

UserLock®

远远超越Windows® 自带功能提供的访问安全

IS Decisions®





在网络中用户登陆是
访问和防护的第一线

往往是
授权用户

（或共享他们登陆权限的人）

泄漏了
企业数据



安全功能需含



监测



限制



警报提示



报告

针对整个网络的所有会话活动



USERLOCK[®]

提供的安全功能

远超

Windows[®] 自带控制

USERLOCK® 数据化



1M+
在用LICENSE



3,000+
客户



遍布
100+
国家

创建一个定制化的访问策略 以应对任何可疑行为



适用于
台式机



适用于
笔记本电脑



适用于
平板电脑



适用于
智能手机



如何 运作

访问管理

限制&控制用户登陆

以支持您的企业策略

根据会话类型



工作站



WIFI



IIS



终端



VPN

按组设定



用户



用户组



组织单位

限制 或防止 并发 登陆

例如

限制用户同时启用会话



限制 工作站 访问

例如

限制用户使用自有设备



设定 时间限制

例如

避免在工作时间
之余进行连接



设定 时间 配额

例如

实行每天连
接时间配额





通过设定限制 您可以掌控

网络保护，拥有更清晰的视野

访问监控 & 智能化

USERLOCK[®]让您能

追踪、记录并自动拦截所有可疑会话

实时 进行 监控

追踪谁，
从哪个系统，
自什么时间起，
连接了多久，
等等。



接收警报 & 即刻响应

这种即时响应有效降低了内部的恶意活动风险。



报告 详细 信息

以支持IT取证和法律调查。





提高
用户
安全意识

您需要
直接告诫
最终用户
内部威胁



密码如同您的贴身衣物



需要时常
更换。



不要将之
与朋友分享。



密码越长，
越安全。

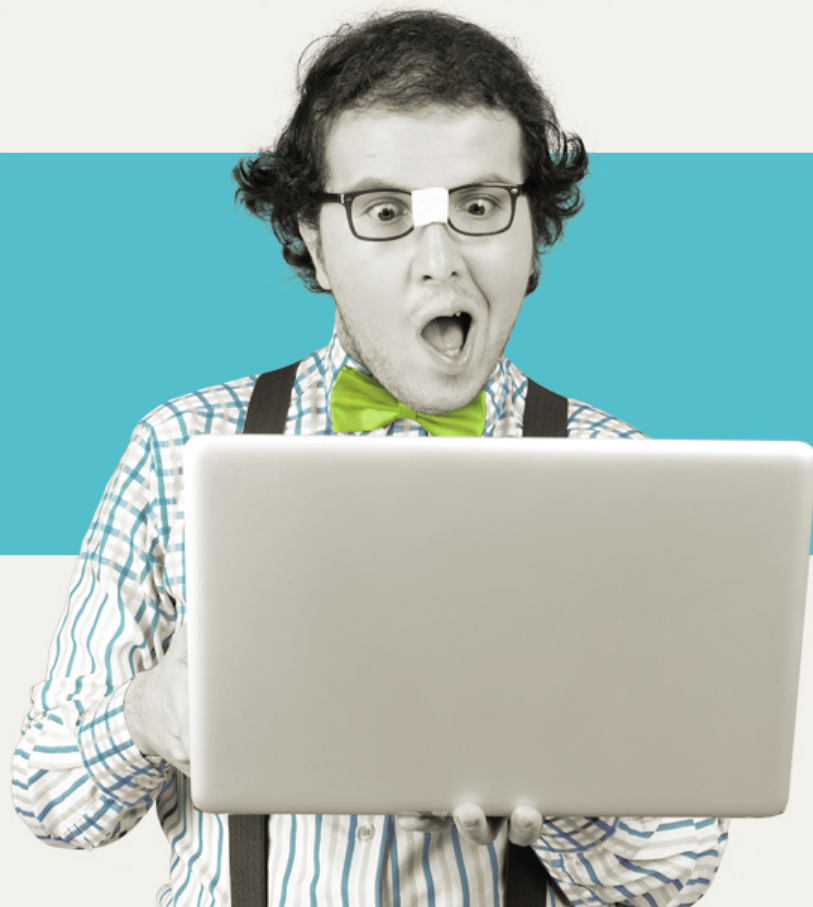


保持
它的神秘感。



让它与您
如影随形。

通过通知系统 公布策略



包含了量身订制的
法律申明





为
您的网络
提供
强大的
保护



减小您WINDOWS® 网络的攻击面

登陆会话控制远远超越了WINDOWS的自带功能，
让企业能够实施并执行高效的访问安全策略。



管理共享密码的 威胁

同时登陆会影响网络访问，
从而降低了用户分享有效凭证的能力。



39 %

的数据泄漏都是由于对
恶意攻击的疏忽所导致，
包括密码被盗。

让破坏性用户无机可趁 无法使用有效凭证

解决网络漏洞，让破坏性用户不能与合法拥有者
同时使用有效凭证（合法用户需要为其作出的任何非法行为承担责任）。



69%

的中小型企业目前还没有针对BYOD（携带自有设备到工作场所）的安全解决方案

确保BYOD环境安全

为无线网络和BYOD提供安全



21%

的电子犯罪都是
来自内部人员



43%

的公司在过去的一年中
都曾经经历过至少一次
内部恶意事件

减轻内部威胁

立即响应可疑或破坏性行为
从而降低内部人员的恶意活动风险



合规

实施CERT最佳实践并确保符合
SOX、FISMA、HIPAA等主要法规



进行精确的IT取证

在IT安全漏洞事件中，详细了解每一个会话访问事件
以支持IT取证和司法调查。



更多 优点

易于使用
与
企业价值

直接从控制台 启动命令

大大节省了管理和响应事件的时间



远程会话 管理

无论您在何处都能迅速响应突发事件。



POWERSHELL 整合

使用UserLock有助于迅速处理某些任务
并对相关信息执行个性化要求。



轻松安装， 易于使用。

几分钟内完成安装，直观的GUI功能为您提供一目了然的分析和大量的个性化选项。



更多优点

授权 管理

有助于指派任务，减少IT工作量！



公开&具备完整 证明文件的API

将UserLock中的有用数据整合到其他平台中，以提高IT安全管理的整体水平。



认证& 合规

经Microsoft认证&支持Windows Server
2012和Windows 8



备份服务器

安装UserLock备份服务器以确保故障切换。





立即下载

功能全面的免费试用版

WWW.ISDECISIONS.COM.CN