ivanti

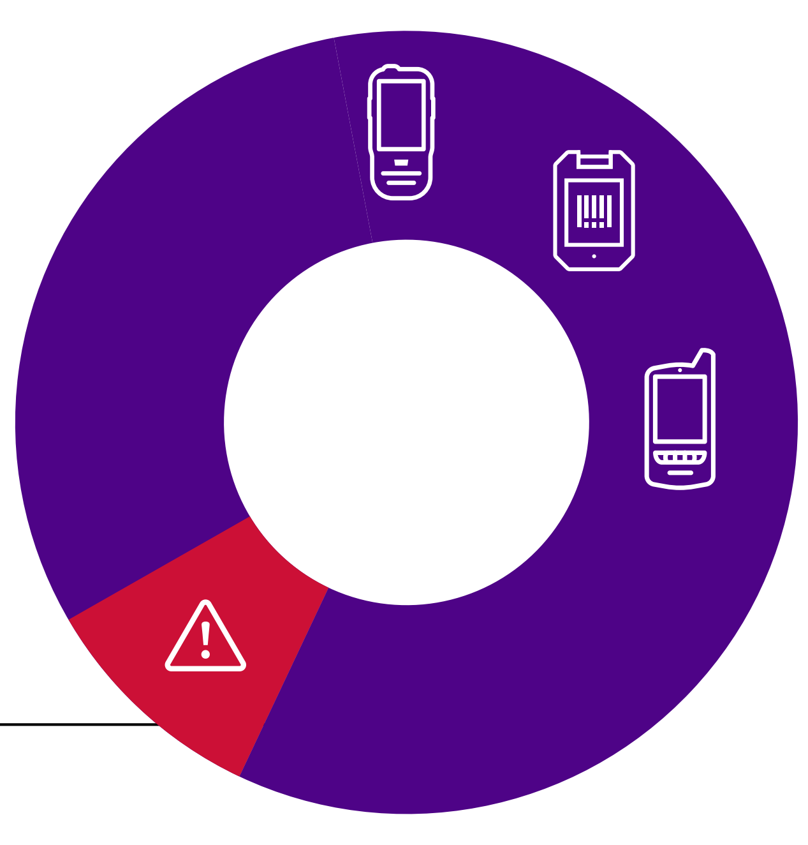
关于漏洞管理要解决的五件事

1 你的漏洞盲点

你无法保护和修补你看不到——或知道要寻找的东西。

在财富 1000 强企业中，
每 3 名员工中就有 1 名使用未经批准的基于云的 SaaS 应用。[i]

三个最流行的扫描器——Nessus、Qualys 和 Nexpose——
仍然遗漏了将近 8% 的
已知勒索软件漏洞。[ii]



2 缺乏团队带宽

想象一下，试图修补每一个存在的漏洞或风险——或者只是手动审查那些与你的组织和环境最切身相关的漏洞。

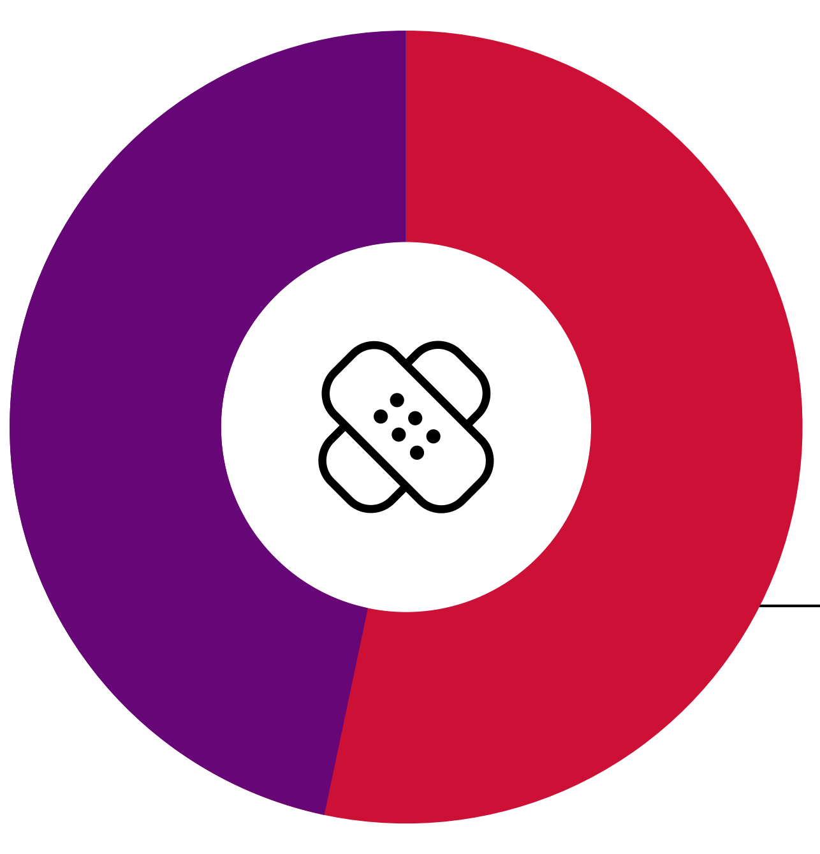
⚠
236,000+
关键漏洞和暴露 (CVE) 的总数

⚠⚠
29,000+
武器化的 CVE

⚠⚠⚠
9,600+
CVE 具备远程代码执行 (RCE) 和/或特权升级 (PE) 能力

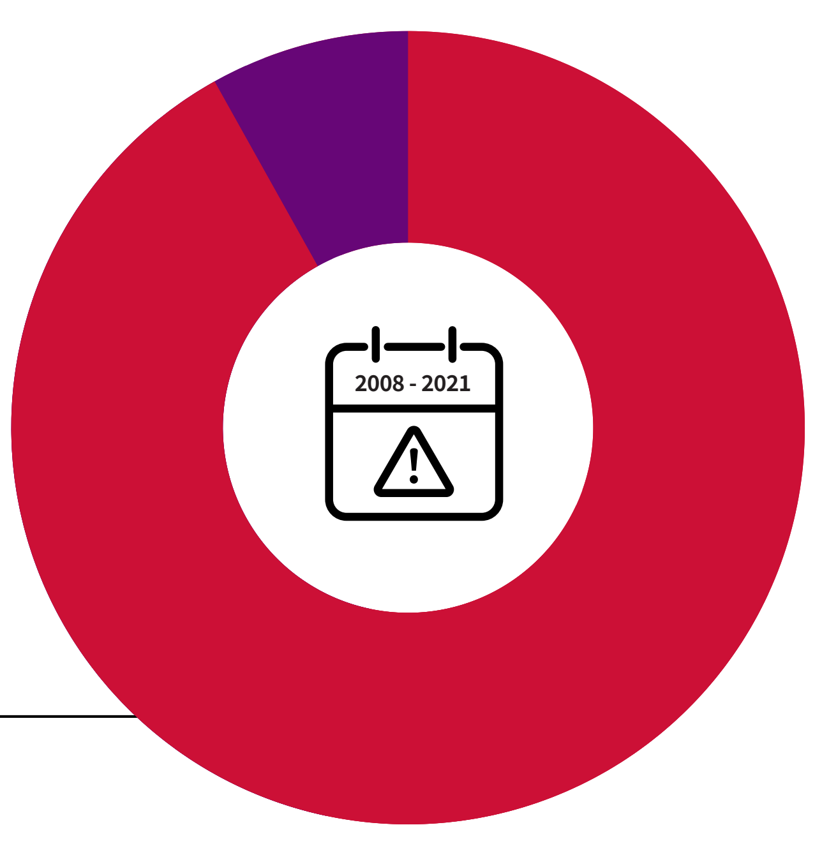
3 暴露于不太“严重”和比较老的 CVE 中

并非所有的漏洞都会带来同样的风险——你不能仅凭年龄或严重程度来判断哪些漏洞与你的组织切身相关。



如果企业只给被评为‘极危’的 CVE 打补丁，
将错过 53%
与勒索软件有关的可利用漏洞。[iii]

在所有正流行的活跃漏洞中，有 92% 的漏洞在去年之前就出现了——更有些漏洞是在早 2008 年首次发布的！[iv]



4 缺乏项目资源和内部认可

基本 RBVM

排序基于 CVSS 评分和扫描器评分

劣势
在很大程度上取决于数据质量和扫描器的更新频率

遗漏了与组织特定风险相关的低评分漏洞

优势
存在漏洞管理功能

中级 RBVM

排序基于去年 CVE 的被利用概率

劣势
需要经常性手动微调及验证

遗漏仍具相关性的旧漏洞（1 年以上）

优势
修复的先后顺序不再仅局限于 CVSS 评分

强调新的漏洞补丁

高级 RBVM

排序基于多来源威胁情报及情境化组织风险

劣势
需要全面的工具套件来覆盖多个数据源

优势
包含所有可能的漏洞数据来源

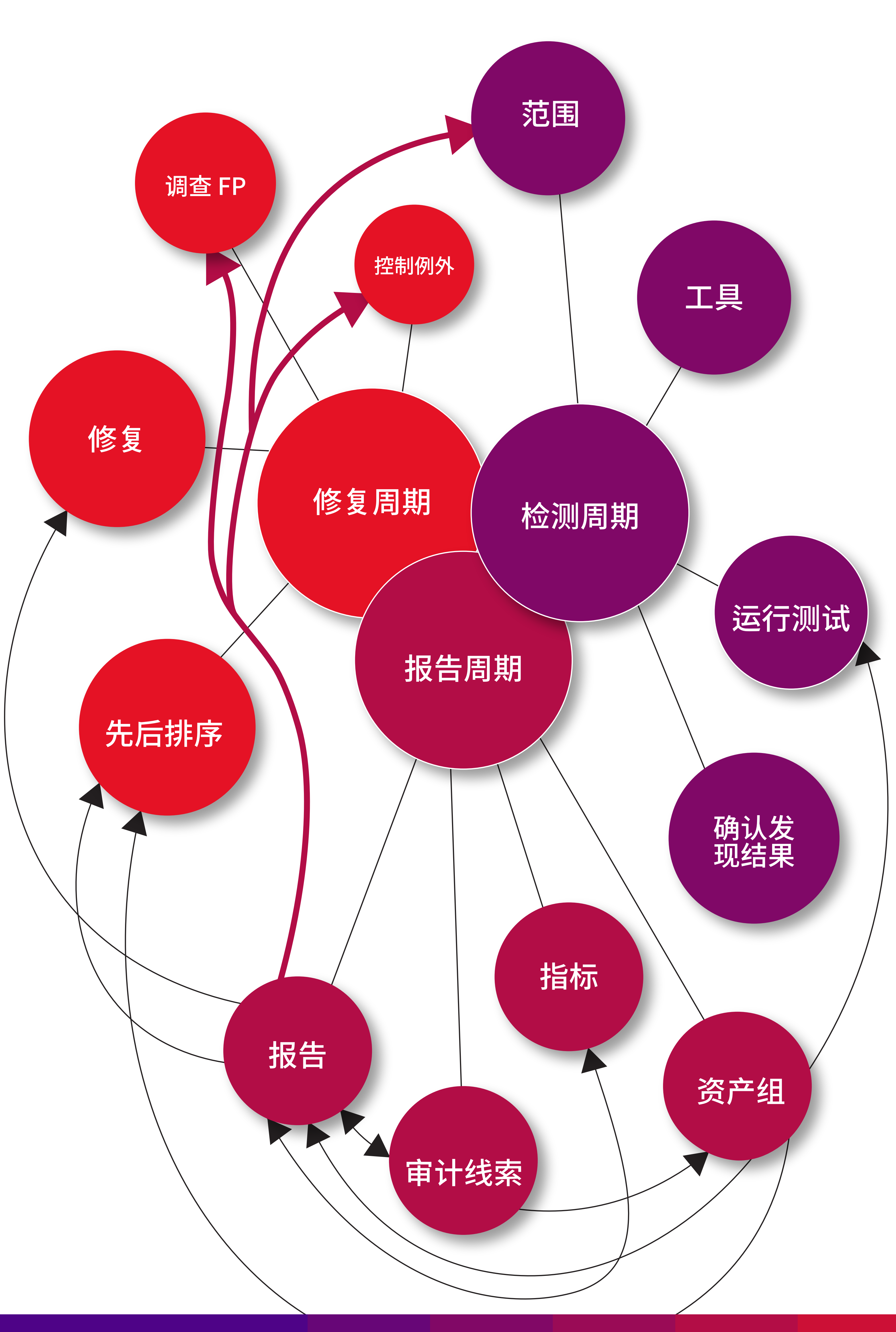
排序基于组织特定风险

迅速进行数据透视，以纳入新的背景信息并完善排序

5 报告

有效的漏洞管理计划可以根据需要迅速集结形成一个跨部门检测、修复和报告网络，以推动正确执行。

如果没有某种自动化工具来对漏洞信息和活动加以汇总、排序和显示，你的网络安全计划可能因无法满足报告要求而“胎死腹中”。[v]



它不必非得如此。阅读
2022 Spotlight Ransomware
报告，了解最新流行漏洞。

下载报告

---

[i] “Why shadow IT is the next looming cybersecurity threat” (The Next Web)
[ii] Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
[iii] Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
[iv] Ransomware 2022 Spotlight Report: Through the Lens of Threat and Vulnerability Management
[v] OWASP Vulnerability Management Guide (OVMG) - June 1, 2020