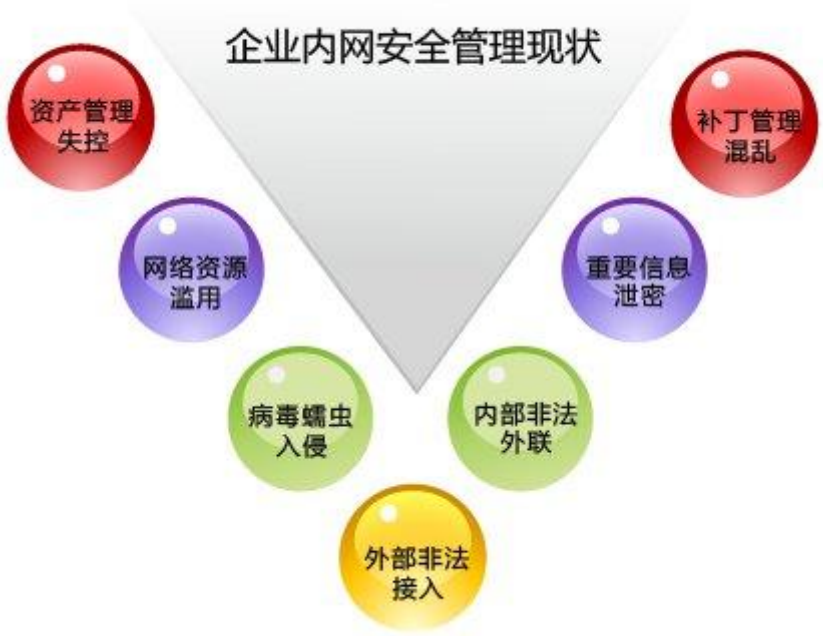
目 录

面对的问题（为什么需要桌面管理系统）



单位资产，员工私产——资产管理失控

部门内用户随意增减调换，每个终端硬件配备（CPU、硬盘、内存等）肆意组装拆卸，操作系统随意更换，各类应用软件胡乱安装卸载；各种外设（软驱、光驱、U 盘、打印机、Modem 等）无节制使用。

网络无限，自由无限——网络资源滥用

IP 地址滥用，流量滥用，工作时间聊天、游戏、疯狂下载、登陆各种娱乐、购物网站等行为影响工作效率，影响网络正常使用。

利用网络容易散布不良信息，如：煽动攻击，传播不真实信息、揭人隐私、诽谤他人等，不仅影响单位对外的形象，更可能带来法律风险。

恶意程序泛滥，危害业务——病毒、蠕虫、木马入侵

由于补丁更新不及时、网络滥用、非法接入等因素导致网络内恶意程序泛滥、引发网络阻塞、数据损坏丢失；无法找到灾难的源头以迅速采取隔离等处理措施，从而为正常业务带来灾难性的持续的影响。

门户大开，长驱直入——外部非法接入

移动设备（如笔记本电脑）未经授权接入公司网络和新增设备（如 U 盘）未经过安全检查连接 PC，这些可能带来病毒传播、黑客入侵等不安全因素。

内部威胁，不可小视——内部非法外联

内部用户通过调制解调器、双网卡、无线网卡等设备进行在线违规拨号上网、违规离线上网，或违反规定将专网专用计算机带出网络进入到其他网络。

网络无界，一损俱损——企业数据泄密

因系统漏洞、病毒入侵、非法接入、非法外联、网络滥用、外设滥用等各种原因与管理不善导致组织内部重要数据泄露或毁灭，造成不可弥补的重大损失。

千里之堤，毁于蚁穴——补丁管理混乱

终端用户不了解系统补丁状态，不及时打补丁，也没有办法统一进行补丁的下载、分析、测试和分发，从而为恶意程序泛滥与黑客入侵提供了机会。

明确目标（具体细节需在测试后明确成文）

资产管理：掌控 IT 资源

计算机软硬件统计，移动存储授权管理

软件管理：掌控终端程序

补丁分发，软件分发，软件升级

效率提升：提升工作效率

杜绝与工作无关的程序运行，控制网络访问，提高工作效率。

资源优化：提高 IT 资产利用率

监控 PC 运行效率，合理调整资源；合理分配带宽资源，提高带宽利用率，降低互联网接入成本。

数据安全：阻止企业信息外泄

确立互联网使用细则，避免公司信息和商业机密的泄露；记录用户行为以便统计、审计、分析。

安全审计：避免法律和政治风险

监控邮件、BBS、IM 等收外发信息，记录相关信息，控制不合规行为，避免引起的法律、政治风险。

网络安全：降低互联网访问安全风险

禁止访问高风险网站，减少病毒、木马、流氓软件的攻击几率，降低互联网访问的安全风险。

公司需求整理（完善中，还需考虑分阶段实现）

当前整理的需求如下表，涉及资产管理、数据安全、网络接入控制、桌面行为管理、网络行为管理、软件分发、维护管理等诸多方面。

需求整理表

类别	说明
一、软、硬件资产管理	
	软、硬件资产信息自动收集；手动添加属性和记录，整合软件版本和 License 管理；可以导出资产记录。
	记录 PC 硬件变化日志，能设置相关报警；硬件发生变化时能产生报警；
	较强的报表统计分析功能；
二、数据安全管理	
计算机外设管理控制	设置并查看每台客户度上禁止访问的外设端口和设备（声卡、光驱、软驱、Modem、mobile modem,网卡等）；能区别 USB 存储设备、USB 狗、网银盘；
三、用户行为管理	
上网行为管理	1、控制客户端接入内网和互联网； 2、控制客户端访问互联网流量，能控制不同程序访问网络的流量； 3、控制客户端不同程序访问网络优先级和带宽； 4、设置客户端网站访问白名单、黑名单,跟踪记录用户对于网站的访问； 5、限制电子邮件的附件类型和大小；并记录进出邮件。Web 方式的邮件及附件也能记录；邮件内容智能报表分析 6、IM 软件限制和聊天记录和智能报表分析，传输文件的历史记录；FTP 等文件传输历史记录； 7、BBS、SNS、blog 等互动网站关键信息记录和智能报表分析； 8、非法外联行为控制审计
文件操作审计	1、能对特定文件（按照类型或目录）操作（创建、修改、复制、拷贝、粘贴、删除）进行记录。包含对 USB 存储设备的文件操作；
程序运行审核	1、设置客户端软件访问黑名单或白名单，记录用户对于软件的访问。注意一定不能仅仅通过简单的程序名称来进行限制；
四、系统维护管理	
	1、能远程控制客户端；能制定不同策略允许客户端接受后才能接受控制；
	2、提供客户端及时通讯功能（用于发布紧急通知和 IT 服务申请）；
	3、可以创建策略对特定 PC 性能（如 CPU 利用率）进行记录、查询、分析
	4、基于策略的远程截屏
五、软件分发跟新管理	
	1、系统补丁分发与管理；补丁分发下去后能撤回；补丁分发必须支持由管理员推送安装，支持 MSI 安装包；
	2、类似 360 的软件管家，能检测需要更新的常用软件和作出前后台提示和处理。
	2、其他软件按策略分发，支持 MSI 安装包（普通用户只有 user 权限）；
六、产品特性要求	

	1、客户端安装简单比如：能主动推送，而不需要每台机器去安装；
	2、产品自身安全性好，售后服务完善
	3、有同行业成功案例，产品稳定性高，扩展性好
	4、整合网络接入控制；用户修改 IP 地址、MAC 地址等时会报警；
	5、客户端所装软件占用资源要少，客户端进程隐藏，不能被用户结束；适用各种网络环境，占用网络带宽低；
	6、相关安全产品证书及许可证等；
	7、能配置灵活离线策略

厂家和产品（厂家考察依据，已备未来审计）

众多选出前十家！
标准：产品实力、营业额、金融行业知名度、口碑

厂家扫描

前十家中的进一步筛选

厂商情况

已经接触了四个厂商，网御神州科技有限公司并未提供桌面安全产品。与北京博睿勤技术发展有限公司交流文档安全管理时，我们了解到其有桌面安全产品且说能实现两者整合，所以加入，但经初步了解其很难满足我们当前需求。
据了解深圳市联软科技有限公司（www.leagsoft.com ，有上海办事处）和网强信息技术（上海）有限公司（www.nstrong.com）在金融行业中成功案例较多，建议考虑未来测试时考虑。

上海互普信息技术有限公司介绍
http://www.hupu.net/introduces/introduces_1.asp
北京北信源自动化技术有限公司介绍
http://www.vrv.com.cn/AboutUs.asp

北京博睿勤技术发展有限公司介绍

http://www.bring.com.cn/gsjj.asp

厂商产品列表

		上海互普信息技术有限公司	北京北信源自动化技术有限公司	北京博睿勤技术发展有限公司
产品信息	公司网站	www.hupu.net	www.vrv.com.cn	www.bring.com.cn
	产品名称	互普威盾	北信源终端安全管理产品	博睿勤主机审计与监控系统
基本层面	产品性能	单一服务器支持?并发用户?	?	支持冗余配置、分级配置
	服务器备份容灾性能	?	?	?
	客户端兼容性	支持最新 win7	支持最新 win7	支持最新 win7
	客户端程序保护机制	有	有	有
	产品管理架构	C/S	C/S	B/S
	与活动目录集成性	支持，需改进	支持，?	支持，，需改进
	后台数据库	MS Sql Server	MS Sql Server	MS Sql Server
	邮件告警	支持	支持	支持邮件
	客户端和控制台加密通信	?	是	?
	离线策略配置	支持	支持	支持
	终端程序安装	灵活，简单	需要交互式安装	灵活，简单
	电脑使用人变动后场景处理	?	?	?
	管理权限配置	支持	支持	支持
	层级管理架构适应	当前不支持	是	是
	能否测试试用	可以	可以	可以
	金融行业成功案例	有	有	无
功能层面	网络准入管理	无	网络接入控制管理系统	可以整合
	非法外联管理	无	内网安全系统：非法外联管理产品包	有
	网站浏览管理	浏览网站模块，编号：V03	主机监控审计系统	?
	网络流量管理	网络流量模块，编号：V04	内网安全系统：终端桌面管理产品包	流量管理系统
	即时通讯管理	即时通讯模块，编	?	无

		号：V12		
	邮件管理审计	邮件监控模块，编号：V11	主机监控审计系统	无
	软件运行管控	应用程序模块，编号：V02	内网安全系统：终端桌面管理产品包	有
	PC 性能参数监测	?	内网安全系统：网络主机运维产品包	无
	资产管理	资产管理模块，编号：V13	内网安全系统：基本产品包	无
	补丁和软件分发	资产管理模块，编号：V13	补丁及文件分发管理系统	无
	外设管理	设备控制模块，编号：V09	内网安全系统：终端桌面管理产品包	有
	移动存储管理	移动存储管理模块，编号：V14	移动介质管理系统	移动介质管理
	文件操作审计	文档操作模块，编号：V05	主机监控审计系统	文档安全管理系统
	屏幕快照	屏幕快照模块，编号：V07	?	无
	打印审计	打印控制模块，编号：V06	主机监控审计系统	无
	远程协助	远程维护模块，编号：V08	内网安全系统：终端桌面管理产品包	无
	数据分析和智能报表	?	?	?

简单分析

从表可以看出当前还没有一款产品能完全满足我们烈出的需求，但是前两款产品已经基本能满足当前需求。
如果从长远发展考虑需要进一步了解各公司实力和其已实施案例。

相关探讨

桌面管理软件能否满足整理出的需求

由于整理的需求涉及资产管理、数据安全、网络接入控制、桌面行为管理、网络行为管理、软件分发、维护管理等诸多方面
具体产品未必能全面解决，须考虑如何取舍，逐步实现需求。

如何有效实现网络行为管理

桌面管理系统中的网络行为管理与专职网络行为管理软件比较还需测试后作出。
必须要安装客户端才能实现的功能（非红色条目均是）：

1、控制客户端接入内网和互联网；

2、控制客户端访问互联网流量，能控制不同程序访问网络的流量；

3、控制客户端不同程序访问网络优先级和带宽；

4、设置客户端网站访问白名单、黑名单,跟踪记录用户对于网站的访问；

5、限制电子邮件的附件类型和大小；并记录进出邮件。Web 方式的邮件及附件也能记录；邮件内容智能报表分析

6、IM 软件限制和聊天记录和智能报表分析，传输文件的历史记录；FTP 等文件传输历史记录；

7、BBS、SNS、blog 等互动网站关键信息记录和智能报表分析；

8、非法外联行为控制审计

长远规划，考虑

如何不只局限于桌面管理层面，借助 ITIL，BSM 理念实现基础维护系统、业务维护系统整合。

如何整合已有的系统，更好服务于业务

认证与域结合、用户分组管理使用域中组账户、
比如临时授权许可的流程审批在 OA 中实现等
资产管理如何与公司层面资产管理融合
如何分析收集到的 PC 终端信息（数据挖掘，智能报表等）

测试工作内容细化，明确目标

测试其功能；
体验其维护管理，思考未来如何适应相应管理维护工作；
测试桌面安全客户端与已有程序的兼容性；
找到适合公司的产品。

相关工作细则梳理

不同部门，不同角色许可的桌面行为，需要告警的行为
不同部门，不同角色许可的网络行为，需要告警的行为
不同部门，不同角色数据安全管理细则，需要告警的行为
软件分发管理流程
临时授权使用 U 盘，外发文件的审批流程

测试、实施计划（待定）

项目实施表