医療業界向けのリファレンスカード

医療業界におけるサイバー攻撃は、医療システムや医療データの利用を妨げるだけでなく、患者の健康や安全に危害をもたらす恐れもあり、深刻な問題となっています。医療業界は、金銭を目的とした攻撃者にとって格好のターゲットとなっており、不正入手された患者情報はダークウェブで取引され、保険などの詐欺に利用されます。

医療機関のサイバーセキュリティ要件を満たし、医療業務の中断を防ぐために、ソフォスのソリューションがどのように役立つかを以下にまとめました。参考資料としてご活用ください。

課題	ソフォスのソリューション	ソフォス製品がどのように役立つか
ePHI の守秘	Sophos Firewall	主要なシステム領域にアクセスするためのディレクトリサービスなど、柔軟な多要素認証オプションをサポートします。
	Sophos Central Device Encryption	Windows および macOS 用のフルディスク暗号化でデバイスとデータを保護。デバイスの暗号化状態を確認し、コンプライアンスを実証します。
	Sophos Switch	ネットワークに接続するために LDAP、MAC アドレス、またはその他の認証方法を使用してユーザーを認証できるようにネットワークアクセス制御を許可します。これにより、認証されていないユーザーやデバイスが LAN にアクセスするのを防ぎます。
	Sophos Managed Detection and Response (MDR)	24時間 365日環境を監視するだけではなく、悪意のあるアクティビティの調査と無力化により、攻撃者の活動によるデータ損失を防ぎます。
	Sophos Email	シームレスな暗号化の統合でグループや個人ユーザーに複数のルールポリシーなどのデータ侵害保護ポリシーをきめ細やかに制御ソフォス コンテンツ コントロール リスト (CCL) を使って独自の CCL を作成したり、特定の CCL 用に事前設定済みのテンプレートをカスタマイズしたりできます。ポリシーに一致したメールの処理は、ブロック、添付ファイルの破棄、隔離、ログして続行など、豊富なオプションから選べます。
	Sophos Mobile	豊富なデバイス管理機能で、モバイルデバイス上の機密情報を含む業務メールや文書ファイルを保護。個人所有のデバイス (BYOD) も同様に保護します。 デバイスの正常性を監視したり、必要な設定からの逸脱した場合にフラグを立てる柔軟なコンプライアンスルールを提供しています。
	Sophos ZTNA	アプリケーションやデータへのアクセスを許可する前に、ユーザー ID、デバイスのセキュリティ状態、コンプライアンスを継続的に検証します。
	Sophos Wireless	Wi-Fi セッションを作成して動的に暗号化。ソフォスが管理するネットワークおよびホットスポット上で、転送中の情報を保護します。
	Sophos Cloud Optix	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 では、パブリッククラウド環境全体で最小権限の原則を採用しています。 この SaaS 型サービスでは、ソフォスの AI を使用して異なるアクションを関連付けて、クラウドプロバイダーコンソールの異常なアクセスパターンや場所を、ほぼリアルタイムで検出し、認証情報の悪用や窃取を特定します。 IAM 視覚化ツールによって IAM の関係性を完全にマッピングし、過剰なアクセス権限をすばやく簡単に特定して、過不足ない IAM ポリシーを作成できるようにします。これにより、サイバー攻撃者による権限の悪用を防げます。

SOPHOS

課題	ソフォスのソリューション	ソフォス製品がどのように役立つか
マルウェアからの保護	Sophos Firewall	ソフォスの業界をリードする機械学習テクノロジー (SophosLabs Intelix を搭載) を活用して、最新のランサムウェアや未知の脅威がネットワークに侵入する前に即座に特定します。 最新のドライブバイ攻撃や標的型 Web マルウェアを阻止する高度な保護機能のほか、URL や悪質サイトのフィルタリング、Web アプリケーションフィルタリングを搭載しています。また、クラウドベースのフィルタリングによって、オフサイトの保護にも対応します。
	Sophos Sandboxing	ファイルがユーザーのデバイスに配信される前に、実行ファイルや実行可能なコンテンツを含むドキュメントを検査してブロックすることで、ソフォスの Web/メールセキュリティ製品、および Sophos Firewall を補完します。
	Sophos Intercept X for Mobile	Android デバイスにインストールされている、悪質なアプリケーションおよび不要と思われるアプリケーションを検出します。検出には、Intercept X のディープラーニングと、グローバルに展開する SophosLabs 解析チームの解析情報が組み合わせて使用されます。管理者は、Microsoft Intune と統合することで、脅威の検出時にアプリケーションおよびデータへのアクセスを制限する、条件付きのアクセスポリシーを作成できます。
	Sophos Intercept X Sophos Intercept X for Server	HIPS、ディープラーニング、エクスプロイト対策、攻撃者対策、および悪意のあるトラフィックの検出を組み合わせて、ホストで発生している悪意のある動作をプロアクティブに検出します。エクスプロイト防止機能により、攻撃者がアプリケーションや OS の脆弱性を悪用することを防ぎます。アプリケーションコントロールのポリシーによって、未承認のアプリケーションの使用を制限します。
	Sophos Intercept X for Server	サーバーシステム上の既知の安全なアプリケーションを自動スキャンし、それらのアプリケーションのみをホワイトリストに登録することで、未承認のアプリケーションが実行されるのをブロックします。
	Sophos Cloud Optix	設定に加えられる変更を継続的に監視・検出し、リソースの構成において誤って、もしくは悪意的な変更の防止、検出、自動的に修正します。
	Sophos Managed Detection and Response (MDR)	Sophos MDR は、ネットワーク、メール、モバイル、ID、エンドポイントなどを含むセキュリティ環境全体から信号を継続的に監視し、潜在的なサイバーセキュリティイベントを迅速かつ正確に検出できるようにします。異常な動作とコードの使用を検出、調査、関連付けて、悪意のあるアクティビティを特定し、イベントを迅速に無力化することができます。
リモートアクセスの保護	Sophos Firewall	VPN 接続に 2要素認証を適用。RADIUS/TACACS を統合してきめ細かな制御を行えます。Sophos SD-RED によって、専用のセキュア VPN トンネルを確立し、安全なネットワークをリモートロケーションに拡張できます。
	Sophos ZTNA	アプリケーションやデータへのアクセスを許可する前に、ユーザー ID、デバイスのセキュリティ状態、コンプライアンスを継続的に検証します。
	Sophos Mobile	豊富なデバイス管理機能で、モバイルデバイス上の機密情報を含む業務メールや文書ファイルを保護。個人所有のデバイス (BYOD) も同様に保護します。 デバイスの正常性を監視したり、必要な設定からの逸脱した場合にフラグを立てる柔軟なコンプライアンスルールを提供しています。
	Sophos Wireless	ワイヤレスネットワークに接続しているデバイスの正常性ステータスを監視し、それに基づいて動作します。不健全で準拠していないエンドポイントやモバイルデバイスの Wi-Fi ネットワークアクセスを自動的に制限し、感染が拡散するのを防ぎます。
	Sophos Cloud Optix	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 では、パブリッククラウド環境全体で最小権限の原則を採用しています。 この SaaS 型サービスでは、ソフォスの AI を使用して異なるアクションを関連付けて、クラウドプロバイダーコンソールの異常なアクセスパターンや場所を、ほぼリアルタイムで検出し、認証情報の悪用や窃取を特定します。 IAM 視覚化ツールによって IAM の関係性を完全にマッピングし、過剰なアクセス権限をすばやく簡単に特定して、過不足ない IAM ポリシーを作成できるようにします。これにより、サイバー攻撃者による権限の悪用を防げます。

課題	ソフォスのソリューション	ソフォス製品がどのように役立つか
接続されている医療機器の保護	Sophos Firewall	ネットワーク上の重要な医療機器から侵入し、医療業務用のサーバーやアプリケーションへと移動しようとする攻撃を阻止します。ゾーンや VLAN を使用した、フレキシブルで強力なセグメント化機能は、ネットワークで複数の信頼レベルを設定することを可能にする一方、ネットワーク内の異なる部分への横断的な拡散に対する保護も強化します。
	Sophos Switch	ネットワークに接続するために LDAP、MAC アドレス、またはその他の認証方法を使用してユーザーを認証できるようにネットワークアクセス制御を許可します。これにより、認証されていないユーザーやデバイスが LAN にアクセスするのを防ぎます。
	Sophos Mobile	モバイルデバイスの各種管理機能や、コンテナ、業界トップクラスの暗号化機能によって、機密情報を含む業務メールや文書ファイルを保護。個人所有のデバイス (BYOD) にも対応します。最先端のマルウェア対策とランサムウェア対策によって、ユーザーおよびデバイスを悪意のあるコンテンツやアプリから守ります。
	Sophos Wireless	ワイヤレスネットワークに接続しているデバイスの正常性ステータスを監視し、それに基づいて動作します。不健全で準拠していないエンドポイントやモバイルデバイスの Wi-Fi ネットワークアクセスを自動的に制限し、感染が拡散するのを防ぎます。
	ソフォス製品の Synchronized Security 機能	テレメトリやセキュリティ状態を共有し、サーバー、エンドポイント、ファイアウォール間で連係してマルウェアの隔離、検出、修復を行い、高度な攻撃を撃退します。
ワイヤレスセキュリティの徹底	Sophos Wireless	ワイヤレスネットワークのセキュリティ状態を詳細に可視化し、医療機関内のモバイルデバイスの増加にも対応して安全に保護します。コンプライアンスに従っていない、リスクの高いエンドポイントやモバイルデバイスからの Wi-Fi ネットワークへのアクセスを自動的に制限し、感染の拡散を防ぎます。ゲストの Wi-Fi アクセスを医療スタッフのアクセスと切り離し、パスワードの毎日更新や時間限定バウチャーを使って管理します。Sophos APX モデルはすべて、医療環境での使用に適していることを示す認定を取得しており、医療機器の動作を妨げないことが保証されています。
サプライチェーンのリスクの軽減	Sophos Intercept X with XDR	AI 検知、エクスプロイト対策、振る舞い検知、ランサムウェア対策などを使用して、サードパーティサプライヤーから侵入する脅威に対し、包括的な徹底した防御を行います。さらに、強力な XDR 機能を使用すると、疑わしいアクティビティを自動的に検出し、脅威インジケータに優先順位を付け、エンドポイントとサーバー全体で潜在的な脅威をすばやく検索できます。
	Sophos Managed Detection and Response (MDR)	専門家による脅威ハンティングと修復をフルマネージドサービスとして提供します。ソフォスの専門家が、潜在的なサプライチェーンの脅威やインシデントをお客様に代わって検出、検証、修復を 24時間体制で積極的に行います。
	Sophos ZTNA	非常にきめ細かなアクセス制御により、サプライヤーがシステムにアクセスすることに依存するサプライチェーン攻撃から保護します。このクラウド配信ソリューションは、リソースへのアクセスを許可する前に、ユーザー ID、デバイスのセキュリティ状態、コンプライアンスを検証します。場所に関係なく、信頼できるパートナーからのリクエストを認証します。
クラウド内のリソースのセキュリティ保護	Sophos Cloud Native Security	環境、ワークロード、アイデンティティ全体に完全なマルチクラウドセキュリティを提供します。Windows と Linux 向けの柔軟なホストとコンテナのワークロードのセキュリティにより、クラウドインフラとデータを保護します。マルチレイヤー技術は、コンテナエスケープ、カーネルエクスプロイト、権限昇格の試みなどの脅威を特定するクラウドネイティブの動作およびエクスプロイトランタイム検出を含むランサムウェアやその他の高度な攻撃から保護します。

課題	ソフォスのソリューション	ソフォス製品がどのように役立つか
プロアクティブなセキュリティの徹底	ソフォス製品の Synchronized Security 機能	テレメトリやセキュリティ状態を共有し、サーバー、エンドポイント、ファイアウォール間で連係してマルウェアの隔離、検出、修復を行い、高度な攻撃を撃退します。
	Sophos Managed Detection and Response (MDR)	Sophos MDR は、セキュリティ環境全体から疑わしいイベントを検出して調査し、脅威と適切な対応が必要なアクティビティを特定します。エンドポイント、ネットワーク、ID、メールなどの保護製品から収集したデータを、強力な AI ツールや、脅威インテリジェンス、人間の専門知識を使って相関分析し、影響範囲および対応を特定します。
	Sophos XDR	エンドポイントや、ネットワーク、メールなどの多様なデータソースを参照し、サイバーセキュリティ対策の全体像を把握できます。必要に応じて詳細を掘り下げて確認することも可能です。各製品からのデータが Sophos Data Lake に流れ込むことで、業務上の重要な質問に迅速に回答でき、さまざまなデータソースからのイベントを相互に関連付け、さらに多くの情報に基づくアクションを実行できます。
	Sophos Cloud Optix	ソフォスの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、セキュリティポスチャをプロアクティブに改善し、安全でない設定や脆弱性を検出できます。Cloud Optix は、セキュリティとコンプライアンス基準を環境に自動的にマッピングすることで、セキュリティ体制を 24時間年順無休で監視および維持するために必要な可視性を提供します。
フィッシング攻撃対策	Sophos Email	SPF、DKIM、DMARC 認証技術やメールヘッダーの異常解析を使用して、有名企業のなりすましや偽装の試みなどフィッシングの主な痕跡についてすべての受信メッセージをスキャンします。これにより、フィッシングメールがユーザーに届く前に、それを検出してブロックします。
	Sophos Phish Threat	自動化可能な攻撃シミュレーション、効果的なセキュリティ意識向上トレーニング、トレーニング結果の分析を通じて、フィッシング、認証情報の収集、標的型メール攻撃に対してエンドユーザーにトレーニングやテストを実施します。
	Sophos Intercept X	Windows、Mac、Linux、仮想マシンなど、すべてのエンドポイントを完全に保護し、認証情報の盗難防止、エクスプロイト対策、ランサムウェア対策、タンパープロテクションなどの多層防御のテクノロジーにより、防御を最適化します。
規制要件の順守	Sophos Cloud Optix	AWS、Azure、Google Cloud 環境全体でコンプライアンスの状態を単一のビューで確認することで、コンプライアンスギャップを解消します。FFIEC、GDPR、HIPAA、PCI DSS、SOC2 などの規格に対応するカスタムテンプレートや事前設定済みテンプレートおよび監査準備の整ったレポートを使用して、コンプライアンス状態を常に監視します。
レガシーシステムの保護	Sophos Firewall Sophos SD-RED	公開されているデバイスの前に Sophos SD-RED を配置することで、トラフィックを保護する Sophos Firewall にトンネリングして、スキャンします。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。

ソフォス株式会社営業部
Email: sales@sophos.com

© Copyright 2023.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。本書に記載されている製品や企業名はすべて、各所有者の商標または登録商標です。

2023-04-17 CC (PS)

SOPHOS