



Unified Endpoint Management 统一终端管理解决方案



LANDESK管理套件



资产的发现与管理
自动发现网络资产, 并且将收集到的资产信息集中展现, 检测资产变更, 便捷查询和报告



仪表盘和报告
为各级管理员设计直观的报告平台, 多格式导出, 自动邮件发送, 高级自定义报表



软件许可证管理
软件的使用分析, 有合理的分配, 优化您的许可证成本, 以便在任何时候应对软件审核



远程协助
跨平台的远程协助工具, 支持基于HTML5的浏览器发起的协助, 支持多种控制模式



软件分发
企业级专业带宽控制技术, 多播, 点对点下载, 快速分发, 支持多操作系统和多软件格式以及脚本分发



电源管理
绿色IT, 对主机用电进行管控, 定时休眠, 待机, 检测分析用电情况以及回报率分析



操作系统部署与恢复
捕获与恢复操作系统以及配置文件, 简化的模板, 支持与硬件无关性的驱动管理, 用户自助系统安装



自助软件门户
帮助企业搭建用户自助软件门户, 基于普通PC的应用商店, 用户可自行安装常用软件



MAC电脑管理
完整的苹果设备管理资产, 软件分发, 远程桌面等常用管理功能, 支持最新的MAC OS



移动管理器



移动设备管理MDM

- 基础设备信息: 设备名称、型号、操作系统、MAC地址等
- 远程锁定, 解锁, 密码重置
- 邮件配置
- 设备功能限制, 禁止摄像头, 禁止软件安装, 加密设备上的所有个人数据, 软件使用控制等
- 设备丢失后的擦除
- 配置证书, 凭据, VPN, WIFI



移动应用管理MAM

- 移动应用管理, 移动应用的下发, 安装, 应用商店管理等
- 应用封装, 将企业APP安全加固, 强制APP通讯以及使用安全



云服务设备

- 使原先LANDESK的安全管理套件在局域网管理的功能, 延伸至广域网, 主机在公网环境下依然可以受控



SHAVLIK 虚拟服务器补丁

- 针对VMWARE虚拟服务器的补丁管理技术
- 支持第三方软件厂商补丁管理
- 独创无代理技术, 无客户端
- 支持微软的SCCM扩展



IT Service Management

IT服务管理解决方案



开箱即用模式支持



移动IT服务管理

一旦员工需要服务的时候, 在任何时间地点, 可以为您的员工提供即时的IT服务和信息



IT服务目录

IT服务的内容直观可见, 轻松进入全天候对IT产品和服务的授权, 以帮助自己提高工作效率



流程自动化, 预置化, 支持开箱即用

服务台集成的IT工具和数据, 来改善服务水平以及响应时间, 并通过自动化流程来改进效率减少错误率



展现IT核心价值

轻松汇报服务台绩效, 以持续改善服务。迅速根据服务台信息, 获得可持续发展的珍贵内容, 以便做出最优决策



Secure Configuration Management 安全配置解决方案

USER-CENTERED



开箱即用模式支持



LANDESK 安全套件



补丁管理

使企业保持安全高效的环境, 及时自动地更新多厂家发布的补丁, 并且考虑带宽和网络的影响, 详细的补丁状态报告



应用程序控制

可以控制主机所运行的程序, 只允许运行合法软件或拒绝执行非法软件, 支持学习模式, 便于维护管理黑白名单



网络防病毒

集成卡斯基安全实验室最新版防病毒程序, 高效可靠的病毒防御体系, 客户端与服务器与桌面管理紧密集成



主机外设控制

阻止外设连接防止数据丢失和安装恶意软件。阻止非法USB设备的使用, 阻止连接非法网络, 允许例外处理



主机入侵保护

主机安全加固, 防止其他程序或恶意代码篡改设备关键位置文件, 注册表, 启动项等, 实时上报



安全准入

阻止非法主机连接网络, 对主机做健康性检测, 自动隔离不合规主机支持802.1X, DHCP, SNMP等多种准入技术



主机脆弱性分析

主机脆弱项, 包括间谍程序, 木马, 主机弱口令, 共享文件夹位置



策略位置感知

可以根据主机物理位置改变而改变, 自动切换正确的安全策略, 确保灵活性



审计套件



活动窗口审计

用户切换应用程序窗口的标题的审计



打印操作审计

记录打印文件名和页数等信息



文件访问审计

针对文件操作动作(新建, 修改, 重命名, 复制, 粘贴, 读取, 写入)



屏幕录像

根据记录特定条件记录桌面截图信息录像回放



存储设备连接使用

记录用户用户连接和断开各类USB设备详细信息。



应用程序使用审计

记录用户使用了那些应用程序、使用时间、使用哪个版本等详细信息;



剪切板审计

用户拷贝的文件名称和文本内容



上网记录

用浏览器所访问过的网站的审计



移动邮件安全 LETMOBILE

- 可以给原生的邮件客户端提供安全保障
- 友好的用户使用体验, 不需要改变用户日常收发邮件的操作习惯
- 使企业邮件与私人邮件的保护区分开来
- 移动设备上不存储任何邮件数据
- 支持双向的安全网关技术
- 安全用户文件夹, 附件存储网盘中
- 实时的DLP规则, 用户无法看到非法邮件, 或带有敏感字段的邮件基于上下文
- 解决了BYOD在企业中无法真正落地的难题



IT Asset Management

IT资产管理解决方案



自动化流程引擎

功能丰富的自动化流程引擎控件, 强化了ITAM管理中的自动化治理步骤, 提升中间过程控制环节



专业的软件资产管理

自动收集客户端软件安装信息, 软件许可证用量分配查看与管理



结构化的资产数据框架

从服务台, 财务软件, 系统管理, 以及更多的外部系统汇总数据



资产信息关联

自动将有关联信息的资产用图形映射到系统中, 看到他们是如何相互关联的。



条码扫描及盘点

支持常规条码扫描设备, 整合到资产入库, 出库以及盘点, 提高资产管理效率与准确性



资产生命周期状态与报告

资产的验收, 入库, 贴标, 出库, 维修, 领用等状态给予企业管理, 财务和IT人员提供更及时准确有效的信息

Unified Endpoint Management

统一的终端管理解决方案的竞争优势

- 用户设备已不只是传统Windows, Linux PC工作站, 还涵盖移动设备的管理Apple IOS, Google Android, WinPhone
- 业界唯一的针对Apple Mac系统全生命周期管理方案, 从操作系统部署-资产管理-远程-软件分发-软件许可证管理-补丁的完整支持
- 业界唯一的可以同时管理移动设备和传统PC的桌面管理以及虚拟服务器管理的专业厂商
- 使用单独的控制台管理传统PC和移动设备
- 确保我们能管理所有的用户终端的平台
- 利用统一的设备资产收集平台, 还可以给第三方应用提供接口
- 全线的无代理补丁管理技术, 技术领域的又一大突破
- 管理目标已从“设备”转向对“用户”, 不仅仅管理用户的设备
- 用户自助服务门户, 同时可应用在PC端和移动设备, 用户在任何地点可以得到来自企业的IT服务, 包括软件自助安装等

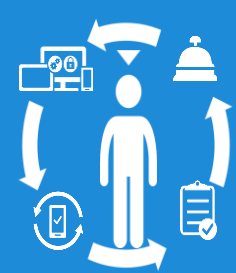
Secure Configuration Management

安全配置管理方案的竞争优势

- 外设使用控制技术升级, 能控制USB, 3G、4G卡, USB热点, WIFI的使用, 随身WIFI, 手机接入等多样行为
- 独立的软件白名单技术, 信任签名技术, 落地的软件使用控制
- 集成的防病毒解决方案, 桌面安全可包含企业版卡斯基防病毒, 除了可以少一台服务器, 还可以简化IT的管理, 并且支持Apple Mac的防病毒扫描技术
- 全面的“事前预防”“事中控制”“事后审计”管理逻辑
- 安全审计套件提供多种审计模式, 方便企业事后取证
- 独特的截屏压缩, 极小的容量提供了实时上传信息的可能
- 触发式的综合行为审计能力确保了获取有效证据的可能
- 移动安全能力提升, 解决了用户邮件客户端, 以往不注重客户使用体验的问题, 保持原生邮件客户端的同时保护邮件安全

LANDESK SCCM2012 Symantec 联软 北信源 MobileIronAirwatch 国信灵通

传统PC操作系统支持Windows	●	●	●	●	●	○	○	○
其他操作系统, Linux, UNIX, AppleMac	●	○	●	○	○	○	○	○
移动设备支持, AppleIOS/Android/WPhone	●	○	●	○	○	●	●	●
无客户端资产发展模式支持	●	○	○	○	○	○	○	○
指定位置, 指定结尾的文件以及注册表发现	●	○	○	○	○	○	○	○
软件分发对等下载带宽控制	●	○	○	○	○	○	○	○
HTML5远程协助, 可以从平板或手机控制PC	●	○	○	○	○	○	○	○
软件许可证管理, 自动检查企业许可证用量	●	●	●	○	○	○	○	○
设备发现技术, 自动发现未受管理主机	●	○	○	●	●	○	○	○
控制主机电源使用, 自动定时, 分析用电量及节省	●	○	○	○	○	○	○	○
支持苹果和Windows 操作系统部署	●	○	○	○	○	○	○	○
操作系统部署支持自动的硬件驱动识别与安装	●	○	○	○	○	○	○	○
PC端用户门户, 软件商店管理	●	○	○	○	○	○	○	○
支持多格式软件分发, EXE\MSI\BAT\VBS\PS1	●	○	○	○	○	○	○	○
支持第三方软件补丁以及无客户端补丁	●	○	○	○	○	○	○	○
基于自学习技术的软件白名单, HASH认证	●	○	○	○	○	○	○	○
支持802.1X, SNMP, DHCP等准入技术	●	○	○	●	●	○	○	○
支持广域网远程管理, 在没有VPN环境下策略同步	●	○	○	○	○	○	○	○
对丢失的移动设备进行信息擦除	●	○	●	○	○	●	●	●
对移动设备进行软件分发, 资产管理	○	○	●	○	○	●	●	●
非法移动设备不允许访问网络	●	○	○	●	●	○	○	○
控制移动设备上的软件使用与安装	●	●	●	○	○	●	●	●
可以审计用户对文件的操作修改和打印	●	○	○	●	●	○	○	○
当违规进程触发时进行截屏和回放	●	○	○	○	○	○	○	○
访问敏感网站时, 自动触发截屏动作	●	○	○	○	○	○	○	○
用户手机丢失时, 阻止手机邮件信息外泄	●	○	○	○	○	●	●	●
使用手机原生邮件客户端, 收发不改变用户习惯	●	○	○	○	○	○	○	○
遇到带机密或敏感字段的邮件, 禁止手机查看	●	○	○	○	○	○	○	○
禁止手机向非法邮件地址发送邮件	●	○	○	○	○	○	○	○
正常收邮件时能自动提醒, 有“叮当”声音的提醒	●	○	○	○	○	○	○	○



LANDESK 战略合作用户协议

- 您将同时拥有上述4套完整的LANESK企业解决方案授权
- 以用户数为产品授权模式
- 需签署专属协议
- 愿意与LANESK在用户为中心的IT管理中一起成长的用户

USER-CENTERED

IT Service Management



LDSO医疗行业开箱即用

- 6大开箱流程: 包含医院主要的事件管理流程、问题管理流程、知识库管理流程、变更管理流程、SLA 服务级别管理、KPI 绩效考核
- 5天的部署时间
- 固定的产品价格 (含软件授权和实施)

IT Asset Management



ITAM分散型企业开箱即用

- 7大开箱流程, 包括资产购置、入库、领用、交接、维修、处置、资产盘点管理
- 适合国内用户习惯的门户
- 7天的部署时间
- 固定的产品价格 (含软件授权和实施)

LANDESK WORKSPACE

用户角色工作台



- 基于用户身份的全新管理界面设计
- 在一个平台上实现不同的角色使用不同的管理控件
- 帮助最终用户更加便捷的自助服务
- 帮助管理员更快捷的使用自己的功能
- 提升了用户使用体验