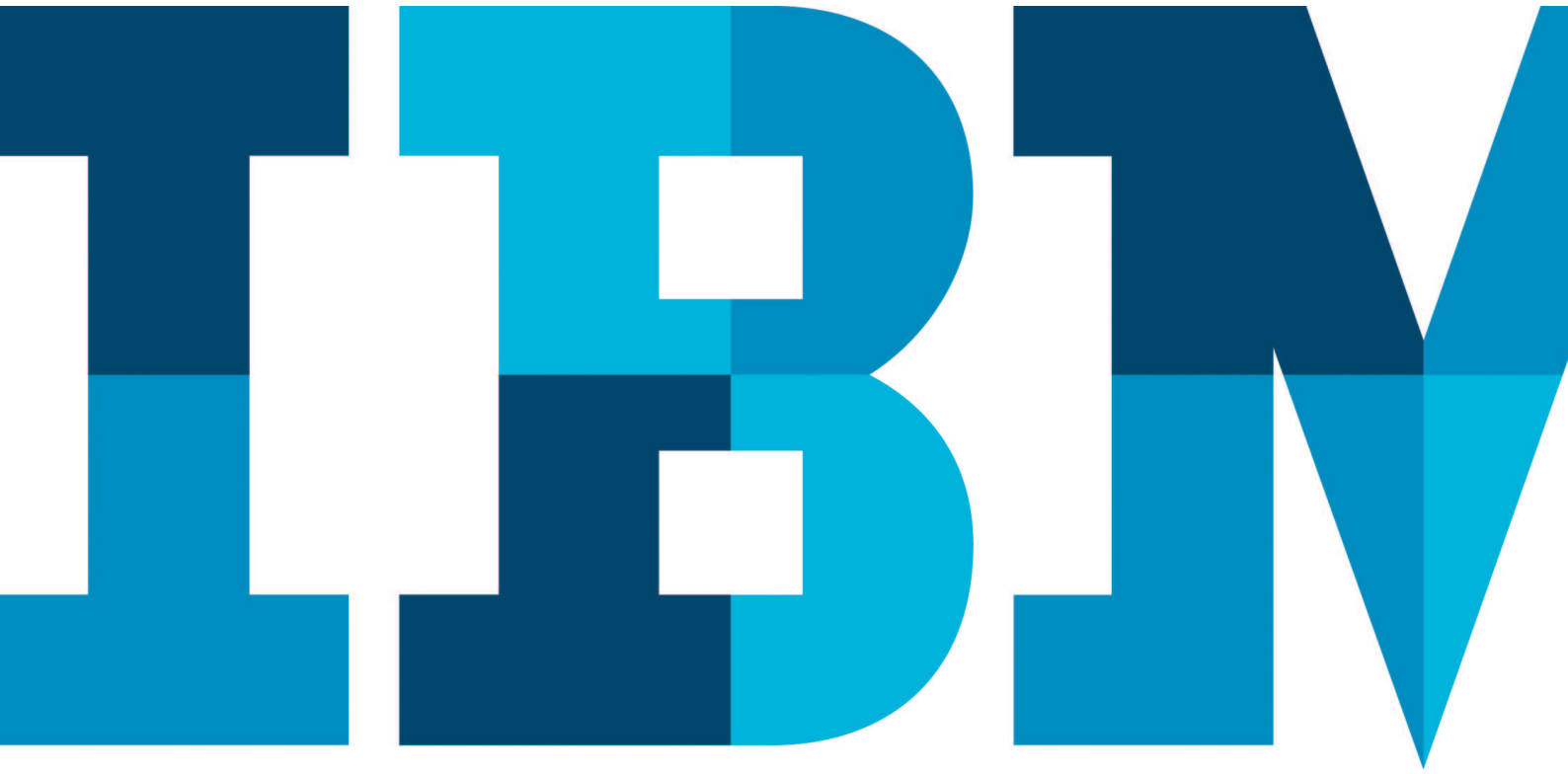
《Select the right solution for endpoint management》（选择正确的终端管理解决方案）

增强对于成千上万台分布式终端的可见性及控制



IBM

IT 企业在管理数千台计算终端（包括工作站、服务器，以及笔记本电脑、智能手机和平板电脑等漫游移动设备）方面面临巨大挑战。使用传统管理方法时，即便是要解决一些简单问题，比如“我们有多少台笔记本电脑？”、“我们的台式电脑系统运行什么操作系统？”或“我们的补丁是不是最新的？”，也会耗费数天时间，而且获取及生成的答案往往不准确也不完整。

正是出于这种原因，许多企业在尝试整合及清除并不会执行的多余管理工具、增强安全性及合规性，以及减少成本和 IT 工作负载的同时，还寻求通过 IT 运营和安全自动化，来满足当今复杂的终端管理需求。

企业正积极克服自身终端基础架构可见性不足的弊端，以便了解相应需求、差距及改良机会。他们正在想方设法来加速及简化新软件部署、实施软件更新和重要安全补丁、维护及验证合规性以适应不断变化的行业和政府法规，以及保护不断扩展且通常极具渗透性又易遭受攻击和安全威胁的周边。

在习惯了多元化、分散技术和单点解决方案的环境中，企业需要可跨多种异构设备和操作系统来支持终端管理的一体化方法。他们需要进行快速部署及加速实现价值。他们需要允许定制和创建公司特定策略而又无需大量编程和脚本编写工作的开放式基础架构。当环境面临威胁时，他们需要实现敏捷、实时的终端可见性、保护、快速补救和报告功能。

高效的终端管理解决方案可借助单一、易用的图形用户界面，简化管理流程、增强终端控制并集中呈现视图，从而满足上述所有目标。这种解决方案可针对任意数量的物理和虚拟终端提供以上管理功能，范围涵盖服务器、台式电脑、笔记本电脑、智能手机和平板电脑，以及销售点设备、ATM 和自助服务终端等专用设备。

要想为客户、员工、业务合作伙伴、管理机构、投资商和其他委托人高效提供安全、可靠的全天候 IT 服务，必须做好终端管理工作。当今 IT 基础架构的高暴露特性，正在改变着企业管理终端、流程和数据的方式。终端管理解决方案是实现 IT 功能从后端操作向关键服务转变的基础，其与业务成功、内部安全策略合规性以及高效流程执行存在紧密集成的关系。

终端管理入门

本采购人员指南概述了高效终端管理解决方案的构成特性和功能:

- 终端发现、库存和软件使用分析
- 补丁管理、操作系统配置和软件部署
- 安全性与合规性
- 移动设备管理
- 绿色 IT
- 管理系统架构

本指南探讨各项功能的优势，并提供检查清单，可帮助您评估特定供应商的解决方案能否高效应对上述任何方面的要求。您还会从中找到一个属性和功能列表，在您选择供应商以全面支持终端管理需求时，有必要查看该列表。

终端发现、库存和软件使用分析

收集终端相关信息远非计数这么简单，需要定期执行“快照”实践。还需要借助全面的可见性和控制功能，快速识别企业所有 IP 可寻址设备及其中安装的应用程序，建立关于更改基础架构条件的近实时动态意识。

一流的解决方案可在涉及成千上万台终端的庞大基础架构中深入探寻潜在信息，快速提供汇总的统计分析和使用状况。它有助于维护对所有终端（包括在企业网络之外漫游的移动设备）的可见性。它可将新发现的终端纳入管理范围，并最大限度减轻对网络运营的影响。它还应尽可能地以近实时方式实现上述所有功能。

终端发现、库存和软件使用分析

寻求具备以下功能的解决方案:	IBM	其他
提供准确、深入且详细的库存数据，其中包括所有硬件、配置和软件属性	✓	
通过单一控制台提供发现和库存管理功能	✓	
支持对包含 100,000 多个即时可用签名的软件识别目录进行搜索、浏览和编辑，并基于软件行业的变更保持目录的时效性	✓	
允许针对软件识别目录进行基于向导的轻松定制，从而纳入面向自有和专用应用的跟踪功能	✓	
提供关于终端上软件发行商、标题和应用程序等的相关细分信息	✓	
包括可汇总历史统计和使用信息的软件计量功能	✓	
跟踪 Microsoft Windows、UNIX 和 Linux 终端的软件使用模式和趋势	✓	

终端发现、库存和软件使用分析

寻求具备以下功能的解决方案:	IBM	其他
将软件使用信息与一系列许可信息相关联，以利于即时、准确的许可协调管理：识别违规实例，进行标记并将其移除	✓	
提供丰富的资产数据，以进行报告，并与其他需要准确、最新库存（例如服务台、资产管理系统、库存仓库、配置管理数据库）的企业系统相集成	✓	
支持即时可用的服务台集成以提供高级功能，例如实施自动化、自助服务企业应用 （“app”） 商店	✓	
允许通过代表性状态传输 （REST） 应用程序编程接口 （API），实现与其他服务台和资产管理工具的无缝集成	✓	
提供入门级软件资产管理功能，同时采用更完善的解决方案，可实现轻松实施和使用	✓	
提供与终端安全及合规性管理的紧密集成	✓	
包括基于代理和无代理的分布式扫描架构，可实施影响小、低延迟的设备检测，以及深层检测和报告	✓	
快速识别包括网络设备和外围设备在内的所有 IP 可寻址设备，例如打印机、扫描仪、路由器和交换机，以及计算机终端	✓	
发现环境内的未记录终端，并识别可疑的“恶意”设备	✓	
提供正在使用的开放式端口和服务的近实时报告	✓	
支持对终端进行特定查询 — 例如: “为我提供所有计算机显示器的序列号” — 它会在几分钟内提供结果并最大限度降低影响	✓	
不管终端位置何在，是处于上线或离线状态，管理范围均可予以全面涵盖，并可保持库存数据的最新状态，即使是不经常连接到网络的终端亦然。	✓	

补丁管理、操作系统配置和软件部署

基础结构复杂性增加、管理工具激增以及 IT 人员负担过重，使得管理快速增长的终端设备和平台基础面临巨大挑战。企业需要一种综合的一体化管理解决方案，来获得实时可见性和控制能力，减少因使用多个工具集而造成的混乱、效率低下以及成本支出。这种解决方案通过将多种工具集中在统一管理范围之内，来优化流程，同时降低成本和风险，并提高管理效率。

高效的解决方案可从单一控制点、跨多平台实现基于策略的安全更新和软件包安装、闭环验证和软件分发管理功能。以相同管理控制台部署重要的操作系统和软件补丁，可帮助系统管理员轻松维护托管终端的所需状态。此外，还可以缩减系统部署和用户配置文件迁移的时间，从而减少与违规配置相关的风险，并最大程度降低对最终用户的影响，同时简化新工作站、笔记本电脑、服务器和移动设备的部署。

补丁管理

寻求具备以下功能的解决方案:	IBM	其他
从单一管理控制台提供自动补丁管理	✓	
从相同控制台和服务器自动管理多个操作系统的补丁，包括 Microsoft Windows、UNIX、Linux 和 Mac OS，以及智能手机和平板电脑	✓	
自动管理多家供应商的应用程序补丁，包括 Microsoft、Apple、Adobe、Mozilla 和 Java	✓	
将补救周期从数周缩短至数天或数小时，最大程度减少安全及合规性风险	✓	
对联网或离线状态下的终端实施补丁管理，包括漫游和联网设备	✓	
甚至在低带宽或全球分布式网络中也能提供一致性功能	✓	
将补丁成功率提升到 95% 至 99%（通常为 60% 至 75%），并确认补救操作	✓	
通过向管理员提供预测试补丁策略，而消除补丁管理开销	✓	
允许将补丁分组到单一部署任务，以简化管理、自动解决任何相关性	✓	
仅下载并应用与各终端相关的补丁	✓	
允许系统管理员快速创建及部署定制补丁，以补救零日漏洞	✓	
对在线虚拟机进行修补，以提升虚拟环境的安全性	✓	
提供离线虚拟机修补功能，使休眠虚拟机在重新提供服务时免受攻击	✓	

补丁管理

寻求具备以下功能的解决方案:	IBM	其他
可针对物理和虚拟环境中的复杂多层服务器应用，协调操作系统的修补操作	✓	
支持可用于服务器构建等关键任务的任务排序（例如部署操作系统、配置设置、部署简单软件、修补、更改主机名及重启计算机）	✓	
凭借实时灵活的图形监控和报告功能，增强有关补丁合规性的可见性	✓	
显示补丁状态 – 需要补丁、补丁处于待定或运行状态、补丁已成功安装、补丁安装失败	✓	
提供关于部署哪些补丁、部署时间及部署人员的信息	✓	
可根据强制性补丁级别等已定义策略，自动评估终端合规性	✓	
检测并修补旧有安装补丁被回滚或覆盖后所产生的问题，并允许对未安装补丁进行自动再应用	✓	
允许将具有或不具有强制实施日期的补丁作为“服务”提供给用户，以最大程度减少中断	✓	
允许对补丁进行分组，并在 windows 定义发生更改时进行快速安装	✓	
允许阻止可选补丁对话框窗口和延迟/计划重启	✓	

与以往相比，企业的业务分布范围更加广泛，这使得诸如分配及管理终端软件等 IT 管理任务极具挑战性。这些企业需要借助强大的功能，快速、可靠地为所有终端提供及管理业务关键型应用。

操作系统配置和软件部署

寻求具备以下功能的解决方案:	IBM	其他
从一体化单一控制点跨多平台提供软件分发管理	✓	
支持在整个分布式环境内，对全新及更新软件包进行基于策略和计算机组的安装	✓	
提供软件安装/取消安装的闭环验证	✓	
支持用户自助执行及去除授权应用程序和软件包的配置	✓	
支持软件包的本地预先缓存，以提升安装可靠性	✓	
消除软件分发中对重复文件的需求	✓	
支持“以客户为本”的软件分发策略	✓	
提供简单但强大的定制功能，以精确定位及部署软件包	✓	

操作系统配置和软件部署

寻求具备以下功能的解决方案:	IBM	其他
在所有操作系统平台上，通过策略驱动型静态/动态带宽限制，包括限制实际可用网络链接带宽的功能，来最大程度降低网络影响	✓	
从核心软件组件分别维护 Microsoft Software Transform （MST） 和 Microsoft Software Patch （MSP） 等配置文件，以高效处理多个软件包配置	✓	
与当前软件分发工具和软件包格式兼容	✓	
支持在整个网络中为新工作站、笔记本电脑和服务器，执行全面集成的“裸机”操作系统部署，并针对现有终端进行操作系统迁移和刷新	✓	
在操作系统迁移中使用终端管理核心基础架构，从而消除独立操作系统部署基础架构的维护成本。	✓	
借助包括远程唤醒支持和部署计划在内的全面自动化运营，来缩短部署和迁移时间	✓	
针对来自多家硬件供应商的机器部署硬件彼此独立的图像，根据需要注入相应设备驱动程序	✓	
实施用户配置文件和数据的就地迁移	✓	
将操作系统部署与安全基准和配置供应需求（包括“完成”修补）相集成，使系统可立即投入使用	✓	
提供多平台远程控制和故障排除	✓	
借助远程诊断功能将实时终端数据送到管理员手中，可简化帮助台呼叫和问题解决流程	✓	
将具体操作定位到终端配置的确切类型或用户类型	✓	
针对终端上安装的应用程序提供远程发现和分析	✓	
允许管理员建立基于角色的访问，以支持不同的用户责任和业务需求范围	✓	
通过将安全实践及合规性方案嵌入并作为 IT 运营流程的一部分，来简化及实施安全管理	✓	

安全性与合规性

在当今运营范围广泛的环境中，企业通常没有定义明确的周边，这使得终端极易受到攻击。更重要的是，攻击速度不断加快，新型漏洞的形成速度已远远超出目前大多数工具可以应对的范围。您能否以足够快的速度检测并更正漏洞，以保护您的服务器、PC 和其他终端免遭侵害？

大多数企业着重于保护其用户免受新恶意软件和病毒的威胁，越来越多的企业还必须为移动用户提供保护，从内部确保敏感数据的安全。并非所有数据泄漏都出于恶意：用户通常会将敏感信息复制到各种设备上，例如 USB 驱动器、内存卡、基于云的同步服务和移动服务。许多员工现在使用笔记本电脑工作，通常会携带敏感数据离开办公室。

面临上述挑战，企业需要数据丢失预防 （DLP） 解决方案，而且应可轻松部署到现有终端安全基础架构中。他们需要采用一体化解决方案，不仅可以应对与安全威胁相关的风险，还可以控制成本、复杂性和人员负担，同时满足合规性要求。此类解决方案可以帮助企业保护终端，并确保满足内部安全策略合规性。

终端安全性

寻求具备以下功能的解决方案:	IBM	其他
可管理物理和虚拟终端配置，而无需考虑地点、操作系统、安装的应用程序或连接（包括连线计算机或间歇连接的移动设备）	✓	
根据合规性基准实施终端补救操作，继而实施在线或离线配置策略	✓	
从单一管理控制台提供针对安全配置和补丁的最新、准确可见性与连续实施	✓	
通过特定闭环补救步骤，实施对零日攻击的实时响应，允许管理员快速、轻松地创建定制补救策略，并在几小时内针对整个组织的在线和离线终端完成实施操作	✓	
包含一个基于著名最佳实践的技术控制综合库，可通过检测和执行安全配置，来帮助实现安全合规性。	✓	
支持安全内容自动化协议（Security Content Automation Protocol，SCAP）	✓	

终端安全性

寻求具备以下功能的解决方案:	IBM	其他
利用基于开放式漏洞和评估语言（Open Vulnerability and Assessment Language，OVAL）标准的预定义、即时可用的策略定义，针对已知漏洞评估托管终端	✓	
能够针对 SANS 机构发布的漏洞和安全风险警报立即采取措施	✓	
将漏洞映射至行业标准，提供国家漏洞数据库（National Vulnerability Database，NVD）的通用漏洞列表（Common Vulnerabilities and Exposures，CVE）和通用漏洞评分系统（Common Vulnerability Scoring System，CVSS）参考和链接	✓	
提供包含 5,000 多个标准配置设置的即时可用清单，这些设置已映射至 Windows、UNIX 和 Linux 行业标准	✓	
自动化及简化合规性报告，例如针对《Sarbanes-Oxley Act》（萨班斯-奥克斯利法案，SOX），《Health Insurance Portability and Accountability Act》（健康保险可携性与责任法案，HIPAA）和《UK Financial Services Act》（英国金融服务法案）	✓	
提供符合美国联邦桌面核心配置（US Federal Desktop Core Configuration，FDCC）和美国政府配置基准（United States Government Configuration Baseline，USGCB）法规的即时可用最佳实践	✓	
提供符合《Defense Information Systems Agency Security Technical Implementation Guides》（国防信息系统局安全技术实施指南，DISA STIG）的即时可用最佳实践	✓	
提供基于互联网安全中心（Center for Internet Security，CIS）安全基准的即时可用最佳实践	✓	
利用自动化策略实施或手动部署，识别并消除已知漏洞	✓	
可与帮助台系统、资产管理系统、配置管理数据库 （CMDB） 和安全信息及事件管理 （SIEM） 系统等相关技术轻松集成	✓	
设置警报以快速识别恶意或误配置终端，并采取措施定位这些终端，以进行相应补救或移除	✓	
可自动对违规终端进行网络隔离，同时继续对其进行管理直至补救完成	✓	
为定制策略制定、报告和实施提供向导	✓	
已通过国家标准技术局（National Institute of Standards and Technology，NIST）评估和补救认证	✓	
通过易用 API（它可支持多个使用相同语言的平台），借助最少量的代码行进行快速定制	✓	
为所有系统管理自动化工具提供中央集线器，允许管理员使用自己熟知的工具（例如 UNIX 的 shell 脚本语言、Windows 的批处理文件和 Apple 脚本等）	✓	
支持技能水平从初级（借助向导创建脚本而无需知晓工具语言）到专家级（具备高度定制灵活性）的管理员使用	✓	
提供与终端生命周期运营管理的紧密集成	✓	

企业需要的合规性信息通常会涉及所有终端的特定平台或终端类型、特定组织或地域细分，或者特定法规或治理目标。而要满足这一需求，则必须借助综合报告功能，充分利用仓储分析和资产数据，来生成快速、及时且易用的报告和视图。

报告和分析

寻求具备以下功能的解决方案:	IBM	其他
收集并归档自动化安全检查结果，帮助识别 IT 安全相关合规性的配置问题和报告级别	✓	
提供相应的分析功能，可通过监控、报告和跟踪进度，以及确定安全方案的成功与否，为企业的技术和配置策略实施提供支持	✓	
提供历史报告，以确定合规性目标的实施进度	✓	
针对终端运行状况与安全性提供富有意义的实时和历史报告，以用于补救违规终端，并确认补救操作	✓	
借助可深入分析详细信息的功能，提供概述演示板和执行汇总，以显示历史安全合规性及热点	✓	
提供以补救技术做出整合的可执行报告（例如特定补丁），而非单纯意义上相互重叠、通常为冗余漏洞的“细目清单”	✓	
识别、管理和报告策略异常和差异	✓	
提供可用于管理 IT 策略检查的全套报告，包括合规性状态和历史、按计算机和计算机组划分的报告，以及异常报告	✓	
帮助创建灵活、随需及特定查询和报告	✓	
提供报告灵活性，包括报告过滤器（例如历史合规性、计算机元数据、检查清单元数据等）、报告列管理、实际测量与所需值对比、报告导出以及保存报告等	✓	
使用户可通过整合解决方案中自带的最佳实践检查与定制检查，在几分钟内轻松创建定制检查列表	✓	
以高级报告显示历史配置合规性及安全变更的趋势和分析	✓	
对基础架构视图的基本分析可通过多种方式进行定义，从单一设备到设备组再到整个基础架构均可	✓	
包括单独的安全分析数据仓库，可用来存储历史合规性数据	✓	
在同一报告或在线视图中，提供合规性状态和漏洞状态的历史视图	✓	
通过提供历史状态和当前状态视图的两相对照来支持审计请求	✓	
借助只读访问及访问选定信息，为审计员提供报告服务器支持	✓	
按照用户权限和角色来限制终端和报告访问	✓	
使用 IT 运营中用到的相同控制台、架构和代理来管理终端	✓	

最近发生的数据泄露凸显了保护敏感数据免受意外或蓄意滥用及丢失的迫切性。面临上述挑战，企业需要可靠的终端保护和数据丢失预防 （DLP） 解决方案，而且应可轻松部署到现有终端管理基础架构中，高效清除障碍以部署有效数据保护。部署一体化终端安全基础架构有助于降低复杂性，并可节省管理时间和成本。

终端保护

寻求具备以下功能的解决方案:	IBM	其他
提供一体化整合方法，为多家供应商的领先产品提供并管理杀毒、反间谍软件、防火墙和加密服务，例如 Symantec、McAfee、Trend Micro、Microsoft 和 Sophos	✓	
监控系统运行状况，确保终端保护客户端始终运行以及病毒签名已获得更新	✓	
通过一键式软件移除和重新安装操作，可将终端从一个安全解决方案快速迁移至另一个	✓	
使用闭环验证来确保已应用及实施安全设置，并已完成更新和其他更改；为那些从网络断开的终端提供互联网驱动验证	✓	
防止用户访问恶意网站，无论是自行访问，还是计算机恶意软件自动进行的隐藏操作	✓	
使用每天可动态排名数百万个单网页、基于云的 web 信誉技术，来防御基于 web 的恶意软件，包括 Web 2.0 威胁和数据窃取恶意软件	✓	
使用实时云数据保护终端免受病毒、特洛伊木马、蠕虫、间谍软件、隐匿程式、新型恶意软件变种和恶意网站的危害，确定文件和网站的安全	✓	
识别并完全移除已发现的间谍软件，包括隐藏的隐匿程式和残余文件	✓	
借助全方位终端管理控制台和基础架构，提供完全集成的杀毒和防火墙解决方案，消除有关单机病毒和防火墙部署基础架构的维护成本和复杂性	✓	
提供以单一控制台和单一代理基础架构所部署的集成数据丢失预防 （DLP） 功能	✓	
包括 DLP 功能，可用以保护所有设备数据并实施安全策略，从而允许用户访问适合自身工作的敏感数据，同时避免数据滥用或丢失，帮助遵守数据隐私法规	✓	
基于可寻找特定格式或编码（例如 Java 代码）并对此作出响应的关键字、正则表达式以及可配置规则，来防止数据滥用	✓	
包括预定义模板，用以遵守特定法规，例如《Gramm-Leach-Bliley Act》（格雷姆-里奇-比利雷法案，GLBA）、HIPAA、《Payment Card Industry Data Security Standard》（支付卡行业数据安全标准，PCI DSS）、California SB-1386 和 US PII	✓	

终端保护

寻求具备以下功能的解决方案:	IBM	其他
提供多渠道监控和实施，阻止或允许数据被复制或发送到各种服务渠道，其中包括电子邮件、剪贴板、FTP、HTTP、HTTPS、SMB、IM 和 Webmail 等，以及监控数据记录器、加密、对等应用程序、可移动存储器等物理渠道	✓	
实现可配置响应，范围从阻止操作、警告最终用户再到自动通知管理员	✓	
监控及控制终端上的物理端口，并可基于设备类型和内容识别扫描限制来启用或禁用这些端口	✓	
包括粒度设备控制，可按照供应商、型号和序列号对 USB 可移动存储设备访问进行限制	✓	

移动设备管理

随着人们在日常生活中广泛应用功能强大的智能手机和平板电脑，这些装置的业务应用也在成倍增长。这些移动终端为员工提供更进一步的灵活性，也相应地将生产力提高到新的水平。但是，与 IT 企业管理多年的传统终端不同，移动设备平台体现出并不符合传统终端管理范式的独特管理需求。IT 企业利用其现有管理技术和基础架构无法满足这些设备的管理需求，通常会为了在工作场所管理员工移动设备的使用情况，而仓促寻找安全有效的方法。

并非针对移动设备实施分离的管理基础架构和流程，而是以一款解决方案提供一体化终端管理，企业将因此而受益 — 该解决方案可跨所有终端类型实施高水准的应用程序和安全管理，同时还能高效满足移动设备的独特需求。理想的一体化管理平台可保护及管理传统终端，以及智能手机和平板电脑。

移动设备管理

寻求具备以下功能的解决方案:	IBM	其他
充分利用单一基础架构，为包括智能手机、平板电脑、台式电脑、笔记本电脑和服务器在内的所有类型的企业终端提供一体化管理和安全	✓	
支持 Apple iOS、Android、Windows Phone、BlackBerry 和 Symbian 等大量移动平台，可最大程度提高灵活性	✓	
为多个管理选项提供单一控制台支持，可囊括不同的员工和承包商使用案例，其中包括全设备管理、电子邮件同步管理、电子邮件和 PIM 容器、应用程序容器和双人操作系统	✓	

移动设备管理

寻求具备以下功能的解决方案:	IBM	其他
实现设备设置的综合配置和实施，包括密码和加密策略、电子邮件、VPN、LDAP、Wi-Fi、照相机和其他设置	✓	
处理最佳实践以遵守各项标准和数据隐私规定，例如互联网安全中心（Center for Internet Security，CIS）安全基准、PCI DSS、SOX、HIPAA，以及州、当地和国际数据隐私法律	✓	
在设备丢失、被盗或退役后，通过启用完整或选定擦除能力来保护企业数据	✓	
使用整合的电子邮件和基于代理的管理功能，提供安全和管理设备方面的灵活性，同时保留本机设备体验	✓	
通过识别违规设备以及自动执行修正操作（例如拒绝电子邮件访问、取消配置文件的配置或移除 VPN 访问），帮助维护合规性	✓	
通过对已安装应用程序进行报告、识别列入黑名单的应用程序以及通过企业应用商店分发应用程序，来提供完整的应用管理	✓	
提供企业级 API，将移动设备和传统终端数据与其他企业系统相集成，例如服务台和配置管理数据库 （CMDB）	✓	
与 Nitrodesk Touchdown、Enterproid Divide 和 Samsung KNOX 等第三方“容器”技术集成	✓	
利用 Samsung SAFE 等第三方扩展操作系统控制钩 （system control hook），获得附加的企业管理功能。	✓	
对整个企业网络以无线 （OTA） 方式或通过网络进行管理	✓	
提供用户自助服务功能	✓	
捕获及存储详细设备数据，包括仓库数据（例如设备型号和序列号）、使用数据（例如最近一次连接时间）、硬件信息（例如固件和内存），以及操作系统版本、地点信息、网络详细信息和已安装的应用程序及证书	✓	
检测根设备或“破解”设备	✓	
帮助管理员分发、安装、撤销、移除和返回第三方认证状态	✓	

绿色 IT

大多数终端都具有内置电源管理功能，许多最终用户都非常熟悉它的控制方式。但若依赖最终用户管理企业能耗，远远无法实现可衡量的结果。更有效的方式是实行集中管理。理想的解决方案可借助由单个一体化控制台所提供的控制功能，来减少耗电量，同时避免系统管理的中断。

这种解决方案允许 IT 企业为整个基础架构应用保护策略，同时提供必要的细致性，可将电源管理策略应用至单一计算机。通过将电源管理与远程唤醒功能相结合，可满足有时甚至是冲突的管理需求（通常倾向于频繁关闭机器电源，以最大程度节省能源）与 IT 需求（在非工作时间运行机器，以尽可能简化应用补丁和更新的操作）。

绿色 IT

寻求具备以下功能的解决方案:	IBM	其他
从相同集中式服务器和控制台针对 Windows 和 Mac 操作系统上运行的所有终端进行电源设置管理	✓	
提供即时可用的功能，以应对常见电源管理问题，例如 PC 失眠和 PC 嗜眠	✓	
必要时提供将策略应用至单一计算机的细致性	✓	
帮助管理员基于检测特性向各系统分配不同的用电量指标	✓	
为休眠、待机和“关机前保存工作”选项提供精细控制	✓	
利用选择加入的方式为最终客户提供支持，这种方式允许用户从管理员定义的电源配置选项菜单中选择其电源配置文件	✓	
让最终用户通过其各自的能耗和节省状况客户端演示板视图参与到保护措施中来	✓	
可创建“假设”业务能耗情景，并提供绿色影响报告，以鼓励用户参与到保护措施中来	✓	
识别并自动修补电源配置文件的误配置	✓	
规划计算机睡眠和休眠状态，保证一定数量的计算机可接收唤醒报警，并将报警分发至处于更深层次睡眠状态的其他计算机	✓	
通过在开始关机或睡眠/待机步骤前自动保存文档来保护用户数据	✓	
规划 Wake-on-LAN （WoL），以在工作日伊始或计划维护之前启用终端唤醒，包括支持远程用户唤醒	✓	
借助将报告数据导出至 Microsoft Excel 以供进一步分析的功能，对汇总用电量和节能情况提供图形报告	✓	

管理系统架构

在大多数分布式环境中，终端数量和类型不断增加，网络状况日趋复杂。终端的可见性和控制力往往不足，服务水平也难以维持。由此产生的挑战是，如何获得准确而全面的、有关该环境的“单一真实信息来源”，然后借此管理大量终端。该解决方案的技术核心在于，能够在整个企业内部整合及简化关键管理服务。

通过在每个终端内放置智能化代理，这种解决方案可执行包括连续自我评估和策略实施在内的各种功能。与等待中央控制点指令的传统主从式架构不同，智能化代理是以自主方式启动操作，将消息逆向发送至中央管理服务器，必要的时候，为遵守相关策略，还可将补丁、配置或其他信息调用传输至终端。

该单一基础架构方法将决策制定分布至终端，以缩短更新周期、提高配置成功率、提升最终用户生产力，并减少 IT 和帮助台劳动力需求。

管理系统架构

寻求具备以下功能的解决方案:	IBM	其他
在单一视图、交付模型和软件产品中整合各项 IT 运营和 IT 安全功能	✓	
使用单一、多用途的智能化代理评估及补救问题	✓	
提供连续的终端自我评估和实时策略实施	✓	
所用终端内存通常不到 10 MB	✓	
平均需要不到 2% 的 CPU 利用率，确保不会影响终端性能	✓	
无论终端是否连接至企业网络，均可自动评估和实施策略	✓	
提供本地资源和基于策略的动态网络带宽利用节流控制	✓	
采用已发布的命令语言，帮助客户、业务合作伙伴和开发人员创建用于托管终端的定制策略和服务	✓	
提供对所有终端的实时可见性，其中包括台式计算机、笔记本电脑、服务器、移动设备、销售点系统、ATM 和自助服务终端	✓	
提供易用的图形用户界面，以及高级命令行接口 （CLI） 和 API	✓	
通过单一管理服务器支持多达 250,000 个终端	✓	

管理系统架构

寻求具备以下功能的解决方案:	IBM	其他
管理无论是否连接至网络的移动终端	✓	
管理异构平台（在物理或虚拟机器上运行的 Microsoft Windows、UNIX、Linux 和 Mac 操作系统）以及智能手机和平板电脑	✓	
使用相同基础架构和资源提供集成式远程控制，以简化帮助台呼叫和问题解决流程	✓	
利用现有服务器或工作站筹划软件安装器和补丁等内容，从而减少管理服务器的需求，确保软件交付速度及最大程度减少网络流量	✓	
允许将任何代理配置为其他代理和集中管理控制台之间的中继或升级代理，以可选方式存储策略和内容，从而减少网络负载	✓	
提供使用 EAL 3 Common Criteria 认证的供应商软件解决方案	✓	
通过用户许可和角色控制并限制对终端、报告和管理控制台的访问	✓	
与以往动辄数周或数月的时间相比，即时是针对规模最大的企业，也能够在几小时或几天内完成全面部署，实现快速安装	✓	
在几分钟内，即可将最新发现的终端用户管理整合到智能化代理的本地部署中	✓	
对各终端管理功能使用相同基础架构，以便轻松解决当前挑战，并可随着企业需求的增长无缝添加其他终端管理功能	✓	
利用自身基础架构进行升级，在几分钟或几小时而非几周或几个月内即可完成主要的产品升级和更新	✓	
验证客户报告以预防欺骗	✓	
为保护敏感信息转移至终端而提供内置加密功能	✓	
利用集成产品和内容更新，尽可能减少将实施保持在最新状态所需的工作	✓	
与综合管理产品组合相集成，可帮助实现整个 IT 基础架构的实时可见性、集中控制和功能增强	✓	
提供包括意大利语、德语、法语、西班牙语、日语、简体中文、繁体中文、葡萄牙语、韩语和英语在内的本地语言支持	✓	

选择正确的终端管理供应商

您所选的供应商，应能全线支持您的终端管理需求。理想情况下，还可为您的整个解决方案实施过程提供支持。选择供应商之前，请务必思考以下问题：

供应商能否通过自身技术为您的企业目标提供支持？
寻找其提供的解决方案与贵企业目标相契合的供应商。其解决方案能否提升效率、减少业务服务部署时间、降低成本、增强合规性及缩短上市时间？

供应商提供部分还是全套的完整解决方案？
如果供应商的解决方案只侧重于应对特定环境或终端需求，与之合作将使您陷入“管理孤岛”的困境。涉及多家供应商时，解决方案成本和管理多个供应商所耗费的时间都会大幅增加。寻求具备终端管理全套产品组合的供应商。

供应商具有何种类型的全球形象？
如果贵企业拥有国际办公室，则应寻求具有国际格局和成熟的国际运营经验的供应商。确保供应商能够借助其当地资源支持您的海外办公室。

为解决方案提供支持的机构，是否具备成熟的支持服务，且拥有值得您依赖的专业知识和带宽？
您的供应商应能提供快速响应和高效客户支持。寻求具有成熟支持机构、可帮助您最大程度提高软件投资价值的供应商。

在当今的经济环境下，如何确定供应商的稳定性和持久性？
极具挑战的经济环境在很大程度上影响着供应商的稳定性和生存力。那些拥有悠久的业界历史、制定了富有远见的稳妥战略、具有可平稳度过经济萧条期的充足资源的供应商，才是您应该考虑选择的对象。

供应商提供的产品是否具备战略性的设计和技术方面的优势？
比较各种解决方案时，应将关注点放在技术优势上：即精心设计的功能、智能化架构设计，以及对各种行业标准的支持能力。

助力终端管理成功的一体化解决方案

为满足自我目标而评估解决方案时，您会发现，IBM 不仅能够提供最佳终端管理解决方案，还能跨功能强大的安全产品组合，提供非凡的广度和集成能力。IBM 解决方案旨在为您提供有关贵企业终端环境的可见性。它们有助于控制管理成本、安全性及合规性。还有助于减少管理异构终端、操作系统和应用程序基础架构的复杂性。

常言道“不可见者无从管理”，这个道理同样适用于终端管理。在所有功能中，IBM 终端管理特别提供一体化可见性和控制，专门设计用于打破 IT 孤岛，以实现及时、有效的终端管理。任务的自动化和集成，与连续性异步管理评估和策略实施的智能化代理相结合，使得大型管理服务器基础架构成为不必要的存在。

IBM® Endpoint Manager 解决方案可快速、准确地跨基础架构实施有效变更，从而大幅弥补管理功能与安全风险之间的空白。该解决方案基于 IBM BigFix® 技术，可帮助降低安全风险、管理成本和管理复杂性，同时增加终端策略实施和补救的速度和准确性。单一代理、单一管理台和单一管理服务器这种经特别设计的方法，可通过补丁管理、配置管理和终端发现等功能，来增加可靠性并加速实现价值。此方法可通过提高运营效率、进行管理基础架构整合及提高 IT 生产力来提升投资回报。

IBM Endpoint Manager 提供的单一代理方法，可进一步帮助企业从当前资产中获取最大价值。由于该解决方案的管理服务器始终借由代理而保持最新状态，因而无需运行冗长的扫描、执行查询，也不必担心系统停机或漫游离开企业网的范围。以代理的自主操作，搭配单一控制台提供的可见性，可帮助管理员查看在整个网络内发生的事件。

IBM Endpoint Manager 是 IBM 综合安全和管理产品组合的一部分，企业可借此应对分布式基础架构的各项挑战。在以设备装配、互联及智能化 IT 运营所构建的智慧地球中，IBM 安全和管理解决方案设计用于确保整个 IT 基础架构的实时可见性、集中控制和高级自动化，其中包括全球分布式终端。

如需更多信息

要了解有关 IBM Endpoint Manager 的更多信息，请联系 IBM 销售代表或 IBM 业务合作伙伴，或者访问：**ibm.com**/tivoli/endpoint

关于 IBM Security 解决方案

IBM Security 可提供最先进的集成式企业安全产品和服务组合之一。该组合由世界知名的 IBM X-Force® 研发团队提供支持，提供充足的安全智能，以身份和访问管理、数据库安全、应用程序开发、风险管理、终端管理、网络安全及其他各方面的解决方案，帮助企业全面保障其人员、基础架构、数据和应用程序的安全。这些解决方案可帮助企业有效管理风险，并针对移动设备、云平台、社交媒体及其他企业业务架构实施集成式安全解决方案。IBM 拥有世界上规模最大的安全研发和交付机构，每天监控 130 多个国家超过 130 亿个安全事件，并持有 3,000 多项安全专利。

此外，IBM Global Financing 可以帮助您以最经济高效和最具策略性的方式获得您企业所需的软件功能。我们将与符合信用要求的客户合作以定制最适合其业务与发展目标的融资解决方案，实现高效的现金管理，并降低其总拥有成本。IBM Global Financing 可为您的重要 IT 投资筹措资金并推动业务向前迈进。如需更多信息，请访问：**ibm.com**/financing

IBM Corporation Software Group
Route 100
Somers, NY 10589

美国印制
2013 年 5 月

TIO14008-CNZH-02