも存在する組織を保護するには、次のことが必要です。

- ユーザーは自宅、オンサイト、オフィスなど、どこからでも安全な接続でリソースにアクセスできること
- これらの接続に使用されるデスクトップ、ノートPC、携帯電話、タブレットなどのデバイスの保護
- クラウドでもローカルネットワークでも、ユーザーがアクセスする必要のあるデータやワークロードの保護
- シンプルな管理により、IT チームはワークロードを追加しなくても、どこからでも分散した組織を管理できること

幸いにも、ソフォスはこれらすべての分野をサポートしています。高度な保護機能を備えた次世代型セキュリティ製品の完全なポートフォリオを提供します。すべてを単一の Web ベースのセキュリティ管理プラットフォームで、管理者の日々のオーバーヘッドを削減しながら、IT チームがどこからでも組織のセキュリティを管理できるようにします。

このソリューション概要では、ソフォスがこれらの各要件にどのように対処するかについて説明します。また、ソフォスのサイバーセキュリティシステムを導入して組織を保護する際にお客様が目にする生産性と保護のメリットについても説明します。

安全な接続

新型コロナウイルスの感染拡大が、リモートワークの大幅な増加をもたらしたことは言うまでもありません。2020年 5月、雇用されたアメリカ人の 62% は在宅勤務 (WFH) をしていました。しかし、リモートワークは新型コロナウイルスが登場する前からすでにトレンドになっており、従業員が週に数日、自宅から仕事している企業も既にありました。英国では、この 10年間で在宅勤務が 74% 増加し、オーストラリアでは、従業員の約 3分の1が通常は在宅勤務をしていました。

リモートワーカーは、企業と従業員にとってお互いメリットがあります。従業員は通勤時間とコストを節約しながら、柔軟性と生産性を向上させることができます。一方、組織はコストと離職率を削減します。しかし、IT チームにとっては、長期的なリモート作業はセキュリティ上の課題を生み出します。従業員がリビングルームからログインしたり、お客様の会社を訪問したり、世界中の何千マイルも離れた Wi-Fi ホットスポットでコーヒーを飲む場合でも、ネットワークとデータは常に保護されている必要があります。

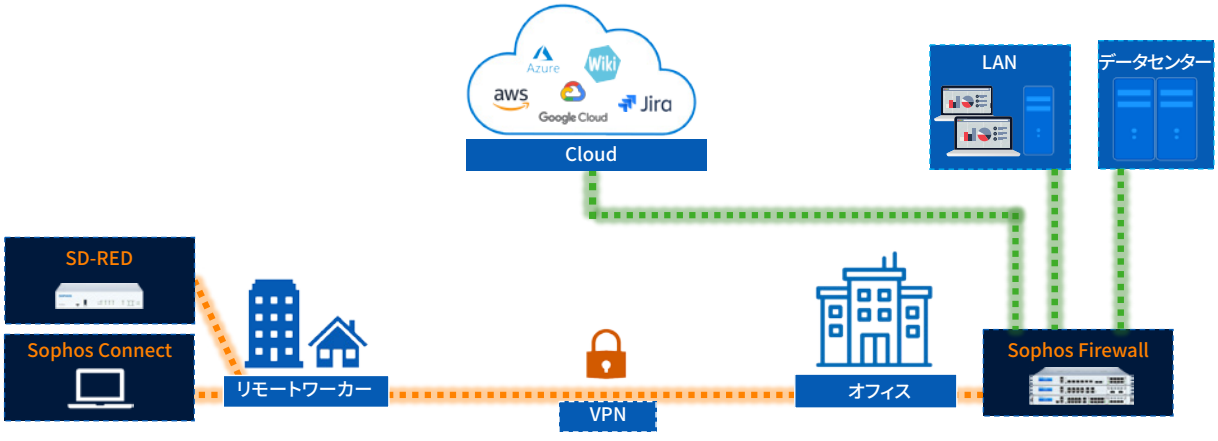
ソフォスを使用すると、従業員はどこからでも迅速、効率的、安全に接続して作業できます。また、従来の VPN ベースと Zero Trust Network Access (ZTNA) の両方のオプションを提供しています。

VPN

ソフォスの無料で導入が簡単な **Sophos Connect VPN クライアント**を **Sophos Firewall** と一緒に使用することで、リモートワーカーを本社やクラウドベースのリソースに接続できます。世界中に 140万人を超えるユーザーがいる Sophos Connect は、リモートユーザーに、Windows や macOS デバイスから企業ネットワークやパブリッククラウドのリソースへ安全なアクセスを提供します。

究極のリモート接続を実現するために、**Sophos SD-RED** (Remote Ethernet Device) は、**Sophos Firewall** と連携して、支社、リモートサイト、自宅をメインネットワーク (物理的でもクラウド上でも)に接続するシンプルなプラグアンドプレイデバイスです。

これは、常時接続の専用の VPN またはスプリットトンネル VPN を提供し、柔軟なオプションで簡単に導入および管理できます。また、とても小さく持ち運びが簡単なため、いつでもどこからでも安全にアクセスする必要がある上級管理職やその他の個人向けにも最適です。



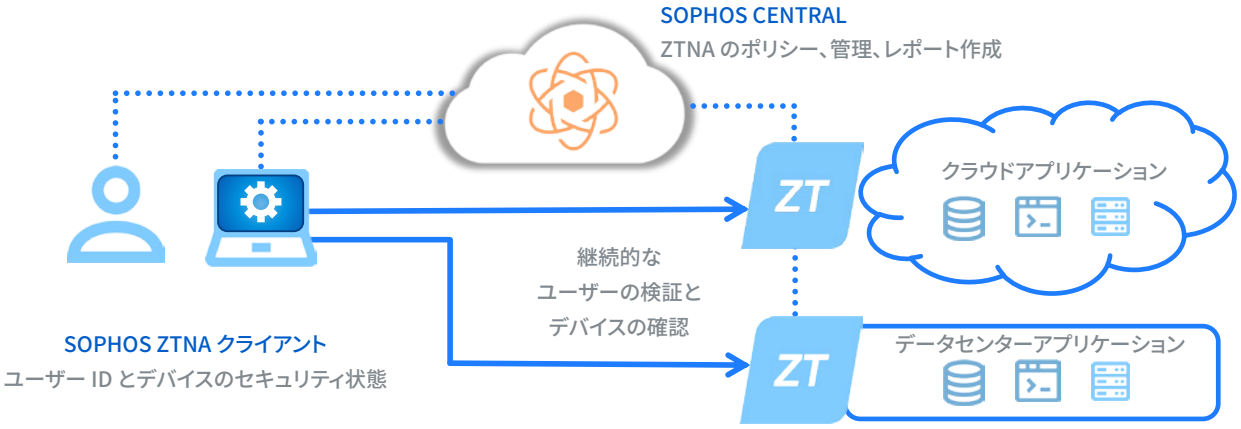
Sophos Firewall と Sophos Connect VPN と SD-RED を使用して安全なリモート接続

ZTNA

長年にわたり、従業員は VPN テクノロジーのおかげで、リモート接続を実現してきました。VPN はパンデミック当初は救世主となっており、組織はたったの数日のうちにセキュアなリモートワークに迅速に移行できるようになりました。しかし、多くの組織は VPN にこれまで設計された以上の機能を提供することを求め始めています。

Sophos ZTNA (Zero Trust Network Access) は、リモートアクセス VPN の代替として最適です。ユーザーはどこからでも簡単かつ透過的に企業のリソースへ接続できます。また、同時にユーザーを常に検証 (通常は多要素認証と ID プロバイダーを使用) し、デバイスのセキュリティ状態とコンプライアンスを検証することで、セキュリティを強化します。

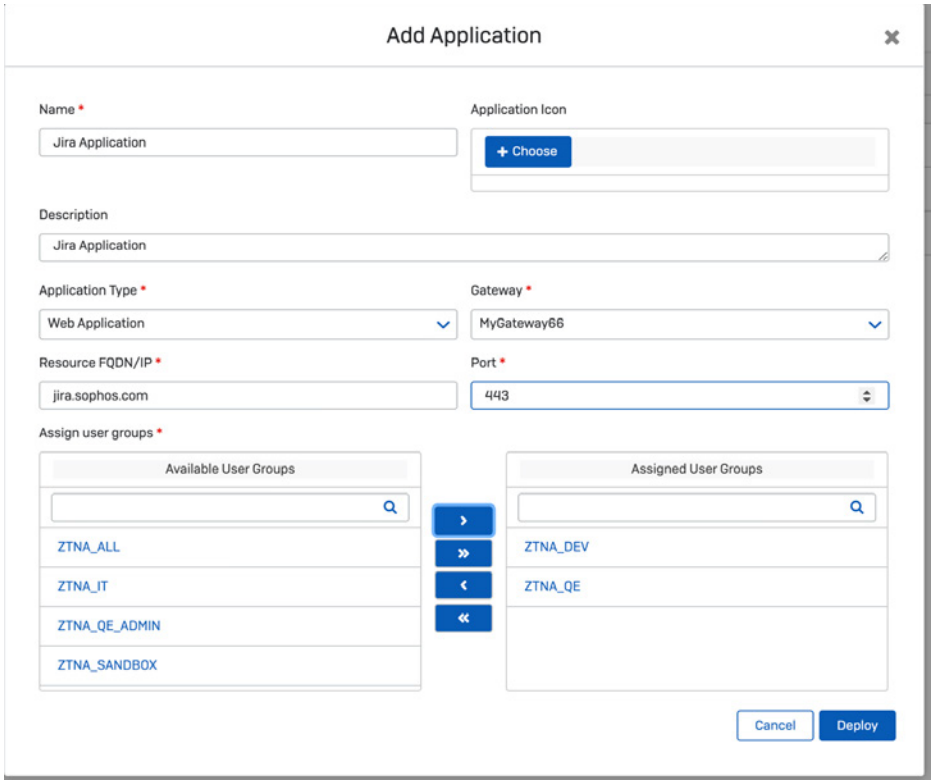
Sophos ZTNA では、デバイスが登録され、最新で、適切に保護され、暗号化が有効になっていることを確認します。次にその情報を使用して、お客様の重要なネットワークアプリケーションへのアクセスおよび権限を決定するためにカスタマイズ可能なポリシーを基にした判定を下します。



Sophos ZTNA のアプローチ

Sophos ZTNA の主な機能

- サイバー攻撃に対する防御が強化されます。Sophos ZTNA では、非常に細かな制御が可能です。ユーザー、デバイス、アプリケーションはすべて、個々の企業ポリシーとお好みのリスクレベルに基づいて制御できます。また、ネットワーク上に存在するという理由だけで個人を暗黙的に信頼するという概念もなくなります。代わりに、アクセスを許可する前に ID とデバイスのセキュリティ状態を継続的に評価することで、保護を強化し、ネットワーク内のラテラルムーブメントのリスクを最小限に抑えます。
- 業務が効率化します。Sophos ZTNA は、Sophos Central プラットフォームを介して管理されるため、新しいユーザーの登録や変化する作業環境のサポートを簡単にできます。さらに、VPN と比較した際に、エンドユーザーに対してより透過的で、摩擦のない「it just works (ちゃんと動く)」タイプの接続エクスペリエンスを提供します。



Sophos ZTNA でアプリケーションを簡単に追加

ソフォスの受賞歴のあるセキュリティ製品は、どちらの方法を選択しても、場所やデバイスを問わず、従業員を保護することができます。

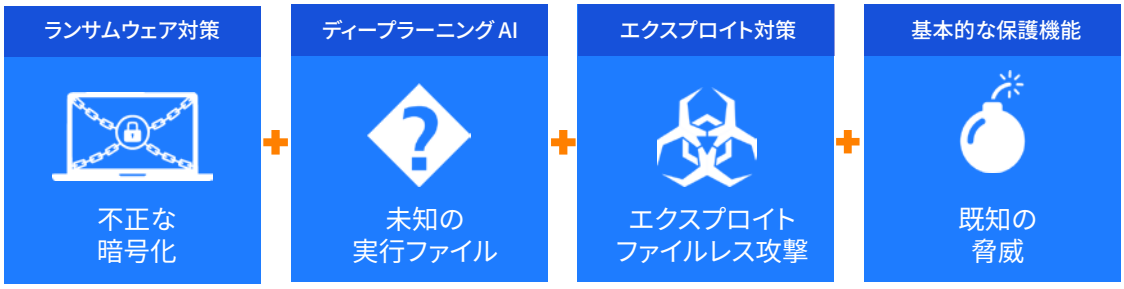
デバイスの保護

過去 1年間で、組織の 51%がランサムウェアの被害に遭い、犯罪者は攻撃[2]の 73%でデータの暗号化に成功しました。

これらの驚くべき統計情報を、デスクトップ、ノート PC、企業、個人用デバイスなどのあらゆる種類の機器と、Windows、macOS、Linux、Android、Chromebook、iOSなどの多数のオペレーティングシステムを保護する必要性と合わせると、サイバーセキュリティの悩みの種が大きくなりそうです。

Sophos Intercept X は、これらすべてのデバイスとプラットフォームにわたり業界最高の保護を提供します。キルチェーンのいたるところで攻撃者を食い止める、次のような何層ものテクノロジーレイヤー備えています。

- ファイル、ハードディスク、ブートレコードの不正な暗号化をブロックし、それらを安全な状態に復元するランサムウェア対策
- 数百万ものファイル属性を使用して、脅威を解析し、既知のマルウェアや未知のマルウェアの両方を阻止し、脅威が実行される前に阻止するディープラーニング AI
- エクスプロイト、アクティブな攻撃手法、ファイルレス攻撃、スクリプトベース攻撃をブロックするエクスプロイト対策テクノロジー
- 既知の脅威を阻止する基本的なシグネチャベースの保護



さらに、Sophos Intercept X は、あらゆるプラットフォーム上のあらゆるデバイスを保護するため、従業員は、次のようなデバイスで安全に作業できます。

- Windows および macOS を実行するデスクトップおよびノート PC
- Windows や Linux サーバー
- クラウドプロバイダーでホストされる仮想デスクトップ環境
- Android、iOS、Chromebook を実行しているモバイル

EDR (エンドポイントでの検出と対応)

最も破壊的なサイバー脅威は、人間主導の攻撃を伴い、PowerShell などの正当なツールやプロセスを悪用することがよくあります。攻撃者は、実際にライブでハッキングすることにより、戦術、手法、手順 (TTP) を変更して、セキュリティ製品やプロトコルを回避することができます。ユーザーのネットワーク内部に侵入すると、攻撃者は横方向に移動し、データを盗み出し、ランサムウェアを展開し、マルウェアとバックドアをインストールして将来の攻撃に備える可能性があります。

こうした人間主導の攻撃を阻止するには、アナリスト主導の脅威ハンティングが必要です。**Intercept X with EDR** (エンドポイントでの検出と対応) は、お客様に必要なツールを提供し、Intercept X と同じ管理コンソールから脅威ハンティングを実行できます。

それは、セキュリティアナリストと IT 管理者向けに設計された最初の EDR です。他社の EDR ツールでは、多くの場合、専用の担当者または社内の SOC (セキュリティ運用センター) が必要ですが、Sophos EDR なら、堅牢な分析を実行しながら、セキュリティアナリストがいなくても簡単に使用できます。

Intercept X with EDR を使用すると、すぐに使用可能でカスタマイズできるパワフルな SQL クエリを使用して、疑わしい信号や脅威を調査し、IT の予防策を向上させることができます。ユースケースは次のとおりです。

- Chrome の動作が遅い。Chrome に不正な拡張機能がインストールされていることを確認
- ネットワークアクティビティのチェック。ログインの失敗と PowerShell からのアクティブな通信を探す
- ソフトウェアクエリ。機密ファイルがデバイスから削除されていることや、ソフトウェアライセンスの使用量を超えていないことを確認
- フィッシング調査。不審なリンクをクリックしたユーザーを特定し、ファイルをダウンロードしたかどうかを確認

さらに、コマンドラインツールを使用してデバイスにリモートアクセスし、デバイスの再起動、アクティブプロセスの終了、スクリプトまたはプログラムの実行、構成ファイルの編集、フォレンジックツールの実行、ソフトウェアのインストール/アンインストールなどの問題を修正できます。

MDR (Managed Threat Detection and Response)

脅威ハンティングや調査を実行する時間、能力、または専門知識がない場合は、**Sophos Managed Threat Response** (MTR) サービスが役立ちます。

Sophos MTR は、フルマネージドサービスとして 24時間年中無休の監視、検出、および対応機能を提供する脅威ハンターと対応の専門家のチームです。その専門家は、潜在的な脅威やインシデントを積極的に探して検証し、害を引き起こす前に阻止します。

また、ソフォスの保護ソリューションからのデータフィードを相互に関連付けて、感染の痕跡を特定します。他の MDR サービスとは異なり、ソフォスは問題をお客様に通知するだけでなく、脅威を無力化するのに最も効果的なアクションを判断して適用します。

モバイルデバイス

従業員が個人用のデバイスを使用して仕事をする場合、IT チームは、ユーザーのプライバシーを損なうことなく、企業データを保護するという課題に直面しています。統合エンドポイント管理ソリューションである **Sophos Mobile** は、iOS、Android、Chrome OS、Windows 10、および macOS デバイスを保護します。個人所有であるか会社所有であるかにかかわらず、最小限の手間でモバイルデバイスを保護できるため、Sophos Mobile は BYOD (個人所有デバイスの業務利用) 環境に最適です。

Sophos Mobile では、次のことが可能です。

- モバイル脅威を阻止する。モバイルマルウェア、フィッシング、中間者攻撃などに対して、Intercept X を活用した業界をリードする防御策を提供。
- 企業データの保護。必要に応じて、フルデバイスまたはコンテナのみの管理を選択
- 管理を削減。ユーザーは、フレキシブルなセルフサービスポータルを利用することで、IT 部門の関与が不要となるため、個人所有の macOS、Windows 10、またはモバイルのデバイスを登録したり、パスワードをリセットしたり、サポートを受けることができます。

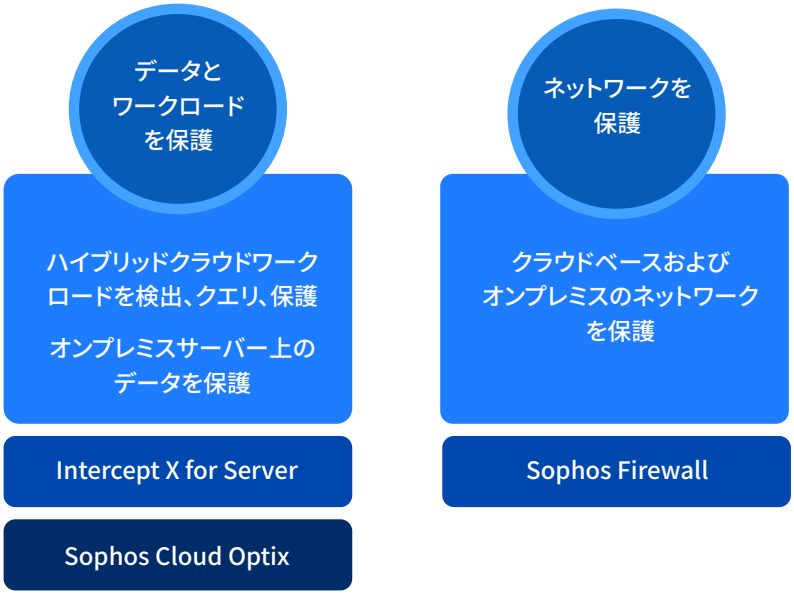
リソースの保護

組織の必要性に応じて、サーバーをオンプレミスで実行したり、クラウドベースのアプリケーションを使用したり、または AWS、Azure、GCP 上のプライベートおよびパブリッククラウド環境でリソースをホストしたりできます。多くの場合、こちらのすべての実行しています。

クラウドは、ほとんどの組織の日常業務において、中心的な役割を急速に果たしています。このため、サイバー犯罪者はクラウドが提供する攻撃の機会を狙っており、パブリッククラウドを使用している企業の 70% が過去 12か月間[3] にクラウドセキュリティインシデント見舞われました。

リソースを保護する場合、リソースがどこにあったとしても、次の 2つのことを行う必要があります。

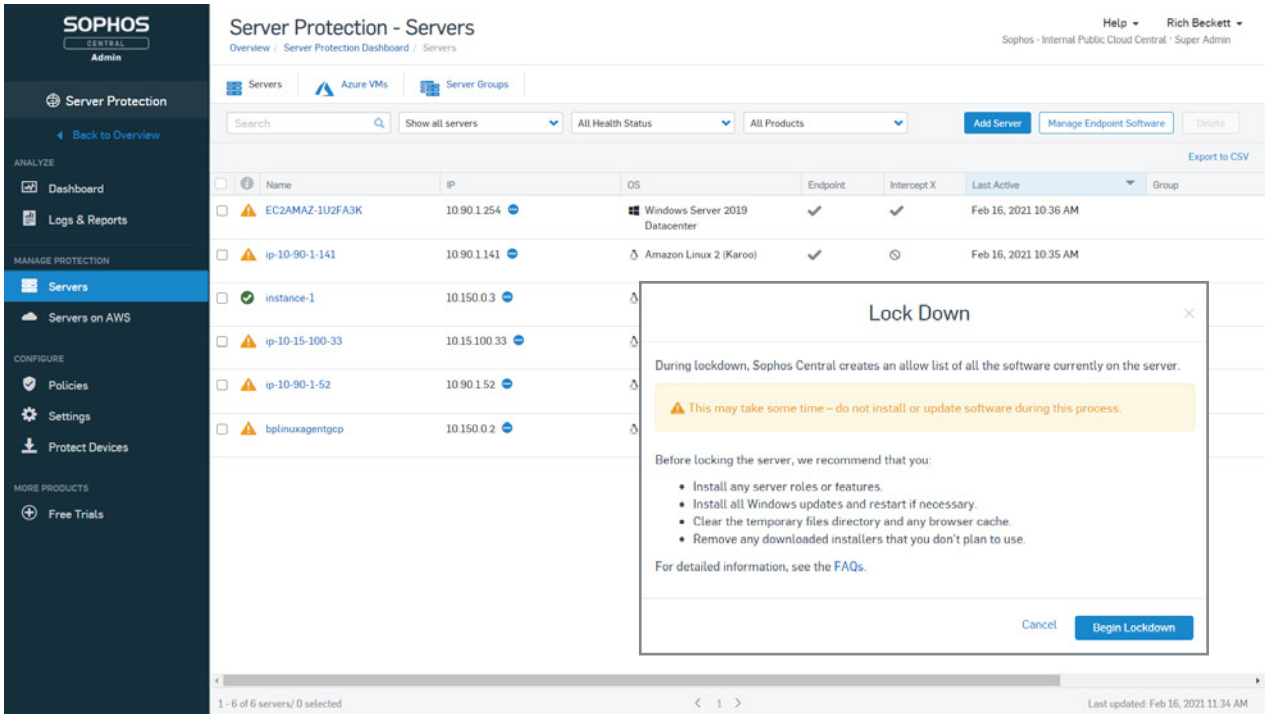
1. データとワークロードそのものを保護
2. 侵入者を阻止するために、ネットワークを保護



データとワークロードを保護

データとワークロードは最も重要な資産です。**Sophos Intercept X for Server** は、クラウド、オンプレミス、またはハイブリッドのワークロード環境を保護します。Windows および Linux 仮想マシンと仮想デスクトップを最新の脅威から守ります。

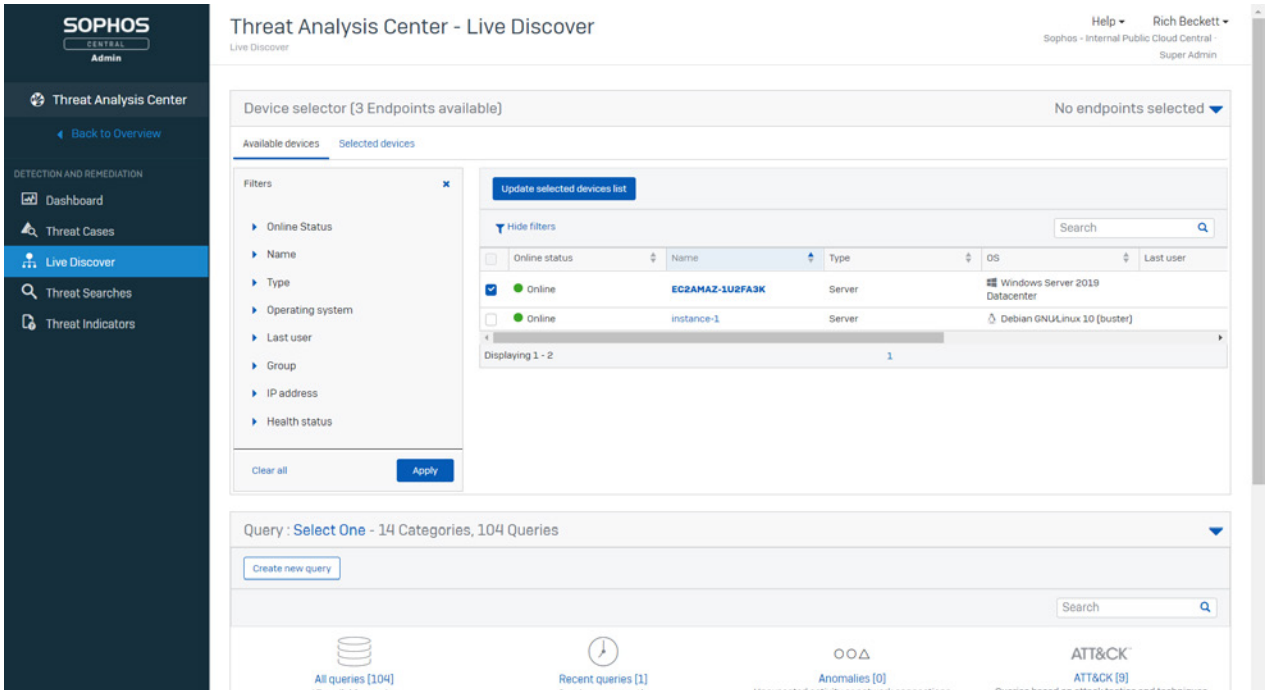
- 高度な脅威を阻止する。ランサムウェア、エクスプロイトベースの攻撃、未知のマルウェアなどが含まれる
- サーバーのワークロードのロックダウン。実行できるもの、できないものを制御し、未承認の変更があった場合は通知を受信
- すべてを一元管理。クラウドワークロードとオンプレミスサーバーが混在する環境も含めて、単一のコンソールからすべてを導入、管理



Intercept X for Server

また、**Intercept X for Server with EDR** を使用して、オンプレミスでもクラウドでも EDR 調査をユーザーのサーバーに拡張することもできます。これにより、次のことが可能になります。

- 重要な IT 運用と脅威ハンティングのタスクを実行。パフォーマンスの問題を特定し、どこに何がインストールされているかを確認して、疑わしいアクティビティを追跡する
- クラウドワークロードを自動的に検出。S3 バケット、データベース、サーバーレス機能など、重要なクラウドサービスに注意を払う
- 安全でない展開を検出。AI を利用してクラウド環境を常時監視し、異常を通知する

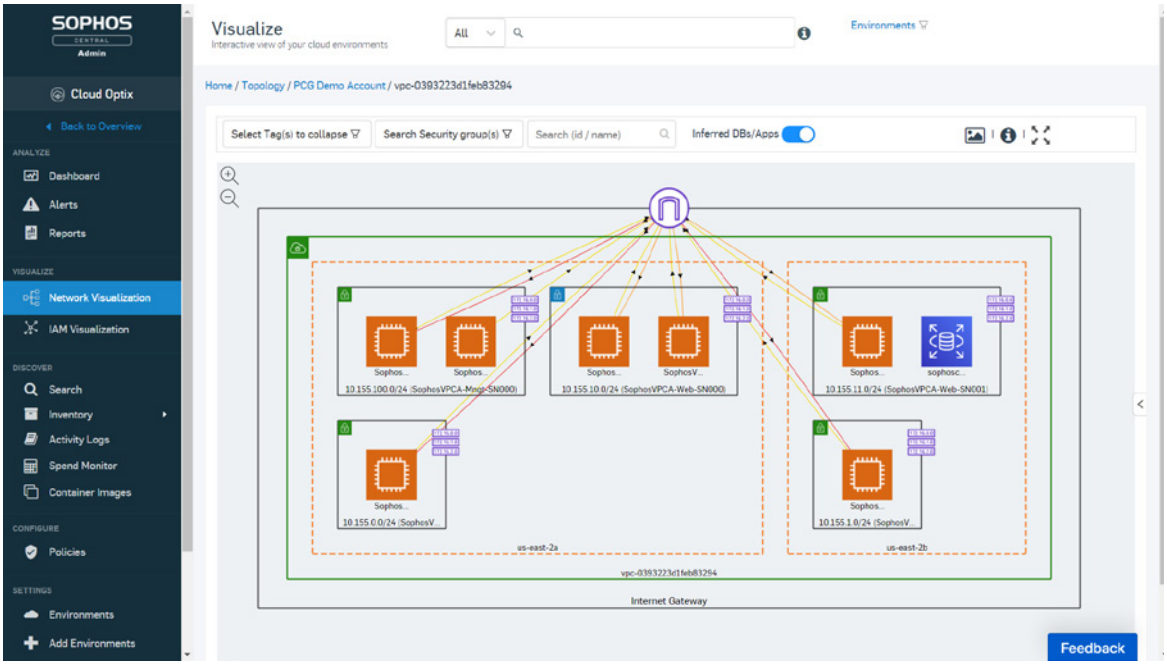


EDR 調査をサーバーに拡張

保護は、データとワークロード保護のコインの片面です。反対の側面は可視性です。実行しているものを継続的かつ明確に把握し、セキュリティ侵害を防止するためにクラウドプロバイダーサービスを構成する機能が必要です。

クラウドセキュリティポスチャ管理ソリューションである **Sophos Cloud Optix** は、組織を保護するために必要な可視性を提供します。これには次のものが含まれます。

- マルチクラウドの可視性。AWS、Azure、GCP 向けのサーバー、コンテナ、ストレージ、ネットワーク、IAM などの詳細なクラウドリソースインベントリ
- リスクに応じた優先順位付け。セキュリティリスクや過剰な権限を持つ IAM アクセスに対して構成を継続的に分析
- コンプライアンス管理。すぐに使用できるテンプレート、カスタムポリシー、コラボレーションツールを使用して、コンプライアンスを継続的に監視
- 統合されたセキュリティ。AWS 上のソフォスのファイアウォール製品とワークロード保護を特定
- クラウドコストの最適化。AWS と Azure の支出を 1つの画面で管理



Sophos Cloud Optix

Amazon GuardDuty などのサービスは優れた価値を提供するため、クラウド環境向けのセキュリティアラートは役立ちますが、膨大な量の通知に圧倒されるでしょう。そのため、実際に処理が必要な通知を把握することが非常に難しくなる可能性があります。

ソフォスでは Sophos Cloud Optix を使用して、サイバーセキュリティ管理プラットフォームである Sophos Central のホスティングに使用される Amazon Web Services 環境を保護しています。Cloud Optix からセキュリティチームが得た主なメリットの 1つは、何が大切かに焦点を当てられることです。

「Sophos Cloud Optix を使用することで、大量の警告による疲弊を大幅に抑制することができます。Sophos Cloud Optix に組み込まれている強力な AI は、データを相関し、本当に意味のある、対処が必要なものを表示します。」
Ross McKerchar, VP and CISO, Sophos

ネットワークを保護

リソースを保護するには、それが実行されているネットワークも保護する必要があります。**Sophos Firewall** は、オンプレミス環境、AWS 環境、Azure 環境のすべてにおいて、卓越した保護と可視性を提供します。

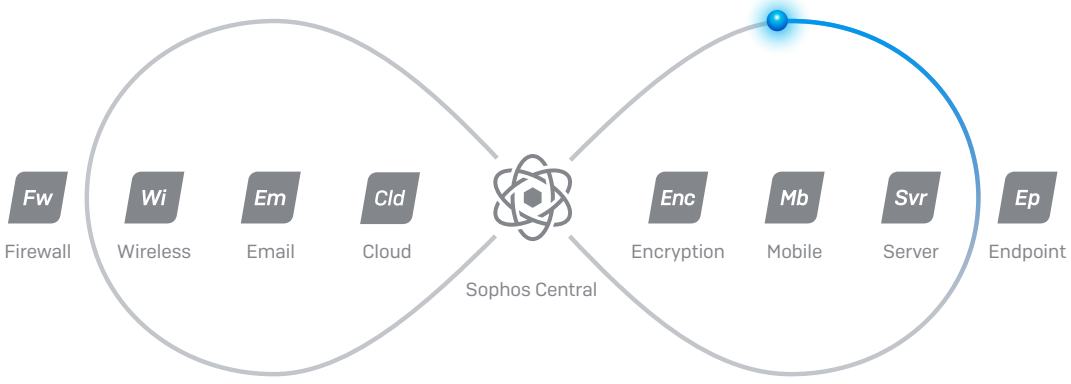
- 統合されたマルチレイヤー保護により、最も高度な脅威も阻止
- ユーザーやネットワークのアクティビティを完全に把握できるなど、充実したレポート機能を備えた、WAF、IPS、ATP、URL フィルタリング、パスベースルーティング、国レベルのブロッキングのための強力なオールインワンソリューション
- クラウドアプリケーションの可視性、シャドー IT の検出、自動化された脅威対応
- リバースプロキシ認証で接続するユーザーには、安全なアクセスを提供する一方、SQL インジェクションやクロスサイトスクリプティングなどのハッカー攻撃に対してクラウドワークロードを強化する機能
- スタンドアロンおよび HA ソリューションとして実行できる柔軟性

また、事前設定された単一の仮想マシンイメージですべてが提供されるので、クラウドベースの導入が容易です。

管理の簡素化

ソフォス製品を使用すると、単一の Web ベースの管理プラットフォームですべてのセキュリティを管理できます。Sophos Central では、組織を保護するために、コンソールから他のコンソールにジャンプする必要はありません。すべてが 1か所にまとめられています。 また、複数のサービスからのデータを相関させて、製品をまたいだ調査を簡単に実行できます。

Sophos Central はクラウドでホストされるため、分散型の IT 部門に最適です。世界に40万人を超えるユーザーが、業界で最も信頼されているサイバーセキュリティ管理プラットフォームを使用しているので、安心してご利用いただけます。



また、Sophos Central を使用すると、ソフォス製品は脅威の状態とセキュリティ情報をリアルタイムで共有し、連係して自動的に脅威に対応できます。これを Synchronized Security と言います。次のようなメリットがあります。

- インシデントレスポンスの自動化。ソフォスの製品は、マルウェア感染やコンプライアンス違反のデバイスなど、疑わしいものを検出すると、この情報を他のサイバーセキュリティシステムと共有します。その後、他の製品は数秒でインシデントに自動的に対応します。以下は例です。
  - Sophos Firewall は、感染したデバイスを即座に隔離し、脅威の拡散を防ぎ、ラテラルムーブメントをブロックします。
  - Intercept X は、侵害されたメールボックスが検出されると、エンドポイントを自動的にスキャンし、メールを脅威の影響を最小化することができます。
  - Sophos WiFi は、準拠していないデバイスのネットワークアクセスを制限し、不正なデバイスや安全でないデバイスをワイヤレスネットワークから隔離します。
- 独自の分析。IT チームは、次の機能を含むネットワークの可視性や制御の向上を享受できます。
  - IP アドレスではなく名前で感染を特定し、セキュリティ調査を迅速化します。
  - ネットワーク上のすべてのアプリを識別。平均して、ネットワークトラフィックの 43% が「未分類」として通過するため、IT チームは、それが良いものか悪いものか、または悪意があるのかを判断できません。Synchronized Security を使用すると、Sophos Firewall と Intercept X が連携して、ネットワーク上のすべてのアプリを自動的に識別し、分類します。

卓越した保護、卓越した効率性

ソフォスのサイバーセキュリティシステムを実行すると、次世代型の保護、単一の管理のプラットフォーム、製品間で脅威インテリジェンスの共有、自動化されたインシデント対応が可能となります。これらの機能を組み合わせることで、IT チームの効率性と生産性が大幅に向上します。

実際に、Sophos Central で管理されている Sophos Intercept X と Sophos Firewall を実行しているお客様は、**IT チームの効率を 2 倍**にしながら、**セキュリティインシデントを 85% 減少**させていると常に述べています。

「ほとんどのセキュリティイベントを自動的に検出し、修正するツールがあることで、当社の小規模な IT チームは会社のセキュリティを管理し、セキュリティが侵害されるのを防ぐことができます。」

Chief Technology Officer, Software Services Provider

あらゆる場所、あらゆるデバイス、あらゆるリソースを保護

柔軟なリモートワークとクラウドの利用拡大への移行から後戻りすることはありません。これらは生活を楽にしますが、IT チームにとっては新たな課題をもたらし、悪意のある人たちにとっては新たな機会をもたらしています。この新しい環境を保護するには、IT に使うオーバーヘッドを増やすことなく、どこにいても安全な接続、安全なリソース、安全なデバイスが必要となります。

ソフォスは、強力で信頼性の高いソリューションを使用して、これらの最新の課題に対処する支援をします。ご要望に関しては、または、ソフォスの製品を試用する際に無償評価版を有効にするには、ソフォスの営業担当者に問い合わせをしてください。

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

2.補足 ランサムウェアの現状 2020年版、ソフォスより

3.補足 クラウドセキュリティの現状 2020年版、ソフォスより

ソフォス株式会社営業部
Email: sales@sophos.co.jp

210215 WPEN (MP)

SOPHOS