ソリューションカタログ

Sophos と Microsoft

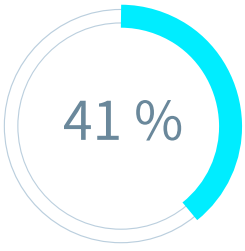
連携によって堅牢なセキュリティを実現

現代のサイバー脅威を防ぐには、Microsoft 環境全体にわたって、より強力で適応性の高い保護が必要です。業界トップクラスのソフォスソリューションと、既に利用している Microsoft のツールを組み合わせることで、保護を強化し、リスクを低減し、セキュリティ投資の効果を最大化できます。

Microsoft を中心とした環境を採用している組織は、重要なセキュリティ上の課題に直面しています。

攻撃者が ID を標的とするケースが増加しており、サイロ化されたセキュリティツールのギャップを突いています。また、セキュリティチームはアラートへの対応に疲弊しています。ビジネスメール詐欺攻撃やセッションハイジャックは、MFA を回避することも多く、Microsoft 環境全体でアイデンティティが重要な脅威ベクトルになっています。一方、リモートランサムウェアによる暗号化とハンズオンキーボードの手法により、攻撃者は Microsoft の防御をすり抜けることがあります。社内の専門知識が限られていることから、これらのプレッシャーは、重大な可視性と対応のギャップを生み出しています。

セキュリティ成果の加速



Microsoft のテレメトリによって開始された Sophos MDR 脅威ケースの割合。

2025 年に Microsoft 環境に対する高度な攻撃で Sophos MDR によって無力化された件数。

Microsoft 環境における Sophos MDR による脅威の平均修復時間。

特長

- **Microsoft への投資を最大限に活用：**深い洞察、脅威検知の強化、専門家主導の対応により、Microsoft ツールの価値を高めます。
- **保護の強化：**アイデンティティ、エンドポイント、メール、ネットワークにわたって攻撃が可能となるギャップを解消します。
- **セキュリティ成果の加速：**Sophos MDR のアナリストがお客様に代わって脅威を迅速に修復します。
- **運用の複雑さの軽減：**統合されたインテリジェンスとワークフロー、専門家によるガイダンスにより、セキュリティ管理を簡素化し、チームの負担を軽減します。
- **レジリエンスの強化：**数十万の Microsoft 環境から収集したテレメトリ情報に基づいて高度な保護を実現できます。

ソリューションを組み合わせ、優れたセキュリティを実現

ソフォスは、深い洞察、迅速なアクション、比類のない専門知識により、Microsoft 環境のセキュリティと価値を高めます。

Microsoft のあらゆるプランを防御：M365 Business Basic、Standard、Premium、E3、E5 のいずれのプランを利用していても、ソフォスは高度な保護、検知、対応を提供します。

コミュニティから生み出される知見を組み込み：数十万の Microsoft ユーザーを保護してきた経験から得られた知見が、ソフォスコミュニティ全体の保護を継続的に強化します。

幅広くスタック全体を保護：エンドポイント、メール、ファイアウォール、ITDR、MDR、アドバイザリーサービスはすべて Microsoft と統合され、リスクを軽減し、進行中の脅威を阻止します。

双方向の緊密な統合：ソフォスは豊富な Microsoft テレメトリを取り込み、攻撃者の行動を特定するとともに、Microsoft 365 環境で直接対応アクションを実行します。

単なるアラートの転送ではなく、セキュリティの成果に責任を持つ：Sophos MDR のアナリストはアラートを通知するだけでなく、Microsoft テナント内で直接かつ即座にアクションを実行します。

Microsoft 認定の専門家：Sophos MDR チームには、カスタム対応プレイブックを使用して高度なサイバー攻撃を検知して対応することを専門とするセキュリティオペレーションアナリストが参加しています。

ソフォスが Microsoft スタックを強化する方法

ソフォスは、Microsoft のツールと連携して動作する包括的なセキュリティ機能スイートを提供します。各ソリューションは、Microsoft 戦略全体に対して、より深い可視性、インテリジェンス、レジリエンスをもたらします。ソフォスは、エンドポイント、アイデンティティ、メール、ネットワークなど幅広い領域にわたり、攻撃者が悪用するギャップを解消するよう設計された、統合的な保護を提供します。

Sophos MDR for Microsoft environments

独自の検知、Microsoft のシグナル、専門的なアナリストを組み合わせ、脅威を迅速に封じる 24 時間 365 日体制の MDR サービス。Microsoft テクノロジー環境やハイブリッド環境を運用しており、単にアラートを送るだけでなく、セキュリティの成果に責任を持つ専門チームを求める組織に最適です。

- Microsoft のシグナルを活用し、テクノロジーだけでは防ぐことができない高度な攻撃を特定して防御します。
- Microsoft Graph Security および Management Activity API からのテレメトリを活用し、E5 ライセンスがなくても高度な検知機能を提供します。
- Microsoft および Microsoft 以外のソリューションとの統合により、IT 環境全体を包括的にカバーします。
- Microsoft 環境で、ユーザーセッションの取り消し、サインインの無効化、悪意ある受信トレイルールの停止などの対応アクションを迅速に実行します。
- Sophos Endpoint (付属) または Microsoft Defender for Endpoint を選んで使用できます。

Sophos MDR は、Microsoft インテリジェントセキュリティアソシエーション (MISA) を通じて、Microsoft によって認定された中小企業 (SMB) 向けソリューションであり、Microsoft Defender for Endpoint および Defender for Business と緊密に統合され、Microsoft 環境全体で強力かつ迅速な保護を提供します。

Sophos ITDR for Entra ID

Sophos ITDR (Identity Threat Detection and Response) は、Entra ID の設定ミスやエクスポージャを継続的にスキャンし、ダークウェブ上で発見された情報など、認証情報の悪用を監視します。アナリストが Entra ID 内で迅速に対応アクションを講じ、アイデンティティを狙った攻撃を封じ込めることを可能にします。Sophos ITDR は、ソフォスの比類のない脅威対策により、Entra ID のネイティブ IAM 機能を強化します。

Sophos Endpoint for superior ransomware protection

現在の手動によるランサムウェア攻撃の 70%* は、Microsoft Defender などのツールによる検知を回避するためにリモート暗号化を利用しています。Sophos Endpoint は、独自の CryptoGuard テクノロジーを搭載し、ローカルおよびリモートのランサムウェアを即座に阻止します。ユーザーベースのライセンスは、チームメンバーが複数のデバイスを利用している場合 (レガシー Windows やサポート終了済みの Windows を実行するエンドポイントを含む) でも、最大限の価値を発揮します。

Sophos Email for Microsoft 365

Sophos Email は、Exchange Online と連携し、フィッシング攻撃やビジネスメール詐欺を阻止。ユーザー意識向上トレーニングとフィッシングシミュレーションも利用でき、メールフローや Microsoft のセキュリティポリシーを妨げることなく運用できます。

Sophos Firewall for Microsoft environments

Sophos Firewall は Microsoft 環境向けに最適化されており、ハードウェア、仮想、クラウド (Azure や Hyper-V を含む) での柔軟な導入オプションを提供します。また、ゼロトラストのリモートアクセスを実現する Entra ID との連携や、SD-WAN オーバーレイネットワーク展開のための Azure Virtual WAN 連携にも対応しています。

Taegis XDR with Next-Gen SIEM for Microsoft E5 + Sentinel

SIEM レベルのデータ保持と、予測可能なストレージコストでスタックを横断した脅威検知が必要な企業向けに、Taegis は Microsoft および Microsoft 以外のテレメトリを統合し、Sentinel と連携しつつ、イベント毎秒 (EPS) 課金の変動を回避します。

Sophos Intelix for Microsoft Copilot

Sophos Intelix は、Sophos XOps の脅威インテリジェンスを Microsoft Security Copilot および Microsoft 365 Copilot に統合し、Microsoft 環境で高度なセキュリティをシームレスに実現します。これらの統合により、防御担当者、IT 管理者、ビジネスユーザーが日常的に利用している環境で、高度なサイバーインテリジェンスを即座に活用できるようになります。

ソフォスと Microsoft の適切な機能の組み合わせの選択

Microsoft 環境を強化するには、ソフォスの機能と Microsoft テクノロジーの適切な組み合わせを選ぶことから始まります。既存の Microsoft プランを基盤にする場合でも、特定のセキュリティ課題に対応する場合でも、ソフォスは保護機能を最大化し、運用を簡素化し、より優れた成果を提供する明確な方法を提供します。

Microsoft のプランに合わせた調整

M365 のサブスクリプションに合わせて、ソフォスと Microsoft の最適な組み合わせを特定します。各組み合わせは、可視性を強化し、脅威への対応を改善し、攻撃者が悪用するギャップを解消することを目的としています。

M365 Business Basic、Business Standard、O365 E1、O365 E3 向け

これらの Microsoft の生産性重視のプランを利用している組織は、現代の脅威に対抗するために、より強力なエンドポイント、メール、検知機能が必要とすることが多くあります。

追加することが推奨されるソフォスの機能：

- **Sophos MDR** — Microsoft のテレメトリを使用して、24 時間 365 日体制の検知と専門家による対応を提供します。
- **Sophos Endpoint** — 堅牢なリモートランサムウェア対策を含む高度な保護機能。
- **Sophos Email** — 強化されたフィッシング対策とビジネスメール詐欺 (BEC) 対策。

M365 Business Premium、M365 E3、E5 向け (Microsoft Defender ソリューションを活用)

これらのプランには多くの保護ツールが組み込まれていますが、多くのチームは、組織のセキュリティポスチャの検知、対応、および検証を強化する必要があります。

追加することが推奨されるソフォスの機能：

- **Microsoft Defender for Endpoint (または Sophos Endpoint に切り替えて) と** Sophos MDR の連携
- **Sophos Advisory Services** — 侵入テストとアセスメントによって、セキュリティギャップを特定します。
- **Sophos Email Monitoring System** — Microsoft 365 メールに対して重層的な可視性と検知機能を提供します。
- **Taegis XDR と次世代 SIEM** — データ保持コストを予測しながら、スタックを横断する脅威を検知します。

セキュリティ要件への適合

ソフォスは、Microsoft 環境で特に多く見られる脅威に対応するために設計された、最適なソリューションの組み合わせを提供します。アイデンティティ、エンドポイント、メール、ネットワークにわたってセキュリティの脆弱性を解消します。

アイデンティティを狙った脅威

攻撃者は、Entra ID とユーザーアイデンティティを標的にして、環境への足掛かりを得ることが多くなっています。

推奨される機能の組み合わせ：

- **Microsoft Entra ID + Sophos MDR**
  - **Sophos ITDR** を追加して、プロアクティブなアイデンティティリスクの検知と対応を実現します。

リモートランサムウェア

現在の手動によるランサムウェア攻撃の 70%* は、Microsoft Defender などのツールによる検知を回避するためにリモート暗号化を利用しています。

推奨される機能の組み合わせ：

- **Sophos Endpoint + Sophos MDR**
  - または、**Microsoft Defender (既に導入されている場合) + Sophos MDR**

ビジネスメール詐欺 (BEC)

BEC 攻撃では、なりすまし、受信トレイルールの操作、MFA バイパスの手法が悪用されます。

推奨される機能の組み合わせ：

- **Microsoft 365 Email + Sophos Email + Sophos MDR**

セキュリティポスチャとリスクの軽減

レジリエンスの強化を検討している組織は、セキュリティの専門家によって提供されるプロアクティブなセキュリティテストを活用できます。

推奨される機能の組み合わせ：

- **ソフォスアドバイザリーサービスによる弱点の把握**
  - さらに、特定されたリスクに対処する **Microsoft とソフォスのソリューション**。

今すぐ専門家にご相談いただき、Microsoft 環境に適したセキュリティ対策を構築してください。ソフォスのチームが、M365 サブスクリプション向けにソフォスと Microsoft の最適な機能の組み合わせを特定し、Microsoft 投資の価値を最大限に引き出せるよう支援します。

詳細情報：www.sophos.com/ja-jp/microsoft

* Microsoft デジタル防衛レポート 2024

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2026-03-02 BR-JA (TA) CRE-4588