云安全现状、挑战和安全事件

algosec

CSA GCR cloud security alliance® GREATER CHINA REGION

CSA cloud security alliance®

致谢

《云安全现状、挑战和安全事件》 (State of Cloud Security Concerns, Challenges, and Incidents)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：魏小强

翻译组：李吉祥　秦益飞　吴潇　于继万

研究协调员：赵晨曦

感谢以下单位对本文档的支持与贡献：

北京奇虎科技有限公司　北京天融信网络安全技术有限公司

海尔集团公司　华为技术有限公司

江苏易安联网络技术有限公司

英文版本编写专家

主要作者：Hillary Baron　Sean Heide　Shamun Mahmud　John Yeoh

设计者：Stephen Lumpe　AnnMarie Ulskey

特别感谢：Yitzy Tannenbaum　Product Marketing Manager　AlgoSec

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

调查创建和方法

云安全联盟（CSA）是一个非营利组织，其使命是广泛推广云计算和 IT 技术中网络安全的最佳实践。CSA 还负责指导行业中的各个利益相关者，了解所有其他计算形式的中的安全性问题。CSA 是行业从业者，公司，专业协会的广泛联盟。CSA 的主要目标之一是进行评估信息安全趋势的调查。这些调查有助于评估信息安全技术在行业中各个方面的成熟度以及安全最佳实践的采用率。

领先的网络安全解决方案提供商 AIgoSec 委托 CSA 进行此项调查，以增加业界对混合云和多云安全性的了解，并输出调查报告结果。AIgoSec 资助该项计划目，并与 CSA 一起参与解决混合云安全性问题的调查。这项调查由 CSA 在 2020 年 12 月至 2021 年 1 月之间在线进行，并已提交给来自不同组织规模和地点的近 1900 名 IT 和安全专业人员。数据分析是由 CSA 的研究小组完成。

研究目的

- 了解当前和未来的云使用情况
- 确立当前阶段上云和云部署过程中的安全问题
- 确定组织用于解决安全问题的安全工具
- 了解与云相关的安全事件的发生和原因

执行摘要

在过去的十年中，云服务的使用持续增长。尤其是在发生 COVID-19 公共卫生危机之后，许多企业的数字化转型正在加速，以便让员工能够在家中工作。CSA 制定并分发了一项调查，以更好地了解当前的云安全的问题、挑战和事件。

关键发现 1

组织正继续向复杂的云环境迁移

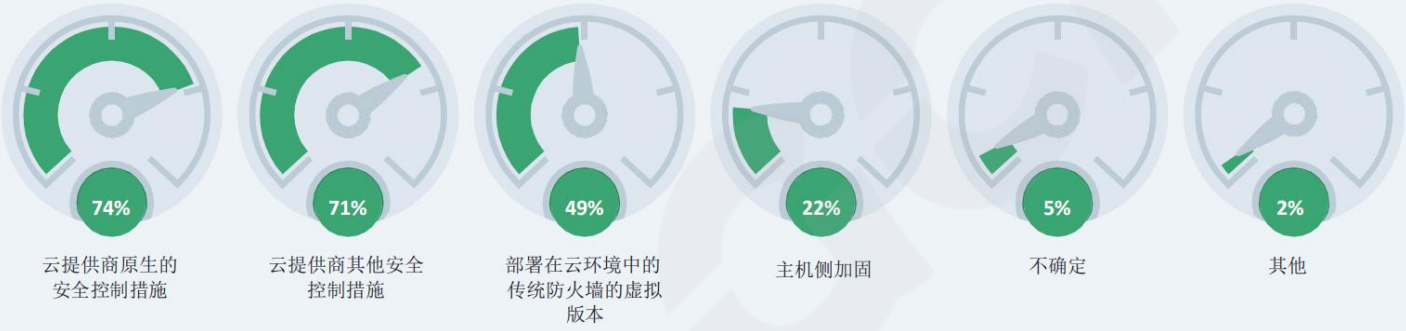
超过一半的企业在公共云中运行 41%或以上的工作负载，是自 2019 年以来的显著增长。2019 年发现只有 25%的企业在公共云中运行 41%或更多的工作负载。2021 年，63%的受访者预计将在公共云中运行 41%或更多的工作负载，这表明这种公共云的发展趋势会持续进行。毫无疑问，由于最近的健康危机，远程工作者的增加将进一步起到推动作用。

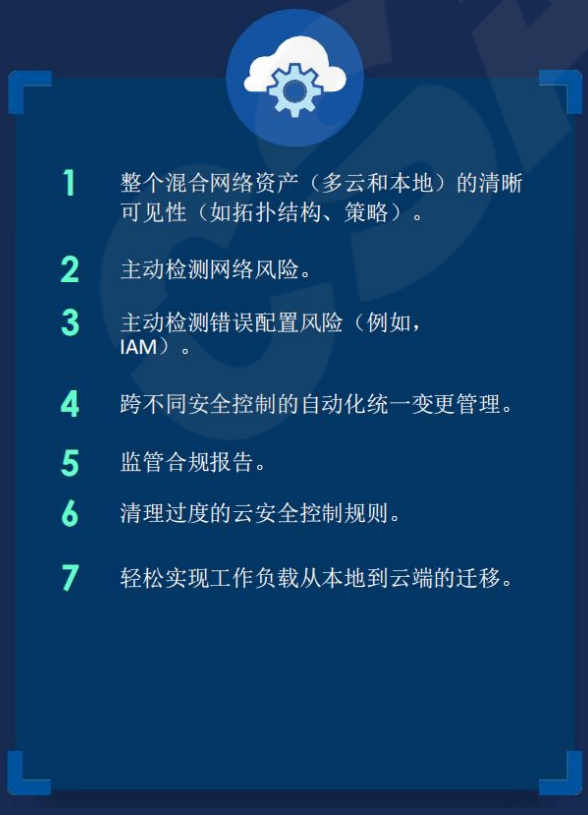
CSA 在 2020 年进行的另一项调查也表明，生产工作负载的多样性（如容器平台、虚拟机）也将增加。结合这一点与本次调查中发现的持续使用多云（62%）和不断增长的远程劳动力相结合，一个越来越复杂的云环境将继续出现。为改善组织的公共云安全，这种复杂的环境将不可避免地导致对补充安全工具的需求。

关键发现 2

对许多企业来说，云供应商的本地安全控制是不够的

企业越来越多地转向云供应商的额外安全控制和虚拟防火墙。使用云供应商的额外安全控制措施的比例从 2019 年的 58%跃升至 2021 年的 71%。约有一半的组织转向第三方供应商的虚拟版本的防火墙进行网络安全控制。这可能表明，虽然许多组织正在向公共云迁移，但许多企业仍在使用传统和混合 IT 环境，这就需要在许多不同的环境中进行统一控制。此外，由于目前的健康危机和远程劳动力的急剧增加，许多组织无法像以前那样保护他们的网络安全，因此必须求助于额外的和替代性的安全控制措施。





关键发现 3

企业正在寻找补充其劳动力的安全工具

复杂的环境，加上安全人员不足和缺乏云知识，促使组织转向可以帮助补充其员工队伍的安全工具。组织寻找的安全管理工具中前四大好处中的三个是用于主动检测风险和自动化的工具。这些类型的工具既可以解决许多组织缺乏专业知识（47%）和员工（32%）所面临的挑战，也可以提高他们朝着不断变化的云环境迈进时的可见性。

使用公有云

组织机构正在使用的公有云平台

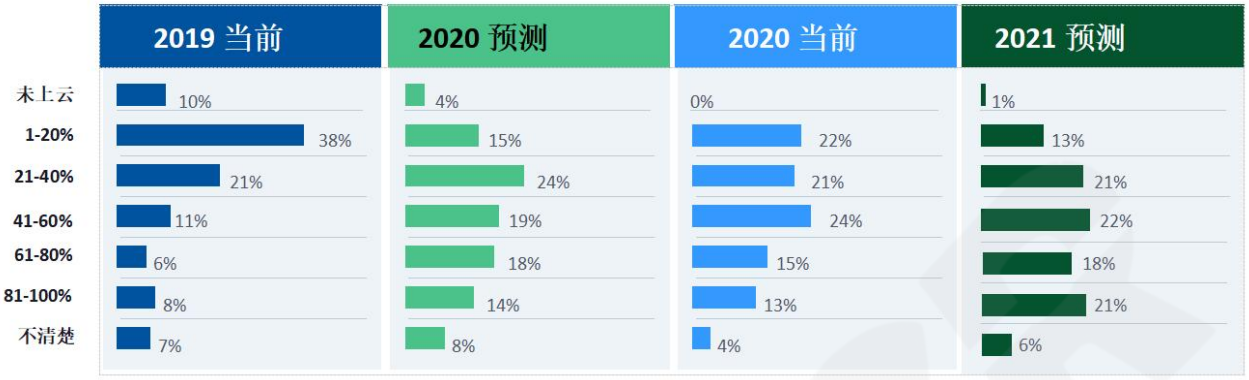
没有一个公有云市场的主导平台。市场顶级供应商之间的份额变得更均匀地分布。被调查的组织中有 67%使用 AWS，而 Azure 以 65%紧随其后。大多数组织也利用多云策略（62%）。没有一个公有云市场的主导平台。市场顶级供应商之间的份额变得更均匀地分布。被调查的组织中有 67%使用 AWS，而 Azure 以 65%紧随其后。大多数组织也利用多云策略（62%），其中有 27%的人使用了三个或更多公有云平台。

公有云可以满足期望

通常而言，组织迁移到公有云源于提供商的承诺和期望，包括：降低成本、增加敏捷性、弹性、DevOps 友好、正常运行时间提高。一般，组织发现公有云会满足甚至稍微超越这些期望。

过去，现在和未来的云工作负载

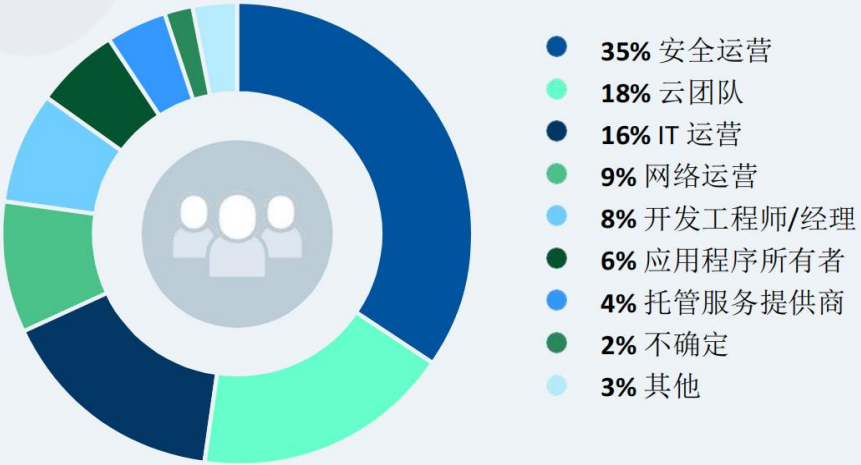
组织被要求根据当前云端工作负载的百分比预测他们在 2021 年底的运行情况。



在我们之前的调查中，我们对他们 2019 年的工作负载提出了类似的问题，并预测了他们在 2020 年底的云工作负载百分比。我们在上图中包括了所有四个估算值。与 2019 年实际云工作负载相比，2020 年实际云工作负载分别在 41-60%、61-80%、81-100%范围内显著增加。1-20%的范围出现了相应的下降，虽然不像之前报告中预测的那样显著。另一方面，云工作负载处于 21%至 40%范围内的组织百分比保持相对不变，维持在 21%的比例，这表明云工作负载要超过 40%的比例还需要更多的时间。也许是由于关注更多样化的工作负载，而不是重新托管方式，这在 CSA 之前的调查中已经提过。

负责管理公有云安全的团队

受访者报告说，有各种各样的团队负责管理公有云安全。安全运营(35%)，其次是云团队（18%）和 IT 运营（16%）。其他所有团队，包括网络运营、DevOps 工程师/经理、应用程序所有者和托管服务提供商，均下降到 10%以下。在这点上，各个组织之间并没有那么多的一致性，关于哪个团队对公有云安全负责也或许存在疑惑。



云安全关注点

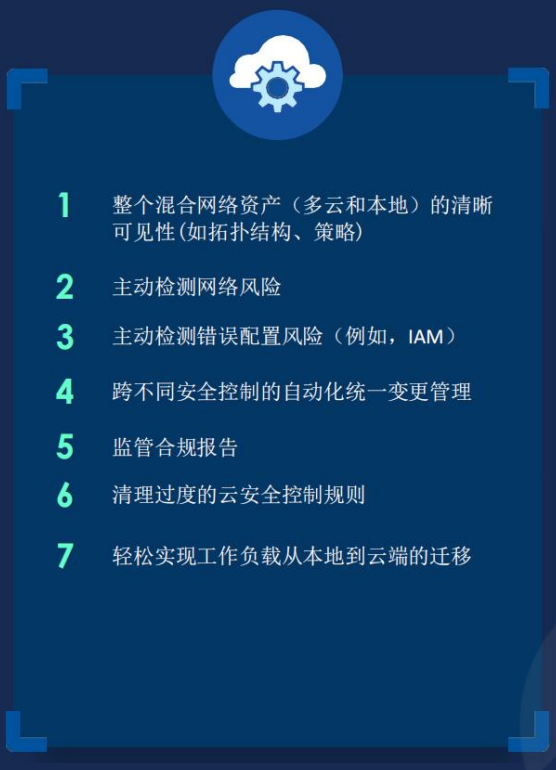
上云时的担忧

受访者被要求选择他们的组织在采用公有云时遇到的麻烦。最常选择的回复是“网络安全”（58％）。其次是“工作人员缺乏云专业知识”（47％），“工作负载迁移到云”（44％）和“管理云环境的人员数量不足”（32％）。值得注意的是，第二个、第四个最常见的选择都与人员问题有关，79％的比例超过了最频繁选择的响应“网络安全”。在 CSA2019 年发布的另一个调查中，类似的问题也被问到。对比二者存在明显的变化，因为前四个中的三个（工作人员缺乏云专业知识，将工作负载迁移到云中，以及员工数量不足以管理云环境）以前在后四位。这种巨大的转变可以归因于应对当前的疫情危机。许多组织可能正在努力解决大部分远程劳动力问题。

解决云安全中技能差距

组织解决技能差距前三种方式是“行业员工培训和认证”（55％），“非正式或员工自我培训”（54％），和“来自供应商的客户培训产品”（53％）。较少选择，27％的人员是外包人员。最少选择的选项是“未解决占 7％。

公有云中运行应用程序时的关注点



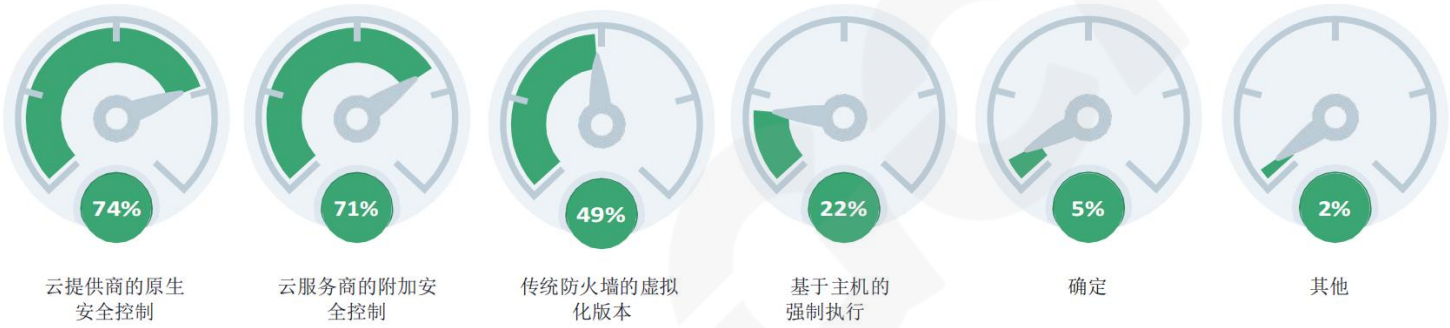
受访者也被问到应用程序在公有云中运行时的担忧

平均而言，排名最高的安全问题是“敏感数据泄漏”，这与上一次 2019 年的调查一致。“停机”、“配置和安全设置”、“未经授权的内部访问”、“合规性”符合法规要求”和“勒索软件”获得了中等关注度的平均排名。尽管“供应商技术漏洞”获得的最低排名，但也获得了略低于平均的关注度。SolarWinds 发生黑客入侵的报道公布时，这项调查正在进行，实际结果有些令人惊讶。不过，即使这个问题更加突出，它仍然是排名最低的问题。

工具

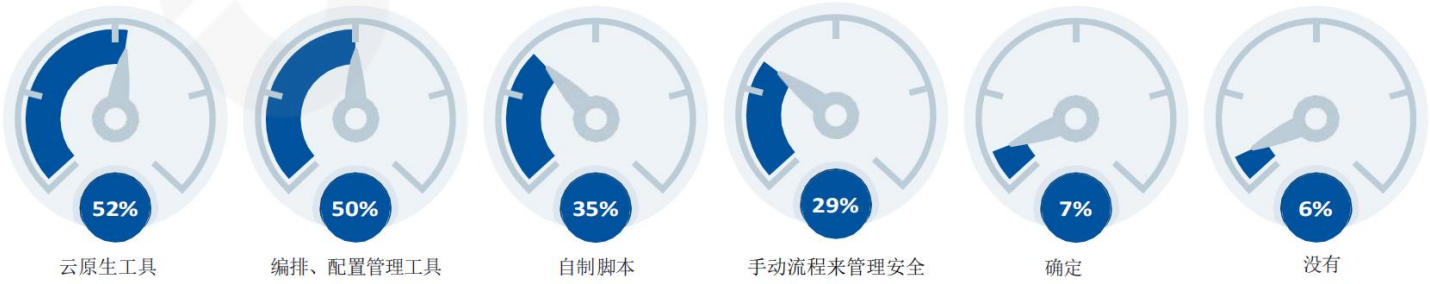
网络安全控制措施

为了更好地了解组织如何推进其公有云的部署安全性，受访者被问到他们使用的网络安全控制措施。许多受访者表示使用了多种控件。最常用的选项是“云提供商的原生安全控制措施”（74%），与 CSA 之前的调查一致。紧随其后的是“云服务商的附加安全控制措施”（占 71%），与之前报告的 58%显著上升。但是，将近 50%的受访者发现了仅这些工具还不够，需要求助于第三方的“传统防火墙的虚拟化版本”。



应用编排工具

安全管理可以采取多种安全应用编排形式。受访者被问及他们当前在应用中用于管理安全性的工具编排流程。超过一半的受访者表示使用了云原生工具(52%)和编排、配置管理工具(50%)。约有三分之一的受访者表示使用自制脚本(35%)和手动流程管理安全(29%)。



1. 轻松实现工作负载从本地到云迁移
2. 清理过度的云安全控制规则
3. 监管合规报告
4. 跨不同安全控制措施的自动化统一变更管理
5. 主动检测配置错误风险（例如，IAM）
6. 主动检测网络风险
7. 整个混合网络资产（多云和本地）清晰可见（拓扑，策略）

从云安全管理工具获得收益

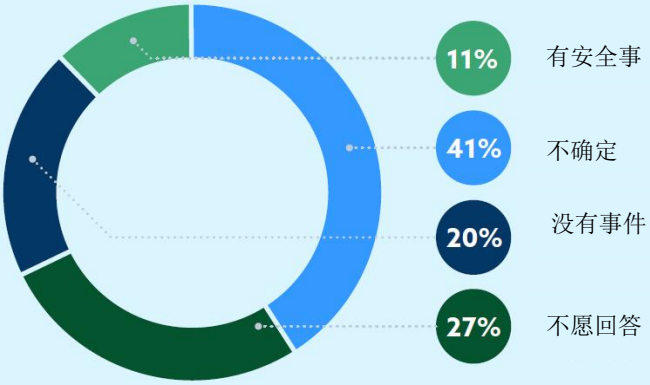
当被问及他们从安全管理工具寻求的好处时，排名最高回复是可见性。这是云环境特别是随着混合和多云环境的普及情况下，很常见的投诉。紧接在关注可见性之后的是主动检测网络风险和主动检测错误配置的能力。受访者分别将跨不同安全控制措施的统一变更管理自动化和合规性排到第四和第五。组织正在寻找工具主要用于解决他们当前面临的人员和云专业知识缺乏的挑战。

云安全事故与中断

云运营的有关事故

许多组织尝试为安全事件(如破坏或中断)做好准备。当被问及组织中过去的一年中是否发生过云运营相关的事件时，11%的受访者明确表示发生过安全事件，20%的受访者表示没有发生任何事件，27%的受访者表示不愿回答。

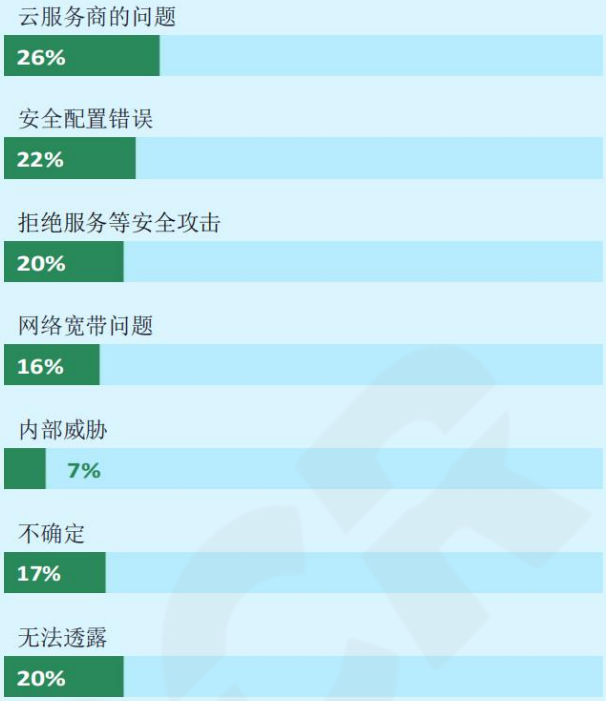
然而有 41%的受访者表示不确定，这与 2019 年的调查相比是一个重大的变化，在 2019 年的调查中只有 18%的受访者表示不知道是否发生了事故。同样有趣的是，表示发生过事故的受访者比例(11%)与 2019 年的调查保持一致。



受访者还被要求报告他们经历过的事故数量，平均回答为 5 次。考虑到大型云平台在一周内会发生许多事件，虽然许多事件可能不足以对用户造成重大影响，但 5 次这仍然是一个较低的数量。

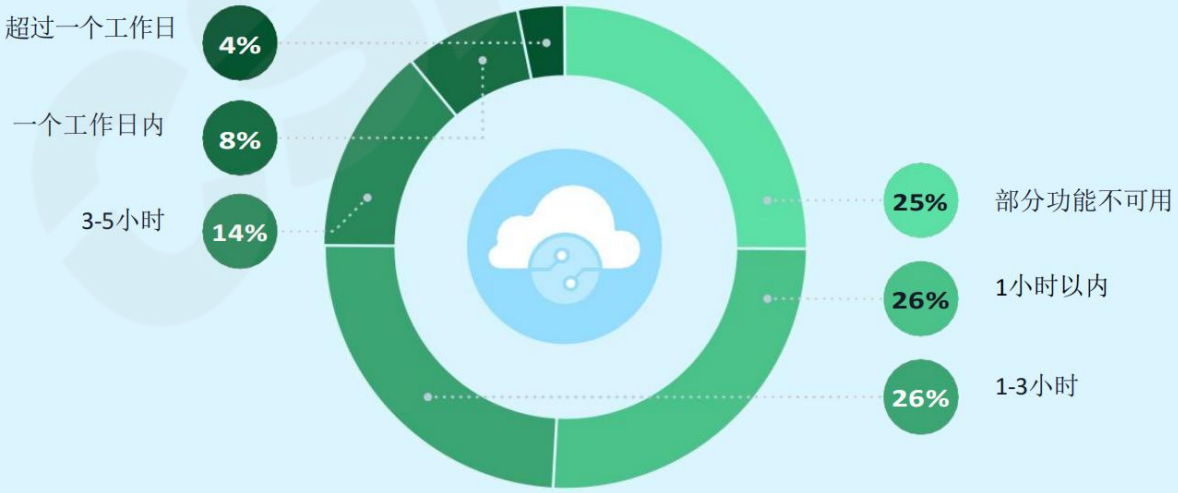
中断原因

在关于事件数量的问题之后，受访者被问及造成这些事件的主要原因。排在首位的反馈原因是云服务商的问题(26%)，其次是安全配置错误(22%)，以及拒绝服务等安全攻击(20%)。还有少部分反馈是网络带宽问题(16%)和内部威胁(7%)。排在前几位的原因可以归纳为人为失误或配置错误，这很有可能是组织缺少人员配备或专业技能造成的，也是组织亟需解决的问题。



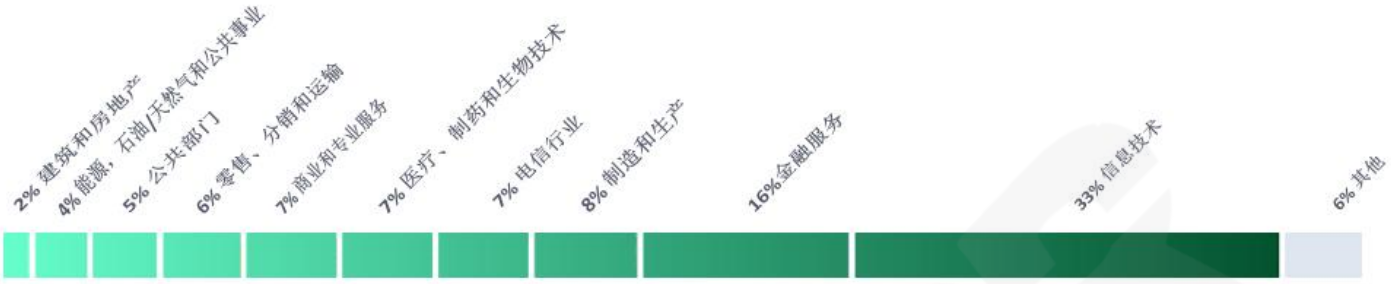
最具破坏性的中断造成的停机时间

受访者还被问及最具破坏性云中断所造成的影响，超过 25%的受访者反馈花了超过三个小时才恢复正常运作，这与 2019 年的调查结果相似。令人担忧的是，这种破坏性中断将继续困扰行业，并使组织蒙受相当大的财务和生产力损失。



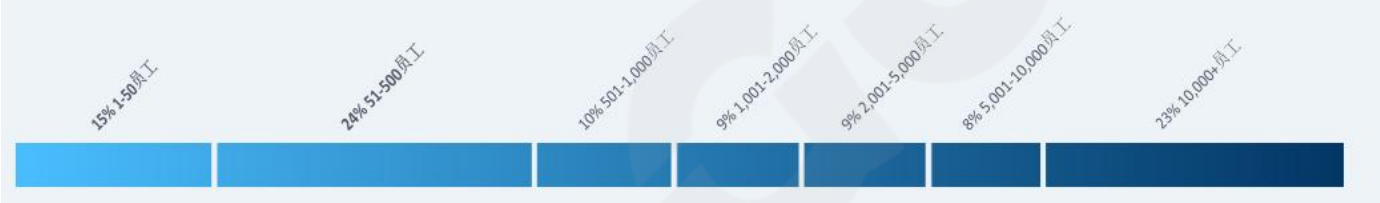
调查对象

这项调查期限从 2020 年 12 月到 2021 年 1 月，收集了来自不同规模、不同行业、不同地点和不同角色的 IT 和安全专业人员的 1900 份回复。



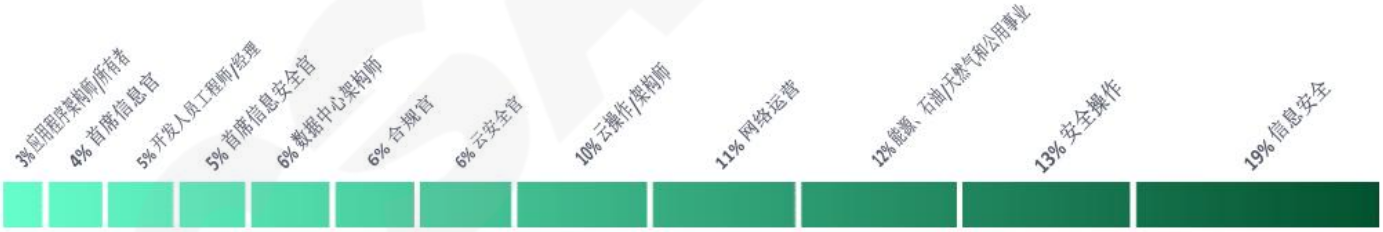
行业

您的组织属于哪个行业？



组织规模

您的组织规模有多大？

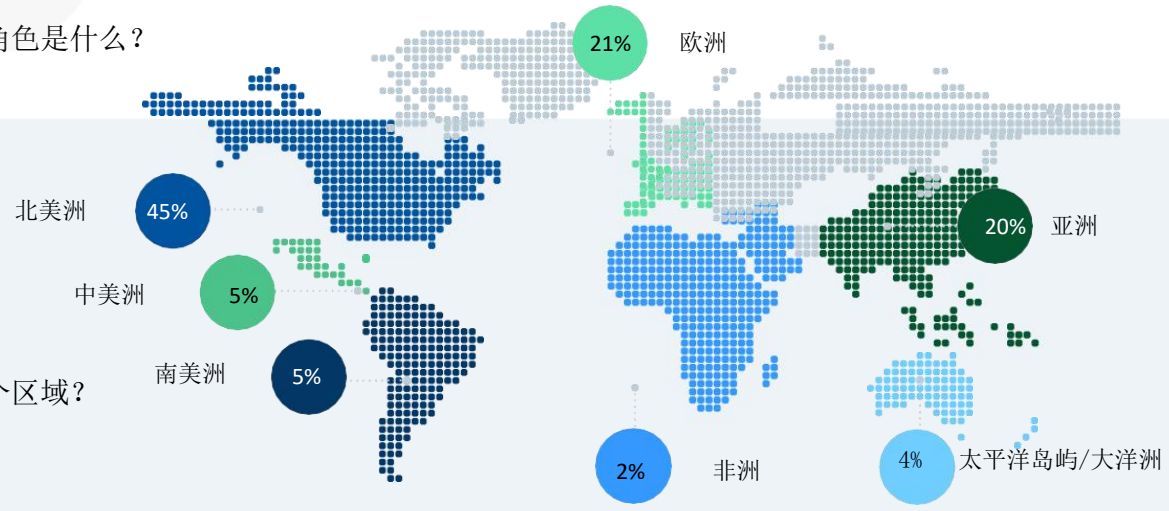


角色

您的主要角色是什么？

地点

您位于哪个区域？



关于阿尔戈斯

AlgoSec 是业内领先的业务驱动型网络安全管理解决方案提供商，帮助世界上最大的组织将安全性与关键任务业务流程结合在一起。与 AlgoSec 合作，用户可以发现，映射和迁移业务应用程序连接，从业务角度主动风险分析，将网络攻击与业务流程联系在一起，并智能实现零接触的跨云自动化网络安全配置，SDN 和本地网络。超过 1800 家企业，其中包括 20 家《财富》50 强企业，已经采用 AlgoSec 的解决方案使组织更敏捷，更安全和更合规。自 2005 年以来，AlgoSec 已通过业界唯一的退款保证显示了对客户满意度的承诺。

赞助商 AlgoSec 是 CSA 企业成员，他们支持研究项目的结果，但没有增加了对 CSA 研究的内容或编辑的影响。