ivanti

基于风险的补丁管理之终极指南

IT 运维和安全在现代化补丁管理实施方面的工作参考

概要

目前在美国国家漏洞数据库 (NVD) 中登记的安全漏洞超过 187,000 个[1]，且平均每天增加 61 个新的漏洞[2]，那么组织实际上不可能把系统中的潜在威胁逐一修复解决。

更甚者，综合考虑所有可用数据表明漏洞总数超过 236,000 个，其中大约 12.4% 真正有威胁的已被网络犯罪分子利用[3]。

传统的补丁管理结构不能全面洞察整个漏洞情况，从而给你的网络安全网留下了危险缺口。

但是就算你知道每一个可能存在的漏洞，你又如何确定应该先给哪些 CVE 抓紧打好补丁呢？什么时候应该中断正常的维护周期，紧急开展最高优先级补丁的推广部署工作呢？

对策：基于风险的补丁管理。

作为最有效的风险缓解方法之一，基于风险的补丁管理超越了基本的通用漏洞评分系统 (CVSS) 得分和扫描器，能够识别和判定对组织设备、数据和最终用户构成最重大风险的特定漏洞。

基于风险的漏洞管理经此扩展，得以将那些对组织安全态势最紧要的已知被利用漏洞的最新信息纳入视野，从而将现实风险背景纳入补丁管理流程。

> “组织无法切实修复对其系统的所有潜在威胁。”

这种方法将漏洞结合了背景信息，使补丁管理员能够优先考虑关键的修复活动，并使运营团队能够透过与安全团队相同的真实风险视角，去理解其活动的紧迫性。

基于风险的补丁管理相较于传统线性补丁排序，需要额外资源来进行优先级确定，包括：

- 多个数据源（包括外部和内部），它们可以动态更新和快速汇总，以产生所需的信息，在与已知漏洞和补丁比对的同时，用于确定组织特有风险。
- 一个排序方案，它根据漏洞的破坏潜力、已知勒索软件活动、修复的难易度等因素，排出组织极具威胁性的漏洞。
- 足够的带宽——要么是足够多的团队人员，要么是日益完善的自动化功能——以便在出现极危漏洞时加以识别、警报并执行修复过程。

目录

紧要关头：漏洞太多，时间太少

美国国家漏洞数据库列出了超过 187,000 个漏洞，每个漏洞严重程度不一，这掩盖了它们对于个别组织的特定风险。[4]

而对于那些能够扩大其监测能力以覆盖所有可能数据源——包括 NVD 和 CISA 数据库、行业扫描器、漏洞赏金、渗透测试和各种行业威胁趋势研究——的组织来说，截至 2022 年 6 月，潜在漏洞的真实数量超过 236,000 个。[5]

其中，12.4% 有被勒索软件和网络犯罪所利用的已知漏洞。[6]

如果企业矢志维持一致安全性，仅凭如此巨大的数量就需要采取积极主动、主次分明的补丁管理方法。

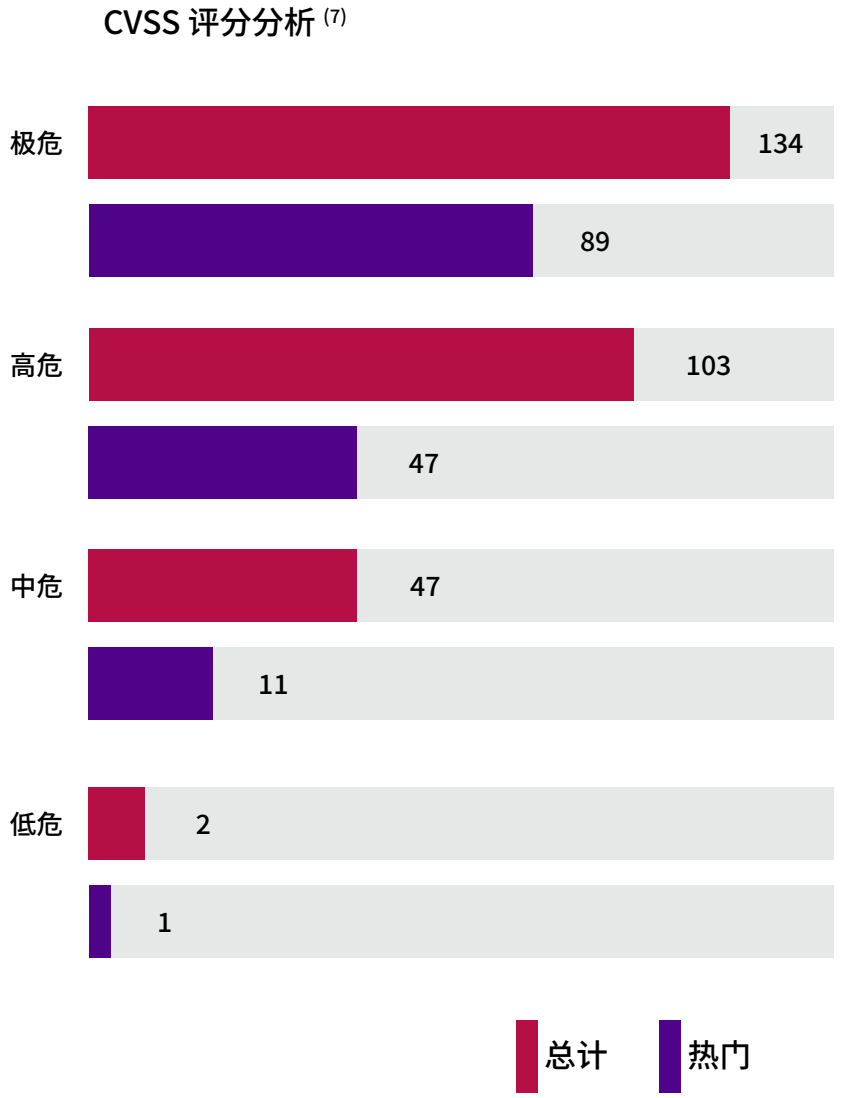
一共有超过 236,000 个已知漏洞。

其中 12.4% 的漏洞被广泛利用或以其他方式与勒索软件产生关联。

遗憾的是，供应商的威胁评级和 CVSS 并没有提供足够的背景信息来帮助企业内部安全团队列出他们应该优先关注的漏洞。

Ivanti 的最新勒索软件报告[8]，其中提到：

- 组织若只给评级为‘极危’的 CVE 打补丁，则会漏掉将近 40% 目前正为勒索软件团伙和其他网络犯罪分子所广泛利用的热门漏洞。
- 所有与勒索软件相关的活跃漏洞中，有 91% 的漏洞已经超过一年。



如果不把漏洞与实际勒索软件威胁——以及容易发生的远程代码执行 (RCE) 和提权 (PE) 漏洞攻击——进行映射，组织就很难在保证安全和生产效率的同时有效地确定修复的先后次序。

毕竟，安全团队必须逐一修补每个相关漏洞，才能保持其组织——设备、数据和最终用户——安全。

而网络犯罪分子只要抓住一次机会就行了。

实际后果：

Microsoft[9]

2021 年，Microsoft 解决了 23 个零日漏洞。

其中 15 个在补丁优先级别上仅被评为‘重要’而非‘极危’。

2021 年的所有零日 Microsoft 漏洞全部都被网络犯罪分子和勒索软件广泛利用。

传统补丁管理流程

传统补丁管理遵循线性的瀑布方法：

1. **安全团队的漏洞扫描器或数据库在环境中检测到**一个新的漏洞，推动CVSS 严重性评估，以便对高分漏洞实现分类修复。
2. **同时，补丁管理员对环境进行评估，**一方面作为定期维护周期的一部分，找出需要更新的软件，另一方面作为其修复排序工作的一部分，评估关键供应商严重程度——独立于安全团队的评估。
3. **安全团队和补丁管理员讨论补丁的先后顺序，经相互核对后，得出**一份需要优先修复的危重补丁列表。
   a. 一般来说，安全部门的建议会优先于补丁管理员和 IT 运维部门从供应商处征求得来的建议。
   b. 补丁管理员和 IT Ops 供应商的建议。
4. **补丁管理员找到相关补丁来修复优先漏洞**——如果存在的话——最好是先在沙盒环境中进行测试，然后再推广到更广泛的组织中去。
   a. 管理员们面临的现实是，测试环境很少包含现实组织网络的每一处细微差别。
5. **补丁铺开部署后，**可能因为干扰正常功能或与其他应用的互连性而导致关机或崩溃——即使该补丁在沙盒测试中的测试结果很好且没有任何预计影响。
6. **于是循环往复的清理工作开始了，**补丁管理员和安全团队都在检查推广部署的结果，并确认那些未能更新或者在这个过程中完全被忽略的机器。

传统补丁管理面临的挑战

任何做过补丁管理的人都能指出传统线性方法的缺点。
例如，勒索软件团伙可以在中央数据库识别出漏洞后几天内就对其加以利用，从而缩短补丁管理员识别并修复漏洞从而防范攻击的窗口期。

去年几个主要漏洞，如 QNAP、Sonic Wall、Kaseya 和 Apache Log4j，– 在被 NVD 收录之前就已经被利用了。[11]

的漏洞攻击发生在补丁面世后 14 到 28 天内[12]，网络犯罪分子只需要中值 22 天就能开发出功能性漏洞利用代码。[13]

实际后果：BlueKeep[10]

2019 年 5 月 14 日
CVE-2019-0708
随补丁发布。

2019 年 5 月 15 日
概念验证研究开始。

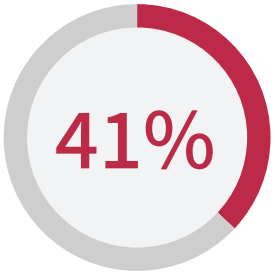
2019 年 5 月 20 日
BSOD 漏洞攻击得到研究机构确认。

2019 年 5 月 28 日
6 家独立研究机构实现了 RCE，
还有更多被网络犯罪分子证实的漏洞利用攻击。

仅仅 14 天就从公布发展到被网络犯罪分子广泛利用

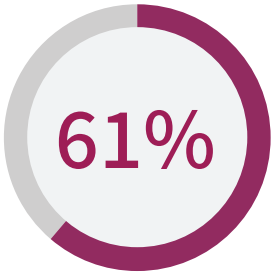
如果没有额外的带宽、资源和人员，补丁管理员和安全团队被迫只能依赖供应商严重程度评级和 CVSS 评分，不能进一步了解其具体的风险环境背景信息。

53% 的受访 IT 运维和安全团队报告称，他们大部分时间只是在对漏洞进行整理和排序，而不是积极修补！[14]

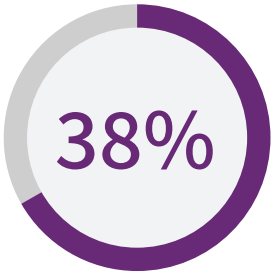


最近一项国际调查发现，在竞争异常激烈的就业市场中，41% 的受访企业由于工作量太大而导致 IT 运营人员流失。[15]

安全部门和 IT 运维部门之间目标不一致往往导致补丁失败和生产效率降低。



61% 的受访 IT 和安全专业人员每季度都会收到 一次推迟维护窗口的请求——28% 的人每个月 都会收到——这使得组织容易为了生产力上 的“眼前小利”而遭受网络攻击。[16]

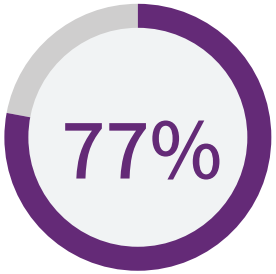


当网络攻击真的来袭时——正如 63% 的受访组织在 2021 年所遭受的那样——38% 的受害组织损失了整个一周的生产力；24% 的组织损失了整整一个月的生产力。[17]

大多数部门没有时间在部署补丁之前测试更新或与其他部门协调。

只有 15% 的 IT 运营和安全团队说他们把大部分时间用来测试补丁，而仅仅 10% 的人说他们把大部分时间用来与其他部门协调。[18]

扫描器和数据库并不能捕捉和公布所有漏洞。

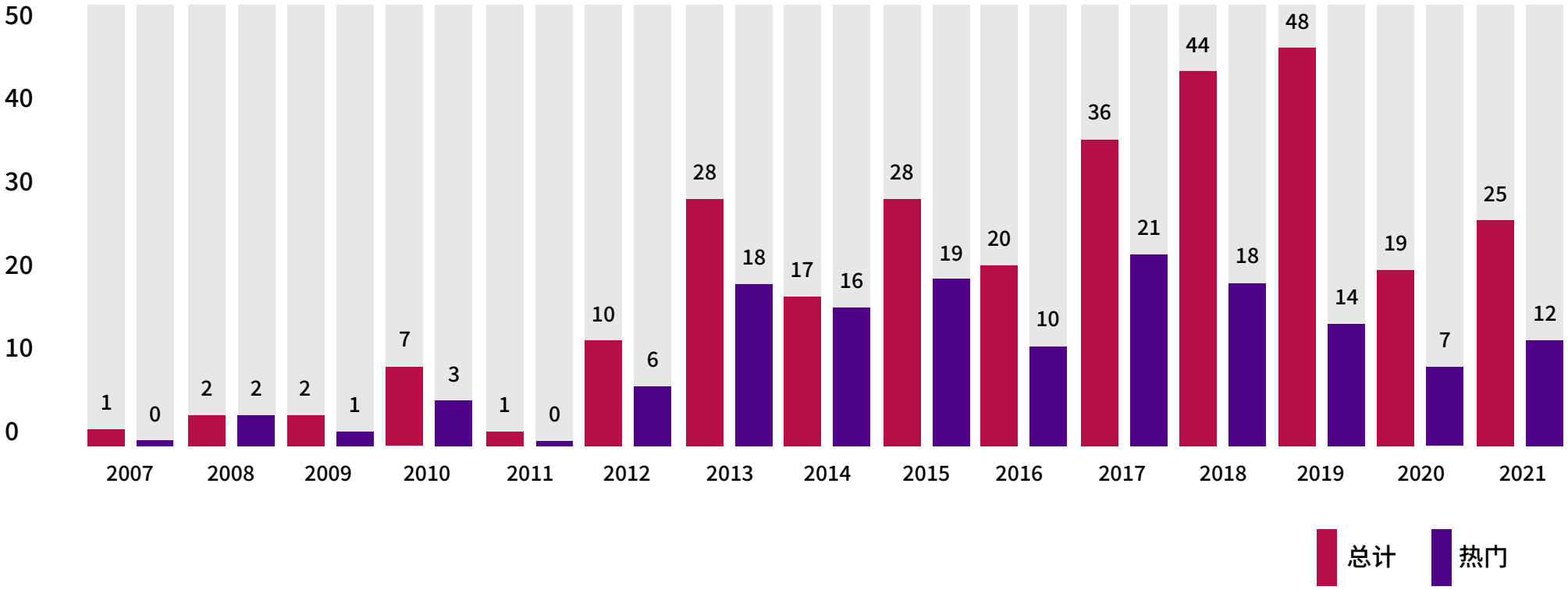


三个最流行的漏洞扫描器——Nessus、Qualys 和 Nexpose——去年仅检测出所有可利用漏洞的 77%。[19]

网络犯罪分子和勒索软件团伙仍然可以在他们的攻击中使用非极危漏洞或以前的漏洞。

- 如果企业只给被 CVSS 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。[20]
- 在所有活跃的热门漏洞中，有 92% 是在2021年之前公开披露的—— 有两个近期活跃的漏洞是在 2008 年首次披露！[21]
- 根据兰德咨询集团的研究，漏洞在首次公布后长达 7 年内仍继续被网络犯罪分子积极利用。[22]

NVD 发布的与勒索软件有关的漏洞及趋势[23]



38%
的网络犯罪受害组织损失
了一个星期的生产力。

24%
损失了整整一个月。

未修补的漏洞仍然是勒索软件团伙的主要攻击途径。缺乏快速反应能力对组织安全环境的损害立竿见影，并且严重影响其生产力和盈利能力。

并且，鉴于勒索软件漏洞的平均总成本估计达 462 万美元[24]，因此一个有效的漏洞修复战略对于安全和 IT 运营团队修补那些漏洞和薄弱环节至关重要。

但是，对任何 IT 运维或安全团队来说，逐一修补每个漏洞根本不是一个可行的解决方案，更别提那些工作超额、人手不足的部门了。

补丁管理员需要一个战略性的攻击计划，最大限度地利用那些通常有限的时间、人员和内部带宽资源，同时抢在网络犯罪分子和其他威胁者前面。

对策：基于风险的补丁管理 (RBPM)。

勒索软件漏洞的平均成本大约为

$4.62 万美元

基于风险的补丁管理：概览

基于风险的补丁管理战略采取一种有的放矢的补丁方法，而不是试图将一个组织独特的风险状况统统套进传统的“一刀切式”线性补丁方法。

首先，管理员从外部来源收集信息：网络扫描器、NVD 和 CISA 等数据库，以及手动研究和渗透测试得出的漏洞发现结果。

他们还收集内部数据点，以绘制出组织整个 IT 布局的确切风险状况。

此数据集包括：

- 组织 IT 和运营团队所支持的在用设备和操作系统清单。
- 组织最终用户目前所用的任何应用和软件——包括官方安装软件和用户自装应用，无论是本地下载还是基于云的。
- 了解如何检索数据——包括专有数据和客户数据——以及数据的存储位置和使用方式。

通过将外部漏洞及威胁信息与组织特有内部安全环境相互对照，补丁管理员可以对威胁信息加以通盘考虑，确定哪些补丁对组织来说是当务之急，而不是单纯以外部信息源作为威胁依据进行判定。

通过基于风险的补丁管理（RBPM），一个小团队就可以应付数量不断增长的漏洞，并保持组织、最终用户和客户的安全，且不会使已经捉襟见肘的 IT 运维和安全团队不堪重负。

基于风险的补丁管理（RBPM）方法对企业的 4 大益处

- RBPM 反映了介于“巨细无遗”和“躺平不管”之间的一条中庸之道。
- RBPM 提供了一种“基于现实”的漏洞排序方法，这种方法是为你的组织度身定制，同时通盘考虑实际的攻击信息，以确定真正重要的东西。
- RBPM 可以比传统的补丁管理方法更快。
- RBPM 构成了安全和 IT 运维各部门间的一座桥梁。

ivanti

1. RBPM 鼓励一种实事求是而非理想化的补丁方法。

基于风险的补丁管理方法承认并适应所有管理员身处的现实境地：漏洞太多，而资源太少，无法面面俱到。

另一方面，也不能就此选择彻底躺平：未打补丁的漏洞是勒索软件团伙和威胁者最主要利用的攻击途径。去年，与勒索软件相关的漏洞同比增长率达到了惊人的 29%。[25]

2021 年，与勒索软件相关的漏洞同比增长了 29%。

介于“巨细无遗”和“躺平不管”之间的一条最优中庸之道是 RBPM。

企业越早明白不加选择逐一修补——哪怕只是每一个被 CVSS 或供应商评为“极危”的 CVE——已不再现实，他们就能越快转换为积极主动、经过更新的补丁管理策略，从而更好地保护他们的用户、系统和资产。

而且，根据 Gartner 研究，即使一个组织不面面俱到修补一切，仅凭一个全面的基于风险的漏洞管理计划——包括RBPM——依然可以将组织的数据泄露事件减少 80%。[26]

理念上的小小转变就能让业务大大改进。

一个积极主动、基于风险的漏洞管理计划可以将组织的数据泄露事件减少 80% 之多。

2. RBPM 是一个“基于现实”的排序过程，它通过组织相关信息对风险进行先后排序。

通过根据勒索软件团伙的行为及其利用的漏洞——以及 RCE 和 PE 潜在危险等其他优先考虑因素——对问题进行排名，组织的补丁管理员可以对漏洞可能产生的影响做出更现实的评估。

这些评估不仅将漏洞视为一个个孤立的威胁，而且还考虑到通过“漏洞链”将几个漏洞组合起来的利用方式。

漏洞链是指勒索软件同时利用几个漏洞——通常是严重程度评级和诞生年数混杂不一的漏洞——对一个组织发动全面攻击。

例如，2021 年的 LockFile 勒索软件攻击(27)串链了源于 Microsoft Exchange 和 Windows OS 的四个漏洞：

“ProxyShell”

漏洞允许网络犯罪分子进入组织网络并触发远程代码执行进一步的额外攻击，以及安装后门以便以后访问。(28)

“PetitPotam”

漏洞让攻击更进一步钻入组织系统之中，以深入访问那些更有价值、更关键的系统 。

组织若仅遵循传统线性补丁管理流程，则不可能修补这次和类似攻击中所涉及的所有漏洞。

在 LockFile 勒索软件串链的四个漏洞中，只有一个被评为急需修补的极危漏洞，两个仅被评为有待修补的 “中危”漏洞。[30]

LockFile漏洞

漏洞	CVSS 评分	CVSS 严重性	产品
CVE-2021-31207	7.2	高危	Microsoft Exchange Server
CVE-2021-34473	9.8	极危	Microsoft Exchange Server
CVE-2021-34523	9.8	中危	Microsoft Exchange Server
CVE-2021-36942	5.3	中危	Microsoft Windows Windows Server 2008、2012、2016 和 2019

而且，尽管 LockFile 勒索软件攻击于 2021 年首次发生，但研究报告称，仍有 超过 34,000 次 ProxyShell 暴露在网上 ——等待新一批不良行为者利用这些漏洞。

3. RBPM 缩短了修补漏洞的时间。

极危漏洞的补丁打得越晚，企业就越有可能遭受数据泄露或产生勒索软件攻击的风险。

2021 年，国土安全部——通过网络安全和基础设施安全局 (CISA) ——发布了约束性操作指令 22-01。

这些对公共部门组织机构的新要求将极危漏洞的修补时间缩短到两周，并建议在组织基础设施面临“严重风险”的情况下可再调整时间。[32]

顺便说一下，这个 CISA 应补漏洞清单包含目前被确认为勒索软件系列积极利用的全部 CVE 的 20%。[33]

因此，即使安全团队利用漏洞排序系统来确定最急需部署的补丁，仍有大量漏洞尚待修补，且没有太多的时间来修补它们。

在传统的补丁管理方法中，管理员每次收到漏洞报告时，往往要花数小时研究和确定要采取什么行动。

相比之下，一些现代化补丁管理系统可以自动将漏洞信息与补丁数据和组织背景信息进行核对。这些核对增加了对组织特定风险的可见性，加快了整个修复过程，并减少了每个维护周期后的剩余清理工作。

CISA 应补漏洞清单只涵盖了所有被广泛利用的漏洞的 20%。

此外，全面基于风险的补丁管理方法也最有可能通过以下方式对抗或限制零日漏洞的影响：

- 知道漏洞确实存在，这样补丁一旦可用，就能在组织系统上得到优先发布和推广部署。
- 制定临时战略，在不妨碍日常运维的情况下减轻对潜在脆弱系统的影响。
- 建立一个内部警报系统，以便及时掌握网络犯罪分子可能利用该漏洞的情况。

通过发现更新并对其加以排序，保护组织内最脆弱的系统，补丁管理员可以充分利用他们的资源，保护系统免受外部网络犯罪分子和勒索软件团伙的侵害。

什么是零日漏洞？

零日漏洞是指具有以下特性的漏洞：

- 通常是在发生漏洞攻击后才得到供应商确认。
- 被网络犯罪分子广泛利用。
- 无法打补丁（或无补丁可用）。

4. RBPM 减少 IT 运维与安全团队之间的自然摩擦。

基于风险的补丁管理创造了共情同理的空间：

IT运营团队

更好理解安全团队的排序和为极危漏洞部署真正重要补丁的理由。

安全团队更好理解

一个糟糕的补丁可以影响业务、破坏关键应用并导致用户工单激增。

当 IT 运营团队相信安全团队正在适当确定补丁的先后顺序——这样他们就不会在每一个可能的漏洞上浪费自己或最终用户的时间——IT 运营团队就更有可能合作并主动找时间排除安全团队所列的最重要风险。

广而言之，基于风险的漏洞管理过程也可以教育这些团队，让他们知道如果不修补某个漏洞，他们可能会有何损失。

所要求的补丁不再只是为了解决众多漏洞中的某一个；风险是兼顾部门和业务结果加以通盘考虑的，因为假如某个可能的漏洞未得到解决，则最终用户体验和收入会受到影响。

2021 年，勒索软件漏洞的平均成本大约为 462 万美元。[34]

抽几个小时去做更新，当下确实会有所不便；然而勒索软件攻击可能造成一周或更长时间的损失；前者短期不便与后者长期风险相比，可谓无足轻重。

同样，当安全团队不希望面面俱到毕其功于一役——而是只堵住最重要的漏洞——他们就可以更灵活地与 IT 运营部门同事进行合作，从而不必非得在关键工作时间内核对补丁、缩减维护周期，并避免因计划外更新而使系统崩溃。

此外，现代化 RBPM 平台将数据分析和先后排序功能集中置于一处易于访问的地点或仪表板上，这么做有几个优点：

IT运营团队

无需等待安全团队递交漏洞报告。他们可以从仪表板上看到对其组织最重要的内容，并立即在一个干净的环境中着手测试更新，以提升响应时间，包括将相关的 CVE 映射到内部环境。

安全团队可以

一目了然地看到补丁推广部署状态、可能的瓶颈，以及那些有待在未来的冲刺或维护周期中予以解决的补丁。

在 RBPM 中，这个过程成为一个相互核对的过程——而不是没完没了的中断。

ivanti

能否手动运行基于风险的补丁管理计划？

基于风险的补丁管理是尝试修补所有内容的自然替代方案，但它远非一个直截了当的过程。

（毕竟，如果它很容易实现，那么本指南就不需要存在了。）

光是设置基于风险的优先级和实时跟踪漏洞变化（更别提适当的测试和补丁推广部署了）很快就会压垮那些没有准备好的团队——如果他们试图手动（而不是通过明确的工具或自动化流程）处理 RBPM 事宜的话。

比方说有一个组织想要实施 RBPM 战略。为了避免被过多的数据源所淹没，他们选择只关注 NVD，该机构去年平均 每天新增 61 个漏洞。[35]

作为他们 RBPM 理念的一部分——要求对新的漏洞进行全局通盘考虑，兼顾内部可能的受攻击面，而不是单纯依靠外部的严重程度评估——该团队必须每天手动审查所有 61 个新增 NVD 漏洞，执行 61 次单独的先后排序指令。(团队周一待办的工作会很可怕。）

而且，我们这里假设公司仅仅参考一个数据源而已，虽然这个数据源很全面。

更不用说他们还可以从其他数据库、研究和报告中获得的大量原始漏洞信息了。

真实后果：

漏洞和补丁核对

在与 Ivanti 专家的交谈中，世界各地公司的 IT 运营和安全团队都表示，他们传统的漏洞和补丁核对报告至少需要 8 小时才能手工完成。手工编写这些报告的专业人员承认，他们知道最终的文件虽然非常重要！但是不会 100% 准确。

不过，为便于讨论，我们假设自己的组织有足够多的安全和 IT 运营人员，能够直接定期监测大型供应商，如 Microsoft、Apple、Linux 和其他应用供应商，以便在漏洞和利用一经披露就立即把它们找出来。

网上甚至有一些地方——如 PatchMangement.org, Reddit 和 Ivanti Patch Tuesday 网络研讨会 ——会整理出特别相关的漏洞。这些和其他相关网站无疑是很好的资源，可以帮助团队免费通过整个 RBPM 过程中的这部分环节！

然而，监控只是在打补丁周期结束前需要完成的诸多任务之一。

作为 RBPM 过程的一部分，我们假设的这个组织的安全和 IT 运营团队仍然需要：

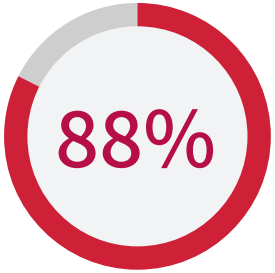
- 识别所有的内部设备和应用，包括IT 批准的和用户安装的。
- 确定哪些最终用户和用例需要首先打补丁。
- 在所有——或对特定漏洞而言尽可能多的——变化和变量中测试补丁。
- 安排并执行补丁推广部署工作。

特别是对于混合型或完全远程的工作场所，这些程序可能发展到无休无止的地步，从而无法跟上现实的速度。

最后但同样重要的是，许多手动系统使用电子表格类型的文档和数据库协同。

然而，依赖电子表格只会让各种错误纷至沓来。你有越多的人经常调整同一份报告，你就越有可能最终陷入错误层出不穷、累积成为代价昂贵的延误和更正的被动境地。

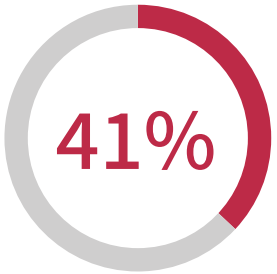
事实上，一项研究发现，88% 的电子表格都有“重大”错误——大多数是由负责编写这些表格的人造成的！[36]



的电子表格有“重大”人为错误。最后同样重要的一点是，许多手工系统需要使用电子表格类型的文档和数据库核对。

因此，虽然手动执行基于风险的补丁管理战略当然是可行的——特别是在开始的时候，这样可以在购买专用工具之前先对该方法有一个感觉——但对于真正希望采纳 RBPM 理念的团队来说，这并非最优配置。

目前有 41% 的受访机构报告称 IT 人员因工作量太大而流失，在这种时候还要增加更多的手工劳动似乎也是不明智的。[37]



的受访组织报告称，关键 IT 人员因工作负担过重而流失。

最终，以手动为先的方法将通过无休止的管理工作和冗长的时间线，从根本上扼杀任何实用的 RBPM 计划。

5个最佳做法助你实现基于风险的补丁管理（RBPM）

1. 您无法修补您不了解的东西。
2. 让 IT 运营部门和安全部门达成共识。
3. 通过内部服务级别协议（SLA）协同工作。
4. 成立试点小组。
5. 利用自动化手段！

1. 弄清楚你目前拥有什么以及你如何使用它。

你无法保护或修补你不知道是否存在的东西。因此，资产发现——找出你有什么，有哪些最终用户资料——在任何漏洞管理举措中都起着关键作用。

RBPM 中的资产管理

现代化资产管理工具可以帮助组织了解和跟踪他们当前的技术栈。它首先要确定所有的设备——笔记本电脑、台式机、电话、平板电脑、服务器和网络设备——以及组织内运行的软件。

就像更广泛的补丁管理计划一样，资产信息将有多个来源，例如：[38]

- ☐ Microsoft Endpoint Configuration Manager (SCCM) 和 Microsoft Intune
- ☐ CSV 文件或电子表格
- ☐ Microsoft Active Directory
- ☐ Workspace One (AirWatch)
- ☐ Ivanti Neurons for Discovery

在列出所有资产后，你需要删除重复信息，并确保所有数据在数据库中是一致的。

最后同样重要的一点是，IT 运营部门的资产管理员将对记录加以归纳整理，使补丁管理员能够找到最关键的终端和任何潜在的薄弱环节——这些信息将帮助你确定补丁的先后次序。

RBPM 中的服务映射

作为发现过程的延伸，服务映射可以帮助你找到需要管理和保护的系统，凸显它们——及其使用的数据——是如何相互连接和访问的。

服务映射可能包含：

- ☐ 基础设施和硬件清单。
- ☐ 应用、配置文档和一个软件库，其中列出了所用软件的最新版本。
- ☐ 设置和网络图，这将凸显信息流和设备在整个组织中的连接方式。
- ☐ 最终用户、用户配置文件和任何高风险终端，以及各自在受到侵害时对组织的关键系统可能产生的影响程度。

安全团队随后可以通过连接的用户系统或应用来映射攻击者可能通过漏洞到达关键系统的路径。

同时，IT 运营团队可以了解到有多少系统可能连接到某个关键应用，为如何最好地配置和实施补丁测试提供重要信息。

2. 确保每个人都能访问同样的信息。

基于风险的补丁管理效率取决于你的 IT 运营和安全团队如何协同工作，对其干预举措加以同步。为此，他们可能需要帮助开展跨职能协调工作，以实现他们所有的目标。

理论上，所有的团队都应该为同一个目标而努力：一个安全的、可以不受网络攻击干扰正常运作的组织。

实际上，他们的目标似乎是截然相反的：安全部门寻求降低风险，而 IT 运营部门希望优化最终用户的性能和体验。

安全团队

习惯于把 一 切都当作风险，往往没有切实可行的方法来识别对组织的切身威胁，也极少意识到补丁推广部署对日常工作的影响。

而 IT 运营团队

必须平衡他们的最终用户服务水平协议 (SLA)，保持正常工作如期进行，防范勒索软件理论上似乎从未罢休的潜在威胁。

一个优秀的 RBPM 系统将通过共享信息和达成共识的风险分析，来缓解摩擦点：

安全部门

将仅处理那些对组织网络安全态势真正要紧的漏洞。

IT运营部门

可以了解漏洞如何实时影响他们的最终用户，从而更愿意腾出时间进行推广部署。

3. 通过 RBPM SLA，协同工作以减少修补时间。

在最好的情况下，基于风险的补丁管理解决方案使所有参与方都能意识到漏洞以及如何实时应对它们。

IT 运营和安全团队将使用和掌握相同的方法来确定风险的先后次序，因此他们可以在修复过程中的多个节点上并行协同工作，以确保他们在需要解决的问题上保持一致。

这种方法可以将维护周期从几周缩短到几天或几小时，具体取决于漏洞的严重程度——以及每个团队与跨部门合作伙伴的同步程度。

IT 运营和安全团队都必须建立内部最佳做法，并共同商定维护窗口，且该窗口兼顾每个团队的目标以及组织整体目标。

为此，应考虑在 IT 运营和安全团队之间建立一个针对补丁管理的服务级别协议。

创建你的服务级别协议（SLA）

这个 SLA 应该确定每个步骤的合作期望和时限，以便每个人都知道所牵涉的事件、时间和人物。

SLA 应当包含：

- **所有的定义——** 即使是像何为“漏洞”这样的基础知识！
- **每个阶段**的必要规范和部署的技术栈。
- **漏洞排序标准。**
- **补丁** 周期内的沟通频率。
- **例外事项** 必须在out-of-band带外和/或常规维护周期之外修复漏洞时。

应特别注意为所有相关部门制定切实可行的关键绩效指标 (KPI)，并尽可能采用共享 KPI。

实际效果：

补丁和漏洞 SLA

一家拥有超过 10 万台设备的大型全球制造商向 Ivanti 介绍了他们在 IT 运营和安全团队之间实施漏洞服务协议的情况。

他们的组织在服务水平协议规定的 2 周时限内达到了 95% 的漏洞修复合规率。

4. 与关键的利益相关者建立试点小组，开展补丁的排序和测试事宜。

试点小组是一群预先确定（并经过预先培训）、有代表性的用户角色和设备配置，他们能够在向整个组织推广部署漏洞补丁之前，在实际环境中对其加以测试。

毕竟，如果某个补丁会使关键的软件崩溃，那么最好是拿几台机器测试，而不是影响整个组织。

试点小组弥补受控测试实验室环境的不足，能更好地预测补丁对业务活动的影响。

由于测试系统很少能确定下游影响，为补丁推广部署设置一个或多个试点小组，这对于减少潜在的负面运维影响至关重要。

“毕竟，如果某个补丁会使关键的软件崩溃，那么最好是拿几台机器测试，而不是影响整个组织。”

赢得对试点小组的支持和认可

这一最佳做法要求你的补丁管理员得到整个组织——不仅仅是 IT 运营部门——的支持和认可，因为相关试点小组应该包括任何设有关键系统的重要应用小组或部门。

为此，**不能局限于 IT 的服务地图，**而应当直接询问目标用户群，了解他们的设备和数据是如何彼此相互作用的，以及每次更新会如何影响他们的常规流程。

事先询问相关部门，而不是任由另一个补丁再次在工作时间内意外关闭他们的应用，这会为你提高用户满意率。此外，你所建立的人脉关系将构成未来试点小组的基础，包括苦心经营的利益相关者，他们将主动提供你在别处无从获得的帮助和洞见。

ivanti

创建你的补丁试点小组

试点小组应当：

- 在组织结构上至少包含一个初始“基本”试点小组——以确保没有什么大的问题——以及扩展试点小组，以确定更为罕见或特定应用方面的问题。
- 兼顾组织整体目标和所有相关部门——也就是 IT 运营和安全——的特定目标。
- 随时沟通反馈意见。
- 能代表组织内使用的所有设备，以确定任何补丁兼容性问题。
- 考虑到组织环境中的所有用户情况（也称为“用户角色”）。

员工和利益相关者——无论他们是否参与试点小组——都必须了解为什么修补漏洞对于减少勒索软件和其他网络攻击的风险至关重要。

传达的讯息要明确：测试对于保持组织和工作安全至关重要。作为试点小组的测试对象，在自己设备上忍受一点不便，意味着你顾全大局，让整个部门免于发生严重故障。

实际效果：

PrintNightmare[39]

2021 年 6 月，一名研究人员在 Windows 后台打印程序内发现一个 RCE 漏洞。

- Windows 当年 6 月发布了一个后台打印程序漏洞补丁时，于是研究人员认为他们特定的漏洞已经得到解决，并公布了他们的发现……结果发现 Windows 修补的是另一个漏洞。
- 网络犯罪分子很快就利用了这项研究结果，通过主动攻击，威胁行动者能够以管理员级别权限远程接管受害者系统。
- 第一个 PrintNightmare 漏洞在 2021 年 7 月 1 日打了补丁，在 2021 年 7 月 16 日又迅速再次发布。
- 此后，又有几个后台打印程序补丁陆续发布——2022 年 5 月又有四个。

由于对运营影响极大，许多组织现在优先考虑对这些补丁进行修复和试点小组测试。

2021 年 6 月
研究人员发现 Windows 后台打印程序漏洞

2021 年 7 月
Windows 发布了首个 PrintNightmare 补丁

2021 年 6 月
Windows 修补了另一个漏洞；研究人员公布了他们的发现

2022 年 5 月
又公布了 4 个后台打印程序补丁

5. 利用自动化功能——尤其是针对推广部署工作。

自动化对基于风险的补丁管理计划有极大好处，特别是在外部漏洞报告的收集、通盘分析和排序方面。

正如我们前面提到的，试图手动搞定一个 RBPM 计划，至少来讲很难维持，更不用说损害你的员工保留考核指标了。

不过，自动化还有助于在大规模修补的同时，对补丁推广部署工作加以细化，确保项目顺利运行。

自动化补丁推广部署的最佳实践

自动化规则和关卡可以围绕测试系统、试点小组和生产小组外围来实施最佳做法，以创建一个在加快执行速度的同时能最大限度地减少业务影响的补丁管理体验。

考虑从规模较小的基本测试小组入手，开始你的自动化补丁推广工作。然后扩展到：

1. 活动环境下的初始试点小组。
2. 早期采用者，他们在你的环境中约占 10%。
3. 其他大部分组织最终用户。

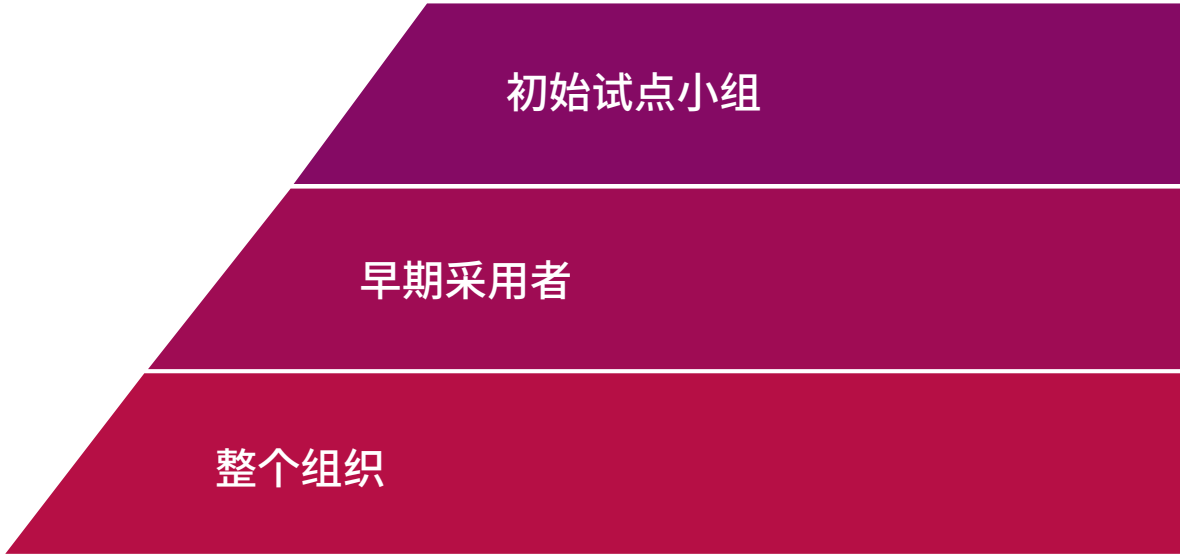
对于这个用例，补丁管理员可以设置标准，并为每个最终用户在各个小组中分配一个特定的角色，以此作为完整补丁推广部署工作的构成部分。然后，自动化将负责安排谁得到补丁，以及他们何时得到。

补丁管理员可以安排自动化流程按复杂的规则和接受标准运行，比如要求达到特定的成功响应率或直接用户反馈才能触发新的推广部署阶段。

自动化维护的优点

自动化可以处理定期维护工作（从而让所有部门的工作人员有更多的时间来改善协作）、支持一致的核对过程，并在特殊威胁到来时加以解决。

IT 运营和安全团队甚至可以共同开发和配置自动化安全控制，允许安全团队运行和监督较小的安全防护活动，这些活动按照预定触发条件激活，无需依赖 IT 运营团队完成每一项任务。

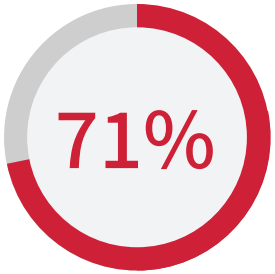


选择基于风险的补丁管理服务提供商

71% 的 IT 和安全专业人士认为打补丁过于复杂和耗时[40]，主要原因是缺乏适当工具来支持他们的补丁管理战略。

在实施基于风险的方法之前，评估你目前的漏洞和补丁管理流程。安全和 IT 运营团队必须协调好项目的目标，并就该项目所用指标达成一致。

具体来说，两个团队必须同意使用相同的基于风险的方法和排名系统，并且该系统不只依靠供应商严重程度和 CVSS 评分来确定更新的先后次序。



71% 的受访 IT 和安全专业人员认为打补丁太复杂和耗时 。[41]

你接下来基于风险的补丁管理平台应该包括：

- ☐ 数据：来自网络扫描器、端点、数据库、手动发现、物联网设备和其他独立来源的数据，能够提供深层信息及洞见。
- ☐ 各种各样的支持服务，涵盖所有内部支持的操作系统。
- ☐ 威胁洞见：它们来自人为生成的来源和其他威胁情报，用于指明哪些漏洞与勒索软件有关或是可被利用的 RCE 或 PE。
- ☐ 对独特风险因素的考虑：依据是组织的资产、多种威胁情报来源和外部可访问性。
- ☐ 自动化功能——或与自动化网络整合——用于修复和风险监测。
- ☐ 可定制的仪表板：用以快速与适当的利益相关者分享相关信息，而无需等待电子邮件转发或连锁提醒消息。
- ☐ 基于威胁的、可定制的筛选器：用于显示被利用的漏洞在组织特定环境中如何具体表现。

Referenced Sources

1. 美国国家漏洞数据库，访问时间：2022 年 5 月
2. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
3. 48,285+ 个漏洞成了 NVD 漏网之鱼：Ivanti 最新研究
4. 美国国家漏洞数据库，访问时间：2022 年 5 月
5. 48,285+ 个漏洞成了 NVD 漏网之鱼：Ivanti 最新研究
6. 48,285+ 个漏洞成了 NVD 漏网之鱼：Ivanti 最新研究
7. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
8. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
9. 只修补极危漏洞存在的问题：Microsoft 零日漏洞案例研究
10. 关于 Bluekeep 你需要知道的一切
11. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
12. 2016 数据泄露调查报告
13. 零日、千夜：零日漏洞及其利用攻击的全过程记录
14. 补丁管理的挑战：企业向无处不在的工作空间转变过程中的一些调查结果和洞见(2021)
15. 无处不在的工作空间中最主要的 IT 趋势 (2021)
16. 补丁管理的挑战：企业向无处不在的工作空间转变过程中的一些调查结果和洞见 (2021)
17. 7 个你需要了解的勒索软件趋势 (2021)
18. 补丁管理的挑战：企业向无处不在的工作空间转变过程中的一些调查结果和洞见 (2021)
19. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
20. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
21. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
22. 零日、千夜：零日漏洞及其利用攻击的全过程记录
23. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
24. IBM Security：2021 年数据泄露成本报告
25. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
26. 实施基于风险的漏洞管理方法
27. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
28. Microsoft Exchange ProxyShell 和 Windows PetitPotam 漏洞被串链用于新攻击
29. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
30. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
31. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
32. 约束性操作指令 22-01：降低已知被利用漏洞带来的重大风险
33. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
34. IBM Security：2021 年数据泄露成本报告
35. 2022 勒索软件聚焦报告：透过威胁和漏洞管理的视角
36. Pank, Raymond R. “What We Know About Spreadsheet Errors.” Journal of Organizational and End User Computing (JOEUC) 10, no.2: 15-21. http://doi.org/10.4018/joeuc.1998040102
37. 无处不在的工作空间中最主要的 IT 趋势 (2021)
38. 为什么 IT 资产管理就像玩拼图游戏一样
39. 2022 年 5 月 Patch Tuesday
40. 补丁管理的挑战：企业向无处不在的工作空间转变过程中的一些调查结果和洞见
41. 补丁管理的挑战：企业向无处不在的工作空间转变过程中的一些调查结果和洞见

关于 Ivanti

Ivanti 让无处不在的工作空间成 为可能。在无处不在的工作空 间，员工使用各种各样的设备访 问 IT 网络、应用和数据，以便能 够在任何地方保持工作效率。Ivanti 自动化平台连接业界领先的 统一端点管理、零信任安全和企 业服务管理解决方案，通过单一 操作窗口让企业能够为设备提供 自我修复和自我保护服务，并为 最终用户提供自助服务。已有超 过 40,000 家客户，包括 78 家财富 百强企业，选择了 Ivanti 来为他 们发现、管理、保护和服务从云 端到边缘的 IT 资产，并为员工提 供卓越的终端用户体验，无论他 们在哪里、用什么方式工作。更 多信息请访问 ivanti.com.cn

关于用于Ivanti Neurons for Patch Management

Ivanti Neurons for Patch Management 是云原生补丁管理解决方案，提供关于风险暴露、补丁可靠性和设备合规性、设备情况 和风险的信息及解决方案，可帮助组织更好地防范包括勒索软件在内的威胁。

ivanti

Ivanti.com.cn
+86 (0)10 85412999
contactchina@ivanti.com