Ivanti 设备控制

移动设备和/或移动介质常因意外或偶尔恶意使用而引发数据泄露，种种案例已然敲响行业警钟。Ivanti® 设备控制能强制实施关于移动设备和数据加密的安全策略。此解决方案使用白名单/“默认拒绝”，可集中管理设备及数据，同时还提供额外保护层，以防恶意软件通过物理途径入侵。

预防数据丢失或失窃

随着远程办公的员工队伍愈发庞大，企业亟需支持员工通过外网访问数据。但此举亦带来严峻的现实问题，即数据可能会意外丢失或遭到恶意窃取。如今，移动介质/设备可谓数据泄露的“罪魁祸首”，究其原因，不外乎包括没有文件复制限制、未制定加密措施、缺乏审核追踪程序以及未予实施集中管理。Ivanti 设备控制能够确保安全使用此类效率提升工具，同时尽可能避免数据泄露或降低泄露影响。

主要功能

白名单/“默认拒绝”

向用户或用户组授予访问已授权移动设备及介质的权限。默认情况下，如果访问未经明确授权的移动设备/介质及用户，即会遭到拒绝。

对移动存储强制执行加密策略

集中加密移动设备（例如 USB 闪存盘）和移动介质（例如 DVD/CD），并在数据复制到设备/介质时强制执行加密策略。

数据复制限制

限制每个用户每天向移动设备及介质复制数据的数量，并限制使用数据的时间或时间段。

文件类型筛选

限制每个用户能够在设备与移动设备/介质之间传输的文件类型，有效遏制恶意软件传播。

集中管理/管理员角色

集中定义并管理用户、用户组、计算机和计算机组对网络上已授权移动设备/介质的访问权限。默认情况下，如果访问未经明确授权的移动设备/介质及用户，即会遭到拒绝。

临时/定时访问

向用户授予临时/定时访问移动设备/介质的权限；专用于授予“未来”特定时间段内的访问权限。

基于环境的权限管理

无论连接状态如何，也不管端点是否联网，均可强制实施并定制访问/使用策略。

基于角色的访问控制

根据用户或用户组的 Windows Active Directory 或 Novell eDirectory 身份，为其授予访问权限，两种身份均可全面支持。

防篡改代理

为网络中的每个端点安装代理。代理受到严密保护，未经授权，一律不能删除，即便是具有管理权限的用户亦不例外。只有设备控制管理员可以停用此保护策略。

灵活/可扩展架构

借助内置性能优化型中央数据库的可扩展客户端-服务器架构，于整个企业范围内实施控制和安全策略。支持虚拟服务器配置。

Ivanti 设备控制的工作原理

1. **发现**当前或曾经连接到端点的所有移动设备。
2. **评估**所有“即插即用”设备，具体根据类别、组别、模型和/或特定 ID，同时参考白名单来制定策略。
3. **设置**文件复制限制和文件类型筛选，并为转移到移动设备的数据进行加密。
4. **监控**所有策略更改、管理员活动和文件传输，确保策略持续生效。
5. **报告**设备和数据使用情况，以便记录使用是否符合企业和/或监管政策。

“部署 Ivanti 设备控制好处多多，其中包括白名单功能，能够阻止任何人使用任何未经授权的设备。闪存 USB 设备存在重大安全风险，可能会窃取企业数据，也可能因引入恶意软件而导致计算机故障，甚至是快速感染处于同一网络中的其他计算机。设备控制是一款功能强大但简单易用的产品，而这也是 Barclays 选择这款产品的原因所在。”

Paul Douglas
ADIR 桌面构建团队经理
Barclays

Ivanti 设备控制的优点

- 防止数据丢失/失窃
- 确保安全使用效率提升工具
- 强化安全策略的实施
- 实现精确控制与访问限制
- 防止恶意软件通过物理途径/集中和分散管理结构的映射入侵
- 支持监控打印机和物理介质的所有文件传输

www.ivanti.com.cn
010-85153668
ContactChina@ivanti.com