SOPHOS
Cybersecurity evolved.

ヘルスケア業界向けのサイバーセキュリティガイド

患者のケアを妨げずに攻撃を即座に阻止する、ヘルスケア業界向けのサイバーセキュリティ

ソフォス ソリューション概説 2021年 4月

サイバーセキュリティと患者ケア

患者ケアについて考えると、最初に思いつくのは、医療サービスを提供する医師、看護師、およびその他の医療専門家です。しかし、AI からクラウドコンピューティング、接続されているデバイスに至るまで、ヘルスケア業界がテクノロジーにますます依存し、攻撃者の手法が進化し続けるなか、サイバーセキュリティは、患者ケアの提供を可能にするうえで、直接的かつ重要な役割を果たしています。

「効果的でないサイバーセキュリティは、患者の安全を脅かす、今そこにある危機です…サイバーインシデントは、医療システムやケアシステムを大幅に中断させて、患者に危害を与える直接の原因となる可能性があります。」

Institute of Global Health Innovation、Imperial College London

新型コロナウイルスのパンデミックは、遠隔地からの患者監視ソリューション、オンライン診療、自宅で使用するデバイスなどのデジタル医療テクノロジーの導入を加速させ、モバイルワーカー / リモートワーカーの増加につながりました。このような変化は、ヘルスケア業界の効率性を大幅に向上させ、これは長期的にも継続していくものと思われますが、同時に、医療機関の IT チームが直面するサイバーセキュリティの課題も増加させました。

「(サイバー攻撃者) は、将来ヘルスケア業界のデジタル化がますます重要になるという事実を悪用しようとしています。」

John Noble、Chair、Information Assurance and Cyber Security Committee、NHS Digital

ヘルスケア業界のサイバーセキュリティの課題

2021年、30か国の 328人の医療機関の IT 専門家を対象にソフォスが行った調査では、サイバーセキュリティの状況は非常に厳しいものになっていることが明らかになりました。回答者の 63%が、2020年の1年間、発生したサイバー攻撃の数が増加したと回答しています。少なくとも部分的には、攻撃者がパンデミックを悪用したことが原動力となっていると思われます。その結果、回答者の 70%が、2020年の 1年間にサイバーセキュリティの作業量が増加したと回答したことは驚くべきことではありません。

攻撃は、発生件数が増加しているだけでなく、同時に複雑化しています。回答者の 60%が、現在、サイバー攻撃は、組織内の IT チームが単独で対処するには高度すぎると回答しています。

63%	60%	70%
2020年の 1年間にサイバー攻撃の数が増加したと報告した回答者の割合	サイバー攻撃は、IT チームが単独で対処するには高度すぎると報告した回答者の割合	2020年の 1年間にサイバーセキュリティの作業量が増加したと報告した回答者の割合

複雑さはセキュリティの敵

医療機関におけるユーザーと IT スタッフの比率は、通常、平均値を上回っています。セキュリティインフラが複雑になればなるほど、過剰な負担がかかっている IT チームは、それを最新の状態を維持したり、利用可能な保護機能を最大限に活用したりすることが困難になります。

ソフォス：ヘルスケア業界の保護

ソフォスは、世界中の医療機関と連携して、サイバーセキュリティの課題に対処し、患者ケアを中断なく提供することを可能にします。攻撃の頻度と巧妙さが増すなか、ソフォスは、顧客のデータと組織の安全性を維持しながら、多忙な IT チームがサイバーセキュリティの作業量を削減できるよう支援します。以下で、医療機関が直面している最も一般的なサイバーセキュリティの課題の対処方法についてお読みいただけます。

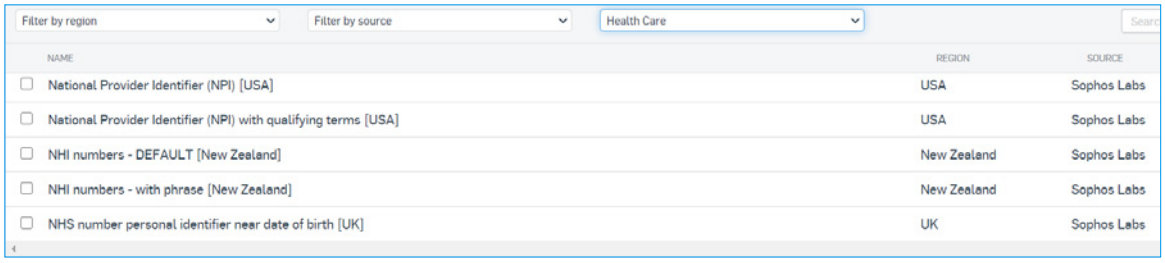
保存場所に関係なく機密データを保護する

医療機関は、医療記録から社会保障番号や個人識別情報 (PII) まで、さまざまな形式の機密データを保有しています。 医療機関には多数の種類の機密データがあり、多数の場所で保管・使用されているため、すべてを保護することは困難な場合があります。

ソフォスの予防的かつプロアクティブな保護ツールは、個々のデバイスを含め、医療機関ネットワーク全体にセキュリティを提供します。

データを保持するデバイスやワークロードの保護

Sophos Intercept X によるエンドポイントおよびサーバー保護は、複数の保護レイヤーを導入して、Windows、Mac、Linux、および仮想マシン上のデータを保護します。医療機関固有のデータ流出防止ルールは、医療用語やデータタイプを使用して保護を強化します。



Sophos Device Encryption は、迅速かつ簡単に Windows および macOS デバイスを安全に暗号化することを可能にし、データの紛失・盗難時にはデータを保護 (およびコンプライアンスを証明) することができます。

データが通過するネットワークの保護

Sophos Firewall は、AI 搭載の脅威検出テクノロジーを使用して、機密性の高い医療データ、重要な医療システム、およびエコシステムの他の部分への攻撃を防ぎます。

メール経由による、故意または偶発的な流出の防止

Sophos Email は、個人識別情報、患者の記録、医療画像、および他の機密データを暗号化し、偶発的なデータ侵害と悪意のあるデータ侵害の両方を阻止します。

データアクセスの制御

Sophos Zero Trust Network Access (ZTNA) は、ネットワーク上のデータにアクセスできるユーザーを確実に制御します。非常に細かい制御により、ラテラルムーブメントをブロックする一方、承認済みユーザーのみが機密データにアクセスできるようにします。

ヘルスケア業界を対象にするランサムウェアの脅威に真っ向から立ち向かう

ランサムウェアは、より巧妙で破壊的になりつつあります。そして、ヘルスケア業界は、攻撃者にとって収益性の高い標的です。ヘルスケア業界にとって、ランサムウェアのコストは身代金の支払いだけではありません。患者データを紛失したり、医療処置を遅らせたりキャンセルしたりするコストは、莫大で壊滅的な被害を与える可能性があります。ソフォスのプロアクティブな脅威ハンティングおよび防御ツールは、ランサムウェアの先手を打つように絶えず進化しており、このような攻撃からデータとネットワークを保護します。

ランサムウェアによる暗号化被害の阻止

ソフォスは、世界的なリーダーとして、ランサムウェアから組織を保護しています。

Sophos Intercept X は、エンドポイントとサーバーに、世界最高レベルのランサムウェア対策を提供します。ランサムウェアを検出して停止するために、次のような複数のセキュリティレイヤーがあります。

- CryptoGuard: 未承認のユーザーによって暗号化されたファイルを、安全な状態に自動的にロールバックします
- AI 搭載のディープラーニング: 既知および未知のランサムウェアをブロックします
- エクスプロイト対策: 攻撃者がランサムウェアのダウンロードとインストールに使用する手法をブロックします
- SophosLabs: 基本的な、シグニチャベースの保護を提供します

Sophos Managed Threat Response (MTR) は、ソフォスの最高レベルのランサムウェア保護を提供し、プロアクティブな脅威ハンティング、検出、および対応機能を、専門家チームが 24時間 365日体制で管理するサービスとして提供します。日夜を問わず、常に監視しています。

Sophos Rapid Response は、ソフォスのお客様でないユーザーも含め、ランサムウェアのライブ攻撃に対して、緊急サポートを提供します。ソフォスのチームは、ネットワーク、アプリケーション、データを保護し、被害や中断を防止するために、迅速に攻撃を制御することを支援します。

どこからでも安全なアクセスをユーザーに提供する

医療従事者は、病院の現場で働く従業員、地域で働く従業員、または在宅勤務している従業員であっても、機密性の高い患者データや医療システムにいつでもアクセスできる必要があります。ソフォスのツールを使用すると、ユーザーは重要な医療業務に影響を与えることなく、どこからでも安全に接続できます。

どこからでもユーザーの安全な接続を実現

Sophos Firewall は、無料の Sophos Connect VPN を介して、Windows および macOS にセキュアな接続を提供します。導入と設定が簡単で、リモートユーザーは、Windows や macOS デバイスからネットワークやパブリッククラウドのリソースへ、安全にアクセスできるようになります。さらに、140万人以上のアクティブなお客様によって使用されおり、安心してご利用いただけます。

医療業界におけるランサムウェアの現実

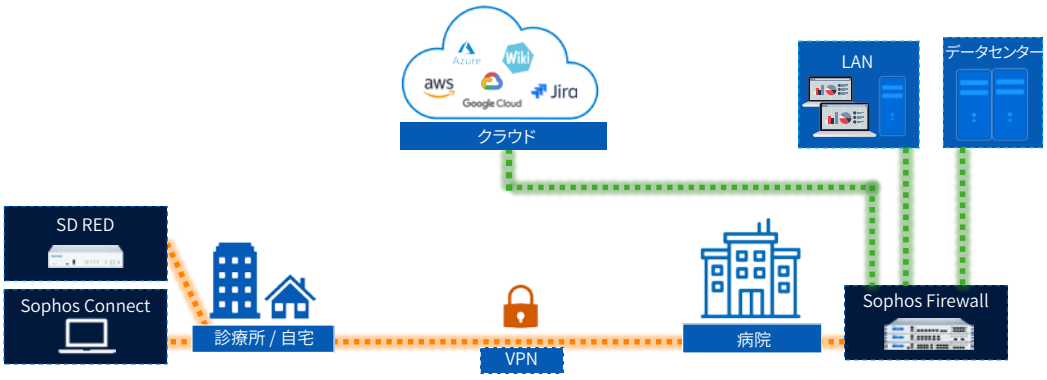
34%: 過去 1年間にランサムウェア攻撃を受けた

65%: データを暗号化した攻撃

34%: 身代金を支払った

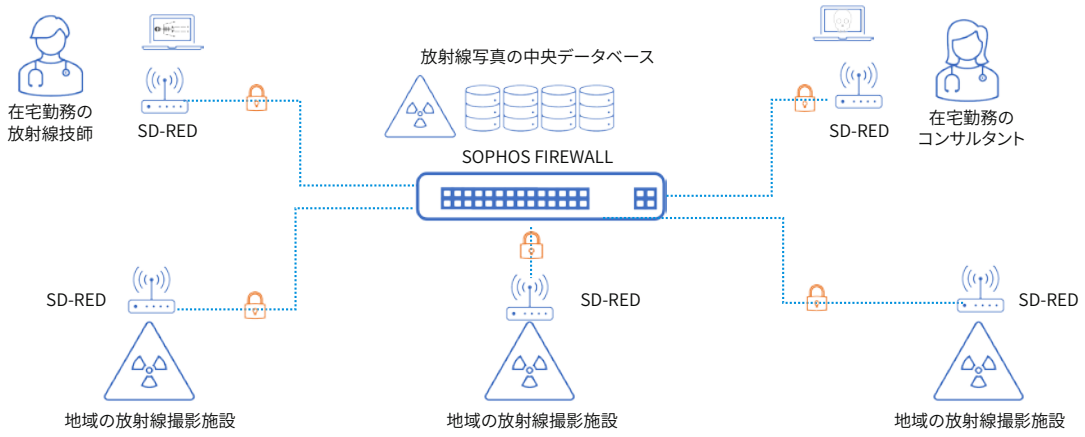
127万米ドル: 平均復旧コスト

ランサムウェアの現状 2021年版、ソフォスより



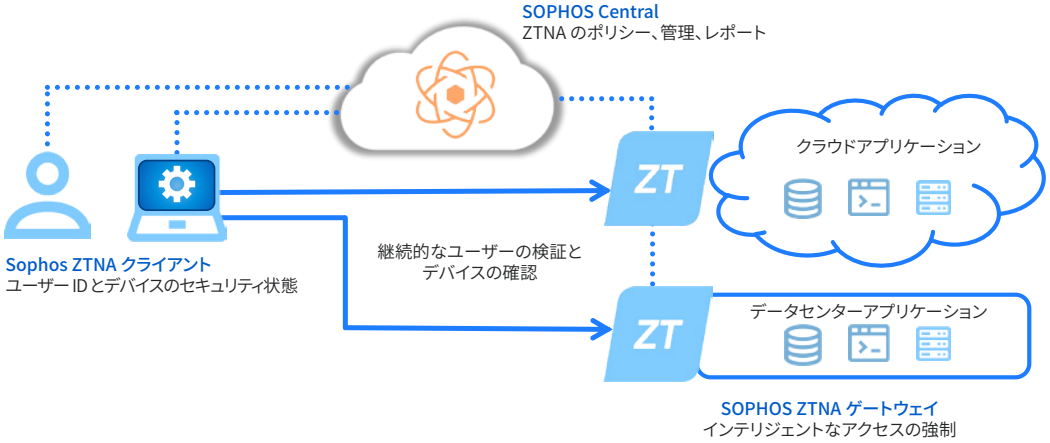
Sophos Firewall は、Sophos Connect クライアントおよび SD-RED デバイスを介して、セキュアなリモートアクセスを提供します

究極のリモート接続を実現する **SD-RED** (Remote Ethernet Device) は、**Sophos Firewall** と連係して、リモートサイトや自宅をメインネットワークに接続する、小型のプラグアンドプレイ デバイスです。この製品は、地域の診療所や医療施設だけでなく、機密性の高いデータを持つユーザーにも最適です。



放射線撮影での Sophos Firewall と SD-RED の使用例

次世代型の安全なアクセスを提供する **Sophos Zero Trust Network Access** は、デジタル ID を防御の中心に置き、ユーザー、デバイス、ポリシーのコンプライアンスを常に検証します。ユーザーに透過的な「Just Works (確認なし)」エクスペリエンスを提供する一方で、IT チームが新しいユーザーの設定を迅速に行うことができるようにします。



IT チームを強化する

ヘルスケア業界を含む、さまざまな業界の 5,000人の IT 管理者を対象に 2020年に実施したソフォスの調査では、調査回答者の 81% が、スキルの高い IT セキュリティ専門家を探して確保することは、IT セキュリティを提供する組織にとって大きな課題である、と回答しています。

専門知識の補充、または組織内のリソースを補完する場合であっても、ソフォスのセキュリティの専門家は、組織内のチームの延長のような役割を果たして、医療システムや患者データを 24時間 365日安全に保管します。

ソフォスの専任サイバーセキュリティ専門家が顧客の IT チームを強化

Sophos Managed Threat Response (MTR) は、脅威ハンティングと対応のエキスパートで構成されるチームで、組織内のチームの延長のような役割を果たします。過剰な負担がかかっている医療機関の IT チームに、あらゆる脅威に対処するために必要なリソースと専門知識を提供します。

Sophos MTR チームは、顧客の環境を 24時間 365日監視し、潜在的な脅威やインシデントを積極的に探して検証します。疑わしい兆候を検出したら、SophosLabs のマルウェア専門家に連絡して、それを調査したり、解析したりすることができます。

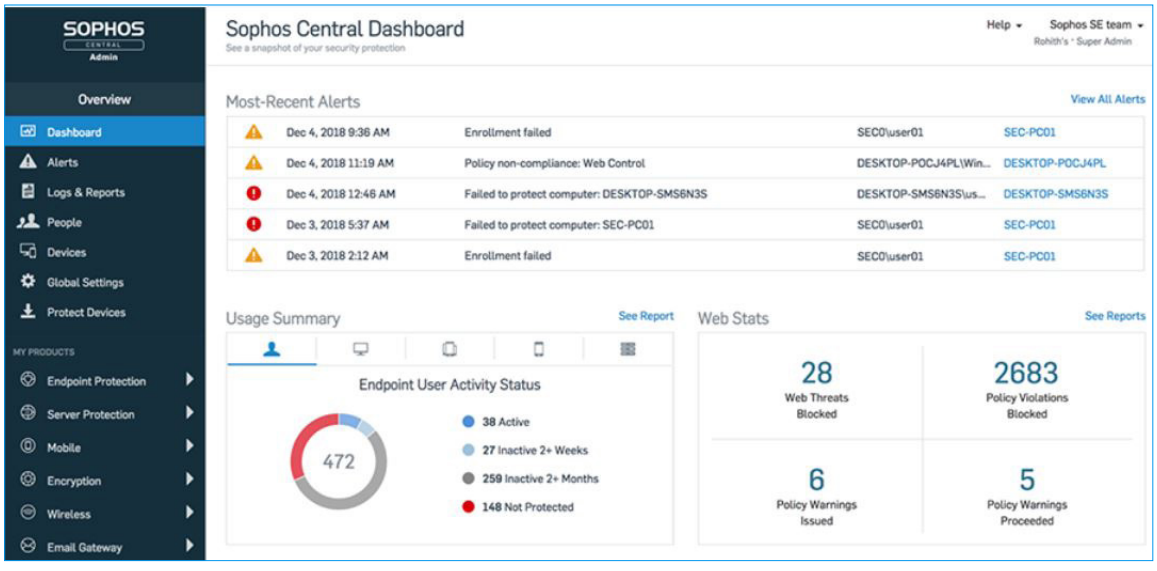
また、Sophos MTR チームは、顧客に代わってアクションを実行することもできます。他の MDR サービスとは異なり、ソフォスのチームは問題を顧客に通知するだけでなく、脅威を無効化することもできます。つまり、ソフォスがどのレベルのアクションをとるべきか、そして組織内のチームとどのように連携するかは顧客が決定します。

サイバーセキュリティの管理に費やす時間を削減する

IT リソースが限られている場合、殺到するセキュリティ警告を選別して、どの警告に最初に対処するかを決定することは困難になります。ソフォスは、セキュリティを単一のコンソールで表示し、対処が必要になる前に問題を解決する自動化機能を備えているため、顧客は、情報を選別して対処し、戦略的な違いを生み出すため作業に集中することができます。

サイバーセキュリティ管理の簡素化

Sophos Central は、すべてのソフォスセキュリティ製品を管理できる、Web ベースの統合プラットフォームです。組織を保護するために、コンソールからコンソールへと移動する必要がなくなりました。Sophos Central を使用すると、保護を簡単に導入および管理し、複数のサービスのデータを相関させる、製品の枠組みにとらわれない総合的な調査を 1つの画面で実施できます。



サイバーセキュリティ対策すべてを Sophos Central プラットフォームで管理

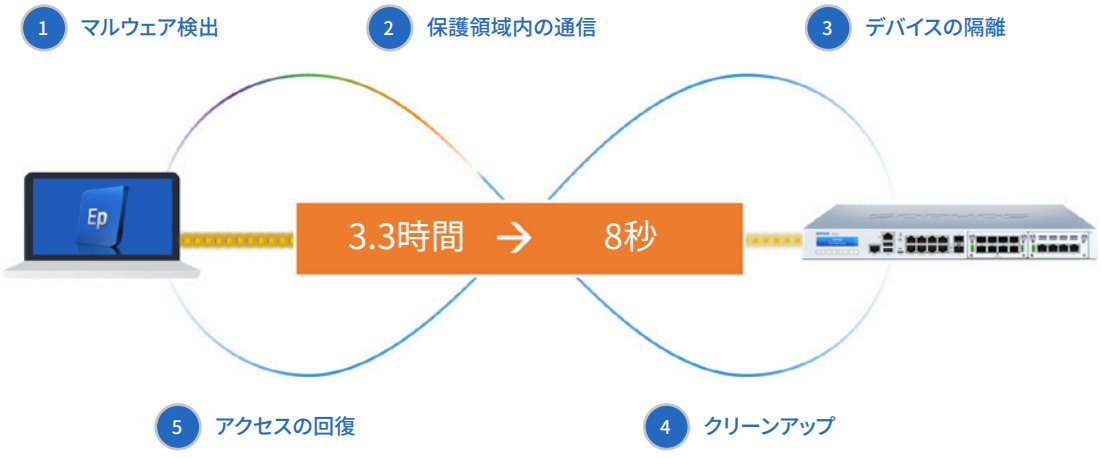
保護機能の自動化

Sophos Central により、ソフォス製品間で情報を共有すること、および、リアルタイムで連係しインシデントに自動対応することが可能になります。この統合と自動化により、IT チームの作業量の負担を軽減しながら、保護を強化できます。

例 1: インシデントへの自動的な対応

- Sophos Intercept X がエンドポイントで脅威を検出すると、即座に Sophos Firewall に通知します。
- Sophos Firewall は、感染したエンドポイントをネットワークから (同じ LAN 上の別のデバイスからも) 自動的に隔離します。
- Intercept X は脅威をクリーンアップし、完了すると Sophos Firewall に通知します。
- Sophos Firewall は直ちにネットワークアクセスを復元します。

手動では約 3時間半を要するこの一連のプロセスが、8秒以内で完了します。

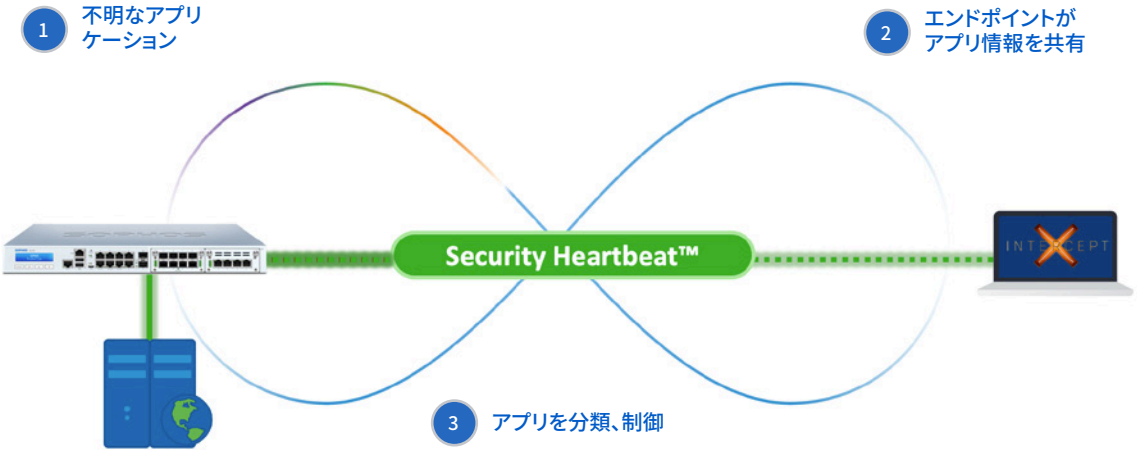


インシデント対応の自動化

例 2: ネットワーク上の不要と思われるアプリすべてを識別

識別されないネットワークトラフィックの割合は、平均で 43% にも上ります。一部は、標準のシグネチャファイルがないカスタムアプリケーションです。また、悪意のあるアプリが、ファイアウォールによる検出を逃れようとしている場合もあります。

- Sophos Firewall が、既存のシグニチャファイルと一致しないアプリケーションを検出した場合、それを「HTTPS」などの汎用トラフィックのバケットに割り当てる代わりに、Sophos Firewall は Sophos Intercept X に連絡します。
- Intercept X は、分類を行う Sophos Firewall にアプリケーション名、パッチ、カテゴリを返します。その後、アプリケーションは、適切なグループに自動的に割り当てられます。
- そのグループに制御手段が適用されている場合 (例: ブロックなど)、そのルールが適用されます。必要に応じて、たとえばカスタムアプリの場合、管理者はカテゴリとポリシーを手動で設定して適用できます。



ネットワーク上のすべてのアプリとプロセスを識別

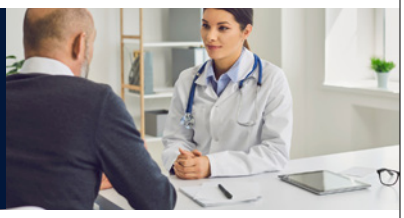
実環境における TCO の削減

ソフォスのサイバーセキュリティのメリットは積み重なります。次世代型テクノロジー、自動インシデント対応、情報のリアルタイム共有、統合管理プラットフォームを組み合わせることで、保護と総所有コスト (TCO) の両方に大きな影響を与えることができます。

Sophos Intercept X エンドポイントと Sophos Firewall を実行している顧客は、ソフォスのシステムがなければ、**同じレベルの保護を維持するのにセキュリティの人員を 2倍にする必要がある**としており、また、セキュリティインシデントの件数が最大 85% 減少したとも報告しています。

CUSTOMER CASE STUDY **HEALTHCARE PROVIDER, U.S.**

A regional healthcare provider whose services include inpatient and outpatient care, medical practices, nursing homes, and a range of specialist services.



Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT security resource requirements
The customer has three employees dedicated to cybersecurity. They calculate they would, if they didn't use Sophos, need to employ three additional full-time security analysts solely to cover incident response.

90%-plus reduction in day-to-day cybersecurity workload
Prior to Sophos, reviewing logs and investigating areas of concern would take an entire day. Now they achieve the same level of confidence in just 30 minutes.

85% reduction in security incidents
Previously, they experienced three incidents each day on average. This has now dropped to an average of one every three days.

90%-plus reduction in time to investigate an incident
Before using Sophos, it took the team roughly three hours to thoroughly investigate an incident. This has now dropped to less than 15 minutes, with everything done remotely via the Sophos Central platform and without disrupting other users and impacting system availability.

CUSTOMER-AT-A-GLANCE

Number of users
4,500 employees

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Intercept X for Server Protection (Windows, Linux, and virtual machines)

CUSTOMER CASE STUDY **CLINICAL TRIALS PROVIDER, U.S.**

A private sector organization that provides the clinical trial data needed to secure regulatory approval for new medications.

Business impact of a Sophos cybersecurity ecosystem

50% reduction in IT resource requirements
Currently, the customer spends one hour a day reviewing logs and investigating issues. They advise that they would need to hire one or two more security engineers just to manage the logs if they moved away from Sophos.

33% reduction in time to deal with a potential issue
Previously, to address a security issue with a device, they would reimage the machine, which took between 90 minutes and two hours. With Sophos, they can conduct a full investigation and remediate in approximately one hour – with no reimaging.

88% reduction in threat risk due to faster issue identification
Prior to using Sophos, it took a full day just to investigate the logs to find the issues. With Sophos, the IT team can identify new issues for investigation within minutes of a suspicious event arriving.

Improved user behavior
As users are aware that the IT team can now address issues quickly and without impacting work, they are far more willing to report issues or concerns.

CUSTOMER-AT-A-GLANCE

Number of users
150 employees across four locations

IT team
Two IT staff, covering all areas including cybersecurity

Sophos solutions
- Sophos XG Firewall
- Sophos Intercept X Advanced with EDR
- Sophos Device Encryption

多忙な医療従事者にセキュリティの安全を提供する

大きなプレッシャーがかかる医療機関の環境では、人為的ミスによるリスクを排除・制御することは常に困難なことです。ソフォスは重要なセーフティーネットを提供するため、ユーザーは心配することなく迅速に作業を進めることができます。

脅威がユーザーに到達することを阻止

脅威がユーザーに到達することを最初から阻止することで、ユーザーへの負担、ひいては IT チームへの負担を軽減することができます。

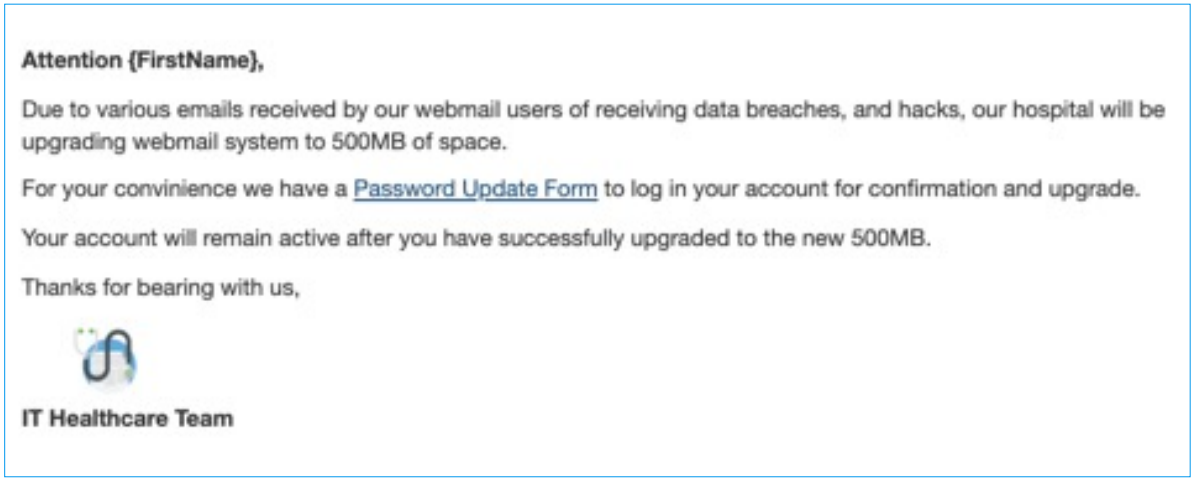
Intercept X with EDR は、ランサムウェア対策、エクスプロイト対策、および AI 搭載の検出機能を組み合わせて、攻撃チェーンのいたるところで脅威を阻止します。ユーザーは、世界最高レベルのエンドポイント保護によって支えられているので、安心して作業を行うことができます。

Sophos Email は、AI 搭載の予測型セキュリティをユーザーの受信トレイに直接配備します。ユーザーが疑わしいリンクをクリックする前に、悪意のあるメールを識別して自動的に削除します。

ソフォスのサイバー セキュリティ エコシステムにより、ソフォス製品は連係して脅威に自動的に対応し、わずか数秒で脅威を阻止してクリーンアップすることができます。

ユーザーが脅威を検出できるようにするトレーニングの実施

Sophos Phish Threat は、フィッシングメールのシミュレーションやオンライントレーニングを通じて、悪意のあるメールを見分けられるようにユーザーを訓練します。ユーザーの職種またはシミュレーションテストの結果のいずれかを基にして、最もトレーニングを必要とするユーザーに対して実施することもできます。



Attention {FirstName},

Due to various emails received by our webmail users of receiving data breaches, and hacks, our hospital will be upgrading webmail system to 500MB of space.

For your convinience we have a Password Update Form to log in your account for confirmation and upgrade.

Your account will remain active after you have successfully upgraded to the new 500MB.

Thanks for bearing with us,

IT Healthcare Team

Sophos Phish Threat のフィッシングシミュレーションのメールのサンプル

医療機関の作業のパフォーマンスを低下させないセキュリティを実装する

医療機関では、他の大半の業界と比較しても、すべての作業が順調に滞りなく進むことは重要です。このため、医療機関のユーザーの多くは、作業を簡素化するために、承認されていないアプリをインストールしています。これによって、ネットワークとデータは高リスクにさらされます。ソフォスは、日々の業務を中断させることなく、シャドー IT に対処することを支援します。

すべてが滞りなく進むようにする高度な保護機能

Intercept X with EDR は、エンドポイントとサーバーを保護し、脅威を阻止して、ユーザーの作業が中断されないようにします。EDR 機能を使用すると、ユーザーのデバイスをリモートでクエリして、必要に応じてマシンを修復できます。

Sophos Firewall は、ネットワークを脅威から保護し、信頼できるネットワークトラフィックの優先的な処理を簡単に設定できます。これにより、重要なプロセスは中断なしで継続されます。さらに、シャドー IT を可視化して制御できるため、組織を危険にさらす可能性のあるアクティビティを特定して停止できます。

ソフォスの製品群は、単体でも優れた製品ですが、互いに連係させることでより高い効果を発揮します。先に説明したように、Sophos Intercept X と Sophos Firewall は連係して、脅威に自動的に対応し、可視性を高めます。

レガシーテクノロジーのセキュリティ保護

多くの医療機関が抱える課題は、レガシー機器を保護する必要性です。このようなデバイスは、規制上の問題が原因で更新できないが、ネットワークに接続する必要がある、古くなった OS を稼働していることがよくあります。デバイスにパッチを適用 / アップグレードできず、それに対応するウイルス対策やマルウェア対策ソリューションがない場合は、物理的なソリューションを検討する必要があります。

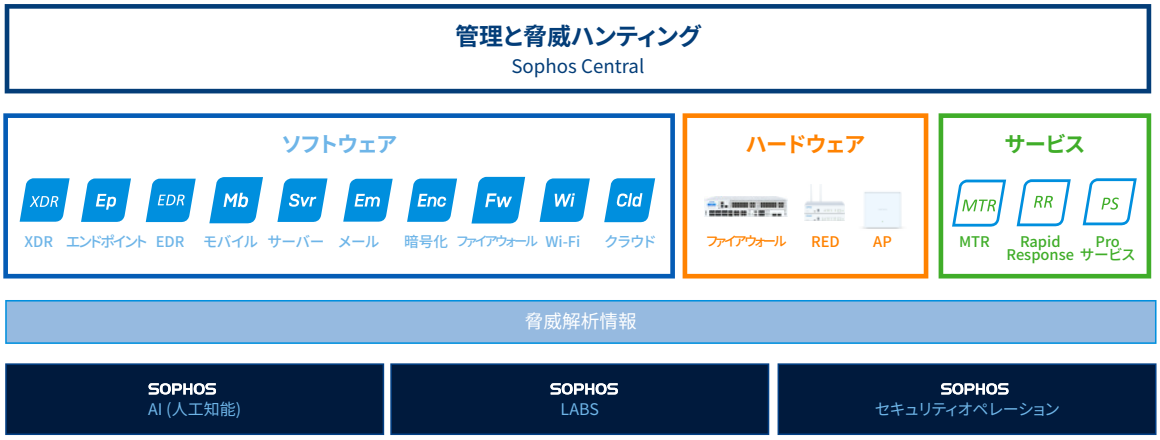
このような場合、**Sophos Firewall** および **SD-RED** (Remote Ethernet Device) が役立ちます。公開されているデバイスの前に SD-RED を配置することで、すべてのトラフィックを保護を提供する Sophos Firewall にトンネリングして、スキャンできます。非常にフラットな構成のネットワークの場合は、IP アドレススキームおよびスイッチトポロジに若干の変更を加える必要があると考えられます。ソフォスの技術担当者は、顧客のそれぞれの状況について相談を受け、その方法をアドバイスすることができます。

レガシー機器の保護

結論

医療機関の IT 環境と、保管されている機密データを保護するには、多層構造のセキュリティが必要です。ネットワークからデータまで、すべての脆弱なポイントにインテリジェントなセキュリティを実装することで、システム、スタッフ、患者を内部および外部のリスクから保護できます。

すべてのソフォスソリューションは、ソフォスの適応型サイバーセキュリティエコシステムの一部です。単体でも優れた製品で、多くの組織は 1つの製品からはじめますが、組み合わせることによってさらに優れた能力を発揮します。ソフォスによって提供される保護が拡大するにつれて、情報の共有、単一のコンソールでの一元管理、自動対応、深い洞察など、統合エコシステムによって追加されるメリットも拡大します。これらすべてが連係することで、保護がさらに強化される一方、顧客の IT チームの効率性も高まります。



ヘルスケア業界の保護：ソフォスのサイバーセキュリティエコシステム

ソフォスが医療機関をどのように保護しているかの詳細、およびお客様の要件についてのご相談は、ソフォス営業部にお問い合わせいただくか、ソフォスのセキュリティ専門家からのコールバックをリクエストしてください。

ソフォスのセキュリティ専門家からのコールバックを
今すぐお申し込みいただけます。

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。

2021-05-05 (SB-NP)

SOPHOS