ソリューションカタログ

Sophos ITDR

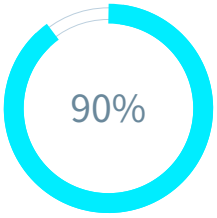
ビジネスに影響が及ぶ前にアイデンティティベースの脅威を無力化

Sophos Identity Threat Detection and Response (ITDR) は、環境内のアイデンティティに関わるリスクや設定ミスを継続的に監視し、さらに漏洩した認証情報に関するダークウェブのインテリジェンスを提供することで、アイデンティティを標的とした攻撃を未然に防ぎます。

アイデンティティの脅威：拡大し続けるセキュリティ問題

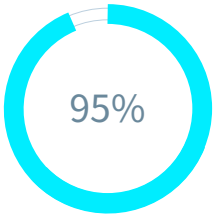
ユーザーベースのアクセス管理と制御は、現代の IT およびサイバーセキュリティの最前線を担っています。しかし、クラウドへの移行やリモートワークの普及に伴い、アイデンティティ攻撃のアタックサーフェスの監視と防御は一層複雑化しています。攻撃者は、侵害された認証情報、インフラの脆弱性、設定ミスを利用して、機密データやシステムへ不正にアクセスしています。そのため、アイデンティティの悪用を検知し、アイデンティティベースの攻撃をブロックすることが、セキュリティの効果を高めるためにますます重要になっています。

数字が示す事実

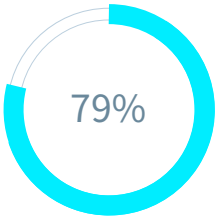


過去 1 年間に少なくとも 1 件のアイデンティティ関連の侵害を経験した組織の割合 [1]

データ侵害の平均コスト [2]



重大な設定ミスが存在する Microsoft Entra ID 環境の割合 [3]



アイデンティティに関連するデータ侵害の割合 [4]

Sophos ITDR ソリューション

Sophos ITDR は、アイデンティティベースの攻撃を防止し、95% の組織に影響しているアイデンティティリスクや設定ミスを継続的に監視しながら、漏洩した認証情報に関するダークウェブのインテリジェンスを提供します。従来のソリューションではアイデンティティリスクを発見するのに数日かかる場合もありましたが、Sophos ITDR なら数分で特定することが可能です。さらに、自社のアイデンティティアタックサーフェスを継続的にベンチマークし、経時的な変化を把握することもできます。

特長

- システム全体のアイデンティティを一元的に**可視化**。
- アイデンティティに関連するリスクと設定ミスを**迅速に特定**し、実用的な対策を推奨。
- アイデンティティポスチャの変化を**継続的にスキャン**。
- **ダークウェブ**に漏洩した認証情報**をスキャン**。
- インサイダー、見慣れない IP アドレスや場所から発生する**潜在的に悪意のある活動を検知**。
- アイデンティティに関する**脅威を迅速に検知**して正確に対応。
- **Sophos MDR と統合**し、専門家による調査と、アイデンティティベースの脅威への対応を実現。

アイデンティティのアタックサーフェスを縮小

Sophos ITDR は、Microsoft Entra ID 環境を継続的にスキャンし、設定ミスやアイデンティティに関連するセキュリティギャップを迅速に特定します。さらに、対応が必要な問題をリスクに基づいて優先順位付けし、効率的な対処を支援します。サイバー犯罪者は、こうしたギャップや脆弱性を悪用して権限を昇格したり、さまざまな攻撃を実行したりして、組織に被害をもたらしています。Sophos ITDR は、条件付きアクセスポリシーのギャップ、孤立したアカウント、過剰な権限が付与されたアカウント、リスクの高いアプリケーションなどのリスクを迅速に解消します。

認証情報の漏洩や窃取のリスクを最小化

Sophos X-Ops の Counter Threat Unit (CTU) のインテリジェンスによると、ダークウェブ最大級のマーケットプレイスで販売されている窃取された認証情報の数は、過去 1 年間で倍増しています。Sophos ITDR は、従来のアイデンティティセキュリティ対策を回避するアイデンティティの脅威を検知・対応し、MITRE ATT&CK の「認証情報へのアクセス」に分類されるあらゆる手法 (100%) から組織を保護します。5 このソリューションは、異常なログインパターンなど、リスクの高いユーザー行動を検出し、窃取または漏洩した認証情報を使用する不正アクセスを可視化します。

Sophos ITDR の機能

アイデンティティカタログ
システム全体のアイデンティティを一元的に可視化します。

アイデンティティポスチャの継続的な評価
Microsoft Entra ID 環境を継続的にスキャンし、設定ミスやセキュリティギャップを特定します。

ダークウェブに漏洩した認証情報の監視
ダークウェブやデータベースで、漏洩した認証情報を検索します。

ユーザー行動分析
窃取された認証情報に関連する異常な活動を監視します。

高度なアイデンティティ脅威の検知
攻撃チェーンの初期段階で、特定の攻撃者が用いている手法を示す不審な活動を検知します。

脅威への対応
迅速かつ正確な対応を可能にします。パスワードリセットの強制、攻撃が疑われる動作があったアカウントのロックなどの対応が可能です。

「Sophos ITDR は、アイデンティティリスクの可視化を大幅に改善します。ソフォスの XDR プラットフォームで一元的に表示・管理でき、Sophos ITDR が特定したアイデンティティや設定ミスのリスクをすべてのセキュリティプログラムに反映させることができます。その結果、組織全体のサイバーセキュリティポスチャを強化し、リスクを低減することが可能になりました。」

– 金融サービス企業、
情報セキュリティ部門
ディレクター

「Sophos ITDR によって、条件付きアクセスポリシーにおけるギャップや、安全性の低いアプリケーション、過度の権限が付与されていたアプリケーションなど、Azure および Microsoft のエコシステムにおいてこれまで懸念されていた領域のリスクを把握できるようになりました。」

– 上級情報セキュリティ責任者

Sophos MDR との統合

Sophos ITDR は、世界で最も信頼されている MDR サービスである Sophos MDR と完全に統合されています。ソフォスのセキュリティ専門家は、この強力なソリューションを組み合わせて、顧客に代わって、アイデンティティに関連する脅威を監視および調査し、対応します。

- Sophos ITDR は、アイデンティティベースの脅威やリスクの高い問題が検知されると、自動的に MDR ケースを作成します。
- Sophos MDR のセキュリティアナリストが、これらのケースを調査し、脅威を無力化するための対応を行います。

例：漏洩した認証情報がダークウェブで特定されたケース

- Sophos ITDR は、広く利用されているダークウェブのマーケットプレイスで販売されているユーザーの認証情報を特定します。
- Sophos MDR のアナリストは、そのユーザーアカウントをロックし、パスワードリセットを強制できます。

例：窃取された認証情報が使用されているケース

- Sophos ITDR は、これまでユーザーが移動したことがない国や、アクセスしたことのないデバイスおよび IP アドレスからの不審なログインを検出します。
- Sophos MDR のアナリストは、侵害されたユーザーアカウントをロックし、すべてのアクティブなセッションを強制終了できます。

Sophos ITDR + Microsoft Entra ID を組み合わせて、優れたセキュリティを実現

Microsoft Entra ID は本質的にアイデンティティおよびアクセス管理 (IAM) ツールであり、アイデンティティおよびグループ管理、RBAC (ロールベースのアクセス制御)、特権アクセス管理、条件付きアクセスポリシーなどの機能を提供します。Sophos ITDR は、これらの IAM ツールの機能以外に、アイデンティティハイジーン、セキュリティポスチャ評価、ダークウェブ監視、高度な脅威検知などの機能を統合型のコンソールで提供。これにより、アイデンティティに関連する脅威やリスクを的確に検知し、迅速に無力化することが可能です。Entra ID と Sophos ITDR を組み合わせることで、企業は最も包括的なアイデンティティセキュリティ対策を実現できます。

シンプルなライセンス

Sophos ITDR は、購入、導入、利用が簡単です。ユーザー数とサーバー数に基づくサブスクリプションライセンスにより、価格が簡明で予測しやすくなっています。さらに、Sophos ITDR を必要に応じて、Sophos XDR ソリューションや Sophos MDR サービスに追加して利用することも可能です。

- **Sophos MDR (Managed Detection and Response) へのアドオン：**ソフォスのセキュリティ専門家は、顧客に代わって、アイデンティティに関連する脅威を監視および調査し、対応します。
- **Sophos XDR (Extended Detection and Response) へのアドオン：**社内チームは、Sophos ITDR とソフォスの AI を活用した検知、調査、対応ツールを活用できるようになります。

Gartner

XDR (Extended Detection and Response) 部門で、2025 年 Gartner® Peer Insights ™ Customers' Choice を獲得。

XDR (Extended Detection and Response) と MDR (Managed Detection and Response) の G2 Overall Grid® レポートでリーダーに選出。

MITRE | ATT&CK® Evaluations

MITRE ATT&CK® 評価のマネージドサービスおよびエンタープライズ製品部門で優れた成績を獲得。

FROST & SULLIVAN

Frost & Sullivan の 2025 Frost Radar ™ for Managed Detection and Response でリーダーに選出。

詳細はこちら
sophos.com/ITDR

1 - 2024 年の Identity Defined Security Alliance (IDSA) による調査。
2 - IBM、2024 年データ侵害のコストに関する調査。
3 - ソフォスのインシデント対応チームによる調査。
4 - Identity Defined Security Alliance。
5 - MITRE ATT&CK フレームワークにマッピングされた検知カテゴリに基づく

ソフォス株式会社
Email: sales@sophos.co.jp

2025-09-15 BR-JP (MP)

SOPHOS