Ivanti 白皮书

立即让您的 IT 安全实现现代化：10 大理由以及 10 大方法

ivanti

目录

简介

让我们直面这个问题。在保护用户和 IT 资源上，您的企业应该还能做得更好。您可能充分了解那些广为人知的黑客和被利用的漏洞，当然您对这些情况也很关注。但您企业中有限的资源并不能全部放在安全问题上，而且，您也还没有遇到过严重违规的事情。至少到目前为止是这样。

“希望”是逆境中的灯塔，但用来建立企业安全策略还远远不够。幸运的是，您现在不仅有充分的理由来改进企业安全性，也有现成的、可大幅提高安全性的方法供采纳。

立即让您的 IT 安全实现现代化的 10 大理由

1. **将风险降到最低。**更有效、全面且普遍的安全将为您的用户和企业 IT 资源提供更好的保护。这可以降低许多风险，不管是违规还是审计失败的风险。
2. **将 IT 和安全成本降到最低。**由 IBM 赞助以及 Ponemon Institute 执行的“2015 数据违规成本研究”，对 11 个国家/地区的 350 家企业超过 1500 名 IT 遵从和信息安全从业人员展开了调查。研究发现“数据违规的平均合并总成本为 380 万美元，相比 2013 年，这一成本上升了 23%。”此外，“每例包含敏感和机密信息的记录丢失或被盗所引发的成本上涨了 6%，即平均合并总成本从 145 美元上涨到 154 美元。”安全性的提高还能减少修补漏洞所耗费的时间和金钱，并更好地实现能大幅降低成本的自动化。
3. **实现静默的保护。**真正现代化的安全是广泛渗透、无所不在并且无法看到的，它对用户的工作效率或业务运营几乎没有影响。能够不打断工作即可改进安全性是保证用户满意度以及新特性和新工具能够被广泛采纳的基本要素。
4. **更多洞察，更多了解，更多保护。**最大程度的保护需要对 IT 环境和安全态势有最大程度的洞察以及了解。只有现代化的集成工具才能提供所需的洞察和了解，从而针对您的环境和企业交出最满意的安全答卷。
5. **增加企业敏捷性。**您的企业必须变得敏捷并保持下去，才能在激烈的市场竞争中生存和成长。简言之，缺少全面一致的安全方法，就无法保证敏捷性。
6. **增加企业恢复力。**一项在 2013 年由 Emerson Network Power 赞助并由 Ponemon Institute 执行的研究发现，数据中心停机成本大约是每分钟 7900 美元。一项在 2014 年由 Avaya 执行的研究发现，每次停机事件的成本在 14 万美元到 54 万美元之间，具体取决于受影响企业的规模和类型。而一项在 2015 年由 Kaspersky Lab 和 B2B International 执行的调查发现，单一网络安全违规的修复可能花费从 38000 美元 到 551000 美元不等。如此高昂的代价使得恢复力 — 也就是企业最大程度缩短计划内和计划外停机时间的能力 — 成为企业绝对必要的一项能力。
7. **增加企业可信度。**全世界最大的 PR 公司 Edelman 在 2015 年的信任度调查中调查了 33000 人。其中 63% 的受访者表示从来不会和不信任的公司打交道，而 80% 的受访者则声称只和信任的人以及公司来往。而没有现代化的高效安全措施，您很难，甚至不可能，确保并展示您企业的可信度。
8. **实现以用户为中心的安全。**现代化的、以用户为中心的 IT 对设备、文件和工具的关注更少，对用户的关注更多。为了实现以用户为中心的 IT，您的企业需要以用户为中心的安全 — 对所有授权用户、资源、连接和设备提供全面的、集成的保护。
9. **可操作化的安全。**现代安全管理的反应性和战术性更弱，相反，它更多地关注操作，主动性更强。在较大的企业，操作人员越来越多地执行安全相关职能，使得安全专员更集中地关注更为复杂和更具战略意义的问题。而不管在大型还是小型的企业中，大趋势都是逐渐脱离被动反应式的“救火行动”，而朝着持续交付新的和改进的安全方法，以及更为有效的主动安全操作（或称为“SecOps”）而努力。
10. **为将来做好准备。**根据 Verizon 2015 年的数据违规调查报告，10 年前，70% 的恶意软件活动都可以归因于仅 7 大系列或类别的恶意软件。到 2014 年，70% 的恶意软件活动已经涉及 20 种不同的恶意软件类型。与此同时，恶意软件已产生了巨大的演变，从电子邮件“蠕虫”到“隐形的指挥-控制僵尸网络成员、凭据盗窃以及各种形式的欺诈。”该研究还估计，世界范围内，每一天每一秒都会发生 5 次恶意软件事件。只有现代化的、以用户为中心的全面安全措施才能为您的企业提供如今和将来所需要的保护和适应能力。

立即让您的 IT 安全实现现代化的 10 大方法

1. 始终如一地为您的所有重要操作系统实施及时而全面的修补。
2. 始终如一地为您的所有重要第三方应用程序实施及时而全面的修补。
3. 始终如一地为您的所有重要设备实施及时而全面的修补，不论设备位于网络上的什么位置，本地、远程抑或是移动设备均可涵盖。
4. 建立非侵入式、无破坏性的应用程序白名单（如果需要还可以建立黑名单）。

即使除了上面四个步骤之外什么也不做，您也在改进企业安全和提供保护方面迈出了重要的一步。

- 根据澳大利亚信号局 (Australian Signals Directorate) 的估计，多达 85% 的针对性攻击都可以通过建立白名单，修补操作系统和第三方应用程序，以及限制管理权限来进行预防。
- 根据美国国家漏洞库 (US National Vulnerability Database) 的研究，在报告的漏洞中，有 86% 都是出自第三方应用程序。
- 根据 Verizon 2015 年的数据违规调查报告，“2014 年，被利用的漏洞中有 99.9% 都是在 CVE（公共漏洞列表）发布超过一年之后才遭到攻击的。”
- Ponemon Institute/IBM 对 200 位遭遇过数据违规的客户的调查表明，这些数据违规案例中只有 45% 是因为恶意活动或软件造成的。其他 55% 则是因为合法用户的操作失误、疏忽大意，或是系统的问题。

现在我们再来看看步骤 5 到 10：

5. 尽可能将您已批准的补丁和安全管理的流程实现自动化。这将最大程度提高执行的一致性以及这些流程的可伸缩性。
6. 集成主动式补丁管理以及您企业的其他重要 IT 方案，尤其是那些关注于 IT 资产管理 (ITAM)、IT 运营管理 (ITOM) 或者 IT 服务管理 (ITSM) 的方案。全面、有效、以用户为中心的安全是这些努力成功的基本条件。
7. 吸引、教育并激发用户去了解他们对于落实有效的安全措施的重要性。您的用户是您企业中的第一道和最后一道防线。全面、有效、以用户为中心的安全目标是保护他们免遭罪犯侵害，也不会成为违法犯罪的工具或帮凶。它还鼓励用户（包括客户）尽快向 IT 支持和/或安全团队报告事件和可疑的行为。
8. 不要“单枪匹马”地行事。企业越来越承认 IT 安全的重要性，以及它们需要 IT 和安全团队独立处置且不受干涉。许多企业也正在把安全预算和安全活动从主流 IT 事务中独立开来，将这些方面预算、努力和认知在整个企业范围内传播开来。记录显示，一些拥有良好口碑的知名公司还采用“众包”安全信息和智能的方式。而在您自己的企业中，您可以通过先吸引其他部门的同事参与其中来开始这一过程。
9. 使用环境和定制报告相关的智能来确定威胁并制定优先级，从而推广和鼓励对安全方案的支持，并推进和支持安全相关的决策。基于您自己环境中“实际”数据的基础架构智能和报告通常是最具说服力且最有效的沟通工具，可以用于和 IT 与安全团队以及其他团队的同事进行沟通。
10. 努力宣传，让安全相关的持续教育和安全态势的发展成为您企业中每个人心中的头等大事。就如同 Gartner 的分析师 Lawrence Pingree 在 2015 年 10 月向《纽约时报》介绍的那样：“已知有 6 亿个文件无恶意软件，而恶意软件高达 4 亿个。但还有 1 亿个文件可能是不需要的广告软件，以及 2 亿个软件包处于未知状态。要鉴别出哪些是正常的，哪些是不正常的，这一工作量非常巨大。”

您没法知道这 4 亿个已知的恶意文件是不是瞄准了您的企业，也不知道它们会在何时瞄准您的企业 — 即使只有一个未知，也就等于全部未知。而即使每年花费了 300 亿美元来开发安全工具，仍然每天都有漏洞和威胁变成实实在在的违规事故。通过将您的 IT 安全工具与流程现代化，您和您的团队可以极大地改善企业的安全态势，它们可扩展当前的防护能力，并针对未来做好准备。

Ivanti® 安全套件：现代 IT 安全

Ivanti® 安全套件提供了多层保护，可保护您的用户和 IT 资源免遭最复杂的攻击侵害。功能包括特定版本 Linux 的漏洞检测与报告、应用程序和网络访问控制、防病毒软件集成，以及 Microsoft Windows 与 Mac OS 补丁的自动测试、部署和管理等。

该解决方案还可以与 Ivanti® 管理套件集成，从而能够同时提供端点安全和端点管理。这实现了安全和 IT 管理策略的快速自动化，并针对 IT 安全和管理活动提供了无可比拟的可见性。集成还增加了 Ivanti® 工作区面向安全管理员的全面、可定制的界面，以及 Ivanti® 移动安全套件的增强移动保护。

Ivanti® 安全套件还提供了全面而可配置的报告和仪表盘选项。这进一步有助于强化对风险和威胁的可见性，简化了对法规和政策的遵从，并改善了总体安全态势。您的 Ivanti 销售代表可提供更多详细信息，您也可以前往 www.Ivanti.com.cn 获得更多信息。