Ivanti Neurons for Risk-Based Vulnerability Management基于风险的漏洞管理(RBVM)

Ivanti Neurons for RBVM 能帮助您将自身漏洞管理策略升级为基于风险的方法。这个 SaaS 产品使您能够高效且有效地优先修复对您造成最大风险的漏洞和弱点，从而更好地防范数据泄露、勒索软件和其他网络威胁。

是时候采用新的漏洞管理方法了

现在已经有超过 270,000 个已知漏洞。[1] 幸运的是，组织并不需要修复其 IT 环境中出现的每个漏洞和弱点。不幸的是，对于使用传统漏洞管理方法的组织来说，识别给他们带来重大风险的罕见漏洞或弱点的过程不仅耗时且容易出错。

企业必须先收集一系列不同数据——从扫描结果到威胁情报，再对其进行规范化处理和准备，然后才能利用它开始对漏洞和弱点进行排序和修复。如果手动完成，这些过程可能需要数天、数周或数月才能完成，并且总免不了产生人为错误。

随后的排序过程也好不到哪去。比如拿勒索软件漏洞来说，74% 的漏洞在 CVSS v3 下未被评为“严重”，CISA 已知利用漏洞 (KEV) 目录中缺少 156 个漏洞。此外，三款非常流行的扫描工具仍未针对总共 20 个勒索软件漏洞添加插件和检测签名。[2]

最重要的是，安全和 IT 决策者实际上将他们团队之间缺乏合作视为防御网络攻击时面临的最大挑战。[3]漏洞管理利益相关者之间的这种摩擦可能会减慢修复速度，并使组织容易受到攻击。

主要功能

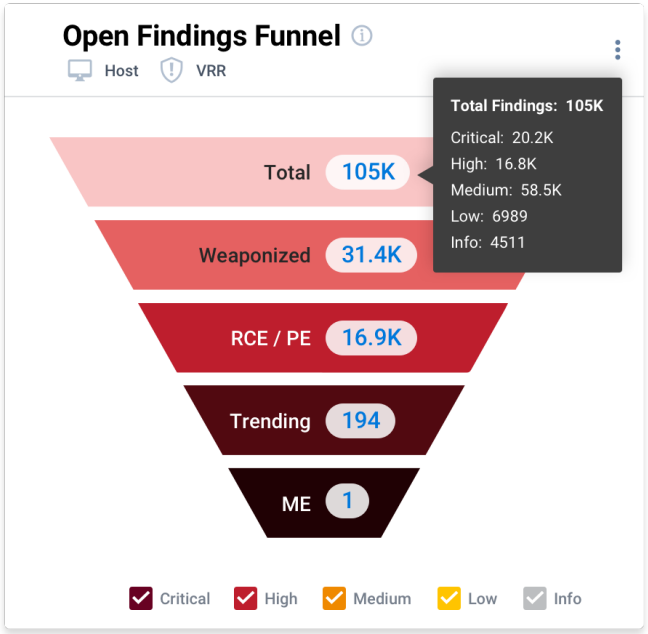
根据威胁风险对即时行动加以排序

从风险角度全面审视企业的网络安全态势，从检测发现漏洞和缺陷到修复只需几分钟——而不是几个月。Ivanti Neurons for RBVM 通过一个流程来衡量风险并对修复活动加以排序，该流程会将组织基础架构与以下信息进行持续关联：

- 内部和外部漏洞数据。
- 威胁情报的智能分析。
- 手动渗透测试和基于研究的发现结果。
- 业务资产的重要性。

最重要的是：您几乎不需要任何手动操作即可制定一个充分知情的攻击计划。

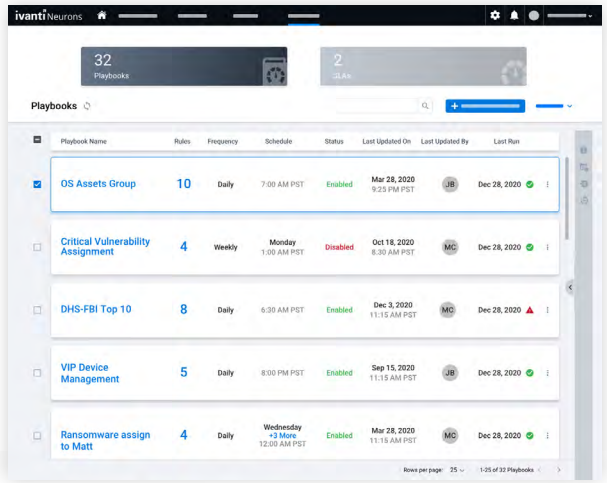
此外，与 CVSS 不同，Ivanti 专有的漏洞风险评分 (VRR) 使企业能够准确地衡量影响，并确定漏洞被利用的可能性大小。Ivanti Neurons for RBVM 还专门识别远程代码执行和权限升级漏洞、勒索软件漏洞，以及正在流行和活跃的漏洞。这些信息帮助企业专注于那些给他们带来最大风险的漏洞。

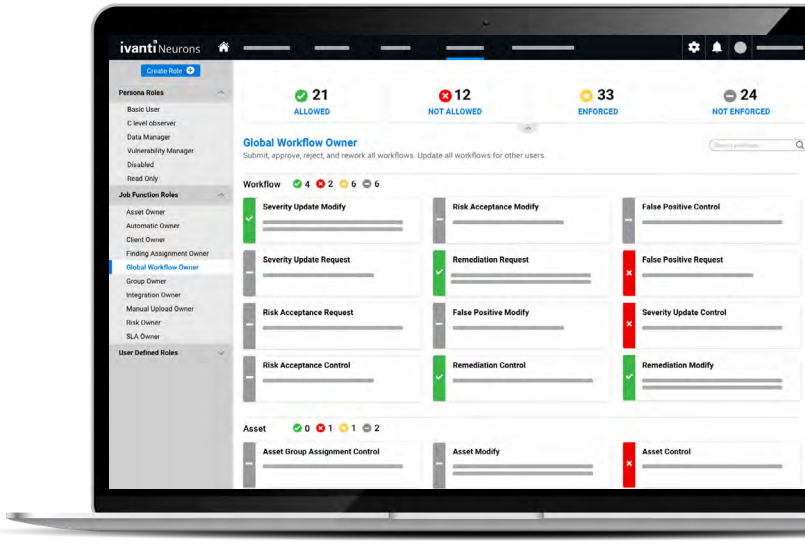


专注于修复，而不是繁琐行政工作

通过一系列自动化和其他提高效率的功能，改善您的网络安全状况，而且免除传统上与此相关的所有时间、精力和错误：

- 创建行动手册以自动执行传统上由安全分析师处理的常见或重复性任务。
- 如果需要，通过服务级协议自动化自动设置漏洞关闭截止日期。
- 可在产品以外接收近实时警报，并且可以通过这些警报中的链接打开包含与订阅事件相关信息的产品页面。
- 使用 Ivanti 安全团队推送的系统视图，依照流行标准轻松筛选主机和主机发现结果，揭示它们遭受高危漏洞（如勒索软件和流行 CVE）的风险大小。
- 将高优先级漏洞直接交付给Ivanti Neurons for Patch Management进行修复——不必再通过电子邮件和聊天发送 CVE ID 的 CSV 表格。





帮助安全利益相关者彼此之间能够更好地协作

及时向整个组织范围内的安全利益相关者提供与其角色相关的信息，促进他们之间的沟通与合作。Ivanti Neurons for RBVM 采用基于角色的访问控制 (RBAC)，因此能够安全地给所有相关人员提供平台访问权限。

进入产品后，用户可以访问专为从 SOC 到最高管理层的人员设计的仪表板。他们可以修改这些仪表板以适应更具体的用例，甚至可以利用用户小部件创建自定义仪表板，以满足不同角色和团队的确切需求。

此外，该产品还以 Ivanti RS3 评分的形式量化组织的风险状况。此分数可确保所有安全利益相关人在组织的整体安全级别上保持一致。与Ivanti Neurons for ITSM等工单系统的双向集成可改善那些致力于提高安全级别的人员之间的协调。

特性与功能

特性	功能
多样化数据源	借助一个可以从网络扫描的程序、对网络，主机、数据库和物联网设备等、来自 100 多个数据源的漏洞进行发现、来自研究和渗透测试团队的手动调查结果，以及自定义数据源中抓取数据，实现对网络风险的广泛了解。
威胁引擎	通过来自 Ivanti Neurons for Vulnerability Knowledge Base 的人工生成及 AI 驱动的威胁情报，获得对漏洞前所未有的清楚认识，比如哪些漏洞与勒索软件有关 。
漏洞风险评级 (VRR)	风险评分综合考虑漏洞的内在属性及其现实威胁背景，有助于快速确定漏洞所带来的风险。
Ivanti RS^3	通过一套专有评分方法综合考虑 VRR、资产业务关键性、威胁情报来源和外部可访问性，实现对企业风险状况的量化认识 。
自动化功能	用自动化功能替代一系列手动任务，使员工能够专注于修复行动和战略举措而不是行政管理工作。
警报和通知	通知引擎能够发出近实时警报，帮助您立即察觉相关事件。同样，通过利用深度链接，引导其他用户查看产品内的重要信息。
可定制的数据组织结构	通过用户小部件创建自定义仪表板，以及对数据进行列表透视处理的能力，从中发现可付诸行动的洞见。
仪表板	利用基于威胁的视图，快速发现高危漏洞（如 Log4j 和与周二补丁日发布相关的漏洞）如何在您的环境中显现。还可以创建并分享您的自定义视图。
基于威胁的视图	通过利用基于威胁的筛选器，快速了解BlueKeep、WannaCry 或 FBI/DHS/CISA 十大最常被利用的漏洞等特定威胁在您的企业环境中的表现。还可以创建并分享您的自定义筛选器。
Neurons 集成	利用与 Ivanti Neurons for ITSM 和 Ivanti Neurons for Patch Management 的现成集成使整个组织的漏洞管理从业人员能够更高效、更有效地执行自身任务。

关于 Ivanti

Ivanti 完善并保护 Everywhere Work，从而使员工和公司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 是为数不多的能够发现、管理和保护组织中每一处 IT 资产和端点的科技公司之一。有超过 40,000 家客户（包括财富 100 强企业中的 88 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.cn

ivanti neurons

ivanti.com.cn/solutions/ivanti-neurons
+86 (0)10 85412999
ContactChina@ivanti.com

1. 该数据于 2023 年 6 月 29 日提取自 Ivanti Neurons for Vulnerability Knowledge Base
2. Cyber Security Works、Cyware、Ivanti、Securin，“2023 Spotlight Report: Ransomware Through the Lens of Threat and Vulnerability Management”，2023 年 2 月 16 日。https://www.securin.io/ransomware/
3. ExtraHop，“Cyber Confidence Index 2022”，2022 年 3 月 1 日。https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/