CISCO
SECURE

安全成果研究

第 2 卷

极致践行 “五强” 安全做法

目录

再次推广“五强”安全做法

2021 年思科安全成果研究旨在评估网络安全管理中最重要的问题。为此，我们研究了 25 种一般安全做法，并测试了每种做法与实现 11 项计划级成果的关联。您可以访问 2021 年思科安全成果研究网站，以交互方式直观查看这些做法和成果间的关联 ，或下载完整报告。

在测试中，综合所有进行评估的成果，我们发现，25 种做法中有 5 种表现突出，它们对安全计划成功的总贡献非其他做法能及，以下我们将这 5 种安全做法称为“五强”。

在接下来的篇幅中，我们将重点探讨助推安全计划成功的“五强”驱动因素，以确定有助充分发挥“五强”效力的战略。“五强”安全做法包括：

积极更新技术	组织制定积极更新技术的战略，以紧跟现有的最佳 IT 和安全技术。
充分集成技术	各种安全技术充分集成并实现协同增效。
及时响应事件	提升事件响应能力，以及时有效地针对安全事件进行调查和补救。
准确检测威胁	提升威胁检测能力，以准确地感知潜在的安全事件，消除明显的盲点。
迅速从灾难中恢复	提升灾难恢复能力，以最大限度地减少灾难影响，并确保提高受安全事件影响的业务职能部门的弹性。

这些做法的广泛成效有目共睹，也由此引发一个问题：“为什么它们这么有效？”是什么让它们成为解锁成功的关键？哪些因素会提高或降低它们的效力？公司应如何实施这些做法以实现最大成果？以上都是我们在本期安全成果研究中想要探讨的问题。

在接下来的篇幅中，我们将重点介绍促使安全计划成功的“五强”驱动因素，来确定最大限度发挥“五强”效力的战略。为此，我们对全球 5,100 多名 IT 和安全专业人员展开了独立的双盲调查。我们深入挖掘数据，提取重要发现，并分享经过审查的可靠要点，希望借此帮助您的组织攀登安全成就新高峰。

主要研究结果

我们向 27 个国家/地区的 5,100 多名 IT 和安全专业人员询问了其组织如何更新和集成安全架构、检测和响应威胁，以及在灾难来袭时保持弹性。正如您所料，他们积极分享了广泛的内容，包括洞察、困难、战略和成功经验。我们以多种方式分析了每个回应，并提炼出以下主要调查结果。

更新和集成架构

- 相比于任何其他安全做法或控制措施，现代化、充分集成的 IT 更有助于促成总体计划成功。
- 较新的云架构更容易定期更新，跟上业务发展的步伐。
- 主要从单一供应商采购产品的组织，其构建集成技术系统的机会将翻倍。
- 集成安全技术实现高水平流程自动化的可能性是非集成技术的 7 倍。

检测和应对网络威胁

- 基于强大的人员、流程和技术构建的安全运维 (SecOps) 计划，其性能比基于较弱资源的计划提高 3.5 倍。
- 外包检测和响应团队通常给人以更卓越的印象，但事实上内部团队的平均响应时间更快（内部：6 天；外部：13 天）。
- 大量使用威胁情报的团队具有出色检测和响应能力的可能性是较少使用威胁情报的团队的两倍。
- 自动化可将经验不足的人员的绩效提高一倍以上，使实力雄厚的团队几乎必定（95% 的几率）可以成功实现安全运维。

在灾难来袭时保持弹性

- 对业务连续性和灾难恢复实施董事会级监督的组织，最有可能制定强有力计划（比平均水平高 11%）。
- 在业务连续性和灾难恢复能力覆盖至少 80% 的关键系统之前，保持业务弹性的可能性无法提高。
- 定期以多种方式测试业务连续性和灾难恢复能力的组织，其保持业务弹性的可能性比一般组织高 2.5 倍。
- 制定混沌工程标准做法的组织，其实现高水平弹性的可能性是一般组织的两倍。

调查简介

抽样	受访者	分析
思科与调查研究公司 YouGov 签订了合同，在 2021 年年中开展了采用分层匿名随机抽样技术的完全匿名调查。	来自 27 个国家/地区的 5,123 名在职 IT、安全和隐私专业人员参与了调查。附录列出了抽样调查对象特征统计数据。	Cyentia Institute 代表思科对调查数据进行了独立分析，并生成本研究报告呈现的所有结果。

5,123 名在职 IT、安全和隐私专业人员参与了调查，他们来自 **27** 个国家/地区

“我们需要确保自己正在竭尽全力实施全方位保护。我们知道攻击者有多高明，他们每天都在不断演进，每天都会推出新的伎俩。我们希望有力保护设备、用户和公司的安全，因此想要减少任何可能的安全漏洞，有效缩小受攻击面。”

Eric J. Mandela，Allied Beverage Group 技术基础设施助理总监

了解详情

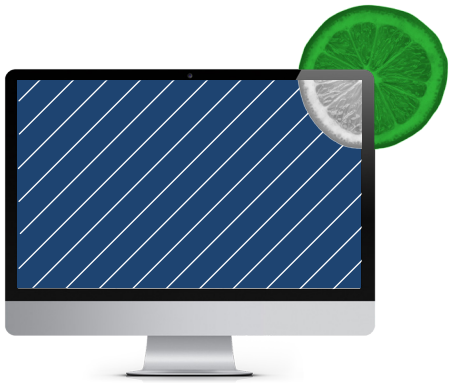
积极更新技术的战略

我们之前的研究发现，积极更新和维护最佳的 IT 和安全技术，对网络安全计划成功的贡献比任何其他做法都突出。考虑到我们测试的所有 25 种做法本身已经被广泛接受为 “最佳做法”，积极更新技术的做法能独占鳌头，实属不易。因此，我们希望在后续研究中深入探究为什么这一做法成效惊人。

在更深入地了解技术更新战略之前，我们先快速了解一下现有基础设施的更新状况。我们询问受访者，在他们目前使用的安全技术中，已经过时的技术占比多少。平均而言，组织使用的 39% 的安全技术被视为已过时。近 13% 的受访者声称，他们使用的 10 种安全工具中至少有 8 种已经暴露出老化的迹象。

仅此一个事实，就可以解释我们从积极技术更新战略中观察到的许多益处。从表面上看，更新的技术带来了高级能力，可以抵御不断演变的大量网络威胁。但实际远不止于此，我们可以继续基于数据深入探讨问题。

平均而言，组织使用的 39% 的安全技术被视为已过时。



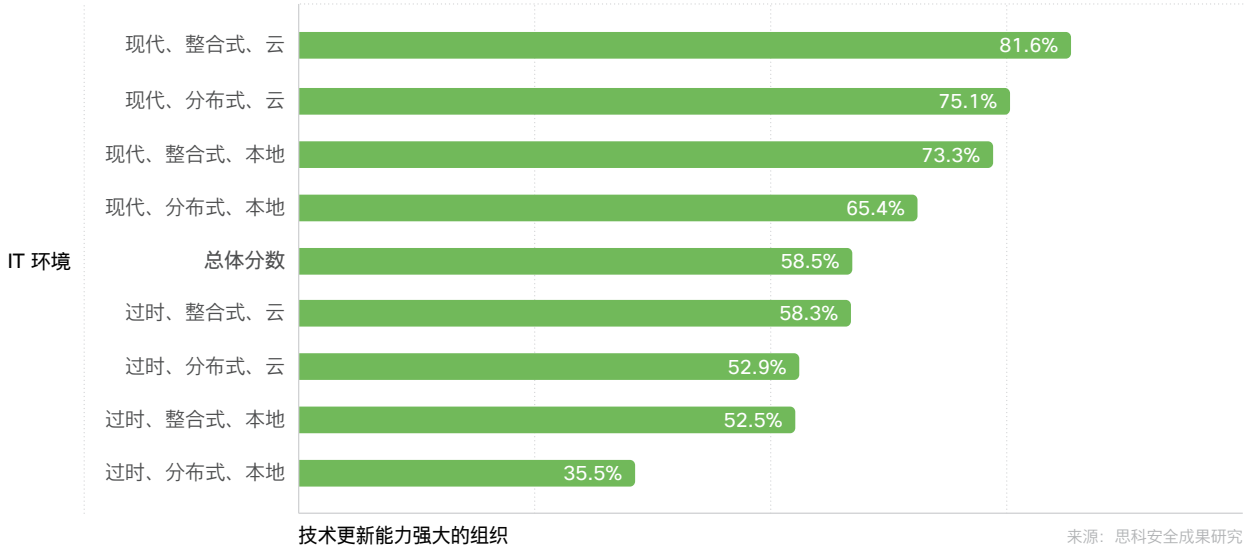
基础设施特征是否影响更新计划？

在最初的研究中，我们推测更现代的云架构可能更有效，因为它们更易于管理，并且内置了原生安全措施。为了验证该假设，我们要求受访者通过选择一组分级的描述语来大致描述他们的技术基础设施，包括：

- 云与本地部署
- 现代与过时
- 整合式与分布式

这些不同的架构特征是否有助于提高技术更新能力的功效？根据图 1，答案非常肯定。**与使用过时分布式本地部署技术的组织相比，拥有现代整合式云架构的组织，其具有强大技术更新能力的可能性是前者的两倍以上。**但是不要急于用这张图指导您的云迁移战略。请注意，主要采用本地环境的组织在实现 IT 现代化之后，表现也仍然超过平均水准。

云原生技术固然可以让技术更新战略更轻松地摆脱束缚，但这里更急迫的问题是技术过时与否。当更新陈旧的基础设施成为一场攻坚战时，与继续更新相比，您可能会从直接迁移到新架构中取得更显著的进展。当然，对于传统或关键基础设施而言，迁移到新架构并不总是可行或具成本效益的做法，但这个一般原则仍然适用。



来源：思科安全成果研究

图 1：IT 架构特征对技术更新表现的影响

81.6% 拥有现代整合式云架构的组织具有强大的技术更新能力

频繁更新是否有助于安全跟上业务发展的步伐？

根据 2021 年思科安全成果研究，与积极更新技术战略最密切相关的成果是，使安全计划能够跟上业务的需求和增长。事实上，这是整个研究中安全做法和成果关联性最强的组合。

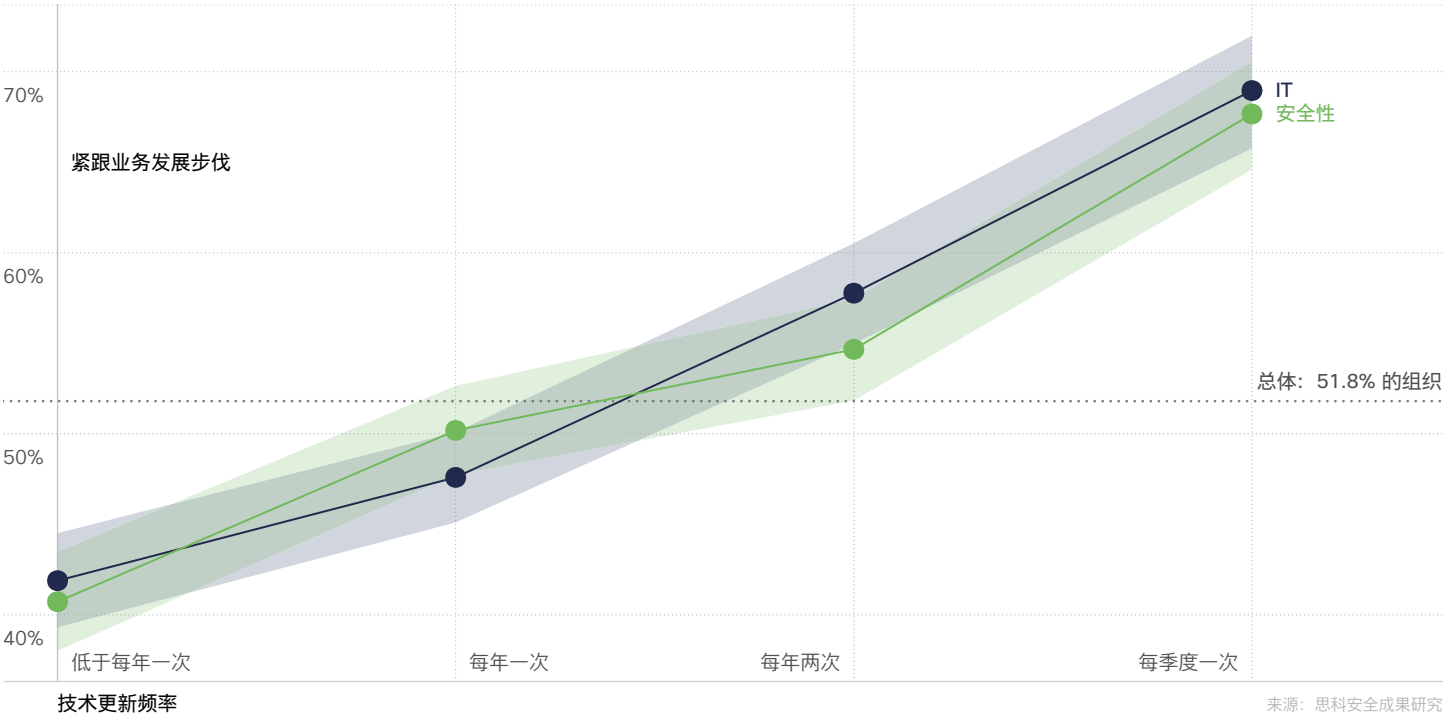


图 2：技术更新频率对安全计划紧跟业务发展步伐的能力的影响[1]

我们向各组织询问了 IT 和安全升级的频率，并将这些回复结果与其安全计划紧跟业务发展步伐的能力进行了比较。两者之间是否存在关系？是的，它们确实存在关系。我们发现，随着升级节奏加快，安全计划推动业务发展这一关键成果也在稳步改善。**总体而言，与每隔几年升级一次的组织相比，每季度升级 IT 和安全技术的组织更有可能跟上业务的发展步伐（可能性高出 30%）。**“与时俱进，勇往直前”，对于重压之下的 IT 团队来说，这是个很好的激励口号。

[1] 在整个报告中，我们将使用特定安全做法或成果的“总体”值标记各个数字。此值代表所有受访者对一组特定问题的回复结果的平均值。提供此值是为了供您参考，帮助您了解哪些组织的成绩超过平均水平，哪些没有达到标准。我们还在一些图表上通过误差线或阴影区域显示不确定性。当阴影区域与“总体”线重叠时，这表明我们无法推断安全计划的特定方面对我们正在研究的成果或做法是否有任何影响。

技术更新应该由哪些因素或人员推动？

我们已经确定的是，经常升级有助于实现业务发展，然而技术升级应该由哪些因素或人员来推动呢？我们要求受访者选择其组织更新安全技术的主要驱动因素，他们的回答分为三大类：

- **供应商驱动：**计划由 SaaS 提供商决定，或者作为大型供应商整合计划的一部分（最常见的驱动因素）
- **主动升级：**按照预先确定的计划，或者当新功能或使用案例需要升级时（其次常见的因素）
- **被动升级：**响应事件、技术过时或满足合规性要求（最不常见的因素）

这些驱动因素本身很值得研究，不过我们真正想知道的是，这些驱动因素是否与更有效的技术更新方法有关。答案在图 3 中可以找到，它基本上表明，当供应商主导或至少积极参与更新时，技术更新计划更加成功。**在采用被动方法的企业中，只有不到一半的企业被报告具有强大的更新能力，而在保持与供应商更新周期同步的企业中，有近三分之二被报告具有同等能力。**

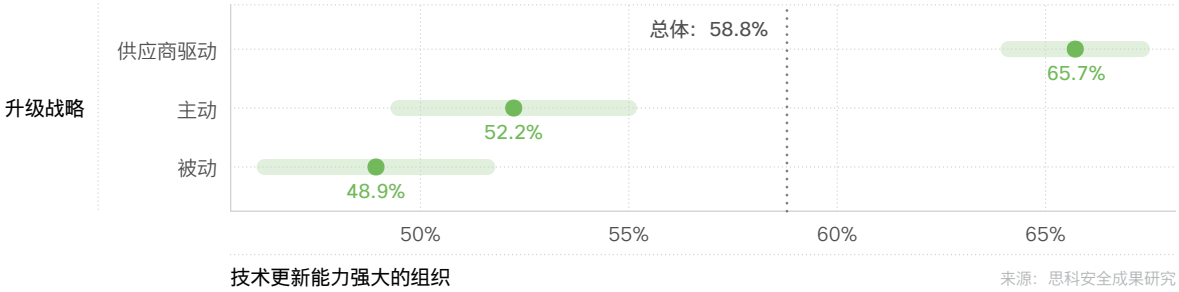


图 3：升级的主要驱动因素对安全技术更新性能的影响

我们知道，这一切听起来像是 IT 和安全产品供应商的自我宣传，确实让人存疑。但实事求是地说，我们没有对这一调查结果施加任何影响。这项调查是由一家独立的知名研究公司完成的，受访者并不知道思科赞助了这项调查，数据分析也是由业内享有盛名的 Cyentia Institute 负责的，这才最终得出图 3 的结果。而且，我们在解释这些结果时，格外谨慎。

我们认为，供应商驱动的做法可提高技术更新能力的原因，大部分与云/SaaS 架构能够更友好地支持频繁升级有关。我们还应注意，这可能不仅仅是因为供应商的出色表现，更可能是因为供应商的参与，让技术更新计划摆脱了组织内部障碍和政治困境。

用歌手 Rob Base 和 DJ E-Z Rock 的歌词来形容，就是“成功需要两人携手。腾飞需要两人合力。”他们的说法完全适用于安全领域！借助技术解决方案合作伙伴的惯性力量来推动安全任务成果，让您的更新战略展翅高飞。

65.7% **与供应商更新周期保持同步的组织拥有强大的技术更新能力**

升级功能还是兼容性？

在前一部分，我们介绍了哪些场景会促使组织升级技术，接下来我们将了解他们如何在众多解决方案中做出选择。图 4 展示了受访者告知我们的选择标准。首选标准是能与现有技术无缝集成，其次是提供同类最佳功能或满足特定需求的解决方案。也许有点出乎意料的是，最大限度地降低成本是排在末位的考虑因素。

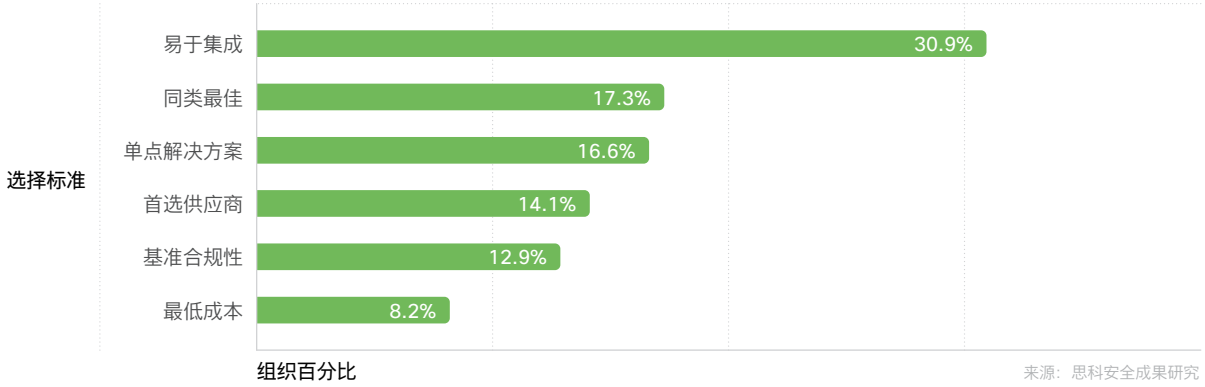


图 4：更新安全产品时的主要选择标准

这一切听上去都言之有理，但是这些标准对构建成功的安全计划是否重要？为了回答这个问题，我们将图 4 中的选择标准分为三类：

- **最低：**最低成本的解决方案；实现基准合规性
- **易于集成：**与现有技术集成；使用首选供应商
- **功能：**同类最佳；单点解决方案

然后，基于每个组织在 11 项安全成果方面的成就，我们给出了其总体得分，并以这些得分为基准测试了以上标准类别。分数的绝对值没有特别含义，但它提供了比较不同技术更新战略的参考点。**如图 5 所示，与基于最小化成本或满足基准合规性要求来选择产品相比，优先考虑集成和功能更能推动安全成果。但是，以集成为主导的方法是明显优于平均水平的唯一方法。**

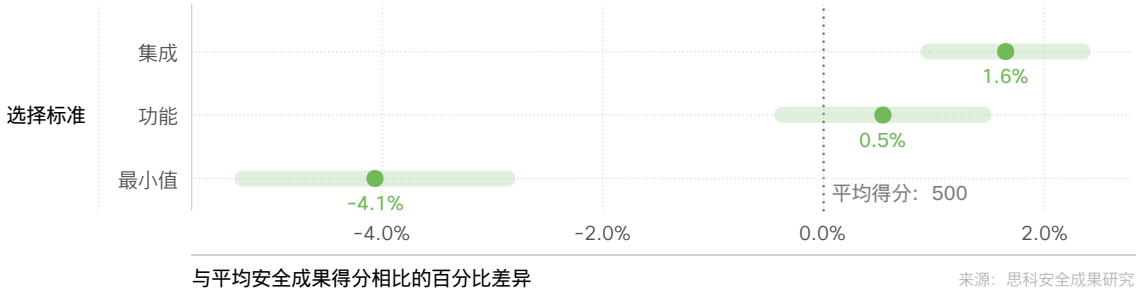


图 5：技术选择标准对总体安全成果得分的影响

请注意，若以总体计划的成功为衡量标准，各类选择标准的结果差异非常小。我们在这里看到的可能只是一扇窗口，供我们了解安全计划中更广泛的优先考虑因素和做法。但这确实表明，一些更温和的问题值得考虑，例如我们为什么选择一种产品，而不是另一种？此外，如果您在更新或升级安全解决方案时难以对功能的优先级进行排名，您可以将其作为合理的理由来推动兼容性和功能，而不是将成本降至最低。

安全成果得分是多少？

我们向受访者了解其组织在 12 项不同的安全计划成果中所取得的成就水平。思科安全成果研究的第一版对此进行了详细分析，您会看到，在本研究中也对其中一些成果进行了单独研究。不过，我们还是希望给出一个总体分数，以记录每个组织在所有 12 项成果中的成就水平，以此衡量安全计划的总体表现。我们将这个分数称为“安全成果得分”，您会在本报告中看到这一称呼被多次引用。

我们使用了一种名为“项目反应理论”的高级统计技术来计算此得分。凭借此技术，我们能够根据组织在实现所有成果时的表现为其评分，同时考虑获得不同成果的难度不一这个事实。这种经过验证的技术也用于给出我们熟悉的标准化测试分数。分数的绝对值没有特别含义，但它确实提供了比较各种安全计划的参考点。

“首席信息安全官必须同时是影响者和教育者。若要最大限度提高效率，我们需要在组织的战略决策过程中处于领导地位。但是，当我们试图说服他人重视安全性、通过适当的投资真正实现安全性，以及亲自参与业务的各个方面时，我们还必须承担教育责任。由于公司高管普遍缺乏安全方面的背景知识，因此我们需要时刻让他们了解每个决策所引入的风险类型。”

Helen Patton，思科咨询首席信息安全官 @CisoHelen

在我们引人入胜的“安全故事”播客中，倾听 Helen 讲述 CISO 不断演变的角色：

实现充分集成的安全技术

根据我们上次的安全成果研究报告，当充分集成的安全技术与范围更广的 IT 基础设施有效协同发挥作用时，所有安全计划都更有可能取得成功。因此我们提出了一系列问题，旨在从安全技术集成背后的意图开始，深入挖掘这一备受称赞的不凡举措的驱动因素。

受访者称，集成安全技术最常见的驱动因素是提高监控和审核的效率。这引起了我们的共鸣，因为我们深知，当组织为了全面洞悉整个网络的实时状态，而不得不检查不计其数的控制台或控制面板时，他们会感到多么抓狂和沮丧。更轻松地进行协作和自动化也是集成安全技术的常见驱动因素（有关自动化的更多信息详见下文）。我们根据报告的技术集成水平和安全计划成果，对这些驱动因素进行了测试，但发现两者的关联性并不强。在集成安全技术时，或许“是什么”或“如何做”比“为什么”更重要？让我们在下面的问题中再着重分析这一点。

受访者称，集成安全技术的最常见动机是提高监控和审核的效率。

购买或构建充分集成的技术？

以前的研究告诉我们，集成安全技术可以推动安全成果，但是实现高度集成的技术系统的最佳方法是什么？购买现成的解决方案？构建适合需求的解决方案？放任自流？让我们看看是否能找到答案。

我们询问各组织他们在安全技术集成方面的典型方法，图 6 列出了答案。**总体而言，超过四分之三的组织宁愿购买现成的集成解决方案，也不愿自行构建。**其中超过 40% 的组织选择那些可以“开箱即用”地集成到其现有基础设施中的技术。超过 37% 的组织则更进一步，他们更愿意从单一供应商处采购解决方案，以更好地实现原生集成，或成为更大平台的一部分。略高于 20% 的受访者愿意自行构建集成方案，前提是产品符合其需求。很少有人采取放任自流的方法。

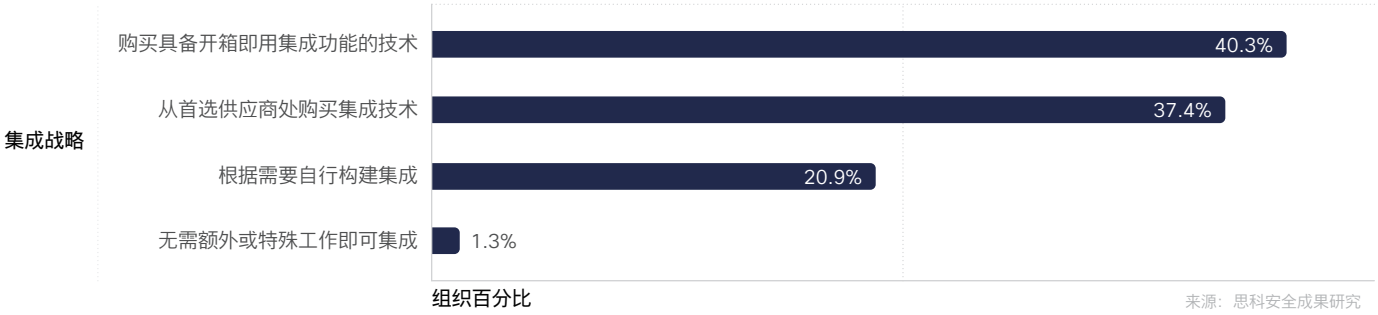


图 6：所有组织采用的常见安全技术集成方法

总体而言，超过 3/4 的组织宁愿购买现成的集成解决方案，也不愿自行构建

图 7 评估了其中任何一种集成方法是否带来差异。在这里，我们再次看到同样的主题浮现，提醒我们与供应商合作，以保持技术现代化和充分集成的优势。**从图表中可以看出，坚持使用首选供应商的组织获得充分集成的安全技术的可能性是采取放任自流方法的组织的两倍以上（~69% 比 ~31%）。**此外，根据我们的研究，这一发现在所有规模的组织中都适用，不过中小企业从使用首选供应商中获得的益处比大型企业略高。

我们意识到，这听上去又像是可疑发现，因为它来自我们这个拥有大量集成安全产品组合的公司。看到这个结果与思科的战略不谋而合，我们确实感到十分欣喜，不过，这的确是一项双盲研究，思科绝对没有在幕后操纵任何结果。

毫不奇怪，不做任何额外工作来集成安全技术的组织变成了一个自我应验的预言，安全性每况愈下。**但是，我们确实预计到了，有些人会惊讶地发现，购买开箱即用的集成产品与自行构建的集成产品之间在成果上几乎没有区别。**在使用这些方法的组织中，只有不到一半（约 49%）的组织报告了强集成水平。

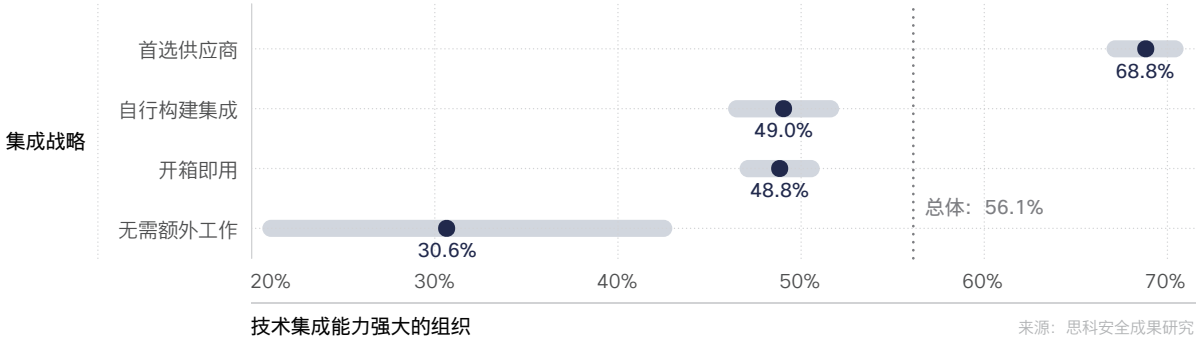


图 7：常用集成方法对安全技术集成水平的影响

云带来更多集成机会

我们已经知道，许多组织正在纠结是否开始或扩大他们在云或本地环境中的安全技术集成工作。如果您也处于这样的困境，我们会提供一些数据来帮助您进行评估。好消息是，许多受访者表示在本地和云环境中都取得了不俗的效果。即便如此，在云中实现强大的技术集成应该容易得多。

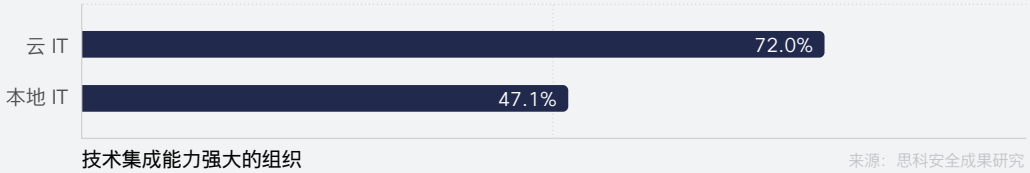


图 8：云环境与本地环境对安全技术集成水平的影响

集成是否有助于自动化？

回顾本节开头，我们知道自动化并不是技术集成的最常见动机。但是，44% 的组织确实将其视为一种额外激励。抛开动机不谈，是否有证据表明，充分集成的技术确实可以实现更高水平的安全流程自动化？图 9 中展示的证据表明，情况确实如此。

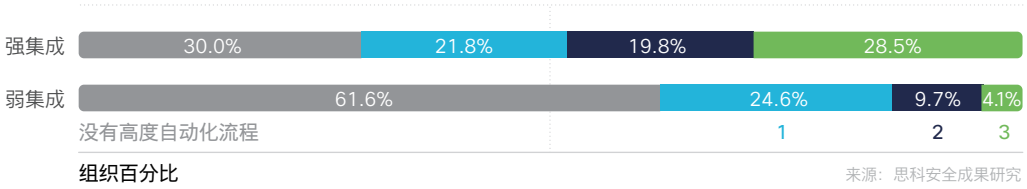


图 9：技术集成对安全流程自动化程度的影响

图 9 所示的两个横条根据安全技术集成的水平（强或弱）来区分组织。彩色分段表示成熟的自动化支持的主要安全流程（事件监控、事件分析和事件响应）的数量。在集成较弱的组织中，没有自动化流程的组织的比例是强集成组织的两倍以上。**相反，拥有充分集成的安全技术的组织实现这 3 个安全流程自动化的可能性要高出近 7 倍（4.1% 比 28.5%）。**听起来，自动化确实是一种有吸引力的动机！

哪些功能应该集成？

接下来，我们询问了受访者他们在支持 NIST 网络安全框架 (CSF) 5 大核心功能的技术方面的集成水平。他们的回答范围很广，从高度分散（孤立技术多数时候孤立地工作）到高度集成（协调技术作为一个功能单元运行）。然后，我们创建了一个模型来确定这对每个组织的总体安全成果得分的影响。

图 10 展示了结果在 5 大核心功能中相当一致。**通过在任何 NIST CSF 功能区域的去碎片化和集成努力，组织可以相应增加其安全计划的成功率（增加 11% 到 ~15%）。**因此，关于本节标题提出的应该集成哪些功能的问题，答案是 “全部功能”。但是，如果您不知道从何处着手，高度集成的 “识别” 功能会推动最大的提升。

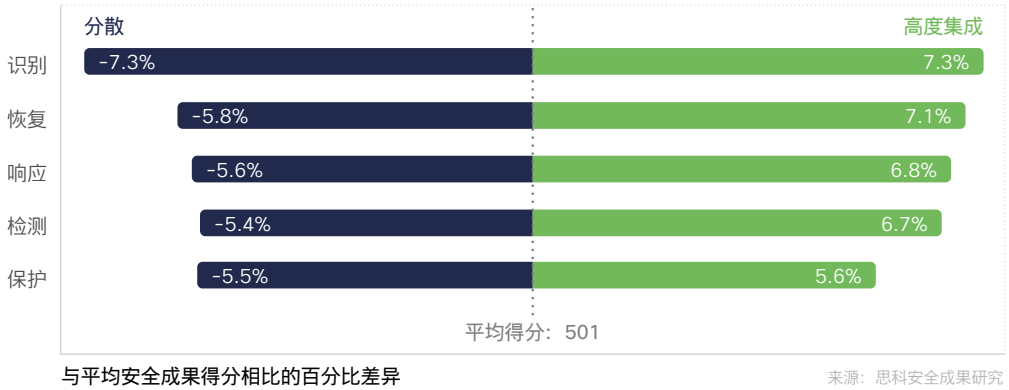


图 10：集成 NIST CSF 功能对总体安全成果得分的影响

显而易见，集成全部功能和我们上一节中了解到的监控、审核和协作是集成技术的最强驱动因素，这两者之间存在联系。总之，它们似乎都支持这样一个主张：在整个企业中提供良好可视性至关重要。毫无疑问，以分散的方式来“发展组织层面的洞察力，以管理系统、人员、资产、数据和功能面临的网络安全风险”（CSF 表述）不会获得理想结果。我们在进入“威胁检测和事件响应”部分时，会进一步加强阐述这个主张。

关于集成、识别和信息

除了我们刚刚讨论的图表之外，本研究收集的数据始终指向集成、识别和信息之间的关键联系。如果您无法识别资产或威胁，您就不会知道它们的存在，因此也无法给予足够关注并建立起明智的防御，直到为时已晚。

图 11 很好地说明了这一概念。我们将每个组织在 NIST CSF “识别” 功能中报告的集成水平与其及时准确检测威胁的能力进行了比较。**利用高度集成系统以识别关键资产及风险的组织具备更强大的威胁检测能力（高出 41%）。**因此，对抗碎片化和对抗网络威胁实际上是两个并驾齐驱的目标。

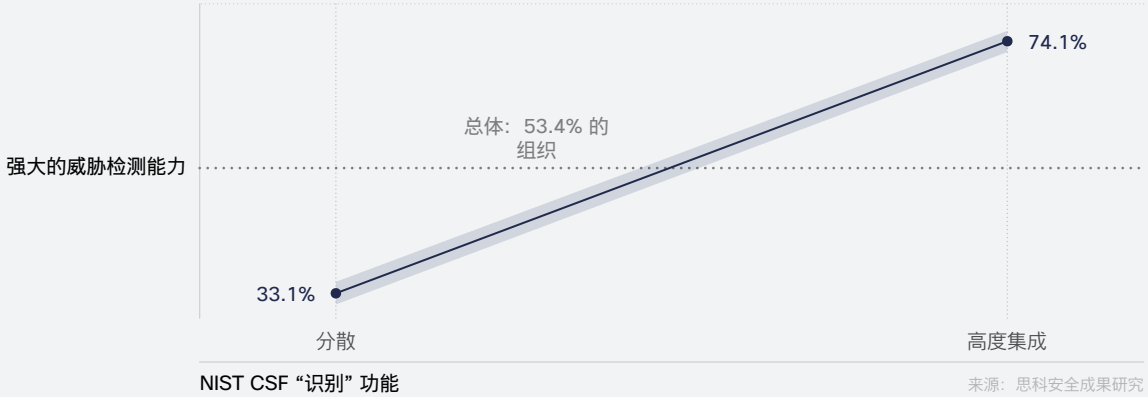


图 11：集成 NIST CSF 识别功能对威胁检测能力的影响

利用高度集成系统识别关键资产及风险的组织，其具有高出 **+41%** 的威胁检测能力

“自动化使我们的工程师能够及时应对新威胁。我们现在可以专注于正确理解安全概念，而不是一直更新相关规则和全天候监控网络。思科深入研究繁杂的数据并提取我们需要的信息，使我们能够更好地保护和维护基础设施。他们的产品实现了机器和人类智能的完美结合。”

Steve Erzberger，Frankfurter Bankgesellschaft (Schweiz) AG
首席技术官

了解详情

提升威胁检测和事件响应能力

本部分涵盖两个独立的安全做法领域，这两个领域分别在 “五强” 安全做法中独当一面。但是，由于威胁检测和事件响应 (IR) 通常在安全运维 (SecOps) 这个整体范畴下共享人员、流程和技术，因此我们在两个领域里提出了一系列共通的问题。因此，我们可以在本研究的同一部分中一起分析两者。

几乎所有（约 92%）拥有强大的人员、流程和技术的组织都实现了高级威胁检测和响应能力。

如何确定人员、流程或技术的优先级？

接下来，我们将对人员、流程和技术（亦称 p-p-t 三要素）进行详细分析。安全功能通常被描述为这三个要素的组合，特别是在威胁检测和事件响应领域。但是，该安全“三位一体”中的任何一个，是否比其他要素更关键？看看我们的详细分析吧。

从图 12 的底部开始，我们可以看到，有些组织的安全计划在所有三个要素方面都缺乏实力，其中只有四分之一对安全运维表示有信心。在人员、流程或技术中的任一领域获得优势，就能将这一比例提高到约 60% 至 64%，具体取决于所属领域。强大的人员似乎带来一点优势，但重叠的置信区间提醒不要我们过分夸大这个事实。重要的启示是，所有这些都为构建更优秀的检测和响应能力提供了良好的起点。

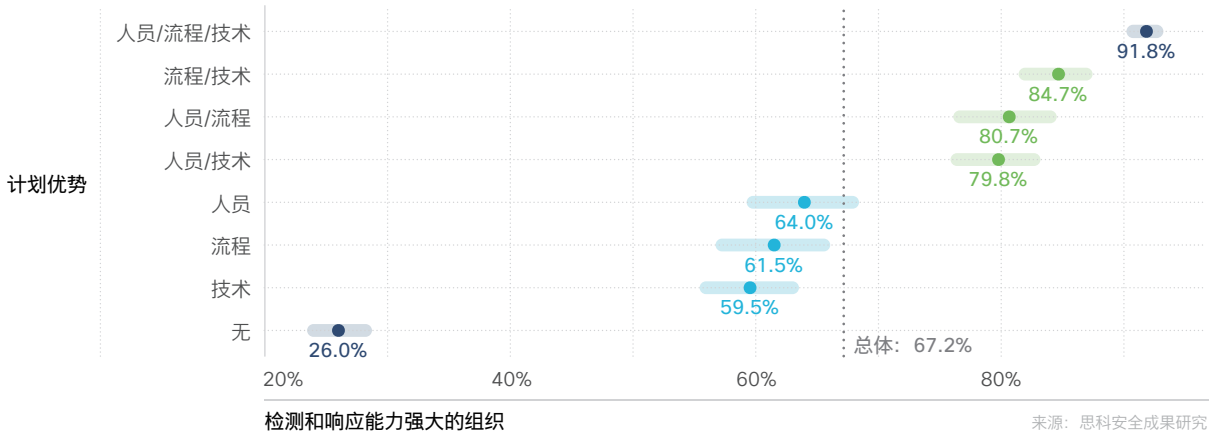


图 12：出色的人员、流程和技术对威胁检测和事件响应能力的影响

让我们继续看图 12，做好三件事中的两件能使安全运维计划的水平稳步高于平均水平，与仅做好一件事相比，能力可提高大约 15% 到 20%。再次强调，人员、流程和技术如何配对并不重要。您只需要加强任意两个方面的优势。因此，知道在制定您组织的安全运维路线图时可以享有一些自由选择，这是个好消息。

现在，让我们来看看图 12 展示的精英计划，它们成功实现了安全运维“三连胜”。**几乎所有（约 92%）拥有强大人员、流程和技术的组织都成功实现了高级威胁检测和响应能力。**与没有任一领域优势的安全运维计划相比，这相当于功效提高了 3.5 倍！因此，您的组织应该从最容易取得进展的地方开始，但不要停止，直到抵达人员、流程和技术的顶峰。

拥有强大的人员、流程和技术的组织，其威胁检测和响应能力获得了 **3.5 倍** 的提升（相较于在所有这些方面缺乏优势的普通组织）

零信任和 SASE 是否能助力实现更出众的安全运维？

我们明白，很难使用 “强大的技术” 等抽象描述在上述发现的基础上形成具体结论。因此，我们提出了一些有关特定架构的后续问题。我们调查受访者关于采用零信任和安全访问服务边缘 (SASE) 的方法，以便更好地了解这些方法如何影响威胁检测和事件响应能力，进而影响安全计划成果。

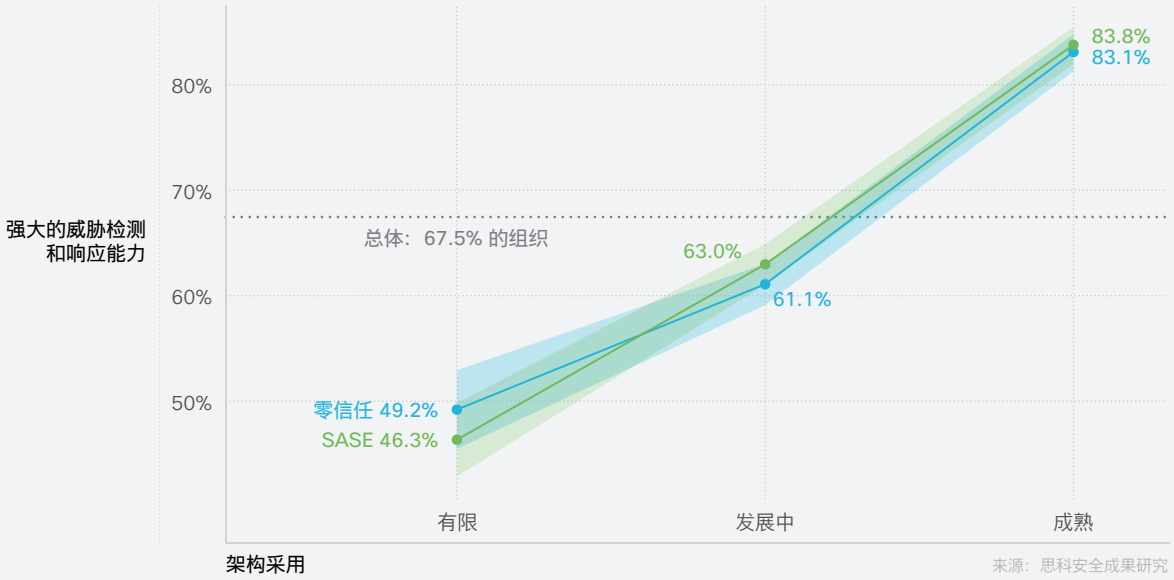


图 13：零信任和 SASE 架构对威胁检测和事件响应能力的影响

声称部署了零信任或 SASE 成熟实施的组织具有强安全运维的可能性比部署新生实施的组织高 35% 左右。这些结果证实了我们之前分享的关于现代架构可以为网络安全计划带来诸多优势的证据。

更多人员是否意味着更少麻烦？

我们知道，优秀人员对于构建强大的威胁检测和事件响应能力不可或缺。但是，我们应该专注于增加员工，还是提高员工的技能？显然，这两者不一定非此即彼，不过在组建成功的安全运维团队方面，究竟有没有证据证明两者孰轻孰重？

为了回答这个问题，我们首先计算了所有组织的安全运维员工与总员工的比例。然后，我们将该比例与组织声称的检测和响应能力强度进行了比较。图 14 显示了这些计算的结果，虽然它没有完全回答数量或质量问题，但确实提供了一些启示。

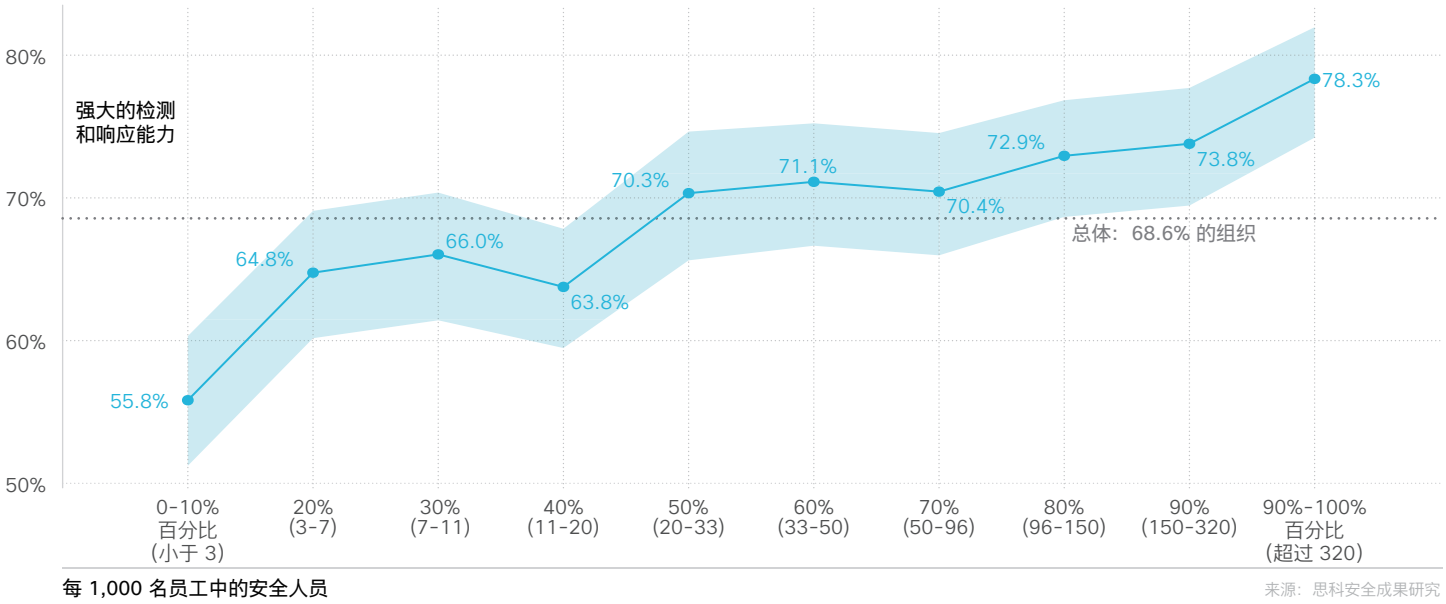


图 14：安全人员配置比例对威胁检测和事件响应能力的影响

我们得出的第一个启示是，安全人员配置比例的确与威胁检测和响应能力有直接关系。比例最高的组织拥有更强能力的可能性比最低的组织高 20% 以上。但是，我们看到代表整体平均值的虚线穿过图 14 中的大部分阴影置信区间。这基本上意味着，即使是人员配置规模不处于两个极端的组织（即大多数组织），也有可能拥有强大的安全运维计划。

这些发现实际上都意味着什么？我们可以肯定地说，与仅拥有骨干人员的组织相比，拥有庞大安全团队的组织更有可能实现强大的检测和响应能力。但是，仅凭员工人数并不能解决所有安全运维问题。而且，即使最小和最大人员配置比例之间的差异，也不足以解释上一部分中讨论的拥有强大人力资源能够带来功效的显著提升。**我们由此可以推断出，在组建优秀的威胁检测和响应团队方面，人员质量同样重要，甚至比人员数量还要重要。**

安全团队的人员短缺问题日益严重。

由于资源紧缩和网络威胁层出不穷，许多网络安全专业人员正在经历巨大的工作压力和职业倦怠。我们可以采取哪些主动措施来帮助他们改善健康和提高幸福感？在这本电子书中，我们请行业领导者和从业人员分享他们在管理精神健康方面的洞察和故事。

安全运维人员配备：外包、内包还是混合模式？

既然安全运维的成功不只决定于员工人数，但人员配置模式是否会影响成果？在所有条件相同的情况下，是外包、内包还是混合模式，更有助于威胁检测和响应的成功？我们来看看能否借助数据找到这个问题的答案，但要注意的是，数据对于这个问题得出的结果有点相互矛盾。

我们向受访者询问了他们的人员配备模式，然后将其与他们的检测和响应能力的评分进行了比较。**如图 15 所示，与采用混合人员配置模式的组织相比，主要依靠内包或外包团队的组织更可能拥有强大的安全运维计划（可能性高出 20% 至 30%）。**由于大多数组织表示他们采用了某种形式的混合模式，因此我们认为在接受以上调查（似乎）认定的结果前，有必要从不同的角度进行分析，然后才能作出混合模式失败的结论。

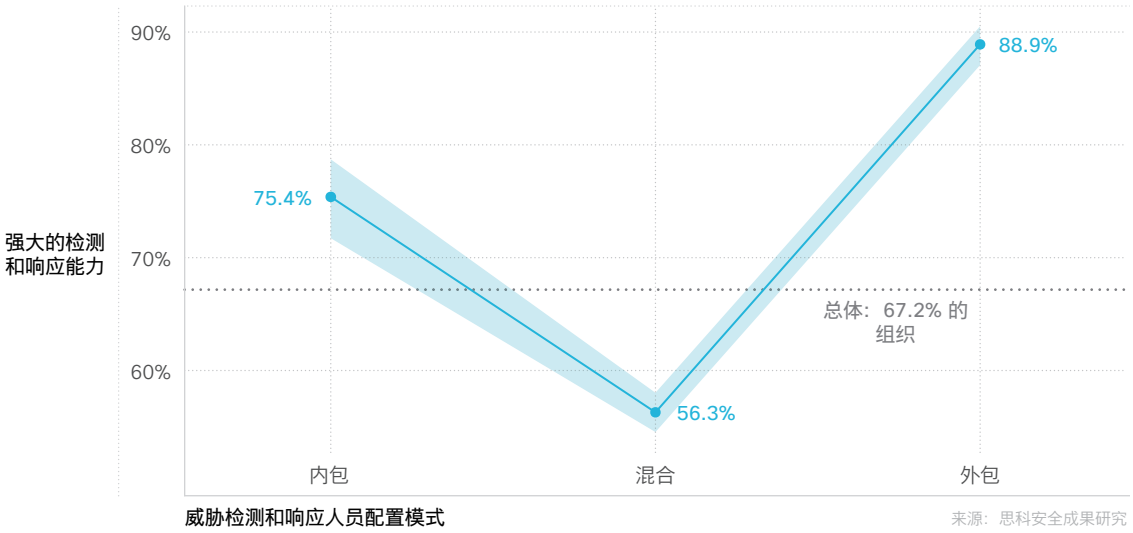


图 15：人员配备模式对组织感知的威胁检测和事件响应能力的影响

主要依靠内包或外包团队的组织，其拥有强大的安全运维计划的可能性高出 **20% 到 30%**（相较于采用混合人员配置模式的组织）

除了要求受访者对组织感知的检测和响应能力的强度进行评分之外，我们还尝试获取更客观的指标，以进行比较。其中之一是平均响应时间 (MTTR)，即修复或遏制安全事件的平均时间。在本报告之外的背景分析中，这些指标往往在大方向上与主观评估一致。然而在我们目前讨论的情况中，如图 16 所示，受访者的评分与客观指标的结论相互矛盾。

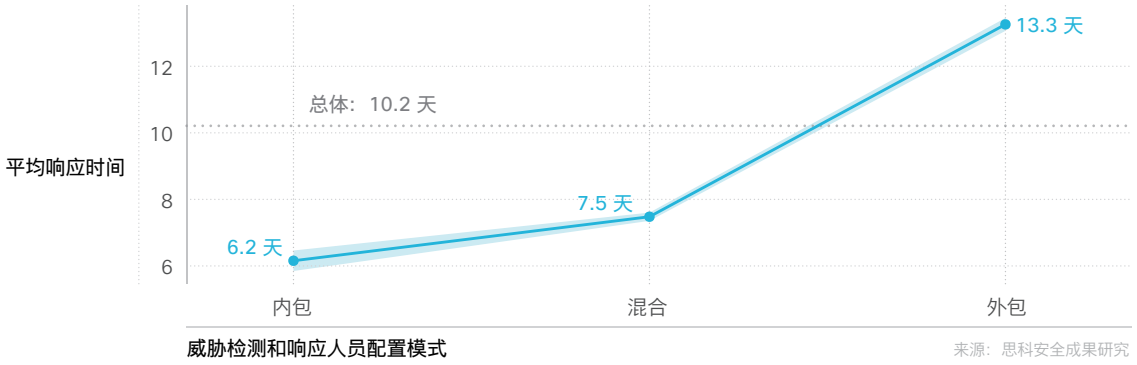


图 16：人员配置模式对安全事件平均响应时间的影响[2]

根据图 16 所示，与采用外包模式的组织相比，拥有内部威胁检测和响应团队的组织，其 MTTR 还不到前者的一半（约为 6 天比 13 天）。而对于那些采用混合人员配置模式的组织，其 MTTR 值处于中间位置（约 8 天），即 MTTR 虽慢于内部团队，但比大多数外包团队要快得多。

显然，我们在这里遇到了一个难题。哪种衡量方式（看法与指标）是正确的？更重要的问题是，在制定采购决策时，您究竟应该参考哪种衡量方式？我们对此先不妄下结论（请先别抱怨我们对这些看似矛盾的数据置之不理）。

当然，补救措施包含很多要素和依赖关系。组织可能依赖供应商发布补丁/漏洞修复来完全解决安全漏洞。这些补丁需要先在其环境中进行实验室测试，然后才能部署到生产环境中。可以说，这其中涉及许多变数。

事实上，我们很难确定期间到底发生了什么。尝试通过调查收集指标可能会产生误导。也许 MTTR 和能力评分存在很大差异，结果就是检测和响应计划在整体上可能的确“强大”，但其实际修复速度并不理想。之所以存在这个问题，也许是因为这些计划较为全面；也许是因为与外包员工进行协调需要占用更长时间；也许是因为这些组织比较自信，因为“我们聘请了专家来完成这项工作，他们肯定能搞定这一切。”也许这就是达克效应在安全运维方面的体现（达克效应是一种认知偏差现象，指的是能力欠缺者往往不能准确评估自身能力）。原因可能是以上种种，或许更多。因此，我们建议您使用此部分来激发讨论，而不是做出决策。

[2] 我们在此图表中使用几何平均值，因为它更能代表“典型”值。受访者报告的 MTTR 通常不到 2 至 3 周，但偶尔也会报告数月，甚至数年。使用几何平均值可以更精确地表示“典型”情况，而不会被那些非常大的极端值所扭曲。

使用情报是否明智？

我们前面提到的达克效应，是本部分的理想知识背景。我们向受访者了解其组织在安全运维计划中使用网络威胁情报的情况。大多数组织 (85%) 表示他们正在某种程度上使用情报，而不到三分之一 (31%) 的组织声称他们正在广泛使用情报。情报是否会带来更出众、更智能、更迅速的威胁检测和响应？让我们来看看图 17。

奇怪的是，大多数根本不使用威胁情报的组织似乎都认为其状况不错。正是印证了那句老话：“无知便是福”，一旦组织对情报领域有所了解，他们就不会如此自信了。（自信心从 84% 降至 46%）。**大量使用威胁情报的组织具有出色检测和响应能力的可能性几乎是较少使用威胁情报的组织的两倍。在一个能力评分和指标一致的示例中，那些更充分利用情报的组织的 MTTR 约为不使用情报的组织的一半。**

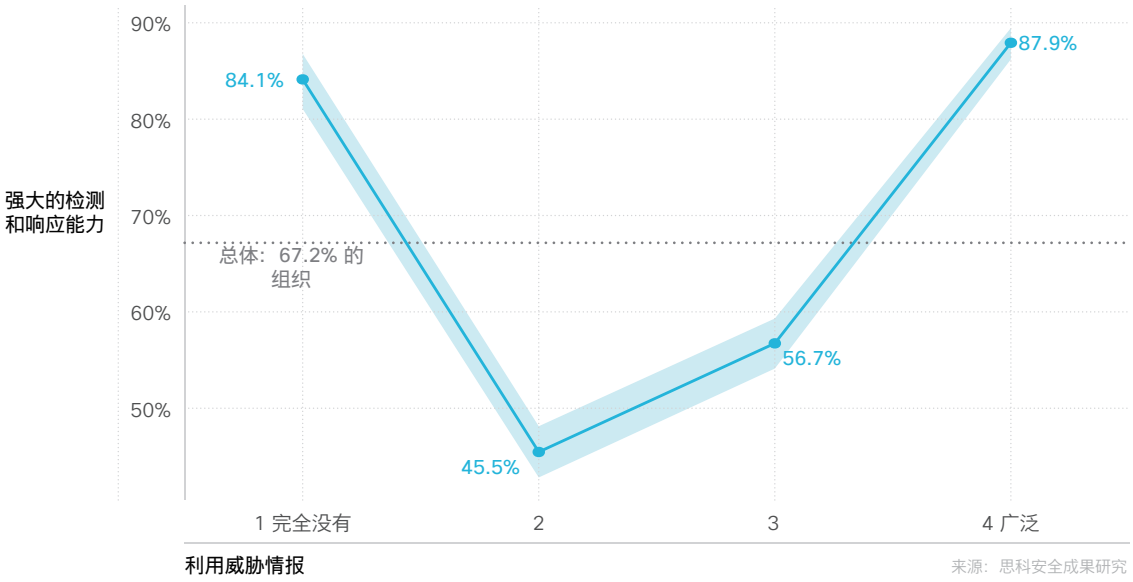


图 17：使用网络情报对威胁检测和事件响应能力的影响

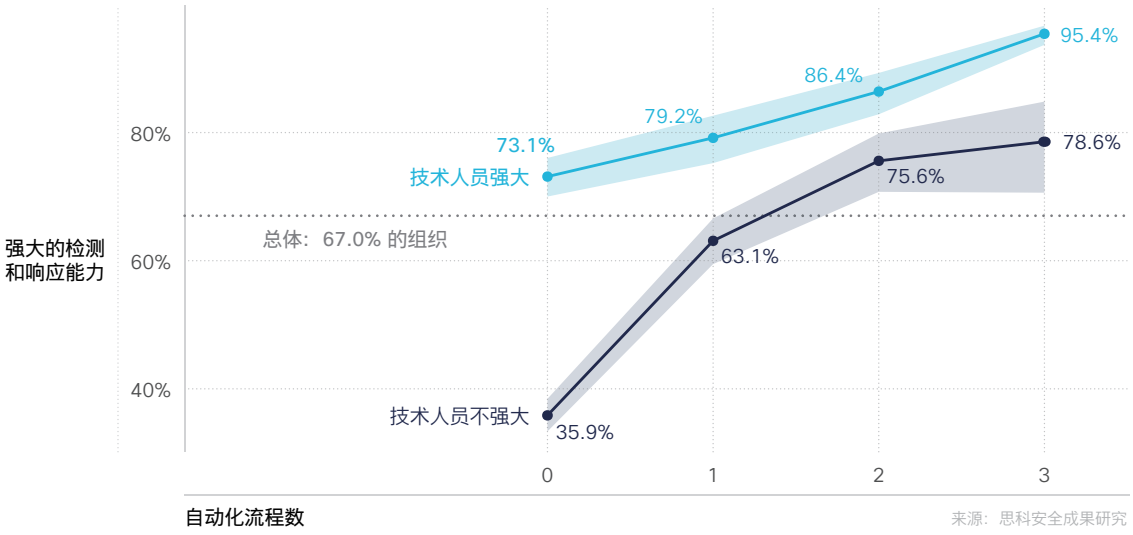
心理学家、畅销书作家丹尼尔·卡尼曼曾说过：“我们对自己的盲目性视而不见。我们对自己的无知很无知。”图 17 显示，一旦组织对他们面临的威胁有一点了解，他们就会恍然大悟，意识到原来还有很多他们不知道的事情。更普遍地使用威胁情报开始让组织重拾信心，而且此时的信心不再建立在无知之上。

大量使用威胁情报的组织具有强大检测和响应能力的可能性近 2 倍于较少使用威胁情报的组织

自动化能否替代人？

看到此标题后，您可能会认为这是一个反问句，答案应该是不能。不要那么快下结论。冒着激怒整个安全行业同仁的风险，我们将在这里尽力通过数据论述我们的观点：自动化实际上可以替代人。这可能不是您想听到的观点。但是，在您决定删除此报告并将我们添加到联系人黑名单之前，请务必接着阅读。（深呼吸，保持冷静）

图 18 包含您之前在单独图表中看到的元素：安全人员和自动化。该图用两条线比较两种不同类型的安全运维计划。第一条（深蓝色线）代表没有强大人力资源的组织，而那些拥有强大人力资源的组织则以天蓝色线表示。在这两种场景中，从左向右的趋势显示了提高自动化级别对威胁检测和事件响应能力的影响。



来源：思科安全成果研究

图18：人员配备和自动化强度对威胁检测和事件响应能力的影响

让我们从“没有充足人力资源”的组织开始。在缺乏能干的安全人员且未实现任何主要流程自动化的组织中，只有约三分之一报告了具有强大的检测和响应能力。在我们调查的三个流程领域（威胁监控、事件分析、事件响应）中，如果有一个流程实现了自动化，情况会大幅改善。两个领域自动化将进一步提升人力资源的价值，而三个领域全部实现自动化，则使经验不足的员工绩效翻倍。**超过四分之三的安全运维计划没有高效的人力资源支持，不过它们仍然能够通过高度自动化实现强大的能力。**

现在，让我们把目光从深蓝色线最右边的点转向天蓝色线上的第一个点。您是否看到了规律？这两个点的水平位置很接近。**它说明员工人数较少而自动化率较高的安全运维计划，其水平与员工人数较多而自动化程度较低的安全运维计划相近。**换句话说，强大的自动化可以成为强大员工的替代。数据说明，我们的结论站得住脚。

但是，图 18 的重点或最重要的启示并不是人与机器的比较。蓝线随着自动化水平连续变化而平稳上升，这为同时追求一流自动化和优秀团队这两大目标提供了无可辩驳的理由。设法组建强大团队并自动执行主要威胁检测和响应流程的安全计划，几乎可以确保安全运维成功（超过 95% 的可能性）。因此，请勿使用自动化技术替代有才华的员工队伍。要用它来让您的高级人才专注于高优先级活动，从而充分发挥他们的价值。

我们应该多久进行一次调整、修改和追踪？

我们可以列出任何可能改进威胁检测和响应计划的重复性活动。在关于该主题的非正式民意调查中，我们推荐了三项最值得尝试的做法：

- 测试和更新检测规则和使用案例
- 主动追踪恶意活动的迹象
- 参与安全红队和/或紫队练习

我们向受访者询问了其组织执行这些活动的频率，然后结合报告的威胁检测和响应能力优势进行了分析。由此生成的趋势在图 19 中再清楚不过。

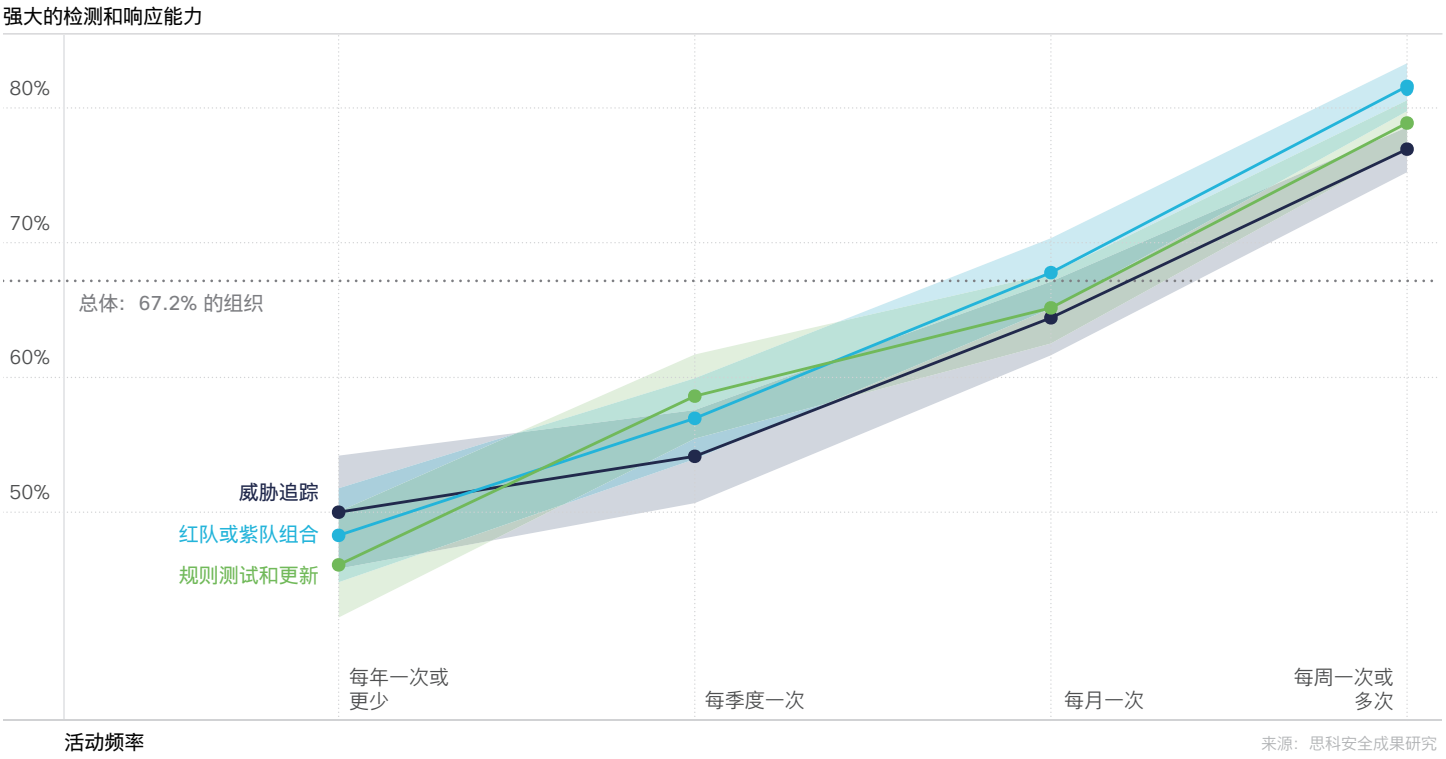


图 19：活动频率对威胁检测和事件响应能力的影响

规则调整、红队/紫队组合及威胁追踪都遵循类似的轨迹。频率越高，就越有利于安全运维计划。**至少每周执行一次这些活动的组织与每年执行一次或更少的组织相比，性能提升大约 30%。**那么，您的组织应该多久执行一次？简单的答案是，“越多越好”。

至少每周执行一次这些活动的组织获得大约 **30%** 的性能提升

“安全一直在变化，我们需要紧跟这些安全趋势。以前，我们在解决安全问题和事件方面浪费了大量时间。由于简化了调查流程、节省了调查时间，我们可以紧跟新的安全趋势和集成新的安全解决方案，从而为我们的教育网络提供更安全的基础设施。”

Bahruz Ibrahimov，AzEduNet 高级信息安全工程师

了解详情

确保迅速从灾难中恢复的能力和高弹性

有趣的是，网络安全方面的“首要关注点”随着时间的推移在不断变化。过去，数据泄露和网络间谍活动是网络安全热点，而现如今，人们把注意力再次聚焦在业务连续性和灾难恢复 (BCDR) 方面。理由很充分。猖狂的勒索软件及主要托管服务提供商的服务中断等，都迫使我们在应对无情威胁的过程中对战略进行了重大变革，以确保实现高弹性。

《2021 年思科安全成果研究》将迅速从灾难中恢复的能力列为构建成功网络安全计划的第 4 大驱动因素。除安全文化之外，它显示了与所有其他 11 个安全成果的重大关联。记住这一点，让我们研究一下如何最大限度地提高这种做法的有效性，并确保高弹性。

猖狂的勒索软件及主要托管服务提供商的服务中断等，都迫使我们在应对无情威胁的过程中对战略进行了重大变革，以确保实现高弹性。

灾难恢复是否应该接受董事会级别的监督？

我们很想知道谁最终负责监督灾难恢复能力。事实证明，首席信息官、首席信息安全官及其他非 IT 成员的企业高管们相当均衡地分担了监督工作，其中大约有四分之一的组织遵循 BCDR 流程，向以上提及的每位人员汇报。在我们的调查中，董事会级别的可视性虽然不那么常见，但仍然存在于 18% 的组织中。

当我们将这些答案与每个受访者对其业务连续性和灾难恢复能力的评估进行比较时，我们很明显地看到，监督不仅仅是为了满足好奇心。**根据图 20，对 BCDR 实行董事会级别监督的组织最有可能拥有强有力的计划（比平均水平高 11%）。**当首席信息官参与业务连续性和灾难恢复职能时，计划成功的可能性最高，但其所占比率最低，远远低于平均水平。

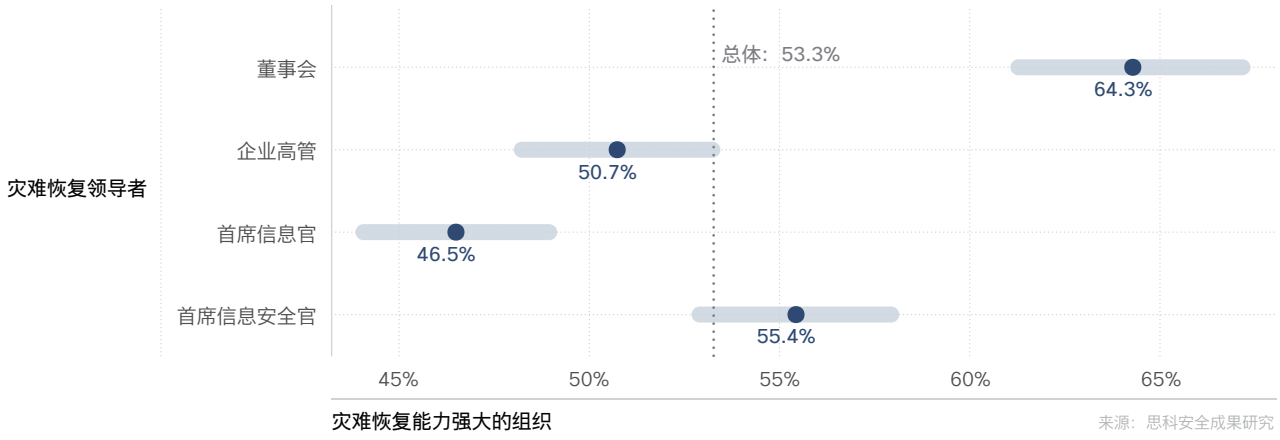


图 20：高层组织监督对灾难恢复能力的影响

对于图 20 中的结果，有许多合理的解释。我们猜测，当组织在灾难恢复问题上需要向董事会负责时，其对运营风险和弹性的担忧可能会加剧。这些担忧或许会转化为更严格的监督、更有力的支持和更庞大的预算。因此，如果您的组织正在为提高灾难恢复能力而奋斗，那么可能需要自上而下地采取行动，而非自下而上。

灾难恢复的日常运行情况如何？

除了最终监督之外，我们还询问了谁负责灾难恢复方面的战术性实操工作。**当网络安全或专业的业务连续性团队负责运营时，绩效往往会达到最佳。**由 IT 运营的计划通常落后。有趣的是，董事会级别的可视性就像一股浪潮，水涨船高地提升了每一个团队的效率。无论日常职责落在何处，只要最终监督掌控在董事会手里，安全运维的成功率在统计学上就会相同。

灾难恢复的范围是否重要？

您可能已经知道了，灾难不会予人方便，它不会仅在您准备就绪的时间或地点来袭。网络安全灾难也不例外，这就是为什么该领域的传统智慧是尽可能为所有可能的事件做好准备。但是，这说起来容易，做起来难。

事实证明，只有不到十分之三的组织表示，他们的灾难恢复功能覆盖了至少 80% 的关键系统。一半受访者属于 50% 至 79% 这个区间，而略低于 20% 的受访者承认覆盖率低于此百分比。乍一看，这似乎还不错。毕竟大多数组织都覆盖了大多数关键系统。遗憾的是，持有这种观点的人忽视了灾难总是乘人不备这个令人不快的规律。我们的数据表明，这种情况的发生频率远超出我们的预期。

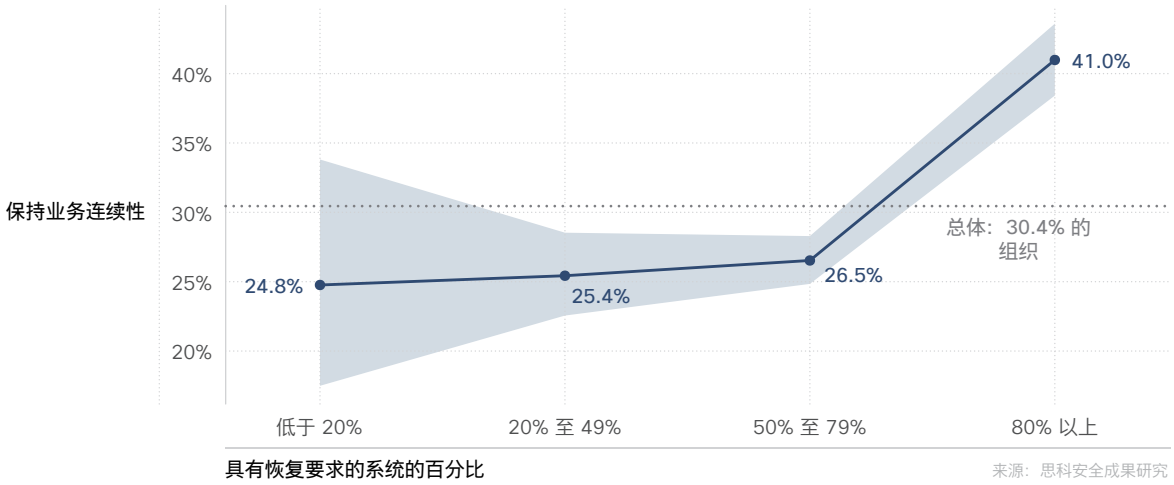


图 21：关键系统覆盖范围对灾难恢复能力的影响

图 21 衡量了本研究添加的新成果，旨在衡量组织在遭遇颠覆性事件时保持业务连续性的能力。调查结果显示，这是受访者最不满意的三个安全结果之一。这使得寻找有效方法来提高成功可能性变得更加重要。

图 21 带来一条关于保持业务连续性的重要信息。**那就是，在 BCDR 功能覆盖至少 80% 的关键系统之前，组织保持业务连续性的可能性几乎无法进一步提高。**

这个结论大概可以归咎于灾难那不可思议的发生规律，即总是在我们尚未准备好的时候发难。这里的教训是，我们不能指望在业务连续性和灾难恢复方面的投资能够产生立竿见影的成果。这个消息可能不受欢迎，但说起来，灾难也绝不是一个受欢迎的消息，所以我们只能调整期望值。

实践能帮助实现完美的灾难恢复吗？

我们可以提前直接给出答案。不能，遗憾的是实践不能实现完美的灾难恢复。但确实比不实践要好得多。到底要好多少？请您继续阅读...

一句著名的军事格言说：“作战无法按计划进行。”事实证明，这句话可以很方便地扩展到网络战场，并且在许多测试点上考验 BCDR 能力，包括计划演练、桌面练习、实时测试、并行测试和全面生产测试。我们向受访者询问了所属组织参与此类测试的频率，并将答案与其保持业务连续性的可能性进行了比较。

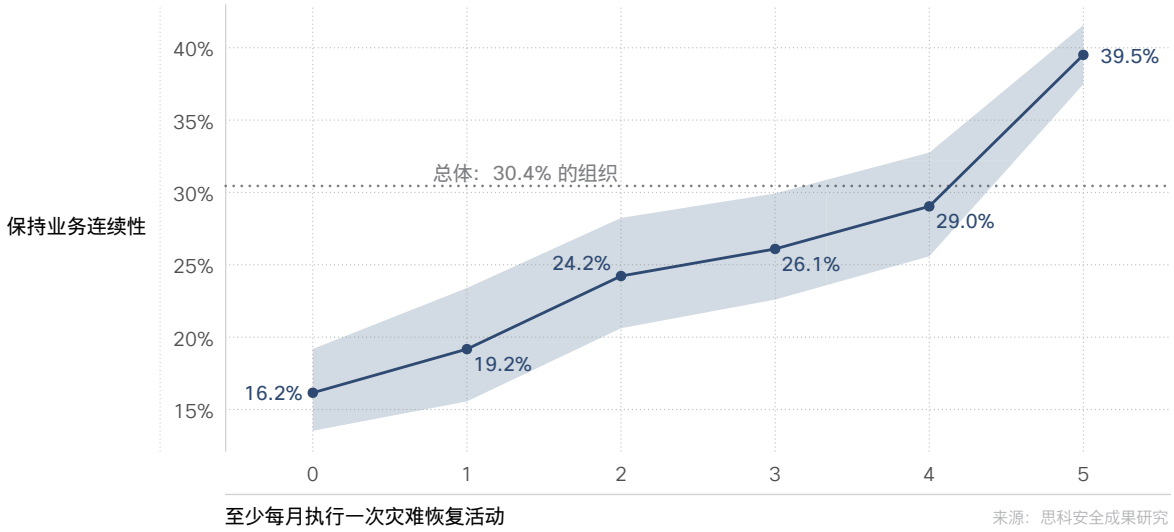


图 22：测试练习对灾难恢复能力的影响

在效果方面，没有哪种做法胜出，不过所有这些做法加起来，有助于提高弹性。**与不参与 5 类灾难恢复测试的组织相比，定期参与所有此类测试的组织，其成功保持业务连续性的可能性是前者的近 2.5 倍。**那么启示是什么？不要对弹性怀有侥幸心理。定期从多个不同的角度对您的业务连续性和灾难恢复能力进行压力测试。

定期参与所有 5 类灾难恢复测试的组织，其成功保持业务连续性的可能性

2.5倍

于不参与此类测试的组织

我们是否应该释放“混乱的猴子”（人为制造故障）？

在压力测试灾难恢复计划这一主题上，让我们将“压力”最大化。我们讨论的是混沌工程，即有意让系统定期中断，以测试系统抵御意外情况和事件的能力。在您的 IT 和安全系统中释放一只猴子（人为制造故障），是否能让您的组织更具弹性？如果您想知道答案，请接着阅读。

我们向受访者询问其组织在多大程度上参与了混沌工程，并了解到这种情况比我们预期的更常见。值得注意的是，我们注意到这种做法与技术集成之间存在关系。根据图 23，超过三分之二采用混沌工程技术作为标准实践的组织表示，他们利用高度集成的技术来支持其恢复能力。集成是必需，还是为了启动混沌工程而存在？我们尚不清楚。与安全领域中的许多事情一样，可能两者兼而有之。让我们密切关注这一新兴学科，特别是如果您需要在复杂且高度集成的 IT 环境中负责 BCDR。

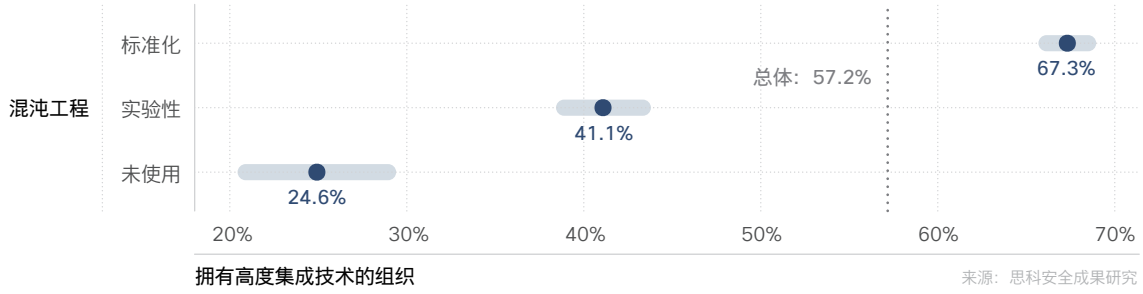


图 23：混沌工程与 IT 集成水平之间的关系

在图 24 中将混沌工程的实施程度与保持业务弹性的成果进行比较后，我们就能得出一个令人信服的理由，来支持我们将“混乱的猴子”引入网络。**制定混沌工程标准做法的组织更有可能拥有强大的业务弹性，其可能性是不使用混沌工程的组织的两倍。**这个结果或许让您震惊，同时许多人都发现这出乎意料。好消息是，您可以在混沌工程的实践中利用“混乱的猴子”进行测试，从而提高弹性，为真正的灾难做好准备。

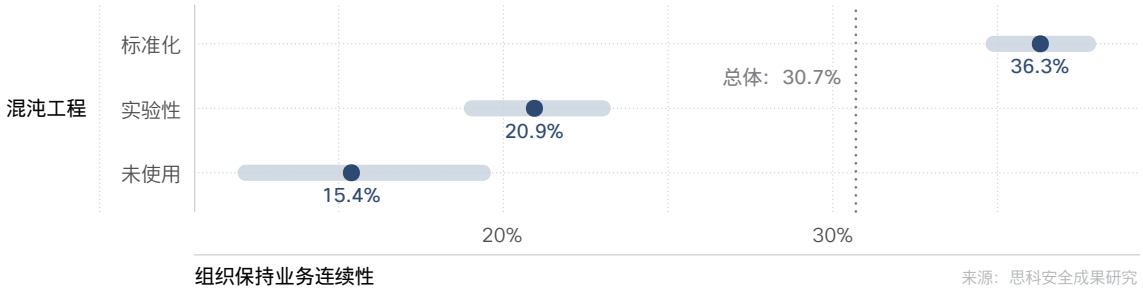


图 24：混沌工程对保持业务弹性的影响

结论和建议

首先，我们从在早期研究中已确定为高度有效的安全做法出发，通过一项新的调查收集了更多信息，以了解它们能够如此高效的原因，并与您分享这些经验。我们希望本报告可以为您提供一些实用技巧，以帮助您的网络安全计划获得更大的成功。

无论如何，思考这样一项研究的发现，并听听其他人从中学到了什么，绝对没有坏处。我们请经验丰富的 CISO 咨询团队评估本报告研究的每个实践领域。下面列出了他们的主要建议。您可以在我们的安全成果研究博客系列中找到更多洞察和启示。

积极更新技术

“安全欠债问题非常严重。对于首席信息安全官，未来的发展方向是制定‘购买、持有、销售’战略。识别您的资产，定义一个适应性强的架构，降低依赖风险，并为将来的更新周期实施审核循环。”

Richard Archdeacon，思科咨询首席信息安全官

充分集成技术

“我们知道，现代化及充分集成的 IT 有助于整体安全计划取得成功，因此，您可以采取一些行动来改善您的环境，比如寻找基于云的安全解决方案、研究自动化机会、确保采购要求中包括了技术集成功能。”

Helen Patton，思科咨询首席信息安全官 @CisoHelen

及时响应事件

“能力强的员工能够助攻事件响应团队。这是一个很好的起点，但需要结合其他要素来发挥作用。一旦企业把精兵强将、高效流程和前沿技术合而为一，就能掌握高超的威胁检测和响应能力。”

Dave Lewis，思科咨询首席信息安全官 @gattaca

准确检测威胁

“为您的安全运维团队选择最熟练的人员，因为关键的因素不仅仅是员工人数。如果您的员工无法达到所需的专业知识水平，自动化可以帮助您弥合初级员工与高级员工之间的差距，并获得一样出色的成果。”

Wendy Nather，思科咨询首席信息安全官 @wendynather

迅速从灾难中恢复

“本报告中的研究结果强调了业务连续性和灾难恢复能力的价值，但不要让其孤立地运行而脱离其他安全功能。它们应该与其他风险管理职能分享资源的优先顺序和风险等级。同样，紧密集成资产管理和威胁管理，以确保所有团队都遵循相同的规则。”

Wolfgang Goerlich，思科咨询首席信息安全官 @jwgoerlich

关于 Cisco Secure

长期以来，思科在推动互联网发展的技术领域里确立了自己的全球领导者地位，同时还在此过程中打造了一个开放、集成的网络安全解决方案组合。我们认为，各项安全解决方案应该像一个团队一样协同合作。它们应该互相学习，作为一个统一整体去发现问题并作出响应。只有这样，安全系统性和效力才能得以提升。作为全球最大的 IT 基础设施和网络服务提供商，以及全球最大的企业网络安全企业，多年来我们一直深受客户的信赖。

Cisco Secure 秉持不断优化、简化的安全原则。我们提供以客户为中心的精简安全方法，可确保各产品不仅易于部署、易于管理、易于使用，而且可以协同工作。我们深知，客户及其相关人员是我们产品和服务的核心，他们希望消除复杂性和干扰，获得可靠的安全解决方案，注重最终成果。这就要求我们尽量简化，而不过于简单。我们的云原生平台在这方面实现了巨大飞跃。

在思科，我们利用 Cisco SecureX 平台为安全行业提供可靠的安全解决方案，确保他们在当下和未来免受威胁困扰。我们通过最广泛、集成度最高的平台，帮助所有财富百强企业随时随地保障工作安全。如需详细了解我们如何简化体验，促进您取得成功并提供面向未来的安全保护，请访问 cisco.com/go/secure。

附录：抽样调查对象特征统计数据

在本附录中，我们包括了本次调查的 5,123 份合格回复中的抽样调查对象特征统计数据。我们希望这些信息有助于感兴趣的读者甄别本调查结果的代表性。

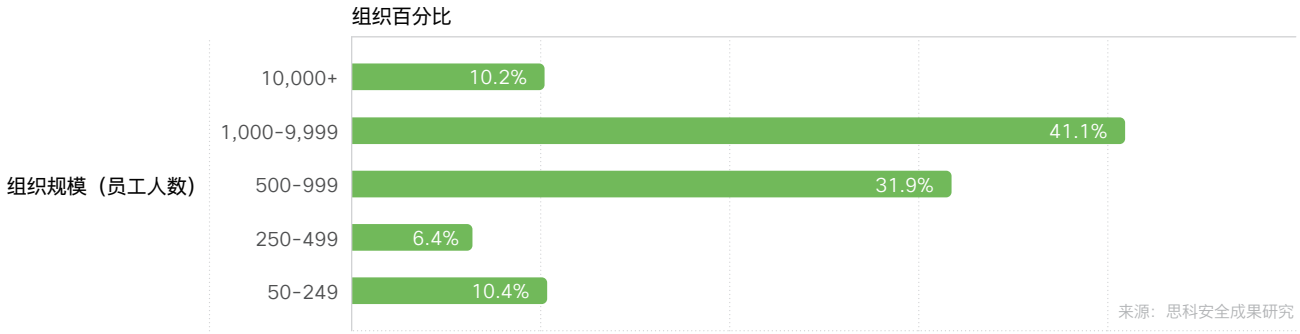


图 A1：参与调查的组织的员工人数

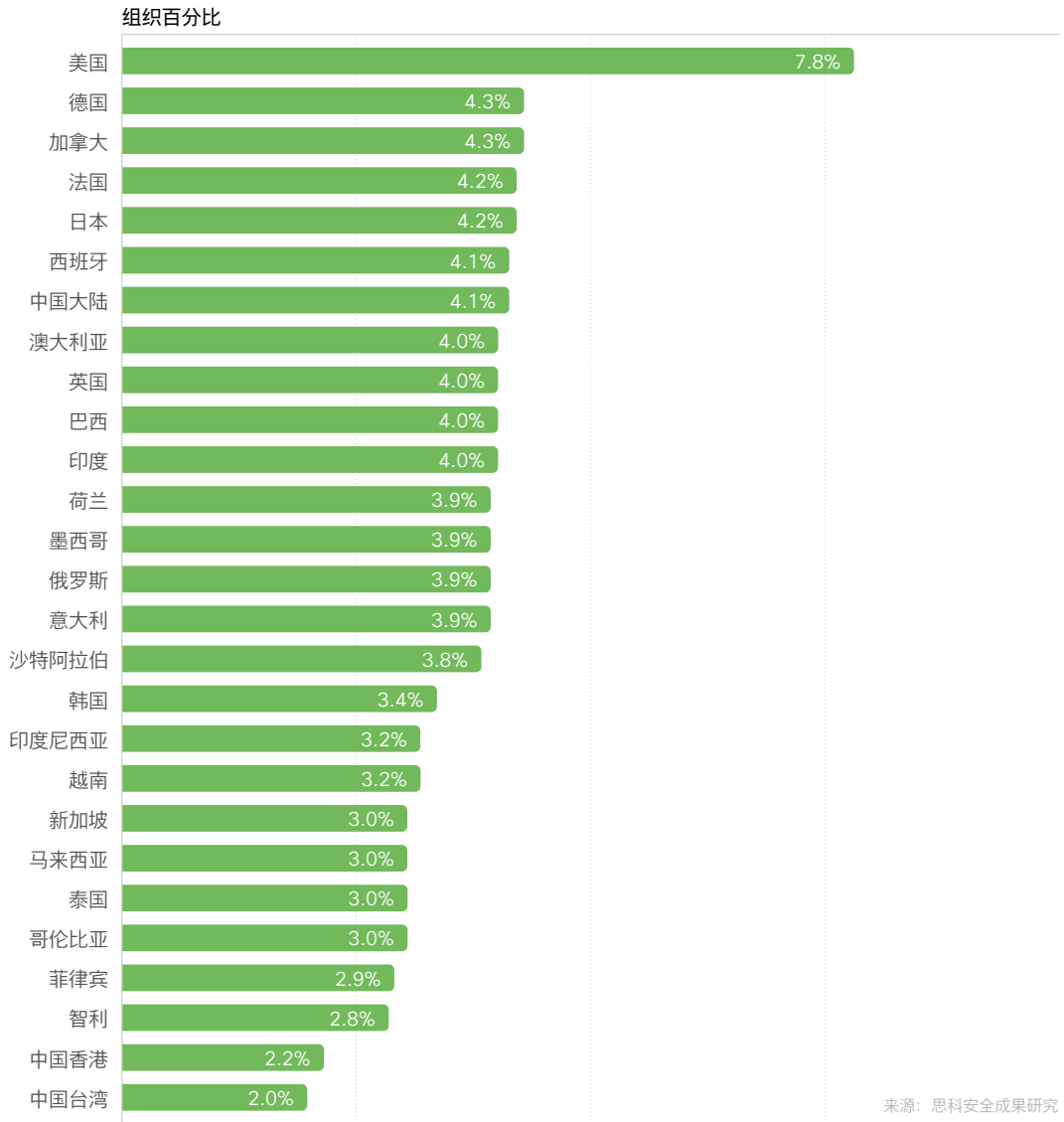


图 A2：参与调查的组织总部所在的市场

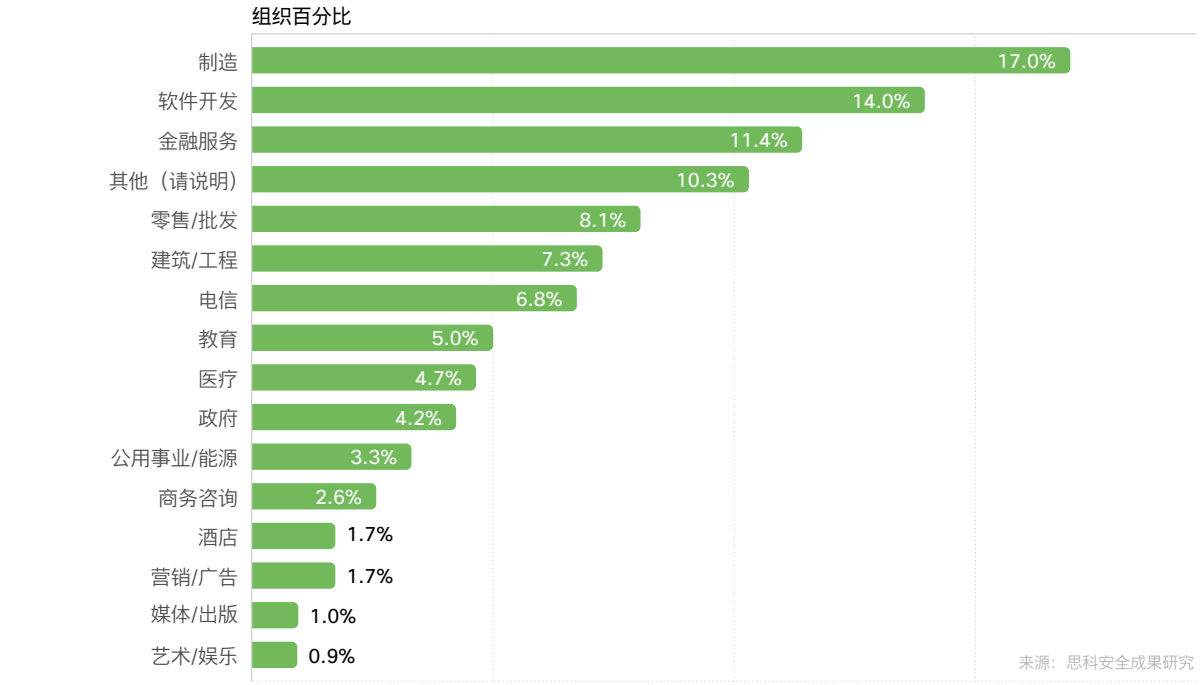


图 A3：参与调查的组织代表的行业

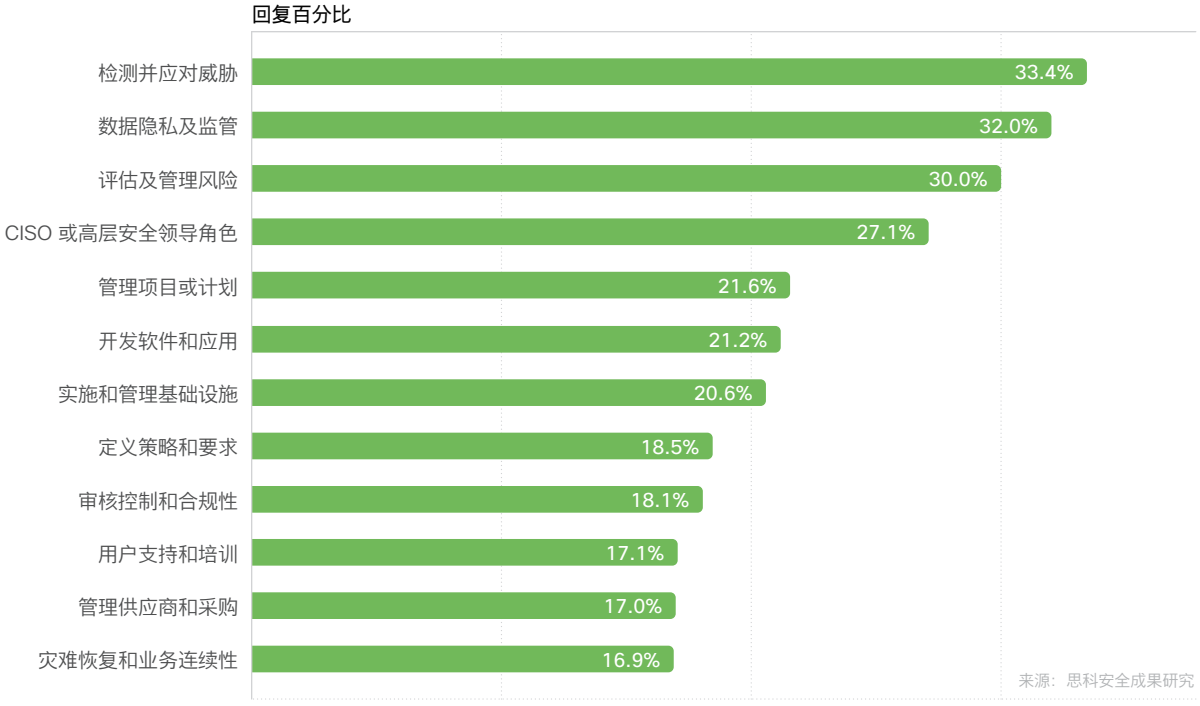


图 A4：受访者的主要工作职责

CISCO
SECURE

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV,
荷兰阿姆斯特丹

2021 年 12 月发布