SOPHOS

サイバーセキュリティの進化：ソフォスのビジネスへの影響

ソフォスのサイバーセキュリティシステムの保護や効率性を実際に導入した 5 社の顧客で数値化

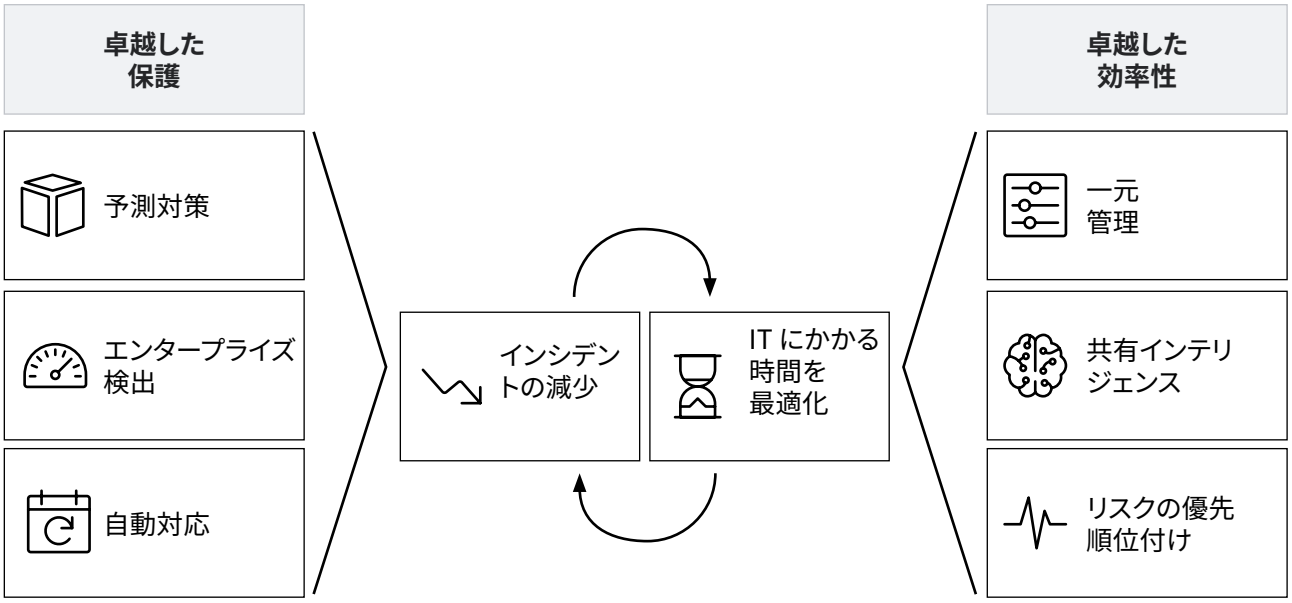
ソフォス ホワイトペーパー 2020年 6月

概要

ソフォス製品を導入すると、世界初で最高のサイバーセキュリティシステムを活用できます。

- **次世代型製品、サービスの包括的なポートフォリオ** ソフォスは、エンドポイント保護、モバイル保護、サーバー保護、EDR、次世代型ファイアウォール、メール、統合エンドポイント管理など、あらゆるサーバーセキュリティのニーズに対応します。完全なクラウド、ハイブリッド、オンプレミスのいずれの環境でも、ソフォスはお客様をサポートします。
- **卓越した保護性能** 最先端のテクノロジー、世界的に名高いデータサイエンス、脅威ハンティング、SophosLabs チームの専門知識の両方を活用できます。エンタープライズレベルの検出機能は、今日の高度な攻撃をブロックし、AI を活用したディープラーニング型ニューラルネットワークが未知の脅威を予測的に阻止します。ソフォス製品は、リアルタイムで連携して、保護をさらに強化します。脅威状況とセキュリティ情報を共有し、インシデント対応を自動化します。
- **一元的な管理プラットフォーム**クラウドベースの管理プラットフォームである Sophos Central を使用してすべてのソフォス製品を管理します。 共有された脅威インテリジェンスを使用してリスク情報を優先的に提供し、手順に従った調査によって各シナリオごとに推奨されるアクションを提供します。

ソフォスのサイバーセキュリティシステムは、**TCO (総所有コスト) を削減**しながら、**保護を強化**します。 比類のない保護と素晴らしい効率性が継続的に相互に強化し合う相乗効果を作り出すことで、これを行います。



この相乗効果により、IT 部門の効率性が大幅に向上し、従業員を増員することなく脅威にさらされる可能性を減らすことができます。

お客様への効果

ソフォスのサイバーセキュリティシステムが実際の顧客環境に与える影響を測定するために、当社は北米、ヨーロッパ、アジアにいるソフォスの顧客 5 社にインタービューしました。顧客のシナリオはそれぞれ異なり、組織構造、課題、ビジネス要件もさまざまでした。しかし、ある主要な調査結果ではすべてにおいて共通していました。

顧客は、もしソフォスの次世代型サイバーセキュリティ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**にする必要があったと述べています。

また、セキュリティインシデントの発生回数が減り、発生した問題をより迅速に特定して対応できるとのことでした。ソフォス製品を使用した結果は次のとおりです。

- IT セキュリティの人員にかかる諸経費を 50% 削減
- 日常的なサイバーセキュリティ管理に費やす時間を 90% 以上削減
- 問題を特定する時間を 90% 以上短縮
- セキュリティインシデントの数を 85% 削減
- 組織全体のダウンタイムを大幅に削減

顧客 A：医療プロバイダー (米国)

- 従業員数 4,500人
- 80 名の IT スタッフのうち 3 名はサイバーセキュリティに特化
- ソフォス製品：Intercept X Advanced with EDR、XG Firewall、Intercept X for Server Protection (Windows、Linux、および 仮想マシン)

顧客 A は、入院患者と外来患者のケア、医療、介護施設、幅広い専門サービスを含む地域の医療プロバイダーです。

ビジネスへの効果

- **IT セキュリティの人材を 50% 削減**
  顧客は現在サイバーセキュリティに特化した人材を 3 名雇用しています。もしソフォス製品を使用していない場合には、インシデントの対応をカバーするためだけに、3 名のフルタイムのセキュリティアナリストを追加で雇う必要があることが分かりました。

  ソフォス製品を使用する以前は、IT 部門はネットワーク上で何が起こっているかを特定するために多くの手作業を行う必要があり、ほとんどの時間をインシデントの特定に費やしていました。今では、ソフォスが問題を事前に特定し、95% のケースで状況を自動的に解決します。その結果、チームは人間の関与を必要とする 5% の問題の対応に集中することができます。

日常のセキュリティ管理が90%以上削減

IT セキュリティマネージャーは、毎日 30 分かけてログを確認し、何か問題がないかを調査します。ソフォス製品を使用する以前は、同じレベルの情報と確実性を得るのに丸一日かかっていました。ソフォス製品を使用すると、すべてのデータが単一の管理プラットフォームに統合され、一貫性のある形式で表示されるため、問題の特化と対応が容易になります。これにより、複数のソース間でデータをマッピングして、疑わしいデータ、悪意のあるデータ、無害なデータを特定するという、日常的な煩わしい作業が排除されます。

セキュリティインシデントを 85% 削減

病院は、個人を特定できる大量の PII (Personally Identifiable Information) や支払い情報を保持しているため、サイバー犯罪者の標的になっています。ソフォス製品を使用する前は、さらなる調査を必要とするインシデントが 1 日平均 3 件発生していました。ソフォス製品を使用することで、3 日間で平均 1 件へと減少しています。

インシデントの調査時間を90%以上短縮

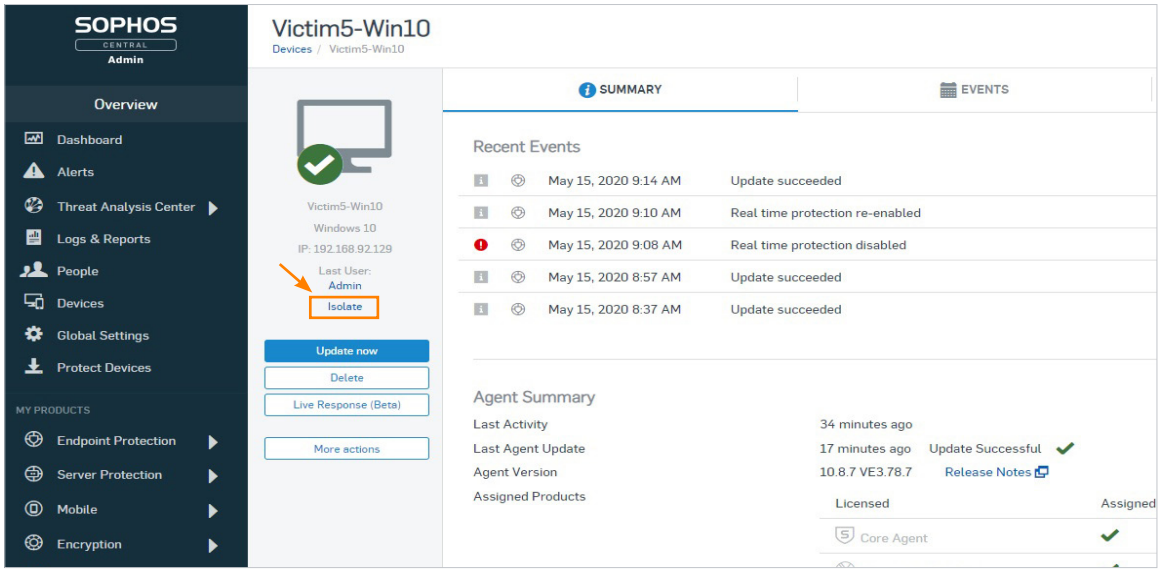
ソフォス使用前は、1 件のインシデントを徹底的に調査するのに約 3 時間かかりました。これには、影響を受けたコンピューターにローカルアクセスすることも含まれます。今では、Sophos Central プラットフォームを介してすべてがリモートで行われるため、最大 15 分です。

以前は、チームはネットワークアダプターを無効にしてから物理的にデバイスへアクセスし、問題を調査、解決してから、手動で再接続する必要がありました。また、ユーザーのワークフローに合わせる必要がありました。たとえば、医師が患者の治療を行わなくなるまで待ってから、そのシステムにアクセスして修復を行っていました。Sophos Central コンソールを介してデバイスを隔離する機能により、ユーザーおよびシステムの可用性に影響を与えることなく、リモートで問題を調査できます。

調査時間の短縮とすべてリモートで管理する機能により、病院内の他のユーザーへの影響も大幅に減少します。

調査中も継続的な保護

以前は、手動で調査していたためにデバイスがネットワークから削除され、オフラインの間は保護を更新することはできませんでした。ソフォス製品を使用すると、IT 部門が問題を調査するためにデバイスを隔離しても、オンラインのままであり、保護の更新を継続して受信します。



顧客 B：教育サービスプロバイダー (インド)

- 従業員数 700人
- バンガロールの本社と、インドおよび東南アジアの広範な地域の現地マネージャー
- ソフォス製品：Intercept X Advanced with EDR、Intercept X Advanced for Server、XG Firewall

顧客 B は、インドおよび東南アジアの広範な地域のカレッジや大学に教育サービスを提供しています。バンガロールの本社に拠点を置く一元化された IT チームと現地のローカル IT マネージャーチームにより、数万人の学生を保護しています。

ビジネスへの効果

- **日々のセキュリティ管理に必要な人材を 50% 削減**
  以前は、4 人のエンジニアを雇って日々のセキュリティを管理していました。ソフォスに移行して以来は、会社全体のセキュリティをカバーするのに必要なエンジニアは 2 人だけです。
- **調査が必要なリスクの高い領域を特定するための時間を 94% 削減**
  ソフォス製品を使用前は、さらに詳細な調査を必要とする重大な問題を特定するのに 3〜4 時間かかりました。今では、Sophos Central で組織全体のセキュリティの優先順位を特定するのにわずか 10〜15 分しかかかりません。
- **ネットワークの不正トラフィックのソースを特定するための時間を 98% 削減**
  以前のネットワークセキュリティの実装では、ネットワーク上のどのデバイスがパフォーマンスやセキュリティの問題に影響を及ぼしているか特定するのに 2 日 (場合によってはそれ以上) かかりました。今では、問題を特定して対処するまでにかかる時間はわずか 15 分です。
- **ファームウェアのアップデートの管理にかかる時間を 95% 削減**
  以前のネットワークセキュリティ実装では、各ソフトウェアのアップデートに 3〜4 時間かかっていたため、可用性やリスクの問題も発生しました。ソフォス製品を使用する現在では、アップデートにかかる時間はわずか 10 分です。年間 20〜25 回のアップデートでは、これにより、年間 75 時間節約できます (2 週間の業務時間に相当)

顧客 C：臨床試験プロバイダー (米国)

- 4 ヶ所で従業員 150 人
- サイバーセキュリティを含むすべての領域をカバーする 2 名の IT スタッフ
- ソフォス製品：Intercept X Advanced with EDR、XG Firewall、Central Device Encryption

顧客 C は、新薬の規制当局による承認を得るために必要な臨床試験データを提供する民間セクターの組織です。ビジネスの性質上、機密性の高い個人情報を大量に保持しています。

ビジネスへの効果

- **IT の人材を 50% 削減**
  こちらの顧客は、ITのすべてを管理するために、わずか 2 人の少人数チームを擁するだけです。現在では、1 日 1 時間かけてログを確認し、何か問題がないかを調査します。もしソフォス製品を使用していなかったら、ログを管理するためだけにさらに 1 人か 2 人のセキュリティエンジニアを雇う必要があったでしょう。

- **潜在的な問題に対処するための時間を 33% 削減**
  以前は、デバイスでセキュリティの問題が発生した場合の解決策は、マシンを再イメージングすることで、これには 90 分から 2 時間かかっていました。現在では、システムの隔離や徹底的な脅威ハンティングから完全なセキュリティのスキャンや最終的な修正まで再イメージングせずに約 1 時間で詳細な調査を行うことができます。ソフォスのアプローチで実現しているもう 1 つの利点は、調査の終了後すぐにユーザーの生産性が向上することです。一方、再イメージングではマシンの設定やカスタマイズをリセットする時間も失われていました。

- **問題をより迅速に特定できるため、脅威リスクが 88% 減少**
  ソフォスのサイバーセキュリティシステムを使用すると、IT 部門は疑わしいイベントが発生してから数分以内に調査が必要な新しい問題を特定できます。ソフォス製品を使用前は、ログを調べて調査が必要な問題を見つけるのに丸一日かかっていました。この対応時間が短縮されることで、脅威にさらされる可能性が大幅に減少します。

- **ユーザーの行動の改善**
  ソフォス製品を使用することで、IT チームがダウンタイムや余分な作業を発生させることなく、問題やインシデントに迅速に対応できることを今ではユーザーは理解しています。その結果、ユーザーは問題や懸念事項 (例えば、メール内の潜在的に悪意のあるリンクをクリックしたなど) を進んでレポートするようになったと IT 部門は報告しています。

顧客 D：公共サービスプロバイダー (セルビア)

- 従業員数 300人
- 10 名の IT スタッフのうち 4 名はサイバーセキュリティに特化
- ソフォス製品：Intercept X Advanced、Intercept X Advanced for Server、XG Firewall、Sophos Email、Sophos Mobile

顧客 D はセルビアの首都ベオグラードを担当するパブリックセクターの組織です。このソフォスの長期的な顧客は、Sophos Central で管理される次世代型製品に移行しました。

ビジネスへの効果

- **日々のセキュリティ管理に費やす時間を 50% 削減**
  現在は、セキュリティ管理に 1 日 30 分を費やしており、Sophos Central の管理コンソールでアラート、ログ、ユーザー、デバイス、トラフィック、アプリケーションをチェックして、すべてが正常であることを確認しています。 これまでは、この日々のセキュリティ管理は優先度の高い問題を特定して対処方法を決定するために、少なくとも 2 倍の時間がかかっていました。

- **他のベンダーと比較して、日常のセキュリティ管理に費やす時間を 90% 以上削減**
  日々のセキュリティ管理は、ソフォス製品を使用すると 30 分であるのに対し、他のベンダーを使用した場合は、これまでの経験に基づくと丸一日かかると顧客は見積もっています。

- **重大なセキュリティインシデントはゼロ**
  顧客はソフォスを長年使用しておりますが、過去 8〜10 年間、重大なセキュリティ問題は発生していません。これは、脅威を受けていないと言っているのではありません。むしろ、ソフォス製品はユーザーに気づかないうちにバックグラウンドで迅速かつ静かに問題を解決します。

顧客 E：規制当局承認機関 (スロベニア)

- 従業員 150 人のうち、3 分の 1 はリモートで、3 分の 2 は本社で勤務
- サイバーセキュリティを含むすべての分野をカバーする 2 人の IT スタッフと、主要なプロジェクトに対する外部プロバイダのサポート
- ソフォス製品：Sophos Endpoint Protection、Intercept X Advanced for Server、XG Firewall、Sophos Mobile、Sophos Device Encryption

顧客 E は、製品が必要な基準を満たすことを保障する責任を負うパブリックセクターです。
このソフォスの長期的な顧客は、Sophos Central で管理される次世代型製品に移行しました。

ビジネスへの効果

- **日々のセキュリティ管理に費やす時間を 50% 削減**
  ファイアウォールのチェック、アラートの確認、隔離メールのクリーンアップなどのセキュリティ管理に毎日 15～30分費やしています。以前は、少なくともその 2 倍の時間を費やしていました。この効率性の向上は、1 か所ですべてのセキュリティ製品を管理できるため、アプリケーションとサーバーを切り替えるする必要がないからです。
- **重大なセキュリティインシデントはゼロ**
  ソフォス製品を使用して以来、顧客は重大なセキュリティインシデントを一度も経験していません。

結論

お客様の証言が示すように、ソフォスのサイバーセキュリティ対するアプローチは、真の保護と効率性をもたらします。IT 部門の効率性が大幅に向上し、人材を増員することなく脅威にさらされる可能性を減らすことができます。

お客様のビジネス環境、リソース、課題は組織によって異なりますが、ソフォスのサイバーセキュリティシステムを実行することで、IT セキュリティのワークロードが常に 50% 削減すると報告されています。お客様は、日々のサイバーセキュリティ管理に費やす時間を 90% 以上削減し、セキュリティインシデントの数を 85% 削減できることに満足しています。

ソフォスのサイバーセキュリティソリューションの詳細については、www.sophos.com にアクセスするか、ソフォスの営業担当へお問合せください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

200612 WPEN (NP)

SOPHOS