Ivanti Neurons for Patch Management

脆弱性を効率的に優先順位付けし、修正します

Ivanti Neurons for Patch Managementは、脅威にさらされたリスク、パッチの信頼性、デバイスのコンプライアンス、健全性とリスクに関する実用的なインテリジェンスを備えたクラウドネイティブのパッチ管理ソリューションであり、ランサムウェアを含む脅威に対して企業・組織の保護を強化します。

リスクベースのパッチ管理

ランサムウェア攻撃の頻度とその深刻さは年を追うごとに高まっており、企業が受ける影響は甚大です。調査によると、ランサムウェアに感染した場合の平均的な総コストは462万ドル（約5億2000万円）とされ、これに身代金は含まれていません。[1]

残念ながら、状況は良くなる以前に悪化していく可能性の方が高いのです。RaaS（Ransomware as a Service）は、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、誰でも攻撃を開始できるようになるサービスです。その上、ネットワークへの共通脆弱性識別子（CVE）の数は、2020年には約4倍に増えています。[2] さらに悪いことに、ランサムウェアの攻撃者は大企業を攻撃することでメディアの注目を浴びることを避けるために、中堅企業を標的にするケースが増えています。[3]

CVEを修正するためのパッチは、ランサムウェアの攻撃に対抗するために組織ができる最善の方法の一つです。残念なことに、ITおよびセキュリティ専門家の71%は、パッチの適用が過度に複雑で時間を要すると感じています。[4] それは、存在する脆弱性の量が圧倒的に多いことが原因かもしれません。米国では10万件を超える脆弱性が National Vulnerability

Database（NVD）に登録されています。しかし、そのうちランサムウェアに関連するものはごく一部、アクティブなエクスプロイトはさらにわずかで、組織にとって最もリスクの高いものを特定するのは困難です。2018年から2020年にかけて、CVSS v3のスコアリングを用いて、重大な脆弱性のみにパッチを適用していた場合、ランサムウェアに対するカバー率は約35%にとどまります。[2]

Ivanti Neurons for Patch Managementは、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、デバイスのリスクに関する可視性を提供し、IT部門が組織に最も危険を及ぼす脆弱性を優先的に修正することを可能にします。Ivanti Neurons for Patch Managementを活用してパッチ適用作業の効率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守ることができます。

主な機能と特徴

アクティブなエクスプロイトに対し積極的にパッチを適用

ランサムウェアに関連するものを含む、既知のエクスプロイトや脆弱性の脅威の背景に関する情報により、敵対的なリスクに基づいて修復の優先順位を決定します。Ivantiの脆弱性リスク評価（VRR）は、最も忠実性の高い脆弱性と脅威のデータに加え、ペネトレーションテストチームによるエクスプロイトの人的検証を取り入れることで、CVSSスコアリングよりもリスクに応じた優先順位による対策を講じることができます。

パッチの信頼性とトレンドのインサイトにより、SLAの短縮を実現

クラウドソースによるソーシャルメディアでのセンチメントデータと匿名化されたパッチデプロイのテレメトリから得られるパッチの信頼性に関するにより、時間を節約し、パッチ適用の失敗を回避することができます。この情報により、パッチを適用する前に、実際のアプリケーションでの信頼性に基づいてパッチを評価することができます。さらに、SLAに抵触しそうなデバイスを可視化するサービス品質保証（SLA）トラッキング機能により、デバイスがコンプライアンスから外れる前に対策を講じることができます。

オンプレミスからクラウドパッチ管理への移行

Ivantiのパッチテクノロジーで、オンプレミスのパッチ管理からクラウドへの移行を開始しましょう。Ivanti Neurons for Patch Managementは、オンプレミスのパッチ管理からクラウドへの移行を、「まるごと入れ替え」ではなく、自社のペースで移行ができるクラウドネイティブのソリューションです。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と、クラウドで管理されているデバイスを単一の画面で可視化することで、段階的な移行が可能となります。

パッチ管理プロセスの合理化

サイロ化したパッチ管理ソリューションの間を行き来する必要がなく、運用効率を向上できます。Ivanti Neurons for Patch Managementは、企業の環境にあるすべてのエンドポイントを一画面で可視化します。高度な脆弱性のパッチインテリジェンスにより、パッチ作業に効果的な優先順位をつけることができ、重要なものだけに集中することができるため、運用効率がさらに向上します。さらに、パッチ適用時にはデバイス上のIvanti Neurons Agentに展開された自律的なパッチコンフィギュレーションが、パッチを数分で数千台のマシンに配布します。

Ivanti について

Ivanti について Ivanti は「Everywhere Workplace（場所にとらわれない働き方）」を実現します。場所にとらわれない 働き方により、従業員は多種多様なデバイスでさまざまなネットワークから IT アプリケーションやデータにアクセスし、高い生産性を保つことができます。Ivanti Neurons 自動化プラットフォームは、業界をリードする統合エ ンドポイント管理、ゼロトラストセキュリティと、エンタープライズサービス管理のソリューションをつなぎ、デバイスの 自己修復および自己保護、またエンドユーザーのセルフサービスを可能にする統合 IT プラットフォームを提供し ます。Fortune 100の96社を含む40,000社以上の顧客が、クラウドからエッジまで IT 資産の管理、検 出、保護、サービスのために Ivanti を選択し、従業員があらゆる場所にいても作業できる優れたユーザー体験 を提供しています。詳細については、www.ivanti.co.jp をご参照ください。

ivanti neurons

ivanti.co.jp/neurons
+81 (0)3-6432-4180
contact@ivanti.co.jp

1. IBM Security, “2021 Cost of a Data Breach Report”, 28 July 2021. https://www.ibm.com/downloads/cas/OJDVQGRY
2. RiskSense, Cyber Security Works, “Ransomware Through the Lens of Threat and Vulnerability Management”, 9 November 2021. https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw
3. Coveware, “Ransomware attackers down shift to ‘Mid-Game’ hunting in Q3 2021”, 21 October 2021. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
4. Ivanti, “Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace”, 7 October 2021. https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges