SOPHOS
Cybersecurity delivered.

# 主要なランサムウェアの制御とソフォスのサポート

ランサムウェアの課題は引き続き拡大しています。ランサムウェアの被害を受けた組織の割合は、12か月でほぼ倍増し、2020年の 37% から 2021年では 66% へとなりました。また、攻撃者はデータの暗号化でも成功率を高めており、2021年は 65% の攻撃でデータの暗号化を成功させています*。

ランサムウェアを阻止するには、熟練した攻撃者が実行する高度なハンズオンキーボード攻撃と、攻撃を展開するのに必要なスキルレベルを下げることでランサムウェアの到達範囲を大幅に拡大するランサムウェア・アズ・ア・サービスモデルの成功の両方を阻止するための取り組みが必要です。

このガイドでは、ランサムウェアの露出と影響を最小限に抑えるトップクラスのサイバーセキュリティ制御、およびソフォスがどのようにサポートするかを詳しく説明します。

## 主要なランサムウェアの制御とソフォスのサポート

| サイバー制御 | ソフォスを活用した対策 | 詳細 |
|---|---|---|
| ランサムウェアが展開される前に、人間主導の攻撃を検出、無効化するためのプロアクティブな脅威ハンティング | Sophos XDR (Extended Detection and Response) | 組織の環境全体において、脅威ハンティングと脅威の無効化を実行できるようにします。エンドポイント、サーバー、クラウドワークロード、ファイアウォール、メール、パブリッククラウド環境、モバイル、Microsoft 365などから検出できます。 |
| | Sophos MTR (Managed Threat Response) | フルマネージド型サービスとして専門家チームが脅威ハンティング、検出、対応を年中無休で提供します。Microsoft 365を含むさまざまなセキュリティや IT ソリューションとのコネクタにより、お客様の環境全体に可視性を拡大し、攻撃に対する防御能力を向上させます。 |
| ランサムウェア脅威が展開される前に自動的にブロック | Sophos Endpoint および Sophos Workload Protection | 次のような攻撃チェーン全体を破壊する高度なランサムウェア保護機能を提供します。<br>› 既知と未知の両方のランサムウェアを防ぐ AI ベースのディープラーニング<br>› マルウェアの拡散や、認証情報の窃取、検出の摺り抜けなどに使用されるエクスプロイトやテクニックをブロックするエクスプロイト保護<br>› 攻撃者が攻撃を開始する際に使用する可能性のあるクラウドワークロード上でアプリケーションが実行されるのを阻止するアプリケーションコントロール<br>› クラウドワークロードの既知で良好な構成を取得し、その状態をロックして不正なプログラムの実行を防止するサーバーロックダウン<br>› 不正な暗号化を検出してロールバックし、ネットワーク全体に拡散される前にプロセスをシャットダウンするランサムウェア対策テクノロジー。ファイルベース型およびマスターブートレコード型の両方のランサムウェア攻撃を防ぎます。 |
| | Sophos Email | 自動的にすべてのファイルプロセス、ファイルアクティビティ、レジストリアクティビティ、ネットワーク接続を分析して、ランサムウェア、その他の形態のマルウェアをブロックします。高度なフィッシング対策、URL スキャン、配信後の保護により、安全な送信者のみが受信箱に到達します。配信されたメッセージの脅威状態が変化した場合は、自動的に削除されます。 |
| | Sophos Firewall | ファイルダウンロードにおいて広範な機械学習とサンドボックス検査を使用して侵害されたサイトや悪意のあるダウンロードから保護し、これまでに見られなかった未知のランサムウェア攻撃さえも特定します。 |

## 主要なランサムウェアの制御とソフォスのサポート

| サイバー制御 | ソフォスを活用した対策 | 詳細 |
|---|---|---|
| パッチが適用されていないデバイス、保護されていないマシンなど、環境を強化するためのセキュリティギャップを特定して埋めます | Sophos XDR (Extended Detection and Response) | 古くてサポートされなくなったソフトウェアやシステムを特定します。デバイス上のすべてのアプリケーション、バージョン情報、SHA256 ファイルハッシュ、パッチ情報、およびアプリケーションの実行履歴、ネットワーク接続、親 / 子プロセスなどを含むログへのアクセスを提供します。インストールされたアプリケーションをオンラインの脆弱性情報と照合するクエリや、レジストリ設定におけるセキュリティ態勢の弱点を特定するクエリも含まれています。 |
| | Sophos ZTNA | システムやアプリケーションへの安全で細やかな制限のリモートアクセスを可能にし、攻撃対象領域と攻撃が横方向に移動する可能性を排除します。 |
| リモートデスクトッププロトコルをロックダウンすることで、攻撃者がそれを利用してアクセスできないようにします | Sophos Firewall | IT チームが RDP を簡単に管理し、ロックダウンできるようにします。 |
| | Sophos ZTNA | システムを攻撃にさらすことなく、RDP およびその他のアプリケーションへの安全なリモートアクセスを可能にします。 |
| | Sophos Cloud Optix | パブリッククラウドのセキュリティベンチマーク評価により、公開されている RDP ポートをプロアクティブに特定します。ガイド付き修正機能では、管理者にセキュリティの設定ミスに対処する方法を説明します。 |
| | Sophos XDR (Extended Detection and Response) | RDP 接続を検出し、アクティビティをログに記録します。リモートターミナルでは、管理者が RDP ポリシーの有効 / 無効を設定できます。すべての管理対象デバイスの RDP ポリシーを可視化し、それに対する変更を検出します。 |
| 攻撃が発生した場合の影響を最小限に抑えるためのサイバーインシデント対応計画 | Sophos Rapid Response | ソフォスの専門家による、24時間年中無休の迅速なインシデントレスポンスを提供します。 |
| | Sophos MTR (Managed Threat Response) | フルマネージド型サービスとして専門家チームが脅威ハンティング、検出、対応を年中無休で提供します。 |
| サイバーセキュリティの意識向上トレーニングおよびフィッシングテスト | Sophos Phish Threat | フィッシング攻撃のシミュレーション、自動化されたセキュリティの意識向上トレーニング、包括的なレポートにより、セキュリティの意識を向上させ、ユーザーを教育します。<br><br>Sophos Email との統合により、セキュリティチームは、リスクプロファイルが原因で Web サイトへのアクセスを警告またはブロックされたユーザーのトレーニングを効率的に特定し、迅速に追跡することができます。 |

## 主要なランサムウェアの制御とソフォスのサポート

| サイバー制御 | ソフォスを活用した対策 | 詳細 |
|---|---|---|
| 攻撃者による悪用を防ぐためのクラウド環境の脆弱性の特定と軽減 | Sophos Cloud Optix | Amazon Inspector との統合により、インターネットに公開されている仮想マシンのポート、有効になっているリモート root ログイン、インストールされた脆弱なソフトウェアバージョンなどをパブリッククラウド環境内のセキュリティの脆弱性、過剰な権限を付与された IAM ロール、ネットワークアクセスの構成ミスを積極的に特定し、緩和することができます。AWS Systems Manager との連携により、Amazon 仮想マシンのパッチステータスを受信します。<br><br>Azure、AWS、Docker Hub 全体のコンテナレジストリを分析して OS の脆弱性を検出する一方、Infrastructure as Code スキャンにより、セキュリティスキャンを CI/CD パイプラインに拡張します。 |

お客様のサイバーレジリエンスの質問とソフォスがランサムウェアの防御をどのように強化するかについては、ソフォスの営業担当者へご相談ください。

* ランサムウェアの現状 2022年版、ソフォス、31 か国の IT プロフェッショナル 5,600 人を対象に調査

ランサムウェアの詳細と、ソフォス製品がお客様の企業の防御にどのように役立つかをご覧ください。

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。

© Copyright 2022.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。

2022-04-08 (SB-NP)

SOPHOS