



利用英特尔® 博锐® 平台管理构建一个 智能、互联世界

利用英特尔® 博锐® 技术，企业可以在日益多样化的设备环境下，甚至在防火墙之外，提高安全性和可管理性，帮助减少支持成本并缩短解决问题的时间。

如果您负责以下领域：

- **IT 投资决策和业务战略：**您将了解英特尔® AMT 和英特尔® EMA 如何简化您的各种设备的管理，帮助减少成本并提高正常运行时间和用户满意度。
- **管理或支持您的组织的设备，包括远程设备：**您将了解架构组件以及它们如何协同工作，为在所有部署方案中（包括在防火墙之外）远程管理这些设备打造一个整体化解决方案。

执行概要

随着智能设备的普及，如个人计算机、数字标牌、销售点 (PoS) 系统和 ATM 等，IT 组织管理的设备及其连接地点变得越来越多样化。每个额外的设备类型和地点均有可能增加支持服务的成本和复杂性。与此同时，支持型组织面临的挑战是帮助降低运营成本并提高响应能力和用户生产力。为此，组织需要第一时间成功解决更多问题，帮助降低与运输设备至支持中心或进行桌面访问有关的成本。在使用他们现有的工具和最佳实践流程的情况下，自动化和可扩展性可帮助 IT 组织实现这些目标以及减少错误。

本文讨论了下述技术和工具：

- **英特尔® 主动管理技术 (英特尔® AMT)** 是英特尔® 博锐® 平台的一个功能，可为资产管理提供基于远程硬件的能力，允许从操作系统进行带外管理。
- **英特尔® Endpoint Management Assistant (英特尔® EMA)** 是一个软件工具，旨在使英特尔® AMT 现代化并在企业防火墙之外管理托管和基于云的环境中的设备。英特尔® EMA 可通过软件代理进行带内通信或通过英特尔® AMT 进行带外通信。

技术和工具共同构成一种有效的解决方案，有助于降低服务成本，同时提高响应能力、安全性和用户满意度。本文详细介绍了该解决方案如何与当前流程以及现有安全性和可管理性企业架构（包括完整解决方案的架构组件）集成。

简介

随着新的设备和工作模式在所有行业中的出现，经济转型正在加速，改变了我们的工作方式和使用的技术。该转型的结果是一个智能的世界，预计至 2020 年联网设备将超过 500 亿台。¹

在各个行业中，组织必须支持越来越多样化的设备，远远超出 PC 和移动设备的范围。在零售业中，联网销售点 (PoS) 和自动售货系统是关键性任务。在银行业中，ATM 必须保持安全并且可用于客户依赖的自助服务业务模式。数字标牌必须能够防篡改，同时联网以进行更新。IT 组织面临前所未有的复杂设备环境，而业务目标从未如此依赖这些设备。

这为 IT 带来了挑战：所有设备必须安全且受到管理，但在每次设备出现问题时均派工程师维修是不现实的。运行技术 (OT) 也面临挑战，因为创新工作者希望获得合适的设备完成这项工作，但是这些设备必须安全并易于使用。为成功转型，企业必须将 IT 和 OT 结合在一起，无论 IT 功能是由服务提供商、系统集成商提供还是由内部提供。

目录

简介	1
所有部署方案中的远程能力	2
针对每个环境的部署	3
管理架构	4
应用案例	4
服务台	4
事件管理	4
服务资产和配置管理	4
发布和部署管理	4
用户界面示例	5
总结	5

管理良好的设备可以更安全，并让 IT 组织能够更迅速地响应安全事件。

许多组织花费数年时间开发基于 IT 基础架构库 (ITIL) 和其他行业标准的流程和软件工具，以管理其设备。重新开始不是一个选项。相反，它们需要新方法，以一种适合其现有管理框架的方式管理不断增加的复杂性。即使添加了性能更强的设备，较旧设备也必须保持安全和可靠，这增加了支持负担。至 2020 年，预计 72% 的用户将是可在任何地点工作的移动用户。² 这些用户需要可靠的解决方案，组织则希望所有设备无论在何处均保持一致的安全性和可用性标准。

系统集成商正在不断寻找降低支持成本同时确保用户满意度的新方法。支持合同通常含有年度费用消减，因为客户希望在技术进步降低成本的背景下避免支付过多费用。以更低的成本提供更好的服务需要自动化和可扩展性。

十多年来，英特尔® 主动管理技术 (英特尔® AMT) 一直是英特尔® 博锐® 平台的一个组件，为设备提供简单而强大的带外端点管理。现在，利用英特尔® Endpoint Management Assistant (英特尔® EMA)，IT 组织可以访问企业防火墙之外的设备，并进入基于云的环境，无论设备位于何处，这均有助于解决当今的挑战 (见图 1)。

受益于该技术的一些行业包括：

- **医疗保健。** 利用最新安全修补程序改进共享设备的维护操作有助于保护患者资料。
- **零售。** 零售业各种设备的流线化管理，如远程售卖机、PoS 系统和数字标牌。
- **金融。** 时间就是金钱，管理良好的设备在设备出故障时能够让员工更快速地恢复生产力。

对于 IT 服务提供商而言，英特尔® 博锐® 平台带来一个交付创新服务的机会。凭借支持云服务的英特尔® EMA，英特尔® AMT 在提高响应能力方面起到重要作用，使得企业在这个智能世界中获得竞争优势。

所有部署方案中的远程能力

英特尔® AMT 提供远程访问设备以进行诊断和管理的功能，即使设备断电或操作系统未运行。利用 TLS 和摘要凭证保证访问安全。

英特尔® EMA 将该能力扩大至企业防火墙内外的所有环境，包括本地、场外、基于混合云的环境和 DMZ 内。可通过目录服务凭证控制对英特尔® EMA 控制台的访问。

可通过有线或无线 LAN 连接实现远程管理功能，包括：

- **电源控制。** 接通一个或多个系统的电源以进行补救或修补。还可以通过 API 访问该能力。
- **闹钟。** 远程对设备进行编程以在预定的日期和时间唤醒或启动。例如，设备可在工作日开始前的 10 分钟启动或定时启动以进行例行的维护任务。
- **远程控制基于硬件的键盘、显示器和鼠标 (KVM)。** 利用基于硬件的 KVM 远程控制查看和解决用户 PC 和操作系统问题，通过重启周期维持 KVM 连接。
- **访问硬件资产信息。** 远程查看硬件配置 (即使 PC 关闭或睡眠)，包括 CPU、内存和硬盘类型等参数。如果一个部件发生故障，硬件资产功能可在桌面访问前确认正确的备件，有助于减少访问次数和解决问题花费的时间。
- **发现和清单。** 远程发现硬件资产及其配置和英特尔® 博锐® 平台功能。自动识别环境中有多少基于英特尔® 博锐® 平台的系统是使用英特尔® AMT 的第一步。
- **可选用户同意。** 显示独立于操作系统的 6 位随机授权代码，以确保设备上的远程补救命令获得用户同意。
- **在防火墙之外的支持。** 借助英特尔® EMA，IT 组织现在可以利用英特尔® AMT 功能远程管理企业防火墙之外的设备。
- **基于云的可管理性。** 采用支持云的英特尔® EMA，英特尔® AMT 让 IT 组织能够管理托管于防火墙内外 (甚至 DMZ 内) 的全球设备机群。

将功能扩展至防火墙之外

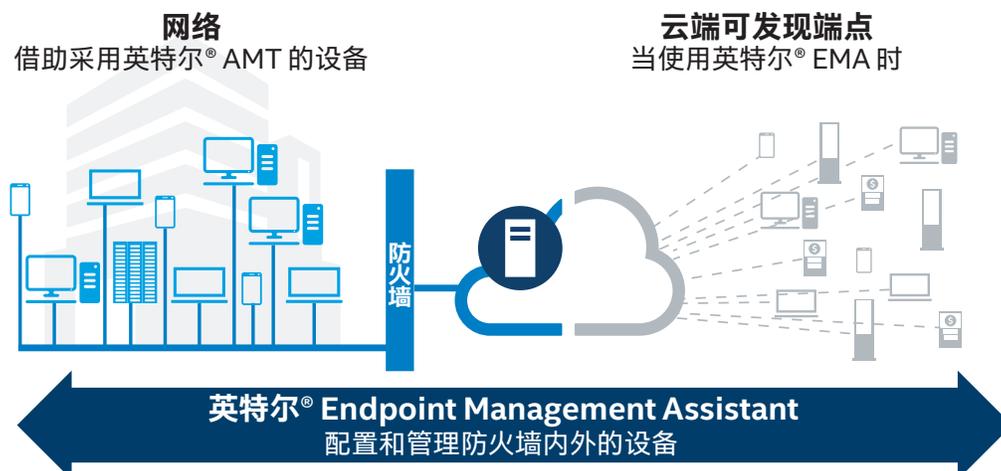


图 1. 英特尔® 主动管理技术 (英特尔® AMT) 可加强现有流程和功能，以改善终端用户体验和资产数据质量。英特尔® Endpoint Management Assistant (英特尔® EMA) 可将功能扩展至防火墙之外和云端。

与现有的 IT 管理工具和流程结合使用，这些服务和功能提高了组织的各种设备的可管理性，使得利用一致的流程和工具进行跨环境远程管理和访问成为可能。采用英特尔® EMA 的英特尔® AMT 通过向更多设备推送更及时的修补程序提高了安全性。

针对每个环境的部署

下述英特尔® EMA 部署模型通过英特尔® AMT 提供远程访问，实现了基于组织个性化需求的灵活性（见图 2）：

- **本地。**当没有云实例时，或在测试和配置功能时，远程管理企业环境中的所有设备。
- **场外。**远程管理托管的场外私有云环境中的所有设备。对于刚刚使用英特尔® AMT 和英特尔® EMA 以及一系列内置工具的 IT 组织，部署至场外云端可以为初始设置和配置提供良好的环境。
- **防火墙之外。**通过更安全的通道访问防火墙之外基于云的设备来远程管理设备。
- **混合云远程管理本地和托管私有环境混合云中的所有设备，这是当今移动客户端最常见的实例。**

如图 3 所示，利用单实例基础服务器，全局管理员可定义一个或多个租户（安装期间，定义全局管理员和首个租户）。在每个租户中有多组系统以及管理这些系统的基于角色的账户。例如，一个政府实体可能会基于不同机构设立租户。然后各个机构的 IT 运营或服务人员为特定的租户分配角色和权限。在这些租户中，系统可由租户管理员进行分组。各机构则可以根据自身要求和运营需求独立管理其 PC。

除了中继服务器和数据库，基于服务器组件的英特尔® EMA 单一实例包括：

- **Ajax 服务器。**处理 JavaScript 库和 API 请求，如带内远程桌面功能。
- **Swarm 服务器。**管理受管理设备与英特尔® EMA 实例之间的带内和带外连接。
- **可管理性服务器。**管理设备的英特尔® EMA 配置和取消配置。

- **文件操作服务器。**用于从英特尔® EMA 服务器至设备的带内文件传输。
- **英特尔® EMA 网站。**当未通过 API 集成至部署中时，这为英特尔® EMA 提供了一个用户界面。

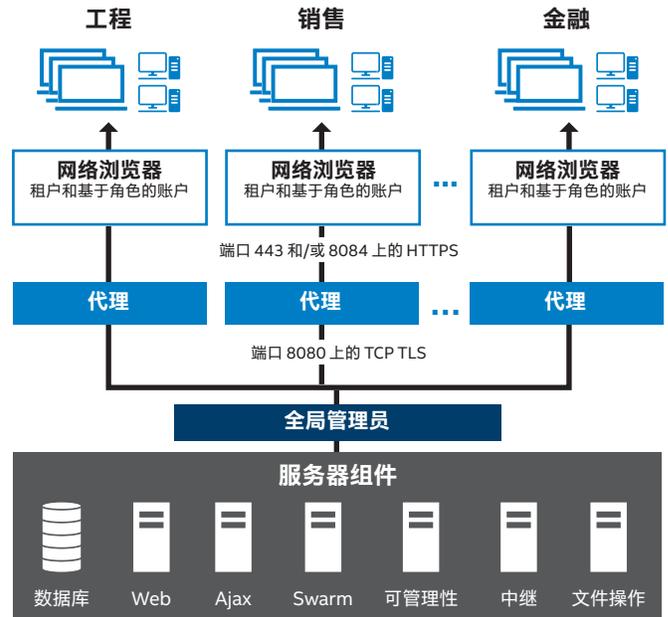


图 3.单一实例基础服务器组件允许全局管理员在任何部署方案下定义和管理租户环境和租户管理员。

英特尔® EMA 部署环境

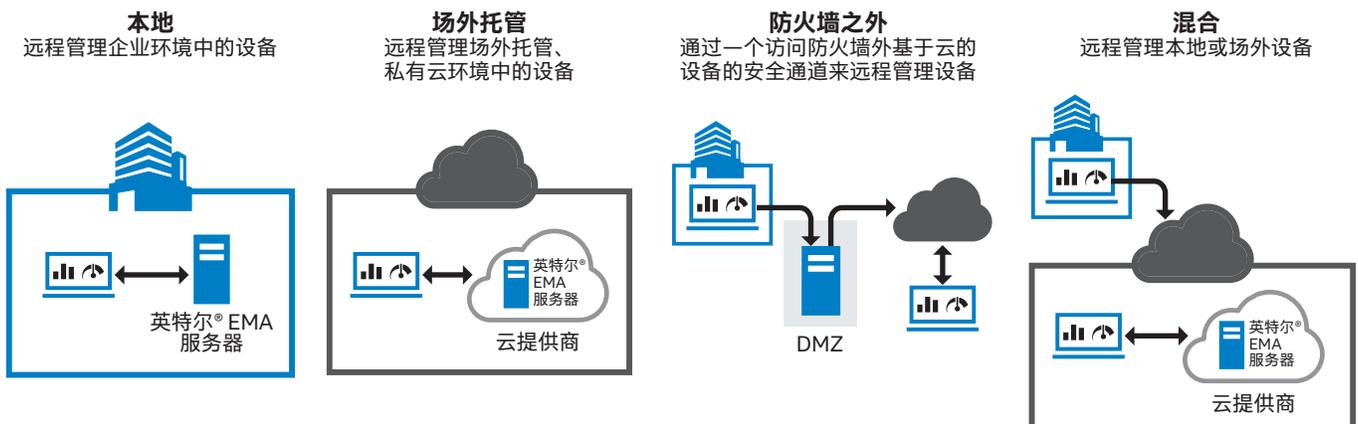


图 2.英特尔® Endpoint Management Assistant (英特尔® EMA) 支持通过英特尔® 主动管理技术 (英特尔® AMT) 远程访问企业防火墙内外的设备。

管理架构

英特尔® EMA 提供了一个实现可管理性的通用方法。IT 组织通过一个单一解决方案管理其所有英特尔® 博锐® 平台，该解决方案可无缝管理不同制造、类型和世代的机器，而现在利用英特尔® EMA，IT 组织可以管理所有环境中的机器（见图 4）。³

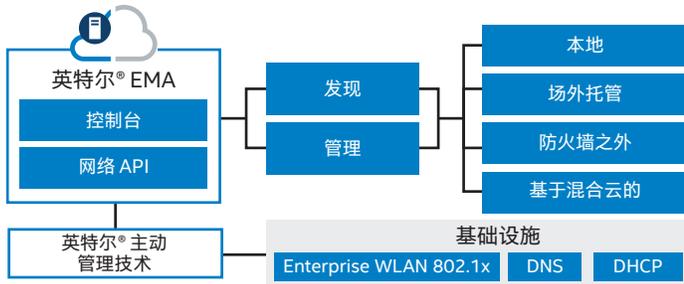


图 4. 配备英特尔® EMA 的英特尔® AMT 提供端对端设备管理。

英特尔® EMA 旨在利用基于云的功能令英特尔® AMT 实现现代化。后端服务器软件包括一个网络用户界面、英特尔® EMA 服务器和英特尔® EMA 数据存储。客户端软件包括具有设置和数据的英特尔® EMA 代理，以建立基于云的通信。许多熟悉的工具，如客户端发起的远程访问，现在均内置于英特尔® EMA，缩短了学习曲线。激活英特尔® AMT 后，组织还可以利用替代解决方案管理设备，包括与英特尔® AMT WebUI 集成的英特尔® Manageability Commander、任务自动化和配置管理脚本以及网络 API。该解决方案可集成至现有的基础架构，如证书授权、目录服务或其他基于 LDAP 的服务。通过管理员定义的用户 ID 和密码或通过域用户 ID 和电子邮件地址对英特尔® EMA 控制台进行身份验证，然后英特尔® EMA 可以为传输层安全通信颁发证书。

应用案例

利用用户界面或 API，管理带内和带外功能。API 使英特尔® EMA 能够与其他第三方工具集成，通过英特尔® 博锐® 平台改进现有的 ITIL 和 IT 组织功能和流程。

服务台

利用英特尔® AMT 和英特尔® EMA，服务台功能可以提高客户满意度，改善针对请求的响应能力，并有助于降低支持成本。根据福瑞斯特最近受英特尔委托进行的一项研究，一个复合型组织的专业人员利用英特尔® 博锐® 平台帮助带来下述改进：⁴

- **减少安全问题。**作为英特尔® 博锐® 平台的一部分，英特尔® AMT 通过减少支持和管理工作，每年可帮助节省约 7,680 个安全支持工时。⁵ 由于英特尔® 博锐® 平台带来的改进，微小的和重大的安全和管理问题均减少了，而且剩余的问题得到了更快速的解决。
- **降低安全支持和管理成本。**作为英特尔® 博锐® 平台的一部分，英特尔® AMT 可在三年内帮助降低安全支持和管理成本总计近 120 万美元。⁵
- **提高员工效率。**借助更好的设备安全和管理，估计可节省 28,160 小时。⁶ 员工花更少的时间等待安装更新、处理需要安全和管理支持的问题以及等候设备从睡眠模式唤醒。

- **提高计算机和数据安全性。**除了安全补救时间的节省，英特尔® 博锐® 平台还借助硬件增强的安全性和可管理性功能，帮助保持公司数据的安全并减少数据泄露的风险。
- **更快和更及时的 IT 修补程序安装。**一个复合型组织的 IT 管理人员和桌面运行专业人员利用英特尔® 博锐® 平台，三年内帮助节省总计 832 小时部署修补程序和处理现场异常的时间，估计带来 81,000 美元的费用节省。⁷

通过自动提供完整和准确的配置信息，可以提高服务代理的生产力并缩短解决问题的时间。使用英特尔® EMA 的服务台可提供一个环境，让用户能够在设备维修时继续工作，同时要求实时访问和控制设备，以进行诊断和解决问题。

事件管理

针对支持工作的常见关键绩效指标 (KPI) 包括解决问题的速度。在多数行业中，设备停机可对收益率和客户满意度造成可衡量的直接影响。较短的恢复时间对于业务至关重要。针对 ITIL 下的服务运行的 KPI 通常包括远程解决的事件数量、第一时间解决率和 SLA 内解决的事件数量。采用支持云的英特尔® EMA，英特尔® AMT 大幅提高了这些 KPI。

英特尔® AMT 帮助加速事件的响应和处理，无论受影响系统的状态如何。与支持功能中经常使用的 PC 管理软件相比，英特尔® AMT 提供对设备的访问，无论操作系统是否正在运行（或能够运行），而且只要设备通电并联网，即可对其进行远程管理。英特尔® EMA 将其范围扩展至企业内部网络和防火墙之外。代理可立即发现相关信息，例如设备配置，无需用户的介入。代理可使用基于硬件的 KVM 访问来维修设备。

服务资产和配置管理

首次构建或购买时，组织会把资产输入配置管理数据库 (CMDB)，但之后很少会根据变化进行更新，从而产生一个普遍问题。当收集硬件和软件配置的清单工具无法访问设备时，就会发生这种情况。不准确的数据可能导致订购错误的维修部件，或因为需要了解正确的配置信息而无法及时采购部件。不合规的系统还会更易受病毒攻击，使 IT 组织难以识别薄弱点。

配备英特尔® EMA 的英特尔® AMT 让 IT 服务组织能够远程访问系统，维护完整和准确的信息（即使在防火墙之外）。英特尔® AMT 在非易失存储器中维护重要的配置信息，这种存储器可以防止篡改，并且可以跨多个操作系统和硬件组件持久保存信息。此外，它可以加强组织识别物理和逻辑关系以及识别并安排任何必要改变的能力。英特尔® AMT 可在管理员模式下激活，允许不经用户同意访问设备，或在客户端模式下激活，这需要终端用户的同意。

英特尔® EMA 纳入下述配置功能，增强了英特尔® AMT：

- **发现。**发现、收集和维持当前、准确的全部设备配置信息，无论其位于何处。
- **基于主机。**基于主机的配置是针对英特尔® AMT 的英特尔® EMA 的首选、默认方法，适用于本地或场外设备。
- **远程。**通过有线 LAN 配置本地设备。

发布和部署管理

无论是重大或次要软件发布、硬件升级或紧急情况，英特尔® AMT 和英特尔® EMA 均可帮助部署更快速、更少人工干预的

系统，无论环境如何。可在保持对终端用户最少干扰的同时，启动、监视和控制部署。

升级操作系统可能最具挑战性，而修补和更新则是常见活动。利用基于硬件的 KVM，英特尔® AMT 和英特尔® EMA 提供监控更新流程或唤醒并更新设备的能力（无论其电源状态如何），这有助于提高安全性和可靠性。

用户界面示例

英特尔® EMA 让管理员能够监控和管理针对远程设备的带内和带外控制，从而在操作系统内提供了机会（见图 5）。



图 5. 管理员可查看系统状态和配置（示例显示带外设备）。

英特尔® EMA 让管理员能够通过脚本执行命令，例如使用接通电源（Power On）来唤醒设备（见图 6）。

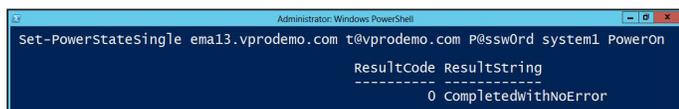


图 6. 利用任务自动化和配置管理框架脚本（来自 Microsoft*），英特尔® EMA 通过 API 控制电源功能（示例显示带外设备）。

总结

英特尔® AMT 为面向用户的设备和智能联网设备的远程管理提供了坚实的基础，而英特尔® EMA 将该能力扩展至企业防火墙之外。英特尔® AMT 在现有业务流程内运行并受到主要 IT 管理工具的支持，可帮助 IT 组织应对在管理其设备过程中不断增长的复杂性，而不必使其管理基础架构变得复杂化。通过提供针对设备的远程访问，无论位于何处，即使断电或缺乏有效运行的操作系统，配备英特尔® EMA 的英特尔® AMT 均有助于实现更快速的事件解决并帮助降低服务台的总体运行成本。英特尔® AMT 可精简常见的 IT 活动，例如用户自助服务、修补和升级、机器恢复和镜像重造和配置审查。十多年来，英特尔® AMT 一直是英特尔® 博锐® 平台的一部分，可通过各种解决方案激活。

参考资料

- 英特尔® 主动管理技术
- 英特尔® 博锐® 平台
- 英特尔® AMT 软件部署套件主页
- 托管服务供应商

¹ Nihar Pachpande, 2018 年 3 月 18 日, “至 2020 年联网设备将达 500 亿台。”

² IDC 预测至 2020 年美国移动工作人口将超 1.05 亿。

³ 英特尔® EMA 支持英特尔® AMT 11.x 及更高版本。英特尔技术特性和优势取决于系统配置，并可能需要支持的硬件、软件或服务得以激活。实际性能可能因系统配置的不同而有所差异。没有任何产品或组件能够做到绝对安全。联系您的系统制造商或零售商，或在如下网址了解详情：intel.com/AMT。

⁴ “英特尔® 博锐® 平台的总体经济影响”是受英特尔公司委托并由福瑞斯特咨询公司 (Forrester Consulting) 实施的一项研究，2018 年 12 月。该研究表明，其他组织可获得的节省因多种因素而异，这些因素包括企业切换到英特尔® 博锐® 平台前的规模、安全基准级别、可管理性和生产力。请参考其他资料来源，并使用特定于您的组织的信息来确定可为您的组织带来的好处。

⁵ 根据福瑞斯特咨询公司在英特尔委托的一项 TEI 研究中以一个复合型组织为模型进行的估计，3 年中利用基于英特尔® 博锐® 平台的设备，每年可减少 7,680 个安全支持工时，共带来 120 万美元的费用节省（2018 年 12 月）。阅读完整的研究报告——[英特尔® 博锐® 平台的总体经济影响](#)。

⁶ 根据福瑞斯特咨询公司在英特尔委托的一项 TEI 研究中以一个复合型组织为模型进行的估计，3 年中利用英特尔® 博锐® 平台获得更好设备安全和管理，提高了员工工作效率，共节省 28,160 小时，带来 130 万美元的成本节省（2018 年 12 月）。阅读完整的研究报告——[英特尔® 博锐® 平台的总体经济影响](#)。

⁷ 根据福瑞斯特咨询公司在英特尔委托的一项 TEI 研究中以一个复合型组织为模型进行的估计，3 年中通过英特尔® 主动管理技术进行自动远程修补程序部署，共节省 832 小时，带来 81,000 美元的费用节省（2018 年 12 月）。阅读完整的研究报告——[英特尔® 博锐® 平台的总体经济影响](#)。

所描述的降低成本方案仅用作示例，表明某些基于英特尔的产品在特定环境和配置下会如何影响未来的成本，并节约成本。环境各不相同。英特尔不保证任何成本或成本降低。

英特尔® 主动管理技术需要激活，以及具有企业网络连接的系统、启用了英特尔主动管理技术的芯片组、网络硬件和软件。对于笔记本电脑，在以无线方式连接、使用电池、睡眠、休眠或关闭电源的情况下，英特尔® 主动管理技术可能会在基于主机操作系统的 VPN 上不可用或受限。具体结果取决于硬件、设置和配置。欲了解详情，请访问 intel.com/AMT。

此处提供的所有信息可随时更改，恕不另行通知。如欲获得英特尔最新的产品规格和发展蓝图，请联系您的英特尔代表。

英特尔、英特尔标志和英特尔博锐是英特尔公司或其子公司在美国和/或其他国家（地区）的商标。

* 文中涉及的其他名称及商标属于各自所有者资产。

© 英特尔公司。保留所有权利。 0919/TCUT/KC/PDF 334533-003CN

