Ivanti Neurons for Patch Management

通过漏洞排序和修复来减少威胁暴露和风险

Ivanti Neurons for Patch Management 是一款云原生解决方案，可针对 Windows、macOS、Linux 和第三方应用程序提供相应的实用情报和设备风险可见性。通过对主动风险敞口、补丁可靠性和设备合规性的了解来确定漏洞的优先级并加以修补。防范包括勒索软件在内的一系列威胁。

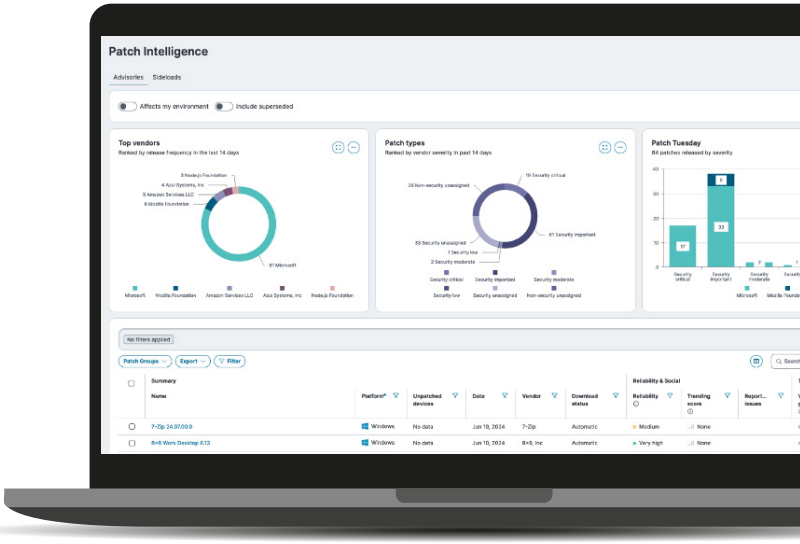
基于风险的补丁管理

勒索软件攻击的频率和严重程度与日俱增，并且对企业造成毁灭性影响。研究显示，数据泄露的平均总成本为 488 万美元，较 2023 年增长 10%，是自疫情爆发以来的最大增幅.[1]

随着技术和人工智能的进步，攻击只会增加。勒索软件即服务 (RaaS) 使任何人都能发起攻击——不需要安全知识或编码专业技能。漏洞增加导致风险增加，漏洞利用率年同比增长 180%。[2] Google 的研究表明，零日漏洞利用率年同比增长 50%。[3] 更糟糕的是，人工智能黑客时代已经到来。伊利诺伊大学的研究人员训练人工智能代理自主入侵网站，发现并利用零日漏洞。[4]

修补常见的漏洞和风险暴露是组织应对勒索软件攻击的最佳措施之一。不幸的是，71% 的 IT 和安全专业人士发现修补过于复杂且耗时。[5] 这可能是由于漏洞数量过多造成的。美国国家漏洞数据库 (NVD) 列出了超过 230,000 个漏洞。6 虽然其中只有一小部分与勒索软件有关，而主动漏洞利用所占的比例还要更小，但确定哪些漏洞对您的组织构成最大风险可能很棘手。

Ivanti Neurons for Patch Management 可针对 Windows、macOS、Linux 和第三方应用程序提供相应的实用威胁情报、补丁可靠性洞见和设备风险可见性。这些关键洞见让 IT 团队能够确定漏洞排序，并优先修复那些对组织构成最大危险的漏洞。通过利用 Ivanti Neurons for Patch Management 来提高补丁工作的效率和效果，企业可以更好地保护自己免受数据外泄、勒索软件和其他源自软件漏洞的威胁。



主要特色和功能

基于风险的先后排序

Ivanti Neurons for Patch Management 采用基于风险的排序策略，首先针对那些解决关键漏洞的补丁——尤其是与勒索软件相关的漏洞。通过专注于缓解最高风险的补丁，IT 团队可以有效地将资源分配给其他战略重点，简化补丁管理流程并提高安全有效性。这种方法可以迅速解决严重的漏洞，大大降低勒索软件和其他安全漏洞的风险，从而在复杂的威胁环境中保持强大的防御能力。

主动威胁情境

使用先进的漏洞风险评级 (VRR) 系统对关键漏洞进行优先排序，从而增强您的 IT 安全性。该评级通过纳入真实世界风险评估，超越了传统的 CVSS 评分。我们的 VRR 系统使用有关对抗风险的详细洞见（例如有关漏洞利用和勒索软件相关漏洞的情报）对补丁进行排名。借助高质量数据和渗透测试团队的专业验证，VRR 系统可以有效地指导补救工作，显著增强您对主动和潜在威胁的防御能力。

按风险部署

随着漏洞的增多，供应商不断发布更新来解决这些问题。这对于降低风险至关重要，尤其是对于零日漏洞或公开披露而言。然而，将这些持续的更新与组织通常的月度维护计划相协调是具有挑战性的——这会导致安全漏洞存在数周之久。

按风险部署功能支持多个并行部署任务：每月定期维护、每周优先更新和即时零日补丁。这使得系统能够实现自动更新管理，无论补丁发布时间如何，都能确保系统始终保持最新状态。

“63% 的 IT 和安全专业人士报告称，孤立数据会减慢安全响应时间。”[7]

打破 IT 和安全之间的障碍

通过为 IT 团队和安全团队提供对关键信息（如 SLA 跟踪和基于风险的情报）的平等访问权限，实现两者之间的对等。这有利于形成全面的视角和共同语言，促进快速有效的跨职能行动。统一的方法可以减少摩擦，并能够对利益相关者做出协调的回应。分享从众包数据和部署遥测中得出的补丁可靠性见解，使得可以进行前瞻性评估并防止部署失败，从而确保遵守 SLA。这一策略改善了协调并增强了组织的安全态势。

从本地到云端

借助 Ivanti Neurons for Patch Management，开始您从本地补丁管理过渡到云端的旅程。我们这款云原生解决方案让您能够按自己的步调完成过渡，而不是强行“剥除并替换”。Ivanti 的迁移体验让您能清楚了解它在云端管理的设备以及通过本地 Ivanti 补丁管理解决方案管理的那些设备。

补丁可靠性

补丁可靠性对于系统完整性和安全性至关重要。Ivanti 利用众包反馈意见、匿名部署数据和高级测试在部署前预先评估补丁的有效性和安全性。Ivanti Neurons Agent 可以自主配置并将经测试的补丁快速分发到数千台设备，从而尽早发现潜在问题。IT 团队可以做出明智的修补决策，最大限度地降低故障风险并提高 IT 环境的稳定性和性能。这种方法减少了停机时间并确保持续防范漏洞。

从本地到云端

借助 Ivanti Neurons for Patch Management，开始您从本地补丁管理过渡到云端的旅程。我们这款云原生解决方案让您能够按自己的步调完成过渡，而不是强行“剥除并替换”。Ivanti 的迁移体验让您能清楚了解它在云端管理的设备以及通过本地 Ivanti 补丁管理解决方案管理的那些设备。

补丁可靠性

补丁可靠性对于系统完整性和安全性至关重要。Ivanti 利用众包反馈意见、匿名部署数据和高级测试在部署前预先评估补丁的有效性和安全性。Ivanti Neurons Agent 可以自主配置并将经测试的补丁快速分发到数千台设备，从而尽早发现潜在问题。IT 团队可以做出明智的修补决策，最大限度地降低故障风险并提高 IT 环境的稳定性和性能。这种方法减少了停机时间并确保持续防范漏洞。

在同一平台上实现异构

异构平台对于在多样化的 IT 环境中保持强大的安全标准至关重要，它可以实现高效且主动的 IT 安全风险管理。Ivanti Neurons for PatchManagement 支持 Windows、MacOS、Linux 和第三方应用，提供统一的管理体验，可以简化各种系统的监督并提高工作效率。

使用单一平台可以提供一致的安全策略并提高运营效率，并且无需在不同的补丁管理系统之间切换。它降低了复杂性和监督风险，确保所有端点的全面保护和可见性。通过快速识别漏洞和不一致性，这种全面的方法可以防止安全漏洞，减少停机时间和恢复成本，并保护组织资产。

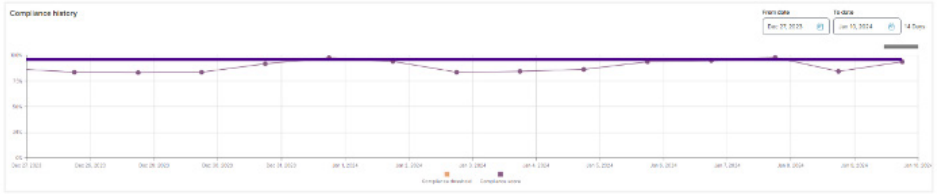
合规报告

补丁管理中的合规报告至关重要。Ivanti 的自动化系统专注于反映现实风险的基于风险的 KPI。它确保所有补丁都记录在案并符合监管标准，大大减少不合规情况。该系统基于更新的发布日期而不是典型的 IT 运营时间表来设定 SLA，从而使补丁管理与安全需求保持一致。这是至关重要的，因为安全团队面临着持续补丁周期带来的挑战。通过从漏洞暴露的角度重新调整 SLA，IT 部门可以在管理运营需求的同时更好地满足安全要求，从而加强组织的整体安全框架。

更改我们的衡量方式：“曝露时间”

追逐数字：

更新持续不断地发布。实现实时合规几乎是不可能的。



衡量重要的事情：

基于风险的 KPI 使团队能够专注于现实世界的风险并实现合规。

关于 Ivanti

Ivanti 完善并确保 Everywhere Work，从而促使员工和企业都能够实现蓬勃发展。我们让技术为人们服务，而不是相反。如今员工使用各类公司和个人设备通过多种网络访问 IT 应用和数据，以便无论他们身在何处以何种方式工作，都能够保持工作效率。Ivanti 是唯一能够发现、管理和保护组织中每一处 IT 资产和端点的科技公司。有超过 40,000 家客户（包括财富 100 强企业中的 85 家）选择 Ivanti 来帮助他们提供卓越的数字化员工体验，并提高 IT 和安全团队的生产力和效率。在 Ivanti，我们努力营造一个倾听、尊重和重视所有观点的环境，我们致力于为客户、合作伙伴、员工和地球创造更可持续的未来。更多信息请访问 ivanti.com

ivanti neurons

如需更多信息或与 Ivanti 取得联系，请访问 ivanti.com。

1. IBM, “Cost of a Data Breach Report 2024,” 2024. https://www.ibm.com/reports/data-breach
2. Verizon, “2024 Data Breach Investigations Report,” 2024. https://www.verizon.com/business/resources/reports/dbir/
3. Google, “A Year in Review of Zero-Days Exploited In-the-Wild in 2023,” March 2024. 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,” 2 June 2024. https://arxiv.org/abs/2406.01637.
5. Ivanti, “Patch Management Challenges: Survey Results and Insights as Organizations move to Everywhere Workplace,” 7 October 2021. https://www.ivanti.com/resources/v/doc/ivi/2634/712cff539c8a.
6. Securin, “Ransomware Report 2023 Year in Review,” 2024. https://www.securin.io/ransomware-report-2023-year-in-review-download/.
7. Ivanti, “2024 State of Cybersecurity Report,” 2024. https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report