

# Ivanti 端点管理器的端点安全

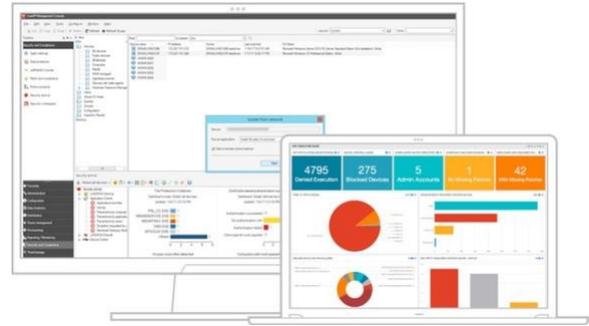
由 Landesk 出品的 Ivanti® 端点管理器的端点安全可预防、检测和修复包括勒索软件在内的最为复杂的安全威胁。它拥有强大的多层保护机制，可自动发现和记录威胁、执行补丁管理，并防止恶意软件运行或传播。与 Ivanti 统一端点管理器结合使用时，该解决方案的独特功能可帮助您隔离设备、远程控制被隔离的设备，进而修复或重镜像受感染的系统。将该解决方案与 Ivanti 端点管理器集成使用可以提高工作效率，增强对 IT 环境的控制。

## 保护您的环境免受勒索软件和其他新型网络威胁的侵害

借助 Ivanti 端点管理器的端点安全，您可以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，以及识别出故障和未经批准的进程。如果勒索软件入侵网络，端点安全将进行捕获和删除，并提醒其他接入网络的计算机，阻止恶意软件在这些计算机上运行。强大的远程功能可以帮助您隔离和调查整个网络中的端点，进而对有问题端点进行修复或重镜像。此外，设备拦截和连接控制功能可以让您可以对 I/O 设备的访问权限进行监控和限制。应用程序控制可预防零日攻击、隐形攻击和其他复杂威胁。而数据保护功能可防止恶意软件加密您的文件。

## 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，即便是所谓的“离群”设备（比如无线集线器）和那些藏在防火墙背后的设备也无处遁形。自动发现功能还可帮助您了解安装在这些设备上的所有软件，包括它们的使用详情。与 Ivanti 云服务设备配合使用时，Ivanti 端点管理器的端点安全无需虚拟专用网络 (VPN) 连接即可记录、扫描、隔离和修补远程设备。



## 自动修补以确保稳定安全的环境

Ivanti 端点管理器的端点安全通过最佳实践、自动化流程和快速部署，能在不影响用户的情况下大幅简化补丁管理。此外，它能够可靠地修补网络中的多个操作系统和第三方软件，无论这些设备是在移动中，或位于远程站点，还是处于睡眠状态。

## 通过设备和连接拦截来强化端点

利用设备控制和应用程序防火墙功能，可以限制端点能够访问的外部设备和网络的类型。您还可以拦截存在风险的设备，防止其通过网络连接引入恶意软件或偷取数据。应用程序防火墙可以阻止恶意软件的自我复制，使其不再具有威胁性。该解决方案还将详细记录那些复制到外部设备的文件，助您轻松通过安全审计。

配置和修补		检测与预防		修复和可见性	
包含	功能	包含	功能	包含	功能
设备发现	利用主动式、被动式和无代理式发现技术搜索设备并生成清单，全面了解需要修补和保护的设备。另外还可以检测并锁定无线接入点。	勒索软件检测	检测出恶意加密软件，将其删除并通知 IT 工作人员和其他设备。	网络隔离	隔离网络上的设备，防止恶意软件在网络中传输，同时保留对设备进行远程控制的权限。
补丁	自动对操作系统和第三方应用程序进行修补。	勒索软件预防	防止文件在其他位置运行和被加密。	遏制恶意软件	对检测到的恶意软件进行隔离。
	通过测试群组 and 日益增大的部署环，有条不紊地安排和分发补丁。	恶意软件检测	基于签名、网络和行为来检测恶意软件。	远程修复	远程控制；远程结束进程；远程文件管理；远程重镜像；远程部署其他取证工具和脚本。
	通过重启管理和维护窗口，防止补丁影响用户的工作效率。	恶意网站检测	防止用户访问可疑网站。	仪表盘和报告	借助 Ivanti Xtraction 仪表盘，无需精通 Excel，也能进行深入分析。该功能还提供漏洞、修补与安全活动仪表盘，以及警示功能和详细的安全报告。
智能修补	收集最终用户有关补丁性能的反馈，把影响用户体验的修补事件关联起来。	无实体文件攻击预防	拦截由 Microsoft 宏启动的无实体文件攻击。	SIEM 集成	将事件日志发送到 SIEM 工具，更进一步地实现商业智能与合规。
安全配置管理	开箱即用的 PCI 合规管理。	应用程序管理器	利用动态白名单功能可以全面了解环境中的应用程序，并阻止未经授权代码执行。	出色的统一 IT 解决方案	功能
	能够编写额外的合规管理脚本。	设备控制	防止在使用可移动存储和端口的过程中引入恶意软件或复制敏感数据，并记录所有数据复制活动。	Windows 10 迁移和 Windows 即服务 (更新)	自动提供已完成个性化设置且一切就绪的 Windows 10 设备，并维护 Microsoft 提供的所有更新和通道。
防火墙	阻止恶意应用程序自我复制和传输数据。			入职和离职	在用户入职或换岗时，提供适当的访问权限、应用和资源，然后在用户离职时移除其权限和许可证。
				自助服务 IT	用户只需简单几步操作，即可创建服务目录并将后台的服务、部署、资产管理所有内容整合在一起。

### 利用先进的应用程序控制防范零日威胁

通过防止恶意软件和脚本的执行以及使用内存保护技术，应用程序控制功能能够有效预防基于文件的攻击和无实体文件的攻击。学习功能可以最大限度地减少误报，并允许安全的应用程序顺畅运行。云端信誉数据库可提供关于环境中应用程序安全性的进一步洞察分析。

### 深入了解、迅速行动并展示结果

Ivanti 端点管理器的端点安全还提供一系列报告功能和仪表盘，帮助您监控安全措施的有效性。丰富多样的仪表盘让您能够利用可视化数据采取有效措施。您还可通过关于策略实施、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获得更出色的可见性。

### 通过统一 IT 加强安全

顾名思义，此解决方案通过与 Ivanti 端点管理器进行集成，将端点安全和管理整合起来。这样便能自动、高效地执行安全与 IT 管理策略，并优化 IT 资源。除此之外，该解决方案还提供 IT 安全性与管理活动方面出色的可见性，从而降低风险，让决策更可靠。

作为强大的附加组件，Ivanti 防病毒管理器能够有效拦截已知的恶意软件，并通过行为分析检测到其他恶意软件。当然，如果您拥有另一款防病毒解决方案的话，Ivanti 端点管理器的端点安全也为第三方防病毒解决方案提供了灵活的管理方式，让您可以根据需要进行选择。

版权所有 © 2018, Ivanti, Inc. 保留所有权利。IVI-1853 11/18 AS/BB/DL

了解更多信息



[ivanti.com.cn](http://ivanti.com.cn)



010-85153668



[ContactChina@ivanti.com](mailto:ContactChina@ivanti.com)