Forrester Consulting

思维领导力白皮书

委托方：IBM

2019 年 5 月

2019 年网络安全复杂性报告

如何降低复杂性，实现更好的安全成效

FORRESTER®

目录

项目主管：

Josh Blackborow 和 Sophia Christakis，

市场影响咨询师

其他贡献者：

Forrester 安全与风险研究小组

关于 FORRESTER CONSULTING

Forrester Consulting 可提供独立、客观的基于研究的咨询，以帮助领导者带领所在组织取得成功。从短期的战略会话到定制项目，Forrester 咨询服务可将您与研究分析师直接联系起来，而分析师可将专业洞察力运用至您特定的业务挑战中。有关更多信息，敬请访问 forrester.com/consulting。

FORRESTER®

执行概要

独立运行且会生成大量数据的互不关联安全解决方案导致出现了复杂性危机。

已采取措施简化其安全生态系统的组织正在收获优势，包括提升了应对安全威胁的弹性。

迅速变化的威胁格局使组织安全比以往任何时候都更加重要、更具挑战性。为应对这种情况，组织投资部署了大量互不关联的单点解决方案。不过，这些相互独立运行且会生成大量数据的互不关联产品最终导致出现了复杂性危机。结果是，安全团队无法充分利用他们的投资，必须投入更多的资金来确保其环境的安全。降低复杂性的需求从未如此迫切。

IBM 委托 Forrester Consulting 对安全复杂性的状态及其对安全效率和有效性的影响进行了评估。为了深入探讨这一主题，Forrester 对全球 200 位负责安全战略和/或安全技术购买的安全专业人员进行了调研。我们发现几乎所有受访者都表示他们关注复杂性。不过，已采取相应措施来简化其安全生态系统（包括将解决方案整合到单个管理平台中）的组织开始展露出一些重大优势。

重要调查结果

- **安全环境日益复杂。**安全专业人员倾向于以孤立的团队运作，因此几乎无法全面了解整个安全学科的数据和流程，更不用说了解整个公司的数据和流程。更糟糕的是，各个位置（尤其是云端）的数据量激增，而且这种趋势可能会一直持续下去。
- **组织的确在增加安全投资，但投资不一定明智。**安全预算的增加以及为避免破坏性数据泄露而给组织带来的压力，导致组织采用了大量互不关联的单点解决方案。我们通过调研发现，最近两年安全产品的数量平均增加了 52%、供应商的数量平均增加了 77%。这种购买狂潮增加了组织的安全复杂性，却不一定会提升组织安全计划的整体成熟度。
- **复杂性会影响 ROI。**安全复杂性已成为组织再也无法回避的一个问题。我们通过调研发现，91% 的组织关注复杂性，而那些环境非常复杂的组织则更有可能表示他们面临着成本挑战及技术和人员效率低下的问题。
- **简化可以释放安全投资的价值。**能够有效简化环境的组织可以充分利用现有的安全投资。他们已开始连接数据和流程，并将解决方案集成到经整合的管理平台中。他们还收获了诸多优势，包括提升了威胁检测、响应和恢复能力。

FORRESTER

被动策略导致众多安全解决方案“一团乱麻”

众所周知的数据泄露让安全性进入了高管团队的视线。如此一来，安全领导者更容易在安全项目融资上获得预算以及高管的支持。实际上，安全开支在 IT 预算中所占的比例正在不断上升。[1] 与此同时，该行业也为此采取了一系列具吸引力的解决方案来应对新威胁。[2] 结果如何呢？仍旧是被动的安全开支及普遍的效率低下。

我们针对 200 位安全决策者开展的调研结果表明，这些安全决策者将会在明年优先考虑优化安全资产和资源，这也印证了以下趋势：“提升安全投资回报率”是其首要任务之一，仅次于“改善高级威胁功能”。此外，许多公司专注于提高员工的生产效率、简化他们的环境并提升运营效率（见图 1）。不过，他们在这些方面面临着巨大的挑战，因为他们现在需要确保以下三项的安全：

- **数量激增的单点解决方案。**安全专业人员 - 尤其是那些曾遭受过数据泄露的公司的安全专业人员 - 已投入了越来越多的预算来购买新的安全解决方案。不过，也有许多公司只为了解决短期需求，而没有充分考虑每一项增投如何促进其安全计划成熟度的长期增长。如此一来，安全团队被众多不同且互不关联的解决方案所淹没。我们的受访组织平均管理着 13 家供应商提供的 25 种不同的安全产品/服务，甚至更多。在最近的 24 个月里，安全产品数量增加了 52%、新供应商增加了 77%，这些都印证了近年来的购买狂潮。
- **猛增的数据量。**在过去的两年里，来自内部环境、端点、虚拟服务器的数据，尤其是云端的数据大幅增加。在我们测试的每个位置中，受访者表示他们在其中存储的数据量平均至少增加了 55%，并且许多受访者表示，同一时期内数据已增加到了原来的两倍、三倍或更多（见图 2）。此外，与安全产品的增加不同的是，安全团队几乎无法控制未来几年可能持续存在的数据增加。

图 1

未来 12 个月安全方面的首要优先事项

受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员

来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

在过去的 24 个月中，受访者所在组织所用的安全供应商数量增加了 77%。

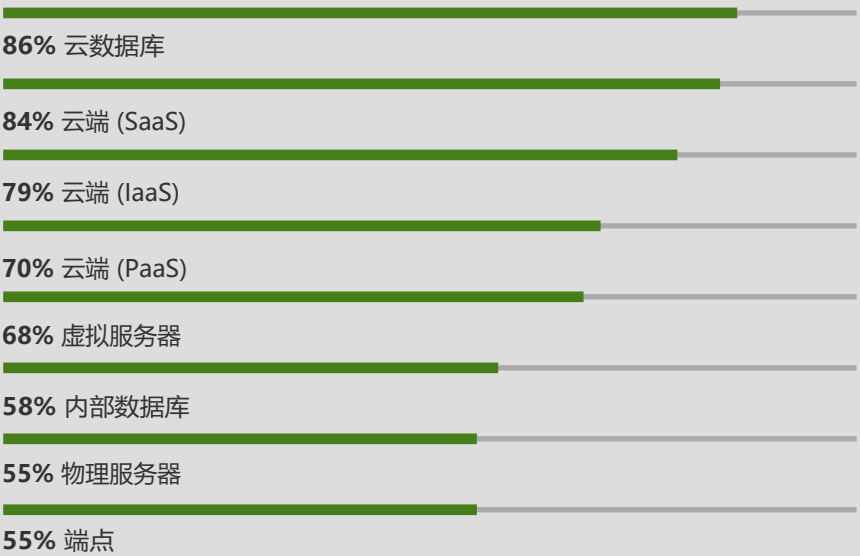
› **跨异构环境的数据。**数据越来越多地从端点和内部服务器中移出，并且在整个企业中不断扩散。许多组织都采用了云优先战略，因此也无怪乎许多组织都开始将数据移至云端，而且安全资产和流程也同样如此。实际上，受访者预测，到 2020 年，其组织在云端拥有的安全资产和流程所占百分比将会比 2016 年增加 200% 以上。分散在异构架构中的数据威胁着安全团队的可视性：他们无法去保护那些不能看到的宝贵数据资产。

尽管组织采取了各种各样的安全防御措施，但大多数安全专业人员仍旧难以实现安全投资价值的最大化并保护其组织的安全。[3] 实际上，不到四分之一的受访者表示，他们对安全产品组合在以下方面所提供的支持完全满意：开发高级威胁情报功能； 提高安全人员的生产效率；从数据中提取洞察力；提高效率。此外，只有 50% 或更少的受访者表示他们正在使用此次调研中所列 11 种安全技术中的所有或大部分可用功能。值得注意的是，只有不到 25% 的受访者表示他们在物联网 (IoT) 安全、身份与访问管理、安全自动化和编排、安全信息和事件管理 (SIEM) 等方面的技术得到了全面优化。

受访者预测，到 2020 年，其组织在云端拥有的安全资产和流程所占百分比将会比 2016 年增加 200% 以上。

图 2：过去两年中，存储在各个位置的数据量猛增

“过去两年中，贵组织在以下各个位置存储的数据量有何变化？” (显示平均增长百分比)



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员

来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

FORRESTER

复杂性削弱了网络安全保护的有效性

在当今的安全领导者努力管理其安全性环境的复杂性的同时，他们也学到了一个深刻的教训：添加更多的单点解决方案并不能简化任何事情。漫长的部署周期、困难的集成以及管理大量解决方案所需的用户培训都会催生导致技术投资失败的风险。[4] 受访者意识到，这构成了一个非常实际的威胁：91% 的受访者对其组织的安全复杂性表示了某种程度的关注（见图 3）。在受访者最关注的问题中，安全复杂性位列第二位，仅次于威胁的不断变化和演变这一性质。

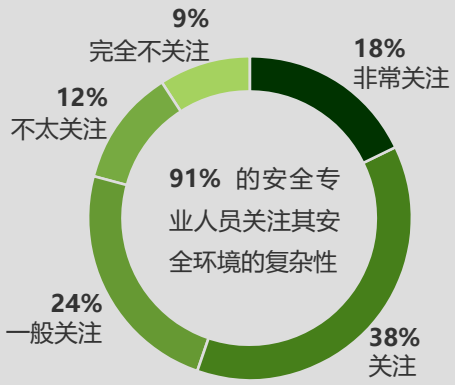
尽管几乎每个受访者都表示他们对环境的复杂性有某种程度的关注，但那些对复杂性最为关注的受访者所在组织的情况已表明，组织的安全环境已变得非常复杂（见图 4）。可以预见，对复杂性的关注越高，组织所拥有的产品和数据就越多。平均而言，对复杂性关注较高的受访者相比不太关注复杂性的受访者，其安全产品的数量高出 45%、供应商的数量高出 36%。此外，前者跨位置管理的数据量也更大。结果是，他们表示难以集成不同的安全技术和数据源以及他们正在苦恼安全相关数据及洞察力可视性的人数是其他组织的两倍（见图 5）。他们费力收集的所有洞察力都很难成为他们采取进一步行动的基础：超过一半的受访者表示他们难以与组织内外的同行就安全洞察力开展协作，这使得他们更加难以开发威胁情报功能，也更加难以发现漏洞模式。

91% 的安全专业人员表示他们关注组织的安全复杂性。

图 3：对复杂性的关注是安全专业人员的首要考虑事项

“就贵组织的安全态势保护而言，您对以下各项的关注程度如何？”

（图中所示为受访者对“安全环境的复杂性”的关注程度）



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员
注：由于进行了舍入，因此百分比总和并非 100%。
来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

安全复杂性是受访者最为关注的问题之一，与受访者对 IT 威胁和合规性不断变化的性质的关注程度不相上下。

FORRESTER

图 4：定义对复杂性的关注

“就贵组织的安全态势保护而言，您对安全复杂性的关注程度如何？”

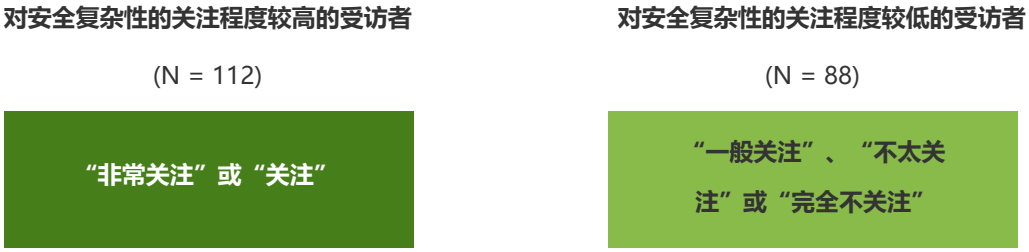
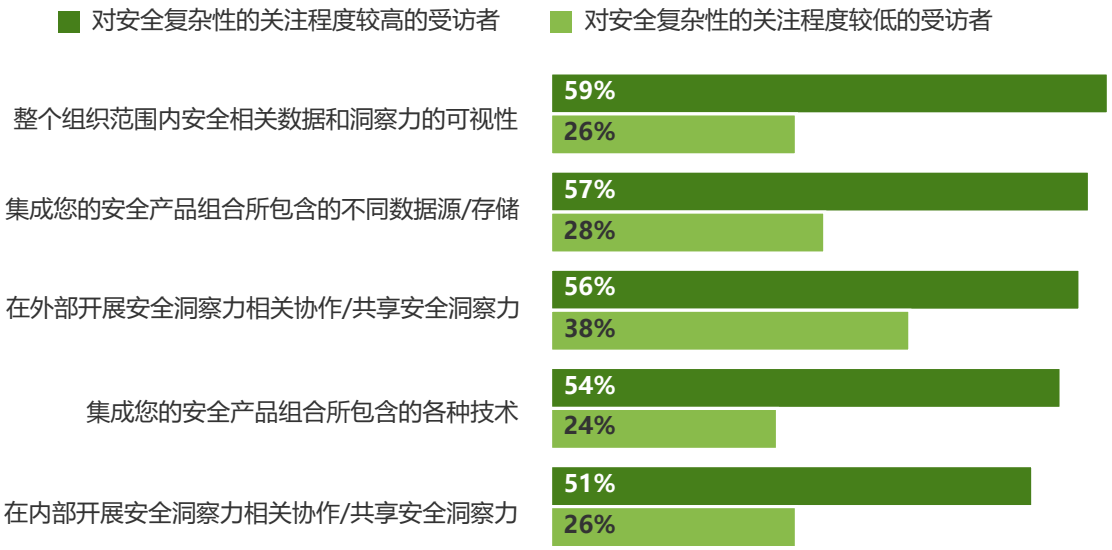


图 5：复杂性越高，所面临的挑战越大

“对于您的安全团队而言，下列各个方面的挑战性如何？”（图中所示为表示“有挑战性”或“极具挑战性”的受访者）



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员
来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

那些对复杂性关注程度较高的组织（如我们前面所述，其复杂性也更高），也会面临一些明显的不利因素，因为：

› **复杂性会影响 ROI。**安全复杂性加剧了一个原本已具有挑战性的问题，即无法充分利用安全资源。那些更为关注复杂性的受访者更有可能会表示他们安全环境的复杂性导致了高昂的成本。他们还更有可能表示他们所在组织在安全技术和安全人员时间的利用方面效率低下，也更有可能发现难以对人员开展新安全产品的培训（见图 6）。

高复杂性的组织更有可能表示他们面临着成本挑战以及技术和人员效率低下的问题。

FORRESTER

› **复杂性会妨碍创新。**政府机构、竞争对手和客户所带来的市场不确定性要求企业要不断变革。只有那些变革快速、确保互联和创新的企业才能在瞬息万变的环境中蓬勃发展。不幸的是，那些具有安全复杂性的企业难以确保所需的敏捷性，进而实现发展：50% 的受访者表示其所在组织的复杂性使其难以替换过时的安全技术，而 37% 的受访者表示，由于担心会进一步增加复杂性，导致他们推迟购买计划。更糟糕的是，有 29% 的受访者认为其所在组织被特定的供应商所束缚。尽管安全环境高度复杂的企业可以通过更加简化的生态系统而受益，但他们在实现现代化的工作方面，要比复杂性较低的组织面临更为艰巨的挑战。

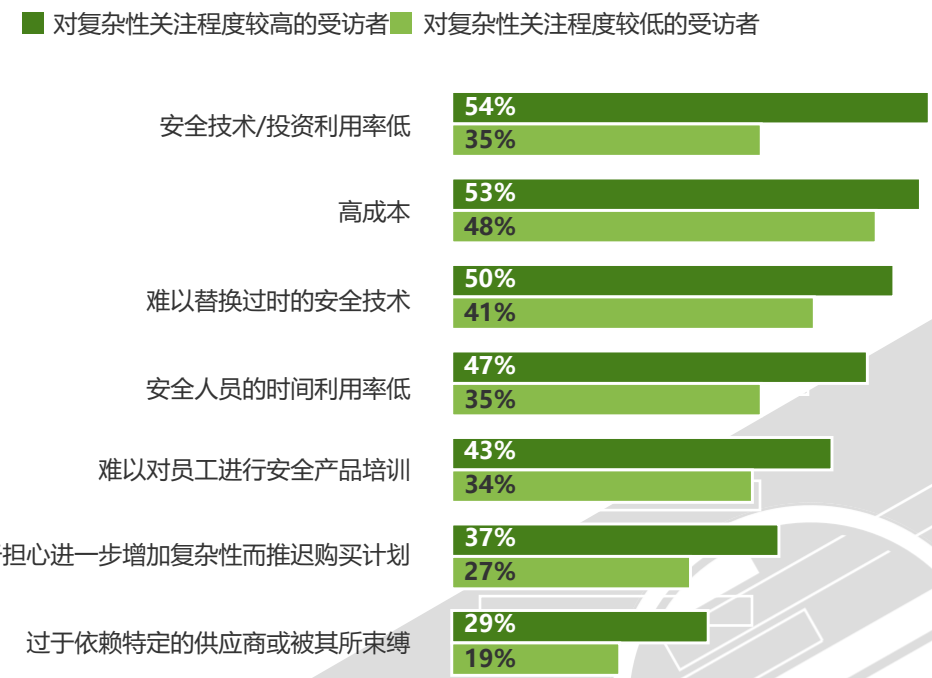
安全简化有助于释放投资价值

尽管简化过程中会面临各种挑战，但最关注复杂性的组织均表示简化是值得的。他们认为更简化的环境能够给他们带来诸多益处：有助于改善在数据洞察力提取、威胁情报、内部协作和用户体验方面的能力。值得注意的是，受访者认为简化有助于“适当”或“显著”提升运营效率 (72%)、安全人员的生产效率 (68%) 和安全投资回报率 (58%)，这些都是他们的首要任务。

组织认为简化的环境有助于他们提升运营效率、安全人员的生产效率和安全投资回报率。

图 6：安全复杂性会影响 ROI、限制灵活性并妨碍现代化工作

“贵组织由于安全环境的复杂性而遇到了哪些挑战？”（请选择所有的适用项）



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员

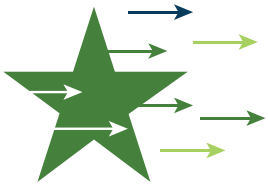
来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

简化的网络安全产品组合是前进方向

在了解了安全复杂性所带来的挑战以及简化带来的益处之后，关键问题就变成了：组织可以采取哪些措施来降低安全复杂性？尽管所有受访者都表示他们至少采取了一定的措施来降低复杂性，但仅有不到一半（44%）的受访者表示他们在这方面的投入取得了成效。在此次调研中，我们将这部分组织称为“冠军组织”，并将所有其他组织（即那些表示自己在这方面的投入“有一定成效”、“不太有成效”或“完全没有成效”的组织）称为“挑战者”（见图 7）。

尽管冠军组织在简化方面上取得的成效更大，但他们的简化之旅并未完成。实际上，他们中的许多受访者仍然表示了对复杂性的关注。不过，他们已开始在安全环境简化方面取得重大进展，也取得了一些对仍在这方面“挣扎”的组织具有指导意义的经验教训。尤其是，冠军组织会：

› **以简化为重点。**尽管看起来很明显，但冠军组织与挑战者之间的最大区别之一在于他们对简化的重视程度。冠军组织不仅更可能以简化为重点，而且更有可能在简化方面投入特定的资源（见图 8）。75% 的冠军组织会投入专用资源，而在挑战者中，这一比例只有 56%。此外，有 63% 或以上的冠军组织采用了我们所测试的所有简化策略。



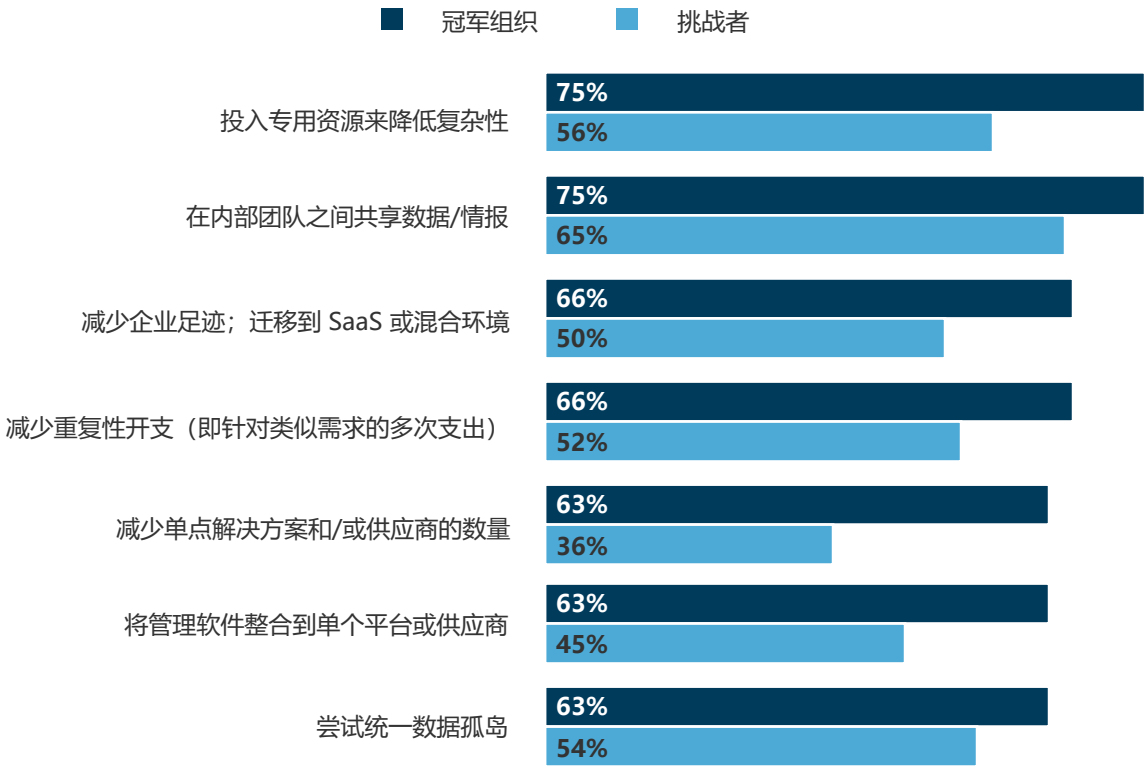
“冠军组织”是指在降低安全复杂性方面取得更大进展的组织。

图 7：定义“冠军组织”和“挑战者”

“到目前为止，贵组织为降低安全复杂性所做投入的成效如何？”

图 8：冠军组织在简化计划方面取得了更多进展

“贵组织为简化安全环境而采取了或计划采取下列哪些措施？”



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员
来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

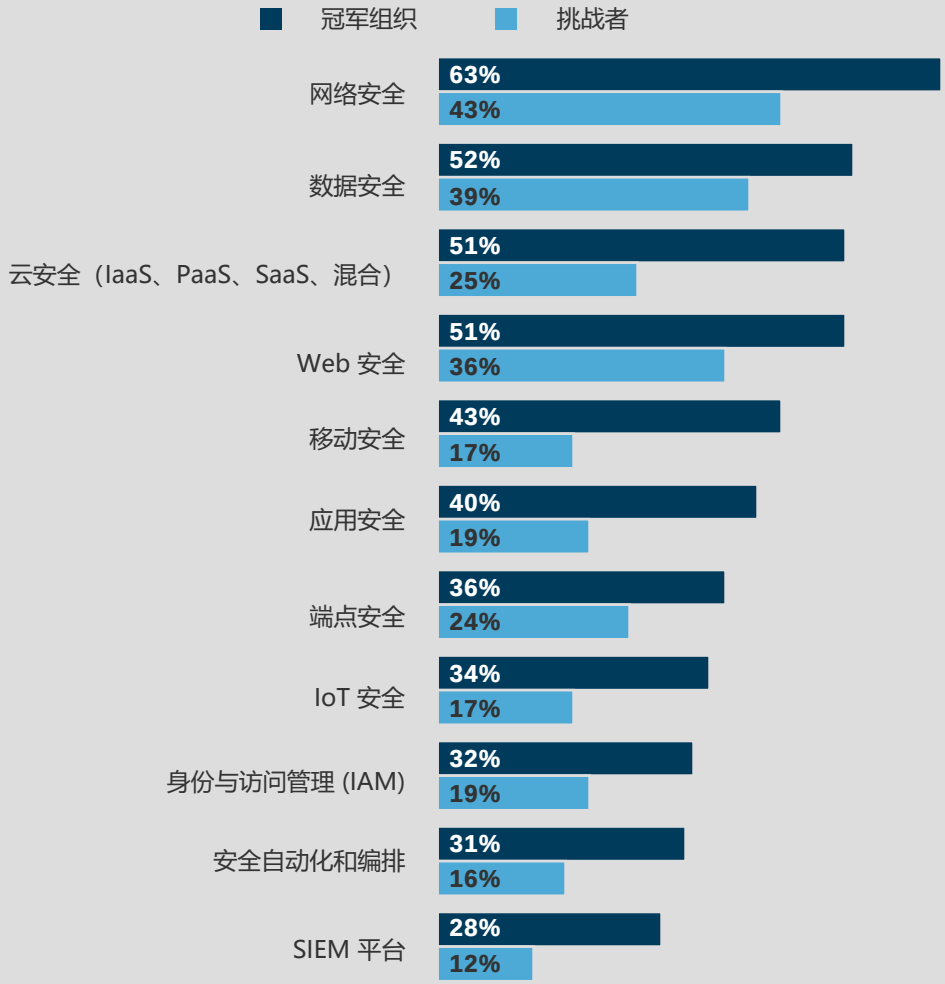
› **实现现有投资的价值最大化。**如果选择采用“光鲜亮丽”的新单点解决方案，而不是优化现有技术，可能会导致出现通过多个互不关联的工具来满足类似需求的情况。更有效的一种方法是寻找机会对较小的现有工具集进行重新改造和再投资，以最大程度地发挥其效用。[5] 冠军组织已经开始采用这种做法：63% 的冠军组织致力于减少其安全产品组合中的单点解决方案或供应商的数量，而在挑战者中，这一比例只有 36%。此外，冠军组织更有可能对重复性支出加以控制（66% 对 52%）。最后，冠军组织会从现有安全工具中发掘更多价值 - 他们对各种安全投资的利用率更高（见图 9）。

冠军组织更有可能将其管理软件整合到单个平台或供应商。

图 9：冠军组织会从现有安全投资中发掘更多价值

“贵组织在以下几个方面对安全技术的利用程度如何？”

（图中所示为“已完全优化 - 即我们会利用这些解决方案的全部或大部分可用功能）



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员

来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

FORRESTER

› **将管理整合到一个平台。**冠军组织更有可能将其管理软件整合到单个平台或供应商（63% 对 45%）。通过在统一平台中管理其安全资产，他们可以将不同的解决方案转变为一个紧密联系的安全套件。整合后的产品能够让安全团队更好地了解和控制其环境；他们还因此降低了管理单点产品的运营复杂性和成本，并为安全防御的自动化和编排奠定了基础。[6]

通过解决复杂性会使组织更具弹性

此次调研中一个特别有趣的发现是，冠军组织不仅能够提高效率，而且在保护公司免受网络安全威胁方面也更加成功。

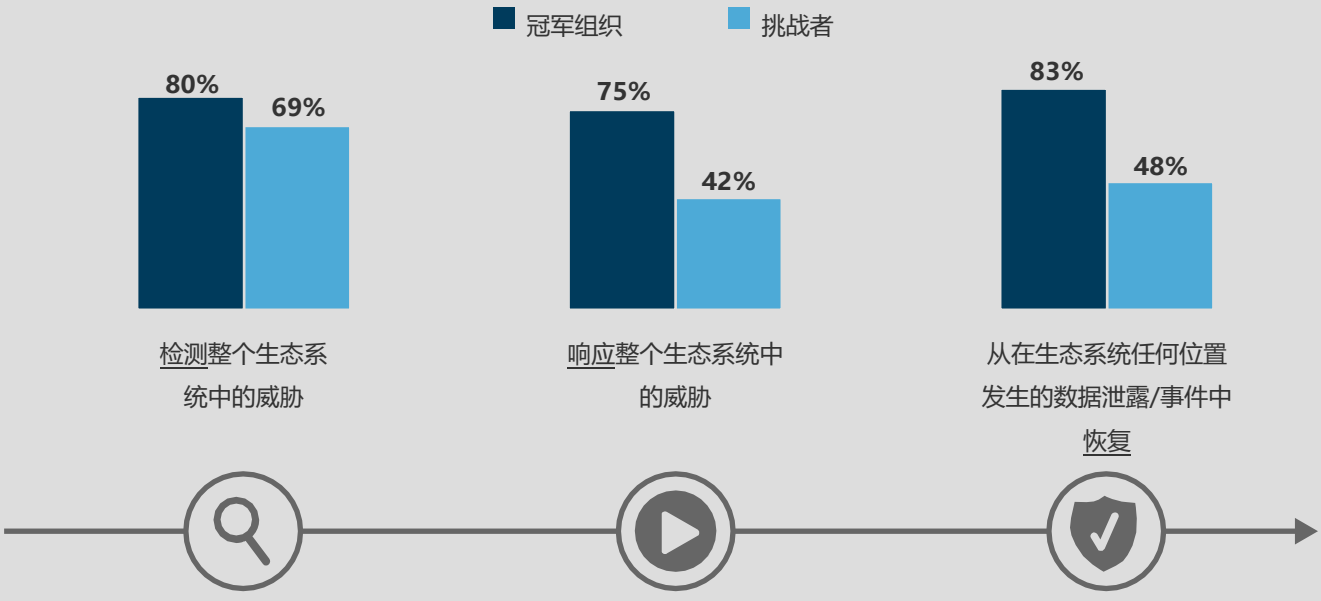
相比效率较低的同行，冠军组织更有可能对其安全产品组合在检测整个生态系统中的威胁方面的能力感到满意，而且他们也更有可能对其安全产品在响应安全事件并从中恢复的能力感到满意，两者在对这两方面的满意认可上分别相差了 33 和 35 个百分点。尽管冠军组织仍旧需要做更多的工作来克服复杂性，但是他们针对该问题所采用的方法（以此项投入为优先、实现现有投资的价值最大化以及将管理整合到单个平台上）使他们能够更好地为保护自己的组织免受安全破坏而做好准备（见图 10）。

冠军组织在检测和响应威胁以及从安全事件中恢复方面更加有成效。

图 10：冠军组织在威胁防范方面更具弹性

“您对贵组织所部署安全产品组合在以下各个方面为您所提供支持的满意程度如何？”

（图中所示为表示“完全满意”或“满意”的受访者）



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员

来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

FORRESTER

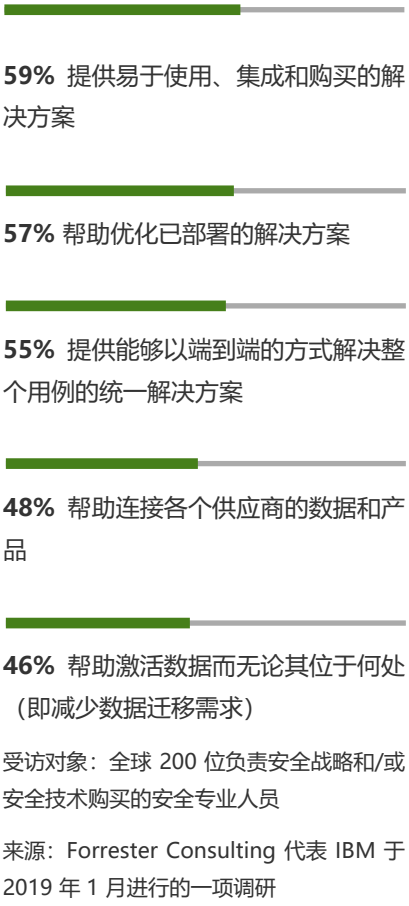
安全供应商在简化过程中发挥着重要作用

就其本身而言，许多组织在简化其安全生态系统方面的投入已取得了一些进展。不过，如果安全供应商不作出能支持此类投入的改变，那么他们看到的益处将会是短暂的。组织必须舍弃那些导致其陷入效率低下恶性循环的供应商。实际上，有 98% 的受访决策者希望他们的安全供应商提供降低复杂性方面的帮助。他们希望供应商提供具有以下特点的解决方案（见图 11）：

- **易于使用、集成和购买。**Forrester 通过之前的调研发现，安全领导者面临着人员和技能短缺的重大挑战。[7] 我们的此次调研也进一步证实了这一趋势：在我们的此次调研中，有 44% 的安全领导者表示人员短缺是他们在保护企业安全方面的关注点之一。采用过多集成不佳的技术只会加剧人力资本问题。这也使组织更难以解决这一问题：40% 的受访者表示技能短缺是他们简化环境的障碍之一。许多安全供应商正在开发兼顾易用性和简化控制的新平台。[8] 参与此次调研的安全专业人员对此类工具以及易于集成和购买的工具表示出了浓厚的兴趣。
- **可以优化并连接到已部署的解决方案。**安全决策者希望他们的供应商了解他们现有的安全格局。他们希望供应商扩展现有安全投资的价值，而且仅集成那些有助于其网络安全计划实现长期成熟的功能。这包括能够与其他供应商的产品无缝集成，而不是仅仅提供其产品组合中的既有功能。
- **无论数据存储在何处，均能够激活并连接数据。**随着数据的增长并散布到企业的每个角落，组织无法合理地将所有数据合并到一个集中的位置进行洞察和分析 - 至少无法在不产生大量成本的情况下做到这一点。安全团队已看到了可为其提供以下帮助的供应商的价值：无论数据存储在何处，均可帮助他们激活并连接数据，进而降低对昂贵、耗时且复杂的数据迁移项目的需求。

图 11：安全专业人员希望供应商支持其安全环境简化工作

“在降低安全环境复杂性方面，您希望您的供应商提供哪些帮助？”（请选择所有的适用项）



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员

来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

关键建议

在当今的安全格局下，复杂性已成为一个日益紧迫的问题；如果不加以解决，这一问题将会继续加剧。对于希望避免这种情况的安全团队而言，应将降低安全复杂性列为优先事项，并让其成为整个组织的重点。我们建议采取下述三个关键措施：

对功能进行整合，以专注于业务目标。限制单个解决方案的数量能够减少保持安全生态系统平稳运行所需的管理和维护量。寻找对现有解决方案进行再投资和变革的方法，可以帮助组织控制人员的增加并提高 ROI。

减少数据孤岛，以减少安全团队所遇到的阻力。无法将安全、信息技术和应用数据集成在一起的公司，将无法获得就安全事件的潜在后果做出快速、准确决策所必需的信息。组织对复杂性的关注程度越高，作为症结出现的孤岛式数据就越多。可帮助安全团队接收和分析不同数据源的工具和技术，将能够帮助他们采取果断行动。

简化您的生态系统，以增强响应和恢复能力。通过经简化的安全产品组合的确能够合理地改善威胁检测能力，但我们发现，简化更有助于提升组织响应事件及从事件中恢复的能力，无论事件发生在客户生态系统中的哪个位置。如果安全领导者也认可这一点的话，那么响应和恢复必定会成为其重点关注的领域。简化安全性是实现这一目标的不二法门。

FORRESTER

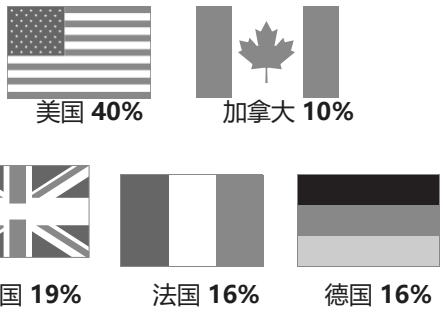
附录 A：方法

在此次调研中，Forrester 对 200 名负责或影响其所在组织安全战略和/或技术购买决策的安全专业人员进行了在线调查。受访者来自美国、加拿大、英国、法国和德国至少拥有 500 名员工的组织。此次调研评估了组织安全技术组合的状态以及复杂性对其所用技术的有效性产生的影响程度。向参与调研者提出的问题主要调查了推动其安全战略的主要目标、不利于他们实现成功的挑战、他们在安全简化方面所采用的策略，以及他们期望通过安全资产和资源优化实现的价值。

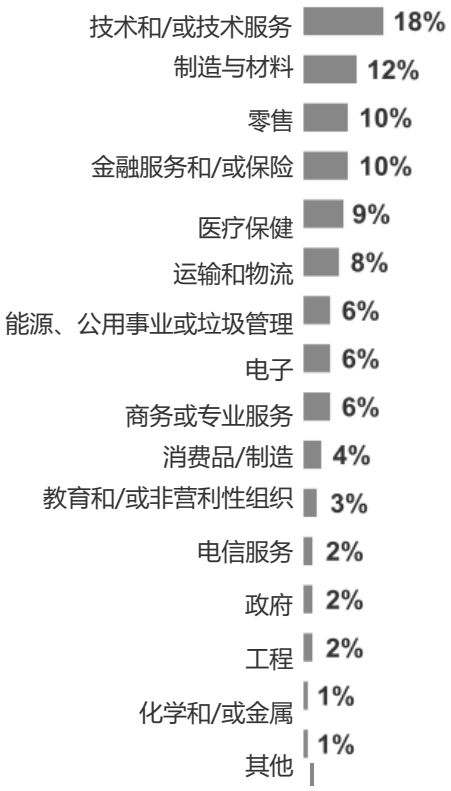
有一些小奖励给到了受访者以答谢他们为本次调研付出的时间。此次调研于 2018 年 12 月开始，并于 2019 年 1 月完成。

附录 B：人口统计数据

国家/地区



行业



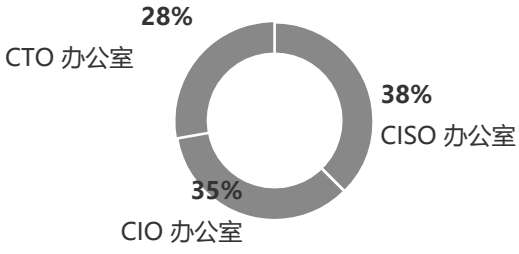
资历

30% 首席高管
11% 副总裁
60% 主管

员工数量

40% 500~999 人
36% 1,000~4,999 人
16% 5,000~19,999 人
10% 20,000 人或以上

部门



受访对象：全球 200 位负责安全战略和/或安全技术购买的安全专业人员
注：由于进行了舍入，因此百分比总和可能不是 100%。
来源：Forrester Consulting 代表 IBM 于 2019 年 1 月进行的一项调研

FORRESTER

附录 C：尾注

[1] 来源： “Security Budgets 2017: Increases Help But Remain Reactionary”，Forrester Research, Inc.，2016 年 11 月 23 日。

[2] 来源： “The Top Security Technology Trends To Watch, 2017”，Forrester Research, Inc.，2017 年 4 月 26 日。

[3] 来源： “The Top Security Technology Trends To Watch, 2017”，Forrester Research, Inc.，2017 年 4 月 26 日。

[4] 来源： “Security Budgets 2019:The Year Of Services Arrives”，Forrester Research, Inc.，2018 年 12 月 17 日。

[5] 来源： “Security Budgets 2019:The Year Of Services Arrives”，Forrester Research, Inc.，2018 年 12 月 17 日。

[6] 来源： “The Zero Trust eXtended (ZTX) Ecosystem”，Forrester Research, Inc.，2018 年 1 月 19 日。

[7] 来源： “The Zero Trust eXtended (ZTX) Ecosystem”，Forrester Research, Inc.，2018 年 1 月 19 日。

[8] 来源： “The Zero Trust eXtended (ZTX) Ecosystem”，Forrester Research, Inc.，2018 年 1 月 19 日。