Ivanti Neurons Patch for MEM (Microsoft Endpoint Manager)

Extend Microsoft Intune with risk-based third-party patch publishing

Ivanti Neurons Patch for MEM extends existing Microsoft Intune implementations to include third-party application updates. Its threat and patch intelligence help organizations properly prioritize remediation of third-party software vulnerabilities.

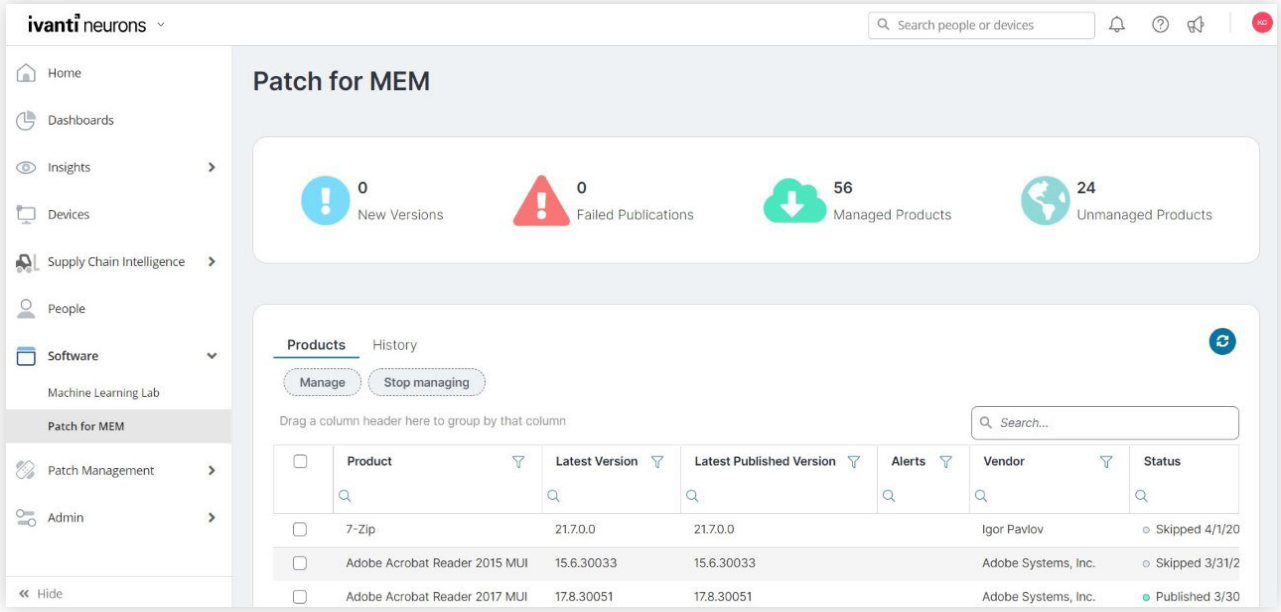
Third-party updates in Intune

Data breaches and ransomware attacks are increasing every year. Similarly, the number of applications organizations deploy is also on the rise, up 24% since 2016.[1] It should therefore come as no surprise that third-party applications have become one of the most attractive attack vectors for cyber adversaries. Unfortunately, data breaches stemming from vulnerabilities in third-party applications are also among the most expensive, costing organizations an average of $4.33M.[2]

Organizations thus need to be diligent about updating third-party applications, which can be challenging with the ever-increasing number of applications they must account for. Further complicating matters is the growing number of vulnerabilities they need to track as well – an average of 61 are disclosed by the National Vulnerability Database (NVD) every day.[3]

The good news is only 4% of all Common Vulnerabilities and Exposures (CVEs) have been publicly exploited.[4] The bad news is that identifying that 4% from the over 130,000 total vulnerabilities in the NVD can be difficult. For example, if an organization were to patch all critical vulnerabilities based on the Common Vulnerability Scoring System (CVSS) v3, they would miss out on patching 73.61% of ransomware vulnerabilities.[3]

This situation can be even more problematic for organizations that leverage Microsoft Intune to deliver applications and updates to their devices. While Intune offers comprehensive patch management capabilities for Microsoft applications, it provides no native functionality for updating third-party applications.



Introducing Ivanti Neurons Patch for MEM

Ivanti Neurons Patch for MEM extends existing Microsoft Intune implementations to include third-party application update capabilities without the need for any additional infrastructure. It also provides actionable threat intelligence and patch reliability insight for IT teams to prioritize and remediate the vulnerabilities that pose the most risk to their organization. With Ivanti Neurons Patch for MEM, organizations can better protect themselves from data breaches, ransomware and other threats that stem from vulnerabilities in third-party applications.

Key features and capabilities

Extend Microsoft Intune with third-party patch publishing

Maximize the return on your Intune investment while protecting against threats that stem from vulnerabilities in third-party applications. Ivanti Neurons Patch for MEM publishes pre-tested third-party application updates from Ivanti's Neurons cloud platform directly to Intune. This lets IT teams deploy third-party application updates alongside Microsoft OS and application updates within Intune as part of their existing application lifecycle management workflows.

Additionally, as a cloud-native solution, Ivanti Neurons Patch for MEM enables Intune customers to migrate their patching workloads entirely to the cloud and achieve Microsoft's vision of modern management without the need for any additional infrastructure.

Proactively protect against active exploits

Prioritize remediation based on adversarial risk with intelligence on known exploits and threat-context for vulnerabilities – including ties to ransomware. Ivanti's Vulnerability Risk Rating (VRR) better arms you to take risk-based prioritized action than basic CVSS scoring by taking in the highest fidelity vulnerability and threat data plus human validation of exploits from penetration testing teams.

Avoid failed patch deployments

Save time and avoid failed patch deployments with pre-tested application updates and patch reliability insights. Ivanti thoroughly tests each patch content package we create. Testing is conducted in an extensive virtual environment to ensure the packages work across a wide array of application versions and operating systems before they are released to the product.

To further bolster your confidence, patch reliability insights from crowdsourced social sentiment data and anonymized patch deployment telemetry enable you to evaluate application updates based on their reliability in real-world environments before deploying them.

Streamline patch management processes

Realize a range of operational efficiencies with Ivanti Neurons Patch for MEM's helpful features:

- Automatically publish third-party application updates into Intune as they become available (auto-publish optional).
- Achieve more reliable patching with fewer failures when leveraging pre-tested application updates coupled with patch reliability insights.
- Effectively prioritize patch efforts with threat intelligence so you focus only on what matters.
- Facilitate data and risk conversations between security and IT operations teams with exploit and malware insight to improve operational collaboration.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com.

ivanti

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

1. Okta, "Business at Work 2022 Report", 2022. https://www.okta.com/report/businesses-at-work-2022
2. IBM Security, "2021 Cost of a Data Breach Report", 28 July 2021. https://www.ibm.com/security/data-breach
3. Cyber Security Works, Cyware, Ivanti, "2022 Ransomware Spotlight Report", 26 January 2022. https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report
4. Cybersecurity and Infrastructure Security Agency (CISA), "Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities", 3 November 2021. https://cyber.dhs.gov/bod/22-01/