瑞星企业终端安全管理系统 中小企业全能版（SME） VS Symantec SEP 12.1功能比较

比较项目	比较类型		中小企业全能版（SME）	Symantec SEP 12.1
1 支持系统平台环境	1.1 服务器 支持操作系统		Windows Server 2003 Enterprise with Service Pack 1 or later（推荐） Windows Server 2003 Standard with Service Pack 1 or later Windows Server 2003 Datacenter with Service Pack 1 or later Windows Server 2003 Web with Service Pack 1 or later Windows Server 2003 R2 Enterprise Windows Server 2003 R2 Standard Windows Server 2003 R2 Datacenter Windows Server 2003 R2 Web Windows Server 2008 Enterprise Windows Server 2008 Standard Windows Server 2008 Datacenter Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Standard Windows Server 2008 R2 Datacenter Windows Server 2012 Windows 7	Windows XP Windows Vista Windows 7 Windows Server 2003 Windows Server 2008 Windows Small Business Server 2003 Windows Small Business Server 2008 Windows Essential Business Server 2008 Windows Small Business Server 2011
	1.2 数据库要求		默认情况下安装MSDE数据库（软件自带） Microsoft® SQL Server™ 2000 SP4 、SQL Server 2005 SP2、SQL Server 2008（可选）	Microsoft® SQL Server™ 2000 SP4 或 SQL Server 2005 SP2 或 SQL Server 2008（可选）
	1.4 客户端支持系统		Windows Server 2003 Windows Server 2003 R2 Windows Server 2008 Windows Server 2008 R2 Windows XP Windows Vista Windows 7 Windows 8	Windows系列: Windows® 2000、Windows® XP、Windows® Vista、Windows® 7、Windows Server® 2003、Windows Server® 2008、 Mac系列: 基于 PowerPC 技术并运行 Mac OS X 10.4-10.5x 的 Mac 基于 Intel并运行 Mac OS X 10.4-10.6 的 Mac Linux系列: Red Hat Enterprise Linux、SUSE Linux Enterprise、Novell Open Enterprise Server、VMWare ES、Ubuntu、Debian、Fedora
	1.5 网络环境	控制台支持http/https	支持	支持
		l支持纯IPV4/IPV6环境	支持	支持
		支持IPV4与IPV6的混合组网环境	支持	支持
		支持动态IP，多网卡	支持	不支持
		中心支持域名地址模式组网	支持	不支持
	1.6 远程控制台	支持多种主流浏览器	支持	支持
		支持移动、手持设备使用、平板、手机	支持	支持
	1.7 其他	B/S、C/S混合架构，增强用户体验及复杂网络环境	支持	支持
		客户端安装支持ghost	支持	不支持
		支持客户端重装，保持识别身份不变	支持	支持
2 安装部署方式	2.1 智能安装	可分单服务器模式安装、单客户端模式安装以及自定义模式安装	支持	不支持 需要不同的安装包
		支持快速安装，最大减少安装过程，部署更容易	支持	支持
		网络允许情况下自动发现上级地址	支持	支持
	2.2 制作定制包，web安装	可根据实际需求制定安装包	支持	支持
		Web站点发布安装包	支持	支持
		定制多个包，方便内部自定义通知安装（比如通过内部邮件发送安装包地址）	支持	支持
		发布通知内容可以定制	支持	不支持
	2.3 域脚本登录安装	自动识别域服务器，为域服务器配置终端登录脚本，自动部署客户端产品	支持	不支持
	2.4 远程控制客户端子产品装卸	可给已经部署了客户端产品的终端，设置具体子产品的部署情况（安装、不安装、不限制）	支持	不支持
	2.5 模块化子产品	每个子产品都是独立的模块，用户可以根据实际情况选择性购买与部署	支持	支持
		平台灵活支持扩展新子产品	支持	支持
		当以后开发了更多新子产品后，可以被无缝整合进现有的平台来，不必重复部署多套软件，大大减少新功能模块的部署成本	支持	不支持
3 升级管理	3.1 独立的升级服务器	可以独立部署一个或多个升级服务器，适应网络升级要求，负载平衡升级网络压力	支持	不支持
		支持以升级服务自身的内容为基础，制作定制安装包	支持	不支持
		支持上传升级包方式手动更新升级服务器内容	支持	不支持
		支持上传第三方软件包，方便分发给其他人下载使用	支持	不支持
		高效的自定制安装包管理、维护以及应用	支持	支持
	3.2 多升级源支持	提供升级服务器产品，客户端向内部服务器升级	支持	支持
		多升级服务器可以级联，下一级服务从上级服务器升级	支持	不支持
		可以同时配置多个升级源，如果访问的其中一个失败了，可以顺序使用下一个指定的升级源地址	支持	不支持
	3.3 升级方式	支持离线升级包，同时可以把升级包上传到升级服务器	支持	支持
		病毒库支持无缝主动式智能升级	支持	支持
		可手动升级，也可设置定时自动升级，不需要人为干涉	支持	支持
		支持游离到外网升级	支持	不支持
		可配置升级网络代理	支持	支持
		可自动根据新版本制作新的包，确保内部下载到最新包	支持	不支持
4 统一管理平台	4.1 客户端代理	可不部署其他任何具体的客户端功能子产品，而只是部署基础客户端代理组件，可实现轻量化安装需求	支持	不支持
		只要部署了基础客户端，就可以通过统一管理平台进行有效管理	支持	不支持
		提供一键式统一的提取客户端日志工具，当客户端有异常时，可以打包生成日志文件，方便通过日志分析解决问题	支持	不支持
		支持远程命令立即通报策略和更新授权信息	支持	不支持
		支持远程执行，管理员可远程传送一个文件部署到客户端，并立即执行	支持	不支持
		客户端组件支持自我保护，包括相关进程防杀、相关服务防止卸载、修改，以及防止安装目录的文件被删除以及创建新的未知文件	支持	支持
		客户端组件卸载或者停止工作有密码保护，防止任意卸载。	支持	支持
	4.2 分布式体系结构	C/S、B/S混合架构，吸收了C/S架构是时效性，以及B/S架构的易用性	支持	支持
		支持大型网络的多中心负载平衡系统	支持	不支持
		各服务器中心产品可部署在一台物理机器上，也可根据实际网络情况分散部署在不同的物理机器上	支持	支持
		对管理员自身在控制台的操作进行行为审计，并实时展示	支持	支持
		审计控制台提供全网安检功能，并提供给管理员自定义安检项重要程度，达到符合实际需要的安检评分	支持	支持
		审计控制台提供快速切换组功能，从分组的角度去了解整体情况	支持	支持
		安装后支持自动寻找上级服务器	支持	支持
		智能网络连接模型，减少网络压力	支持	支持
		支持通知客户端立即升级、客户端主动升级	支持	支持
		具有设置安全密码保护功能，防止用户随意卸载停止软件的使用，或使用一些需要管理员权限的功能	支持	支持
		l 支持制作管理员U盘身份，此U盘可直接作为管理员密码使用	支持	不支持
		l 强大的站点跨级管理：支持建立多级站点的树形级联网络结构，可以直接对任意下一级进行管理	支持	支持
		l 日志管理支持级联模式下，上级允许灵活的动态订阅所需要的来自下级的各种日志	支持	不支持
	4.4 客户端管理	把整个网络计算机划分三大组：正常管理(根管理组)、黑名单组、未知计算机组，全局综合性管理全部客户端	支持	支持分组
		根管理员支持无限分级创建子组，便于符合企业管理员的管理习惯	支持	支持
		组可以配置最大客户端的容量	支持	支持
		支持给客户端做备注，方便识别，并可导出，方便重新部署系统的时候导入使用，导入时并可设置匹配IP、计算机名称、MAC组合条件，提交识别准确率。客户端备注贯穿所有客户端信息展示，方便管理员对应具体的客户端行为、事件、日志等等	支持	支持
		支持按计算机名称、MAC、IP、版登录状态、组以及是否包含子组去搜索查找客户端	支持	不支持
		支持未知计算机监控发现，最大最快程度发现那些没有受管理的客户端计算机	支持	不支持
		未知计算机支持自动入组配置，可以配置好自动入组条件，减少入组管理成本	支持	支持
		支持按组或指定客户端发各种管理命令	支持	支持
		可指定客户端设定静态授权，避免动态抢占造成特定客户端抢不到授权场景	支持	不支持
		可视化统计客户端在线情况，客户端版本分布情况，以及授权实时占用情况，方便管理员了解客户端基本情况。	支持	支持
		集成客户端助手，包括垃圾文件清理、隐私痕迹清理、隔离中心、电脑修复、开机优化、文件粉碎、使用痕迹清理、引导区工具、进程管理、右键菜单管理。	支持	不支持
		全面的U盘助手工具，能够方便的管理企业内部的u盘，包括u盘的打开使用、自动弹出功能，并集成了其它病毒扫描、制作ukey等功能。	支持	不支持
	4.5 服务器管理	集中式服务器管理、使用，方便用户统一维护	支持	支持
		支持定义外围服务器：SMTP邮件服务器	支持	支持
		可以修改数据中心的各种参数，动态切换数据库系统	支持	不支持
		管理中心提供本地高级数据中心使用工具，方便维护内部数据	支持	不支持
		业务中心组件可配置负载均衡，以及负载客户端的上限	支持	不支持
		客户端支持智能连接，如果上次连接的业务中心不在时，会自动寻找其他在线的业务中心	支持	不支持
		能够在同一个子网网段内部署多套完全隔离的产品系统而不冲突	支持	不支持
	4.6 用户管理	支持多用户以及自定义权限，根据企业管理人员需求灵活分配账户权限	支持	支持
		支持系统管理员、操作管理员、审计管理员权限分离	支持	不支持
		管理员权限支持按照功能分配，同时支持按照域、组分配，保证在管理上各司其职	支持	支持
	4.7 策略管理	支持共有策略、组策略、客户端策略三种不同作用域的策略模式	支持	支持组策略
		支持策略模板，方便管理员实现配置多套策略做准备	支持	不支持
		策略模板支持导入导出、复制、分配使用	支持	支持
		支持继承模式，组策略自动继承父组的策略，方便管理员做统一化管理	支持	支持
		统一化管理下的又可以差异化处理，组策略也可以根据需要转为私有使用，快速配置	支持	支持
		可跟踪查看组策略的下发详情（哪些客户端已经同步到了最新的策略，哪些没有）	支持	支持
		策略的具体项可支持管理锁定功能，如此客户端只能看不能修改此项值	支持	不支持
	4.8 日志报告	支持查询不同种类的详细日志，并根据不同的日志类型提供不同的详细查询条件	支持	支持报表 但不详细
		出厂内置各种专业报告，提供给管理员图形化的展示效果，并可以根据不同的报告类型提供不同的查询条件	支持	
		可创建定时报告，可在指定时间生产指定报告发送到指定的邮箱里去	支持	
		支持综合报告查询，可根据用户需求定制报表并收藏，方便随时查看	支持	
5 防病毒功能	5.1 全网防护	支持公有云、私有云查杀	支持	支持
		支持多核cpu的并行计算，提高文件扫描速度	支持	不支持
		可检测并清楚隐藏域电子邮件、公共文件夹的计算机病毒、恶性程序等	支持	支持
		支持压缩文件查毒、清毒，压缩层次不少于50层，支持的压缩格式不少于15种.	支持	支持
		能够对各种加壳病毒文件进行病毒查杀，支持的加壳种类不少于80种	支持	支持
		可手动配置选择引擎，内部也智能选择引擎，适当的环境选用适当的方案，加快查杀效率	支持	不支持
		邮件病毒检测及清除能力：支持smtp以及pop3协议的邮件接收、发送检测；邮件文件静态检测、清毒；邮箱静态检测、清毒。同时，至少同时支持Foxmail、Outlook、Outlook Express、Notes和Netscape等客户端邮件系统的防（杀）病毒	支持	支持
		邮件监控支持smtp以及pop3的多端口设置功能，可以对设置的所有端口的进行邮件监控	支持	支持
		采用宏指纹识别技术更有效的查杀OFFICE宏病毒。	支持	支持
		采用无毒文件安全码技术提高病毒查杀速度。	支持	支持
		支持网络下载文件的病毒实时查杀。	支持	支持
		能够准确查杀计算机病毒不少于700万种。	支持	未知
		具有未知病毒检测、清除能力。	支持	支持
		支持族群式变种病毒的查杀。	支持	支持
		具有智能解包还原技术能够对原始程序的入口进行检测	支持	不支持
		支持病毒库智能增量升级模式，可以快速高效的升级文件而占用最少的网络带宽；	支持	支持
		系统监控，包括文件监控、邮件监控，可远程集中式查看监控状态及开关监控	支持	不支持
		U盘监控，可在U盘刚接入时就进行一次安全扫描，确保接入环境的U盘安全	支持	不支持
		系统扫描，包括快速扫描、全盘扫描、自定义扫描；并且管理员可以在控制台上远程查看客户端扫描状态信息、并控制快速扫描或者全盘扫描的扫描过程；	支持	支持 定义名称不一样
		染毒文件的隔离与恢复；并且管理员可以在中心控制台远程恢复可能误杀的文件；	支持	支持
		支持多种客户端的工作模式，中心控制台内建多种工作安全策略模板，方便管理员对不同用途的客户端快速应用合适的安全策略；	支持	支持
		支持引导扇区和主引导记录区备份和恢复	支持	不支持
		可根据监控状态、未执行扫描状态以及根据计算机名称、IP地址等信息快速查找计算机，方便更有针对性的进行全网管理	支持	不支持
		自定义白名单、排除列表，提交企业内部防护效率	支持	支持
		支持单独给全盘扫描、快速扫描设置定时查杀任务	支持	支持
		可远程锁定客户端用户不能关闭监控功能，提高全网安全	支持	支持
		支持智能监控模式，减少因监控带来对系统资源占用的影响	支持	不支持
		变频杀毒，支持办公模式、自动模式、高速模式三种模式.可按需配置查杀毒时对CPU的使用情况，最大程度减少查杀毒时对用户使用计算机的影响，又不失安全	支持	不支持
		支持杀毒后自动关机	支持	支持
		文件监控发现病毒提示没有倒计时，避免用户遇到短时间内无法判断的问题	支持	不支持
		智能日志更新系统，能及时最快把病毒详情、查杀毒状态展示在日志系统	支持	支持
	5.2 病毒分析	病毒日志的详细查询；可以在控制台上看到实时病毒上报信息，并查看网内病毒爆发趋势图，以及各种相关统计报表；	支持	支持
		按指定时间范围提供近期病毒概况与排行，提供本组、子组及客户端病毒信息统计表	支持	支持
		病毒来源分析与跟踪，可以根据病毒的名称及ID分析病毒的传播途径与爆发方式；可以让管理员通过图形直观的分析不同时间点网络染毒的情况；	支持	不支持
	5.3 病毒详情	可通过指定时间范围查询发现的病毒情况	支持	支持
		通过病毒发现来源、病毒状态以及病毒名称、染毒文件名快速过滤病毒详情	支持	支持
		按病毒显示查看某病毒具体染毒客户端详情	支持	支持
		按客户端显示查看客户端染毒总数	支持	支持
6 漏洞扫描及修复	6.1 漏洞扫描及修复	客户端漏洞扫描支持多引擎，支持整合开发第三方漏洞扫描引擎接口	支持	不支持 没有相关功能
		支持简体中文、繁体中文、英文多种语言环境补丁	支持	不支持
		可识别漏洞对系统的安全影响分类（远程执行、拒绝服务、特权提升等等）	支持	不支持
		定义漏洞对系统安全等级的划分，方便管理员核定安全级别	支持	不支持
		支持扫描系统、IE、.net以及office、flash等类型漏洞并修复	支持	不支持
		支持目前主流的各种windows操作系统版本	支持	不支持
		可配置定时漏洞扫描策略（开机、每周、每天）	支持	不支持
		方便统一修复漏洞，可以配置扫描后立即修复或统一下发修复命令再修复	支持	不支持
		可以选择修复指定级别的漏洞补丁，对于不重要的功能性补丁可以做到不修复；	支持	不支持
		可配置多个补丁瑞星补丁分发服务器产品，逐个尝试下载，提供网络环境兼容性	支持	不支持
		支持客户端使用P2P从互联网上直接快速下载补丁	支持	不支持
		支持客户端HTTP协议下载补丁从各种升级源下载补丁	支持	不支持
		根据实际网络及计算机性能，可指定顺序或并行下载补丁方式	支持	不支持
		节省客户端磁盘空间，可指定修复后删除补丁文件	支持	不支持
		可统一进行漏洞操作（修复、忽略、不处理）	支持	不支持
		可选定客户端进行统一的远程扫描命令	支持	不支持
		对未修复漏洞、及已发现未修复漏洞的客户端计算机进行前10的图表展示	支持	不支持
	6.2 漏洞管理	可按漏洞的修复情况查查看详情（已修复、修复失败、已忽略），修复失败的，可展示失败原因	支持	不支持
		按漏洞显示，查看某个漏洞涉及的客户端情况, 按客户端显示具体某客户单的漏洞修复详情，及最后上报时间.	支持	不支持
	6.3 补丁服务器	提供内部的补丁服务器支持，支持外围被隔离的网络环境使用漏洞扫描功能	支持	不支持
		瑞星公司可不定期的提供可导入补丁服务器的补丁包	支持	不支持
		支持手工导入已下载好的补丁到补丁服务器	支持	不支持
		补丁服务器的补丁支持导出，方便二次部署或导入到其他补丁服务器使用	支持	不支持
		补丁服务器可配置多补丁下载源	支持	不支持
		补丁服务器可自动适应是否使用P2P下载	支持	不支持
		补丁服务器之间可以级连，方便外网下载的统一管理	支持	不支持
		可根据客户端已扫描发现的补丁自动进行相关补丁下载，由此提供补丁下载服务	支持	不支持
		管理员也可根据补丁库指定补丁下载	支持	不支持
		提供补丁管理操作，进行未下载、正在下载、已下载补丁的统一管理	支持	不支持
		支持导出补丁下载地址，方便管理员二次使用（使用自定义的其他方式去下载补丁）	支持	不支持
		控制台及时反馈补丁服务器可用磁盘剩余空间，避免磁盘不足风险	支持	不支持
		l 支持热补丁（虚拟补丁）功能，在没有打微软补丁时，依然能够防止恶意程序利用漏洞，实时监测风险，保护安全	支持	不支持
7 IT 资产管理	7.1 软件管理	已安装软件统计，可以统计所有终端的应用软件的部署详情，包括软件名称、软件大小、版本、发行厂商	支持	不支持
		按软件统计其在已安装客户端总数及详情	支持	不支持
		按客户端显示其已安装的软件总数及详情	支持	不支持
		可对快速指定软件增加关注，如此系统会对关注软件进行统一汇总报告	支持	不支持
		软件扫描识别引擎及库，库里支持较系统的软件分类及安装环境检测以及其他识别信息，方便从软件逻辑角度去识别文件、进程等	支持	不支持
		扫描引擎库支持识别主流上千款软件信息	支持	不支持
		支持保护指定软件（可从软件库、服务、自定义方便增加保护规则），可使得指定软件不能在客户端被异常关闭、服务异常被卸载等保护行为	支持	不支持
		支持记录受保护软件在客户端被尝试破坏的日志，并提供管理员展示查看	支持	不支持
		支持禁止使用指定软件（可从软件库、服务、自定义方便增加保护规则），确保禁止使用的软件不被客户端计算机运行，并可指定进行警告性提示	支持	支持
		支持记录被禁用软件在客户端被尝试使用的日志，并提供管理员展示查看	支持	支持
		可配置软件白名单，方便支持企业自定义的允许对被保护软件的更多行为	支持	不支持
		实时远程进程查看，可查看指定客户端的进程运行列表及CPU、内存使用情况	支持	不支持
		进程启动审计，记录客户端进程启动日志	支持	支持
	7.2 软件部署	企业可以自定义内部的appstore分发中心	支持	不支持
		推送第三方的应用可以使用软件库里的软件，也可以使用自定义的软件	支持	不支持
		虽然使用软件库的软件，但是用户可以自定义软件包下载地址	支持	不支持
		软件下载源支持多下载源，顺序优先下载	支持	不支持
		控制台可统计推送软件的部署情况（已部署客户端、未部署客户端），也可查看某客户端对整体部署的情况（已支持安装、未安装）	支持	不支持
		具有自动强制重新部署能力，客户端用户自己卸载后，系统检测到没有部署，又会自动部署上	支持	不支持
	7.3 硬件管理	获取到客户端硬件详情以及设备详情信息，提供统一展示	支持	不支持
		提供按异动类型、硬件类型等信息过滤查杀异动	支持	不支持
		硬件异动审计，可以看到硬件的变化信息；	支持	不支持
		设备异动审计，可以从设备角度看到硬件的变化信息	支持	不支持
		支持异动情况的确认，确认的异动就不做为风险	支持	不支持
		支持按客户端查看单客户端的整体异动详情	支持	不支持
8 行为审计功能	8.1 文档访问审计	可以审计U盘、网络盘或指定磁盘位置的文件的操作动作	支持	支持
		可以禁止U盘、网络盘或指定磁盘位置的文件的复制、删除等等文件操作	支持	支持
		可审计记录的内容包括用户名、操作、时间、动作、文件名、结果	支持	部分支持 不够详细
		可以灵活的设置审计功能的有效时间段，并且设置是否违规时的警告通知	支持	支持
	8.2 文档打印审计	记录客户端打印的内容的概要信息，包括打印机名称、文档标题、打印页数等等；	支持	不支持
		可以禁止客户端使用打印机	支持	不支持
	8.3 邮件收发审计	对支持POP3、SMTP协议的邮件客户端收发邮件进行审计	支持	不支持
		可以指定各种过滤条件，包括设置过滤收件人、发件人、主题词、是否包含附件，审计的内容包括收件人、发件人邮件标题、附件名称等等；规则可以自定义设置多条；	支持	不支持
		可以设置只监控包含附件的邮件	支持	不支持
		可以控制是否拦截指定规则的邮件	支持	不支持
	8.4 U盘审计	U盘的统一登记管理；可以禁止使用未登记的U盘; 可以只允许使用已经登记的U盘; 可以禁止使用已经登记的U盘; 客户端可以查看U盘的使用历史;	支持	可禁止U盘使用
		使用记录支持跟踪操作到用户（非计算机），提供按用户名统计查看；客户端本地支持查看U盘使用历史记录，方便纯离线环境应用的审计	支持	不支持
		客户端具有U盘申诉功能，U盘已被禁用的客户端可通过申诉直接向控制台申请使用;	支持	不支持
		已安装杀毒客户端终端可随时自行制作绿色杀毒U盘，方便特殊环境机器杀毒使用;	支持	不支持
	8.5 设备管理	可以禁用指定的设备：光驱、1394、蓝牙、串口、并口、PCMCIA卡、红外设备；	支持	支持
	8.6 上网审计	可以记录主流的各种浏览器的上网记录，记录的内容包括域名、路径、网页标题；	支持	不支持
		可以对指定的多个URL地址进行记录或者禁止访问并跳转到指定的URL	支持	不支持
		可以灵活的设置审计功能的有效时间段，并且设置是否违规时的警告通知	支持	不支持
	8.7 联网程序管理	联网程序审计，可以对有数字签名的程序自动识别并放行	支持	不支持
		对于未知的程序联网，可以设定允许、拒绝、询问用户	支持	不支持
		指定的某个进程/软件/服务的联网行为发生时，进行可以防文件篡改检查、是否允许作为服务端监听、包括是否允许联网；	支持	不支持
		可以灵活的设置审计功能的有效时间段，并且设置是否违规时的警告通知	支持	不支持
	8.8 网络攻击拦截	对外网络攻击拦截，可以拦截到SYN攻击、ICMP攻击、UDP攻击，并提示用户	支持	支持
		阻止黑客远程网络攻击：内置了包括针对微软、adobe、迅雷、apache等等的相关软件漏洞的黑客攻击进行实时监控，并在遭到攻击时阻止对应IP并报警提示	支持	支持
	8.9 防火墙IP规则定义	支持自定义IP规则编辑	支持	支持
		支持自定义端口规则编辑	支持	支持
		支持IP地址访问的白名单设置	支持	支持
		支持IP地址访问的黑名单设置	支持	支持
	8.10 流量管控	可以查看全网每个终端的网络流量；并以时间轴做图表展示	支持	不支持
		可以设定指定终端的下行流量大小限制	支持	不支持
		可以设定查看每个终端的每个联网程序/软件/服务的流量信息，并以时间轴做图表展示	支持	不支持
	8.11 非法外联	允许禁用上网设备：VPN、ADSL、MODEM、无线网卡；	支持	支持
		非法外联审计，如果检测到终端连接到互联网，可以报警并记录；	支持	不支持
		非法外联审计检测支持智能检测模式，可以实时发现外联行为	支持	不支持
	8.12 网络共享资源	可以记录共享的文件夹被其他终端的访问情况，记录内容包括资源名称、IP、访问动作（读、写）	支持	部分支持 可禁止访问
		可强制关闭终端的系统默认共享或者远程管理	支持	支持
		可以对指定单个在线的终端的共享文件夹进行管理，允许设置指定范围的IP地址访问，也允许立即关闭指定的共享资源	支持	支持
9 网络安全功能	9.1 网络安全审计	可以对不符合以下检测规则的终端进行有效的网络隔离，防止其访问其他网络资源；规则包括:	支持	部分支持
		系统漏洞数量超过指定阀值		
		未安装指定的安全类软件		
		客户端未在线		
		发现客户端感染指定的病毒名或者指定的病毒类型，可以设置隔离有效时间		
		发现客户端有arp出站攻击行为，可以设置隔离有效时间		
		发现客户端有非法外联行为，可以设置隔离有效时间		
		被隔离的终端，可以被管理员在控制台上手工从网络隔离状态恢复到正常状态	支持	
		支持网关型NAC终端准入控制，有效控制未被管控终端连接互联网	支持	支持
		支持ARP型NAC终端准入控制，可以在小规模网络中，不依赖硬件低成本实现未知终端的准入控制	支持	支持
	9.2 系统环境的审计与运维	计算机的开机/关机进行记录；	支持	不支持
		用户登入/登出事件进行记录；	支持	不支持
		能够在中心控制端对网内任意安装了客户端的计算机进行锁定、关闭、重启、注销	支持	不支持
		可以控制客户端用户对计算机的操作权限，允许管理员设置策略来控制终端用户禁用操作系统提供的系统功能：控制面板、计算机管理、计算机属性、网络连接管理、IE浏览器插件管理；	支持	部分支持
		扫描用户操作系统以及磁盘的详细情况，并把系统盘磁盘空间不足的终端列出来；	支持	不支持
		能够在中心控制端对网内任意客户端进行文本消息发送通知；	支持	不支持
	9.3 安全软件部署	扫描客户端计算机是否安装了常用的反病毒软件，并以图标形式展示	支持	不支持
	9.4 开机启动审计	启动项的管理，可以集中查看和手动优化全网的终端的启动项;	支持	不支持
		可以一键优化全网的开机启动项	支持	不支持
		开机时间的跟踪审计，可以根据开始启动时间来评估客户端机器的资源使用趋势;	支持	不支持
	9.5 IP地址管理	客户端IP地址与mac自动上报并列表	支持	不支持
		客户端IP防篡改，防止终端用户自己随意更改本机IP地址;	支持	不支持
		ARP欺骗检测，防止本机发ARP欺骗包，并检测内网的恶意ARP欺骗包。	支持	支持
		本机IP保护功能，可以防止IP地址冲突时，本机网络断开	支持	不支持
10 XP保护盾	10.1 XP保护盾功能	启用虚拟补丁实时监控	支持	不支持
		启用漏洞免疫		
		发生攻击时提醒用户		
		记录漏洞攻击日志		
11 即时通讯	11.1 即时通讯软件内容审计	可以监控的通讯工具包括QQ、MSN、TM、RTX;	支持	不支持 没有此功能
		管理员可以设定监控客户端使用即时通讯工具的时间段境;	支持	不支持
		可设定审计内容关键字，设定关键字可以支持正则表达式，已达到高级使用用法。只审计出现关键字的内容，包括聊天内容、网站、邮件。并对设定的关键字结果进行按关键字、按客户端统计查看，并可进一步查看具体详细。对统计结果进行趋势分析，按日期查看出现频率曲线;可设定出现关键字内容的审计方式：审计、替换、阻断.	支持	不支持