Ivanti® 安全套件

Ivanti® 安全套件可以对最复杂的勒索软件和其他安全威胁进行预防、检测、隔离和修复。其拥有强大的多层保护机制，可自动发现和记录威胁，执行补丁管理，防止恶意软件运行或传播，并实现对受感染系统的远程控制和修复。灵活的报告和信息可视化功能可提高合规性，并有助于通过多种审核。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。

保护您的环境免受勒索软件和其他现代威胁的侵害

如果勒索软件入侵网络，Ivanti 安全套件将进行捕获和删除，并通知其他连接的计算机，阻止恶意软件在这些计算机上运行。数据保护功能可防止文件或硬盘驱动器被恶意加密。IT 人员可利用单个控制台查看所需的一切信息，以便于查找和修复恶意软件、诊断问题以及识别故障或未经批准的进程。强大的远程功能意味着 IT 可以隔离、调查和清理整个网络的端点。应用程序控制、基于主机的入侵防御系统 (HIPS) 和基于云的文件信誉功能可预防零日攻击、隐秘攻击和其他复杂威胁。

发现并记录所有的联网设备与软件

主动与被动发现技术能实时识别并记录所有启用 IP 的设备——哪怕是所谓的“离群”系统和那些藏在防火墙背后的设备。通过自动发现功能，可以看到这些设备中所有的软件，包括它们的使用详情。与 Ivanti® 云服务设备配合使用时，Ivanti 安全套件无需虚拟专用网络 (VPN) 连接即可在云端记录系统和设备。

在异构环境中实现综合性分层安全

通过多级防恶意软件保护、主动威胁分析和补救、防火墙、设备强化、USB 加密、网络访问控制、策略实施、漏洞修正等功能，Ivanti 安全套件能够为 Windows 和 Mac OS X 提供全面保护。该解决方案还可以检测和报告 Red Hat Linux、SUSE Linux 以及 CentOS 系统的漏洞。

通过自动修补功能确保用户环境稳定安全

Ivanti 安全套件提供最佳体验和自动化流程，能在不影响用户的情况下快速部署，从而简化了补丁管理。它能够可靠地修补网络中的所有设备，无论这些设备是在移动中、是位于远程站点处，还是处于睡眠状态。

ivanti

以更好的合规性来保护您的客户数据和盈亏线

Ivanti 安全套件针对各种政府和行业法规（包括 PCI-DSS、SCAP、FERPA、HIPAA/HITECH 以及 SOX）提供标准化的配置和工作流。这意味着您可以保护客户数据，维护企业的声誉，向审计者和主管展示合规性，并且保护盈亏线，免遭经济处罚和诉讼。

通过工作区、仪表盘和报告发现威胁、快速行动并展现结果

Ivanti 安全套件还提供一系列报告和执行仪表盘，帮助您监控安全措施的有效性，其中包括关于策略的实施、合规性水平、用户行为、补丁状态、实时安全违规警报等的详细报告。

结合端点安全与系统管理来降低风险

Ivanti 安全套件与 Ivanti® 管理套件集成，可统一端点安全性和端点管理。这样便能快速自动执行安全与 IT 管理策略，从而节省 IT 部门的时间与资源。Ivanti 安全套件还提供 IT 安全性与管理活动方面的出色可见性，从而降低风险和改善决策。管理套件集成还为安全管理员增加了可自定义的综合 Ivanti 工作区界面，并且强化了 Ivanti® 移动安全套件的移动保护。

通过设备和连接拦截来强化终端

通过设备控制功能，可以根据用户位置来限制用户终端可以访问的外部设备或连接的类型。此解决方案还可以检测并锁定连接到终端的存储设备上存在的恶意软件。此外，它还可以记录复制到外部设备的文件，以用于安全审计。

管理和保护远程设备

此解决方案使用 FIPS140-2 认证的加密技术来保护通过 Ivanti® 云服务设备连接的远程设备的管理数据。

集成首选的防病毒解决方案

除了提供 Ivanti® 防病毒管理器来防范已知恶意软件之外，Ivanti 安全套件还可以集成并管理用户选择的第三方防病毒解决方案。

有关安全的远程控制、电源管理以及其他功能的信息，请访问 www.Ivanti.com。

访问我们的网站：http://www.ivanti.com
与销售沟通：010-85153668 转产品咨询

ivanti