ivanti neurons

Ivanti Neurons for Patch Management

脆弱性の優先順位付けと修正により、脅威へのエクスポージャーとリスクを低減

Ivanti Neurons for Patch Managementは、Windows、macOS、Linux、およびサードパーティのアプリケーションにわたって、実用的なインテリジェンスとデバイスリスクの可視化を実現するクラウドネイティブなソリューションです。アクティブなリスクエクスポージャー、パッチの信頼性、デバイスコンプライアンスに基づいて、インサイトによる脆弱性の優先順位付けと修復を行います。ランサムウェアを含む様々な脅威から保護します。

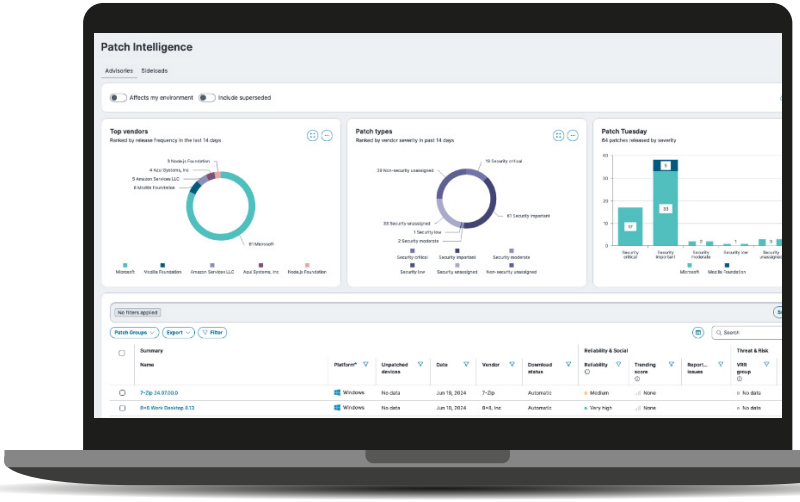
リスクベースのパッチ管理

ランサムウェアによる攻撃は年々その頻度と深刻さを増しており、企業に壊滅的な打撃を与えています。調査によると、データ侵害の平均総費用は488万ドル（約7億円）にも達し、2023年から10%急増し、パンデミック以降で最大の増加となっています[1]。

テクノロジーとAIの進歩に伴い、攻撃は増加の一途をたどっています。RaaS（Ransomware as a Service）が登場したことで、セキュリティの知識やコーディングの専門知識がなくても、誰でも攻撃を仕掛けることができるようになりました。脆弱性の増加はリスクの増加を意味し、脆弱性の悪用は前年比で180%増加しました[2]。Googleの調査によると、ゼロデイ攻撃は前年比で50%増加しています[3]。さらに悪いことに、AIハッキングの時代が到来しています。イリノイ大学の研究者たちは、AIエージェントに自律的にウェブサイトをハッキングさせ、ゼロデイ脆弱性を発見・悪用するよう訓練しました[4]。

一般的な脆弱性とエクスポージャーを修正するためのパッチは、ランサムウェア攻撃に対抗するための最善策のひとつといえます。しかしながら、ITおよびセキュリティの専門家の71%は、パッチ適用が複雑で時間がかかりすぎると感じています[5]。米国の国家脆弱性データベース（NVD）には、23万件以上の脆弱性がリストアップされています[6]。ランサムウェアに関連する脆弱性はごく一部であり、アクティブなエクスプロイトの割合はさらに低いものの、どの脆弱性が企業にとって最大のリスクとなるかを特定するのは容易ではありません。

Ivanti Neurons for Patch Managementは、Windows、MacOS、Linux、およびサードパーティ製アプリケーションにおいて、実用的な脅威インテリジェンス、パッチの信頼性に関するインサイト、およびデバイスリスクの可視化を実



現します。これらの重要なインサイトにより、ITチームは企業を最も危険にさらす脆弱性に優先順位を付け、修復することが可能になります。Ivanti Neurons for Patch Managementを活用してパッチ適用の効率性と効果を高めることで、企業はデータ漏洩やランサムウェアなど、ソフトウェアの脆弱性に起因する脅威から身を守ることができます。

主な機能と特徴

リスクベースの優先順位付け

Ivanti Neurons for Patch Managementは、リスクベースの優先順位付け戦略を使用して、クリティカルな脆弱性、特にランサムウェアに関連する脆弱性に対処するパッチを最初に対象とします。これにより、最も高いリスクを軽減するパッチに集中することで、ITチームはリソースを他の戦略的優先事項に割り当てることができ、パッチ管理のプロセスを簡素化し、セキュリティの有効性を向上させることができます。このアプローチは重大な脆弱性を迅速に対処し、ランサムウェアやその他のセキュリティ侵害のリスクを大幅に低減します。その結果、複雑な脅威環境においても強固な防御を維持することができます。

アクティブな脅威コンテキスト

高度な脆弱性リスク評価（Vulnerability Risk Rating）システムにより、重要な脆弱性に優先順位を付けることで、ITセキュリティを強化します。この評価は、実際のリスク評価を含むことで、従来のCVSSスコアを上回ります。当社のVRRシステムは、エクスプロイトやランサムウェア関連の脆弱性に関するインテリジェンスなど、敵対的リスクに関する詳細ないんサイトを用いてパッチをランク付けします。高品質のデータとペネトレーションテストチームからの専門的な検証によって強化されたVRRシステムは、修正作業を効果的にし、アクティブな脅威や潜在的な脅威に対する防御力を大幅に強化させます。

リスクベースでの展開

脆弱性が増加する中、ベンダーは一貫してその対策となるアップデートをリリースしています。これは、特にゼロデイエクスプロイトや公開された脆弱性に対するリスクを軽減するために重要です。しかし、これらの継続的なアップデートを組織の通常の月次メンテナンススケジュールと一致させることは困難であり、その結果、数週間にわたるセキュリティのギャップが生じることがあります。

リスクベースの展開機能は、月次の定期メンテナンス、週次の優先アップデート、および即時ゼロデイパッチなど、複数の並行展開タスクをサポートします。これにより、リリースのタイミングに関係なく、システムを最新のパッチで自動的に管理することが可能になります。

「データがサイロ化されているためにセキュリティ対応時間が遅くなっている、とITとセキュリティの専門家の63%が報告しています」[7]。

ITとセキュリティの垣根を取り除くには

ITおよびセキュリティチーム間で、SLA追跡やリスクベースのインテリジェンスなどの重要な情報への平等なアクセスを提供することで、パリティ（均衡）を確立しましょう。これにより、包括的な視点と共通言語が醸成され、迅速かつ効果的なクロスファンクショナルな対応が促進されます。統一されたアプローチは摩擦を減少させ、ステークホルダーへの協調的な対応を可能にします。クラウドソースデータとデプロイメントテレメトリから得られたパッチの信頼性に関する洞察を共有することで、事前の評価が可能となり、失敗するデプロイメントを防ぐことができ、SLAの遵守を確保します。この戦略は連携を改善し、企業のセキュリティ態勢を強化します。

オンプレミスからクラウドへ

Ivanti Neurons for Patch Managementで、オンプレミスのパッチ管理からクラウドへの移行を始めてみましょう。当社のクラウドネイティブソリューションは、「総入れ替え」を強いることなく、お客様のペースで移行することができます。Ivantiの移行体験では、クラウドで管理されているデバイスとオンプレミスのIvantiパッチ管理ソリューションで管理されているデバイスの可視化ができます。

パッチの信頼性

パッチの信頼性は、システムの整合性とセキュリティにおいて極めて重要です。Ivantiは、クラウドソースされたフィードバック、匿名化されたデプロイメントデータ、および高度なテストを活用して、パッチの効果性と安全性を評価し、デプロイメント前に確認します。Ivanti Neurons Agentは、テスト済みのパッチを自動的に設定し、数千台のデバイスに迅速に配布し、早期に潜在的な問題を特定します。これにより、ITチームは情報に基づいたパッチ適用の判断を下すことができ、障害のリスクを最小限に抑え、IT環境の安定性とパフォーマンスを向上させます。この方法はダウンタイムを減少させ、脆弱性に対する継続的な保護を確保します。

異種環境を一つのプラットフォームで管理

異種プラットフォームは、多様なIT環境において強力なセキュリティ 基準を維持するために不可欠であり、効率的かつ積極的なITセキュリ ティリスク管理を可能にします。
Ivanti Neurons for Patch Managementは、Windows、MacOS、Linux、 およびサードパーティアプリケーションをサポートし、統一された 管理体験を提供します。これにより、さまざまなシステムの監視が 簡素化され、生産性が向上します。

単一のプラットフォームを使用することで、一貫したセキュリティポリシーの維持と運用効率の向上が図れます。異なるパッチ管理システム間を切り替える必要がなく、複雑さと管理の見落としリスクが減少します。これにより、全てのエンドポイントに対する包括的な保護と可視性が確保されます。この包括的なアプローチにより、脆弱性や不整合を迅速に特定し、セキュリティ侵害を防止します。また、ダウンタイムと復旧コストを削減し、企業の資産を保護します。

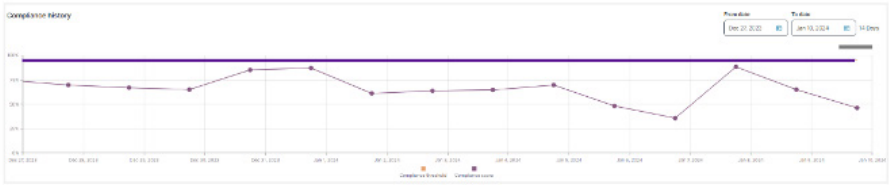
コンプライアンスレポート

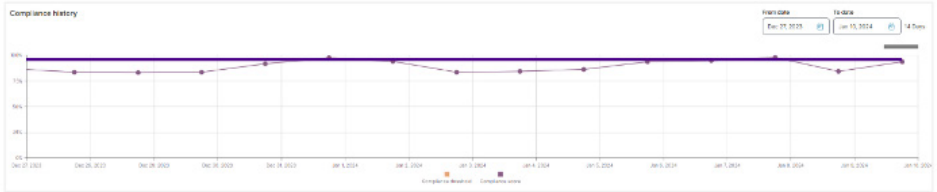
パッチ管理におけるコンプライアンス報告は非常に重要です。Ivantiの自動化システムは、実際のリスクを反映するリスクベースのKPIに重点を置いています。これにより、全てのパッチが文書化され、規制基準を満たすことが保証され、非コンプライアンスのリスクが大幅に削減されます。このシステムは、更新のリリース日を基にSLA（サービスレベルアグリーメント）を設定することで、パッチ管理をセキュリティニーズと調和させます。これは、セキュリティチームが継続的なパッチサイクルに直面している際に特に重要です。脆弱性のエクスポージャーという観点からSLAを再調整することで、IT部門は運用上の要求を管理しながらセキュリティ要件をより適切に満たすことができます。これにより、企業全体のセキュリティフレームワークが強化されます。

測定方法の変更：「エクスポージャータイム」

数値を追求する：

更新は継続的にリリースされます。コンプライアンスを達成することはほぼ不可能です。





重要なことを測定する：

リスクベースのKPIにより、チームは現実のリスクに集中し、コンプライアンスを達成することができます。

Ivantiについて

Ivantiは、ITとセキュリティ部門間の障壁を取り除きEverywhere Work（場所にとらわれない働き方）を実現します。IvantiのCIOとCISO向けに特化したプラットフォームは、ITとセキュリティ部門へ組織のニーズに合わせて拡張できる包括的なソフトウェアソリューションを提供し、セキュアに従業員体験を向上させます。Ivantiプラットフォームは、クラウドスケールのインテリジェントなハイパーオートメーションレイヤーであるIvanti Neuronsを搭載しており、組織全体でプロアクティブな修復とユーザーフレンドリーなセキュリティを実現し、ユーザーが満足するような従業員体験を実現します。Ivantiのエンドツーエンドのソリューションは、Fortune 100社のうち85社を含む40,000社以上の顧客によって採用されています。Ivantiは、すべての視点が聞き入られ、尊重され、評価される環境づくりに尽力し、顧客、パートナー、従業員そしてよりサステイナブルな未来を実現するために取り組んでいます。詳細については、www.ivanti.com/jaや@GoIvantiをフォローしてください。

ivanti neurons

詳細について、またはIvantiへのお問い合わせは、ivanti.com/jaにアクセスしてください。

1. IBM、「データ侵害のコストに関する調査 2024年」 https://www.ibm.com/reports/data-breach
2. ベライゾン、「2024年度データ漏洩/侵害調査報告書」 https://www.verizon.com/business/resources/reports/ dbir/
3. Google、「2023年のゼロデイを振り返る」、2024年3月 https://cloud.google.com/ blog/topics/threat-intelligence/2023-zero-day-trends
4. Richard Fang、Rohan Bindu、Akul Gupta、Qiusi Zhan、Daniel Kang、「Teams of LLM Agents can Exploit Zero-Day Vulnerabilities」、2024年6月2日。 https://arxiv.org/abs/2406.01637.
5. Ivanti、「パッチ管理の課題：Everywhere Workplaceへの移行に伴う調査結果と考察」、2021年10月7日。 https://www.ivanti.com/ resources/v/doc/ivi/2634/712cff539c8a.
6. Securin、「2023年ランサムウェアレポート」2024. https://www.securin.io/ransomware-report-2023-year-in-review-download/.
7. Ivanti、「2024年サイバーセキュリティ ステータスレポート」 https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report