製造業向けのリファレンスカード

SOPHOS

製造業はインダストリー 4.0 時代を目の当たりにしています。産業用 IoT デバイス、ロボティクス、高度な分析を備えたスマートファクトリーは、製造業の業務に革命をもたらし、コスト削減、効率の向上、運用を容易化につながります。しかし、従来の製造技術、急速なデジタル化、IT/OTの融合、この業界の広大で複雑なサプライチェーンネットワークにより、製造業では攻撃対象領域が拡大しています。

ソフォスは、次世代のサービスと製品により、製造企業の脅威への対応時間を大幅に短縮し、企業が 1つのベンダーでセキュリティ管理を統合できるようにします。このドキュメントでは、ソフォスのソリューションが製造企業のサイバーセキュリティ要件を満たし、業務が中断されないようにする方法についての一般的なリファレンスを提供します。

セキュリティの課題	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
重要な産業用制御システムへのアクセスの保護	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 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。
	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。
知的財産（IP）を盗難から保護	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 Intercept X	既知の脆弱性を軽減し、ランサムウェア、ファイルレス攻撃、エクスプロイト、マルウェアなどの最新のサイバーセキュリティ脅威をエンドポイントデバイス全体で阻止します。DLP (情報漏洩対策) 機能は機密データを特定し、メール、アップロード、ローカルコピーによる漏洩を防ぎます。
	Sophos Firewall	Sophos Firewall with Security Heartbeat™ を使用すると、次世代型のエンドポイントおよびネットワークセキュリティが、拡張された IT エコシステム全体で疑わしいイベントに関する役立つ情報を継続的に共有し、侵害された/不正なエンドポイントデバイスを検出します。これにより、このエンドポイントを自動的かつ瞬時に隔離できるようになり、機密データの漏洩を防ぎます。
	Sophos Mobile	柔軟なコンプライアンスルールが、デバイスのセキュリティ状態を監視し、デバイスが侵害された場合に機密データへのアクセスを自動的に拒否します。 豊富なデバイス管理機能とコンテナ、業界トップクラスの暗号化機能で、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。優れたマルウェア対策とランサムウェア対策機能が、悪意のあるコンテンツやアプリから従業員とデバイスを守ります。
	Sophos ZTNA	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。
	Sophos Email	ユーザー向けに複数のルール DLP ポリシーを作成して、すべてのメールや添付ファイルの機密コンテンツを検出して機密情報を確実に保護できるようにします。また、機密データをシームレスに暗号化して、侵害を阻止します。
	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。

セキュリティの課題	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
インサイダーによる脅威からの防御	Sophos Firewall	ネットワーク内で使用される Web カテゴリ、アプリケーション、リムーバブルメディア、モバイルデバイスに対する完全なポリシー制御により、機密データを偶発的または悪意のある開示から保護します。 Sophos UTQ (User Threat Quotient) の実用的なインテリジェンスを使用して、最もリスクの高いユーザーとアプリケーションに関する洞察を提供し、セキュリティが侵害される前にポリシーを確実に適用します。 Active Directory との統合や、ファイアウォールとエンドポイント全体でシームレスなユーザー認証を促進するソフォス独自の使いやすい Synchronized User ID ソリューションなど、あらゆるファイアウォールで利用可能な最も広範なユーザー認証オプションのセットを提供します。これにより、より厳密で、きめ細やかなユーザーアクセスを提供し、外部の攻撃者だけでなく悪意のある内部関係者が機密システムやデータにアクセスするのをブロックします。
	Sophos Cloud Optix	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 の関係性を完全に把握できる IAM 視覚化ツールを使用すると、IT チームは過剰な権限が付与されたアクセスを特定し、サイバー攻撃者に悪用される前に適切なサイズの IAM ポリシーを迅速かつ簡単に作成できます。
攻撃対象領域を最小限に抑え、中断のない製造業務を確保	Sophos Firewall	高度なマルウェアの脅威を寄せ付けない Web、メール、ゼロデイ保護機能が組み込まれているため、セロデイマルウェア、APT、ランサムウェア攻撃による侵害の試みを防ぎます。
	Sophos XDR	豊富なネットワーク、メール、その他のデータソースを利用し、必要に応じて詳細に掘り下げる機能でサイバーセキュリティポスチャをより広範に把握できます。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 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。データは、エンドポイント、ネットワーク、ID メールなどで収集され、強力な AI ツール、脅威インテリジェンス、人間の専門知識を使用して相関付けられ、影響と対応を特定します。
フィッシング攻撃への対策	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。

セキュリティの課題	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
高度なマルウェアと脅威の防止	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。 SophosLabs がサポートする統一シグネチャ形式を使用して、ハッキングや攻撃から高度な保護を提供する次世代 IPS が含まれています。
	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 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。 エンドポイント保護のアプリケーションコントロールのポリシーは、未承認のアプリケーションの使用を制限します。 ホワイトリスト化されている特定のアプリケーションと、そのアプリケーションに関連付けられているファイルのみ実行を許可します。
	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。
	ソフォス製品の Synchronized Security 機能	テレメトリとセキュリティ状態を共有し、サーバー、エンドポイント、ファイアウォール全体で調整された分離、検出、およびマルウェア修復を可能にし、高度な攻撃を阻止します。
	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 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。
サードパーティベンダーのリスクの軽減	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。
	Sophos Intercept X Advanced 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 機能により、疑わしいアクティビティを自動的に特定し、脅威インジケーターに優先順位を付け、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。

セキュリティの課題	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
分散型製造企業のセキュリティを保護	ソフォスのセキュアアクセス製品群	アプリケーションへの安全なアクセスをサポートする Sophos ZTNA、ブランチオフィスやリモートデバイスにネットワークを安全に拡張するための Sophos SD-RED リモートイーサネットデバイス、簡単かつ安全なワイヤレスネットワークを実現する Sophos Wireless アクセスポイント、LAN 上での安全なアクセスを実現する Sophos Switch が含まれています。すべては、単一のクラウドベースのセキュリティプラットフォームである Sophos Central によって管理されます。
	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。
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。
従来の製造システムの保護	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.co.jp

Oxford, UK
© 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。
2023-04-20 RC-JA (PS)

SOPHOS