部署 ASD 四大策略，规避高达 85% 的端点攻击

时至今日，网络安全漏洞日益激增，用户和端点的境况也愈发危及，对于信息安全和 IT 团队而言，在企业安全保护方面时刻如履薄冰。行业专家不断强调，在这场保护企业计算资源和数据安全的持久战中，端点安全是真正关键的切入点。

为帮助信息安全和 IT 团队从容防范各种勒索软件及其他恶意软件，Ivanti 推出了功能强大且丰富多元的安全产品组合，其中包括端点权限管理、动态白名单、精细化审核收集和全面的补丁管理。

此产品组合可协助部署 ASD 四大“基本”缓解策略，即国际公认能有效防范网络攻击的 35 项措施之其中四项。澳大利亚信号局 (Australian Signals Directorate) 的一项研究发现，只要部署这四项措施，就可减少高达 85% 的入侵。

ASD 四大安全控制策略	解决方案
1. 应用程序白名单	Ivanti 应用程序控制
2. 修补应用程序	Ivanti Windows 补丁插件
3. 修补操作系统	Ivanti Windows 补丁插件
4. 尽可能减少管理权限	Ivanti 应用程序控制

白名单

Ivanti® 应用程序控制为 IT 和信息安全团队提供前所未有的端点控制能力，帮助显著降低安全风险，亦不会影响用户体验。Ivanti 采用了受信所有权™ 检查，令方案更胜一筹，执行白名单和黑名单作业之余，更能大幅减少传统方案在持续运维的相关麻烦。借助 Ivanti 的工具，应用程序访问权限可以根据用户、位置、设备名称、IP 地址、防火墙设置甚至时间等因素来对单个用户进行定义。这样，就能全面控制哪些程序/代码可以执行，以及执行程序/代码的人员、位置和时间。

修补操作系统/应用程序

Ivanti Windows 补丁插件是一款简单易用的软件解决方案，旨在探寻环境中缺失的补丁，并运用基于代理或无代理的方案，将缺失补丁部署至整家企业。除了修补操作系统外，Ivanti 还增加了第三方软件修补、虚拟设备修补，以及适用于网络内外所有 Windows 系统的补丁扫描。有了 Ivanti Windows 补丁插件，企业便能根据专属定义的策略，定期执行全面且一致的检查，以期发现、评估并修复成千上万个客户端系统，并且不必担忧整个过程引起网络堵塞或影响用户效率。

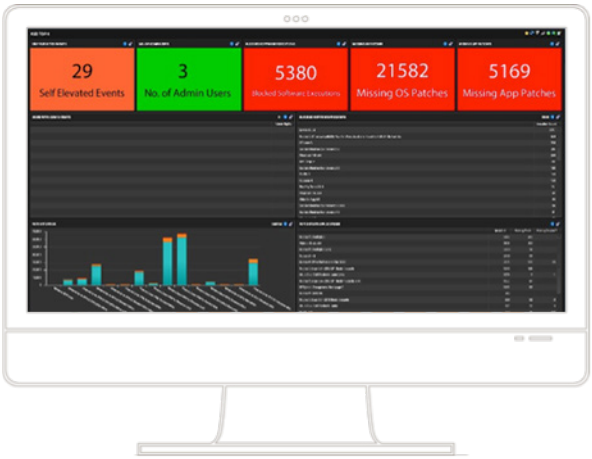
此解决方案兼容数据中心的所有物理和虚拟服务器，可以定位在线及离线系统，并对其执行扫描，最终妥善部署缺失补丁。适用对象范围广泛，包括 Windows 操作系统、虚拟机 (VM)、虚拟模板，甚至 VMware ESXi 虚拟机管理程序。

权限管理

Ivanti 应用程序控制不仅能对用户权限和策略执行精细管理，还支持用户自行选择权限提升。一经采用，即可对最终用户权限实施精准的动态控制，即只为用户提供所需的管理员权限，从而有效避免 IT 支持成本急剧攀升。Ivanti 无需本地管理员用户帐户，可从应用程序或单个任务层面进行权限管理，而非会话或帐户层面。既可以针对每个用户、应用程序或任务而提升、降低甚至取消权限，又可以提升或降低某个用户、组或角色的应用程序和控制面板程序权限级别。虽然不设本地管理员帐户，但用户仍可以访问需要管理权限的应用程序或任务，也能对访问进行全面审核和问责。

业务价值报告

Ivanti Xtraction 是一款功能强大的报告解决方案，可轻松整合多个来源的数据。各供应商工具和应用程序的报告界面可能各不相同，但有了 Xtraction，用户就能从多个工具和应用程序中提取相应数据，然后整合至单一的业务视图之中。企业能够（实时）整合并显示来自各企业系统的数据，包括安全管理、IT 服务管理、IT 资产管理、客户端管理等。IT 经理和业务主管则可直观了解各自的安全现状，然后进行深入研究，重点关注安全分析人员更加复杂的需求。



www.ivanti.com.cn

010-85153668

ContactChina@ivanti.com