

部署全盘加密解决方案以确保企业数据安全

英特尔的成功建立在我们的知识产权基础之上，信息是我们公司的基石，没有人能够承担得起任何信息管理方面的失误。

— Diane Bryant
首席信息官

Rex Rountree
英特尔 IT 部门，加密服务经理

Carol Kasten
电子发现和调查
英特尔 IT 部门，团队经理

Michael Amirfathi
英特尔 IT 部门，工程设计信息保护与
加密服务经理

执行概述

为保护英特尔公司的知识产权以及员工的个人信息，英特尔 IT 部门于 2009 年开始在所有向员工提供的公司笔记本电脑上部署全盘加密解决方案。借助此方法，整个磁盘驱动器可得到加密，其中包括数据、应用、操作系统以及可用空间，因此即使系统丢失或被盗，不怀好意的人也无法访问数据。在 12 个月之内，我们已对 75% 以上的所有符合条件的公司笔记本电脑安装了全盘加密解决方案。

我们实施了分阶段计划，以确保顺利部署加密程序。为了尽量减少工作中断，我们在 2009 年初开始“拉动式 (pull)”部署，员工可在方便的时候安装软件。一旦达到第一阶段的目标（即员工在 70% 的公司笔记本电脑上安装加密系统），我们将采取“推动式 (push)”部署方式，以便对所有余下的笔记本电脑实施安装。

我们实施了许多战略来管理我们的部署，其中包括：

- 在部署之前，针对运营和服务台员工进行培训，并建立资源以及管理基础设施。
- 开发自动化客户端安装包，使安装过程尽可能简单化。
- 定期安排会议，以确保公司高层和集团管理层随时了解情况，同时快速制定相关决策以解决部署过程中出现的问题。

- 借助加密笔记本电脑数量以及服务台呼叫数量方面的指标来跟踪进度，从而把握好采用率，规划目标以及支持服务负担之间的平衡。
- 通过面向终端用户的培训和资源，以及来自高管人员的目标电子邮件，推广加密系统的采用。

这些以及其它战略可帮助我们在满足具有挑战性的部署规划需求，以及尽可能减少对员工效率的影响之间实现平衡，并且通过解决与加密部署有关的问题，使我们的支持服务资源不至于负担过重。我们预计，通过最后的推动式部署阶段，我们将在 2010 年中旬实现对余下笔记本电脑部署全盘加密程序的目标。

目录

执行概述	1
背景	2
解决方案	2
规划部署	2
分阶段部署	4
跟踪进度	4
推广加密技术的采用	5
实施新的支持流程	6
应对部署挑战	7
结果	7
未来计划	7
总结	8
了解更多信息	8
缩写词	8

IT@INTEL

IT@Intel 致力于促进 IT 专业人员、管理人员和高管与英特尔 IT 部门同仁以及数千名其他 IT 业界精英进行紧密交流，帮助您深入了解可有效应对当前严峻 IT 挑战的工具、方法、战略和最佳实践。如欲了解更多信息，请访问：www.intel.com/IT 或联系当地英特尔代表。

背景

最近几年的行业趋势表明，企业面临的安全攻击形势日趋严峻，攻击目标更具针对性，组织更加严密，且会造成严重的经济损失。一份英特尔 IT 部门内部风险分析报告显示，一个主要的安全漏洞可能会给英特尔公司造成 500 万美元或更多的直接经济损失。

为应对这种日益增长的威胁以及因数据丢失或被盗而导致的成本问题，在 2008 年底，英特尔 IT 部门决定对所有员工的笔记本电脑部署全盘加密解决方案。借助全盘加密技术，整个磁盘驱动器可得到加密，其中包括数据、应用、操作系统以及可用空间，因此即使系统丢失或被盗，不怀好意的人也无法访问数据。如果得到正确的实施，全盘加密技术将会提供一个强有力、自动化的安全解决方案，且无需依赖员工的积极参与。全盘加密基于一种成熟的技术，可在所有笔记本电脑上实施，它提供了一个安全基础层，而且能够与其它技术进行集成。

我们在规划过程中发现，实施全盘加密将带来相当大的风险，因为其涉及到英特尔公司 80% 使用笔记本电脑的员工。为降低这一风险，我们对部署战略进行了仔细规划。我们确定了表 1 所列的要求，在实施前对产品和供应商进行广泛的评估，提供相关的培训并建立资源和管理基础设施。¹

在产品评估流程中，我们通过分析报告和第三方评估来研究加密产品，在实验室对产品进行测试，并且从实施过大规模加密

¹ 有关此流程的详细描述，请参阅“借助笔记本电脑加密增强企业安全性（Strengthening Enterprise Security through Notebook Encryption），”英特尔公司，2008 年 12 月。

部署的其它企业汲取经验和教训。评估和访谈流程不仅可以帮助我们做出决定，同时还使我们了解到产品在部署时的实际缺陷以及最佳方法（BKMs），这对我们的部署规划产生了一定的影响。表 2 显示了访问同行公司后所得到的调查结果。

解决方案

通过精心规划和准备，我们在 2009 年初开始部署加密解决方案，并设定了在一年之内对所有符合条件的笔记本电脑进行加密的具有挑战性的目标。在这一时间段内，我们要尽可能减少员工工作中断的情况，并降低对运营和服务台工作人员的影响。

规划部署

为确保安装流程的顺利实施，我们首先对运营和服务台工作人员进行培训，并建立资源和管理基础设施。我们同时对终端用户创建了有针对性的通信、资源以及培训材料。

运营

我们针对初期部署和后期的更新、笔记本电脑恢复、电子发现、监控以及审计建立了运营团队。恢复和电子发现是特别重要的流程，因为它们必须要符合法律和公司的相关要求，同时还要保护最终用户的隐私。英特尔在处理这些流程方面已经具备一套全面的授权框架，该框架经扩展已涵盖笔记本电脑加密问题。例如，如果一位员工已不在英特尔公司工作，使用一台笔记本电脑需获得相关法律、业务和技术经理的授权。

表 1. 英特尔 IT 部门针对全盘加密部署的要求

要求	说明
安全互操作性	我们的解决方案必须与英特尔现有的笔记本电脑安全解决方案保持一致并能够彼此互操作。此外，它还需要提供笔记本电脑的安全密钥存储并支持多重身份验证功能。最后，为确保解决方案符合法律和法规要求，该解决方案必须采用标准认证，如联邦信息处理标准（FIPS）和美国国家标准与技术研究院（NIST）。
企业可管理性	为确保高效管理，该解决方案必须与现有的管理工具和流程保持一致，其中包括与英特尔® 博锐™ 技术的互操作性。
尽可能降低对笔记本电脑用户的影响	为尽可能减少工作中断、培训时间以及服务台需求，该解决方案针对笔记本电脑用户进行简化，同时对笔记本电脑性能的影响也需降至最低。我们不希望妨碍员工的工作流程或使工作效率降低。
顺利部署	该解决方案必须使用英特尔 IT 部门现有的笔记本电脑管理基础设施实现自动部署。同时，它还需要提供相应的工具来检测和解决部署问题，以避免针对安装问题提供成本高昂的手动支持。
操作系统兼容性	该解决方案必须与英特尔笔记本电脑环境中的所有操作系统和操作系统版本相兼容。
笔记本电脑资格要求	只有采用英特尔® 酷睿™2 双核处理器或更高级别的笔记本电脑才有资格安装加密程序。我们之所以做出这样的决定，是因为发现在对采用旧处理器的笔记本电脑进行加密时，系统性能将会严重下降。

表 2. 来自同行公司的信息反馈

要求	具体需求
数据丢失	我们的受访者称，在他们部署期间并无数据丢失，尽管在极个别情况下，需要使用供应商工具来恢复笔记本电脑数据。
磁盘错误扫描	企业认为在部署前有必要在笔记本电脑上运行磁盘错误扫描和磁盘碎片整理实用程序。那些没有运行上述程序的企业经历了 1% 或 2% 的故障率。过去，在加密过程中击中硬盘内的一个坏扇区会造成系统崩溃。现在，当发现坏扇区时，领先的解决方案会自动停止安装。接下来这些系统会执行磁盘错误扫描，然后重试安装。
部署时间表	部署时间表存在较大的差异，少至 18 个月内 6,000 台笔记本电脑，多则 3 个月内 15,000 台。然而，更多时候部署时间乃取决于公司及内部 IT 问题，而不是所选的加密产品。
服务台与服务支持呼叫数量	在部署初期，所有企业均经历了服务台与服务支持呼叫数量的增长，但在几周之后便恢复到正常水平。
恢复与电子发现	恢复和电子发现工具与流程并未发现。

服务台

我们为支持人员提供培训材料和脚本，以帮助员工下载、安装、配置软件，以及处理后续问题。根据我们的研究，我们预计用户主要在创建和重置密码这两个方面需要帮助。启动加密程序需要这些密码，并使用多词且容易记忆的短语（例如一个句子）进行设置，而且单词之间需要空格。我们决定使用密码而非单点登录（SSO）的方式进行身份验证，因为更长、更复杂的密码可提供更高的安全性。

最终用户

在部署之前，我们通过电子邮件向所有笔记本电脑用户公布了员工沟通结果。这些沟通结果阐述了用户对加密的需求，以及在部署和使用相关技术方面的期望。特别是，用户需要了解新密码的要求，并做好磁盘加密过程中出现部分性能下降的准备。电子邮件沟通结果还解释说，安装全盘加密系统后，在正常使用该系统的情况下，他们并未发现任何性能延迟。然而，他们发现在启动、关闭以及休眠切换状态时，可能会发现轻微的性能延迟。此外他们还预计，采用固态硬盘（SSD）的笔记本电脑安装完该系统后，性能延迟现象更

为明显，这是因为其速度比传统硬盘更快。如欲了解更多有关性能延迟以及我们如何解决的信息，请见“固态硬盘介绍”部分。我们同时告知员工，具有更快处理速度的新笔记本电脑在安装完加密程序后，其性能延迟几乎可以忽略。

为了使安装过程尽可能简单，我们在员工内联网的一个网址上提供了自动化客户端安装包。该网址包含了可下载的加密程序以及培训材料，例如高级安装说明、系统资格条件要求、提升员工安全意识的材料、高层管理人员强调公司范围内加密重要性的视频以及常见问题（FAQ）。

分阶段部署

为了尽量降低对笔记本电脑用户工作效率的影响，我们实施了“拉动式”部署方式，员工可根据其工作日程，选择合适的时间来安装加密程序并对硬盘实施加密。员工可在方便的时候从我们的下载站点下载、安装并配置该程序。当 70% 的笔记本电脑用户下载加密程序后，我们开始向余下未加密的笔记本电脑实施“推动式”部署方式，以便强制执行硬盘加密。

我们通过一系列小规模部署对解决方案和流程进行了全面测试。我们针对各种情况记录相关的技术和运营问题，开发了相应的修正方案。我们还对部署与规划流程进行协调，从而根据实际应用结果来改良基础设施和培训课程。

我们定义了四个部署阶段，如图 1 所示：

- **小规模评估** 针对大约 20 位最终用户进行部署，加密团队的全部同事。
- **概念验证** 针对更大规模的测试组进行部署（由来自不同工程和客户支持团队的

100 名最终用户组成）。这些员工比普通用户更精通电脑，并且在解决问题方面较为积极主动。

- **全面部署试点** 针对来自各个部门的 1000 名最终用户进行部署，从而模拟全面部署。该测试组可确保我们为所有用户提供有效的支持，并帮助我们找寻哪些可能会在企业范围部署中出现的问题。
- **普遍部署** 针对所有余下的员工笔记本电脑实施加密部署。当 70% 的笔记本电脑完成加密后，我们将从拉动部署阶段过渡到推动部署阶段。我们目前正处于普遍部署阶段，公司超过 75% 的笔记本电脑已经完成加密。

跟踪进度

在整个部署阶段，我们定期举行会议，以确保管理层随时掌握情况，帮助我们迅速做出决策。这些会议帮助我们：

- 审查项目的进展情况，讨论工程设计方面的挑战和部署问题，使我们尽可能实施高效管理。

- 对我们部署的业务影响方面尽作了解并以高效的方式及时做出应对。
- 向高层管理通报项目进度，并审查问题以及相关的解决方案。

我们最初制定目标是在一年内实现全面部署。我们需要在规划目标与尽可能减少对支持服务和员工工作效率的影响之间寻求平衡。我们制定并跟踪部署标准以监控项目进展情况，从而帮助我们在部署期间调整战略：

- **整体部署进度** 我们与公司高层和集团管理部门共同制定内部部署目标。我们利用这些目标来确定如何监控部署，并衡量如何安排跟踪。跟踪对于决定何时从拉动部署转为推动部署起着重要的作用。
- **服务台呼叫数量** 我们跟踪与加密有关的呼叫的数量及相应的原因。如果呼叫数量超出了我们的限值，我们将减少向员工发送的鼓励其部署加密程序的电子邮件，从而放慢实施步伐。

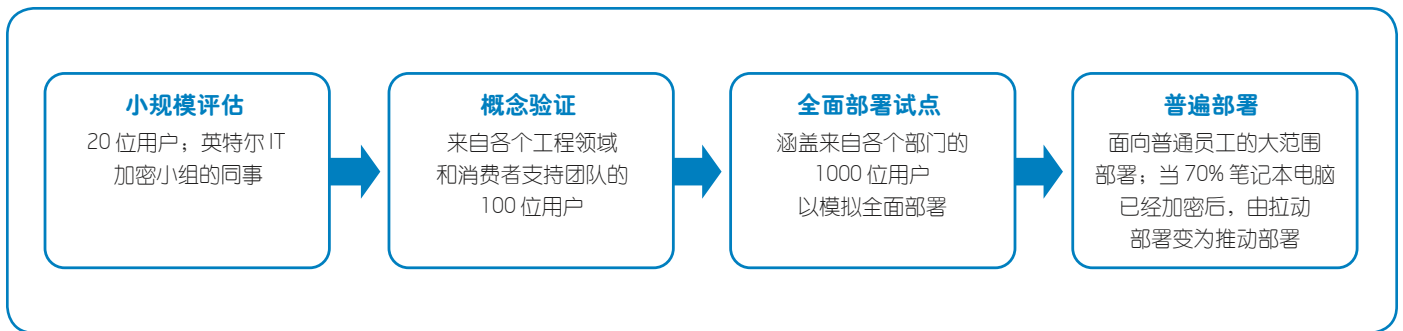


图 1. 英特尔 IT 部门分四个阶段实施全盘加密部署，以便在普遍部署之前对解决方案进行全面测试。

推广加密技术的采用

我们的目标是降低对员工工作效率的影响，因此在最初的“拉动式”部署阶段，员工可自行安排进行安装。然而，这一决定同时也使进度变得较为缓慢。当员工通过同事、英特尔 IT 宣传和培训材料了解到安装时间要求和其它事宜后，纷纷推迟了安装时间。

当员工连接到公司网络时，我们的安装说明会鼓励他们注册并下载加密程序，该过程用时 10 分钟。至于启动加密流程因为取决于硬盘的大小和速度，可能需时 2 至 4 小时，员工可在晚上或者周末不使用笔记本电脑时启动加密流程。

为了提高安装速度，我们会尽快处理出现的问题，改进安装说明以帮助员工避免常见的问题，同时通过相关的宣传材料鼓励员工积极采用这一技术：

- 我们在服务台中心放置了海报来描述加密的重要性，每个来维修笔记本电脑的人均可看到这些海报。
- 英特尔公司的首席执行官和首席信息官通过电子邮件，向员工解释加密的重要性，并鼓励他们安装加密程序。在首席执行官发送电子邮件后，我们看到安装加密程序的人数增加了 8 倍，如图 2 所示。获得高层管理人员的支持对我们加密程序的成功部署至关重要。

- 在早期部署阶段，我们首先部署包含最敏感数据的高风险笔记本电脑，例如人力资源部数据。我们针对风险最高的群体指定电子邮件活动并优先对其电脑进行更新，以确保这些群体能够更快速地完成安装。
- 我们将电子邮件宣传活动与服务台接到的有关加密问题的呼叫数量进行绑定。当呼叫数量低于预先定义的阈值，我们将会增加电子邮件宣传活动的次数和频率，从而鼓励更多的员工安装加密程序。当服务台和服务支持呼叫数量超过了预先确定的阈值时，我们便会放缓电子邮件宣传活动。

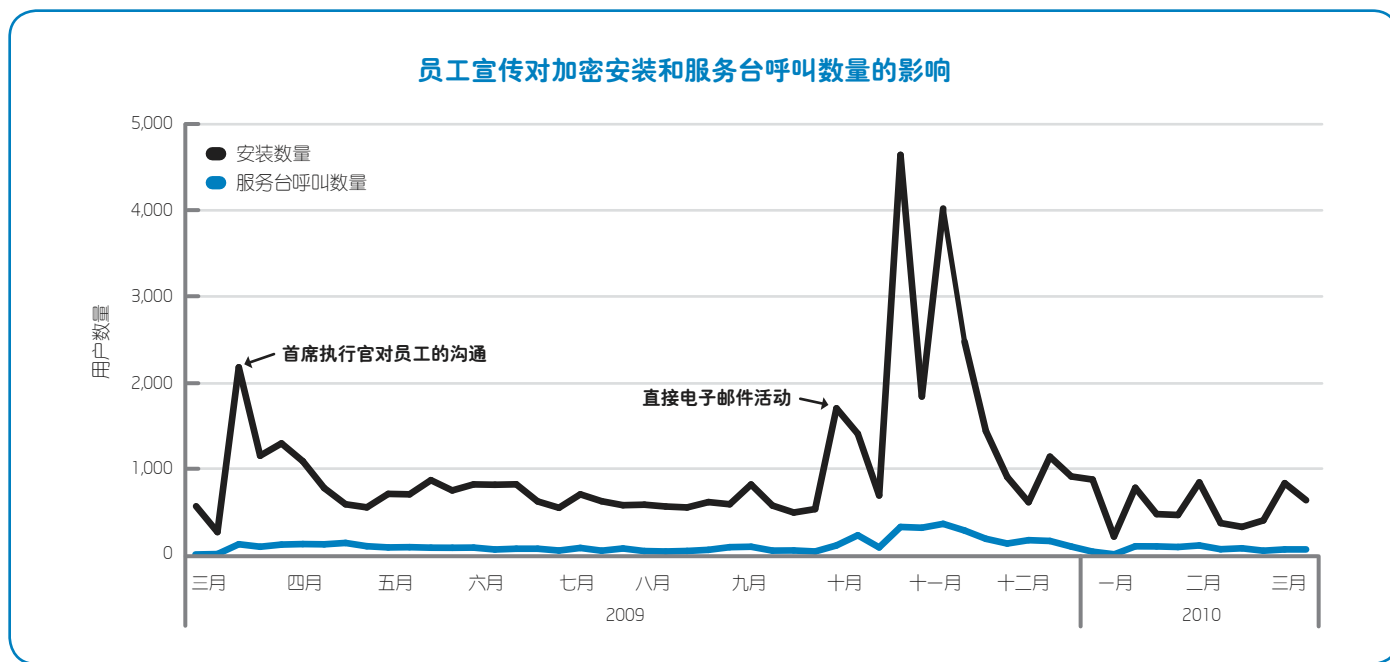


图 2. 英特尔高层人员电子邮件沟通与英特尔 IT 部门针对员工的电子邮件活动增加了加密程序的安装数量与服务呼叫数量。如果呼叫数量超出了限值，我们将通过减少这些宣传来放慢部署步伐。

通过增强管理提高安全性

仅凭数据加密不能确保员工笔记本电脑的数据安全。同时需要高效的客户端管理来确保配置具备较高的安全性。为了帮助我们更有效地管理员工的笔记本电脑（和台式机），同时显著削减成本，英特尔 IT 部门目前正在实施一项为期多年的计划，旨在升级我们的客户端系统和支持基础设施，进而充分利用英特尔®博锐™技术。到 2009 年底，我们已为 5 万台个人电脑配置了英特尔®博锐™技术。

采用英特尔®博锐™技术的客户端系统包括内建、基于硬件的动能，有助于提高安全性、可维护性和资产跟踪能力。即使当系统关闭、操作系统无响应、软件代理被禁用或者硬盘出现故障时，具有授权的管理应用和支持人员可以通过有线和无线网络访问这些个人电脑。

我们针对英特尔®博锐™技术在提高工作效率和减少支持成本这两个方面开发了几个使用案例场景。其中一个包括帮助最终用户远程重置密码。服务台可控制个人电脑并在几分钟内远程输入密码恢复令牌。密码恢复令牌是一个由 26 至 32 个字符组成的字母和数字字符串；远程输入该字符串能够节省时间并减少因服务台工作人员与用户之间的沟通不当而造成的错误。如欲了解更多与英特尔®博锐™技术远程管理功能相关的案例信息，请观看：<http://communities.intel.com/docs/DOC-4165> 中的视频——“有关英特尔®博锐™技术的三个使用案例”。

实施新的支持流程

我们的早期试验部署证实，针对加密部署的服务台主要问题是向笔记本电脑用户提供创建新密码的指导。员工以往在使用其笔记本电脑之前需要输入两个密码：启动系统的硬盘认证密码以及操作系统登录密码。当员工的硬盘完全加密后，我们便不再使用硬盘认证密码，取而代之的是一个笔记本电脑加密密码。

然而，在部署新的加密解决方案时，我们认为增加密码长度和强度需求非常重要。尽管员工可继续使用他们现有的操作系统登录密码，但每个人必须为加密解决方案创建一个新的密码以满足新的需求。

大多数员工对密码的概念都感到困惑，该密码使用多词、便于记忆的短语（例如一个句子）进行设置，并且单词之间需要空格。多数员工常常忘记他们输入的较长的、复杂的字符串（像是一个没

有空格的冗长密码），因此需要呼叫服务台。

为了减少这种困惑，我们改进了加密程序的安装说明，阐明了安装步骤并消除了对于如何设置强密码的误解。我们通过电子邮件和英特尔的员工内部门户网站提供指导，并协助服务台员工处理密码问题。我们还培训服务台工作人员使用供应商工具，以便远程重置加密密码。最后，已经安装加密系统的员工开始向其同事传授如何设置便于记忆、安全的密码。

减少与忘记密码相关的恢复故障

当员工因忘记密码而呼叫服务台时，服务台员工将会给他们一个仅限一次使用的临时性恢复令牌。使用该临时令牌可让员工跳过验证登录系统，但部分员工在退出系统之前可能会忘记更改他们的密码。

这将导致系统重建，并从备份执行数据恢复。在最初发现该问题后，我们修改了支持流程，以确保我们的服务台工作人员不仅能够帮助员工借助恢复令牌登录笔记本电脑，同时能够帮助他们立即重置密码。服务台员工通过电话向用户解释该流程，用时大约 15-20 分钟。如果笔记本电脑启用了英特尔®博锐™技术，服务支持工作人员可在 3-5 分钟之内远程执行相同的流程。（参阅侧边栏“通过改进管理增强安全性。”）

针对电子发现访问硬盘

如果员工从英特尔分离出来，服务台工作人员需访问笔记本电脑的数据来协助电子发现。我们建立了一个流程，即通过适当的授权，服务台工作人员能够帮助电子发现员工使用临时恢复令牌重新登录，然后帮助他们立即重置密码以便访问笔记本电脑上的数据。

应对部署挑战

我们在整个部署过程中克服了无数的挑战。

企业数据备份

我们在部署前与其他公司进行了讨论，确认了需要部署企业范围的备份流程以实现数据恢复。由于加密流程涉及到硬盘的每一个扇区，如果硬盘在加密过程中触击到一个坏扇区，系统可能会崩溃，甚至导致数据永久丢失。

作为一项预防措施，我们要求员工在安装加密程序之前对硬盘进行备份。我们发现部分英特尔位置还不具备备份所有系统的能力。因此在这些位置解决该问题之前，我们暂停了这些区域的加密部署。然而，在部署加密程序之前进行备份还可带来一种优势。现在英特尔的大部分员工都能够对其数据进行备份。

更新资产库存

为通知员工安装加密程序，我们需要一份包括所有笔记本电脑及其使用人的完整列表。然而，我们发现资产库存系统中的信息已经过期。因而我们更新了该系统以便提供更加准确的信息。

新旧笔记本电脑区分

我们发现在给旧笔记本电脑安装加密程序时会出现严重的性能延迟问题。为了解决该问题，我们决定仅对采用英特尔® 酷睿™2 双核处理器或更新处理器的笔记

本电脑实施加密。在我们 2-4 年的电脑定期更新周期内，我们为所有新的笔记本电脑配备了加密系统。

识别配置不兼容性

英特尔公司大约有 10% 的笔记本电脑用于满足专门的业务需求，因此配置比较独特，与我们的标准版本有所偏差。这些配置在部署期间需要定制的修补程序。在要求用户进行加密部署之前，我们需要一种能够便捷地识别这些独特配置的方法，以避免出现安装问题以及工作效率下降。

我们开发了一种应用程序，可帮助确定独特和标准平台版本之间的不同，因此在安装期间，我们可为这些员工提供操作步骤以处理他们的独特配置。如果一台笔记本电脑存在不兼容程序或安装了其它加密程序，我们会在员工安装新的加密程序之前告知他们怎样删除之前的程序。对于具有多版本和其它系统变量的笔记本电脑，例如多引导系统、多个分区或者多个虚拟环境，我们将告知员工如何在安装期间管理这些变量。

固态硬盘介绍

评估显示，使用英特尔® 固态硬盘 (SSD) 的益处包括减少 IT 支持成本和提高用户工作效率 — 我们开始采用固态硬盘作为标准 IT 版本的一部分来部署笔记本电脑。我们在加密部署中期阶段做出这一决定。鉴于固态硬盘的数据访问率比普通硬盘更快，因此在实施加密后，我们

最初看到的固态硬盘性能下降百分比要高于普通硬盘。

为了解决这一问题，我们与供应商合作以帮助重新设计适用于固态硬盘的加密程序。供应商提高了代码性能，提供了 256 位或 128 位两种加密部署选择，并利用了采用英特尔® 酷睿™ i5 处理器的最新笔记本电脑中的英特尔® 双核技术和英特尔® 超线程技术。该加密程序经重新设计后性能提高了两倍。

结果

迄今为止，英特尔公司已有超过 75% 的符合条件的笔记本电脑实施了加密解决方案，推动部署工作有条不紊地进行。我们延长了加密程序部署规划的时间，从最初估计的 1 年延长至 18 个月。这将帮助我们为英特尔的最终用户提供更好的支持，同事确保支持人员不会负担过重。我们预计公司所有余下的笔记本电脑将会在 2010 年中旬完成加密部署。

未来计划

我们计划与供应商通力合作，在部署下一代加密产品过程中，充分利用采用英特尔® 酷睿™ i5 处理器和英特尔® 酷睿™ i7 处理器的笔记本电脑所带来的性能优势。此外，我们预计下一代加密产品能够利用针对英特尔® 高级加密标准新指令 (英特尔® AES-NI) 而优化的新软件。这些指令基于这些处理器而构建，实现了更快、更安全的数据加密与解密。我们预计加密程序安装的安装速度将显著提升，而且会在启动、关机和休眠状态切换方面实现大幅的性能提升。

总结

在我们实施全盘加密部署的整个过程中，我们采取了多种战略措施来逐步解决所遇到的挑战。我们最成功的战略涉及员工培训、与高层和集团管理层的沟通、支持流程的修改、解决技术和运营问题以及与我们的供应商合作，旨在提高加密程序的性能并解决其它技术问题。

到 2010 年初，英特尔员工已经成功对 70% 符合条件的公司笔记本电脑安装了全盘加密程序，这也正是我们从拉动部署转变为推动部署的目标。然后，我们开始实施加密程序的强制性推动部署，以确保余下的笔记本电脑实施安装。我们预计公司所有余下的笔记本电脑将会在 2010 年中期完成加密部署。

随着加密程序部署接近尾声，在我们对所有英特尔 IT 部门管理范围内的笔记本电脑实施推动部署后，我们的加密专家团队

将手动加密所有余下的笔记本电脑，这些电脑不属于英特尔 IT 部门的管理范围，因此要予以特别的关注。

鉴于受到严重攻击及笔记本电脑丢失而导致的风险和成本每年持续上升，我们意识到必须提高企业安全战略的警觉性。英特尔 IT 部门在推动全盘加密解决方案部署方面的持续努力便是这些战略的重要组成部分。

了解更多信息

访问：www.intel.com/IT，可获得其它 IT@Intel 白皮书。

- “通过笔记本电脑加密增强企业安全性。” 英特尔公司，2008 年 12 月。
- 请参见《在企业范围内部署采用固态硬盘的笔记本电脑》，英特尔公司，2009 年 8 月

缩写词

BKM	最佳方法
FAQ	常见问题
FIPS	联邦信息流程标准
HDD	硬盘
Intel® AES-NI	英特尔® 高级加密标准新指令
NIST	美国国家标准与技术研究院
SSO	单点登录
SSD	固态硬盘

如欲与英特尔 IT 高管针对本文主题进行直接对话，请访问：

www.intel.com/it

本白皮书仅供参考之用。本文件以“概不保证”方式提供，英特尔不做任何形式的保证，包括对适销性、不侵权性，以及适用于特定用途的担保，或任何由建议、规范或范例所产生的任何其它担保。英特尔不承担因使用本规范相关信息所产生的任何责任，包括对侵犯任何专有的责任。本文不代表英特尔公司或其它机构向任何人明确或隐含地授予任何知识产权。

英特尔、Intel 标识、英特尔酷睿和英特尔博锐是英特尔公司在美国和其他国家（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。

版权所有 © 2010 英特尔公司。保留所有权利。

♻️ 请注意环保

0510/JLG/KC/PDF

323002-001

