FORRESTER®

Dell 委托进行的定制技术采用概况分析 | 2017 年 10 月

为满足现代工作者需要而不断演变的安全政策

开始 ▶

为满足现代工作者需要而不断演变的安全政策

安全政策应该提供保护和支持

为了跟上业务移动性的发展速度，而又不受其潜在风险的影响，IT 部门必须能够有效地解决服务供应、设备采购和安全监管等各种复杂问题。原因何在？信息工作者需要从他们所在的任何位置跨各种业务应用程序和设备访问通常敏感的信息。换言之，不妨碍最终用户工作效率的安全和隐私策略将赋予员工权力并提升他们的绩效。

项目背景

2017 年 7 月，戴尔委托 Forrester 对 21 世纪的员工队伍，及其新习惯、态度和工作方式如何重塑工作环境开展了一项调查。随着单个组织中需要更多的服务角色，企业无法满足员工的需求。为了完成其任务，员工正在绕过安全政策，以在需要时获得他们所需的内容。组织必须了解员工的不同行为，谨慎、平等地平衡安全需求，否则就有可能使他们自己面临现有威胁和前所未有的新威胁。

国家/地区

- 澳大利亚：**25%**
- 印度：**25%**
- 美国：**25%**
- 英国：**25%**

公司类型

- 本地：**11%**
- 区域：**35%**
- 跨国：**54%**

年收入（美元）

- 4 亿至 4.99 亿：**21%**
- 5 亿至 9.99 亿：**31%**
- 10 亿至 50 亿：**28%**
- >50 亿：**20%**

角色类型

- 办公室工作人员：伏案办公人员：**32%** 以及无线办公人员：**23%**
- 非办公室工作人员：移动办公专业人士：**24%** 远程工作者： **22%**
- **专业角色：**知识产权工作者：创意工作者：**30%** 和工程师：**24%**

为满足现代工作者需要而不断演变的安全政策

1 2 3

当今不同的员工队伍使用大量设备

工作场所的数字化使信息工作者能够随时获得所需信息。专职工作者周内每天上下班往返于一个地点的日子即将结束。移动技术的广泛应用、灵活的工作政策以及员工的偏好现在都意味着当今的数字员工队伍可在家中、公共场所以及多个地点工作。信息工作者同样使用各种设备。IT 部门面临的挑战是帮助其员工安全地使用这些设备以遵循 IT 部门自己的安全协议，并使业务更加高效并获得巨大成功，同时不会干扰员工的自主性或工作效率。

出于本调查的目的，我们定义了以下类型的工作者：

- **办公室工作人员：**伏案办公人员和无线办公人员。
- **非办公室工作人员：**远程工作者和移动办公专业人士。
- **知识产权工作者：**创意工作者和工程师。

笔记本电脑仍然是所有类型的工作者中最受欢迎的设备，平均有 57% 的人使用它们来完成工作，而无论他们在哪里工作。

“在典型的一周内，您会在何处使用以下设备进行工作？”

	远程工作者	移动办公专业人士	伏案办公人员	无线办公人员	创意工作者	工程师
任何类型的台式机	58%	45%	67%	63%	58%	53%
任何类型的笔记本电脑	69%	50%	63%	38%	61%	63%
任何类型的具有触摸屏和可旋转屏幕的 2 合 1 设备/“可转换设备”	26%	34%	17%	23%	33%	38%
任何类型的共享工作空间	20%	28%	16%	22%	31%	19%
任何类型的用于协作的临时显示器	19%	20%	17%	12%	24%	20%
任何类型的可移动数据存储和配件	21%	34%	26%	21%	36%	32%
任何类型的屏幕大小在 7 到 12 英寸之间的平板电脑	17%	35%	20%	18%	27%	28%
手机	13%	22%	6%	6%	15%	14%
智能手机	56%	64%	57%	41%	70%	59%
专用移动连接设备	10%	16%	5%	18%	9%	10%

受访对象：美国、英国、印度和澳大利亚各行各业的 400 位信息工作者
资料来源：Forrester Consulting 代表戴尔开展的一项委托调查，2017 年 9 月

为满足现代工作者需要而不断演变的安全政策

员工认为其公司的安全流程是被动的

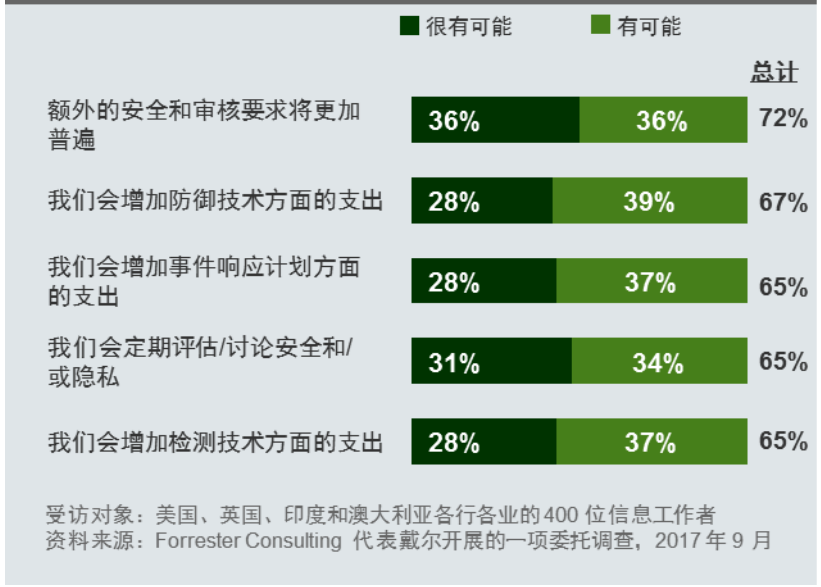
数据是当今数字业务的命脉；确保它免受盗用、误用和滥用是全球各组织的头等大事，特别是由于公司不需要看得太远，甚至不需要关注新闻就知道对数据的威胁正在蔓延。

信息工作者透露，如果确实出现安全漏洞，会导致更多支出、更多安全项目以及更多要求。例如，受访者表示，由于安全漏洞，会导致更多安全和审核要求 (72%)、更高的预防支出 (67%) 以及更高的检测技术支出 (65%)。

此外，安全漏洞不仅会增加组织范围内的关注，而且会直接影响业务，因为这会导致负面地描绘品牌形象 (62%) 并引来负面宣传 (59%)。

82% 的信息工作者认为，其公司对安全漏洞的反应非常灵敏或反应迅速。

“您认为最有可能发生的安全漏洞事件或后果是什么？”
（仅显示“很有可能”和“有可能”的前五项）



受访对象：美国、英国、印度和澳大利亚各行各业的400 位信息工作者
资料来源：Forrester Consulting 代表戴尔开展的一项委托调查，2017 年 9 月

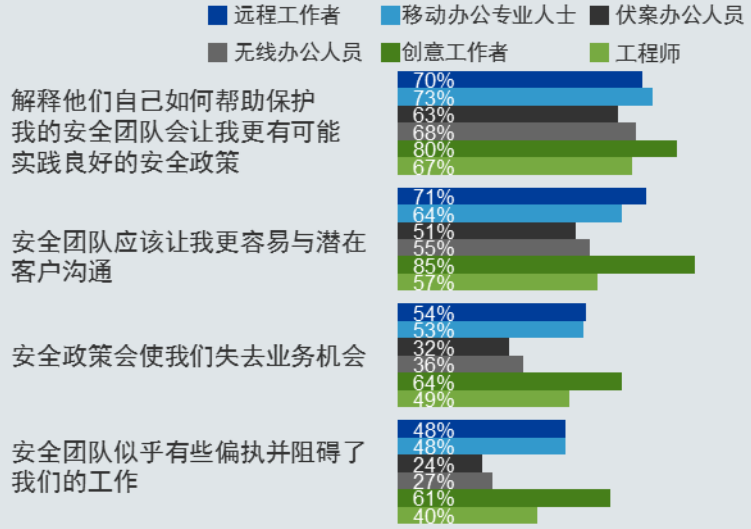
为满足现代工作者需要而不断演变的安全政策

指导，而不是控制，会带来更好的安全实践

组织很难了解其员工队伍的信息和组成，以及如何管理当今多元化的员工类型组合。所有类型的工作者都非常同意或同意，安全团队应解释如何帮助保护他们，这将使他们更有可能执行良好的安全实践。

然而，角色中出现了一些有趣的变化。非办公室工作人员（平均 54%）和知识产权工作者（平均 57%）表示，安全政策使其失去业务机会，而且员工应该更容易与潜在客户沟通。此外，安全团队必须能够支持甚至推动员工使用不同的设备；然而，非办公室工作人员和知识产权工作者表示，他们发现很难与安全团队合作：他们遇到偏执情况并阻碍了他们的工作。

“您在多大程度上同意以下有关管理您所使用设备上的安全协议的团队的陈述？（仅显示“非常同意”和“同意”）



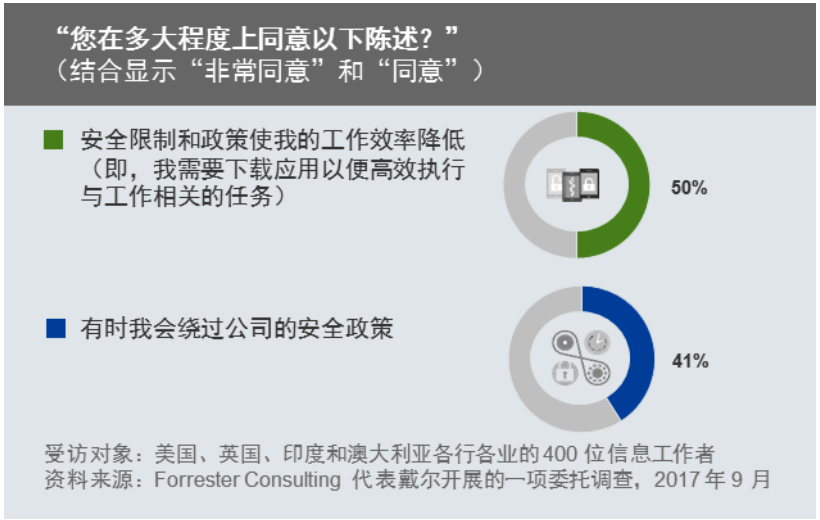
受访对象：美国、英国、印度和澳大利亚各行各业的400 位信息工作者
资料来源：Forrester Consulting 代表戴尔开展的一项委托调查，2017 年 9 月

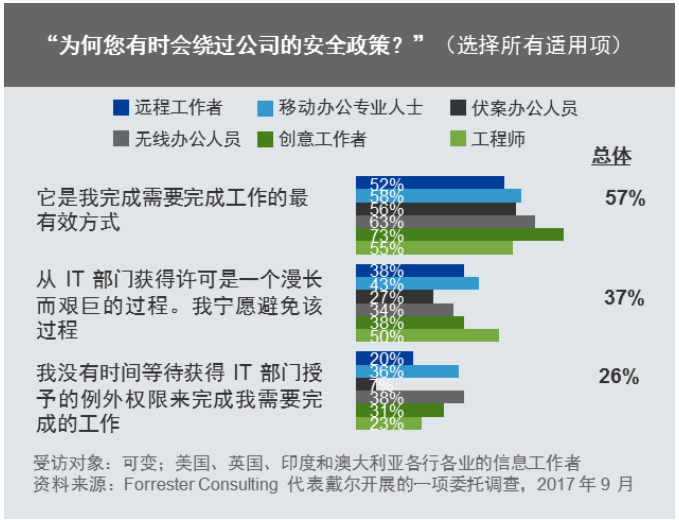
为满足现代工作者需要而不断演变的安全政策

员工表示自己组织的安全政策妨碍了他们的工作

员工在努力完成工作，但安全控制措施阻止他们高效完成任务，因为这些措施设计不佳而且它们不够动态，无法满足不同角色的需求。这就解释了为何一半 (50%) 的信息工作者表示，安全限制和政策降低了他们的工作效率，而且 41% 的人表示他们有时会绕过公司的安全政策。

换言之，员工选择阻力最小的途径来完成工作，因为这是最有效的方式 (57%)。员工需要和要求从他们的设备访问敏感的公司信息，而从 IT 部门获得许可是一个漫长而艰巨的过程 (37%)。有趣的是，非办公室工作人员和知识产权工作者更有可能违反安全协议以获得他们所需的内容。例如，75% 的移动专业人士和 IP 工作者，以及工程师 (49%) 和创意工作者 (52%) 更有可能违反安全政策；因此，公司应该关注他们，因为他们带来了更多问题。



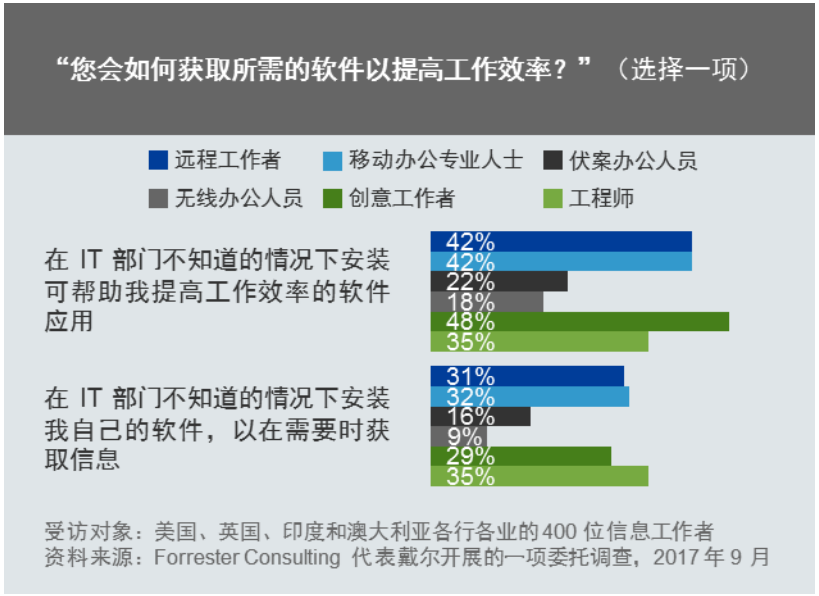


为满足现代工作者需要而不断演变的安全政策

员工希望提高工作效率，而没有恶意

员工希望访问软件和应用，以帮助他们完成工作。如果安全团队通过自己的方式（例如访问应用或下载软件）设定过多的政策和控制措施，员工将在 IT 部门不知道的情况下，从其他来源寻找替代方案，并绕过安全流程，这将增加安全风险。但是，这些行为并非员工出于恶意；他们在需要提高工作效率时需要访问应用和软件。

不足为奇，与非办公室工作人员（远程工作者和移动专业人士）和 IP（创意工作者和工程师）相应人员相比，办公室工作人员（伏案办公人员和无线办公人员）不太可能在 IT 部门不知道的情况下安装软件或应用。相反，他们更有可能做他们想做的事情，如果这意味着他们可以提高工作效率，并随时随地获得所需信息。



在安全方面存在明显差距：*62% 的远程工作者担心会由于安全违规或事件而受到指责。工程师担心造成客户数据泄漏 (73%)，但他们认为需要在 IT 部门不知道的情况下安装应用，以帮助他们提高工作效率。*

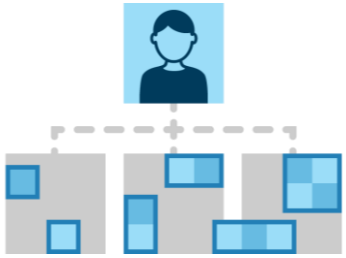
为满足现代工作者需要而不断演变的安全政策

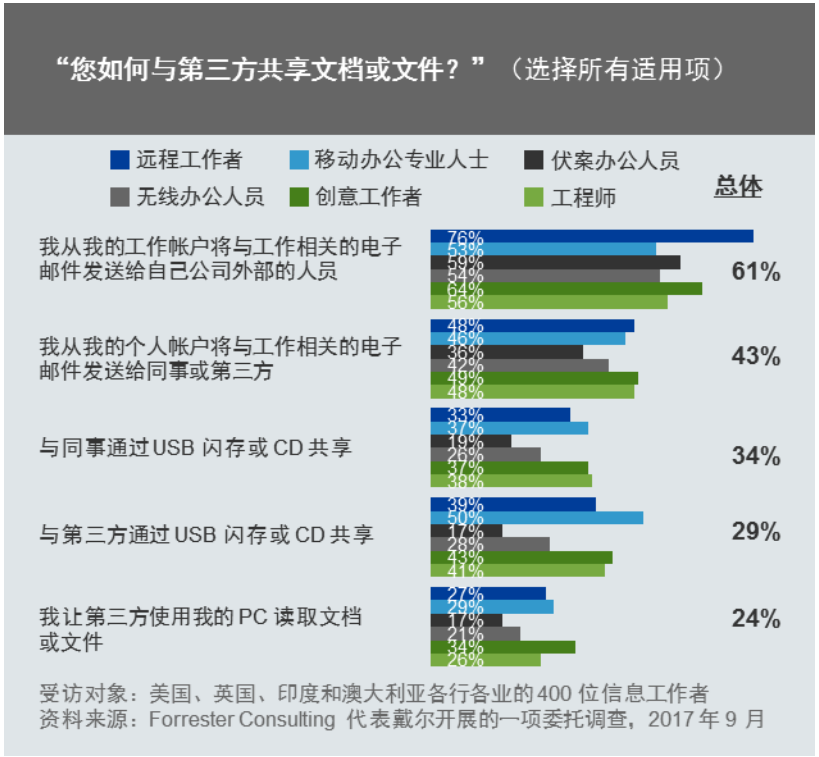
员工需要共享数据：IT 部门应该以安全的方式支持他们

在 21 世纪，数据经济对于了解数据有其自己的生命是至关重要的。组织正在收集大量数据，这意味着由于最终用户生成的数据量日益增多，并且他们在各种位置（云、USB 闪存驱动器等）存储和复制这些数据，而导致保护数据的工作负担不断增加。

尽管知道这种影响，以及发生安全漏洞时将意味着什么，但是员工希望、需要而且将会在同事或第三方组织之间共享数据。但是，员工在不安全的环境中共享信息会使企业面临风险。安全专业人士必须找到解决方案，以一种易于访问和无缝使用的更安全的方式帮助当今不同的角色。

71% 的工作者表示他们每天或每周与第三方共享文件。





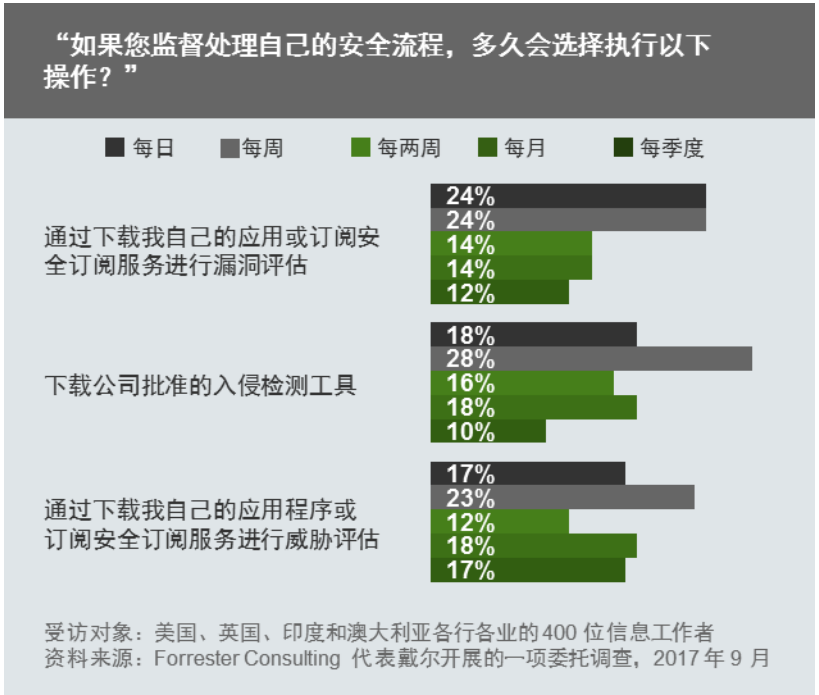
为满足现代工作者需要而不断演变的安全政策

1 2

考虑到权限和工具，工作者将获得安全政策的所有权

不可否认，在寻求不同类型的工作角色时，当前的安全方案非常分散。工作者重视安全政策，但他们希望安全政策在其日常任务中少一些干扰。安全政策干扰越少，员工就会越欢迎它。但是，如果 IT 部门通过身份验证过程阻碍了他们的工作效率，或者对某些应用和工具设定限制以使其无法高效完成工作，员工会借助他们自己的方法变得来去自如。

但是，员工也明白制定安全政策不是一项简单的任务；员工态度的改变是因为他们与安全团队产生了共鸣。这就解释了为什么，鉴于该控制措施，员工至少每月都要进行一次漏洞评估。目标是在为员工实施过多控制与减少安全政策的干扰之间找到适当的平衡。将文件保护功能嵌入自然的工作流程中，并安装恶意软件防护功能是让员工高效工作并保持安全的关键。各种安全解决方案可以利用此行为数据将其他层（端点、网络、物理/地理）的潜在威胁活动关联起来，或对给定事务或行为的风险做出更明智的决策。



为满足现代工作者需要而不断演变的安全政策

1 2

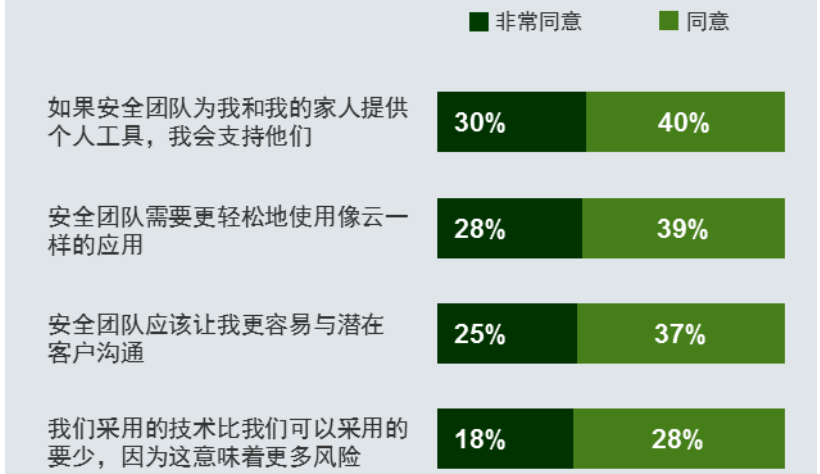
通过提供合适的工具，安全团队可以成为员工队伍的支持者

技术多样性和不断变化的员工工作方式带来了一系列威胁到组织品牌和安全性的安全问题。例如，增加的员工对应用程序和数据访问的需求将促使安全团队确保新员工队伍技术并不会将敏感信息置于风险之中，但仍允许授权员工无限制地访问，而不管公司是否拥有员工正在使用的设备。

因此，不足为奇，员工需要个人安全工具 (70%) 以及访问云中的应用 (67%)。为所有类型的员工提供安全工具，使他们在访问敏感信息时更加谨慎行事。

寻求让员工能够高效、安全协作的安全解决方案的公司从长远来看将保护自己的企业。为了在不阻碍工作效率和业务成果的情况下提高安全性，安全专业人士应该让员工能够使用更好的工具和指导来照管自己。IT 安全团队的职责应该是信任员工且验证其身份。

“您在多大程度上同意以下有关管理您所使用设备上的安全协议的团队的陈述？（仅显示“非常同意”和“同意”）



受访对象：美国、英国、印度和澳大利亚各行各业的 400 位信息工作者
资料来源：Forrester Consulting 代表戴尔开展的一项委托调查，2017 年 9 月

为满足现代工作者需要而不断演变的安全政策

为所有员工考虑：可提供更好的员工体验的安全性需求

技术正在改变员工的工作方式和地点。安全团队必须跟上步伐并满足所有类型工作者的需要。该调查发现了三个主要结论：

› **安全团队必须保护非办公室工作人员并为其提供服务。**一方面，办公室工作人员的安全要求较低而且风险较小，因为他们受到所处设施或办公室的保护。另一方面，非办公室工作人员和 IP 工作者更容易被忽视。公司还必须满足他们的需要，并了解一刀切方法并不适用于所有人。

› **信息工作者绕过安全政策是为提高工作效率，而不是恶意的。**当今的数字环境需要员工快速行动。显然，安全政策并不会帮助他们，尤其是不在公司办公室的工作者。为了在需要时获得所需内容以更好地服务客户，他们会绕过安全政策。

› **员工习惯会放大不好的安全实践。**不同的角色类型将以一种有利于他们完成工作的自然方式执行和开展工作。例如，非办公室工作人员和 IP 工作者必须与同事和第三方人员共享数据，但 USB 或 CD 可能会丢失。换言之，风险存在于不安全的设备中，而工作习惯会放大风险。

方法

本技术采用概况分析应 Dell 委托开展。共向澳大利亚、印度、英国和美国各行各业的 400 位信息工作者提出了定制调查问题。

该定制调查开始于 2017 年 7 月，完成于 2017 年 10 月。有关 Forrester 数据面板和技术行业咨询服务的更多信息，请访问 Forrester.com

项目主管

Tarun Avasthy
市场影响顾问