并购如何影响数据安全性

以Equifax和Marriott数据泄露事件为例

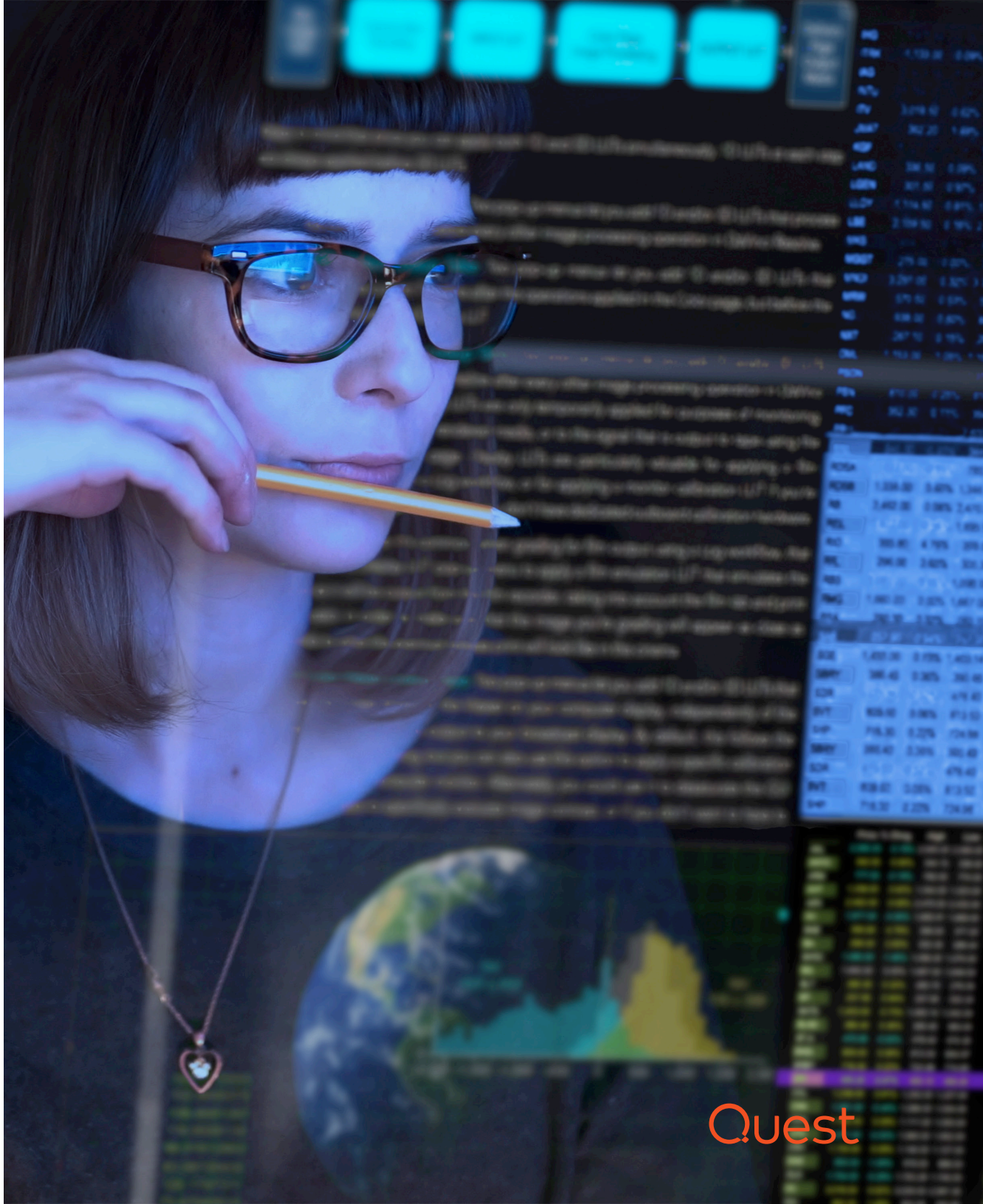
Quest

简介

实现适当的IT集成是实现并购协同的关键所在

2018年是大型复杂并购活动纷至沓来的一年，而今年的并购活动预计会更庞大。根据Deloitte的2019年并购趋势报告显示，76 %的并购在总部位于美国的公司中发生，而且美国私人股本公司中87 %的并购负责人预计他们企业在下一年完成的并购数量将会增加。此外，70 %的受访者预计他们的并购数量将超过2018年的并购数量。

并购的主要目标是协同 - 确保新合并公司的价值和业绩超过单独每家公司所实现价值和业绩的总和。合并实体实现协同的速度越快，实现财务业绩改进的速度也就越快。而影响实现这些优势的重要因素是进行成功的IT集成。实际上，Gartner报告显示，“25 %的典型并购相关集成工作源自IT，而且超过一半的协同相关集



成活动高度依赖IT，这意味着CIO拥有很大的机会来加速并购执行。”[1]

遗憾的是，在预期协同的光芒下，公司通常会犯一些严重的错误，而且无法实现适当的IT集成。因此，他们会遇到严重的安全问题，使新成立的公司面临风险。本电子书将揭示如何避免那些错误，并实现所需的安全性以获得预期通过并购所实现的优势。

“数年之前，网络安全尽职调查包含收购公司要向目标公司询问的一系列问题。而且可进行现场访问或电话联系来进一步完善该调查。现在，安全性是董事会关注的问题，而且与其相关的影响会大大降低未来企业的价值，尤其是在敏感数据和知识产权方面。”

Gartner，“Cybersecurity Is Critical to the M&A Due Diligence Process”（网络安全对于并购尽职调查过程至关重要），Sam Olyaei，2018年4月30日。

1 Gartner，“The CIO's Role in Making Mergers and Acquisitions Faster”（CIO在加速并购方面的作用）(ID G00226390)，Ansgar Schulte，2018年12月5日更新，2012年2月1日发布。

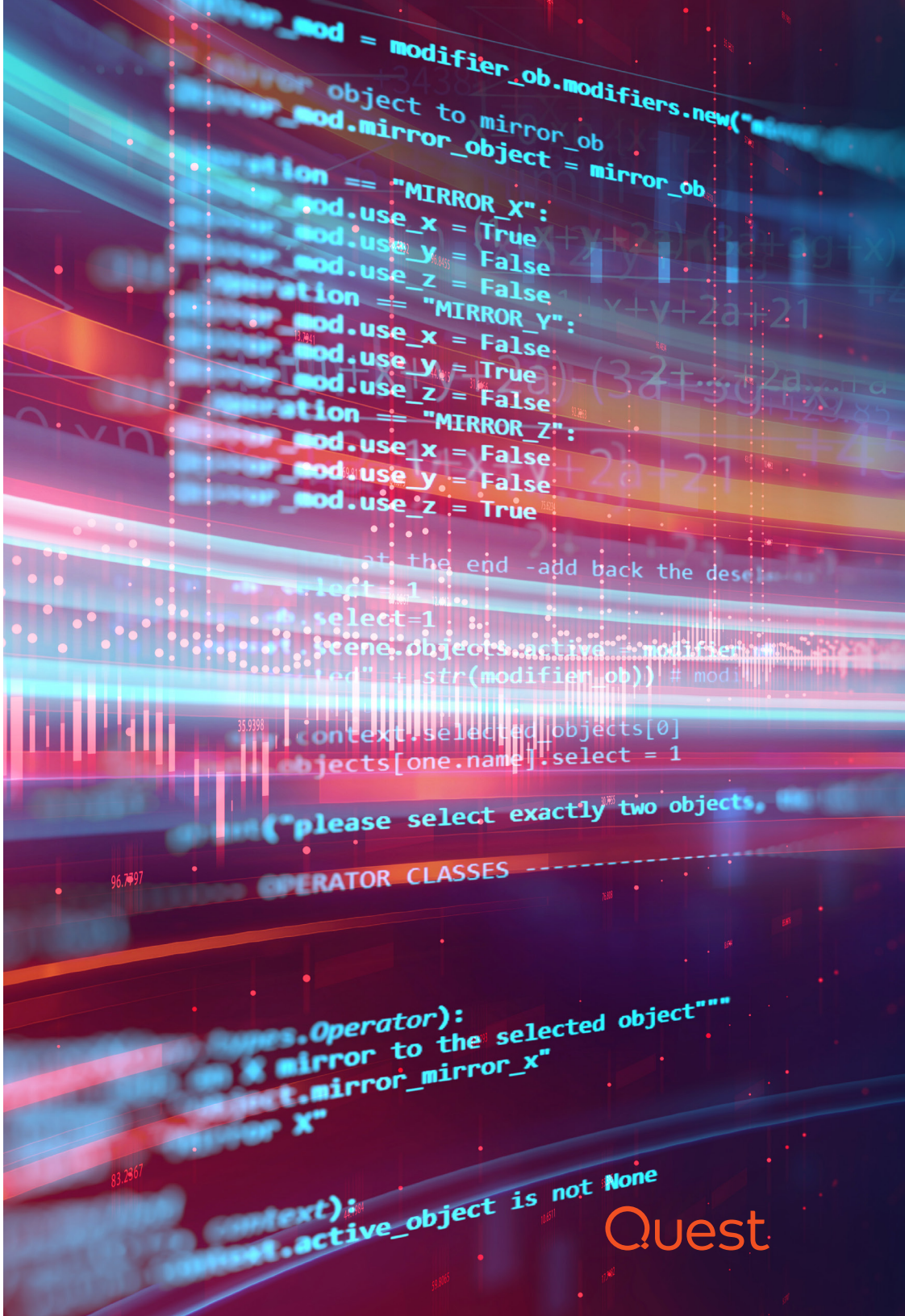
Quest

并购如何影响安全性

LD1之前

在宣布并购之后，争分夺秒地向法定第1天(LD1)迈进的过程就开始了。IT团队面临压力，需要快速完成IT集成，牺牲了适当的IT尽职调查以实现业务敏捷性。以下是在并购过程中导致危险的安全问题的一些常见错误：

- **未确定迁移范围 —** LD1的目标不是在并购所涉及的企业之间完成集成；而是实现某种程度的互操作性和通信，以及对外呈现出统一的样子。未能仔细确定迁移范围会对安全性产生严重影响。确定的范围过小（例如忘记云中需要迁移的所有B2C帐户）会导致用户没有所需的访问权限，以致用户在LD1无法高效工作。确定的范围过大无疑会导致更糟的结果；例如，如果迁移属于裁员范围的员工的用户帐户，则会使这些员工或他人有机会滥用其帐户，实现恶意目的。
- **在执行网络安全分析之前建立Active Directory信任 —** Active Directory在任何Windows环境中都是核心身份验证和授权机制。为了在两个AD域之间共享资源，需要在它们之间建立AD信任，因此要在并购所集成的IT环境的AD域之间建立信任会带来巨大的压力。但是，与另一个域建立信任会为该域中



的任何人（包括恶意内部人员或受到危害的帐户）提供通道，用来横向遍历到您的环境中。为避免该风险，您需要充分了解其他AD域中既有的安全政策和程序。

- **使用脏数据 —** 存在超过数年之久的任何AD基础架构都很有可能经历过大幅增长和变化，且通常未经过充分的监督和管理 - 换句话说，存在无序增长的情况。因此，并购涉及的每个AD基础架构几乎都存在一定数量的重复、陈旧和不必要的数据。未能清理所有这些脏数据会增加IT集成项目的成本和复杂性，致使IT专业人员将更少的时间用于执行按时履行LD1所需的所有任务。此外，忽视清理工作会在多个方面增加安全风险。首先，每个未使用的计算机和未经过适当禁用和删除的用户帐户都是攻击者的合适目标。第二，IT团队往往过度依赖SID历史记录，在新环境中为用户提供与在旧环境中相同的访问权限，没有停下来考虑这些访问权限是否合适。这种IT状况就像是买了房子后没有换锁一样。

在争分夺秒地迈向LD1的过程中，公司通常会牺牲适当的IT尽职调查以实现业务敏捷性，这会导致严重的安全后果。

Quest

相关案例：Marriott对Starwood的收购

2015年，Marriott的CEO预计该公司对Starwood Hotels的收购将会通过利用卓越的后台办公室和运营效率实现2亿美元的年度成本协同效应。但是，完成收购两年后，Marriott发现黑客自2014年起便已经毫无顾忌地进入Starwood的宾客数据库，访问、加密和下载多达五亿客户的个人数据。很明显，Marriott未能在并购IT集成项目中进行适当的网络安全尽职调查，否则早已发现Starwood安全流程方面存在的大量问题，而且甚至可能会发现该泄露问题。

现在，Marriott不但没有享受并购带来的协同优势，还遭受空前巨大的风暴。预计该数据泄露事件的直接成本在2亿美元到6亿美元之间，但是这只是开始。监管机构可能因其未遵守欧盟的通用数据保护条例(GDPR)而开出多达9.15亿美元的罚单，而且诉讼成本很可能多达数百万美元。此外，美国 证券交易委员会可能因其未能立即披露泄露问题而起诉Marriott。最后，还有不可见的成本，包括品牌受损和客户忠诚度损失。

总之，损害总计可能高达35亿美元，而Marriott本可通过仔细、彻底的IT集成过程避免所有这些损失。

Marriott因未能在并购过程中执行适当的IT尽职调查，造成多达35亿美元的成本损失。

Quest

快捷方法和变通方法通常是进入LD1所必需的。但是，在之后不能清理它们则会带来灾难。

LD1之后

在实现基本通信和互操作性这些LD1目标的过程中，IT团队通常会做出一些让步，例如将旧系统留在原地，使用变通方法支持相关的工作流；所有这些快捷方法都需要进行清理。当然，仍有一些工作会超出LD1的范围，例如各种服务器、应用程序和工作站的迁移。

遗憾的是，企业通常在LD1之后的阶段中犯一些错误，从而导致安全问题，这包括以下错误：

- **未迁移旧应用程序 —** 迁移旧应用程序（尤其是依赖AD的内部开发应用程序）通常看起来不太值得。由于涉及的工作和复杂性，企业选择将旧目录留在原地以用于旧环境，并在旧AD与主要AD之间设置某种共存。但几乎不可避免的是，旧AD会变得与主要AD不同步，或者旧服务器未能正确地安装补丁 - 导致出现内部人员和入侵者可以利用的安全缺口。
- **尝试通过本机工具勉强应付 —** 尽管本机工具是免费的，但它们的功能有限，而且根本无法扩展到大多数AD和Office 365迁移的规模和复杂性。此外，没有用于租户到租户迁移的本机工具。因此，在权衡可信供应商提供的专门构建的迁移工具和支持的ROI时，请务必考虑迫使IT团队疲于应对手动流程和有限可见性方面的成本，以及由于依赖基本工具而可能导致安全事件的直接和间接成本。
- **没有为意外情况做好规划 —** 企业即使成功避免了前面所有问题，也不能感到万事大吉了。事情总有出错的时候。确保您可以快速轻松地回滚未按预期工作的迁移任务，否则企业会受到损害。在迁移之前、之中和之后，必须设置好适当的备份和恢复系统，以便及时回滚错误并确保不会丢失信息。

Quest

相关案例：Equifax的多次并购

2005年，信用报告机构Equifax实施了激进的增长策略 - 到2018年，它已收购了18家公司，成为全球最大的私有信用跟踪公司之一。不论以哪种标准来说，该并购方法都取得了广泛的成功：Equifax的市值提高了四倍以上 - 2005年12月为每股38美元左右，到2017年9月，已增加到138美元每股。

但是，在这些收购过程中进行IT集成的方式正是该公司在2017年出现数据泄露事件的一大原因，该事件泄露了1.48亿人员的敏感个人数据。根据美国 众议院监管和政府改革委员会的报告，“尽管收购策略对于Equifax的盈利和股票价格来说是成功的，但是该增长增加了Equifax的IT系统复杂性，并且增加了数据安全风险。”[2]

该言辞激烈的报告指出该泄露事件“是完全可避免的”。具体问题包括：未能修补某个版本的Apache Struts，其在20世纪70年代自定义构建的面向互联网的消费者纠纷门户中使用；过期的证书，其允许往来于互联网的流量不经过入侵检测或预防系统的分析，该问题持续达19个月。

Ponemon Institute（从事网络攻击成本追踪的研究机构）主席Larry Ponemon对此事件的评论是，“这似乎将成为历史上代价最高的数据泄露事件”。[3] 他估计该数据泄露事件的总成本可能“超过6亿美元”，其中包括技术和安全升级、法律费用，为被窃取数据的消费者提供免费的身份被盗服务，以及解决政府对该事件的调查和针对该公司的民事法律诉讼所需的成本。

Equifax因未能处理并购产生的IT复杂性，导致出现代价高昂的数据泄露事件。

2 美国 众议院监管和政府改革委员会，多数派报告，“The Equifax Data Breach”（Equifax数据泄露），2018年12月。

3 Reuters，“Equifax breach could be most costly in corporate history”（Equifax数据泄露可能是企业历史中代价最高的数据泄露事件），2018年3月2日。

如何保护自己

如您所见，有许多因素导致并购的IT集成部分误入歧途，以上所列只是部分因素。您此时可能感到诧异，但是在以下两个方面有好消息。

首先，这不是从未涉足的领域。许多企业已进行了AD迁移和整合以及Office 365或Azure AD租户到租户迁移，而且您通过他们的经验可以学习到许多知识。第二，尽管迁移在具体方面存在不同，例如涉及的平台和迁移的数据量，但是相同的基本妥善做法适用于几乎每个迁移。在较高层面，您需要确保可以：

- **执行发现 —** 确保透彻了解源和目标环境的用户、应用程序、系统、权限和其他详细信息，以及它们的交互和相关性。然后，与您的业务伙伴进行合作，发现不需要迁移的未使用邮箱、帐户和服务，以及应当归档的内容。该过程将简化迁移并改进目标环境中的安全性和管理。

Quest

- **备份和恢复数据 —** 在开始任何迁移之前，需要对来源的林、邮箱存储库和协作站点进行彻底的备份，以防在迁移过程中出现错误。当然，可靠的备份和恢复解决方案将在IT集成过程完成后继续提供价值。
- **确保高效工作 —** 迁移过程会花费很长时间，而且您需要确保无论各个参与者位于什么系统中，用户都可以组织会议，而且每个人都可以无中断地访问其所有电子邮件，等等。因此，确保可以在两个系统之间同步公共文件夹内容、忙/闲信息、邮箱和重要数据非常重要。此外，您应确保迁移到新系统的所有用户都迁移现有帐户和密码，并且您可以在迁移这些用户后更新用户的AD和Outlook配置文件。
- **确保为管理层提供最新信息 —** 确保您可以向各个利益相关方报告迁移的进展情况，或者使他们可以按需安全地自行访问这些信息。
- **妥善监管和保护目标环境 —** 通过建立妥善的监管以及跟踪异常或可疑更改和用户活动并发出相应警报，确保合并后的新IT环境安全无忧。理想情况下，您希望能够避免更改大多数重要对象，例如拥有巨大权限的管理组。

在IT集成过程中遵循既定的安全妥善做法有助于您的企业避免Marriott或Equifax的悲剧再次上演。

借助Quest的成熟解决方案和卓越支持，解决并购IT集成的复杂性。

结论

并购在数量和规模方面不断增长，而且它们的成功取决于正确执行IT集成的程度。遗憾的是，许多企业在匆忙迈向LD1和之后的数月内会犯一些常见错误，这些错误会严重危害新合并企业的安全性，并导致巨大的成本损失，而不是预计通过并购将会实现的节省。

但是，遵循本文提供的专家建议，您的企业可以避免Marriott或Equifax的悲剧再次上演。您不必担心孤军奋战。Quest开发了全面的框架来实现对内部部署、云和混合Microsoft环境的有效集成、整合和管理 - 始终值得信赖的软件和服务。更好的是，它可重复：您会熟悉一系列解决方案、一个支持团队和一个服务团队，当接到下一个并购项目时，您早已准备就绪。

要详细了解并购IT集成的安全影响、妥善做法以及Quest解决方案如何帮助您解决相关的复杂性，请阅读白皮书《IT Integration Best Practices in Mergers & Acquisitions (M&A)》（并购中的IT集成妥善做法）。

Quest

关于QUEST

Quest致力于为瞬息万变的企业IT领域提供软件解决方案。我们帮助简化数据爆炸、云扩展、混合数据中心、安全威胁以及合规要求所带来的挑战。我们是一家全球性服务提供商，向遍及100个国家/地区的130,000家企业提供服务，其中包括95 %的财富500强企业以及90 %的全球1000强企业。自1987年以来，我们构建了丰富的解决方案产品组合，现在包括数据库管理、数据保护、身份和访问管理、Microsoft平台管理以及统一端点管理。借助Quest，企业可以缩短IT管理时间，将更多时间用于业务创新。有关详细信息，请访问：www.quest.com。

如果您对可能使用的本材料存有任何问题，请联系：

www.quest.com/cn-zh/company/contact-us.aspx

Ebook-M&AImpact-US-GM-zh_CN-WL-38204

Quest