機能一覧

Sophos Firewall の機能一覧

Sophos Firewall

主な特長

- Xstream アーキテクチャが、ストリームベースのパケット処理により、最高レベルの可視性、保護、パフォーマンスを提供
- Xstream TLS インスペクションが、高性能、ダウングレードなしの TLS 1.3 のサポート、ポートに依存しない、あらかじめ例外を組み込んだエンタープライズレベルのポリシー、独自のダッシュボードの可視性、および互換性のトラブルシューティングを提供
- Xstream DPI エンジンが、単一の高パフォーマンスエンジンを備えた IPS、AV、Web、アプリ制御、および TLS インスペクションのストリームスキャン保護を提供
- Xstream Network Flow FastPath が、ポリシーベースでインテリジェントに信頼できるトラフィックを高速で処理
- Xstream SD-WAN は、ゼロインパクトの再ルーティング、SD-WAN モニタリング、SD-WAN マルチサイトのオーケストレーションツール、IPsec VPN トンネルトラフィックの FastPath アクセラレーションを備えたパフォーマンスベースのリンク選択を提供
- インタラクティブなコントロールセンターを備えた専用設計のユーザーインターフェースで、信号機のようなわかりやすい色分け（赤、黄、緑）で、注意が必要な情報を一目で確認可能
- Control Center が、エンドポイントのセキュリティ状態、不明な Mac および Windows アプリケーション、クラウドアプリケーションとシャドー IT、不審なペイロード、リスクの高いユーザー、高度な脅威、ネットワーク攻撃、不適切な Web サイトなどに関する情報を即座に提供
- 高度な検索機能により、2 回クリックするだけで目的の場所に移動できる最適化されたナビゲーション
- ポリシーコントロールセンターのウィジェットは、ビジネスに関するポリシーアクティビティ、ユーザー、およびネットワークポリシーを監視し、使用されていないポリシー、無効化されているポリシー、変更されたポリシー、および新しいポリシーを追跡
- 統合型のポリシーモデルで、すべてのファイアウォール、NAT、および TLS インスペクションルールをグループ化、フィルタリング、および検索オプションを備えた単一の画面に統合
- 自動および手動でカスタムグループを作成でき、一目で分かるマウスオーバー機能と強制インジケーターを備えた大規模なルールセット向けの合理化されたファイアウォールルールの管理
- すべてのファイアウォールルールは、アンチウィルス、サンドボックス、IPS、Web、アプリ、トラフィックシェーピング (QoS)、およびハートビートに適用されるセキュリティとコントロールの概要を分かりやすく提供
- 事前に定義された IPS、Web、アプリ、TLS、およびトラフィックシェーピング (QoS) ポリシーにより、一般的な展開シナリオ (CIPA、一般的な職場ポリシーなど) の迅速なセットアップと簡単なカスタマイズが可能
- Sophos Security Heartbeat™ が、ソフォスのエンドポイントとファイアウォールを連携し、セキュリティの状態とテレメトリを共有し、感染したエンドポイントや侵害されたエンドポイントを即座に識別可能
- Active Threat Response が、SophosLabs、MDR アナリスト、サードパーティから提供される脅威フィードによってアクティブアドバーサリーを特定、およびブロックして自動的に対応
- Synchronized Application Control が、ネットワーク上のすべての不明な Mac/Windows アプリケーションを自動的に識別、分類、制御
- Cloud Application Visibility が、シャドー IT の検知を即座に有効にし、ワンクリックでトラフィックシェーピングを提供
- ポリシーの検証シミュレータツールを使用することで、ファイアウォールルールと Web ポリシーのシミュレーション、ユーザー、IP、時刻ごとのテストを実行可能
- Secure by Design の原則により、ファイアウォールを攻撃から確実に保護

SOPHOS

- RMM/PSA 統合のすべての機能向けの構成 API
- クラウドベースの NDR インテグレーションによって、アクティブアドバーサリーの検知を強化
- すべてのファイアウォールに ZTNA ゲートウェイが統合され、どこからでもアプリケーションへの安全なアクセスを簡単に実現
- クラウドベースの管理およびレポート機能を提供する Sophos Central は複数のファイアウォールをサポートし、すべてのソフォスの IT セキュリティ製品に対応するグループポリシー管理と一元的なコンソールを提供
- 簡単で合理化されたセットアップウィザードにより、数分で導入可能
- 新しいファイアウォール向けの Sophos Central のゼロタッチ導入とゼロタッチ設定
- Sophos MDR と XDR とのシームレスな統合

Base Firewall

一般的な管理

- 目的に合わせて構築された合理的なユーザーインターフェースと、一目で分かるルール機能と強制インジケーターを備えた大規模なルールセットに対応するファイアウォールルールの管理
- 管理者アクセス、ユーザーポータル、IPsec、SSL VPN、および WAF に対する 2 要素認証 (ワンタイムパスワード) のサポート
- GUI で利用できる高度なログとトラブルシューティングツール (パケットキャプチャなど)
- 2 台のデバイスをアクティブ / アクティブまたはアクティブ / パッシブモードでクラスタリングする高可用性 (HA) をサポートし、冗長化した同期リンクを複数サポートしながら、プラグアンドプレイで素早く HA を設定可能
- GUI からアクセス可能な完全なコマンドラインインターフェース (CLI)
- Azure AD との統合により、ロールベースの管理とシングルサインオンを実現
- SSL によるファームウェアの更新 (証明書ピン留めによるセキュリティの強化)
- ネットワーク、サービス、ホスト、時間帯、ユーザーとグループ、クライアント、サーバーの再利用可能で検索可能なシステムオブジェクト定義
- セルフサービスユーザーポータル
- 構成変更のトラッキング
- ゾーン別のサービスに対する柔軟なデバイスアクセス制御
- メールまたは SNMP トラップ通知オプション
- SNMP v3 (ハードウェア監視を含む) および Netflow/sFlow の監視
- Sophos Central によって一元的な管理をサポート (有効なサポート契約をしているお客様のみ利用可能)
- 設定のバックアップと復元：ローカル、FTP、またはメール経由で、オンデマンド、日次、週次、または月次で設定をバックアップ。 ハードウェアアプライアンスのアップグレード時にポートの再マッピングオプションも提供
- WAF、SMTP、TLS 構成、ホットスポットのサインイン、Web 管理コンソール、ユーザーポータル、キャプティブポータル、VPN ポータル、および SPX ポータルで Let’ s Encrypt 証明書をサポート
- サードパーティ統合のための API
- インターフェース名の変更
- Sophos Support のためのリモートアクセスオプション
- MySophos アカウントを使用したクラウドベースのライセンス管理

ファイアウォール、ネットワーク、およびルーティング

- ステートフルディープパケットインスペクションを実行するファイアウォール
- Xstream のパケット処理のアーキテクチャは、ストリームベースのパケット処理により、最高レベルの可視性、保護、パフォーマンスを提供
- Xstream TLS インスペクションは、高性能、ダウングレードなしの TLS 1.3 のサポート、ポートに依存しない、エンタープライズレベルのポリシー、独自のダッシュボードの可視性、および互換性のトラブルシューティングを提供
- Xstream DPI エンジンが、単一の高パフォーマンスエンジンを備えた IPS、AV、Web、アプリ制御、および TLS インスペクションのストリームスキャン保護を提供
- Xstream ネットワークフローの FastPath がポリシーを利用して、信頼されるアプリケーショントラフィック、IPSec VPN トラフィック、TLS 暗号化トラフィックの処理をインテリジェントかつ自動的に高速化
- ユーザー、グループ、時間、またはネットワークベースのポリシー
- ユーザー / グループ別のアクセス時間ポリシー
- ゾーンやネットワーク全体、あるいはサービスタイプ別にポリシーを適用

- ゾーン分離とゾーンベースのポリシーをサポート
- LAN、WAN、DMZ、ローカル、VPN、Wi-Fi のデフォルトゾーン
- LAN または DMZ 上のカスタムゾーン
- カスタマイズ可能な NAT ポリシー (IP マスカレード、フルオブジェクトのサポート) により、複数のサービスを単一のルールの元でリダイレクトまたは転送可能であり、便利な NAT ルールウィザードにより、複雑な NAT ルールであっても数回クリックするだけですばやく簡単に作成可能
- グローバルで高度なフリーテキスト検索により、すべてのルールにネットワークオブジェクトの定義を再利用
- フラッド攻撃対策：DoS、DDoS、ポートスキャンのブロック
- GeoIP に基づき国別にブロック
- ルーティング：スタティック、マルチキャスト (PIM-SM)、ダイナミック：RIP、BGP、OSPFv3 (IPv6) BGPv6
- スタティックルートのクローンを作成し、オンまたはオフに切り替え、ダイナミック BGP ルートを OSPFv3 に再分配。ブラックホールルートオプションを利用し、ロードバランシングのために ECMP (等価コスト複数経路) を利用
- アップストリームプロキシ対応
- IGMP スヌーピングを使用したプロトコルに依存しないマルチキャストルーティング
- STP 対応のブリッジングと ARP ブロードキャスト転送
- VLAN DHCP 対応とタグ付け
- VLAN ブリッジのサポート
- ジャンボフレームのサポート
- 物理インターフェースの有効化 / 無効化
- ワイヤレス WAN のサポート (仮想環境では不可)
- 802.3ad インターフェースのリンクアグリゲーション
- DNS、DHCP、および NTP の完全な構成
- ダイナミック DNS (DDNS)
- IPv6 Ready Logo Program 承認証明書
- IPv6 DHCP プレフィックス委任
- IPv6 トンネリングのサポート。 IPsec を介した 6in4、6to4、4in6、および IPv6 Rapid Deployment (6rd) に対応

Xstream SD-WAN

- Xstream SD-WAN プロファイルは、VDSL、DSL、ケーブル、LTE/ セルラー、MPLS などの複数の WAN リンクオプションをサポート
- パフォーマンスベースの SLA では、ジッター、遅延、またはパケット損失に基づき、最適な WAN リンクを自動的に選択
- 重み付きラウンドロビンやセッション永続戦略を使用して、複数の SD-WAN リンク間で SD-WAN のロードバランシング
- ゼロインパクト再ルーティングは、リンクパフォーマンスがしきい値を下回り、パフォーマンスのより優れた WAN リンクに移行した時にアプリケーションセッションを維持
- SD-WAN モニタリンググラフにより、すべての WAN リンクの遅延、ジッター、パケット損失をリアルタイムに把握
- SD-WAN IPsec トンネルトラフィックの Xstream FastPath アクセラレーション
- Synchronized Security の機能の 1 つである Synchronized SD-WAN は、ソフォスが管理するエンドポイントと Sophos Firewall 間で Synchronized Application Control の情報を共有することで、アプリケーション識別の明瞭性と信頼性をさらに向上
- ファイアウォールルールやポリシーベースのルーティングにより、最適なリンクを介してアプリケーションをルーティング
- IPsec や SSL VPN などの堅牢な VPN に対応
- ルーティング機能を備えた独自の RED レイヤー 2 トンネル

基本的なトラフィックシェーピングおよびクオータ

- ネットワークまたはユーザーベースの柔軟なトラフィックシェーピング (QoS) (Web Protection サブスクリプションに含まれる拡張 Web およびアプリトラフィックシェーピングオプション)
- アップロード / ダウンロード、総トラフィックを基準とする、周期的 / 非周期的なユーザーベースのトラフィッククオータを設定
- リアルタイムでの VoIP 最適化
- DSCP マーキング

セキュアワイヤレス

- ソフォスのワイヤレスアクセスポイント (APX シリーズのみ) をプラグアンドプレイで簡単に導入でき、ファイアウォールのコントロールセンターに自動的に表示
- 内蔵ワイヤレスコントローラーにより、AP や無線クライアントを一元的に監視および管理可能
- クライアントの隔離オプションを使用して、LAN、VLAN、または個別のゾーンに AP をブリッジ
- 隠し SSID を含む複数の SSID を無線ごとにサポート
- WPA2 パーソナルやエンタープライズなど、さまざまなセキュリティおよび暗号化標準に対応
- チャネル幅の選択オプション

- IEEE 802.1X (RADIUS 認証) に対応し、プライマリおよびセカンダリサーバーをサポート
- 802.11R (高速移行) のサポート
- (カスタム) バウチャー、今日のパスワード、利用規約 (T&C) の合意のためのホットスポットのサポート
- ウォールドガーデンオプションによるワイヤレスゲストインターネットアクセス
- 時間帯ベースのワイヤレスネットワークアクセス
- サポートされている AP を使用したワイヤレスリピートおよびブリッジングメッシュネットワークモード
- 自動チャネル選択のバックグラウンド最適化
- HTTPS ログインのサポート

認証

- Synchronized User ID は、Synchronized Security を利用して、Active Directory サーバーやクライアントにエージェントを設置することなく、ソフォスのエンドポイントとファイアウォールの間で、現在ログインしている Active Directory ユーザー ID を共有
- 認証方法：Active Directory、eDirectory、RADIUS、LDAP および TACACS+
- Active Directory SSO、STA、SATC のためのサーバー認証エージェント
- シングルサインオン：Active Directory、eDirectory、RADIUS アカウンティング
- Webadmin コンソールへの管理者アクセスに対して、Azure AD のシングルサインオンを使用
- ユーザーがキャプティブポータル経由でウェブアクセスを認証するために、Azure AD のシングルサインオンを使用
- HSTS を強制した状態での透過的な AD シングルサインオンにより、Kerberos および NTLM ハンドシェイクを HTTP または HTTPS 経由で実現
- Azure AD グループのインポートと RBAC のサポート
- Windows、Mac OS X、Linux 32/64 対応のクライアント認証エージェント
- ブラウザ SSO 認証：透過型、プロキシ認証 (NTLM)、Kerberos
- ブラウザキャプティブポータル
- iOS および Android の証明書認証
- IPsec、SSL、L2TP、PPTP の認証サービス
- Active Directory と Google G Suite を使用する環境での Google Chromebook 認証のサポート
- Google Chromebook を使用した、LDAP クライアント経由での Google Workspace 統合
- API ベースの認証

ユーザーセルフサービスと VPN ポータル

- SNMP v3 (ハードウェア監視を含む) および Netflow/sFlow の監視
- Sophos Authentication Client のダウンロード
- SSL リモートアクセスクライアント (Windows) と構成ファイル (他の OS 向け) のダウンロード
- ホットスポットのアクセス情報
- ユーザー名とパスワードの変更
- 個人のインターネット利用状況の表示
- 隔離されたメッセージへのアクセスと、ユーザーベースの送信者ブロック / 許可リストの管理 (Email Protection が必要)

基本的な VPN オプション

- サイト間 VPN：SSL、IPsec、256 ビット AES/3DES、PFS、RSA、X.509 証明書、事前共有キー
- Sophos RED サイト間 VPN トンネル (堅牢で軽量)
- IPsec トンネルトラフィックの Xstream FastPath アクセラレーション (サイト間およびリモートアクセスの両方)
- AWS VPC のインポート、監視、管理ツール
- L2TP および PPTP
- トラフィックセレクターによるルートベースの VPN
- リモートアクセス :SSL、IPsec、iPhone/iPad/Cisco・Android VPN クライアントに対応
- IKEv2 のサポート
- RBVPN、PBVPN、およびリモートアクセス VPN における IPsec 接続のステートフル HA フェイルオーバーにより、HA フェイルオーバー時でもセッションを失うことなく接続を維持
- SNMP を介した IPsec VPN トンネルステータスの監視
- ユニークな事前共有鍵 (PSK) および DH グループ 27-30 / RFC6954 に対応した高度な IPsec サポート
- Windows 用の SSL クライアントと、ユーザーポータルからの構成のダウンロード

Sophos Connect クライアント

- 認証 : 事前共有鍵 (PSK)、PKI (X.509)、トークン、および XAUTH
- Entra ID (Azure AD) シングルサインオンをサポート
- リモート接続ユーザーに対して、Synchronized Security と Security Heartbeat を有効化
- 最適なトラフィックルーティングを実現するインテリジェントなスプリットトンネリング
- NAT トラバーサルをサポート
- 接続状況をグラフィカルに表示するクライアントモニター
- Mac (IPsec) および Windows (SSL/IPsec) クライアントサポート

Network Protection

侵入防御 (IPS)

- 高性能な次世代 IPS ディープパケットインスペクションエンジン、ファイアウォールルールを基準として適用可能な選択的な IPS パターンにより、最高クラスのパフォーマンスと保護を実現
- 数千のシグニチャ
- 詳細なカテゴリ選択
- カスタム IPS シグニチャに対応
- IPS ポリシースマートフィルタにより、新しいパターンが追加されると自動的に更新される動的なポリシーを有効化

Active Threat Response (アクティブな脅威対応) と Security Heartbeat™

- Active Threat Response は、Sophos-X Ops の脅威フィードを通じて特定された APT やその他の脅威を自動で監視およびブロックし、ボットやアクティブアドバーサリーが悪意のある送信先にアクセスを試みる行動に対して、マルチレイヤーの DNS、AFC、ファイアウォール検知を活用した高度な脅威対策を提供します。
- Sophos Firewall で Xstream Protection が有効になっていて、Sophos MDR/XDR と組み合わせて使用している場合は、ソフォスまたは顧客 / パートナーの SOC アナリストが公開した MDR/XDR の脅威フィードによって特定された脅威も、Active Threat Response により自動的に監視およびブロックされます。
- また、業界、業種、各国のサードパーティの脅威インテリジェンスソースから提供される脅威フィードにも Xstream Protection を通じて対応でき、これらのフィードで検知される脅威も Active Threat Response により自動的に監視およびブロックされます。
- Sophos Synchronized Security Heartbeat は、Active Threat Response およびその関連する脅威フィードによって特定される脅威指標と一致する感染デバイスを即座に検知し、赤色のハートビートのステータスでフラグを立てます。ハートビートステータスは、ソフォスが管理するエンドポイントによっても監視され、ファイアウォールと共有されます。このステータスには、デバイスのホスト名、ログインユーザー名、実行中のプロセス、インシデントの件数、感染が検知された時刻などの詳細が含まれます。
- ソフォスのセキュリティハートビートのステータスは任意のファイアウォールルールに関連付けることが可能です。感染したデバイスはネットワークリソースや特定セグメントへのアクセスが自動的に制限され、脅威がクリーンアップされるまでそのステータスが維持されます。
- さらに、Sophos Firewall は、感染したエンドポイントが検知された際に自動でラテラルムーブメントを防止し、ソフォスが管理しているネットワーク上のすべての正常なエンドポイントに対して、感染したデバイスからの通信を拒否するよう通知します。これにより、同一 LAN セグメント内であっても、感染したデバイスは完全に遮断されます。

SD-RED デバイス管理

- すべての SD-RED デバイスの一元管理
- 構成なしで、クラウドベースのプロビジョニングサービスから自動設定
- X.509 デジタル証明書と AES 256 ビット暗号を使用した安全な暗号化トンネル
- 仮想イーサネットにより、ロケーション間のすべてのトラフィックを信頼性の高い方法で転送
- DHCP および DNS サーバー構成を一元的に定義して、IP アドレスを管理
- 一定期間使用されていない SD-RED デバイスの認証をリモートから解除
- トンネルトラフィックの圧縮
- VLAN ポート構成オプション

クライアントレス VPN

- RDP、SSH、Telnet、VNC に対応するソフォス独自の暗号化された HTML5 のセルフサービスポータル

Web Protection

Web の保護と制御

- ストリーミング DPI Web 保護、または明示的なプロキシモードのインスペクション
- 明示的なプロキシモードでは、同じソース IP 上で複数ユーザーに接続ごとの認証をサポート

- Advanced Threat Protection の強化
- SophosLabs が提供する 92 のカテゴリにおよぶ数百万のサイトに対応する URL フィルタデータベース
- ユーザー / グループ別のネットサーフィンのクオータ時間ポリシー
- ユーザー / グループ別のアクセス時間ポリシー
- マルウェアスキャン：HTTP/S、FTP、および Web ベースのメールのあらゆる形態のウイルス、Web マルウェア、トロイの木馬、およびスパイウェアをブロック
- JavaScript エミュレーションによる高度な Web マルウェアからの保護
- 最新の脅威情報をクラウド上でリアルタイムに検索する Live Protection
- 独立した第 2 のマルウェア検知エンジン (Avira) によるデュアルスキャン
- リアルタイムまたはバッチモードスキャン
- ファーミングからの保護
- O365 のテナント制限を強化
- SSL プロトコルトンネリングの検知と強制
- 証明書の検証
- ハイパフォーマンスな Web コンテンツキャッシング
- エンドポイントアップデートの強制キャッシュ
- MIME タイプ、拡張子、アクティブコンテンツタイプ (Activex、アプレット、Cookie など) によるファイルタイプのフィルタリング。
- ユーザー / グループ別の YouTube for Schools ポリシーの適用
- ポリシー (ユーザー / グループ) 別に主要な検索エンジンでセーフサーチを強制 (DNS ベース)
- Web キーワードによるモニタリングと強制的な措置により、キーワードリストに一致する Web コンテンツを記録、レポート、またはブロック可能。また、カスタムリストをアップロードするオプションも利用可能
- 不要と思われるアプリケーション (PUA) のブロック
- 教師やスタッフがブロックされたサイトやカテゴリに一時的にアクセスできるようにする Web ポリシーオーバーライドオプション。これは、完全にカスタマイズ可能で、特定のユーザーが管理可能
- 制限対象の Web カテゴリを閲覧しているすべてのユーザーを瞬時に警告 (5 分ごとに通知)

クラウドアプリケーションの可視化

- コントロールセンターのウィジェットには、クラウドアプリケーションにアップロードおよびダウンロードされたデータ量が、新規、承認済み、未承認、または許容として分類されて表示される
- シャドー IT の状況を一目で確認可能
- ユーザー、トラフィック、データの詳細を表示するドリルダウン機能
- トラフィックシェーピングポリシーへのワンクリックアクセス
- クラウドアプリケーションの使用状況をカテゴリやボリュームでフィルタリング
- クラウドアプリケーションの使用状況レポートをカスタマイズして、過去の利用状況を詳細にレポート可能

アプリケーションの保護と制御

- ソフォスが管理するエンドポイントとファイアウォールの間で情報を共有し、ネットワークのすべての未知の Windows および Mac アプリケーションを自動的に識別、分類、制御する Synchronized App Control
- 何千ものアプリケーションのパターンを使用したシグネチャベースのアプリケーション制御
- クラウドアプリケーションの可視化と制御によるシャドー IT の検知
- 新しいパターンが追加されると自動的に更新される動的なポリシーを有効にするアプリケーションコントロールスマートフィルタ
- マイクロアプリケーションの検知と制御
- カテゴリ、特性 (帯域幅や生産性への影響など)、テクノロジー (P2P など)、リスクレベルに応じたアプリケーション制御
- ユーザーまたはネットワーク単位でのアプリケーション制御ポリシーの強制

Web およびアプリケーションのトラフィックシェーピング

- Web カテゴリまたはアプリケーションによるトラフィックシェーピング (QoS) オプションを強化して、アップロード / ダウンロードまたはトータルトラフィックの優先度とビットレートを個別または総合的に制限または保証

DNS Protection

クラウドベースの DNS サービス

- ドメイン名解決サービス
- 高性能なクラウドベースの DNS サービス
- SophosLabs および AI を活用
- DNS ルックアップで悪意のある URL をブロック
- カテゴリごとに不要な Web サイトをブロックできる詳細なコンプライアンスコントロール
- Sophos Central から集中管理

NDR Essentials

Network Detection and Response

- クラウドベースの NDR
- AI の活用
- TLS を復号せずに、暗号化された脅威の通信を検知
- ドメイン生成アルゴリズムを検知
- 潜在的な脅威をスコア付けし、設定したしきい値を超過する脅威についてアラートを発行
- 詳細なレポート作成とログのサポート

Zero-Day Protection

動的なサンドボックス分析

- ソフォスのセキュリティ製品のダッシュボードに完全統合
- 実行ファイルおよび実行ファイルを含むドキュメント (.exe、.com、.dll、.doc、.docx、docm、.rtf、PDF など)、および上記のファイルタイプを含むアーカイブ (ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet など) を検査します。
- 積極的な挙動、ネットワーク、およびメモリ分析
- サンドボックス分析を回避する挙動の検知
- ディープラーニングを使用する機械学習テクノロジーにより、ドロップされたすべての実行可能ファイルをスキャン
- Sophos Intercept X のエクスプロイト防御機能とランサムウェア対策機能 (CryptoGuard) を搭載
- スクリーンショットを含む悪意のあるファイルの詳細レポートと、ダッシュボードからのファイル解放機能
- オプションのデータセンター選択機能と、ファイルの種類に基づく処理や、除外、分析結果に基づく処理など、柔軟なユーザーとグループのポリシーオプションを提供
- ワンタイムダウンロードのリンクをサポート

静的な脅威情報解析

- Web 経由でダウンロードされたアクティブコードを含むすべてのファイル、またはメールの添付ファイルとしてファイアウォール内に送信された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 (.exe、.com、.dll、.doc、.docx、docm、.rtf、PDF など)、および上記のいずれかのファイルタイプを含むアーカイブ (ZIP、BZIP、GZIP、RAR、TAR、LHA/LZH、7Z、Microsoft Cabinet など) が、脅威情報分析のために自動的に送信される
- ファイルは SophosLabs の膨大な脅威インテリジェンスデータベースと照合され、複数の機械学習モデルを用いて新規および未知のマルウェアを識別
- 分析されたファイルを表示するダッシュボードウィジェット、分析したファイルと分析結果の詳細なリスト、各機械学習モデルの結果をまとめた広範で詳細なレポートを利用可能

Central Orchestration

SD-WAN オーケストレーション

- SD-WAN と VPN のオーケストレーションは、最適なアーキテクチャ (ハブアンドスポーク、フルメッシュ、またはそれらの組み合わせ) を使用して、ネットワーク間のサイト間 VPN トンネルをウィザードベースで簡単かつ自動的に作成可能
- IPsec、SSL、RED VPN トンネルに対応 SD-WAN 機能とシームレスに統合され、アプリケーションの優先順位付け、ルーティングの最適化、複数の WAN リンクを活用した耐障害性とパフォーマンスを向上

Central Firewall Reporting Advanced

- 30 日分のクラウドデータを保存でき、カスタムレポートの保存、スケジュール設定、エクスポートなどの高度な機能を備えた、ファイアウォールの履歴レポートを作成可能

XDR と MDR の統合

- Sophos XDR および MDR を統合し、テレメトリおよび脅威インテリジェンスを供給して、脅威ハンティングや分析を支援
- ソフォスの Active Threat Response は、MDR および XDR のアナリストが提供する脅威フィードを活用し、ネットワークで進行している脅威を自動的に特定、ブロック、隔離
- Synchronized Security の IoC (侵害の指標) テレメトリは、脅威や、感染したユーザー、プロセス、デバイスに関する重要な情報を収集

Email Protection

メールの保護と制御

- SMTP、POP3、IMAP に対応するメールスキャン
- 特許取得済みの再発パターン検知 (Recurrent-Pattern-Detection) テクノロジーに基づくスパム発生モニタリング機能を搭載するレピュテーションサービス
- SMTP トランザクションにおけるスパムやマルウェアのブロック
- DKIM および BATV によるスパム対策
- スパムグレーリストと SPF (Sender Policy Framework) による保護
- メールアドレスの誤入力に対する受信者認証
- 独立した第 2 のマルウェア検知エンジン (Avira) によるデュアルスキャン
- 最新の脅威情報をクラウド上でリアルタイムに検索する Live Protection
- シグネチャとパターンの自動更新
- アウトバウンドリレーのスマートホストサポート
- 添付ファイルのファイルタイプ検知 / ブロック / スキャン
- サイズ超過メッセージの受け入れ、拒否、削除
- メール内のフィッシング URL の検知
- 定義済みのコンテンツスキャンルールを使用することも、詳細なポリシーオプションと例外を使用し、さまざまな条件に基づいて独自のカスタムルールを作成することも可能
- SMTP、POP、IMAP の TLS 暗号化をサポート
- すべての送信メッセージに自動的に署名を追加
- メールアーカイバー
- 各ユーザーが、ブロックおよび許可する送信者リストをユーザーポータルで保守可能

メール隔離管理

- 隔離したスパムの処理および通知オプション
- 日付、送信者、受信者、件名、および理由で検索およびフィルタリングしてマルウェアおよびスパムを隔離可能。また、隔離したメッセージをリリースおよび削除するオプションも利用可能
- 隔離されたメッセージを表示およびリリースするセルフサービスユーザーポータル

メール暗号化と DLP

- 特許出願中の SPX 暗号による一方向性メッセージの暗号化
- 受信者による自己登録 SPX パスワード管理
- SPX のセキュアな返信に添付ファイルを追加
- 完全に透過的で、追加のソフトウェアやクライアントが不要
- メールと添付ファイルに機密データが含まれていないかどうか自動スキャンする DLP エンジン
- SophosLabs が管理する PII、PCI、HIPAA などの機密データタイプのコンテンツコントロールリスト (CCL) をあらかじめパッケージ化

Web Server Protection

Web アプリケーションファイアウォール（WAF) の保護

- リバースプロキシ
- URL ハードニングエンジン。ディープリンクとディレクトリトラバーサルを防止
- フォームハードニングエンジン
- SQL インジェクション対策
- クロスサイト スクリプティング対策
- デュアル型のマルウェア対策エンジン (Sophos および Avira)
- HTTPS (TLS/SSL) 暗号化のオフロード
- 署名付きクッキー (デジタル署名に対応)
- パスベースのルーティング
- IP 地理情報ポリシーの適用
- 独自の暗号構成と TLS バージョンの適用
- HSTS および X-Content-Type-Options の適用
- Outlook Anywhere プロトコルのサポート
- サーバーアクセス時のフォームベース認証とベーシック認証のリバース認証 (オフロード)
- 仮想サーバーと物理サーバーの抽象化
- 統合型ロードバランサーによる訪問者の複数サーバーへの分散化
- 必要に応じて、個別のチェックを詳細な指定の元でスキップ
- ソースネットワークのリクエストまたは指定されたターゲット URL の照合
- 論理演算子 (AND/OR) のサポート

- さまざまな構成および非標準環境との互換性の問題をサポート
- Web アプリケーションファイアウォールのパフォーマンスパラメータを変更するオプション
- スキャンサイズ制限オプション
- 許可 / ブロックする IP 範囲の設定
- サーバーパスとドメインでのワイルドカードのサポート
- 認証用の接頭辞 / 接尾辞の自動追加

レポートとログ

Central Firewall Reporting

- 柔軟なカスタマイズオプションを利用可能な事前定義レポート
- Sophos Firewall のレポート : ハードウェア、ソフトウェア、仮想、およびクラウド
- 直感的なユーザーインターフェースにより、データをグラフィカルに表現
- レポートダッシュボードでは、過去 24 時間のイベントを一目で把握
- ネットワークアクティビティ、トレンド、潜在的な攻撃を簡単に特定
- ログを簡単にバックアップでき、監査で必要となる場合には迅速に取得可能
- 技術的な専門知識を必要としない簡素化された導入

Central Firewall Reporting Advanced

- 複数のファイアウォールの情報を集約したレポート
- カスタムレポートテンプレートの保存
- 定期的なレポート作成
- レポートを PDF、CFV、HTML 形式で出力
- 各ファイアウォールで最大 1 年分のデータを保管
- 脅威ハンティングのための MDR/XDR データレイクコネクタ

オンボックスのレポート機能

- 注 :Sophos Firewall のレポート機能は追加料金なしで利用できますが、各プロテクションモジュールのライセンスによっては個々のログ、レポート、ウィジェットの利用について料金が発生する場合があります。
- 数百種類のオンボックスレポートに加え、次のようなカスタムレポートオプションも利用可能。ダッシュボード (トラフィック、セキュリティ、ユーザー脅威指数)、アプリケーション (アプリケーションリスク、ブロックされたアプリ、Synchronized Apps、検索エンジン、Web サーバー、Web キーワード一致、FTP)、ネットワークと脅威 (Active Threat Response と脅威フィード、Security Heartbeat、IPS、ワイヤレス、ゼロデイ脅威対策)、VPN、メール、コンプライアンス (HIPAA、GLBA、SOX、FISMA、PCI、NERC CIP v3、CIPA)。
- 現在のアクティビティモニタリング：システムヘルス、ライブユーザー、IPsec 接続、リモートユーザー、ライブ接続、ワイヤレスクライアント、隔離、DoS 攻撃
- ジッター、遅延、パケット損失の SD-WAN リンクパフォーマンスモニタリング
- レポートの匿名化
- レポートグループを設定して複数の受信者向けに、さまざまな頻度を設定してレポートを作成可能
- レポートを HTML、PDF、Excel (XLS) で出力。
- レポートブックマーク
- カテゴリ別にログ保管期間をカスタマイズ
- カラムビューと詳細ビューを備え、豊富な機能を搭載したログビューアを利用可能。このビューアでは、強力なフィルタと検索オプション、ハイパーリンク付きのルール ID 、データビューのカスタマイズが可能

集中管理 (SUM)

Sophos Central

- クラウドベースの管理およびレポート機能を提供する Sophos Central は複数のファイアウォールをサポートし、すべてのソフォスの IT セキュリティ製品に対応するグループポリシー管理と一元的なコンソールを提供
- グループポリシー管理により、オブジェクト、設定、およびポリシーを一度変更すると、グループ内のすべてのファイアウォールに自動的に同期可能
- タスクマネージャーでは、グループポリシーの変更に関する完全な履歴の監査証跡とステータスの監視が可能
- Sophos Central のバックアップとファームウェア管理では、各ファイアウォールの過去 5 回分の構成バックアップファイルが保存され、永続的な保存して簡単にアクセス可能
- Sophos Central のファームウェアの更新スケジュールにより、いつでも簡単に自動更新が適用可能
- ゼロタッチ展開では、Sophos Central で初期の構成を実行し、デバイスの起動時にフラッシュドライブからロードしてデバイスを自動的に Sophos Central に接続できるようにエクスポート可能

Zero Trust Network Access

- Sophos ZTNA ゲートウェイを統合し、ファイアウォールの内側にあるアプリケーションへのアクセスを保護
- Sophos Central から集中管理

Secure by Design (セキュリティを基盤とした設計)

- Sophos Firewall のセキュリティ状態のチェックでは、数十の設定とベストプラクティスを比較して潜在的なリスクを特定し、ドリルダウンで簡単に問題を解決
- ダウンタイムなしで脆弱性にパッチを適用するゼロタッチの OTA 自動ホットフィックス適用
- 強化されたカーネルにより、セキュリティ、パフォーマンス、拡張性を向上させ、厳格なプロセス分離とサイドチャネル攻撃への対策を実現
- ソフォスによるリモートからの整合性監視。内蔵 XDR センサーにより、不正な設定、悪意のあるコードの実行、ファイルの改ざんなど、システムの整合性をリアルタイムで監視し、攻撃を特定して迅速に対応
- 最高のセキュリティと拡張性を実現する新しいコントロールプレーンを備えた次世代 Xstream アーキテクチャ
- 信頼境界にあたる重要な領域やユーザー /VPN ポータルをコンテナ化して隔離
- Sophos Central による暗号化され安全な一元管理により、リモートの管理者アクセスが不要
- すべてのシステムに多要素認証を適用し、認証情報の窃取やブルートフォース攻撃から保護
- より安全なリモートアクセスとアプリケーションの保護のための統合 ZTNA ゲートウェイ
- 導入時から安全性を確保し、厳格なアクセス制御を含むセキュリティのベストプラクティスを確実に実装

サブスクリプション別の Sophos Firewall の機能概要

	Xstream Protection Bundle					別売				
	Standard Protection Bundle					別売				
	Base Firewall	Network Protection	Web Protection	DNS Protection	バンドル専用の機能	Zero-Day Protection	Central Orchestration	Central Firewall Reporting Adv.	Email Protection	Web Server Protection
一般的な管理 (HA を含む)	✓									
Xstream アーキテクチャ	✓									
ファイアウォール、ネットワーク、およびルーティング	✓									
Xstream SD-WAN	✓									
基本的なトラフィックシェーピングおよびクオータ	✓									
セキュアワイヤレス	✓									
認証	✓									
セルフサービスユーザーポータル	✓									
VPN（IPsec、SSL など）	✓									
RED サイト間 VPN	✓									
Sophos Connect VPN クライアント	✓									
侵入防御 (IPS)		✓								
アクティブな脅威対応										
Sophos X-Ops 脅威フィード		✓								
MDR/XDR 脅威フィード					✓					
サードパーティの脅威フィード					✓					
Synchronized Security Heartbeat		✓								
SD-RED デバイス管理		✓								
クライアントレス VPN		✓								
アプリケーション同期と制御			✓							
Web の保護と制御			✓							
アプリケーションの保護と制御			✓							
クラウドアプリケーションの可視化			✓							
Web およびアプリケーションのトラフィックシェーピング			✓							
DNS セキュリティとコンプライアンス				✓						
NDR Essentials					✓					
動的なサンドボックス分析						✓				
脅威情報の解析						✓				
SD-WAN オーケストレーション							✓			
Central Firewall Reporting のデータ *		7 日間	7 日間	7 日間	7 日間	7 日間	30 日間	最大 1 年間	7 日間	7 日間
CFR アドバンスド機能							✓	✓		
メールの保護と制御									✓	
メール隔離管理									✓	
メール暗号化と DLP									✓	
Web アプリケーションファイアウォールの保護										✓
オンボックスのログ / レポート	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sophos Central での管理 **		✓	✓	✓	✓	✓	✓	✓	✓	✓
ZTNA ゲートウェイ **		✓	✓	✓	✓	✓	✓	✓	✓	✓
Secure by Design	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

注：一部の機能は (オンボックスレポート、デュアル AV スキャン、WAF AV スキャン、メールメッセージ転送エージェント (MTA) 機能)、XGS 87 および XGS 88 モデルではサポートされません。

MSP のライセンスオプションは、上記とは若干異なります

* データの保存期間は平均的なネットワーク使用量に基づく推定値であり、実際のログデータの量によって変動します。ストレージサイズ見積もりツール。

** すべてのバンドル、サポート、または保護サブスクリプションに含まれます。Base License のみをご利用のお客様が、これらの機能を利用するには、サポート (Enhanced Support または Enhanced Plus Support) の追加が必要となります。

サブスクリプション別の Sophos Firewall の機能概要

	Enhanced Support (Standard Protection および Xstream Protection バンドルに含まれます)	Enhanced Plus Support (Enhanced Support からのアップグレードとして利用可能)
24 時間 365 日対応のマルチチャネルサポート (電話、Web ポータル、チャット) を提供。リモートサポートのほか、ナレッジベースやサポートフォーラムへアクセスしてセルフサービスで問題を解決することも可能。	✓	✓
ファームウェアダウンロード、アップデート、メンテナンスリリース **	✓	✓
Sophos Central の管理、レポート機能、ZTNA ゲートウェイ	✓	✓
アクティブデバイスのハードウェアアドバンス交換	✓	✓
パッシブ HA デバイスのハードウェアアドバンス交換 *		✓
SD-RED/APX デバイスのハードウェアアドバンス交換		✓
VIP アクセス (シニアエンジニアへ通話を転送)		✓
リモートコンサルティング (1 年間で 2 ～ 8 時間)		✓

* パッシブ HA デバイスを Advanced RMA の対象として有効にするには、アクティブデバイスに Enhanced Plus Support ライセンスが必要です。
詳細については、ソフォスサポートサービスガイドを参照してください。
** 注：ファームウェアアップデートを受けるためには、購入した個別のモジュールにサポートを追加する必要があります。

ソフォス株式会社営業部
Email: sales@sophos.co.jp

2025-12-15 JA (DD)