ivanti neurons

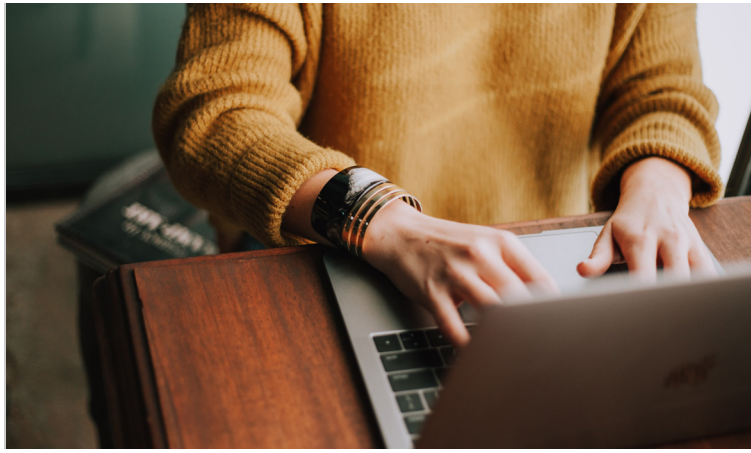
Ivanti Neurons for Patch Management

有效率的區分漏洞的優先順序並加以補救

Ivanti Neurons for Patch Management 是一款雲端原生修補程式管理解決方案，提供與現行的曝險、修補程式可靠性與裝置合規性、健康和風險有關的可行動情報，協助組織更妥善的防護威脅，包括勒索軟體。

Risk-based patch management

風險基礎修補程式管理勒索軟體攻擊的頻率和嚴重性每年不斷的增加。這為企業帶來毀滅性的影響。研究顯示扣除勒索成本後，勒索軟體入侵的平均總成本是 462 萬美元。遺憾的是，情況在好轉前似乎變得越來越惡化。第1，勒索軟體即服務 (RaaS) 讓每個人都可以發動攻擊，不需要有資安知識或編寫程式碼的專業技能。最重要的一點是，網路的通用弱點揭露計畫 (CVE) 的數目在 2020 年增加了將近四倍。第 2，更嚴重的是，勒索軟體攻擊者逐漸將目標對準中型市場的企業，避免媒體對攻擊大企業的注意。第 3，修復 CVE 的程式修補是組織為了反制勒索軟體攻擊所能做的最棒的事之一。遺憾的是，71% 的 IT 和資全專業人員發現程式修補太過複雜與耗時。第 4，可能是存在難以計量的漏洞所造成。美國國家漏洞資料庫 (US National Vulnerability Database，簡稱 NVD) 中列有超過 100,000 個漏洞。只有一小部份與勒索軟體有關，甚至只有更少的部份是現行的漏洞利用，識別哪一個對您的組織造成最大風險並不是件易事。自 2018 到 2020 年，使用 CVSS v3 計分後，如果您只修補重大 漏洞，您對勒索軟體的安全防護範圍 只有約 35%。



Ivanti Neurons for Patch Management 提供 可行動的威脅情報、修補程式可靠性洞察力和裝置風險可見度，讓 IT 團隊可以區分出對他們帶來最大危險的漏洞的優先順序並加以補救。藉由調整 Ivanti Neurons for Patch Management 來增加 其修補的效率和有效性，企業可以更好的防止自身發生源自軟體漏洞的資料入侵、勒索軟體和其他威脅。

關鍵特點和功能

主動修補現行的漏洞利用

根據對抗風險區分補救的優先順序，運用關於已知漏洞利用的情報和漏洞的威脅情境，包括與勒索軟體的關係。Ivanti 的漏洞風險評估 (VRR) 可以讓您做更好的準備，採用最高真實度漏洞和威脅資料，結合穿透測試團隊的漏洞利用人為驗證，採取 CVSS 計分以外的風險式優先行動。

運用修補程式可靠性和趨勢洞察力更快達到 SLA

以來自群眾外包的社會情感資料和匿名的修補程式部署遠端探測，節省時間和避免修補程式部署失敗。這些資訊讓您可以在部署修補程式前，根據其在真實世界運用中的可靠性評估修補程式。此外，服務等級協助 (SLA) 追蹤提供近似於 SLA 的裝置的可見度，讓您可以在其超過符合性的範圍前在裝置上採取行動。從內部部署轉換成雲端修補程式管理 運用 Ivanti 的修補技術的優勢，開始從內部部署修補程式管理到雲端的旅程。Ivanti Neurons for Patch Management 是一款雲端原生的解決方案，讓您可以從依照自己進度為主的內部部署修補程式管理轉換成雲端，而非強制「重整並取代」。這種漸進式的轉換以解決方案的單一窗口體驗作為開始，提供其在雲端中管理，以及透過內部部署的 Ivanti 修補程式管理解決方案管理的裝置的可見度。

簡化修補程式管理流程

減少在孤立的修補程式管理解決方案之間轉換的需求，改善操作的效率。Ivanti Neurons for Patch Management 透過單一窗口，提供對您環境中的所有端點的可見度。您可以透過進階漏洞洞察和修補程式情報有效區分修補的優先順序以進一步改善操作效率，因此可以只專注在最重要的部份。此外，在進行修補時，部署在裝置的 Ivanti Neurons Agent 上的自動「修補程式組態」可在幾分鐘內，將經過測試的修補程式徹底分配給數以千計的機器。

關於 Ivanti

Ivanti 讓 Everywhere Workplace (無處不在的工作場所) 成為可能。在 Everywhere Workplace，員工使用五花八門的裝置存取 IT 網路、應用程式和資料，以在任何地方工作時保持工作效率。Ivanti 自動化平台將公司領先業界的統一端點管理、零信任安全和企業服務管理解決方案連接起來，為企業提供單一管理平台，使裝置能夠自我修復和自我保護，終端使用者能夠自助服務。超過 40,000 個客戶 (包括財星雜誌 (Fortune) 百大企業中的 96 間企業) 選擇 Ivanti 來搜尋、管理、保護和服務從雲端到邊緣的 IT 資產，並爲員工提供卓越的終端使用者體驗，無論他們在哪裏工作，以何種方式工作。如需更多資訊，請瀏覽 ivanti.com

ivanti neurons

ivanti.com/neurons
1 800 982 2130
sales@ivanti.com

1. IBM Security, “2021 Cost of a Data Breach Report”, 2021 年 7 月 28 日 https://www.ibm.com/downloads/cas/OJDVQGRY
2. RiskSense, Cyber Security Works, “Ransomware Through the Lens of Threat and Vulnerability Management”, 2021 年 11 月 9 日 https://www.ivanti.com/resources/v/doc/white-papers/spotlight_ransomware2021_risksensecsw
3. Coveware, “Ransomware attackers down shift to ‘MidGame’ hunting in Q3 2021”, 2021 年 10 月 21 日 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”, 2021 年 10 月 7 日。https://www.ivanti.com/resources/v/doc/datasheets/ivi-2634-patch-management-challenges