

SOPHOS

XG Firewall の 教育機関向け販促資料

教育機関向けに設計しました

XG Firewall は、教育機関向けに最適化されたソリューションであり、卓越した可視性、セキュリティと制御力、ユニークな脅威の検知とレスポンス機能を提供します。ネットワーク上のアクティビティの監視や、ファイアウォールの管理、脅威への対応を行えるパワフルな機能を提供します。



教育機関向けに設計

XG Firewall は、教育機関が直面する課題を克服できるように、教育機関向けに考案された機能を提供します。

強力な Web フィルタリングポリシー

XG Firewall には、通常、大企業向けの高額な Web フィルタリング製品にしか搭載されることのない、直感的に設定できる強力な Web ポリシーモデルが装備されています。複数のユーザーベースおよびグループベースのカスタムポリシーを簡単に管理できます。さらに、CIPA や教育現場にふさわしくないインターネットの利用に対応するビルトインのポリシーも搭載されています。これは、導入後すぐに使い始めることができ、個別の用途に応じて簡単にカスタマイズすることも可能です。また、SafeSearch、YouTube、ファイルのダウンロードも、各ポリシーのオプションできめ細やかに制御できます。

子供の安全とコンプライアンスの徹底

米国における児童インターネット保護法 (CIPA: Child Information Protection Act) や、英国における子供の保護を目的とする Safeguarding and Prevent Duty of Care Guidelinesをはじめ、子供が安全にインターネットを利用するための同様のコンプライアンスが多く、多くの国で義務付けられています。こうした活動は善意的である一方、多くの企業にとって困難な課題にもなり得るものです。XG Firewall には、手早く簡単に組織のコンプライアンスを徹底するための機能とポリシーの設定項目が備わっています。CIPA や、教育現場にふさわしくないものなど事前に定義された活動に対し、ビルトインのポリシー、およびセーフサーチ、YouTube の制限機能、キーワードフィルタリングなども搭載されており、児童が安全にインターネットを利用できる環境を整えます。

コンテキストアウェアなキーワードフィルタリング

XG Firewall を導入すれば、潜在的な問題行動を早期に見つけ出すことが可能です。XG Firewall では、いじめ、自傷行為、過激な思想などに関連するキーワードのリストに基づいて、ログの記録や、監視、ポリシーの適用を行うことができます。定期的にレポートを出力し、危険性の高い学生を特定して、それらの学生がいつどこで投稿しているか、どのサイトを閲覧しているかなど、詳細なアクティビティを確認できるのも大きな特長です。

危険性の高い学生を可視化

ソフォス独自の「ユーザー脅威指数: User Threat Quotient (UTQ)」は、ユーザー (学生や教職員) の挙動を認識したうえで対応につなげることでできる知見を提供します。XG Firewall は、各学生のネット閲覧の習慣やアクティビティと、高度な脅威の攻撃パターンや閲覧履歴との関係を比較して、インターネット上でリスクにつながる行為を行っているユーザーを特定します。これにより、自分自身やネットワークに危険をもたらす行為を行っている学生に対して直ちに対策を講じ、対応することが可能です。レポートの自動送信により、教師や保護監督者との間で、危険な学生に関する情報を常に共有することもできます。

最高レベルの脅威対策

XG Firewall には、ハッキングや攻撃を徹底的に阻止するのに必要な最新の脅威対策テクノロジーがすべて搭載されています。Sandstorm Sandboxing は、次世代型エンドポイント製品「Intercept X」の最新のディープラーニング技術を駆使し、インターネットやメール経由で受信するすべてのファイルの挙動を、安全なサンドボックス内でチェックし、悪意がある動作を検知します。ソフォスの侵入防止システム (IPS) は、業界トップクラスの評価を獲得しており、ネットワークに存在する脆弱性を狙った攻撃やハッキングの試みを検知・防御します。さらに、Web プロテクション機能で、JavaScript によるエミュレーションを実行し、クリプトジャッキングなど、不正な Web サイトに潜む脅威を検出します。

Chromebook のサポート

XG Firewall は、Chromebooks をはじめとした幅広い認証方式 (その他ディレクトリサービス、クライアントベース、クライアントレスなど) に対応しています。手軽にインストールできるエージェントで、すべての Chromebook ユーザーに詳細なユーザーベースポリシーを適用したり、レポートを生成したりすることができます。

Synchronized Security

XG Firewall は、Sophos Intercept X と連携し、ソフォス独自の機能「Synchronized Security」を有効にして、ネットワークとエンドポイントの両方に究極の保護機能を提供します。Security Heartbeat™ により、ソフォスのマネージドエンドポイントとファイアウォールがリアルタイムにセキュリティ情報を共有し、XG Firewall が感染システムを自動的に隔離して脅威の拡散を防ぎます。また、暗号化や回避技術により、これまで検出できなかったネットワーク上のアプリケーションもすべて検出できるようになります。このような可視性や、保護性能、対応力の追加機能は、Sophos Synchronized Security を導入した場合のみに得られるメリットです。



パワフル、シンプル、そして低価格

Sophos XG Firewall は、教育機関が必要とするすべての可視性、セキュリティ、制御機能を備えているだけでなく、日々の管理とレポーティングが簡単なうえ、価格もきわめて手頃です。

Xstream アーキテクチャ

XG Firewall は、パフォーマンスを低下させることなく、隠れたリスクを特定、脅威から保護、インシデントに対応する新しいアプローチを提供します。Xstream Architecture for XG Firewall は、極めて高いレベルの可視性、保護、およびパフォーマンスを提供する独自のパケット処理アーキテクチャを採用しています。

究極のセキュリティと制御機能

XG Firewall は、企業ネットワークを最新のランサムウェアや高度な脅威から防御するのに必要な高度なテクノロジーをすべて備えています。また、業界でもっとも強力な Web フィルタリング ポリシーと保護機能を搭載し、セットアップとローカルもしくはクラウドでの管理が簡単な点も大きな特徴です。

ユニークな脅威レスポンス機能

XG Firewall は、ネットワーク上の感染源を完全に特定し、他のネットワークリソースへのアクセスを自動的に制限できる唯一のネットワークセキュリティソリューションです。これを可能にしているのが、ソフォスのマネージドエンドポイントと XG Firewall の間でテレメトリとヘルスステータスを共有するユニークな Sophos Security Heartbeat です。

SD-WAN で接続して節約

ユーザーの区域から学校へ接続するのは大きな試みとなる場合があります。そういうわけで、ソフォスは SD-WAN (Software-Defined Wide Area Networking) を XG Firewall に統合しました。SD-WAN を使用することで、地域内のすべての学校や本部を MPLS (Multi-Protocol Label Switching) よりもはるかに低価格で接続できます。機密性の高い受講者およびスタッフの情報をサイト間で安全に送信します。ネットワーク上の教育テクノロジーやアプリケーションの変化に対応 Dropbox Education、G Suite、ClassDojo などのクラウドアプリケーションがあればどこでも教室や管理オフィスで、一貫したパフォーマンスと可用性を実現できます。

抜群のコストパフォーマンスと手頃な価格

XG Firewall は、最高レベルのパフォーマンスとセキュリティの効率性を追求し、RoI を最大化するよう設計されています。第三者機関の業界アナリストによるトップレベルの性能テストで、常に高い評価を獲得しており、単一のアプライアンスにこれほどの機能が集約されているファイアウォール製品は他にありません。

管理やレポーティングがシンプルに

XG Firewall は、ネットワークでの管理とレポーティングを容易にします。Sophos Central Firewall Management を使用すると、任意の場所から 1 つまたは複数の XG Firewall を管理できます。すっきりとしたデザインでさまざまな情報が載っているダッシュボードと、信号カラーの色分けにより、対応すべき問題がログインをしてすぐに一目で把握できるようになっています。Sophos Central Firewall Reporting は、アプリケーション、リスク、トレンド、ネットワークに影響を与える状況を即座に把握できるカスタムレポートを作成するツールを提供します。すべてクラウドで追加料金なしで利用できます。また、ソフォスの Web フィルタリング ポリシーには、ネットワークのコンプライアンスを管理するためのさまざまなオプションが用意されており、その操作性と制御力は業界随一です。教育現場のスタッフは、授業内容に応じて、Web ポリシーの除外を日々管理することさえできます。



購入方法

目的や用途に合わせて保護機能をお選びください。



ネットワーク保護

業界でもっとも高い評価を得ている侵入防止テクノロジー、ディープラーニング、高度な脅威対策テクノロジーで、最新の脅威を徹底的に阻止します。



Sandstorm プロテクション

ディープラーニング、エクスプロイト検知、CryptoGuard を統合し、最新のファイルベースの脅威を検知する、クラウドベースの次世代型サンドボックステクノロジーです。



Web プロテクション

キーワードによるコンテンツフィルタリング、セーフサーチ、YouTube の制御、アプリケーションの識別・制御により、強力な Web フィルタリングと保護を提供します。



Security Heartbeat™

ソフォスのマネージドエンドポイント製品と XG Firewall を相互連係させることにより、ネットワークに潜むセキュリティリスクを可視化、攻撃を防御、エンドポイントを自動隔離します。



メール対策

送受信メール (SMTP、POP) のスパム、フィッシング、データ流出対策に加えて、ポリシーベースのメール暗号化、データ流出防止 (DLP)、スパム対策を組み合わせたソフォス独自のオールインワンソリューションです。



Web Server Protection

Web サーバーや業務アプリケーションをハッカー攻撃から防御する一方、外部から接続するユーザーにはリバースプロキシ認証で、安全なアクセスを提供します。

Sophos XG Firewall バンドル

高い信頼性および優れた保護を低予算で提供するバンドルをご検討ください。

EnterpriseProtect Plus : 次世代型ファイアウォールのバンドルパッケージ。XG シリーズのハードウェアアプライアンスと Enhanced Support (拡張サポート) のほか、ネットワーク保護、Web プロテクション、アプリケーション制御、サンドボックス機能が含まれます。

TotalProtect Plus : すべての保護機能が含まれるバンドルパッケージ。XG シリーズのハードウェアアプライアンス、Enhanced Support (拡張サポート) のほか、ネットワーク保護から、サンドボックス機能、Web、メール、Web サーバーの保護などセキュリティスイート全般が含まれます。

30日間無償評価版

XG Firewall をお試しになる場合は、30日間無償試用にご登録いただくことで、製品のすべての機能をご利用いただけます。

ソフォス株式会社営業部
Email: sales@sophos.co.jp