DATASHEET

WATCHGUARD PATCH MANAGEMENT（パッチ管理）

OSやサードパーティアプリケーションにおける脆弱性管理のリスクと複雑性を軽減

Ponemon Institute[1] によると、サイバー攻撃の被害者の57%がパッチを適用していれば攻撃を回避できたと回答しており、37%が攻撃を受ける以前から脆弱性について認識していたと報告しています。

WannaCryやPetyaといったランサムウェア攻撃は、OSに対するパッチ管理ポリシーが不十分な企業に甚大な被害を及ぼしましたが、それだけではありません。脆弱性の86%はパッチが適用されていないJava、Adobe、Firefox、Chrome、Flash、OpenOfficeといったサードパーティのアプリケーションに起因しています。

脆弱性：潜在的なリスク

脆弱性の悪用は、未だにセキュリティ攻撃における最も多い手法となっています。WannaCry、Petya、BlueKeepなど、世界中で大混乱を引き起こした悪名高い事件は、記憶に新しいところです。

攻撃のほとんどは既知の脆弱性を悪用したものであり、未知の脆弱性（ゼロデイ攻撃）を突いた攻撃はほんの一部です。

また、デジタルトランスフォーメーションによって、常にアップデートが必要となるユーザー、デバイス、システム、そしてサードパーティアプリケーションが増え続けており、攻撃対象領域が増えています。

脆弱性の管理は、一般的に最低以下の3つの運用上の課題を抱えています：

- 脆弱性の発見には長い時間を要しますが、インシデント発生時には即時対応が必要になります。
- 企業の拠点は分散化が進み、従業員は常に企業ネットワークにつながっているとは限らず、オンプレミスの脆弱性管理ツールはこうした環境には対応していません。
- 一般的にパッチ管理機能を提供するセキュリティソリューションは、脆弱なエンドポイントの検知には対応しておらず、攻撃に対するレスポンスと軽減を早急に実践することがままなりません。

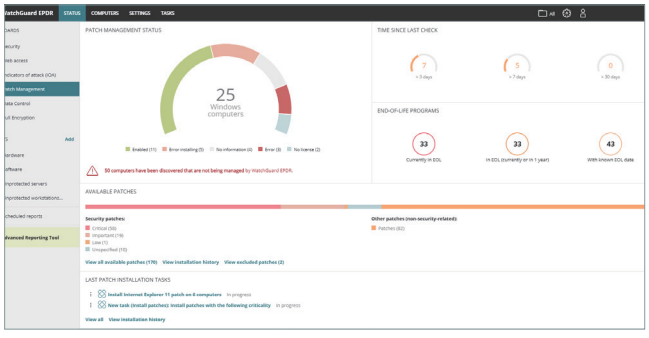


図1：パッチ管理の総合ステータス - メインダッシュボード

WATCHGUARD PATCH MANAGEMENT（パッチ管理）

WatchGuard Patch Management（パッチ管理）は、オペレーティングシステムやWindowsのワークステーションやサーバ上で稼働するサードパーティアプリケーションにおける脆弱性管理を容易に実現するソリューションです。攻撃対象領域を削減し、組織の防御および封じ込め能力を強化することができます。

このソリューションは、ウォッチガードのエンドポイントソリューションと完全に統合されているため、新たにエンドポイントエージェントや管理コンソールを追加する必要がありません。

また、ソフトウェアの脆弱性におけるセキュリティステータス、パッチの未適用、アップデート、サポートされていない（EOL）[2] ソフトウェアを一元的にリアルタイムで可視化し、ディスカバリからプランニング、インストレーション、モニタリングまで、パッチ管理全体のサイクルに対応したツールを提供します。

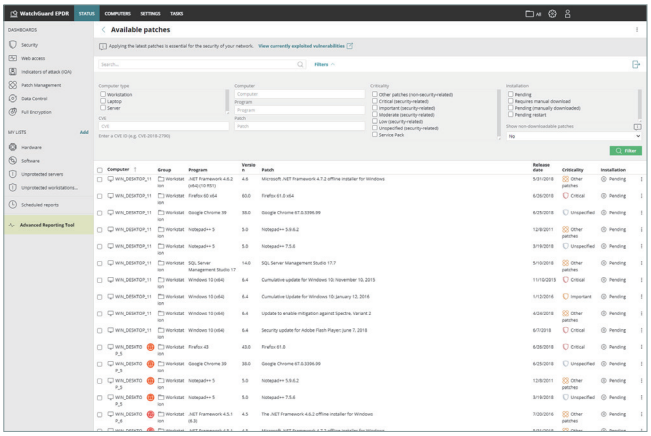


図2：有効なパッチ - パッチ管理

[1] Cost and consequences of gaps in vulnerability response（脆弱性対応におけるギャップがもたらすコストと結果）- Ponemon

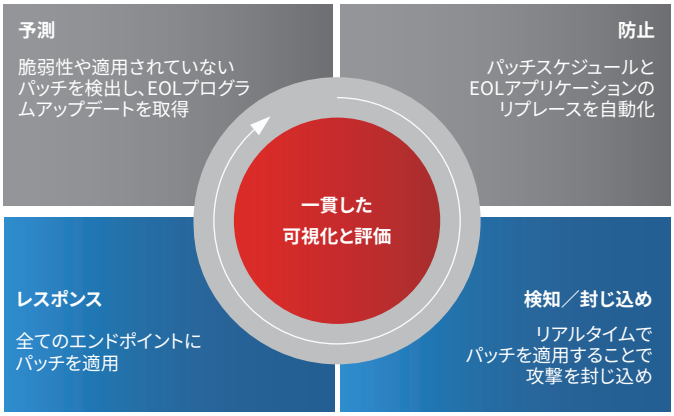
[2] EOL（End-of-Life）：耐用年数が経過し、セキュリティアップデートが受けられなくなった製品

特長

WatchGuard Patch Management（パッチ管理）は操作性に優れた一元ソリューションであり、以下の特長を備えています：

- オペレーティングシステムやアプリケーションのアップデートを監査、モニタリング、優先順位付けします。また、1つの画面に、組織における複数のシステムやアプリケーションの脆弱性、パッチ、適用されていないアップデートなど、最新のセキュリティステータスを集約し、可視化します。
- インシデントの発生を効率良く防ぎ、ソフトウェアの脆弱性がもたらす攻撃対象領域を削減します。操作性に優れたリアルタイムの管理ツールでパッチやアップデートに適宜適用することにより、脆弱性を悪用した攻撃を事前に防止することができます。
- Webコンソールからアップデートやパッチを迅速に適用することにより、脆弱性を悪用した攻撃の封じ込めと修復を実現します。感染したPCはネットワークから隔離し、攻撃の拡散を防止することができます。
- 運用コストを削減します：
  - 新たにエンドポイント専用のエージェントをインストールする必要もなく、その他のエージェントのアップデートも不要なため、容易な管理を実現します。
  - クラウドベースのコンソールよりリモートでアップデートできるため、パッチの作業を最小限に止めることができます。
  - 全ての脆弱性、未適用のアップデート、EOLアプリケーションを包括的かつ迅速に可視化します。
- 多くの規制に不可欠な説明責任の原則を遵守することにより、組織の管理下にある機密データを適切に保護するために、最適な技術的および組織的対策を講じることが可能になります。

WATCHGUARD PATCH MANAGEMENT（パッチ管理）
適応型セキュリティアーキテクチャ



「Designing an Adaptive Security Architecture for Protection from Advanced Attacks（高度な攻撃から身を守るための適応型セキュリティアーキテクチャの設計）」
- ガートナー社

主な機能

ディスカバリ：

- 全ての脆弱なPC、未適用のパッチ、サポートされていない（EOL）ソフトウェアに関する修復ステータスなどリアルタイム情報を一元ビューで表示
- 未適用のパッチおよびアップデートや、関連するセキュリティ勧告（CVE）の詳細情報を把握
- リアルタイムあるいは一定期間（3、6、12、24時間ごと）で有効なパッチを自動検索
- 不正を検知した際に未適用のパッチを通知
- 感染したPCやサーバを隔離し、パッチ適用後に隔離を解除

パッチやアップデートのプランニングとインストレーション作業：

- パッチを当てる際の重要度とソフトウェアの種類を設定
- 緊急時の一時的な実行や定期的な実行（日／時）をスケジューリング
- コンピュータの再起動を制御し、例外を設定
- 既存の設定と予期せぬ衝突を引き起こす可能性のあるパッチを、アンインストールするためにロールバックを実行

エンドポイントとアップデートステータスのモニタリング：

- ダッシュボードと実行リストを利用し、ハイレベルの詳細レポートを取得
- アップデートされたPCやアップデートが未適用のPCをリスト化

権限の異なるグループやロールに基づくきめ細かい管理：

- 脆弱なPC、パッチ、サービスパックに関してロールベースで可視化

アップデート、パッチ、ソフトウェアを一元的に制御：

- Windowsアップデートを無効化し、オペレーティングシステムのアップデートを集中管理
- バージョンやタイプごとに特定のパッチを除外
- 特定のソフトウェア（例：Java）を除外
- ダウンロードされたパッチをキャッシング

WatchGuard Patch Management（パッチ管理）の対応プラットフォームとシステム要件

WatchGuard EPDR、WatchGuard EDR、WatchGuard EPPと互換性があります

対応しているオペレーティングシステム： Windows

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

脆弱性対応のパッチ管理：
https://www.watchguard.com/wgrd-resource-center/vulnerabilities

対応しているサードパーティアプリケーション：
https://www.watchguard.com/wgrd-resource-center/patch-management

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　https://www.watchguard.co.jp　Email: jpnsales@watchguard.com