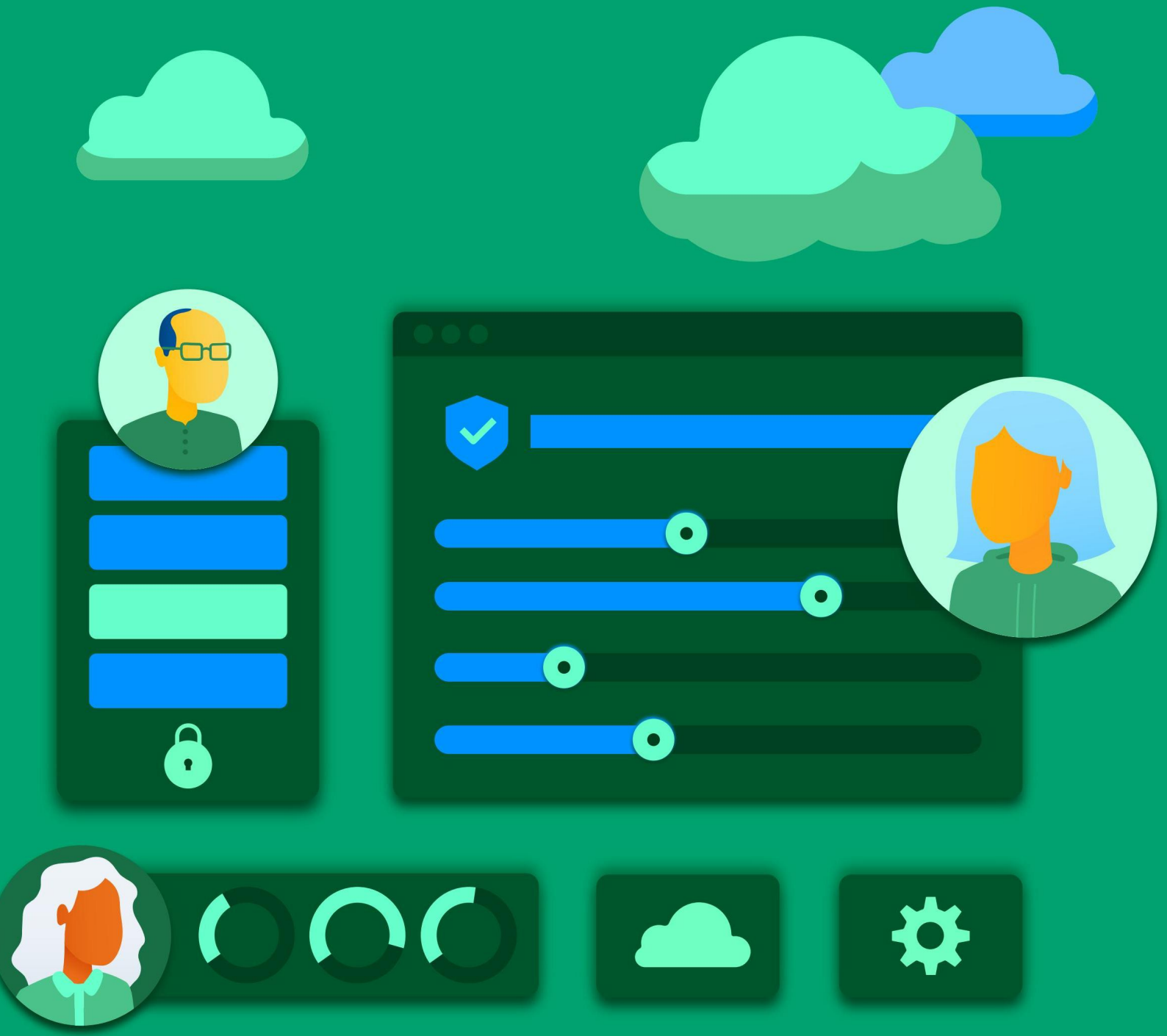
安全驱动创新和云趋势



expel®

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网（https://c-csa.cn）

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《安全驱动创新和云趋势（Security-Enabled Innovation and Cloud Treads）》由 Hillary Baron 编写，并由 CSA 大中华区多云安全工作组组织翻译并审校。（以下排名不分先后）：

多云安全工作组组长：魏小强

翻译：罗春、苏泰泉、李安伦、伏伟任、徐岩、张见

审校：魏小强

研究协调员：张见

贡献单位：亚信安全

摘要

随着云计算的高速发展，如何在云环境中保障数据和应用的安全性日益成为企业共同的关注点，企业也正在考虑多云和混合云策略。云原生技术如容器、微服务和无服务器架构也在迅速崛起，在此背景下，如何更好地保护云环境和云服务中的数据和资源安全，正在成为行业重点关注的问题。

为了解企业在这一领域的实践与观点，CSA 发布了《安全驱动创新和云趋势（Security-Enabled Innovation and Cloud Treads）》（以下简称“报告”），本报告通过对来自全球不同国家和地区、不同行业和规模企业、不同企业工作角色的 1100 多家企业进行了调研分析，让读者系统了解到最新云安全发展趋势。其中一些值得关注的洞察有：

1. 安全被视为创新的推动力，但企业高管和员工对这一看法仍然存在分歧。报告发现有 65%的受访企业高管认为安全是产品开发和云战略中很关键的一个环节，是产品的一个重要竞争优势，也是推动创新的关键因素。

2. 企业正在尝试通过安全驱动创新实现预期成果。60%的受访企业认为安全可增强企业和合作伙伴的信任度。

3. 多云架构是一把双刃剑，既有优势，也会带来成本和资源管理的挑战。数据显示其中 71%正在采用两个或更多的云架构环境，这种情况表明企业的战略正在向多云架构转变，但相应的运维工作也更加繁重，有 61%的企业报告称在多云环境下存在成本管理和资源分配的挑战。

4. 将工作负载迁回本地的趋势日益增长。令人震惊的是，59%的企业已经将工作负载从云端迁回本地，其中大部分迁移发生在过去 12 个月之内（34%）。这个趋势意味着企业的 IT 战略格局正在发生改变，标志着在最近几年云计算优先的趋势过去之后，重心可能会重新转向本地解决方案。

5. Kubernetes 和容器将成为主角。在云原生技术的采用上，超过 60%的企业正在应用容器技术改造应用，服务网格和无服务器架构也在快速崛起。28%的企业已将所有应用全部迁移到了 Kubernetes 上，而 57%的企业已经迁移了部分应用。

报告总体反映出企业对云计算中安全驱动创新的推动作用和积极性普遍较高。它为

读者深入理解全球企业的云计算实践、面临的安全与管理难题，以及最新的技术部署动向提供了详实的第一手资料。详细信息请阅读本报告全文。

目录

1. 调查的创建和方法

云安全联盟(CSA)是一个非营利性企业，其使命是广泛推广并确保云计算和 IT 技术领域中网络安全的最佳实践。CSA 还对行业中的各利益相关方进行不同形式的安全培训。CSA 是一个包括行业从业人员、企业和专业协会等组成的广泛联盟。CSA 的主要目标之一是开展信息安全趋势评估。这些评估展现了企业在信息安全和技术方面的成熟度、行业观点、关注点和未来趋势等信息。

Expel 委托 CSA 编制一份调查报告，以更好地了解该行业内安全创新的最新近况、以安全为驱动带来的创新成果以及当前云计算最新的使用趋势。

Expel 为该项目提供资金，并与 CSA 的分析员共同开发了调查问卷。CSA 于 2023 年 5 月进行了在线调查，收到了来自不同规模地区和企业的 IT 和安全专业人士的 1018 份回复。本报告由 CSA 的分析员对问卷进行了分析并汇总而成。

1.1. 研究目标

本次调查的主要目的是对安全创新和一些关键领域的云计算趋势作更深入的了解。

- 安全专业人员对企业的安全与创新之间关系的最新观点
- 确定以安全驱动的创新的实际成果和预测效果
- 研究云计算的使用趋势，如多云环境、容器的使用，以及云上云下的转移

2. 主要结论

在当今快速发展的数字环境中，了解安全驱动创新的作用和云计算使用的趋势至关重要。安全不仅能为企业资产保驾护航，也能作为创新的催化剂，加强信任并促成新的业务模式。与此同时，云计算技术具有灵活、可扩展和成本低的优点，改变了企业的运营、发展和创新模式。然而，要有效地利用这些技术，就必须了解它们的优势、面临的挑战以及未来发展的趋势。正是出于这些原因，我们开展了一项调查，并取得一些关键发现和成果。

这些调查成果为了解企业 IT 策略中不断变化的模式和趋势提供了独特的视角。虽然安全在促进创新方面发挥着不可或缺的作用，且已成为一个重要趋势，但高管和员工之间的观念存在明显的脱节。这种分歧表明，企业需要在安全策略方面加强共识。

以安全为驱动的创新为企业带来了预期的收益，例如客户和伙伴的信任感增加，还有降低了数据泄露的风险。然而，对于以安全为驱动的创新带来的成本影响则看法不一。从技术角度而言，由于可以充分利用不同供应商的优势，满足系统性能和弹性的更高要求，多云环境的使用受到偏爱。然而，在管理成本、资源配置、多云服务供应商（CSP）的整合以及跨平台安全策略的一致性等方面，都面临的巨大挑战。

将工作负载迁回本地部署的趋势也日益明显，这主要出于战略转变和性能优化的需求。与此同时，Kubernetes 和容器在企业日常运营中的重要性也日益凸显，大多数企业都或多或少的采用 Kubernetes 和容器来运营业务。这一趋势与业界对"左移"的实践和 DevSecOps 日益增长的偏好相吻合。总体而言，该调查报告描绘了当前 IT 环境的复杂蓝图，各企业都在不断努力平衡和优化以应对业务挑战，并根据多种因素调整战略。

2.1. 主要结论 1：安全被视为创新的推动力，但高管和员工对这一看法存在分歧

最近的调查显示，在安全与创新之间的关系方面，各企业内部存在着有趣的两级分化现象。研究发现的一个普遍认识是企业对安全及其在创新中不可或缺的作用持积极态

度。在产品研发过程中，安全被优先考虑，并被视为一种竞争优势，尤其是在云战略方面。此外，企业认为安全对于培养创新土壤至关重要，大多数企业预测未来五年内安全与创新之间的相互依存关系将日益增强。

然而，调查也发现，企业的高管和员工对安全和创新的关系存在分歧。高管认为安全是产品开发和云战略中很关键的一个环节，是产品的一个重要竞争优势，也是推动创新的关键因素。安全的重要性在产品研发、云战略、竞争优势和创新因素四个方面的占比分别达 43%、50%、51%和 65%；但是员工却认为安全在产品研发和云战略中的参与度较低，与产品竞争优势和创新因素两者的关联度不高。安全在产品研发、云战略、竞争优势和创新因素四个方面的占比，对员工的调查结果分别为 27%，31%，36%和 44%。安全与创新存在一定的关系，但是与高管的看法相比，员工感受到的力度要弱很多。这种观点表明企业内部在如何看待安全的作用方面存在分歧。

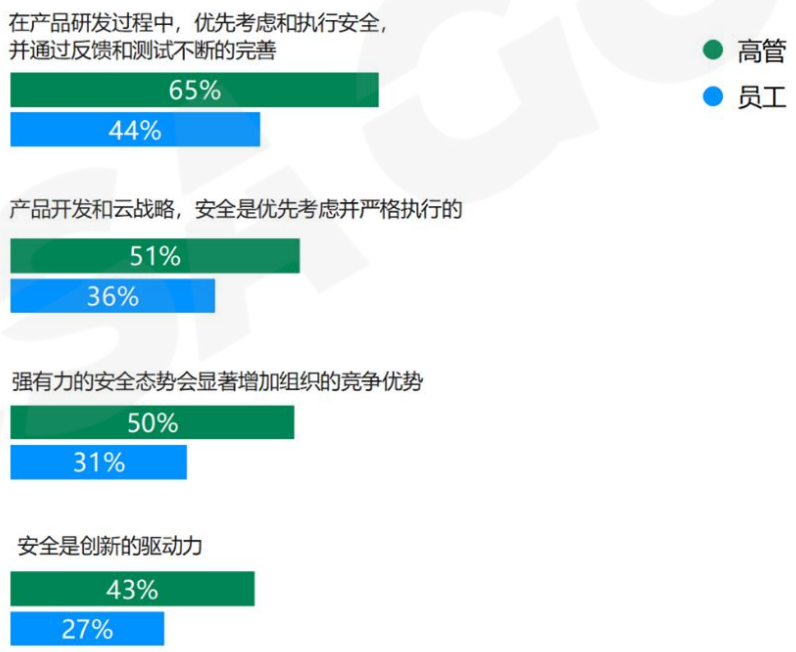


图 1 企业的高管和员工对安全和创新之间关系的看法

高管与员工之间的分歧还延伸到创新对业务成本的影响。有 35%的高管更倾向于认为创新可以降低成本，有 20%的高管认为创新会增加成本。有 22%的员工认为创新降低成本，有 38%的员工认为创新会增加成本。

有几个原因可以解释这种观点分歧，企业的高管从大局角度出发，可能会更加乐观，因为这反映出企业的愿望，而在特定领域工作的员工则可能从日常运营的角度出发，更为落地。此外，高管和员工的关注点和出发点不同也是一个重要因素，58%的员工关注的重点是招聘和留住有技能的人员，这点上仅有 25%的高管关注；相比较之下，有 50%的高管主要关注的是在竞争环境中如何快速创新，而只有 19%的员工关注于此。

在企业内部创建统一的愿景和文化，对解决这种分歧是至关重要的。高管必须建立有效的沟通策略，向员工反馈其工作所带来的影响，并争取他们对企业愿景的认同。同样，建立让员工能够向高管分享现实情况和所遇挑战的沟通渠道也同样重要。通过促进这种双向交流，企业内部可以就安全在创新中的作用方面达成共识，最终提升其市场竞争地位。

2.2. 主要结论 2：创新成果：企业通过安全驱动创新实现预期成果

调查显示在安全驱动创新的预期和实际结果之间尽管有一些明显的不同，但总体相近。企业要么精准的预测安全措施所带来的效益，要么展示出它所期望的创新优势。虽然在复杂的基础设施和专业人才的缺乏方面存在挑战，但主要困难大体一致。

成果

从企业实施安全措施的实际成果来看，其中最显著的实际成果是增强了客户和合作伙伴的信任度（53%），降低了数据泄露和网络攻击的风险（52%）。这些成果与实施创新安全措施的初衷相吻合，其中包括了期望增强客户和合作伙伴的信任度（60%）以及期望减少合规或被攻击的风险（57%）。有趣的是，尽管企业已经意识到安全是一种竞争优势，但加强该竞争优势却是最少被选择的选项之一（23%），究其原因可能是因为它所带来的好处比较抽象，不够具体。

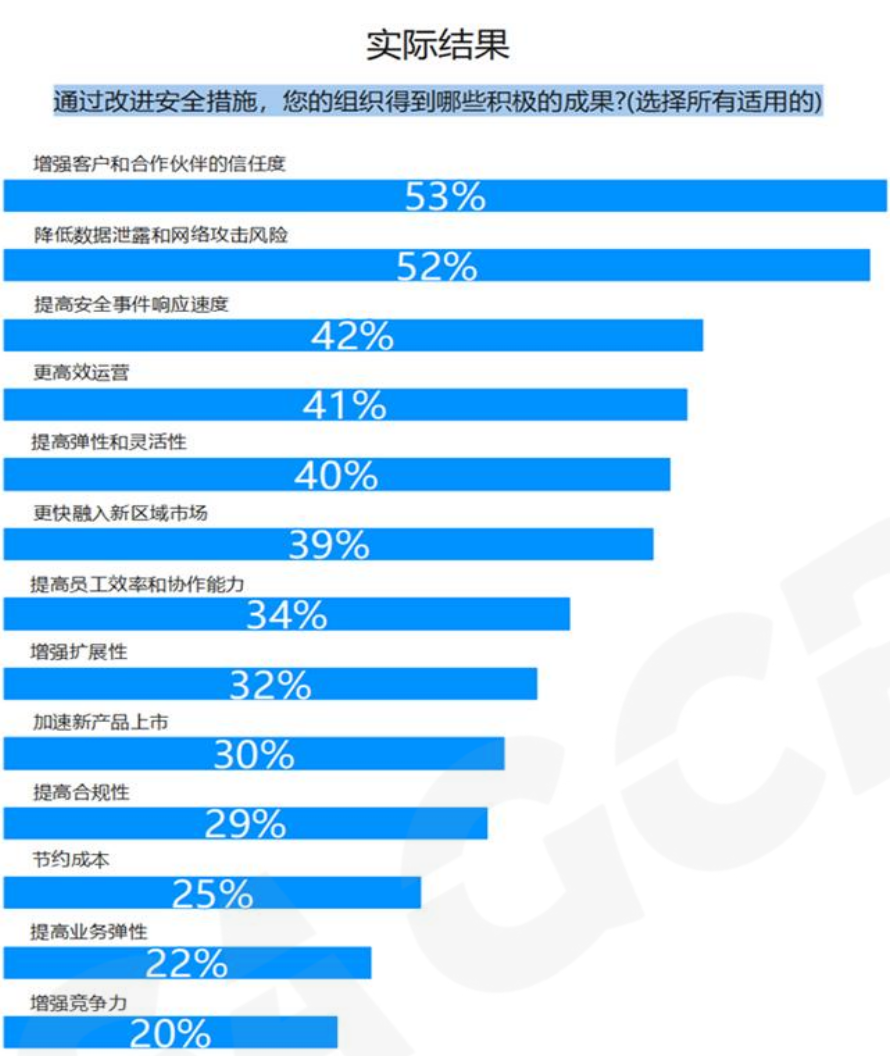


图 2 企业实施安全措施的实际成果

影响领域

调查显示，受到安全驱动创新影响最大的领域是安全运营(43%)和网络安全风险管理(42%)，紧随其后的是自动化和人工智能(36%)、云计算/虚拟化(34%)。对那些尚未实施安全驱动创新的企业的预测结果与上述调查结果近似，这表明这些企业对受影响最严重的部门或团队有着深刻的了解。同时也表明企业对创新将会影响到的领域以及创新对目标领域的影响都有清晰的了解。

成本

就成本影响而言存在着不同的观点。虽然大多数受访者认为基于安全驱动的创新会在一定程度上降低总成本（30%）或显著地降低总成本（28%），但仍有相当大比例的受访者预计成本会增加（26%）。那些仍需要继续采用这些措施的企业也预测到了类似的成本影响。这种存在分歧的调查结果表明企业对创新的态度可能直接与创新带来的成本增加或减少有关。也表明在创新初期，企业对创新是否会增加成本的认识是清晰的。

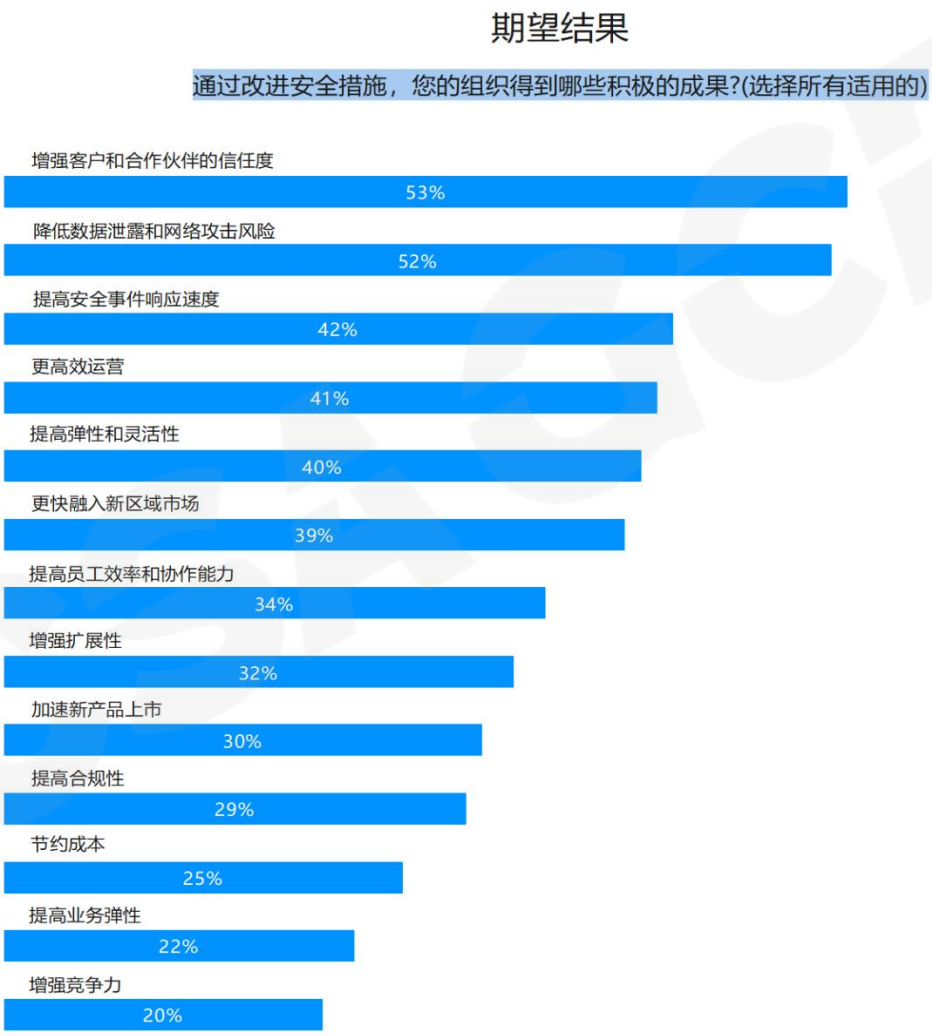


图 3 通过改进安全措施获得的积极成果

2.3. 主要结论 3：双刃剑:采用多云架构带来了优势，但也带来了成本和资源管理的挑战

调查显示，大多数企业都更加偏爱多云架构。数据显示其中 71%正在采用两个或更多的云架构环境，这种情况表明企业的战略正在向多云架构转变。采用多云架构并非是偶然的，事实上，79%的企业表示这是有计划的战略转变，只有 19%的企业表示采用多云架构是无意的行为。

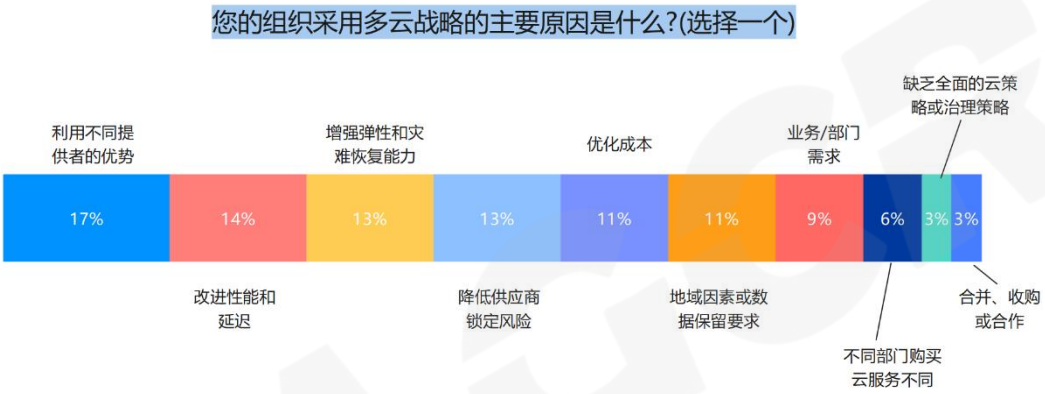


图 4 组织采用多云战略的主要原因

这一趋势的主要原因是多云基础架构自身潜在的好处。企业采用多云架构是为了利用不同供应商的优势（17%），改善性能和时延（14%），增强可靠性和灾难恢复（13%），以及减少供应商锁定（13%）。本次的调查对象主要是负责管理这些环境的安全和 IT 人员，他们对多云架构的积极态度可能会受到这些调查对象的影响。

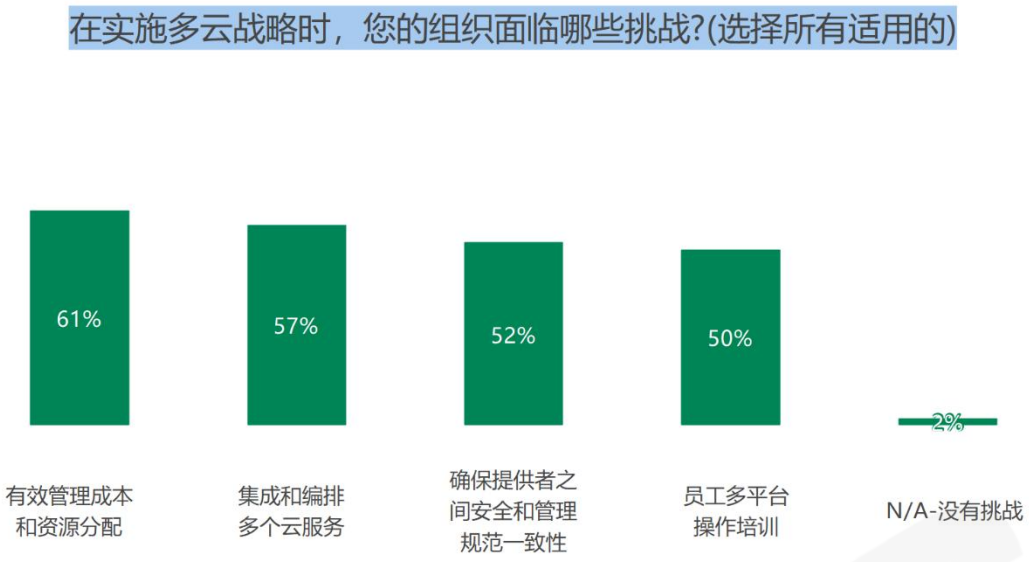


图 5 实施多元战略后组织面临的挑战

尽管采用多云架构为企业带来了许多好处，但也会面临一系列独特的挑战。值得注意的是，61%的企业报告称在多云环境下存在成本管理和资源分配的挑战。其他的严峻挑战还包括整合或编排多个云服务供应商（Cloud Service Providers, CSPs）（57%）、在不同平台上创建相同的安全管理规范（52%）以及对员工开展多平台操作的培训（50%）。

这些挑战导致企业需要重新考虑他们的云战略，包括回归本地的解决方案。这表明多云架构具有双刃剑特性：虽然它提供了灵活性、性能和弹性方面的明显优势，但也存在成本管理、资源分配以及跨平台安全管理相关的复杂性。因此，企业在制定云战略时必须谨慎评估与权衡。

2.4. 主要结论 4：将工作负载迁回本地的趋势日益增长

调查结果显示了一个令人震惊的趋势：59%的企业已经将工作负载从云端迁回本地，其中大部分迁移发生在过去 12 个月之内（34%）。这个趋势意味着企业的 IT 战略格局正在发生改变，标志着在最近几年云计算优先的趋势过去之后，重心可能会重新转向本地解决方案。65%的企业将业务策略或方向的转变视为推动工作负载迁回本地的首要原因。这一变化与近期因疫情导致的工作方式的改变也有关联。在企业加速数字化转型以适应远程工作的情况下，若员工回到现场办公时，他们需要将这些工作负载重新分配到本地。

迁移的直接原因是性能优化和更低的延迟需求，这意味着对云服务供应商的不满。正如前面提到的重要结论所述，企业倾向多云环境的关键因素是性能。企业在考虑特定需求或战略变化时，尽量在不同优势的云服务供应商与迁回本地的解决方案之间寻求最佳平衡点。

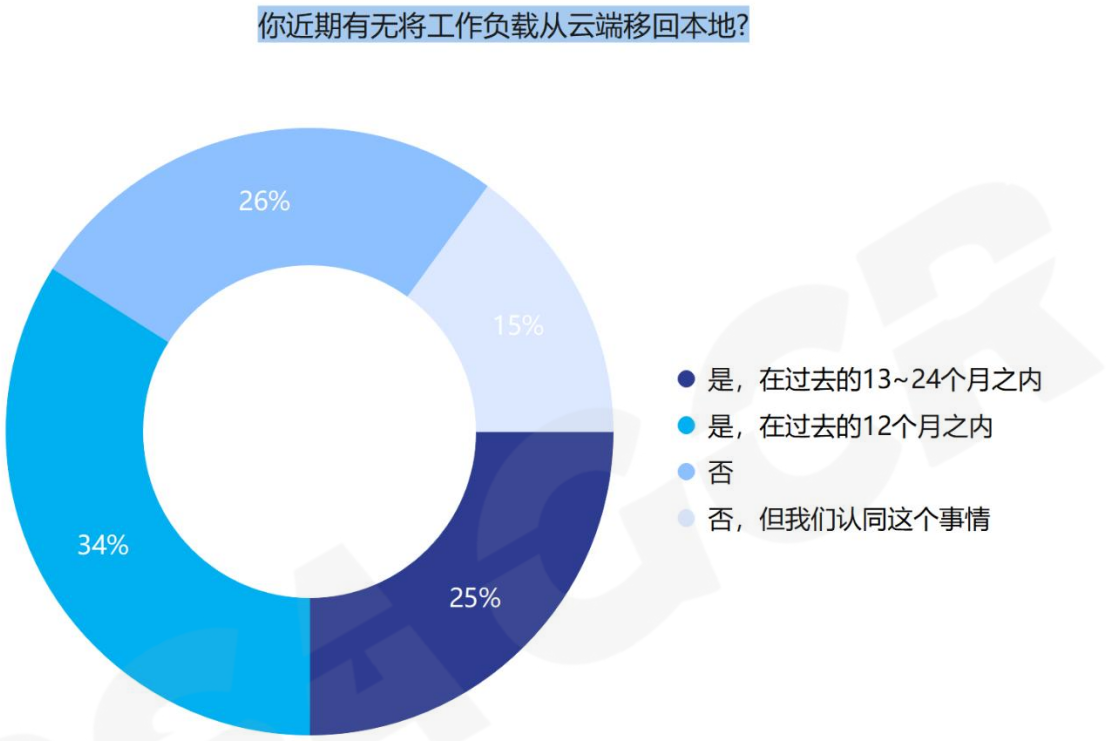


图 6 近期有无将工作负载从云端移回本地？

2.5. 主要结论 5：Kubernetes 和容器成为主角

调查结果还显示 Kubernetes 和容器在企业的日常运营中地位日益突出。随着企业努力加快流程以适应业务需求，越来越倾向于使用容器环境，其中 Kubernetes 是首选工具。调查显示，28%的企业已将所有应用全部迁移到了 Kubernetes 上，而 57%的企业已经迁移了部分应用。10%的企业考虑使用但尚未使用 Kubernetes。仅有 5%的企业声称他们尚未考虑使用 Kubernetes 或容器。这一趋势可能归因于行业内越来越多地采用 DevSecOps 和“左移”的实践。“左移”是指在应用程序开发的生命周期早期即引入安全措施，从而更早地发现漏洞并将风险降至最低。由于 Kubernetes 和容器具有可扩展性、可移植性和

灵活性等固有特性，能够很好的与这种理念相契合，从而使其成为敏捷、迭代式开发环境的理想选择。

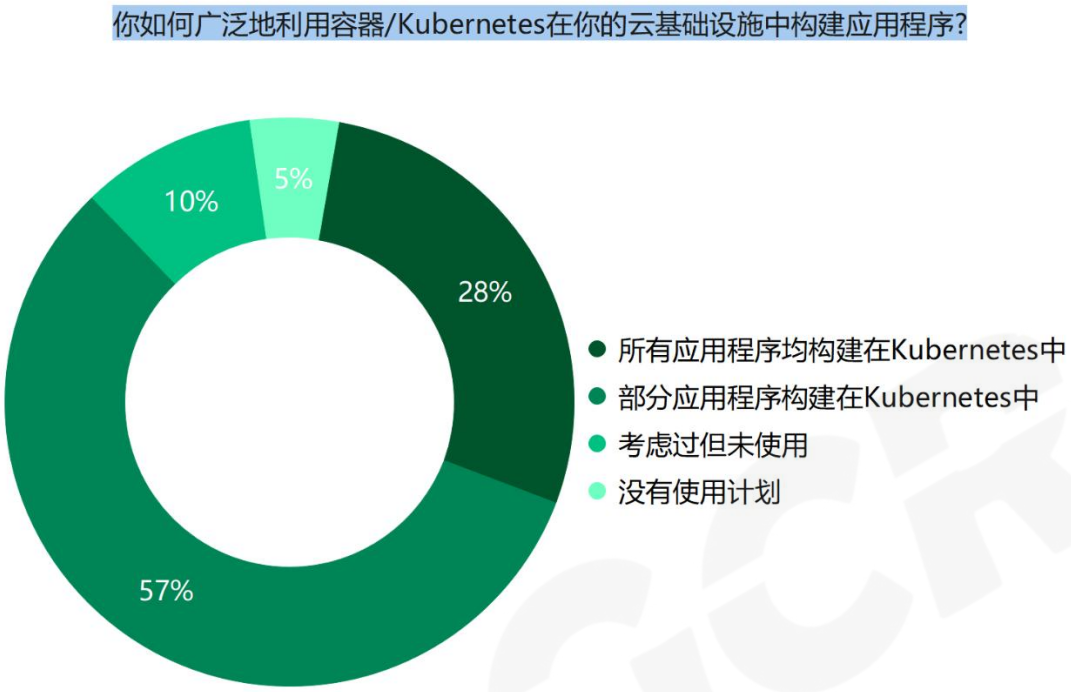


图 7 如何广泛的利用容器/Kubernetes 在云基础设施中构建应用？

3. 调查结果

3.1. 对安全的态度及其与创新的关系

安全在产品开发中的作用

大多数企业（61%）都将安全放在首位，24%的企业将安全放在首位并在开发过程中严格执行，37%的企业将安全放在首位，严格执行并持续优化。另有 20%的企业表示已将安全问题纳入开发流程。只有 6%的企业表示在开发过程中没有考虑安全。

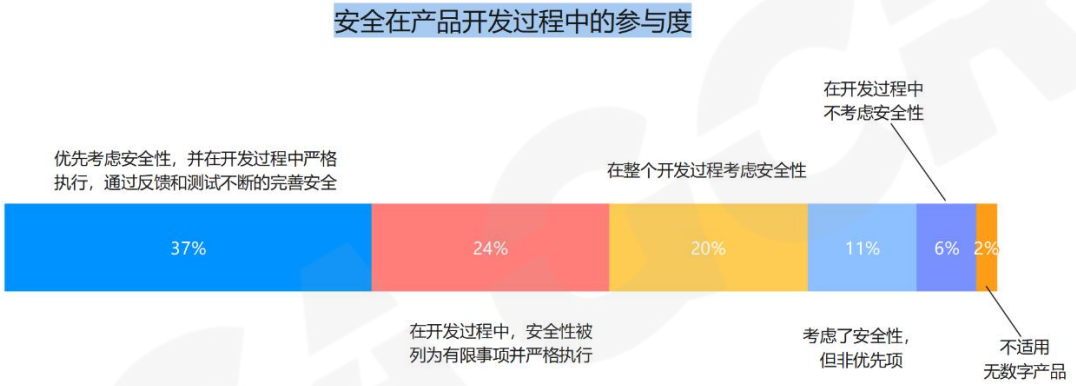


图 8 安全在产品开发过程中的参与度

安全在云计算战略中的角色

安全在企业的云计算战略中扮演着重要的角色，40%的企业表示会优先考虑安全，29%的企业表示已经采购了安全服务。只有 2%的企业声称没有做过任何安全方面的咨询。

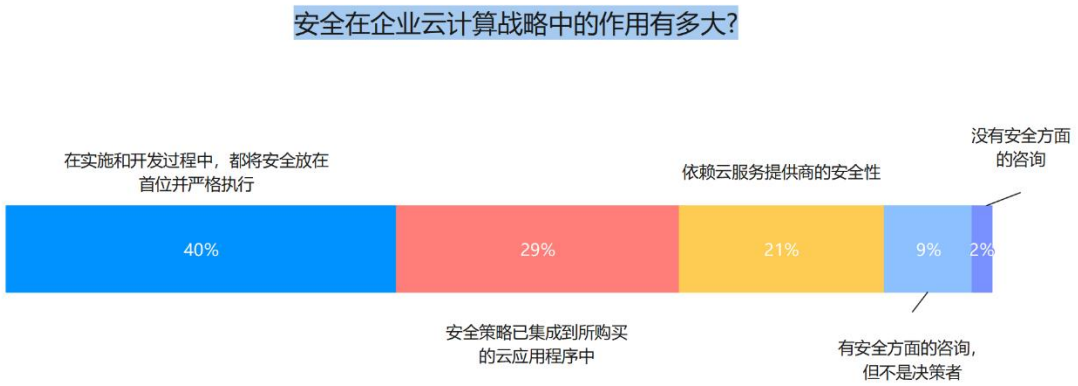


图 9 安全在企业云计算战略中的作用有多大？

安全运营的成熟度

调查要求受访者基于早期成熟度模型（最低成熟度）到高级成熟度（最高成熟度）模型的演变对企业的安全成熟度进行评级。大多数企业（70%）表示自己处于中间位置，40%的企业认为自己处于成熟状态，而相对成熟的有 30%。其余的 30%则分别位于高低两端，其中 14%属于低成熟度，16%属于高成熟度。

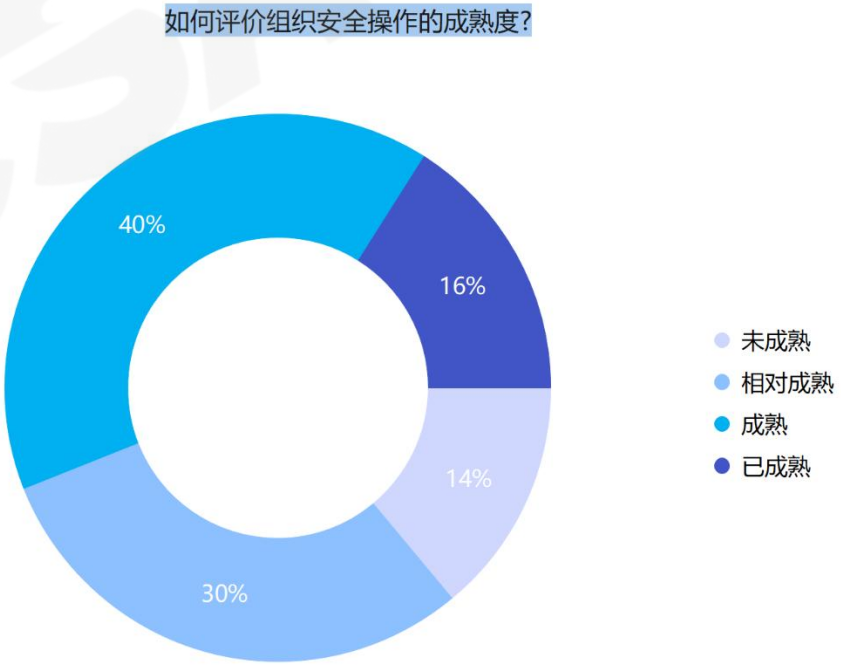


图 10 如何评价组织安全操作的成熟度？

安全态势感知能力对竞争优势的影响

大多数受访者（83%）认为，强大的安全态势感知能力将会提高企业的竞争优势。只有 10%的受访者认为安全态势感知能力不会影响企业的竞争优势，而有 6%的受访者则认为安全态势感知能力会降低企业的竞争优势。这些比例可能反映了企业对安全的重视程度，因为数据泄露和网络攻击会给企业带来巨大的经济和声誉损失。不过，由于被调查者主要是安全专业人员的原因，这个结论可能存在一些偏差。

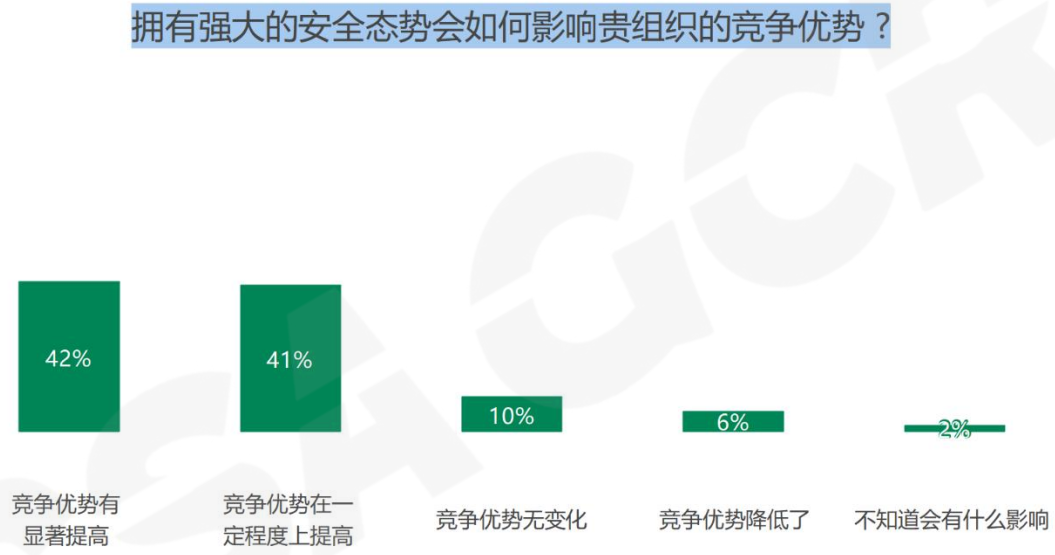


图 11 拥有强大的安全态势感知能力会如何影响贵组织的竞争优势？

实施新安全措施的驱动力

增加客户和合作伙伴的信任（60%）以及降低数据泄露或网络攻击的风险（57%）是推动企业采用新安全措施的主要驱动力。这也是目前为止最符合期望的驱动力。这些推动因素之间有着内在联系，因为数据泄露会导致客户或合作伙伴的不信任。有趣的是，尽管安全态势感知能力也被视为可以增加竞争优势，但增加这个竞争优势却是被选最少的选项（23%）。这可能是由于关于这个竞争优势的说法太过抽象而导致。能以更具体的方式表现竞争优势的选项则获得了更多认可。不同层级的员工认为的首要驱动因素也存

在一些差异。企业的高管和经理认为采用新安全措施的主要驱动因素是增加与客户和合作伙伴的信任度（分别为 68%和 63%），而降低数据泄露和网络攻击的风险则是总监和一般员工的主要关注点（分别为 63%和 59%）。

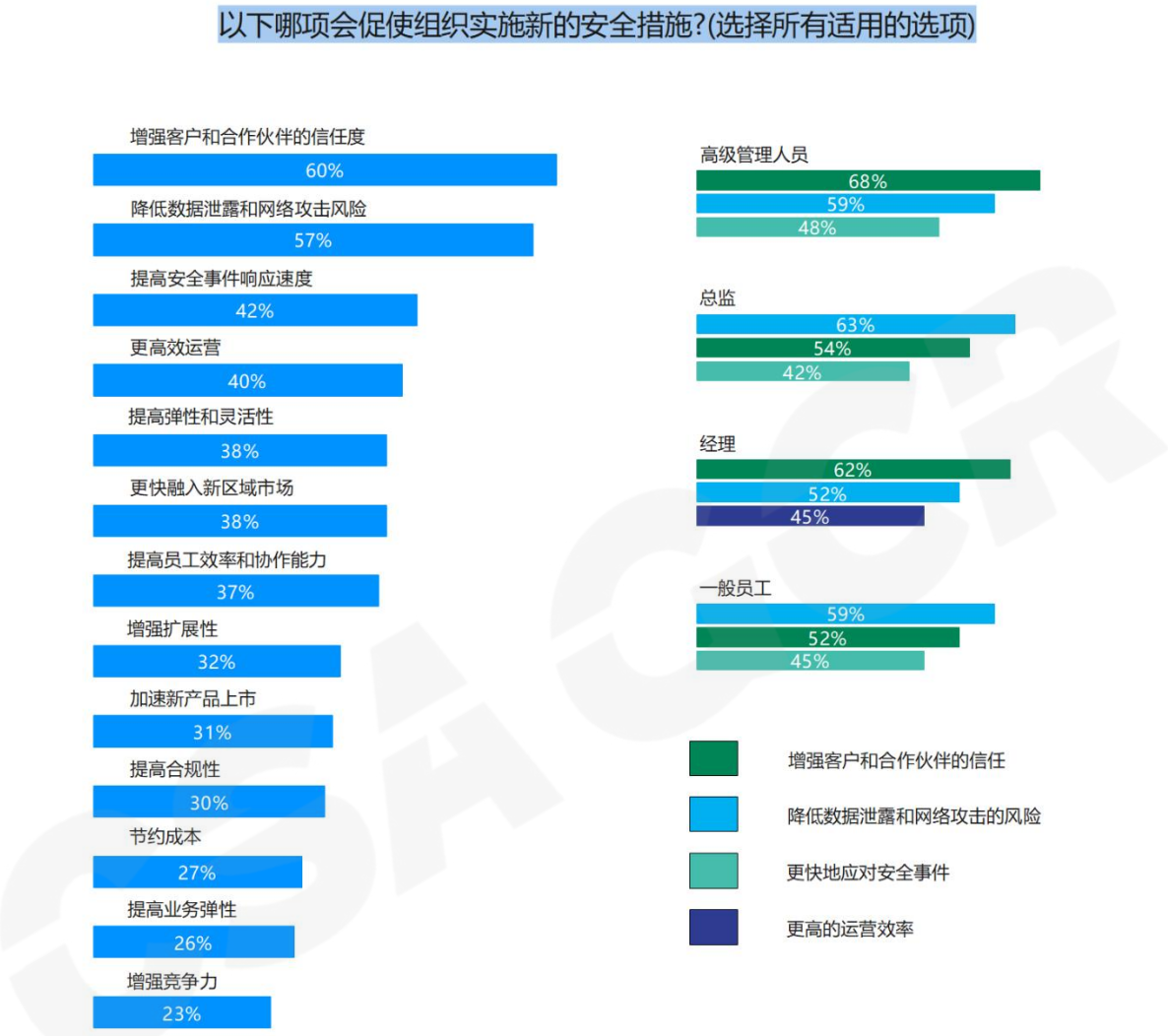


图 12 哪些选项会促使组织实施新的安全措施？

3.2. “安全是促进企业创新文化基本要素”的认可度

重视安全除了能提高企业竞争优势、云战略和产品开发之外，企业还认为安全与培养创新文化紧密相关。其中 47%的受访者表格非常赞同，36%的受访者表示基本赞同，只有 7%的受访者不赞同创新和安全之间存在联系。同样值得注意的是，由于受访者主要是安全专业人员和 IT 人员。如果受访者是其他部门人员，调查结果可能会有所不同。

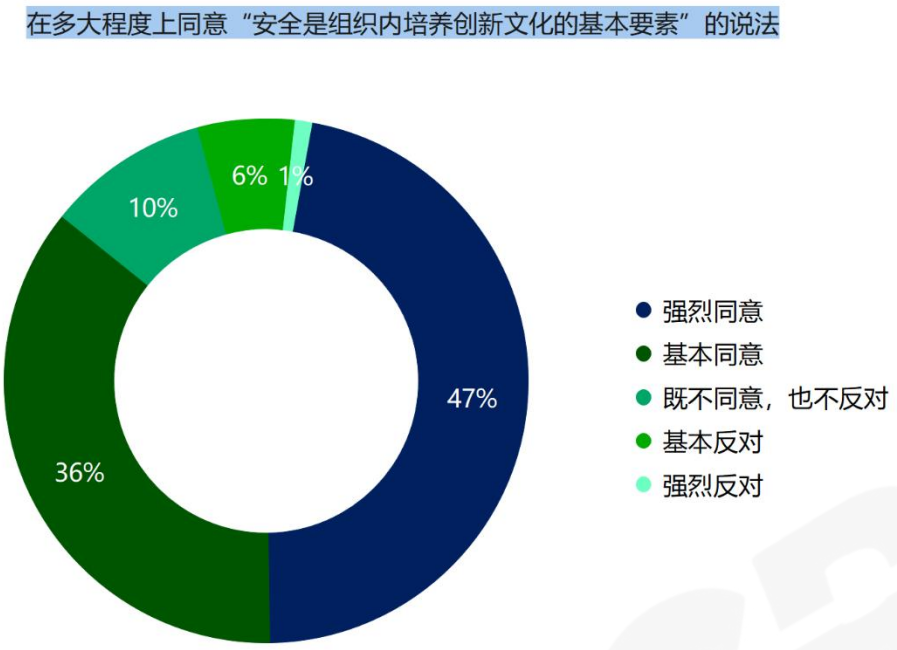


图 13 多大程度上同意“安全是组织内培养创新文化的基本要素”？

安全与创新之间的关系

当受访者被进一步问及对安全与创新之间关系的看法时，55% 的受访者认为安全是创新的重要推动因素，有 27% 的受访者认为安全很重要，但没有直接关系。只有 11% 的受访者认为安全会阻碍创新，另有 7% 的受访者认为两者之间没有关系。结合上一个问题的结果来看，专业的安全人士在安全是直接促进创新还是间接促进创新的问题上有些不确定。

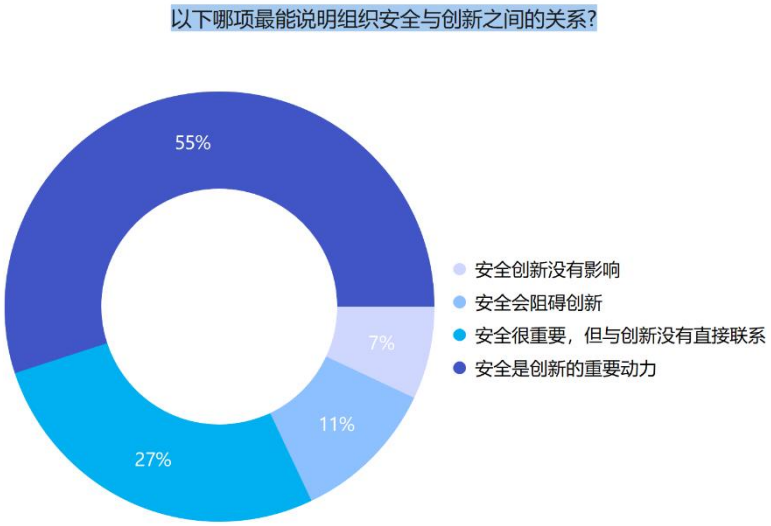


图 14 以上哪项最能说明组织安全与创新之间的关系？

对未来 5 年安全与创新之间关系的预测

对于未来 5 年安全与创新之间的关系预测，58%的人认为两者关系将会相互依赖且日益密切，另有 29%的人相信两者之间是两个独立但很重要的问题。最后有 9%的人认为安全会成为创新的一个次要方面。而只有 3%的人认为安全和创新之间的关系将不会有重大变化。

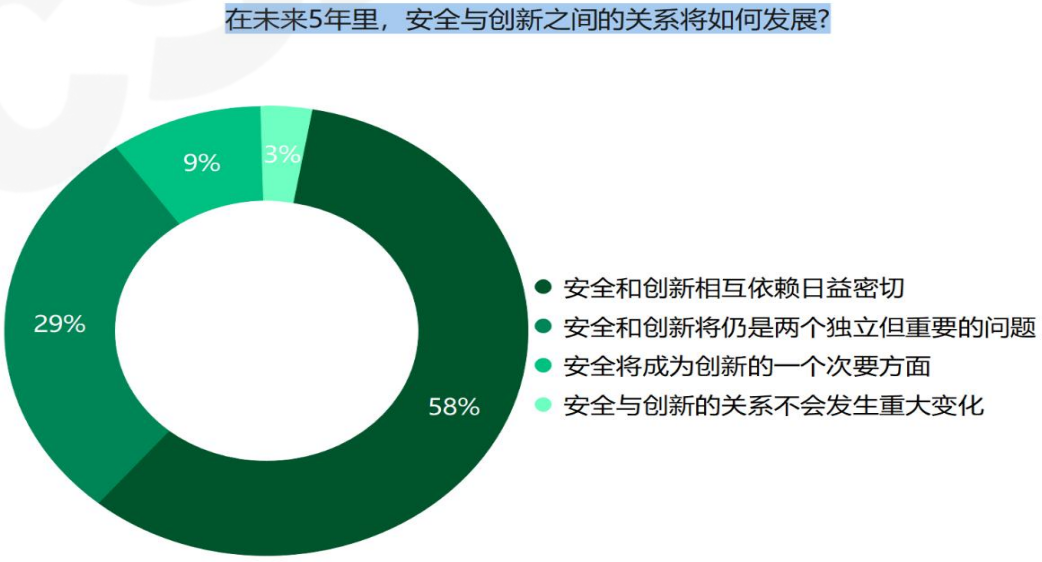


图 15 未来 5 年里，安全与创新之间的关系将如何发展？

实施支持创新的安全措施

许多企业都坚信安全能够促进创新，并采取了安全措施来支持创新（91%），只有 5%的企业明确表示没有采取此类措施，另外还有 4%的企业表示不确定是否采取了安全措施。

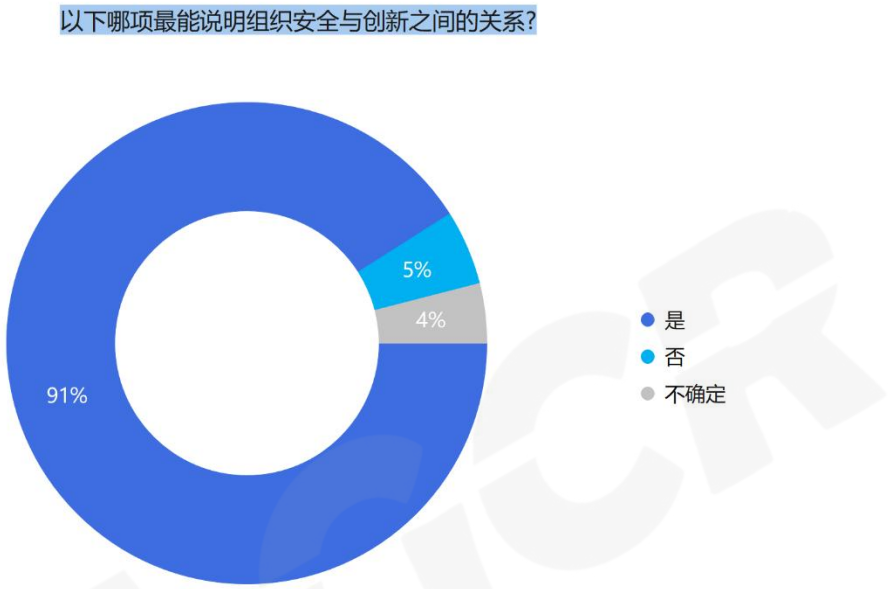


图 16 是否实施了支持创新的安全措施？

3.3. 安全驱动创新的实际状态和预测

安全驱动创新所带来的积极成果

企业已经通过采用安全驱动创新措施获得了积极的成果，包括增加了来自客户和合作伙伴的信任度（53%）和降低了数据泄露和网络攻击的风险（52%）。这个问题的结果与最初采用安全措施的驱动因素之间惊人地相似。这极大的鼓舞各个企业，因为这些好处正是他们采用这些措施时所期望的。

由于改进了安全创新措施，您的组织得到了哪些积极的成果？（选择所有适用的）

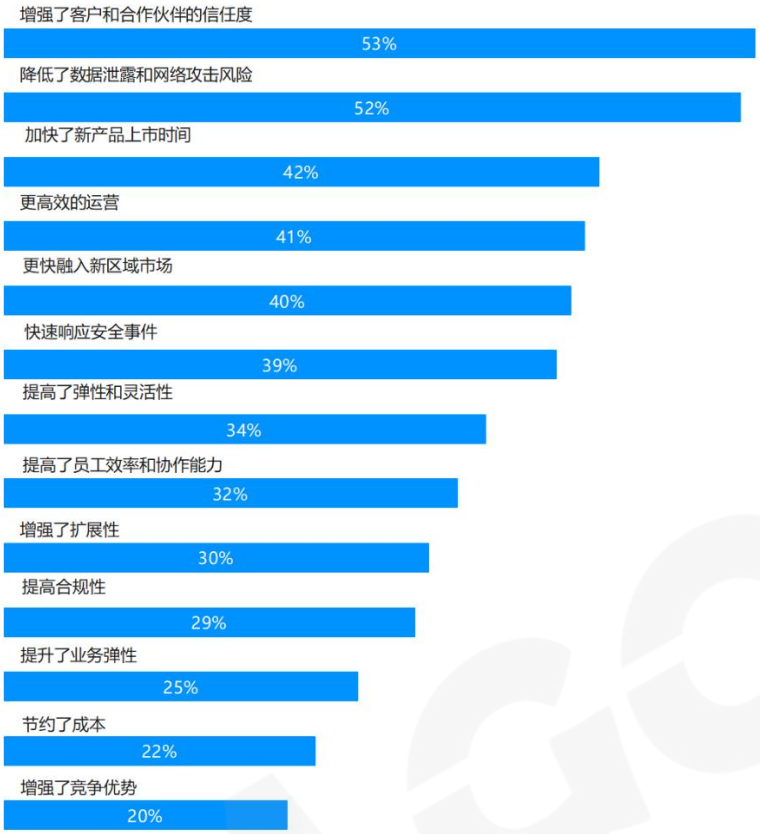


图 17 由于改进安全创新措施得到了哪些积极的成果？

安全驱动创新的成本

大多数已实施安全驱动创新的企业在评估业务成本时，认为稍微降低（30%）或显著降低（28%）了整体成本。有趣的是，第二个最常见的反应是增加了多少成本（26%）。在安全驱动创新和成本方面，结果喜忧参半。那些还没有采用安全措施来实现创新的企业，他们预测对业务成本的影响也遵循了类似的模式，但在稍微降低成本（40%）和稍微增加成本（33%）方面的比率略高。

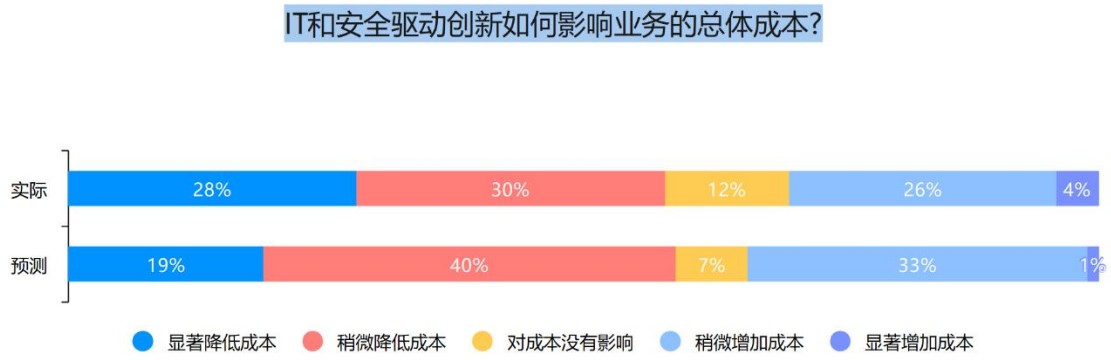


图 18 安全对创新的成本有多大影响?

受安全驱动创新影响最大的领域

受到安全驱动创新影响最大的领域是安全运营（43%）和网络安全风险管理（42%）。这可能是由于安全和技术团队对维护或运作这些安全措施的需求增加所致。排名第三的选择最多的是自动化和人工智能（AI），占 36%，其次是云计算、虚拟化，占 34%。那些还没有采用安全措施来实现创新的企业对自己将受到最大影响的领域的预测也类似。前四名是相同的，但顺序略有不同，网络安全风险管理的选择最多（38%），其次是自动化和人工智能（37%），然后是云计算、虚拟化（35%），最后是安全运营技术（34%）。类似于安全驱动创新的预测成本和实际成本相比，企业大致了解安全驱动创新对哪些部门的影响最大。

在哪个领域，IT和安全创新对组织的业务有重大影响?(最多选择3个)

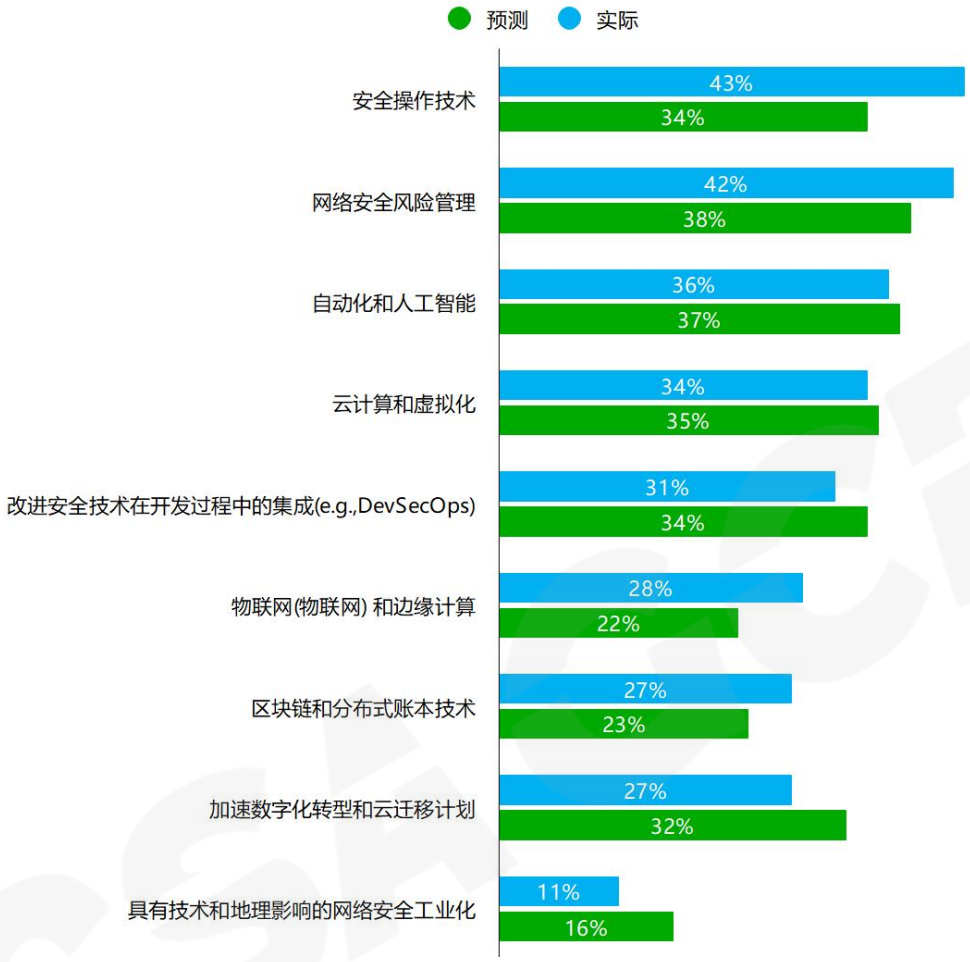


图 19 安全驱动的创新对组织有多大影响？

安全驱动创新带来的挑战

在安全驱动创新面对的实际挑战与预测中也发现了类似的模型。企业实际面临的最大挑战是 IT 和安全基础设施的复杂性（56%）、招聘和留住熟练的安全专业人员（54%）、合规性和数据隐私（45%），以及安全与用户体验之间的平衡（44%）。对于那些尚未采用安全措施来实现创新的企业来说，预测的四大挑战几乎完全相同。结合本节中的其他结果，企业似乎高度意识到安全驱动创新对其企业的影响，无论这些影响是积极的还是消极的。

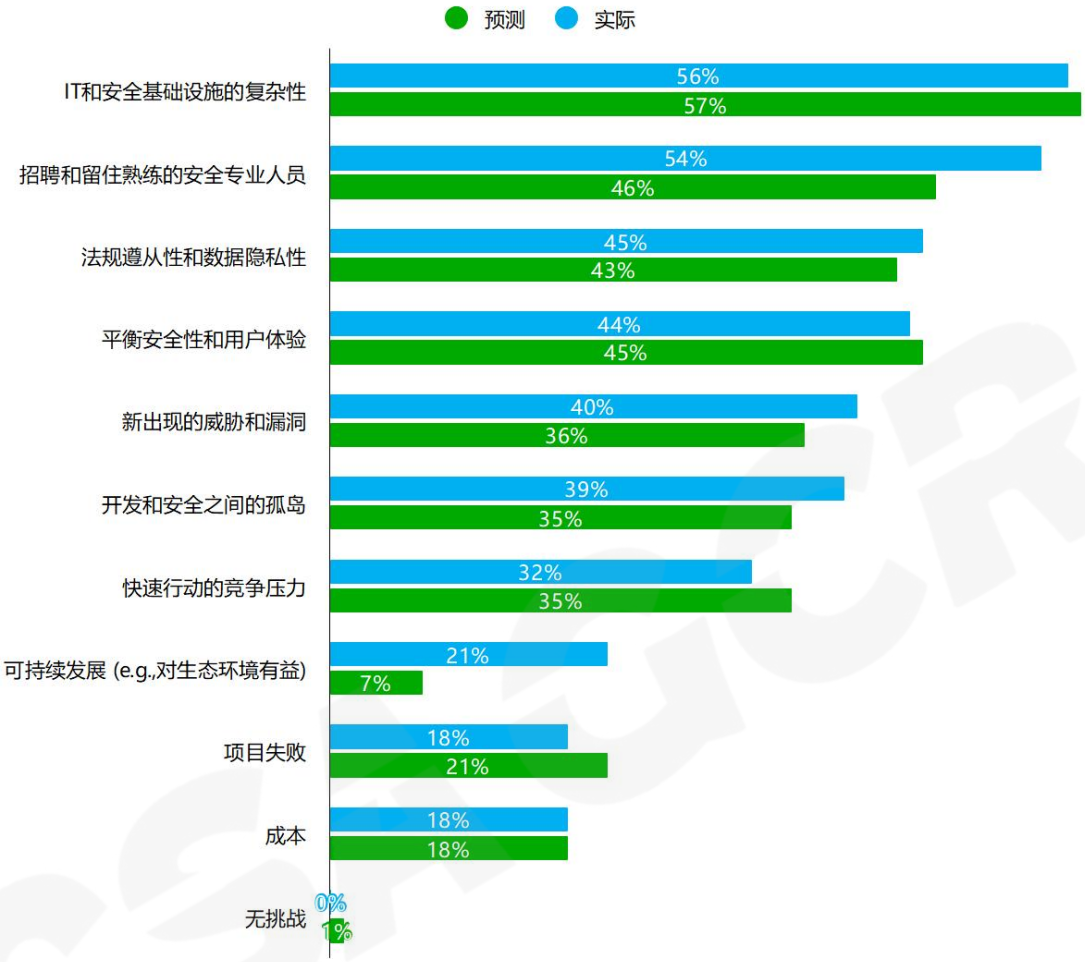


图 20 安全和 IT 功能创新会导致业务面临哪些挑战？

3.4. 云趋势：多云的使用

企业所使用的 CSP 数量

大多数企业(71%)采用两个或更多的云环境，显示出对多云环境的强烈偏好。只有28%的企业表示采用单一的云供应商。本节中的问题仅由采用多云环境的企业回答。

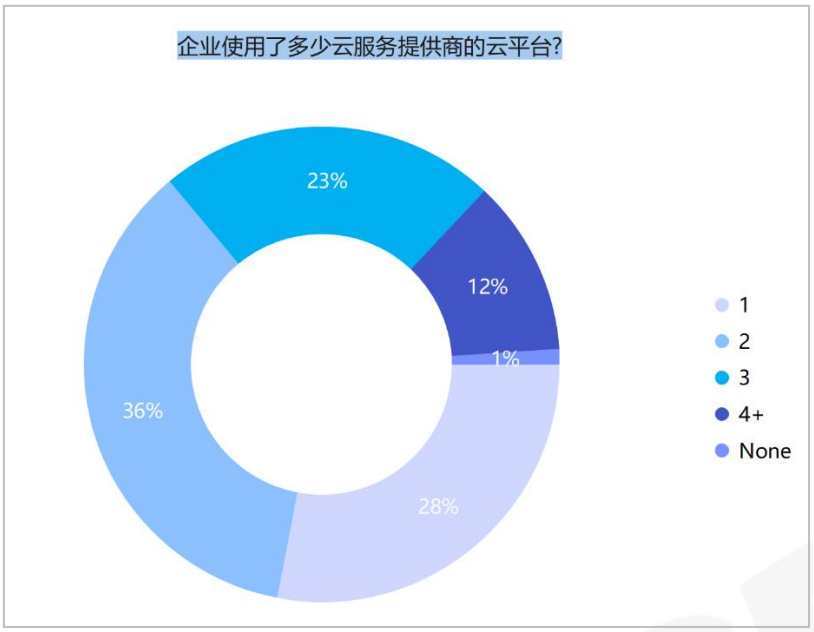


图 21 企业使用多少种云平台？

主动 vs. 被动采用多云环境

评估了采用多云环境的目的性，得到如下结论。大多数企业(79%)声称他们主动采用了多云环境，只有 19%的企业声称他们在某种程度上采用多云是被动的。这进一步表明了采用多云环境是业界当前的首选想法。

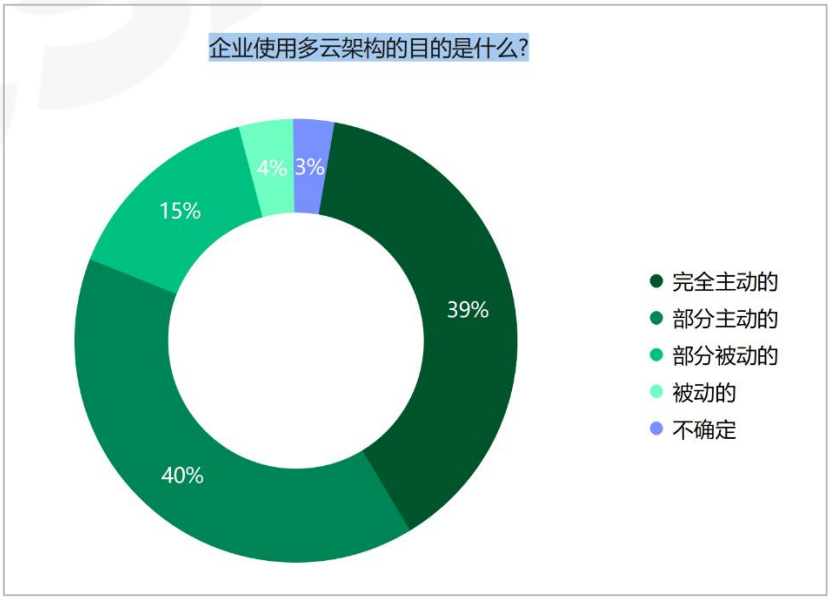


图 22 企业使用多云架构的主动性

采用多云的原因

企业采用多云的主要原因是利用不同供应商的优势(17%)，提高性能和降低延迟(14%)，其次是增强弹性、灾难恢复能力(13%)，以及减少供应商锁定(13%)。排名前三的原因反映出，功能和性能是多云战略受到青睐的原因。关于主动采用多云的原因，例如合并、收购或合伙(3%)、缺乏全面的云或治理策略(3%)以及不同部门购买云服务时缺乏协调(6%)等，则是最少的选项。这些结果强有力的支持了企业是主动采用多云的观点。

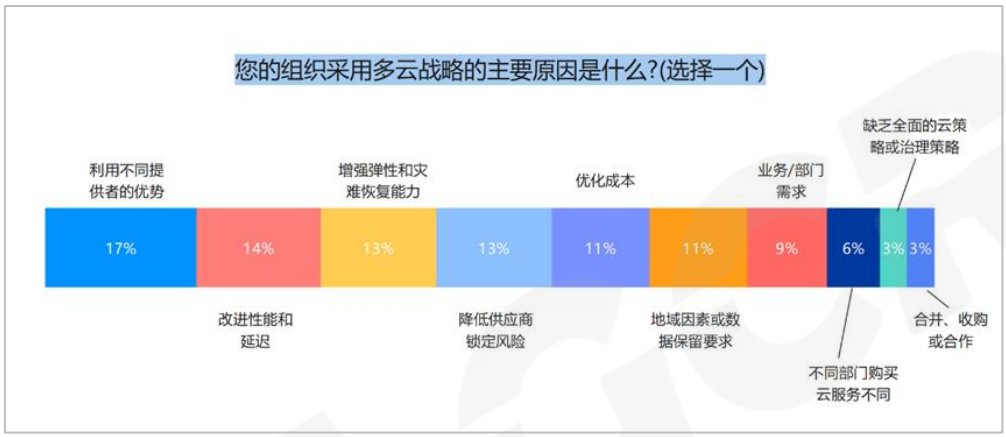


图 23 组织采用多云战略的原因

管理多云环境时的复杂程度

近一半的企业认为管理多云环境比较复杂(49%)。非常复杂和有些复杂的占比相似，分别为 23%和 24%。

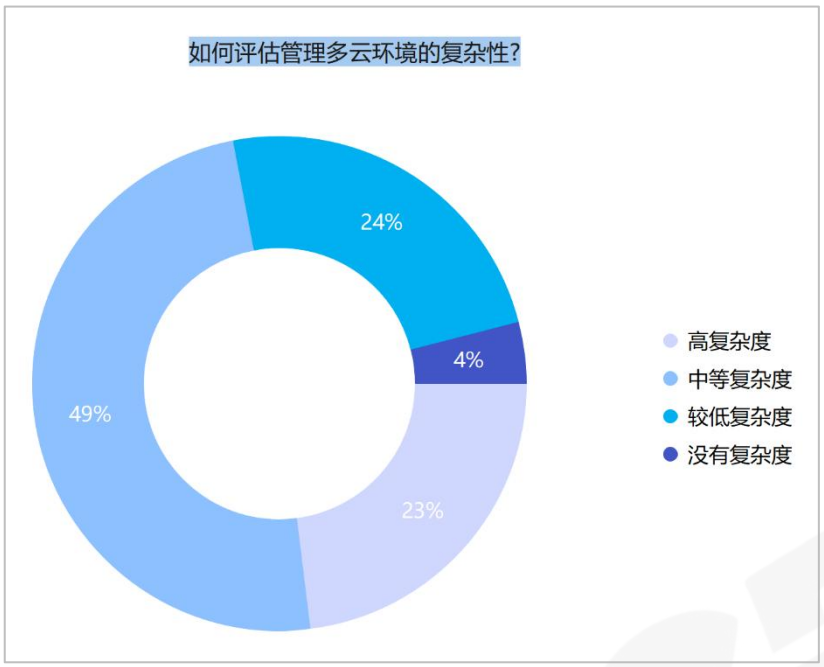


图 24 管理多云环境的复杂度

实施多云战略的挑战

企业在实施多云战略时面临的最常见挑战包括：成本管理和资源分配(61%)，整合和协调多个 CSP (57%)，确保跨平台安全管理策略的一致性(52%)，以及对员工进行多平台和技术培训(50%)。在之前采用多云战略的原因中，有 11%的人表示成本优化是主要原因。结合这些结果来看，成本管理更像一个挑战，而不是多云的好处。只有 2%的企业表示多云战略没有挑战。

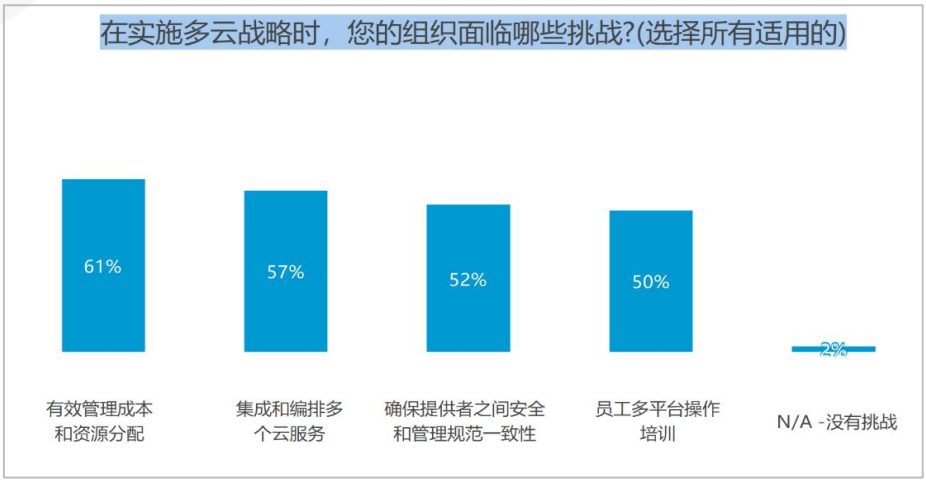


图 25 实施多云战略面临的挑战

使用 Kubernetes 或容器

大多数企业在云基础设施上使用 Kubernetes 或容器构建应用程序。57%的企业部分应用程序使用了 Kubernetes/容器，28%的企业所有应用程序都使用 Kubernetes/容器。另有 10%的企业表示还未使用 Kubernetes/容器但正在考虑使用，只有 5%的企业表示根本没有使用 Kubernetes/容器的计划。可能是受 DevSecOps 或安全战略“左移”的趋势驱动，整体上大多数企业对 Kubernetes/容器表现出了明显的偏好。

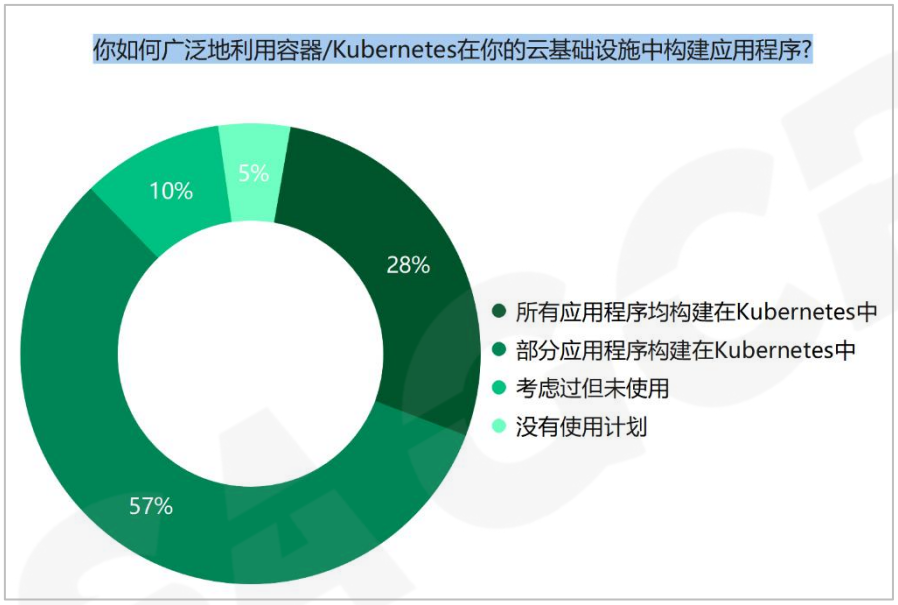


图 26 采用容器构建云基础设施的参与度

云战略中使用的环境

最常用的三个云平台是 AWS(62%)、GCP(54%)和 Azure(52%)。结果有些不同寻常，因为在之前的调查中，GCP 云平台的使用率通常只有 30%左右，而 AWS 和 Azure 一般都是首选平台。这表明受访者数据可能存在一些偏差。因为到目前为止，市场份额并没有发生重大变化。

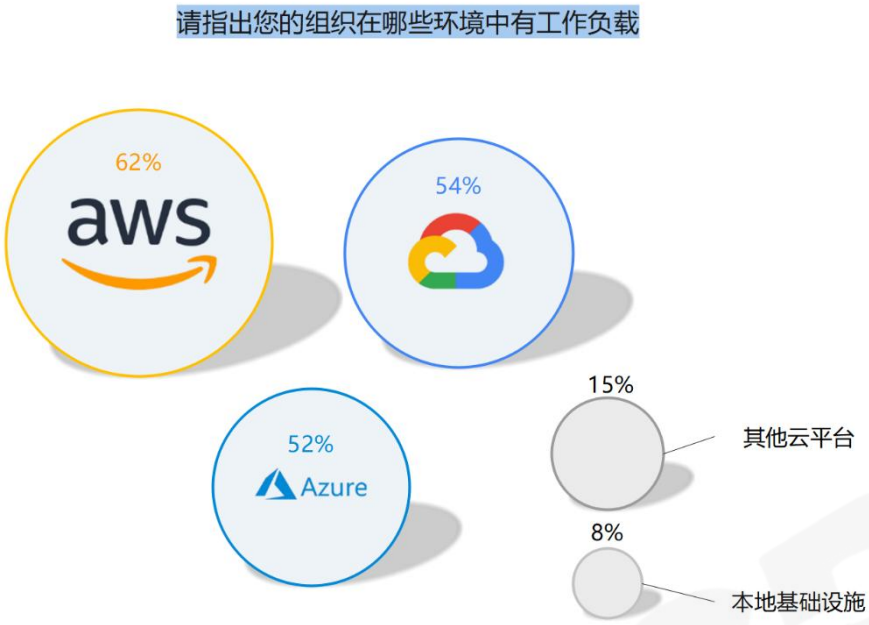


图 27 采用了哪些云？

云和本地环境的主要用途

在确定了企业的基础设施所使用的环境后，他们被要求指出每个环境的主要用途。尽管不同环境的主要用途没有太大差异，但一个显著的趋势是 AWS 主要用于部署企业 IT 应用程序。相比之下，其他环境则主要用于部署企业 IT(如：协调工作的应用程序)和生产/LOB 应用程序(如：自定义应用程序或特定功能的内部应用程序)。

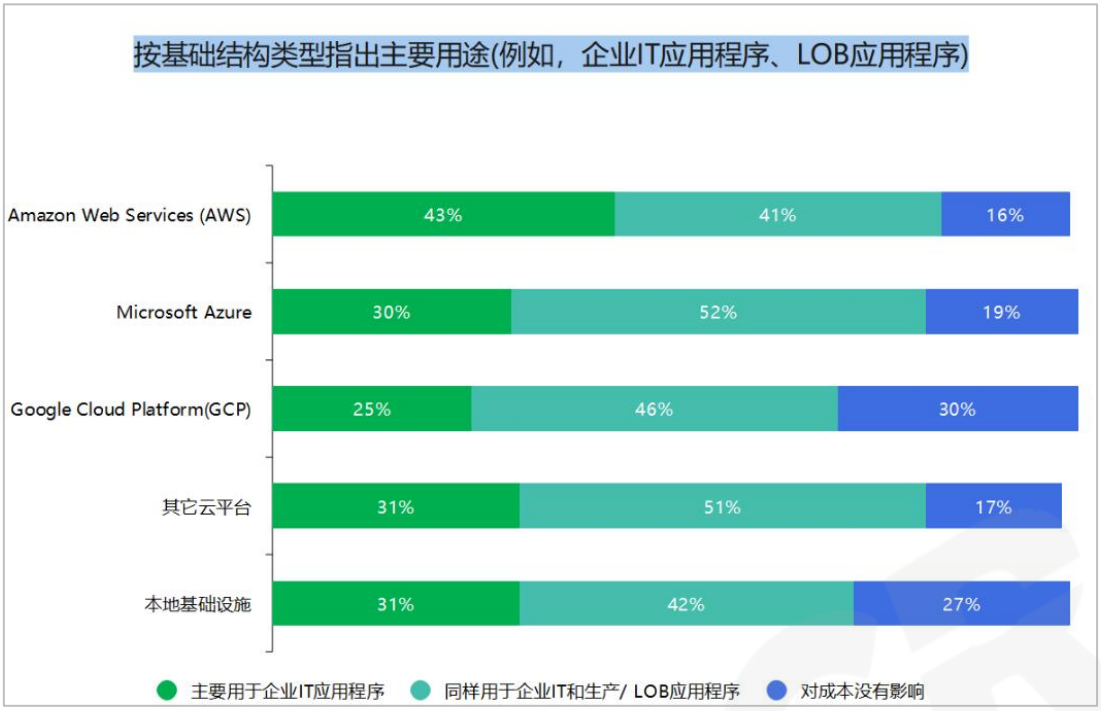


图 28 云和本次基础设施的主要用途

3.5. 迁出云

最近迁回本地的工作负载

以下是一些令人感到震惊的数字：59%的企业表示，他们已经将云上的工作负载重新迁回本地，大多数企业是在过去 12 个月内迁回（34%）；还有 15%的企业正在考虑迁回；大约四分之一（26%）的企业表示，他们不会将工作负载从云中迁出，也没有考虑过这样做。这些数据说明，企业存在将工作负载迁回本地的趋势，而且这种趋势可能还在逐渐上升。本节中的以下问题主要针对那些表示他们已将工作负载迁回本地的企业。

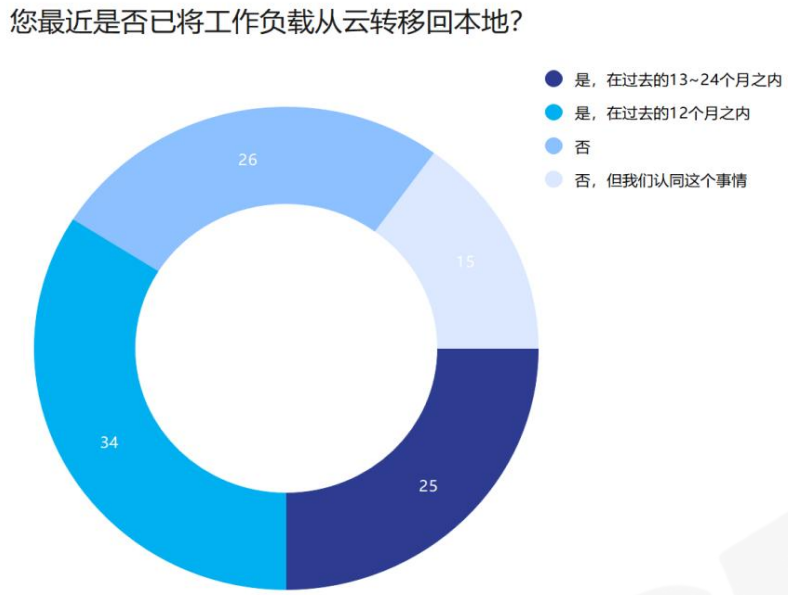


图 29 工作负载是否迁回本地?

将工作负载迁回本地的主要原因

将工作负载从云端迁回本地的前三个原因，第一个是性能优化（55%），其次是数据隐私问题（48%）和更低的延迟（40%）。这些结果表明，性能因素是工作负载迁出云的主要原因。

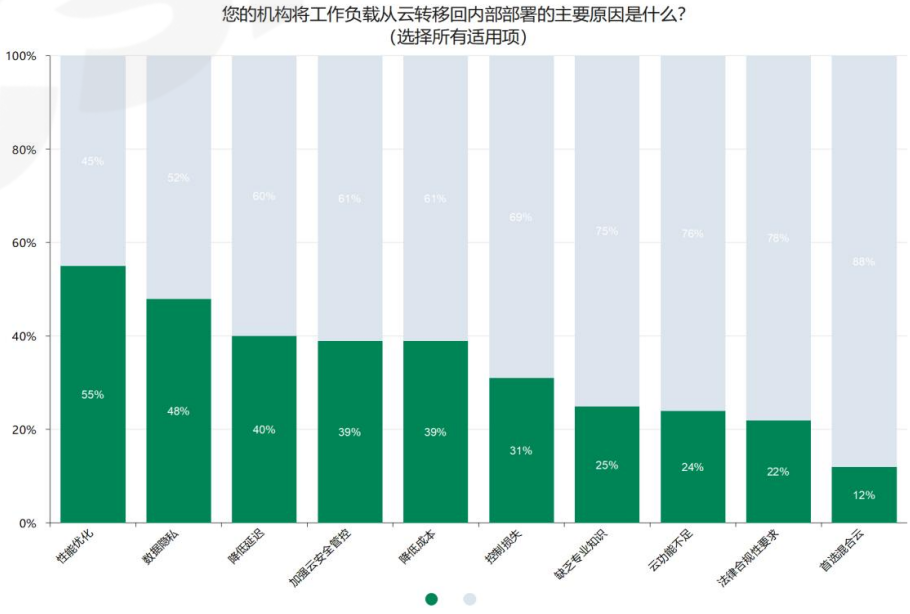


图 30 将工作负载迁回本地的原因

导致迁回本地的情况

导致将工作负载重新迁回本地的首要情况是企业业务战略或方向的变化（65%）。部分原因可能是员工办公方式从远程逐渐回归办公室。在最近的新冠疫情期间，许多企业加快了数字化转型，以实现远程办公。当员工回归办公室时，他们会将这些工作负载重新转移到本地。导致迁回本地的其他常见情况包括对云服务供应商的不满（47%），这可能也是由于上一个问题中提到的性能和延迟问题引发的。最后，对云服务供应商的不满、数据泄露和安全事件（44%）被选为最常见的三种情况。同样，这可能与上一个问题中提到的数据隐私问题有关。

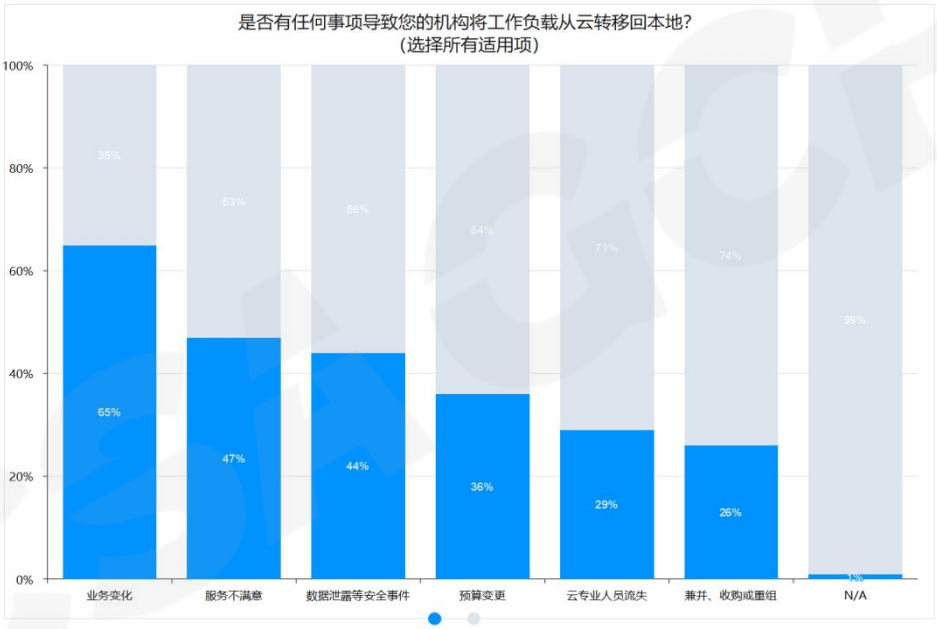


图 31 导致迁回本地的原因

从云中迁回本地的工作负载类型

企业最常见的迁回本地的工作负载的类型是开发和测试环境（58%）以及客户关系管理（CRM）系统（56%）。测试和开发环境的迁回可能更多地是由于它们的动态性，而不是正式从云迁回本地。也就是说，这些类型的工作负载（测试和开发、CRM）符合迁回本地的前两个原因，即性能优化和数据隐私问题。其他常见类型的工作负载包括数据存储和备份（41%）以及应用程序托管（39%）。

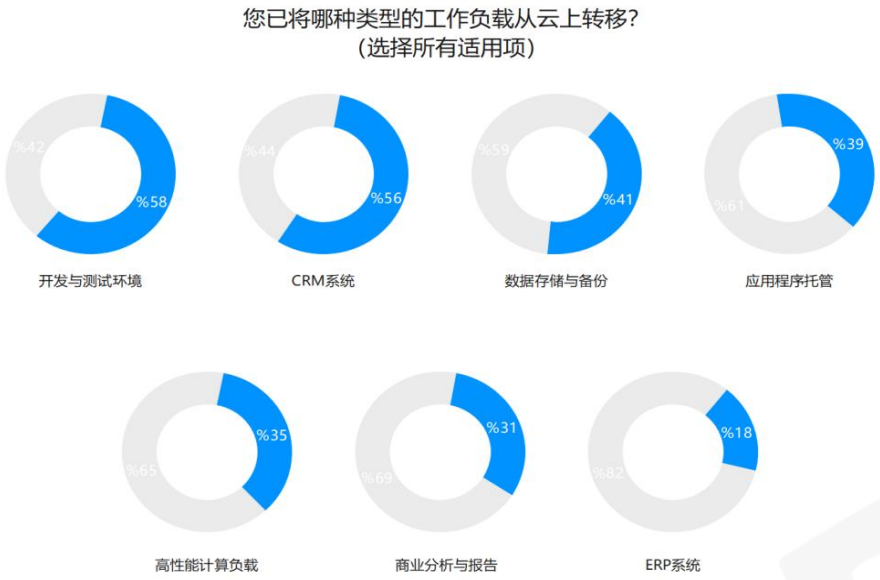


图 32 将工作负载从云上迁回的业务类型

将工作负载从云中迁回本地的复杂性

大多数企业统计结果显示将工作负载从云中迁回本地的复杂度为中等复杂（48%）到非常复杂（27%）。另有 22%的企业表示这有点复杂，只有 4%的企业表示根本不复杂。

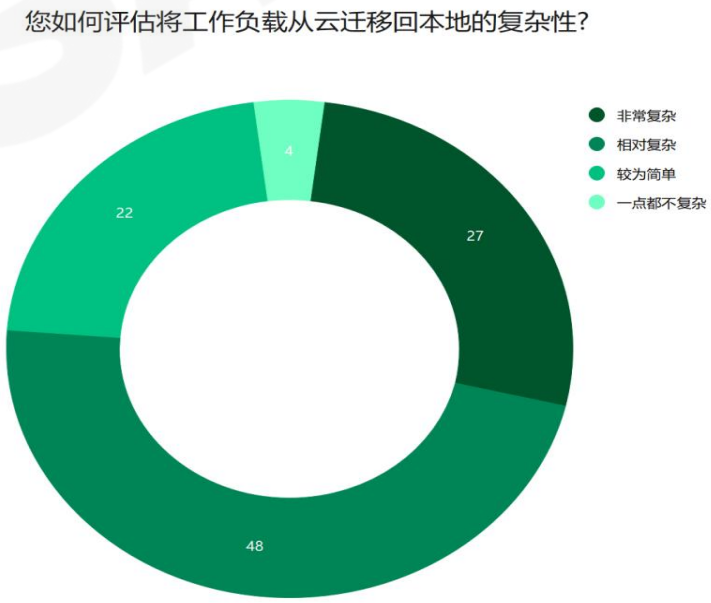


图 33 对工作负载从云上迁回本地的复杂度评估

4. 结论

总之，调查结果凸显了企业 IT 策略的发展趋势，这是由于安全在促进创新方面日益不可或缺的作用、多云环境的采用以及将工作负载迁回本地的解决方案的趋势所驱动的。容器化的趋势和 Kubernetes 的兴起进一步加强了这种演变，这也反映了业界对适应性、可扩展性和可移植解决方案的偏好。而更重要的是，企业应促进与员工对安全策略达成共识、充分利用多云环境的优势，并仔细权衡潜在的挑战，来应对多云环境的复杂性。

与此同时，企业高管和员工在看待安全在创新中的作用这一观点上存在差异，这表明企业急需改进内部沟通策略。在企业努力优化运营、提高绩效和降低管理成本的同时，建立一个对企业安全策略有一致认识的文化愿景。通过促进有效的双向沟通，企业高管和员工可以在对安全在创新中的作用方面达成共识，并能够成功应对不断变化之环境的机遇和挑战。

5. 本报告的统计范畴

该调查由 CSA 于 2023 年 5 月在线进行，收到了来自不同规模和地点企业的 IT 和安全专业人员的 1018 份回复。

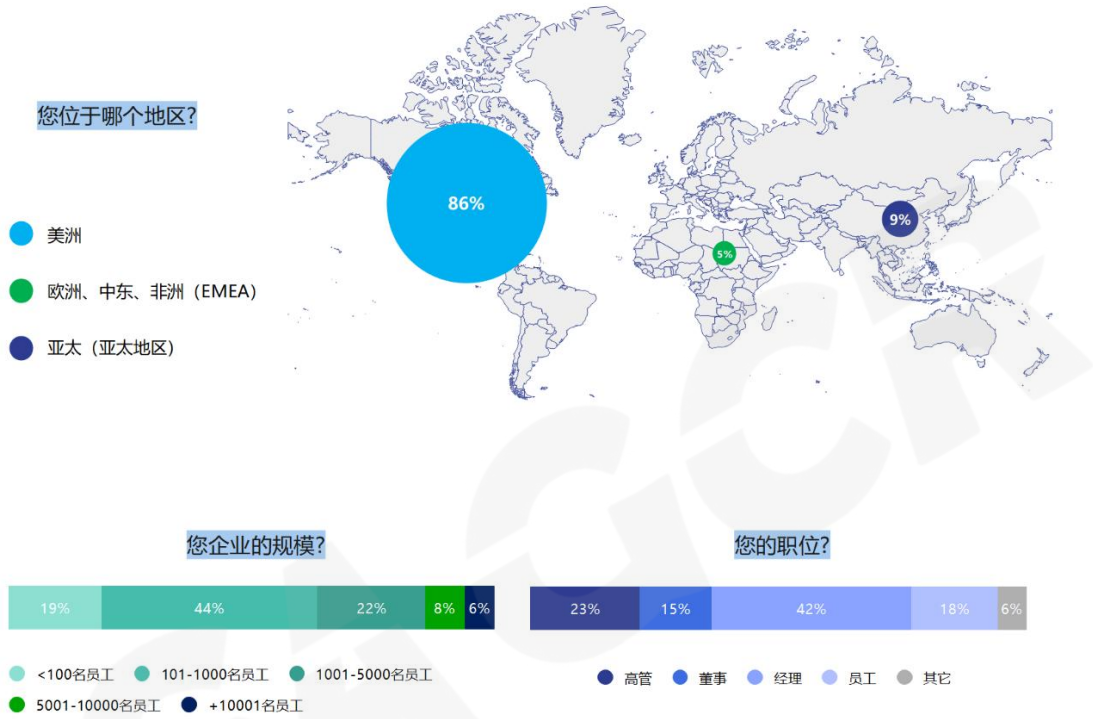


图 34 本次调研对象所处地区、职位和企业规模

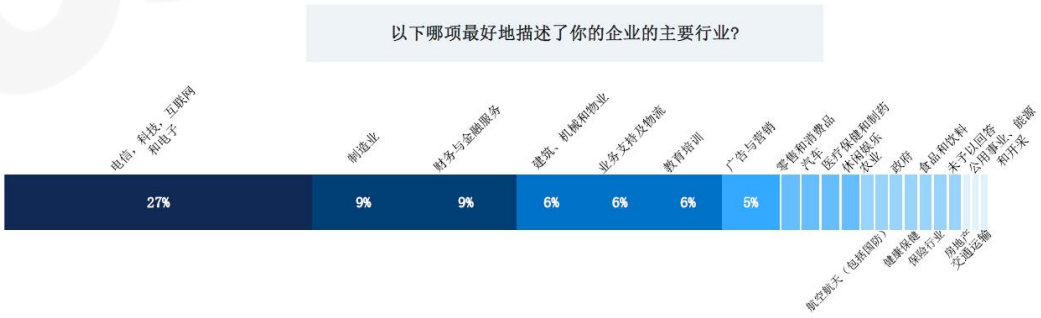


图 35 本次调研对象所处行业

CSA GCR cloud security alliance
GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905