DATASHEET

WATCHGUARD EPP

強力なエンドポイント保護プラットフォーム

サイバーセキュリティの課題

組織はあらゆるサイバー攻撃から身を守る必要がありますが、現在、エンドポイントはサイバー犯罪者の恰好の標的になっています。つまり、機密情報を扱い、企業ネットワークに内部／外部から接続するエンドポイントを保護・監視することが増々重要になってきています。

事実、昨年では350,000万件もの不正プログラムが日々新たに作成されています。ハッカーたちは、企業が貴重な資産を保管する脆弱なエンドポイントを標的にしています。理由としてはこれまで同様、金銭的価値があるからです。現在、マルウェアやランサムウェアは最も流行している脅威になっていますが、被害によるコストだけでなく、ビジネスの停止が大きな問題になっています。こうした状況により、企業は自社のセキュリティ体制を改善するための対策を強いられています。

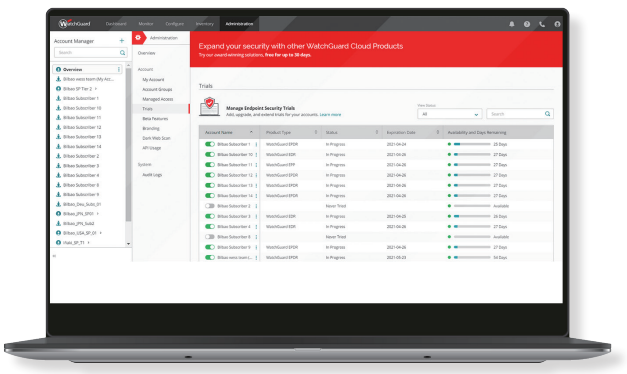
マルウェアやランサムウェアから企業を保護

マルウェアやランサムウェア、およびその他の脅威により、企業は益々危険に晒されており、攻撃による影響を軽減するための新たなアプローチが求められています。

WatchGuard EPPは効果的なクラウドネイティブのセキュリティソリューションであり、Windows、macOS、Linuxのデスクトップ、ラップトップ、サーバを始めとして、著名な仮想化システムやAndroidデバイスを対象に、次世代アンチウイルス機能を一元的に提供します。また、ネットワーク（ファイアウォール）、メール、Web、外部デバイスなど全てのベクターを網羅し、包括的に保護します。

WatchGuard EPPはマルウェア、ランサムウェア、および最新の脅威を防御する総合的なEPPテクノロジーを採用しています。例えば、最新の機械学習アルゴリズムを活用した巨大なレポジトリである、ウォッチガードの脅威インテリジェンスをリアルタイムにチェックし、迅速に不正な攻撃を検知します。

さらに、ハードウェアやソフトウェアを維持する手間がありません。軽量エージェントはエンドポイントのパフォーマンスに影響を及ぼすことなく、セキュリティ管理をシンプル化し、運用効率を高めることができます。



メリット

マルチプラットフォームセキュリティ

- 未知の高度な脅威に対するセキュリティを提供し、マルウェア、トロイの木馬、フィッシング、ランサムウェアを検知・防御します。
- ブラウザ、メール、ファイルシステム、およびエンドポイントに接続している外部のデバイスなど、あらゆる攻撃に対するセキュリティを提供します。
- PC/サーバにおける自動分析と駆除を行います。
- 振舞い分析により、既知／未知のマルウェアを検知します。
- クロスプラットフォームセキュリティを提供しており、Windowsシステム、Linux、macOS、Android、仮想環境（VMware、仮想PC、MS Hyper-V、Citrix）に対応しています。また、パーシスタントおよび非パーシスタントの仮想インフラ（VDI）に属するライセンスを管理します。

シンプルな管理

- 容易に維持することが可能で、ソリューションをホストするための特定のインフラは不要であり、IT担当者はより重要な業務に集中することができます。
- クラウドと通信することで、追加インストールを不要とし、リモートオフィスやユーザーを容易かつ迅速に保護することができます。
- 容易に実装可能で複数の実装方法があり、他社製品の自動アンインストールにより、サードパーティソリューションからの迅速な移行を実現します。
- 直感操作に優れたシンプルなWebベースの管理インターフェースを備えており、特に使用頻度の高い機能は素早く操作することができます。

パフォーマンスの影響を軽減

- 全ての運用がクラウドで実行されるため、エージェントにおけるネットワーク、メモリ、CPUの使用は最小限に抑えられています。
- 組織のインフラにおけるハードウェアのインストール、管理、保守が不要です。

一元化されたデバイスセキュリティ

企業ネットワーク上の全てのワークステーションやサーバに対するセキュリティと製品アップデートを一元管理します。単一のWebベースの管理コンソールにより、Windows、Linux、macOS、Androidデバイスを保護します。

マルウェアやランサムウェアに対する保護

振舞いやハッキング技術を分析し、既知／未知のマルウェア、ランサムウェア、トロイの木馬、フィッシングを検知・防御します。

高度な駆除

セキュリティ侵害の際に、高度な駆除ツールと疑わしいアイテムや削除されたアイテムを保存する検疫により、感染したコンピュータを感染前の状態に迅速に復元します。

また、管理者がリモートでワークステーションやサーバを再起動し、最新の製品アップデートがインストールされているようにすることができます。

リアルタイムモニタリング／レポート

包括的なダッシュボードと見やすいグラフにより、リアルタイムで詳細なセキュリティモニタリングが可能になります。

レポートが自動生成され、保護状況、検知内容、デバイスの不適切利用などが報告されます。

プロファイルのきめ細かい構成

ユーザープロファイルによって特定の保護ポリシーが割当てられ、ユーザーグループごとに最適なポリシーが適用されます。

デバイスを集中制御

各種のデバイス（フラッシュドライブ、USBモデム、Webカメラ、DVD/CDなど）の防御や、許可リストを作成したり、読み取り専用、書き込み専用、読み書き可能なアクセスの許可を設定したりすることで、マルウェアや情報漏えいを防ぎます。

迅速かつ柔軟にインストール

ダウンロードURLを記載したメールで保護機能を実装したり、あるいは配布ツール経由で指定したエンドポイントにサイレントに実装したりすることができます。MSIインストーラーはサードパーティツール（Active Directory、Tivoli、SMSなど）と互換性があります。

マルウェアフリーザー

マルウェアフリーザーは、検知されたマルウェアを7日間検疫し、誤検知の場合、影響を受けたファイルをシステムに自動で復元します。

ISO 27001とSAS 70コンプライアンスを 24時間365日遵守

WatchGuard EPPはWatchGuard Cloudにホストされ、包括的なデータ保護を保証します。ウォッチガードのデータセンターはISO 27001とSAS 70の認定を受けており、コストが発生するサービス停止やマルウェア感染を防ぎます。

WatchGuard EPP がサポートするプラットフォームとシステム要件

サポートしているオペレーティングシステム：Windows（Intel と ARM）、macOS（Intel と ARM）、Linux、Android

互換性のあるブラウザ：Google Chrome、Mozilla Firefox、Internet Explorer、Microsoft Edge、Opera

ウォッチガードの統合型セキュリティプラットフォーム


ネットワーク
セキュリティ


セキュアWi-Fi


多要素認証


エンドポイント
セキュリティ

詳細についてはセールス担当者にお問い合わせいただくか、
https://www.watchguard.co.jpをご覧ください。

ウォッチガード・テクノロジー・ジャパン株式会社

〒106-0041 東京都港区麻布台 1-11-9 BPR プレイス神谷町 5 階
TEL：03-5797-7205　FAX：03-5797-7207　www.watchguard.co.jp