白皮书

企业在安全终端方面的当务之急

赞助商：苹果

Tom Mainelli　　Michael Suby

2023 年 9 月

IDC 观点

是什么让 IT 决策者夜不能寐？安全问题。聪明的 IT 决策者深知，无论一家企业经营得多么好，或者它的产品或服务有多么受欢迎，一旦出现安全问题，整个企业都可能在一夜之间陷入困境。

不幸的是，这个世界并没有变得更加安全。企业间谍、流氓国家、有组织的犯罪，甚至是寻常小偷都提高了技术水平。为了比坏人抢先一步，IT 部门必须保持警惕，随时准备采纳新的供应商和技术，确保员工、客户和数据的安全。

IT 所面临的安全挑战不胜枚举，涉及从终端（计算机）到数据中心、连接万物的网络以及运行所有设备的软件等方面。在本文中，我们将重点讨论确保终端安全的重要性。原因在于，归根结底，如果终端不安全，所有其他领域的安全都没有什么意义。

保障终端安全所面临的主要挑战之一是，传统安全的终端往往意味着要牺牲最终用户的使用体验，因为锁定的设备很难使用。而当这种情况发生时，任何安全方案中的另一个主要薄弱环节——用户，常常会本着完成工作的主旨找到规避安全措施的方法。当安全成为用户的障碍，就无法达到安全的目的了。

技术进步使我们越来越有可能在保障安全的同时维持高质量的用户体验。恶意软件检测、数据保护、身份验证以及芯片和软件融合等方面的进步意味着，如今的终端不需要为了增强安全性而牺牲生产力。

方法

IDC 于 2023 年 7 月对美国和加拿大的 IT 决策者进行了一项在线调查（n=513），调查他们对广义安全的看法，特别是保护计算机终端安全的重要性的看法。受访者代表了来自不同行业、拥有 500 名或更多员工的各类公司。这些 IT 决策者支持多种计算机操作系统，包括微软 Windows、苹果 macOS 和谷歌 ChromeOS。他们要么为自己的公司选择、购买或部署安全软件，要么管理从事这些工作的员工。

概况

安全问题仍然是 C 级高管的当务之急。具有前瞻性思维的公司认识到，良好的安全性不仅仅是“锦上添花”，而是企业在不断变化的威胁环境中健康、蓬勃发展所必需的，而这种威胁环境是由行动协调一致、资金充足的不良行为者所驱动的。

根据 IDC 于 2023 年 3 月针对拥有 500 名或更多员工的公司的企业 IT 决策者开展的未来企业复原力和支出调查，全球超过 50%的受访公司在过去 12 个月中遭受过破坏业务的勒索软件攻击。超过三分之一的受访者表示，勒索软件攻击导致业务中断了一周或更长时间。尽管大型公司可以说拥有更强大的安全协议，但它们也远不能幸免于此类攻击。事实上，受勒索软件破坏影响最大的是员工人数在 1000 到

2499 人（71%）、2500 到 4999 人（72%）和 5000 到 9999 人（70%）的公司。换句话说，无论公司规模大小，都无法幸免于难。

该调查还指出，终端是勒索软件攻击的主要入口。最初的入侵点包括网页浏览（21%）、可移动媒体（18%）、电子邮件附件（17%）、供应链（17%）、电子邮件中的网址（14%）和内部人员访问（8%）。

越来越多的员工在混合环境和远程环境中工作，这种持续转变只会使 IT 部门更难以对付勒索软件和其他的安全风险。IDC 于 2022 年 12 月开展的终端安全调查显示，超过 97%的企业有一部分员工进行远程办公。尽管预计这一数字在未来 12 个月内会有所下降，但在可预见的未来仍将居高不下。

在各公司努力应对大量远程员工带来的持续挑战之际，越来越多的公司开始实施零信任战略。最佳实践的重点领域包括建立安全控制基准、高级终端安全防御、设备验证（确保连接到网络的设备是合法的）以及强用户身份验证。

当考虑到上述所有因素时，此项调查的绝大多数受访者都选择提高整体数据安全性和确保计算机安全，并将之作为最重要的 IT 优先事项，如图 1 所示。

值得注意的是，在下图中，第三重要的 IT 主题是通过更好的设备提高员工的生产力。当我们要求受访者选出他们认为最重要的三个主题时，选择“更好的设备”选项的人数最多。这让 IT 记住了一个关键信息：安全固然重要，但不能以牺牲员工的生产力为代价，最好的设备能将出色的安全性和最终用户满意度结合起来，让用户不会受到安全问题的影响。

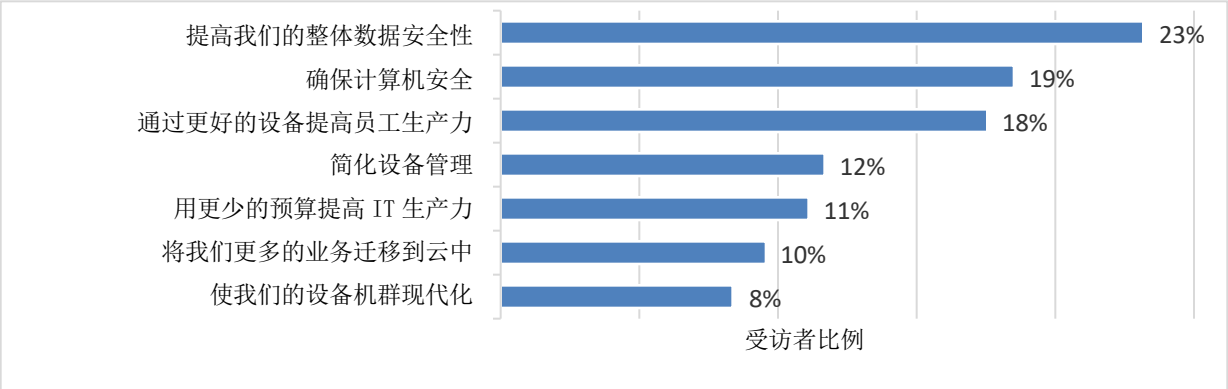
当我们问 IT 决策者在选择下一个计算机供应商时的首要决定因素是什么时，安全性排在第一位，超过了性能、对现有应用程序的支持以及与现有 IT 基础架构的集成。最值得注意的是，规格选项的排名几乎倒数。

如需了解最重要的 IT 优先事项，请参见图 1。如需了解选择计算机供应商时的首要考虑因素，请参见图 2。

图 1

IT 的重中之重：数据和终端安全

问：以下哪些 IT 主题是贵公司当前的重中之重？



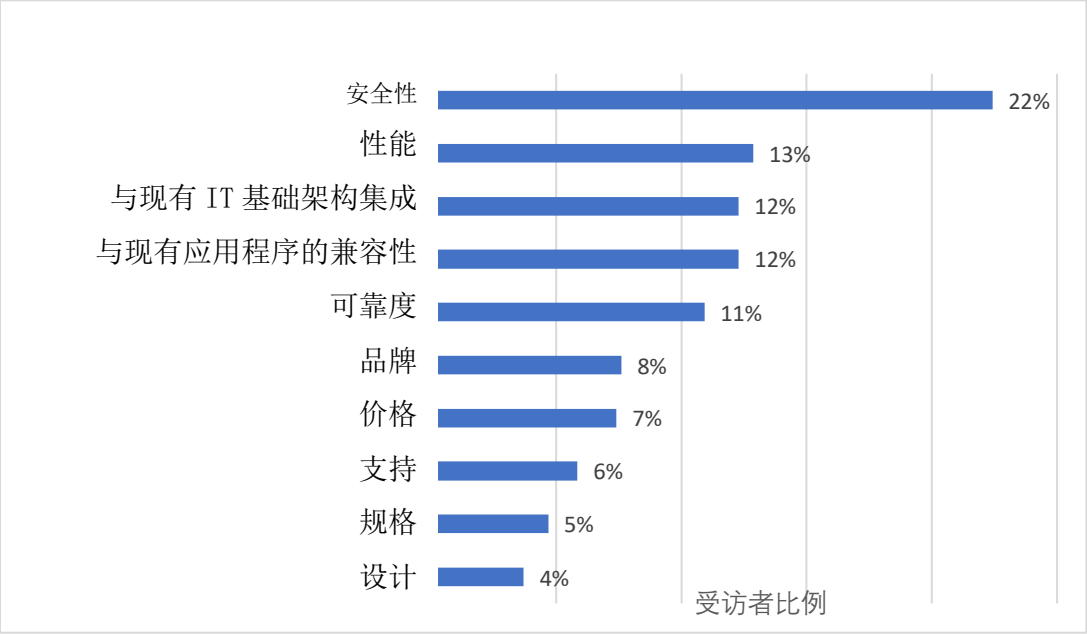
来源：IDC 安全终端调查，n=513

注：数据包括被评为最重要的主题（排名第 1）

图 2

选择计算机供应商时的首要因素

问：在为自己的公司选择电脑时，最重要的决定因素是什么？



来源：IDC 安全终端调查，n=513

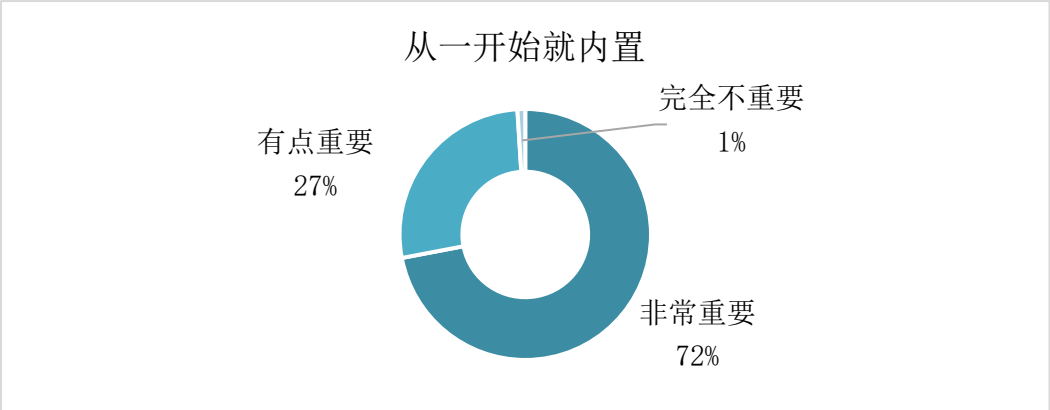
注：数据包括被评为最重要的因素（排名第 1）

“内置安全功能”和“集成数据保护”这两个概念在受访者中引起了强烈共鸣。当被问及“从一开始就在计算机（包括芯片、固件和操作系统）中内置安全功能，以保护计算机免受当前和未来威胁的影响，您认为这有多重要？”绝大多数人的回答是积极的，72%的人认为非常重要，27%的人认为有点重要。只有 1%的人认为这根本不重要。在深入研究这些数据后，值得指出的是，在医疗保健和金融组织的 IT 决策者中，认为它非常重要的比例甚至更高（分别为 84%和 75%）。集成数据保护这一概念的得分同样很高。我们的问题是“您认为将数据加密功能集成到计算机硬件中有多重要？”71%的人认为非常重要，29%的人认为有点重要，0%的人认为不重要。 如需了解内置安全功能和集成数据加密的详细信息，请参见图 3。

图 3

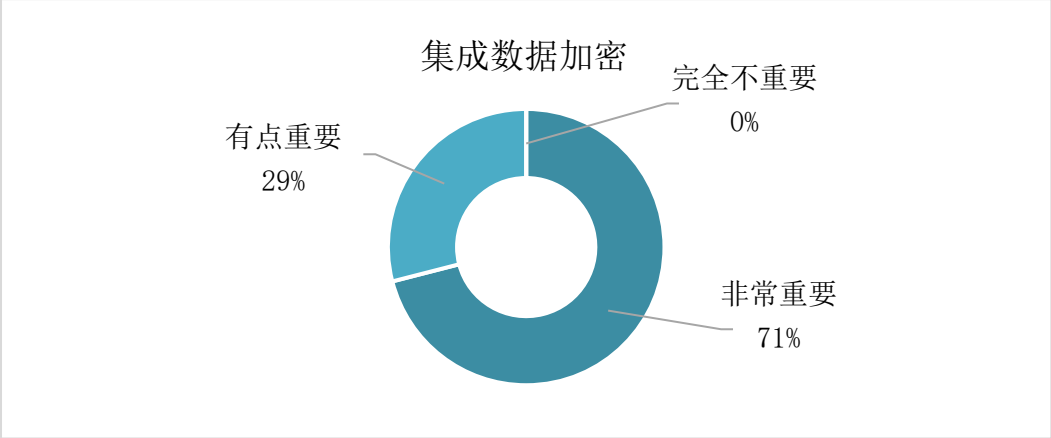
内置安全功能和集成数据加密的重要性

问：从一开始就在计算机（包括芯片、固件和操作系统）中内置安全功能，以保护计算机免受当前和未来威胁的影响，您认为这有多重要？



来源：IDC 安全终端调查，n=513

问：您认为将数据加密功能集成到计算机硬件中有多重要？



来源：IDC 安全终端调查，n=513

虽然从一开始就内置安全功能的硬件非常重要，但集成数据加密也是一项关键要求；因为安全专家都知道，任何安全链中最薄弱的环节通常是用户自己。这就是用户身份验证如此重要的原因，也是技术供应商努力发展身份验证技术的原因。遗憾的是，我们的调查显示，许多企业在这一领域的工作滞后。

从积极的方面来看，我们的调查显示，68%的受访者表示他们的公司要求使用复杂的密码，63%的受访者表示他们使用双因素身份验证。在不太积极的方面，只有 23%的受访者使用单点登录技术（SSO），只有 20%的受访者使用生物识别安全技术（如指纹或面部识别）。值得注意的是，在我们的受访者中，有 56%的人认为生物识别身份验证比密码安全得多，35%的人认为生物识别身份验证比密码更安全一点，9%的人认为生物识别身份验证与密码同样安全，没有人（0%）认为生物识别身份验证比密码不安全。

最近推出的一种重要的新身份验证技术是通行密钥。通行密钥是一种数字凭据，利用密钥对来提供比密码更安全的解决方案。由于这项技术尚属新生事物，只有 14%的受访者表示自己的公司使用了这项技术，但明智的 IT 决策者如今应该密切关注这项技术。如需了解用户身份验证使用情况的详细信息，请参见图 4。

图 4

用户身份验证方法

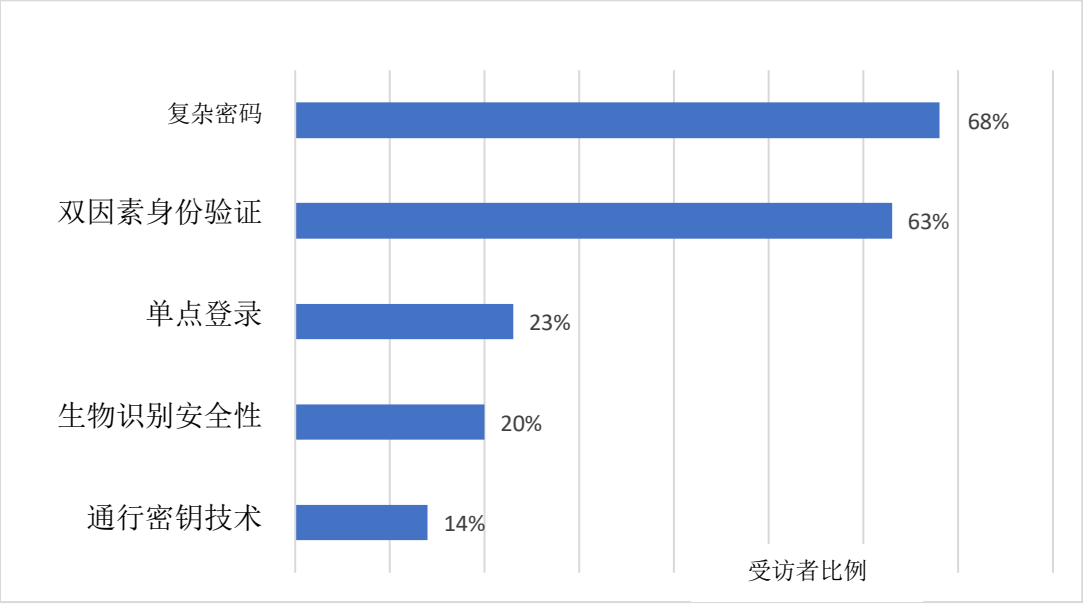
问题 1：贵公司是否要求员工使用复杂密码登录计算机？

问题 2：贵公司是否部署了支持指纹扫描等生物识别安全措施的计算机？

问题 3：贵公司是否已开始研究使用通行密钥技术的好处？

问题 4：贵公司是否要求使用双因素身份验证？

问题 5：贵公司是否利用了单点登录（SSO）功能？（是/否）



来源：IDC 安全终端调查，n=513

数据显示的是回答“是”的百分比。

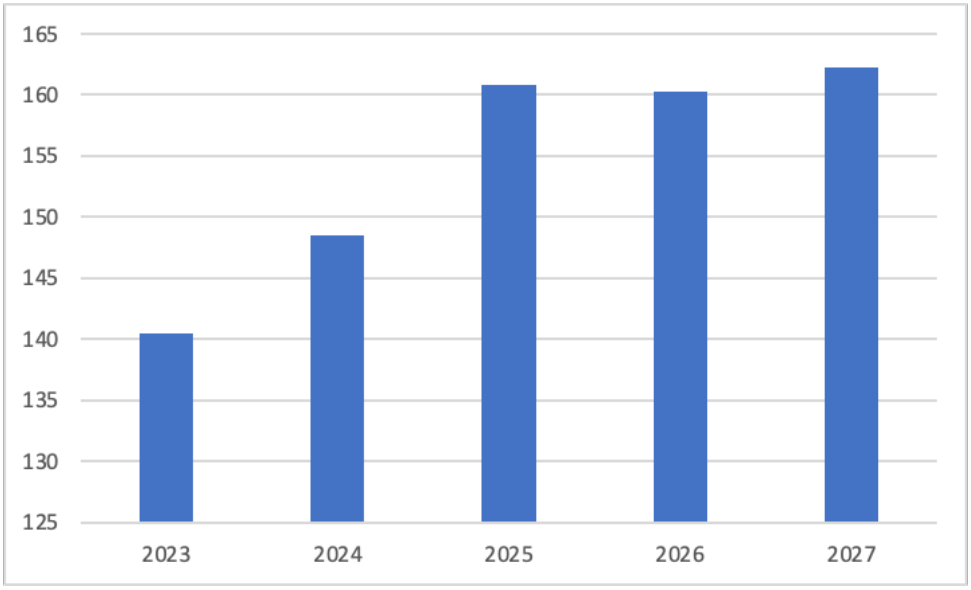
有相当高比例的受访者甚至没有实施复杂密码（32%）或双因素身份验证（37%）等基本身份验证协议，令人震惊。**值得借鉴的最佳实践**是确保贵公司在整个公司范围内实施统一的身份验证形式。在确定了这个基线之后，再开始考虑将 SSO 功能与强大的主身份验证协议结合起来。最后，在完成下一次硬

件更新换代时，深入了解能够支持最高级别身份验证的计算机：生物识别安全和通行密钥技术。 启用生物识别技术和通行密钥意味着未来员工可以快速、安全地登录计算机，并从计算机立即登录应用程序和网站。

我们将在本节最后面讨论最后一点，即您的下一次硬件更新换代。许多公司安装的计算机已经老化，需要更换。即使贵公司在 2020 年之前就购买了相当大比例的新终端，这些计算机也将很快接近四年大关。在此期间，硬件安全不断发展以应对现实中的威胁。此外，这些产品大多是在向远程和混合工作方式广泛转变之前出厂的，这意味着许多产品缺乏高质量的摄像头、麦克风和扬声器，而这些都是员工使用当今关键的网络会议和协作应用程序所必需的。在经历了数年出货量放缓之后，IDC 的“个人计算设备跟踪报告”预测该类别产品在未来几年将出现增长。注：商用单位指非消费者实体购买的单位。如需了解 IDC 的消费/商用计算机预测，请参见图 5。

图 5

全球商用计算机预测



来源：IDC PCD 跟踪报告，2023 年 8 月

企业应不断重新评估员工的计算机需求，只有这样才能保持市场竞争力，吸引并留住顶尖人才。过去，IT 部门必须在安全性和员工满意度之间做出重大权衡取舍，而如今，合适的供应商可以帮助找到无需妥协的解决方案。最后，**另一个值得考虑的最佳实践**是在下一次硬件部署中采用零信任访问原则。这种策略假设，每当有设备试图访问公司资源时，在通过验证之前都不应该加以信任。零信任采用各种技术和流程来证明设备（最好是从芯片到关键 IT 和安全应用程序）、所连接的网络（例如，公共 Wi-Fi 与专用网络）的安全状态和用户身份。

考虑在企业中使用 Mac

如今，越来越多的 IT 部门开始支持 Mac，我们的调查指出了其中的关键原因之一。在我们的受访者中，有 76%的人认为 Mac 比其他计算机更安全。而在未来 12 个月内，采用更多 Mac 的首要原因是受访者认为 Mac 更安全（47%），紧随其后的是易于部署和管理（36%）。

苹果客户聚焦

“苹果产品的一个真正重要的特点是，隐私和安全实际上已经嵌入了产品本身，这不是马后炮，这也是我们非常欣赏的一点。" — Linda Jojo，美国联合航空公司执行副总裁兼首席客户官

苹果公司致力于提供出色的用户体验，同时通过软件将安全性嵌入苹果芯片，从而增强了安全性。苹果公司的触控 ID 就是一个例子，这是一种内置的生物识别安全功能。苹果芯片具有 Secure Enclave 功能，可对用于保护触控 ID 数据的密码进行加密和保护。

为了解决操作系统和引导序列被破坏的风险，MAC 配备了安全引导和签名系统卷。安全引导确保在启动时只启动经过加密认证的 macOS 版本，而签名系统卷可在运行时保护操作系统的完整性。过时的软件还会带来网络风险，苹果公司可以自动执行软件更新的端到端分发和安装并加以保护，从而最大限度地降低这种风险。

优秀的第三方软件有助于提高员工生产力，但这些软件也绝不能包含恶意软件。苹果公司采用多层次的方法来防止恶意软件。苹果的 Mac 应用程序商店会扫描每个应用程序以检测是否存在恶意软件。由于 MAC 上的软件也可以从网上下载，苹果要求开发者将其应用程序提交给苹果公司的公证服务，该服务也可以扫描检测是否存在恶意软件。MacOS 中包含的苹果 Gatekeeper 会检查是否经过公证，并阻止未签名的应用程序运行。此外，苹果公司的反恶意软件工具 XProtect 可以阻止和删除任何已知的恶意软件。

数据是企业价值最高的资产之一，必须得到相应的保护。在 Apple 服务（如 iMessage 和 iCloud）中，芯片强制 FileVault 加密、苹果公司支持的 VPN 协议和端到端加密相结合，确保数据在静态、传输和使用过程中都受到保护。

随着社会工程成为威胁行为者的熟练技能之一，最终用户必须提高警惕。这是一项艰巨的责任，但苹果公司通过 Safari 欺诈网站警告来协助履行这一责任。此外，由于身份验证凭据经常被威胁分子窃取，苹果公司的通行密钥支持简化了企业实现身份验证方法现代化的途径，同时又不会牺牲积极的最终用户体验。

良好的安全性与可靠的设备管理密切相关。为此，苹果公司提供了一系列设备管理功能，包括内置的移动设备管理 (MDM) 管理框架。Apple Business Manager 实现了零接触部署并链接到 MDM 解决方案，而适用于 Mac 的端点安全 API 可让开发人员构建解决方案来监控、分析和响应安全威胁。苹果公司还提供了与内置 SSO 框架的身份集成，该框架可与现代身份提供商（IdP）协同工作。

最后，苹果公司在 macOS 中提供了这些安全功能，包括主要和次要软件更新，企业或消费者无需支付额外费用。

挑战/机遇

尽管威胁环境不断演进，但 IT 部门仍要秉承少花钱多办事的主旨：用更少的资金、更少的 IT 人员和更少的资源应对更复杂的威胁环境。除了应对每家企业都面临的日常安全风险，许多 IT 组织还肩负着通过部署硬件、软件和服务来显著提高员工生产力和满意度这一任务。要成功完成这两项任务——提高安全性，以及提升员工生产力及满意度——看似很难。但这也为 IT 部门带来了重要机遇。即有机会重新评估所购买的硬件、软件和服务、供应商，以及为越来越多的混合型员工部署这些硬件、软件和服务的方式。此外，现在显然应该重新计算总拥有成本（TCO）模型，以更好地反映企业购买和使用技术的现状。

结论

安全性现在和将来都是 IT 部门最关心的问题。在 IT 预算紧张、重大硬件更新换代迫在眉睫之际，有必要重新评估未来的供应商。考虑实施有关身份验证和零接触部署的最佳实践，并采购可实现这些转变的硬件。如果有供应商提供具有内置安全功能和数据加密功能的计算机，您可以借此既实现安全性又提供积极的最终用户体验，就不必再为安全性而牺牲生产力和员工满意度。

关于 IDC

国际数据公司（IDC）是全球著名的信息技术、电信和消费科技咨询、顾问和会展服务专业提供商。IDC 旨在帮助 IT 专业人士、业务主管和投资机构制定以事实为基础的技术外包决策和业务发展战略。IDC 在全球拥有超过 1100 名分析师，他们具有全球化、区域性和本地化的专业视角，对 110 多个国家的技术发展趋势和业务营销机会进行深入分析。在 IDC 超过 50 年的发展历史中，众多企业客户借助 IDC 的战略分析而达致关键业务目标。IDC 是 IDG 旗下子公司，IDG 是全球领先的媒体出版、研究及会展服务公司。

全球总部

140 Kendrick Street
Building B
Needham, MA 02494
美国
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com