ソリューションカタログ

Sophos Workspace Protection

リモートワーカーとハイブリッドワーカーを簡単かつ低コストで保護

Sophos Workspace Protection により、ビジネスワークスペースのセキュリティ管理を取り戻すことが可能になります。アプリ、データ、従業員、ゲストへのアクセスをあらゆる場所で、簡単かつ低コストで保護します。

働き方の変革

従来のネットワークの境界が消え去り、従業員はさまざまな場所で働き、アプリやデータも至る所に散在しています。自社で所有やホスティングするプライベートアプリケーションに加え、レンタル型の SaaS アプリケーションも利用されており、従業員が日常的に使用するアプリケーションやサービス、Web サイトがインターネット上で運用されています。また、多くの組織では、社内勤務とリモート勤務、モバイルワーカーを組み合わせたハイブリッドな働き方が一般的で、社員はオフィス、自宅、移動中、さらには公共の場でも業務を行っています。これらの要素が組み合わさることで、あらゆる組織にとって、適切な監視、制御、セキュリティ保護を実現することが非常に大きな課題となっています。

クラウドで提供される従来の SASE または SSE ソリューションは、運用コストが高く、購入コストも高くなります。これらのソリューションでは、トラフィックをクラウド上の拠点に戻して検査する必要があり、さらに中間者復号 (暗号化された通信を途中で解読して安全性やポリシーをチェックし、再び暗号化して送信する仕組み) を実行するため、不要な遅延が発生し、使い勝手の問題も生じます。より優れた方法を探らなければなりません。優れた利便性と安全性をもたらす Sophos Workspace Protection をご利用ください。

アプリ、データ、従業員、ゲストを保護

Sophos Workspace Protection は、あらゆる場所で、アプリ、データ、従業員、ゲストユーザーを保護する、コストが手頃で簡単に操作できるソリューションを提供します。1 つのアプリ (ブラウザ) のみを利用して、必要なすべての保護機能を統合するため、トラフィックの検査やクラウド処理、追加の復号化が不要で、透過的で安全なエクスペリエンスを実現します。

保護対策

Sophos Protected Browser

単一のアプリで他のすべてのアプリを保護します。ハードニングした Chromium ブラウザに、ZTNA、DNS Protection、SaaS アプリコントロール、Secure Web Gateway、ローカルデータコントロールが統合されており、ユーザーは違和感なく、これまでと同じ感覚でブラウザを使用できます。

Sophos ZTNA：

ユーザーが必要なアプリケーションにのみ、安全にアクセスできるようにします。また、他のユーザーや外部からはそのアプリケーションが見えないようにして、攻撃から守ります。

Sophos DNS Protection for Endpoints

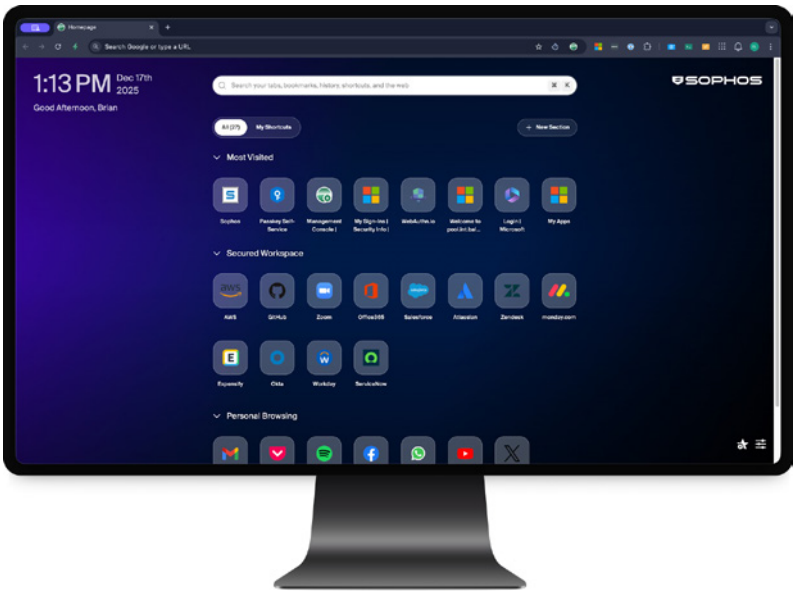
ブラウザおよび Web アプリケーションで、悪意のある Web サイトや不適切なコンテンツを確実に防ぎ、従業員がどこで作業しても確実に保護します。

Sophos Email Monitoring System

既存のメールソリューションと連携し、セキュリティ、可視性、レポート機能を強化します。これにより、他のソリューションでは逃してしまうような高度なメール脅威も捉えることが可能となります。

特長

- アプリ、データ、従業員、ゲストを保護します。
- 攻撃からアプリを保護しながら、アプリへの安全なアクセスを可能にします。
- シャドー IT を排除し、生成 AI のような新しいテクノロジーを安全に取り入れることができます。
- Web ワーカーを保護し、セーフブラウジングポリシーを適用します。
- ゲスト、買収した企業の従業員、一時的にアクセスが必要な従業員を簡単に安全に管理できます。
- Synchronized Security をリモートワーカーとハイブリッドワーカーにまで適用できます。
- 攻撃や侵害からの保護



Sophos Workspace Protection の利点

シャドウ IT を排除：
未承認の Web アプリケーションや SaaS アプリケーションの使用を監視、制御できます。

生成 AI の効果的な導入：
承認済みの AI ソリューションを推進、監視することで、アクセスを制御し、データの移動を制限します。

Web 上での従業員の保護
Web アプリおよびそのアクセスに関して、利用場所に関わらず一貫したポリシーを適用できます。

高額な損失につながるデータ操作ミスの防止：
Web サイトやアプリ上での機密データのコピー、貼り付けなどのやり取りをブロックして、誤操作によるデータ流出を防ぎます。

アプリの保護：
自社でホストしているアプリケーションに安全な ZTNA アクセスを提供し、外部からはこのアプリケーションが見えないようにします。

安全なゲストアクセス：
ゲストユーザーや、契約社員、企業買収によって加わったスタッフに対して、アプリやシステムへのアクセスを簡単に有効にできます。

Synchronized Security の拡張：
ソフォスの Synchronized Security を使って、感染デバイスからの重要アプリやシステムへのアクセスを一時的にブロックします。

侵害の防止：
システム、アプリ、従業員がインターネット上で無防備に晒される状態を回避し、ネットワーク侵害のリスクを防ぎます。

メールセキュリティを強化：
既存の防御機能を補完するセキュリティレイヤーを追加して、メールのセキュリティポスチャを強化します。

簡単、低コスト、優れた安全性

Sophos Workspace Protection は、クラウドで提供される SASE や SSE ソリューションよりも容易かつ手頃な価格で、バックホールや中間者復号が不要で、導入や拡張も容易です。すでに利用しているブラウザというシンプルなアプリで、他のすべてのアプリを保護でき、しかも、クラウド上の 1 つの管理コンソールである Sophos Central からすべてを一元管理できます。Sophos Protected Browser は、これまでセキュリティ上のリスクだったものを、強化されたセキュリティ資産へと変えます。

ファイアウォールとエンドポイント保護の統合と拡張

ファイアウォールはネットワークを、エンドポイントはデバイスを守ります。Sophos Workspace Protection は、アプリやデータ、従業員やゲストなど、その他のすべてを包括的に保護します。Sophos Workspace Protection は、ネットワークとエンドポイント保護を統合および拡張し、ワークスペースを保護します。さらに、Synchronized Security Heartbeat をリモートワーカーやハイブリッドワーカーにまで拡張することで、Sophos Firewall や Sophos Endpoint との連携が一層強化されます。デバイスが侵害された場合、ハートビートポリシーにより、クリーンアップされるまで重要なアプリケーションやデータに接続できなくなります。

シンプルなライセンス体系によって優れた価値をもたらす

シンプルなユーザーベースのライセンス体系と魅力的な価格設定により、これまでにないほど簡単に Sophos Workspace Protection を導入できるようになりました。

- **スタンドアロン：**Sophos Workspace Protection の単体販売。Sophos Protected Browser、Sophos ZTNA、Sophos DNS Protection for Endpoints、Sophos EMS が含まれ、あらゆるファイアウォールやエンドポイントソリューションと連携します。
- **Sophos Endpoint と同時購入：**両製品をより簡単に購入できる便利なバンドルであり、Synchronized Security による高度な連携が可能で、どちらも Sophos Central から一元管理できます。
- **Sophos Firewall と同時購入：**リモートワーカーやハイブリッドワーカー、ゲストへネットワークセキュリティを拡張します。また、ZTNA によるアプリの保護も可能です。これらすべては Sophos Central から管理できます。

Sophos Workspace Protection は、ソフォス製品がすでに導入されている環境にも新しく導入する場合にも最適な拡張ソリューションです。

技術仕様

Sophos Workspace Protection 製品は、既存の環境にシームレスに適合するように設計されており、一般的なアイデンティティプロバイダーやプラットフォームと統合できます。

アイデンティティプロバイダー：

ZTNA と Endpoint DNS Protection：
Microsoft Active Directory (オンプレミス)、Microsoft Entra ID (Azure Active Directory)、Okta

保護されるブラウザ：
Microsoft Entra ID（Azure Active Directory）、Okta

オペレーティングシステムとプラットフォーム：

ZTNA ゲートウェイ：
VMware ESXi 7+、Hyper-V 2016+、Sophos Firewall

ZTNA エージェント：
Windows 10、Windows 11 (Intel および ARM プロセッサ)、macOS Sonoma、Sequoia、Tahoe (Intel および Apple プロセッサ)

Endpoint DNS Protection：
Windows 10、Windows 11 (Intel および ARM プロセッサ)

保護されるブラウザ：
Windows 10、Windows 11、Windows Server 2022、Windows Server 2025 (Intel プロセッサのみ — ARM 近日発売)、macOS Sonoma、Sequoia、Tahoe (Intel および Apple プロセッサ)

デバイスポスチャ：

ZTNA エージェント：
Sophos Security Heartbeat (Sophos Endpoint)

保護されるブラウザ：
OS、Endpoint Protection (ソフォスおよびその他のベンダー)、ディスク暗号化の状態

ZTNA ゲートウェイの仕様

推奨される VM：
2 コア / 4GB

複数ノードクラスタリング：
VM は最大 9 ノードまでクラスタ化でき、Sophos Firewall を高可用性構成で導入することで、ゲートウェイのパフォーマンス、処理能力、ビジネス継続性を向上できます。

ノードの容量と拡張性：
1 つのノードに 10,000 エージェントコネクション、1 つのクラスタに最大 90,000 エージェントコネクション (最大 9 ノード)

詳細と無料トライアルについては、sophos.com/workspace-protection をご覧ください。

ソフォス株式会社営業部
Email: sales@sophos.co.jp