

保护 桌面安全

大家都理解保护终端的问题。其他人想要您拥有的私人数据和知识产权。另一方面，您的员工在工作时需要能够获取那些私人数据和知识产权。

为何终端总是饱受攻击

应用

- ▶ 每一行代码都可能是受攻击对象
- ▶ 攻击者正研究如何滥用代码中的缺陷
- ▶ 软件始终都会有攻击者可以滥用的缺陷

员工

- ▶ 每一个用户都可能是受攻击对象
- ▶ 攻击者对目标用户了解的比以前更多了
- ▶ 用户可能被欺骗安装恶意软件或提供信息

无论您扰乱哪一方，都将击碎攻击链。

“一个无需管理员批准或用户记录事件目的的例外进程 [用于应用控制] 能够极大地提升系统的易用性。”

FORRESTER®

有效的终端安全解决方案必须满足三个不同的实体

用户需求

- ▶ 性能
- ▶ 灵活性/控制性
- ▶ 一致性

所需的安全性

- ▶ 保护
- ▶ 合规性
- ▶ 审核的可行性

所需的桌面

- ▶ 终端可管理性
- ▶ 许可证管理
- ▶ 配置文件管理

代码执行。
禁用恶意软件！

应用控制是最后一道防线。它阻止绕过一切其他防御的未知恶意软件。无论它来自网站或是 USB 接口。无论它是可执行文件、自解压文件、脚本、注册表项或是屏幕保护程序。



1

推出“被动模式”的 Ivanti AppSense 用于应用控制和权限探索

2

回顾结果；谁真的在使用管理者权限，具体是什么权限，频率如何？

3

基于分析和激活创建配置。

保证终端的安全
仅仅是一个开始

- ▶ 彻底杜绝配置文件受到损坏
- ▶ 简化用户数据管理
- ▶ 增大用户密度
- ▶ 缩短登录时间
- ▶ 提高桌面响应速度
- ▶ 简化镜像管理

访问 www.ivanti.com 了解 Ivanti AppSense 可以提供哪些帮助

ivanti