多层安全让一切更简单

“网络攻击呈上升态势。”我们常听到这种报道，对吧？来看看现实数据。仅美国一地，2016 年公布的数据违规就逾 500 次之多——接近上一年的两倍。[i]2017 年 2 月，调研公司 Opinium 在采访欧美各大公司的 IT 决策者后发现，78% 的企业去年至少遇到了一次勒索软件攻击。泄漏一系列（包括臭名昭著的 WannaCry 所利用的）漏洞的黑客组织 Shadow Brokers 口出狂言，表示将通过“Wine of the Month Club”模型定期发布更多漏洞。世界上公开的勒索赎金第一次达到了百万美元级。[ii] Petya 只是让我们稍微体验了一把未来恶意软件武器的滋味。

如何阻止这一切的发生？如果没有集中的安全战略，设备蔓延将带来沉重的代价，让我们失去控制。IT 团队为管理这些设备花费了太多的时间。
而网络安全人员的严重短缺迫使公司优化其安全团队并确定使用综合技术的战略重点，以便简化管理、聚焦安全基础、针对现实网络攻击采取最高的防范措施，展现出远超其它解决方案的优势。

93% 的数据违规会在数分钟甚至更短时间内危害到企业，[iii] 在保护企业安全时，错误呼叫带来的成本是企业不能承受之重。

从软件修补开始

事实是，现在的许多漏洞其实早有补丁。比如，早在 2017 年 3 月，Microsoft 就针对其支持的操作系统发布了 WannaCry 漏洞的补丁（当时 Microsoft 甚至为旧版操作系统也发布了补丁）。但许多如 WannaCry 之类的漏洞依然存在，因为安全补丁虽已发布很久，却一直未部署。2015 年，Verizon RISK 团队发现，许多漏洞可以追溯到 2007 年。[iv]前 10 大已知的漏洞？85% 的攻击发生在它们身上。[v]

如何在不给 IT 人员和预算造成更多麻烦的前提下有效记录、修复和报告所有漏洞？您需要能够便捷地研究、评估、测试和部署整个企业内的补丁。而且，由于绝大多数漏洞影响到第三方应用程序，因此只是修补和更新操作系统还不够。

节省时间和资金，专注于支持核心业务活动。Ivanti 在数分钟内就能启动运行，根据您制定的策略自动帮助您发现、评估和补救整个企业中的 Windows、macOS、Linux 及 UNIX 系统。我们的工具可简化所有物理及虚拟系统中的修补。找到在线以及离线的工作站和服务器，扫描缺失的补丁并进行部署。然后修补从操作系统和应用程序到虚拟机 (VM)、虚拟模板的所有内容，甚至还能够通过产品与 VMware 的深度集成来修补 ESXi hypervisor。

Ivanti 还提供 Microsoft System Center Configuration Manager 插件，用于通过 SCCM 控制台自动化和简化第三方应用程序补丁的发现与部署。

用于修补解决方案的高级 API 堆栈与安全解决方案、漏洞扫描程序、配置管理工具（如 Chef 和 Puppet）及报告工具相集成。此集成不仅能在安全产品的大型生态系统中进行修补操作，还可以帮助弥合安全、IT 与 DevOps 之间的差距。例如，您可以自动将最新漏洞评估导入到下一批要测试的补丁中，帮助 IT 运营更有效地保护企业。就其本身而言，DevOps 主要涉及持续改进和自动化——然后集成补丁管理，促成更灵活、更一致的基础设施和系统。您可以将重要数据导入 Splunk、Reporting Services、Archer 和 Crystal Reports 等解决方案，加快对重大安全事件的分析、响应和解决速度。

阻止无法修补的程序

当然，修补无法防范零日攻击。另外，如果您无法进行修补（比如运行的是旧版系统），或者担心修补对您的环境造成某种破坏时，该怎么办？您需要通过应用程序白名单和权限管理等工具阻止未修补的应用程序。

必须让用户只能接收工作所需的应用程序，而不能引入可能降低桌面稳定性、影响安全性、违反许可规范、导致用户停机、提高桌面管理成本的未授权应用程序。

不过，锁定桌面虽然可以降低风险，但也会严重影响最终用户的体验。体验差会降低用户的效率，他们会更频繁地给帮助台打电话。这些用户可能还会因为系统被锁定转而向“影子 IT”寻求帮助，导致新的安全风险。

Ivanti 提供领先的解决方案，帮助防范未授权的代码执行，无需 IT 手动管理详尽的列表，也不会影响用户的生产力。Trusted Ownership™ 可自动阻止执行不受信任的所有者（如常见的 user 帐户）引入的任何代码，甚至是未知的代码。您可以轻松、精细地管理用户权限和策略，同时允许在发生异常时自行上报。我们可以简单而恰到好处地为用户提供他们履行职责所需的相应权限。

我们还将对 SCCM 环境的支持扩展到了应用程序控制。使用集中式控制台控制端点上的应用程序和最终用户操作。并且利用系统中心操作管理器 (SCOM) 收集应用程序控制的事件和审计细节。

通过安全管理提升保护等级

Ivanti 的端点安全平台结合自动化补丁管理和应用程序控制，以及强大的集成式端点安全管理——全局策略、安全诊断、远程端点控制、安全仪表盘和报告等。

Ivanti 可为您的安全解决方案增加高级防病毒和防恶意软件功能。我们还可以提供设备控制（控制可移动设备的使用，对可移动设备和硬盘进行加密）和高级保护，防范无文件攻击（禁用从互联网下载的脚本、学习应用程序行为、只允许受信任的应用程序运行脚本、防范内存攻击，等等）。此外，您还可以限制访问授权的网络或 IP 地址，针对个别系统或系统组自定义防火墙配置，包括配置最新的 Windows 防火墙。您可以侦测到企图对本地机器文件进行加密的动作，停止加密过程，并通知网络中其他所有电脑，将恶意软件列入黑名单，从而有效地遏止攻击。

方便的单一界面可让您轻松管理集成式安全组件及服务的设置和任务。强大的远程控制功能意味着您可以隔离、调查和清理整个网络的端点。控制运行迟缓的机器或者解决安全问题。获取实时信息，快速查找问题根源——显示应用程序声誉的相关信息、发现/运行时间及其他元数据，并从同一个控制台进行修复。此外，与系统管理工具集成可提高工作效率、增强对 IT 环境的控制。

实时仪表盘报告

最后，Ivanti 可帮助您知道结果。

您没有实时防护，也就无法实时了解您的环境，而 Ivanti Xtraction 可将报告形成检查表，通过实时数据和轻松创建新仪表盘及报告的选项，将正确的数据交到高管、董事、业务线 (LOB) 和应用程序所有者手中。

几乎您使用的每个工具（服务台、监控和 ITAM 工具集、电话系统等）都有预构建的连结器，让您摆脱编程、商务智能专家、电子表格以及数据仓库带来的诸多问题。Xtraction 还可以进行自定义，连接到更多系统，让每个人都能在环境中查看其企业范围内的数据，通过将海量信息浓缩成关键点来帮您轻松做出更明智、快速的决策。

[i] 隐私权利交流中心
[ii] https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/
[iii] Verizon 2016 数据违规调查报告 (DBIR)
[iv] Verizon 2015 DBIR
[v] Verizon 2016 DBIR