SOPHOS

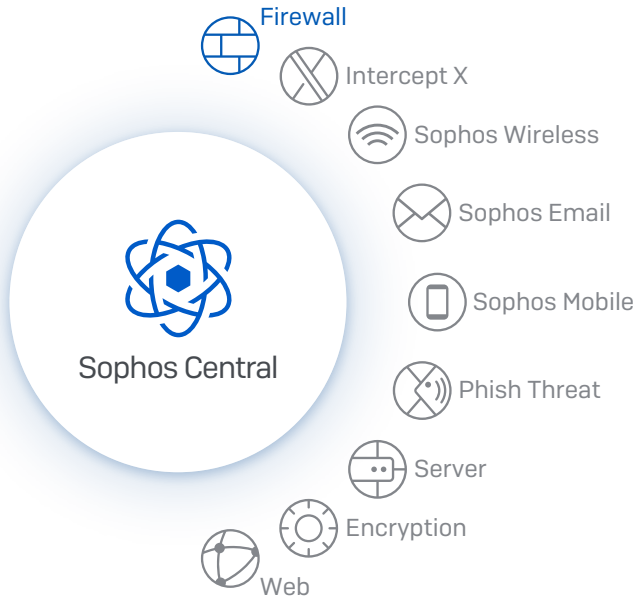
Sophos Central Firewall

Sophos Central Firewall 管理とレポーティング

Sophos Central は、Sophos Firewall 環境向けの究極のクラウド型管理およびレポートエコシステムです。Sophos Central を使用すれば、単一のファイアウォールであっても、数百のファイアウォールであっても、追加料金なしで簡単に管理できます。ゼロタッチ導入、ファイアウォールのグループ管理、柔軟なレポートツールなど、すべて追加料金なしで利用できます。

包括的なセキュリティエコシステム

Sophos Central は、すべてのソフォス製品へのゲートウェイとして、あらゆる拠点で最高の保護を実現できます。また、情報共有と脅威への対応も統合・同期化され、すべて比類のない可視性と洞察を提供する、使いやすい単一のクラウドコンソールから管理されます。

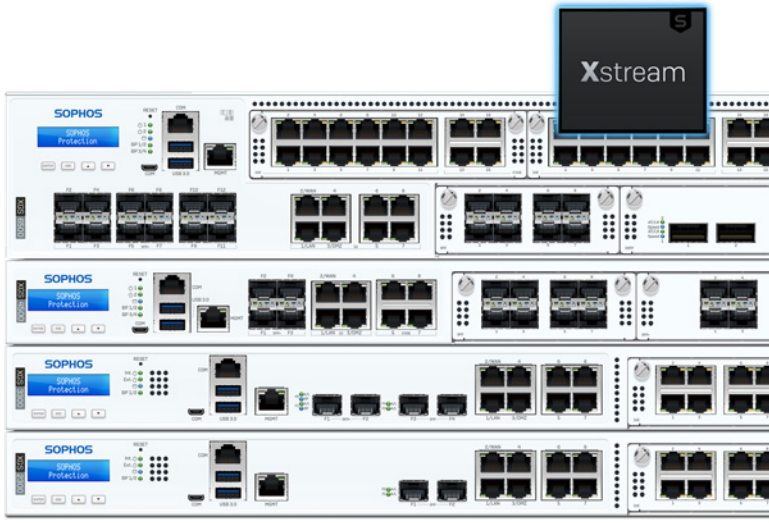


Synchronized Security

Sophos Central は、Sophos Synchronized Security を管理する唯一のコンソールです。Sophos Intercept X は、エンドポイント、サーバー、およびモバイルデバイスに導入して管理すると同時に、Sophos Firewall や SD-RED デバイスを、さまざまな支社やリモートオフィスに導入することもできます。その後、サイバーセキュリティは自動的に運用でき、Sophos Central を使用して、すべて製品を単一の画面から監視および管理できます。

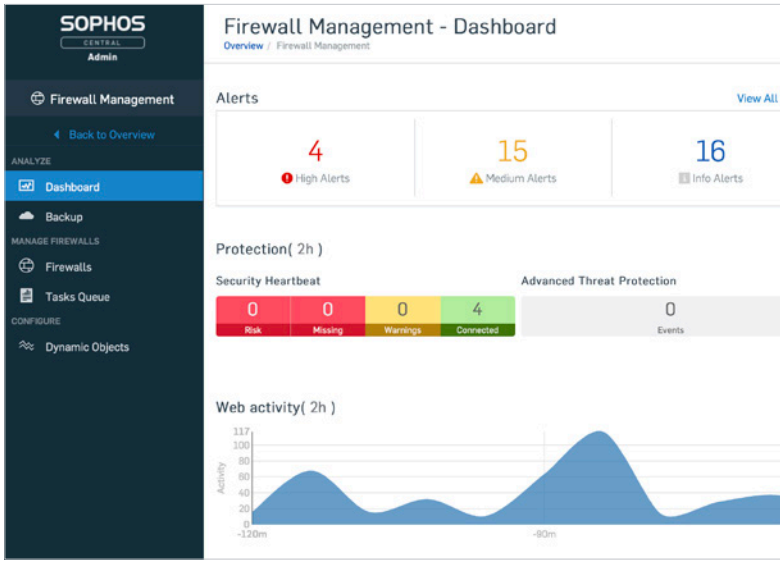
ファイアウォールのグループ管理

複数のファイアウォールを管理している場合、ファイアウォールすべての一貫性を確保し、同期し、最新の状態に保つことは大きな課題となります。Sophos Central は、これをシンプルにします。強力なグループ管理オプションにより、ファイアウォールを簡単にグループ化して、グループポリシーを同期させることができます。グループポリシーを一度変更するだけで、グループ内のすべてのファイアウォールで自動的に同期されるため、ネットワークの一貫性とコンプライアンスを確保できます。



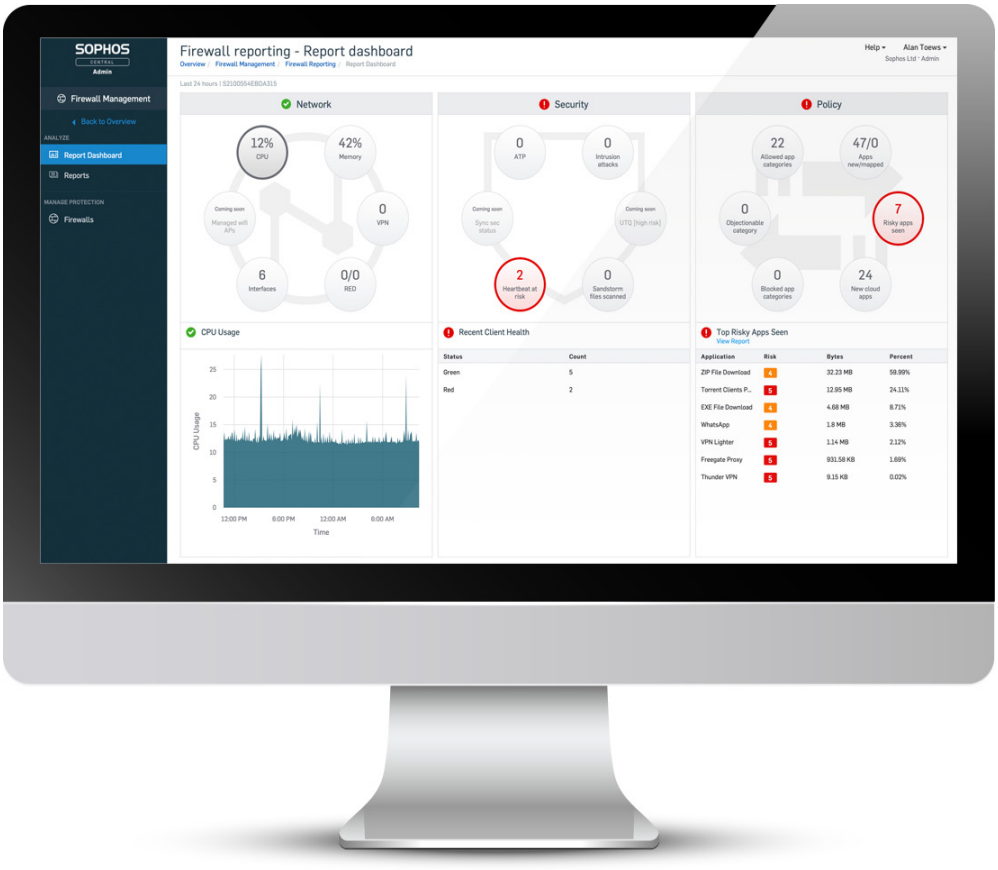
ネットワーク監視

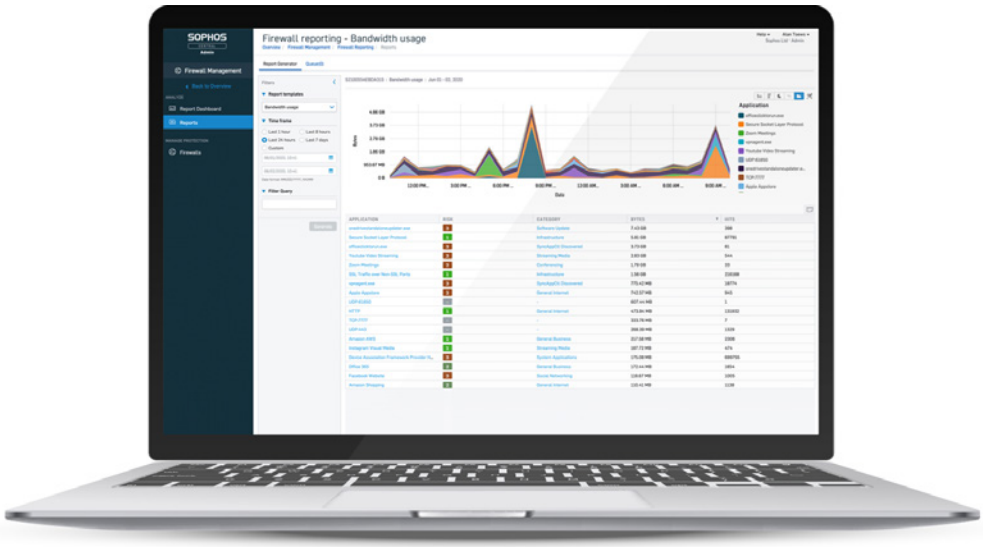
すべてのファイアウォール、その状態、および使用状況に関する情報は、Sophos Central の便利なダッシュボードから一目で把握できます。また、アクティブな脅威やセキュリティ警告を即座に把握し、VPN や SD-RED デバイスの状態やコンプライアンスリスクを監視することもできます。



ゼロタッチ導入

Sophos Central では、新しいファイアウォールデバイスに触れることなく導入を実行できます。Sophos Central で初期セットアップと設定を実行した後、設定をエクスポートします。オンサイトの担当者が、新しい Sophos Firewall デバイスを、フラッシュドライブにロードした設定で起動すると、ファイアウォールが Sophos Central に接続されるので、管理者はその後、リモートで設定を完了することができます。





マルチ ファイアウォール レポート

Central Firewall Reporting (CFR) では、Sophos Firewall 環境からネットワークアクティビティをキャプチャおよび分析する強力なツールセットを用意しています。すべてのファイアウォールからのログデータは、クラウド内の Sophos Central アカウントに送信されるので、各デバイスに個別にアクセスすることなく、ネットワークアクティビティを 1か所で明確に把握できます。管理サイト全体や特定のグループ、または特定のファイアウォールに簡単にドリルダウンして、レポートを生成できます。

事前定義レポートおよびカスタムレポート

まずは、事前に定義されている便利なレポートのいずれかを使用し、その後、データフィールド、表示オプション、フィルタを変更して、独自のレポートを生成できます。各レポートをカスタマイズし、任意のレポートから数百種類のバリエーションを作成して、特定のユースケースのデータやトレンドを視覚化します。そして、データをエクスポートしたり、定期的に関係者に送信するレポートをスケジュール設定したりできます。

解析によるネットワークインテリジェンス

ファイアウォールの syslog データをドリルダウンし、直観的かつ視覚的な形式の詳細なビューを表示して、ネットワークインテリジェンスを収集します。その後、データは、セキュリティギャップ、疑わしいユーザーの振る舞い、ポリシーの変更を必要とするその他のイベントを特定するトレンドを分析します。

ログのバックアップと管理

Sophos Central Firewall Reporting は、迅速な取得、監査、フォレンジックに対しスマートインデックス機能と簡単な検索機能を使用して、Sophos Firewall からデータをログに記録します。組み込みフィルタを使用すると、レポートから直接ログデータにピボットして、レポートビューのデータの背後にあるものをより詳細に確認できます。

コンプライアンスを支援

グループ ファイアウォール ポリシーの同期、タスクキュー、および詳細なレポート機能により、規格および社内のコンプライアンス要件に常に準拠することができます。コンプライアンス監査の場合は、いつでもネットワークイベントに関するレポートを作成できます。

Sophos Central を使用したバックアップとファームウェアのアップデート

Sophos Central を使用して、ファイアウォール設定のバックアップをクラウドに保存することで、必要に応じて簡単にアクセスできます。前回 5個までのバックアップファイルは自動的に維持され、また、バックアップの 1つをお気に入りとして「固定」することもできます。Sophos Central では、ファームウェアアップデートのスケジュール設定も簡単に実行できるので、ネットワークを中断することなく、最新の機能、パフォーマンス、およびセキュリティパッチで、ネットワークを常に最適化しておくことができます。

Managed Threat Response の有効化

Sophos Central Reporting を使用することで、24時間 365日体制の Sophos Managed Threat Response (MTR) サービスに Sophos Firewall を接続して、ネットワーク脅威の情報を共有できます。 特に、Sophos Firewall コネクタは、ATP イベントと IPS イベント情報を MTR アナリストに提供し、ネットワーク上での脅威ハンティングと調査を強化します。

購入方法

Sophos Central Management と Central Firewall Reporting は、v18 以降のファームウェアを稼働している Sophos Firewall に追加料金なしで含まれています。Central Firewall Reporting に、詳細なレポート機能とストレージ容量を追加して、データ保持期間を延長するライセンスは、CFR Advanced ライセンスと共に購入可能です。Sophos Firewall の Xstream Protection バンドルには、追加料金なしで30日間のストレージを備えた CFR Advanced が含まれています。ログデータは、FIFO (先入先出法) ベースで保存されます。詳細は以下の表を参照してください。

機能	CFR	CFR ADVANCED
データの保管期間	ストレージ容量の制限あり – 最大 7日間の保管期間	拡張性のあるストレージ容量 - 最大 365日の保管期間
Syslog の検索と表示	あり	あり
Sophos Central での Syslog データストレージ	あり	あり
Sophos Central での オンデマンドのレポート	あり	あり

機能	CFR	CFR ADVANCED
複数のファイアウォールに わたるレポート生成	なし	あり
レポートの保存、エクスポート、スケジュール設定	なし	あり
XDR / MTR コネクタ	なし	あり
価格とライセンス体系	追加料金なし – 永続使用	ファイアウォールごとに追加データストレージを購入

機能リストと技術仕様

サポート対象のファイアウォール

- ハードウェア、ソフトウェア、仮想、クラウドなど、v18 以降のファームウェアを実行している Sophos Firewall
- スケジュール設定されたファームウェアアップデートには、SFOS v18 MR3 以降が必要

ファイアウォール管理

- グループポリシーと設定の同期を維持するためにファイアウォールをグループ化
- 冗長化 (HA) のサポート
- バックアップファイルの管理
- Sophos Central からのファームウェアアップデート
- 任意の日時にファームウェアアップデートをスケジュール設定
- USB フラッシュドライブを使用したゼロタッチ導入
- タスクキューは、監視および監査の変更のために、すべてのファイアウォールグループの同期アクティビティを追跡

ログ表示と検索

- アーカイブされたログに対するログの検索および取得
- Web ベースの管理コンソール
- レポートダッシュボードにより、セキュリティ状態を一目で確認
- 標準 Web ブラウザを使用して、任意の場所からアクセスできるレポート

Firewall Reporting

- カスタマイズツールを備えた広範な組み込みレポートモジュール
- 個々のファイアウォール、複数のファイアウォール、グループ、またはすべてのファイアウォールを対象としたレポートの生成 (CFR Advanced のみ)
- レポートの保存、エクスポート、またはスケジュール設定 (CFR Advanced のみ)
- 標準レポート: 帯域幅の使用状況、アプリケーションの使用状況、Web の使用状況、ファイアウォール、ATP、Geo アクティビティ、IPS、Sandstorm イベントなど
- マルチ形式のレポート：表形式、グラフ形式
- 詳細な検索オプションによるカスタムレポートおよび特別なレポート
- Sophos Firewall と Sophos XDR および Managed Threat Response Service を統合する XDR / MTR コネクタ (CFR Advanced のみ)

無償評価版

無償評価版の登録 (30日間) sophos.com/firewall

ソフォス株式会社営業部
Email: sales@sophos.co.jp

21-04-03 JA (PS)