JCS
Japan Computer Services Inc.

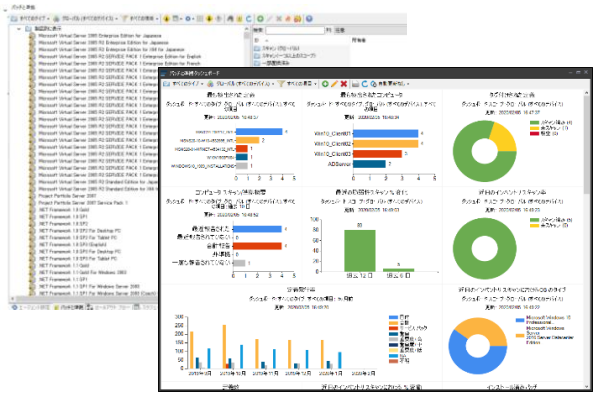
ivanti Patch for Endpoint Manager

PE 全てのエンドポイントのセキュリティ対策はパッチ適用から

■セキュリティを強化
一貫したポリシーを作成/自動化することで、モバイル、リモート、スリープなどの状態を問わず、あらゆる資産に対してパッチが適用されます。

■リスクを削減
様々なシステム上でOSおよびサードパーティ製アプリの脆弱性を検出して修正し、法律や規制に準拠するようにします。

■事業を常に継続
ユーザーデバイスの動作が遅くなるような問題を回避し、適切な条件のもとで夜間にパッチを施すことで、ユーザーへの影響を最小限に抑えることができます。



脆弱性パッチソリューションは、
次の3つの領域で有効にする必要があります。

1 , 脆弱性を評価し、最新のパッチコンテンツを活用してすぐに修正する

2 , パッチプロセスの自動化、管理、および最適化する

3 , パッチの失敗と、ユーザーおよびビジネスプロセスへの影響を最小限に抑える

様々なシステムが混在したクライアント機能を監視、評価、保護します

Patch for Endpoint Manager は、パッチのインストール元がソフトウェアかIvantiかその他の場所かを問わず、すべてのクライアントシステムにインストールされているすべてのパッチを瞬時に表示します。このソリューションは、業界標準の情報源を使用して脆弱性の評価も実行します。Microsoft Windows、Red Hat Linux、SYSE Linux、Apple Mac OS Xを実行中のシステム上でオペレーティングシステムとサードパーティ製アプリケーションの脆弱性を検出、修正します。さらに、HP-UXを実行中のシステムの脆弱性も検出、報告します。

オートメーション(自動化)とビジネスポリシーでさらに効率的なパッチ適用を支援します

Patch for Endpoint Managerは、パッチ管理と展開を自動化し、ポリシーに基づいてパッチ適用先、適用タイミング、適用頻度を詳細に管理することを可能にします。このソリューションのWake-on-WAN機能により、ネットワーク設定なく社内全体のマシンを起動できるため、パッチ適用成功率を上げ、自動化展開時間を短縮できます。複雑な手作業でのプロセスを自動化します。スケジュール設定、ポリシー、その他パッチ適用オプションを個別またはまとめて起動し、パッチ適用の取り組みの範囲と効果を最大限に拡大します。

コンプライアンスを強化し、クライアントシステムと収益を守ります

組織に課せられる法律と規則の数が増えつつある中、システムにパッチを完全に適用させる作業は一層重要になっています。
Patch for Endpoint Managerは、遵守要件や、規制企画を満たし、機会の喪失を軽減し、刑罰や罰金のリスクを軽減する上で企業の役に立ちます。

ネットワークへの影響を最小限に抑え速やかにより多くのシステムにパッチを適用します

Patch for Endpoint Manager は、業務妨害となり帯域幅需要を生じさせることや専用のハードウェアやルータ設定を要求することなく、企業のネットワーク全体で速やかにパッチを適用、配信するため、複数のテクノロジーを採用しています、パッチを適用し、ソフトウェアパッケージをアップデートするため環境が整ったエンドポイントを使用して、ハードウェアコストを軽減します。変更管理委員会による承認が得られた後すぐに展開するため、パッチ適用が必要なシステムにローカルで前段階のパッチを適用します。帯域幅の使用量とハードウェアリソースを最適化しつつ大規模かつスピーディにパッチを適用するため内臓のプロジェクト展開機能を使用します。

場所を問わずデバイスにアクセスしパッチを適用します

Patch for Endpoint Manager は Ivanti Cloud Service Applianceと相互運用します。この組み合わせにより、場所を問わず世界中にあるシステムを評価、修正できます。リモートのシステムや出張中の社員が携帯しているシステムももちろん評価、修正できます。しかも仮想プライベートネットワーク(VPN)に接続する必要はありません。

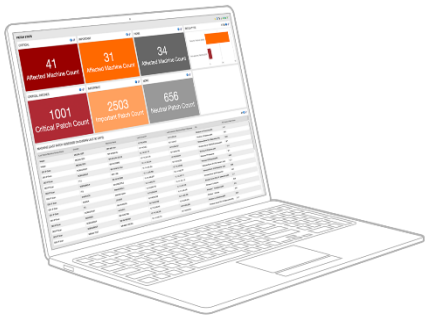
パッチとシステム管理を統合します

Patch for Endpoint Managerは単独で展開できるだけではなく、Ivanti Endpoint Managerへのアドオンとしても展開できます、フラグシップ製品と統合すると、パッチとシステム管理を簡単に統合でき、共通のユーザー及び管理者インターフェースからの管路が簡単になります。Ivantiのツールはわずか数分で起動し、お客様が定義したポリシーに基づいて、社内ネットワーク上のすべてのWindows,MacOS,Linux,UNIXシステムすべてを自動的に特定、評価、修正します。当社のツールは物理システムと仮想システムの両方へパッチ適用を簡単な操作に変えます。オンラインとオフラインのワークステーションとサーバーを検出し、不足しているパッチをスキャン、展開します。その後、OSやアプリから仮想マシン、仮想テンプレートまで、あらゆるシステムにパッチを適用します。さらに、Vmwareとの統合により、ESXiハイパーバイザーにもパッチを適用します。

ユーザーへの妨害を最低限に抑えつつセキュリティを最大化します

より優れたパッチを適用することで、セキュリティを強化できますが、パッチ適用が業務を大幅に妨害する場合、ユーザーや企業の生産性が低下してしまいます。Patch for Endpoint Managerを導入することで、管理者は一貫性のあるタイムフレームを設定し、パッチ適用やメンテナンスのスケジュールを設定できるようになります。業務を妨害せずに静かに保護するため、適切なタイミングかつ適切な環境下でシステムにパッチを適用します。

IT部門の手間を取らせずにクライアントシステムを守りましょう。



コンプライアンスの規定や脆弱性に溢れたサードパーティ製アプリが乱立する中、パッチを包括的な管理は今や欠かせない要素となっています。ただし、これは手間のかかる作業となります。
検証、パッチがソフトウェアに影響しないことのテスト、実装、時間浪費、そしてネットワークへの負担について考えてみましょう。

Patch for Endpoint Managerをご利用になれば、Windows、Mac OS、Linux、さらには数々のサードパーティ製アプリ（Acrobat Flash/Reader、Java、Webブラウザーなど）に潜む脆弱性がすばやく検出され、必要であれば、その場所を問わずテスト済みのパッチが着実に適用されます。

Patch for Endpoint Managerがあれば、
1つのコンソールから保護・管理を行う機能により、物事の進め方を簡素化することができます。

サードパーティ製アプリへのパッチ
OSおよびサードパーティ製アプリ向けのパッチコンテンツをまとめた最大のカタログ

パッチのライフサイクル管理
マイナスの影響を最低限に抑え、変更管理委員会の度肝を抜く段階的なパッチ展開を実現

可視性
スキャン、ダッシュボード、レポートを介して、パッチの状態を評価

異なるプラットフォームにも対応
Windows、Red Hat Linux、SUSE Linux、およびMac OS Xの脆弱性すべてを検出して修正
HP-UXを実行するシステムの脆弱性検出およびレポート作成

自動化されたアップデート
選択したペースでパッチを適用できるようにするため、自動化された展開でアップデートの実現

パッチインテリジェンス
ユーザーからのフィードバックを収集し、パッチがユーザーの生産性に与えている影響の表示

パッチをリモートに配布
テスト、複数のアプリケーションのパッケージ作成を実行し、ネットワーク全体でパッチをプリキャッシュすることで、ネットワークやユーザーに影響を与えることなく素早く実装

時間や場所を問わないパッチ適用
Wake-On-WAN、デバイスの起動中、応答不可の状態、メンテナンス期間中のデバイスに対してパッチの適用方法を選択

Endpoint Managerのアドオン機能
1つのコンソールからシステムを保護・管理

EP Endpoint Manager

【お問合せ】
株式会社ジャパンコンピューターサービス
担当: Ivantiセールス
〒101-0025
東京都千代田区神田佐久間町１-１１ 産報佐久間ビル7階
TEL:03-5298-8868 FAX: 03-5298-8874
E-Mail: ivanti_sales@japacom.co.jp