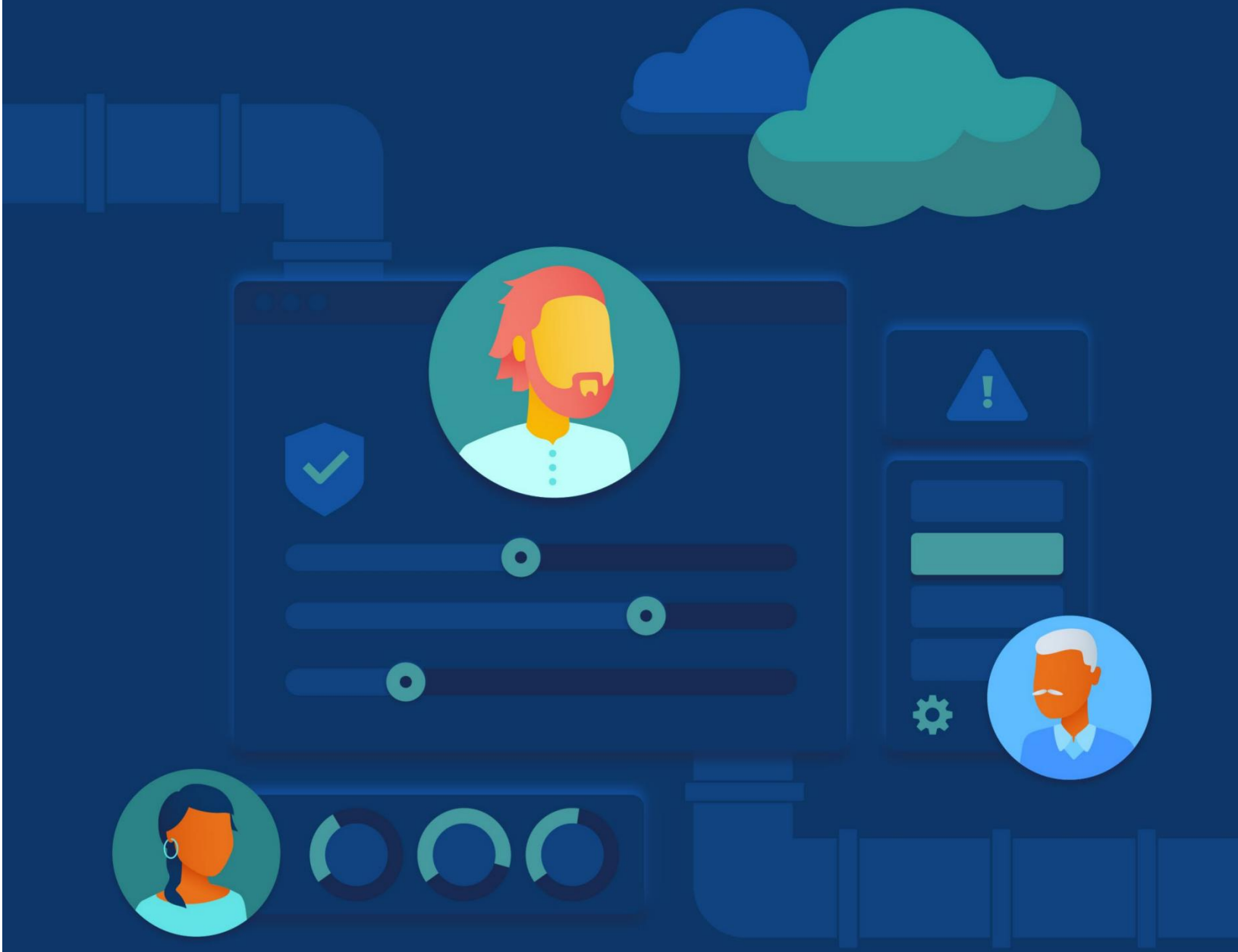
云安全风险、合规性和配置不当报告



CloudHealth by vmware

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

致谢

本文档《云安全风险、合规性和配置不当报告》(The State of Cloud Security Risk, Compliance, and Misconfigurations)由 CSA 工作组专家编写，CSA 大中华区秘书处组织翻译并审校。

中文版翻译专家（排名不分先后）

组 长：李岩

翻译组：林艺芳 沈勇 欧建军 吴贺 江澎 王彪 杨喜龙 伏伟任 江楠 王永霞 杨天识

审校组： 李岩 郭鹏程 姚 凯

感谢以下单位对本文档的支持与贡献：

启明星辰信息技术集团股份有限公司 北京天融信网络安全技术有限公司

北京北森云计算股份有限公司 腾讯云计算（北京）有限责任公司

上海缔安科技股份有限公司

英文版本编写专家

主要作者：Hillary Baron

贡献者：Josh Buker Sean Heide Alex Kaluza Shamun Mahmud John Yeoh

设计者：Stephen Lumpe AnnMarie Ulskey

特别感谢:：Nikhil Girdhar *Product Marketing Leader CloudHealth® by VMware*

Lauren van der Vaart *Senior Content Marketing Specialist Multi-Cloud, VMware*

在此感谢以上专家。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给与雅正! 联系邮箱：research@c-csa.cn；国际云安全联盟CSA公众号。

目录

致谢 3

1.调研的开展和方法论 6

1.1研究目的 6

2.概要 7

关键发现 1 7

关键发现 2 8

关键发现 3 9

安全部门仍然在努力对齐安全方针及(或)方针落地 9

部门间在安全方针和执行方面的一致性对主动安全至关重要 10

3.云安全程序的当前状态 11

3.1使用共有云提供商 11

3.2公有云的年度预算 11

3.3对抗云安全漏洞的总体信心水平 12

3.4对防御云漏洞威胁的能力充满信心 12

3.5 解决安全问题的障碍 13

3.6安全方针制订与落地执行的跨部门协作 13

3.7度量安全性和合规性状况 14

4.正在使用的云安全工具 14

4.1用于云安全的解决方案 14

4.2对云服务提供商安全解决方案的满意度 15

4.3使用托管服务提供商 15

5.云安全状态管理 15

5.1识别配置不当 15

5.1.1负责检测、跟踪和报告配置不当的团队 15

5.1.2云配置不当的原因 16

5.1.3检测到配置不当的流水线交付阶段 17

5.2因配置不当造成的破坏和事件 18

5.2.1设计用于管理云配置不当的安全性和合规性标准 18
5.2.2 防止或修复云配置不当的障碍 18
5.3治理与合规 19
5.3.1设计用于管理云配置不当的安全性和合规性标准 19
5.3.2跨团队和组织执行标准 19
5.3.3平衡安全性与项目交付 20
5.4解决配置不当的解决方案 20
5.4.1负责纠正配置不当的小组 20
5.4.2修复配置不当的流水线过程阶段 21
5.4.3修复配置不当的时间 21
5.4.4改进解决安全性或合规性配置不当的方法组织中最常见的方法 22
5.4.5使用自动修复的障碍 22
6.人口统计资料 23
6.1组织行业 23
6.2组织规模 23
6.3工作等级 23
6.4组织公有云支出 24
6.5公司部门主要工作 24

1.调研的开展和方法论

云安全联盟（CSA）是一个非营利组织，其使命是广泛推广最佳实践，确保云计算和IT技术中的网络安全。CSA还负责教育这些行业内的各种利益相关者(涉及所有其他形式计算中的安全问题)。CSA的成员是由从业者、公司和专业协会组成的广泛联盟。CSA的主要目标之一是开展调研评估信息安全趋势。这些调研有助于衡量信息安全技术在行业内各方面的成熟度，以及安全最佳实践的采用率。

VMware的CloudHealth®为了增加业界对公有云安全的了解，委托CSA开展一项调查并编写这份调查结果报告。CloudHealth为该项目提供资金，并与CSA一起参与制定针对云安全的调查问题，从而共同制定了该倡议。该调查由CSA于2021年5月至2021年6月在线进行，收到1090份来自不同组织规模和地点的IT和安全专业人士的答复。数据分析由CSA的研究团队进行。

1.1研究目的

本调研的目的是评估组织在降低配置不当导致的公有云安全和合规风险方面的准备度。主要研究课题包括：

- 云安全计划的现状，包括最主要风险和安全工具的使用情况。
- 组织在缓解配置不当导致的漏洞方面面临的云安全态势管理（CSPM）挑战。
- 组织准备情况、成功关键绩效指标（KPI）以及负责云安全态势管理不同方面的团队。

2.概要

云配置不当一直是使用公有云的企业最关心的问题。这种错误会导致数据泄露，允许删除或修改资源，导致服务中断，并对业务运营造成严重破坏。最近，由于配置不当导致的漏洞成为头条新闻，为了更好地了解云安全计划的现状、用于减轻安全风险的工具、企业的云安全态势以及企业在减少安全风险方面面临的障碍，我们进行了这项调研。

关键发现 1

知识和专业技能匮乏不断困扰着安全团队

知识和专业技能匮乏是信息安全行业内众所周知的问题。毫不奇怪，知识匮乏和专业技能被一致认定为:

- 通用云安全的主要障碍 (59%)
- 配置不当的主要原因 (62%)
- 主动预防或修复配置不当的障碍(59%)
- 实施自动补救的主要障碍(56%)

这些发现突出了“知识匮乏”对安全团队可能产生的涓滴效应。它首先是实施有效的云安全措施的一般障碍，导致了错误的配置，这是数据泄露的主要原因。但它也阻碍了安全团队实施解决方案，如自动修复，这些解决方案可以补充知识和技能的不足。

通用云安全的主要障碍

配置不当的主要原因

主动预防或修复配置不当的障碍

实施自动补救的主要障碍

关键发现 2

信息安全及IT运营团队对降低云配置不当风险承担责任

每年都有由于配置不当而导致的数据泄密事件，涉事公司也因此上了新闻头条；因此很多公司都把配置不当风险当成首要关注点。

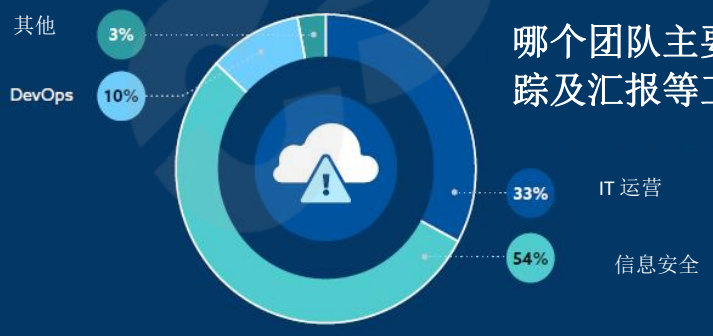
很多公司没有处理好配置不当风险的可能原因之一就是，对潜在配置不当问题的发现、监控、及追踪，IT运营及信息安全团队承担主要责任 (**信息安全54%, IT运营33%**) 同样两团队对问题的修复也需要承担主要责任 (**信息安全 36%, IT 运营 34%**), 公司没有将这些责任分担给其他团队，比如DevOps或应用工程团队，这些问题可能就是这些团队产生的，从而更加适合直接修复这些错误。

基于这个原因，公司就需要将问题修复的职责转移给DevOps及应用工程团队，这样可以更好的管理配置不当风险。

另外，很多公司表明由于配置不当而导致安全事件的主要原因是”缺乏可见性“(68%)，公司在选择工具的时候，下面三种功能同样重要:

- 提高可见性
- 有效的风险管理
- 自动化

这些功能将帮助企业快速识别及修复配置不当问题，不管是哪个团队对此负责。



哪个团队主要负责公司云配置不当问题的发现、追踪及汇报等工作？

哪个团队主要负责确保云配置不当问题被修复？

关键发现 3

DevSecOps 方式对安全部门仍然遥不可及

安全部门仍然在努力对齐安全方针及(或)方针落地

DevSecOps 及安全左移等话题在安全行业越来越热，虽然这些转型将会导致一个更牢固、更安全、更有弹性的应用，但很多组织在落地这些方针时还是很困难。他们甚至在跨部门之间对安全方针及方针落地达成共识方面都较吃力。只有三分之一的组织能成功实施这些转型。

部门之间缺乏共识将会导致文化差异，也就是不同的领导有不同的优先级，经常会发生的情况是，这些问题将会先从领导开始，然后蔓延到他的团队。部门之间缺乏共识的一个解释是对前面的关键问题点缺乏知识。如果部门对DevSecOps的战略及最佳实践都没有足够的知识，那将很难在关键问题上达成共识。

另外同样值得注意的是，尽管有近70%的组织在对安全方针及方针落地上对跨部门间达成共识存在困难，但只有39%的组织认为这是解决安全问题的最大障碍。所以这些部门可能遇到更多的根本问题，这些问题将会阻碍DevSecOps或安全左移模型的落地。

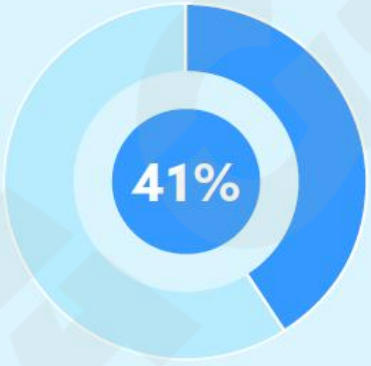
安全，IT 运营、及开发团队对安全方针和落地方针的关系

部门间在安全方针和执行方面的一致性对主动安全至关重要

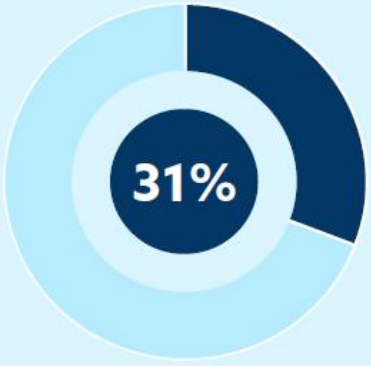
如果组织能够在部门之间获得关于安全方针和执行方针的一致性，并且正在转向DevSecOp方法，那么就能够更好地处理配置错误。这些组织更有可能在错误发生一天内检测到错误配置 (**完全一致 – 56%, 部分一致 – 41%, 没有一致 – 31%**)，也更有可能在检测到配置不当一天内纠正这个错误(**完全一致 – 51%, 部分一致 – 24%, 没有一致 – 19%**)。由于配置不当是导致据数据泄露的主要原因之一，检测和纠正这些错误的时间越短，企业总体上就越安全。很明显，这种对DevSecOps方法的协作和进步是组织解决配置不当的关键，而且也减少了数据泄露或其他重大安全事件的风险。

在一天内检测配置不当

与安全方针保持一致并且强制执行

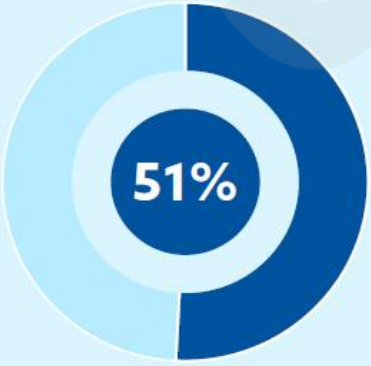


与安全方针保持一致但没有强制执行

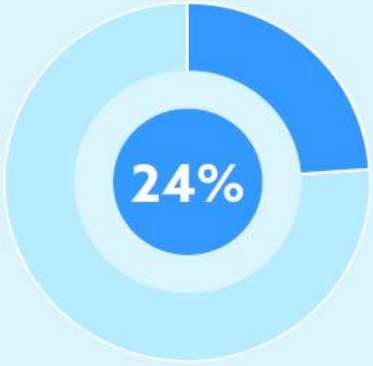


没有与安全方针保持一致而且没有强制执行

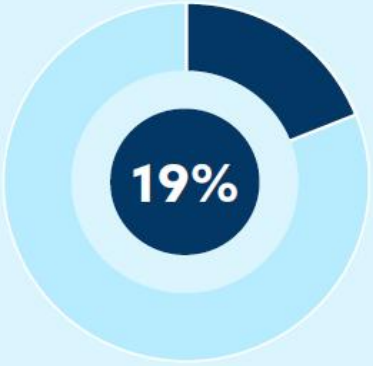
在一天内纠正配置不当



与安全方针保持一致并且强制执行



与安全方针保持一致但没有强制执行

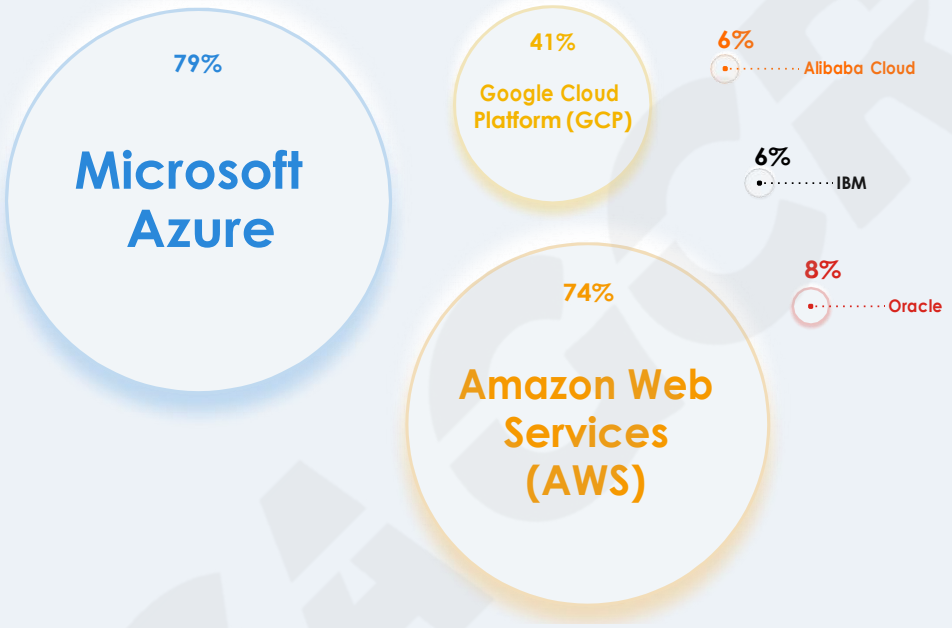


没有与安全方针保持一致而且也没有强制执行

3.云安全程序的当前状态

3.1使用公有云提供商

市场上还没有一个占主导地位的公共云平台，但是Amazon Web Services (AWS)、Microsoft Azure和谷歌云平台(GCP)仍然是主要的公共云提供商。在这项调研中，74%的受访者使用AWS，79%使用Azure，41%使用GCP.



3.2公有云的年度预算

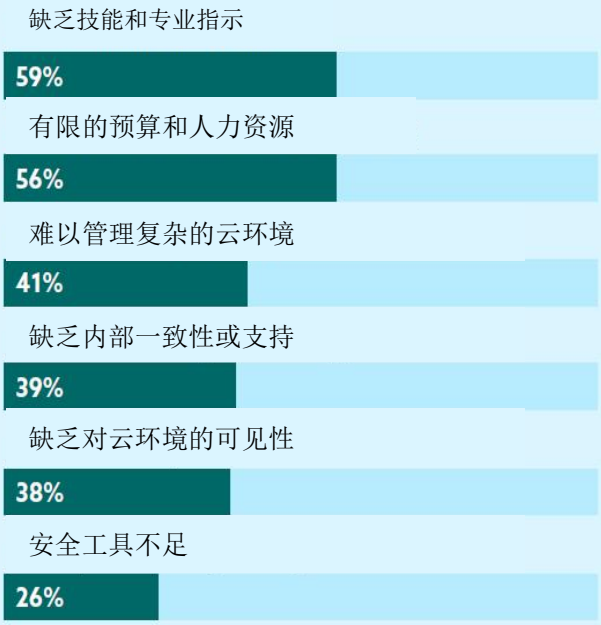
参与者之间云预算差异很大。然而，最常见的三个回答都在150万美元以下。“$0-$250,000”占22%，“$500,001-$1,500,000”占15%和“$250,001-$500,000”占13%。不确定的人也占显著比例(16%).

3.3对抗云安全漏洞的总体信心水平

为了评估受访者对其组织安全计划的信心，受访者被要求评估他们对组织防御及处置云安全漏洞的能力的总体信心水平。大多数受访者表示 **“一般有自信”(42%)** 或 **“非常有信心”(31%)**。

3.4对防御云漏洞威胁的能力充满信心

受访者对其组织在不同领域抵御威胁和漏洞的能力的信心水平，平均处于居中水准。不同类别选项之间的置信水平差异很小。 其中，信心水平最高的“合规与监管”和次高的“网络”，也仅是略高于“错误配置”选项。



3.5解决安全问题的障碍

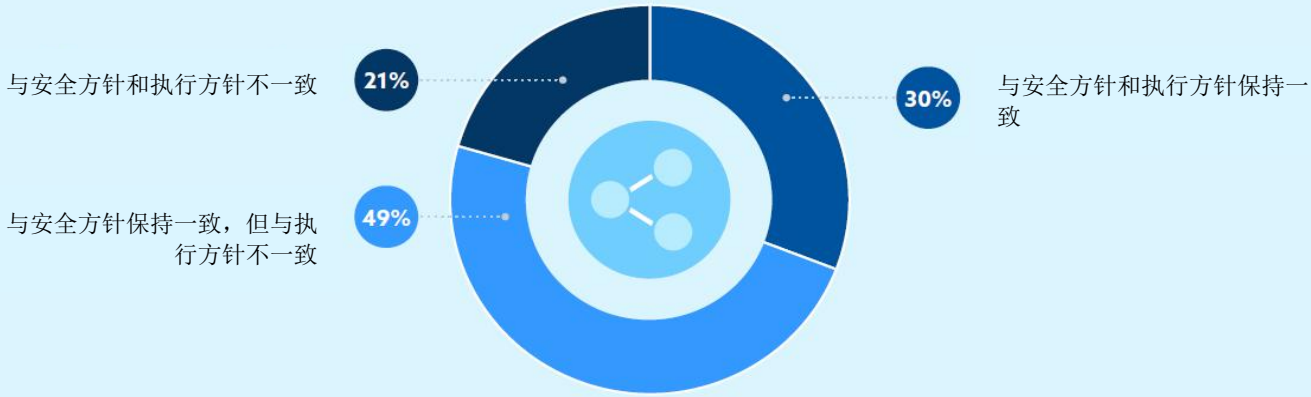
解决安全问题的主要障碍并不令人意外，**“缺乏技能和专业知识”(59%)和“预算和人力资源有限”(56%)。**这两个问题已经困扰了行业一段时间，并且与其他选项密切相关。 这表明预算、人员配备和专业知识的问题可能掩盖了其他关键问题，例如“缺乏可见性”和“安全工具不足”。

3.6安全方针制订与落地执行的跨部门协作

DevSecOps和“安全左移”已成为安全行业中的流行概念。 然而，对于许多组织来说，这些概念的落地执行仍很难把握。只有 31% 的人反映他们的内部团队能在安全方针制订和执行上保持一致。“内部缺乏支持的一致性“可能是由于不同部门间的文化差异，例如不同的目标优先级。 另一方面也可能是“缺乏相应的专业知识”，这也是上一个问题中提到的。

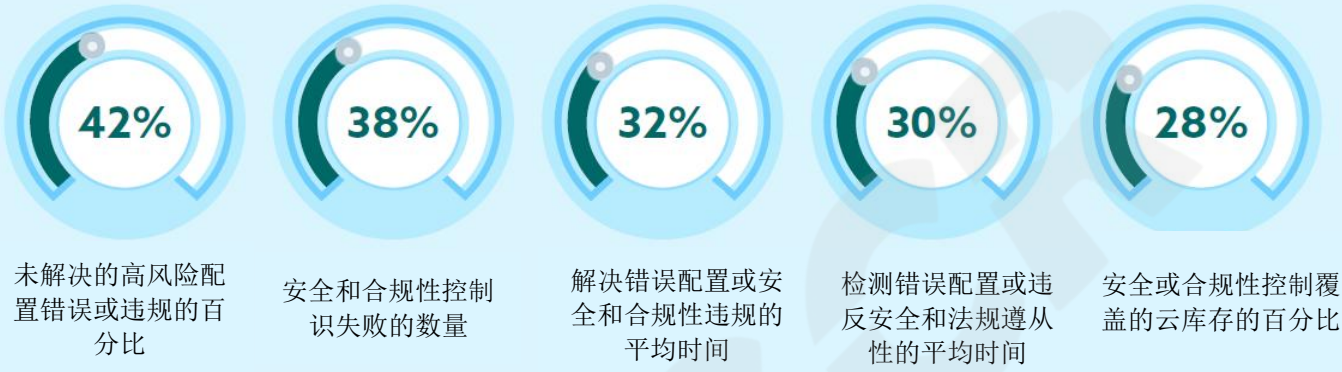
还值得注意的是，尽管大约 70% 的组织致力于“安全方针和执行方面获得跨部门的一致性”，但只有 39% 认为这是解决安全问题的主要障碍。

此外，在安全方针及落地执行上跨部门协作性更好的受访者更高概率反馈他们对自己抵御安全漏洞的能力“非常有信心”或“非常有信心”（非常有信心：完全一致 – 15%，部分对齐 - 2%，不对齐 - 1%；非常有信心：完全对齐 - 49%，部分对齐 - 27%，不对齐 - 16%）。 综上，我们可以得出结论，“内部一致性”是希望改善云安全状况的组织应关注的关键决定因素和基线要求。



3.7度量安全性和合规性状况

组织用来度量其安全性和合规性状况的指标视情况而异。受访者被要求选择他们组织使用的前三个指标。选择最多的回答是 “未解决的高风险错误配置或违规的百分比”(42%), “安全和合规性控制失败的数量” (38%), 和 “解决错误配置或安全和合规性违规的平均时间” (32%)。

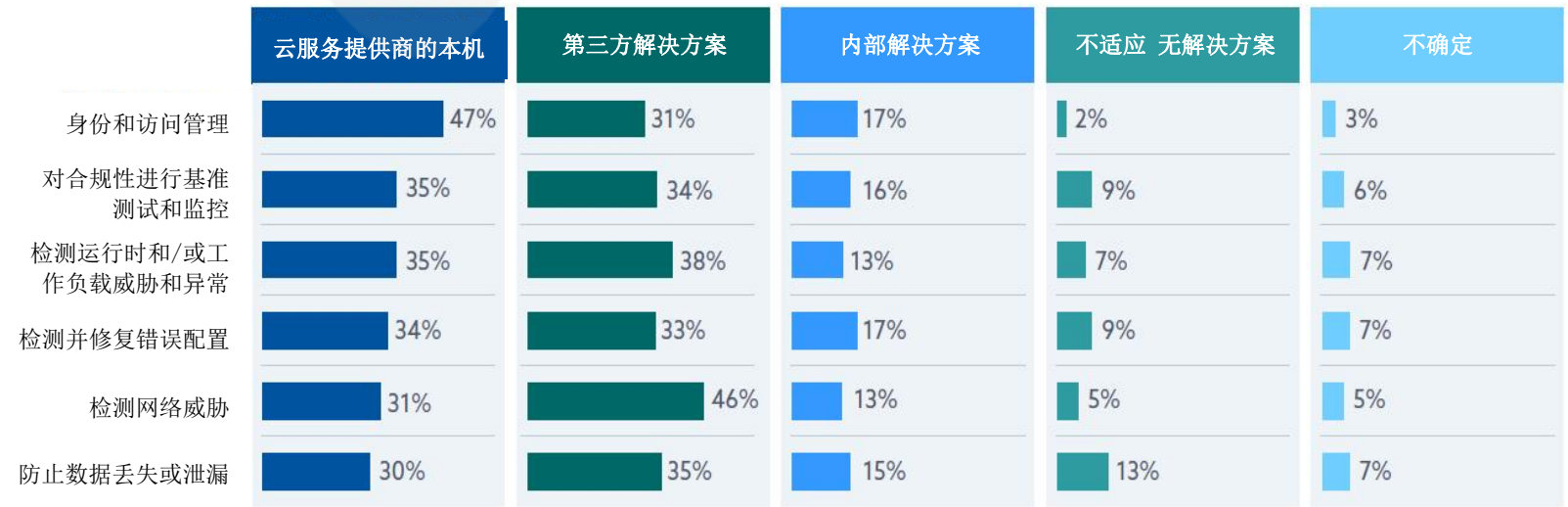


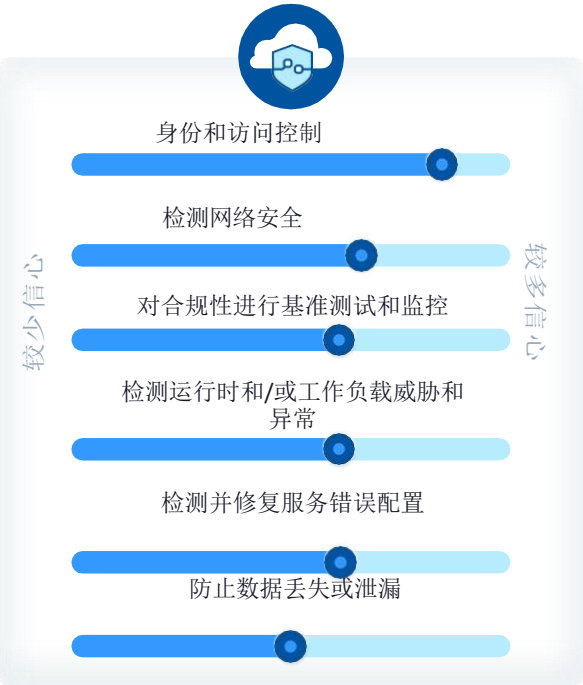
4.正在使用的云安全工具

4.1用于云安全的解决方案

通常，使用云服务提供商的本地工具和第三方解决方案的组织之间存在相对平均的比例。然而，有几个类别的云安全有明显的赢家。云服务提供商的解决方案是原生工具，用于 “身份和访问管理” (47%), 而第三方解决方案用于 “检测网络威胁” (46%) 和“防止数据泄漏” (35%)。

需要注意的一个特别令人担忧的模式是，未使用数据防防丢失的组织所占比例(13%)远远高于其他任何类别。这将可能反映出这些类型的解决方案实施的难度。





4.2对云服务提供商安全解决方案的满意度

平均而言，受访者对他们的主要公有云服务提供商的安全解决方案感到**“适度满意”**在不同类别之间差异很小。平均满意度最高的领域，如“身份和访问管理”，仅略高于评分最低的“防止数据丢失或泄露”。

4.3使用托管服务提供商

大多数组织没有使用托管服务提供商**(MSP, 59%)** 管理公有云环境下的安全性和合规性。但只有31%的人在使用MSP。还需要注意的是，拥有1-50名员工的小型企业(72%)比拥有50名或更多员工的组织(57%)更有可能不使用MSP。

5.云安全状态管理

5.1识别配置不当

5.1.1负责检测、跟踪和报告配置不当的团队

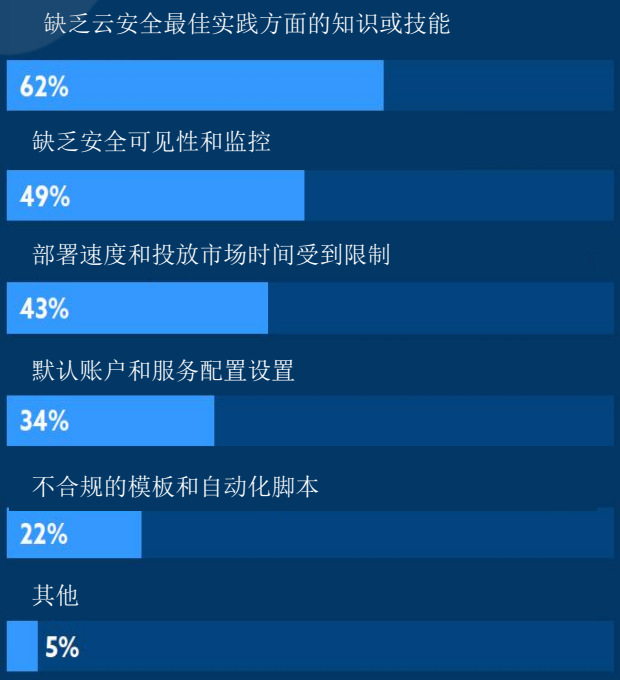
负责检测、跟踪和报告云配置不当的主要团队通常是**信息安全团队 (54%)**。 IT 运营是排在第二位的部门 **(33%)**。

有趣的是，配置不当的来源通常是DevOps团队，因此更有可能意识到已发生配置错误的人员不会被标识为负责检测、跟踪或报告云配置错误的团队。这突出了为了提高部门间的一致性和可见性，转向DevSecOps方法，从而最终更快地检测和纠正错误配置的重要性。

同样重要的是，确保组织拥有正确的工具，使整个组织中的所有这些部门都能发挥作用。特别是能够实现有效风险治理的工具，使组织能够更好地识别和管理风险及合规性。自动化也是快速识别和纠正错误配置的关键。这将要求组织将其架构转向云端。

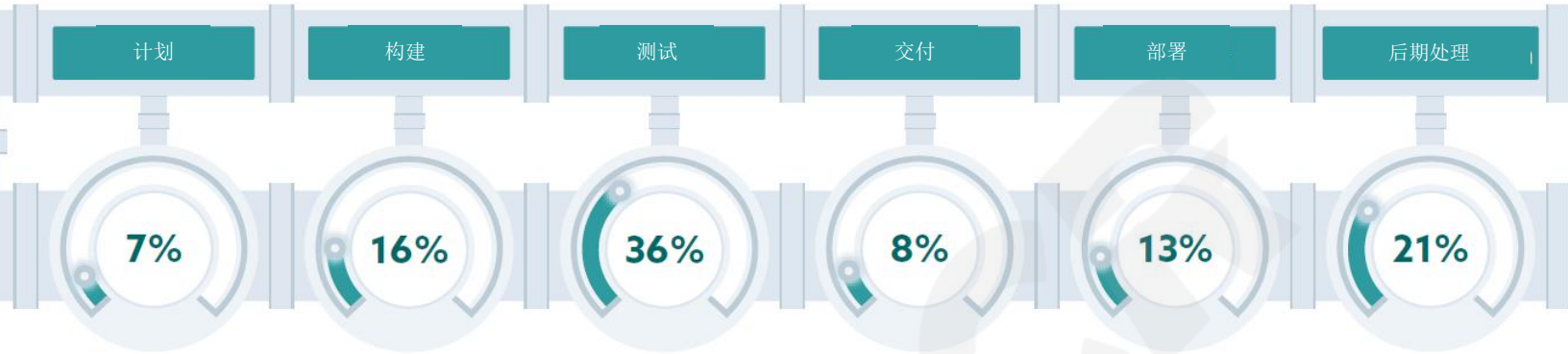
5.1.2云配置不当的原因

组织中配置不当的主要原因是**“缺乏云安全最佳实践方面的知识或技能”(62%)**。这并不令人惊讶，因为早些时候这被认为是一个主要的安全障碍。更令人惊讶的是，第二个选择最多的回答是**“缺乏安全可见性和监控”(49%)**，因为在之前的调查中，可见性没有被认为是解决安全问题的主要障碍。这可能表明组织没有优先解决可见性方面的挑战，因此，可见性是配置不当的主要原因。



5.1.3检测到配置不当的流水线交付阶段

在流水线流程中检测到云配置不当的最常见阶段是**“测试”阶段 (36%)** 和**“后期处理”阶段 (21%)**。这意味着大多数配置不当都是在部署之前检测到的 (67%)，至少在某些方面表明组织已经能够“左移”。



5.1.4检测配置不当的时长

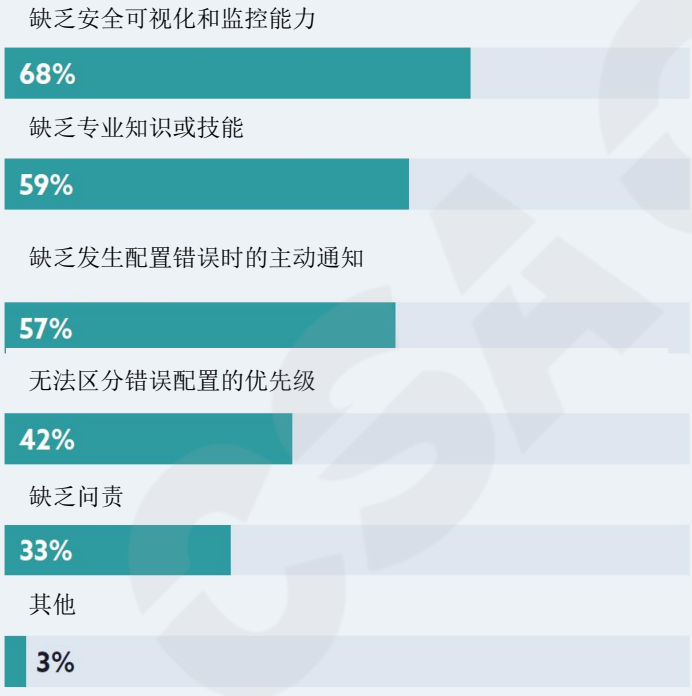
组织检测云配置不当所需的时间长短差别很大。最常见的情况是会在**一天内 (23%)** 或者**一周内 (22%)**。找到问题。然而，更令人担忧的是，22%的组织甚至需要超过一周的时间才能找到配置不当，更不用说解决配置不当了。

还需要注意的是，报告部门间协调方针及其执行情况的组织更有可能在错误发生后的一天内检测到配置不当(完全协调-56%，部分协调-41%，无协调-31%)。

5.2因配置不当造成的破坏和事件

5.2.1设计用于管理云配置不当的安全性和合规性标准

大多数组织报告称，他们在过去的一年中没有经历过**公有云安全事件或漏洞问题 (65%)**。大约**17%的人表示他们经历过这样的事件**，剩下**18%的受访者表示不确定是否经历了相关问题**。鉴于调查受访者的工作角色直接涉及其组织的云安全态势，出现如此高比例的受访者不确定是否发生了安全事件或漏洞问题，令人不禁有些担忧。



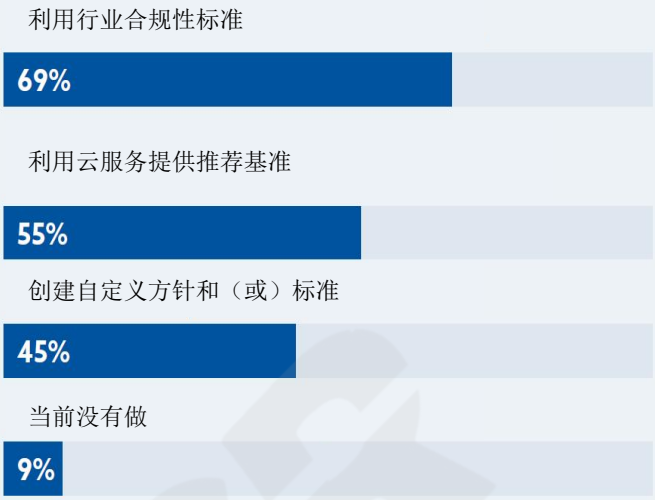
5.2.2 防止或修复云配置不当的障碍

在经历过发生云安全事件或漏洞的17%的组织中，主动预防或解决问题的最常见障碍是**“缺乏安全可见性和监控能力”（68%）**，其次是**“缺乏知识或专业技能”（59%）**。再一次说明，知识和可视化是主要障碍。

5.3治理与合规

5.3.1设计用于管理云配置不当的安全性和合规性标准

组织主要利用**“行业合规性标准”（69%）**、**“云服务提供商推荐基准”（55%）**）和**“自定义方针和（或）标准”（45%）**。 只有**9%**的组织报告说他们目前没有设计安全合规性标准。



5.3.2跨团队和组织执行标准

安全性和合规性标准的执行水平因组织而异。 报告**“在所有环境中完全实施”(23%)**、**“仅在关键环境中完全实施”(26%)** 和**“在所有环境中实施部分标准”(24%)**的组织数量大致相等。 其中一点特别有趣，因为 70% 的公司报告称，他们的安全方针及（或）其执行方面难以实现部门间协调。

还应注意的是，与“方针一致但执行不一致的组织”17%）和“两者都不一致的组织”（7%）相比，在跨部门的方针及其执行方面具有一致性的组织，更有可能报告“在所有环境中完全执行”（占44%）。

5.3.3平衡安全性与项目交付

接受调研的组织倾向于优先考虑风险缓解，即使这会导致**产品交付速度有所延迟(41%)**。 另有 **29% 的组织优先考虑交付速度，接受风险缓解方面有所延迟**。 为确保这些回答不会因为由于大量信息安全专业人员回应而使调研的数据结论有所偏差，我们特意忽略部分回答，并对数据进行了对比分析，暂未发现明显差异。

另一个值得注意的发现点是，按方针与执行一致性来看，执行上保持一致的组织更有可能报告说“优先考虑缓解风险胜于交付速度”，其占比35%。而那些方针与具体执行不一致的组织约占12%。

5.4解决配置不当的解决方案

5.4.1负责纠正配置不当的小组

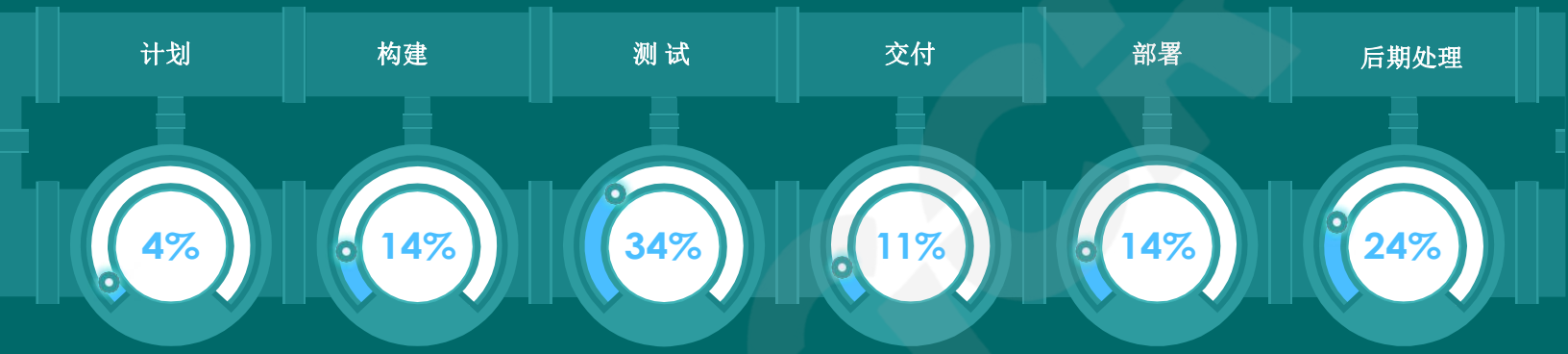
早些时候，我们发现负责检测、跟踪和报告云配置不当的主要群体是信息安全人员(54%)，其次是 IT 运营人员 (33%)。 在解决配置不当方面，信息安全和 IT 运营仍然是两个主要的负责群体。 两者的责任分工似乎也极为接近，其中，有**36%的组织错误信息上报是由信息安全人员**主要负责，而由 **IT 运营人员主责承担的组织占比 34%**。

有趣的是，导致此类错误产生，或更能直接修复这些错误的DevOps或应用程序研发工程师团队并不需要承担修复的责任，而往往是由 IT 运营和信息安全人员负责修复这些错误。这结论再次显示了这些部门之间保持一致的重要性。 如果组织能够通过引入 DevSecOps 的工作方法，使各参与者都可以更清楚地了解其他部门的活动，通过协同工作以便于更快地解决出现的配置不当或其他问题。

5.4.2修复配置不当的流水线过程阶段

在流水线过程中，对云计算配置修复最常见的阶段是**“测试”阶段（34%）**和**“发布后”阶段（24%）**。这意味着大多数配置不当能够在部署之前得到纠正(63%)，这再次表明组织至少在某些方面已经能够实现“安全左移”。

这些发现几乎与前文提到的流水线过程中检测到云配置不当的阶段相同（测试，36%；发布后，21%，部署前修复，67%）。

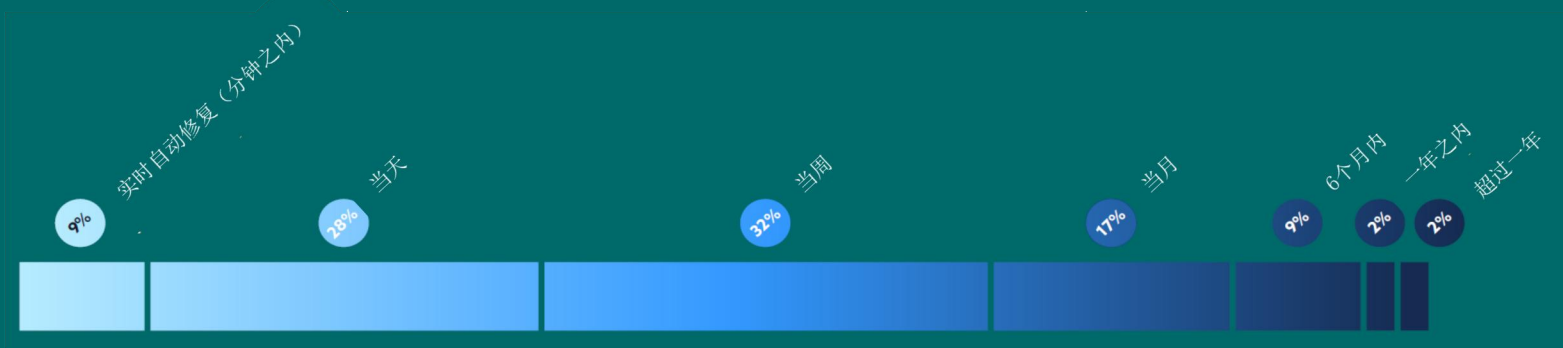


5.4.3修复配置不当的时间

大多数组织都能在一周内修复这些云配置不当，总数占比约60%。其中，**32%的组织能够在一周内完成修复，28%的组织能够在当天完成修复**。同时，也有30% 的组织需要超过一周的时间修复这些错误的配置。

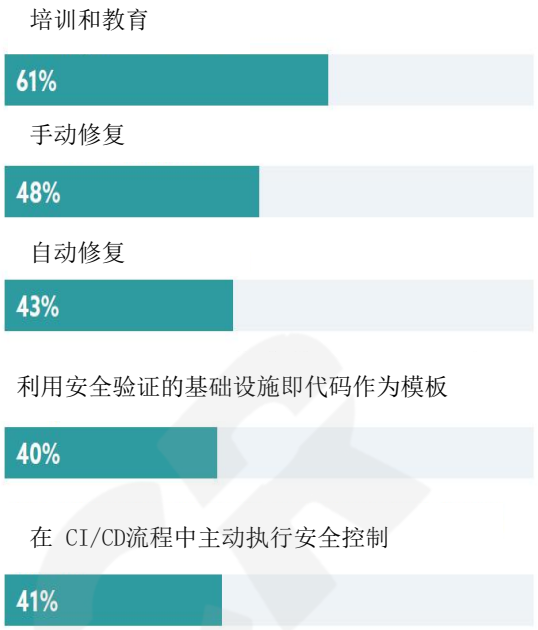
关于检测到配置不当的时间长度的问题发现，78% 的组织能够在一周内检测到错误。在修复配置不当的用时与检测到配置不当的用时方面有类似的趋势，69%的错误能够在一周内修复。

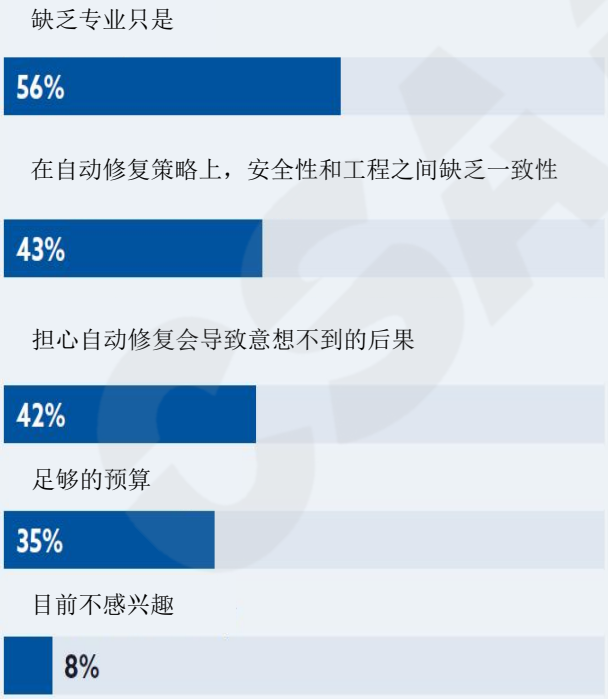
另一个值得注意的发现是，方针制订和执行的部门一致的组织，则更有可能在检测到配置不当的一天内纠正该错误（完全一致的占51%，部分一致的占24%，不一致的占19%）。



5.4.4改进解决安全性或合规性配置不当的方法组织中最常见的方法

用于改进云环境中安全性和（或）合规性配置不当的解决方法是“培训和教育”。这并不奇怪，因为缺乏知识已多次被指出是安全的一个关键障碍。第二和第三个最常见的回答是**“手动修复”(48%)**和**“自动修复”(43%)**。尽管自动化是最常用的三种方法，但很明显，许多组织还没有完全实现自动修复，因为当被问及他们的组织需要多长时间修复上一个问题中的配置不当时并不是一个普遍选择的回答。





5.4.5使用自动修复的障碍

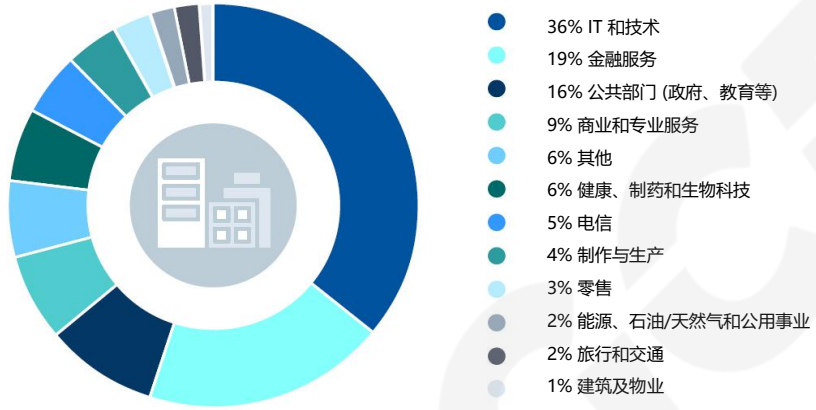
对于那些不使用自动修复的人来说，不使用该解决方案的最常见原因还是**缺乏专业知识(56%)**。第二大常见原因是**部门之间在自动补救策略上缺乏一致性(43%)**。这一点也不奇怪，因为70%的组织正在努力在安全方针或方针执行方面获得部门间的一致。

与之接近的第三个原因是，人们担心**自动修复可能会导致意想不到的后果(42%)**。这可能与缺乏专业知识和知识的问题有关。如果团队不知道如何正确地利用这项技术，就很有可能会遇到意想不到的后果。

6.人口统计资料

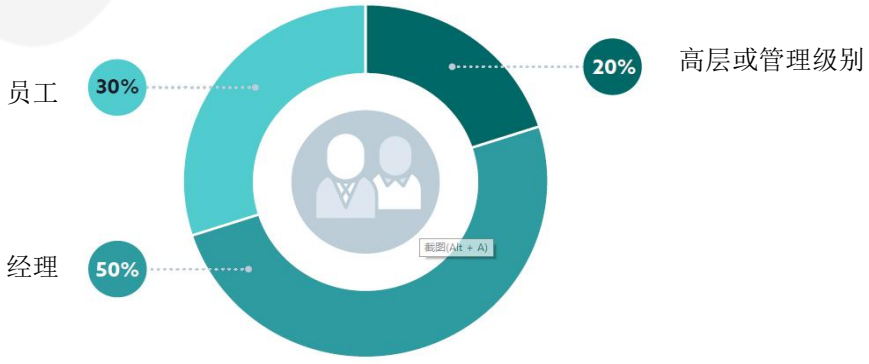
这项调研于2021年5月至6月进行，收集了1090份来自不同组织规模、行业、地点和角色的IT和安全专业人员的回复。

6.1组织行业



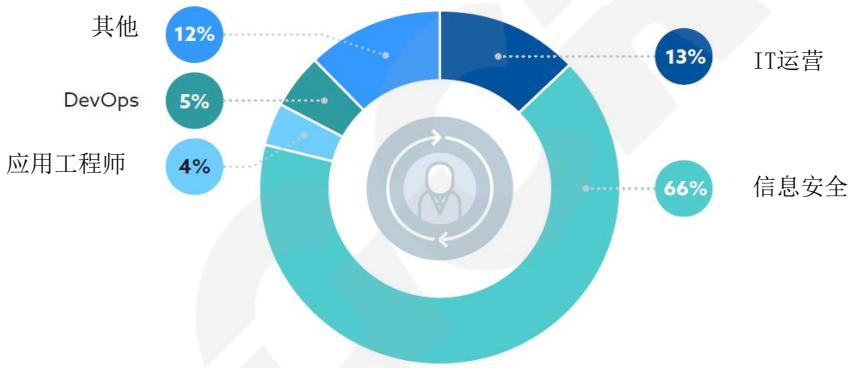
6.2组织规模

6.3工作等级

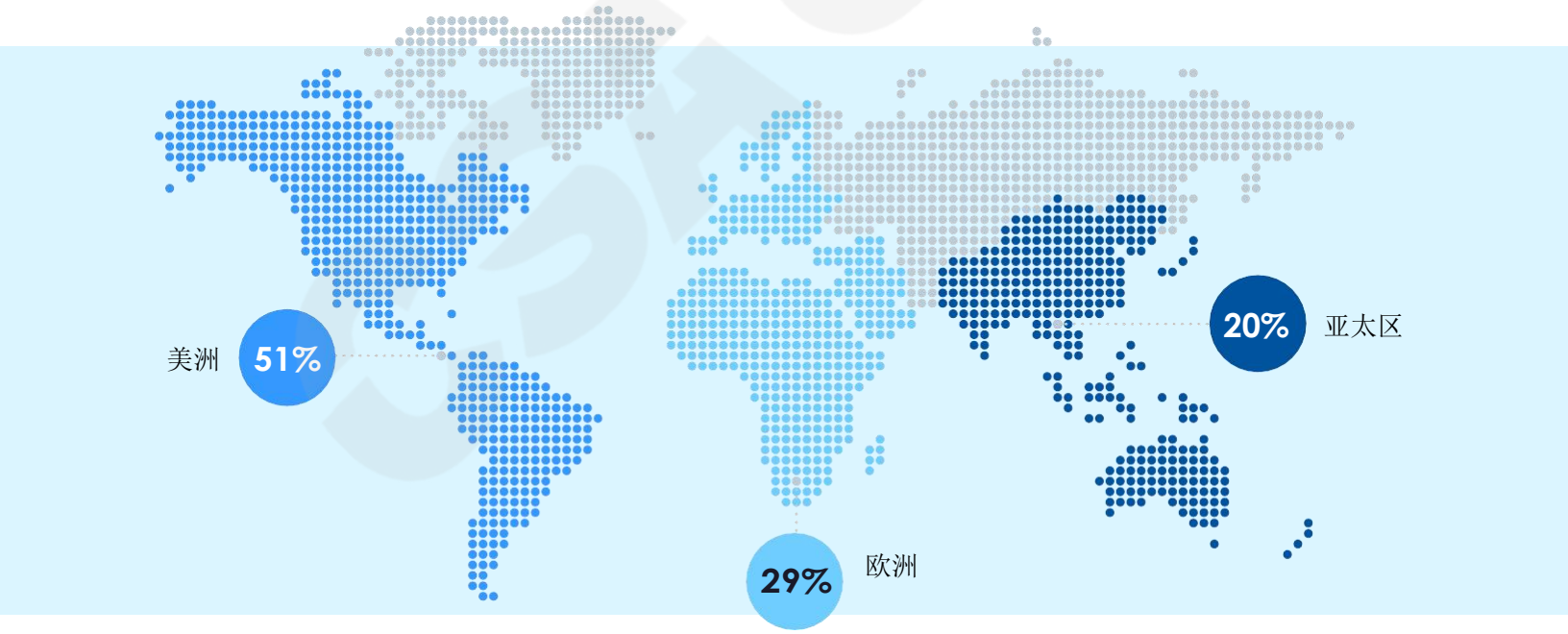


6.4组织公有云支出

6.5公司部门主要工作



6.6区域



贡献最多的国家和地区包括：美利坚合众国、印度、大不列颠及北爱尔兰联合王国、加拿大、澳大利亚、新加坡、德国、瑞士、法国

关于赞助商

VMware 是企业软件领域的领先创新者。我们为世界数字基础设施提有力的支撑。

我们的云计算、应用程序、网络、安全和数字工作区平台构成了一个弹性的，一致的数字基础。

该基金会授权企业建立、运行、管理、连接，并在任何地方保护应用程序—实现技术驱动的转型而不中断。

VMware 于2018年10月收购了 CloudHealth Technologies, Inc.

CloudHealth by vmware®

赞助商是CSA 的成员单位，但该成员仅支持项目研究，不具备影响CSA研究内容的开发权和编辑权。