数据防泄露和数据安全性调查报告

CSA GCR GREATER CHINA REGION cloud security alliance®

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

《数据防泄露和数据安全性调查报告（Data Loss Prevention and Data Security Survey Report）》由 CSA 工作组专家编写，CSA 大中华区秘书处组织翻译并审校。

中文版翻译专家组（排名不分先后）：

翻译组：伍海桑　张岳　刘俊红

审校组：姚凯

研究协调员：马逢兴

感谢以下单位的支持与贡献：

北京志翔科技股份有限公司

英文版本编写专家

主要作者：Hillary Baron

贡献者：Josh Buker　Ryan Gifford　Sean Heide　Alex Kaluza　John Yeoh

设计师：Claire Lehnert

特别感谢：Chad Berndtson　Carmine Clementelli　Tim Whitman

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 秘书处给予雅正！联系邮箱 research@c-csa.cn；国际云安全联盟 CSA 公众号。

序言

随着数字化时代的到来，数据已经从背后的支撑变成了组织的核心资产。但在全球化和云计算的浪潮下，如何确保数据的安全和完整性成为了各大组织的首要挑战。为了深入了解这一问题，云安全联盟发起了一项全球在线调查，探讨在云计算为主导的技术环境中，各大组织如何应对数据保护的挑战。这一调查的成果已整理为《数据防泄露和数据安全性调查报告》，为我们揭示了当前的数据安全现状，并预测了未来的发展趋势。

在远程工作和混合办公成为新常态的背景下，传统的数据安全策略已经难以满足需求。DLP 解决方案作为新的策略核心，正在受到越来越多的关注，其在数据泄露防护和企业资产保障中的角色日益凸显。与此同时，零信任安全战略也开始受到重视，它提醒我们在任何情况下，都不能盲目信任任何实体，无论其在系统内还是外。

本报告基于 2022 年的在线调查数据，全面展示了业界对于数据保护的态度和观点。随着远程工作和云环境的普及，数据安全策略也在不断演变。我们深入探讨了 DLP 策略的应用，分析了其面临的挑战，以及企业如何应对远程工作模式下的数据安全问题。希望这份报告能为各大组织提供有价值的参考，帮助他们更好地应对未来的挑战。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

调查创建和方法

云安全联盟(CSA)是一个非营利组织，其使命是广泛推广确保云计算和 IT 技术中网络安全的最佳实践。CSA 还向这些行业中的各个利益相关方介绍所有其他计算形式的安全问题。CSA 是由行业从业者、公司和专业协会组成的广泛联盟。CSA 的主要目标之一是进行评估信息安全趋势的调查。这些调查提供了有关组织当前在信息安全和技术方面的成熟度、意见、兴趣和意图的信息。

Netskope 委托 CSA 开展了一项调查和报告，以更好地了解业界对云计算优先技术环境中的数据保护的知识、态度和意见。Netskope 资助了该项目，并与 CSA 研究分析师共同开发了调查问卷。该调查由 CSA 于 2022 年 10 月和 11 月在线进行，共收到来自不同规模和地点的 IT 和安全专业人员的 2673 份回复。CSA 的研究分析师对本报告进行了数据分析和解读。

研究目标

研究的目的是为了更好地理解如下内容：

- 组织使用的当前 DLP 策略
- DLP 策略遇到的棘手问题和挑战
- 对远程工作人员在数据安全方面的担忧
- 面向员工的安全培训

关键发现

随着迁移到远程或混合工作环境，传统的边界减少或消除，针对云优先环境的数据安全方法必须调整。数据安全也是零信任安全战略的关键租户，这一战略得到了普及，进一步刺激了人们对数据安全的关注。DLP 解决方案通常是组织数据安全战略不可或缺的一部分，但组织仍在努力制定其战略并实施这些解决方案，尤其是要管理和维护传统 DLP 解决方案的复杂性。

关键发现 1:

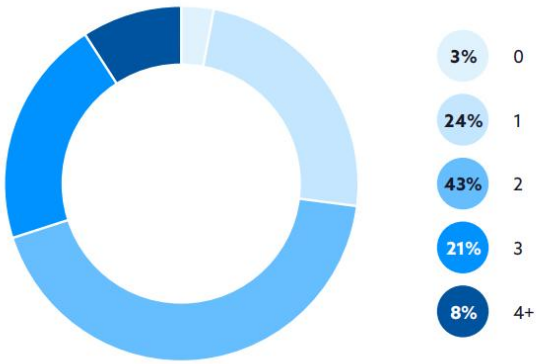
云是传输和共享数据的主要方式

当今时代，组织主要通过云传输和共享数据，这是 COVID-19 全球大流行催化的趋势。组织使用各种不同的方法。最常用的方法是云存储应用程序(46%)，如 OneDrive、Box 或 Dropbox。其他常见方法包括云到云(39%)，使用率略高于电子邮件(38%)或云协作和消息传递应用程序(31%)，如 Slack 或 Teams。无论采用哪种方法，组织显然都在信任云，即使是他们最敏感的数据。

关键发现 2:

大多数组织使用两种以上 DLP 解决方案

大多数组织(72%)使用两或更多 DLP 解决方案作为其 DLP 数据的一部分安全策略。对于较大的组织（员工数量超过 5000），50%使用三个或更多 DLP 解决方案。单个 DLP 解决方案不能满足大多数组织的需求,而需要将多个 DLP 解决方案拼凑在一起这可能是由于组织使用复杂的 IT 环境，需要使用多个解决方案完全覆盖其环境。除了复杂的多云环境之外，当今大多数组织还在处理旧式环境。



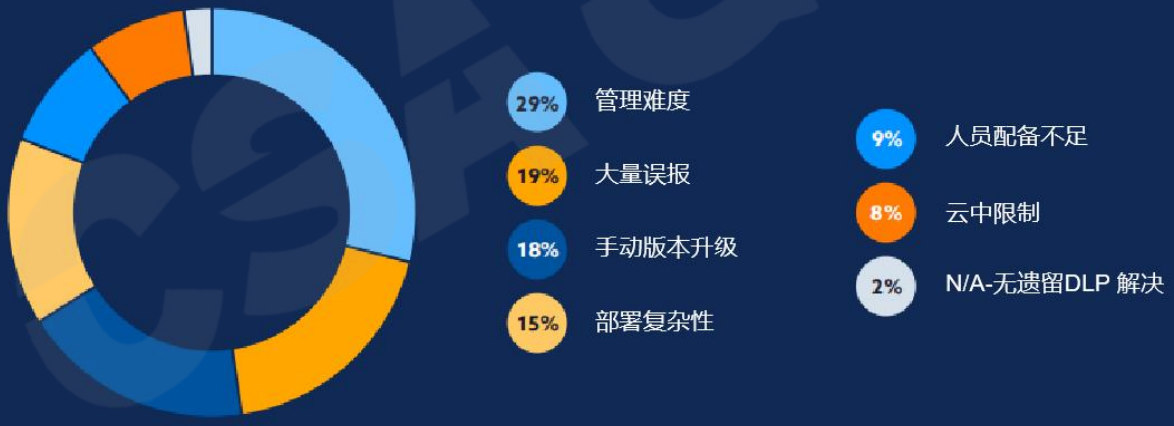
关键发现 3:

企业难以管理其复杂的 DLP 环境

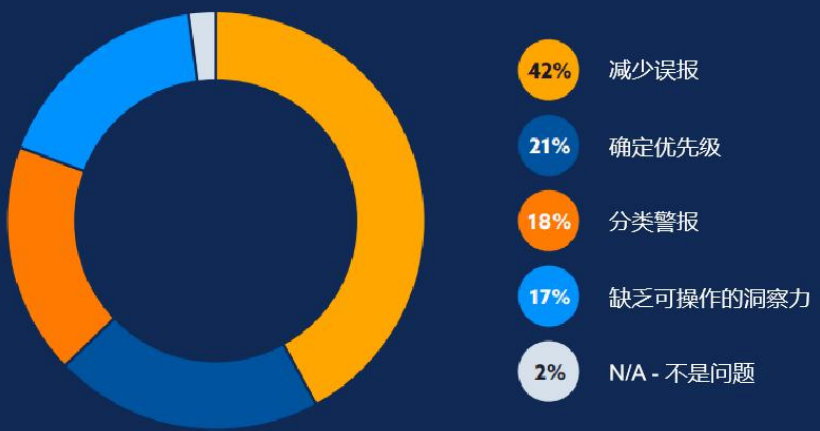
DLP 面临的许多主要挑战都与管理问题直接或间接相关。安全团队已经超负荷工作，当前将多个 DLP 解决方案拼凑在一起的方法使问题更加严重。组织面临的最大挑战是管理难题(29%)。调查受访者提到的第二个最常见的问题是误报太多(19%)，这表明难以针对其环境优化 DLP 产品。当涉及到误报时，组织主要是在努力减少误报以及误报造成的手动管理负担。

DLP 面临的其他挑战包括需要手动版本升级(18%)，这可能会进一步导致管理困难，以及部署复杂性(15%)，这可能是由于需要多个解决方案来满足其复杂环境或安全需求。除了这些挑战之外，员工还在努力寻找政策模板，86%的受访者认为这是一项适度到高难度的任务。总而言之，组织当前使用的 DLP 策略过于繁琐，而且组织需要更加简化的方法/策略。

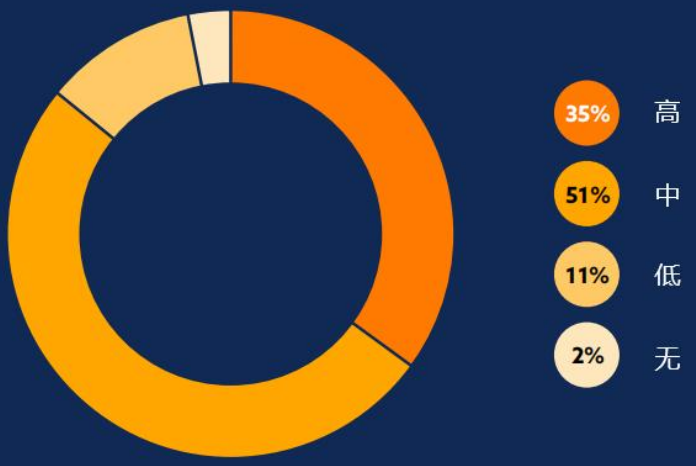
旧式企业 DLP 面临的主要挑战



误报率的主要挑战



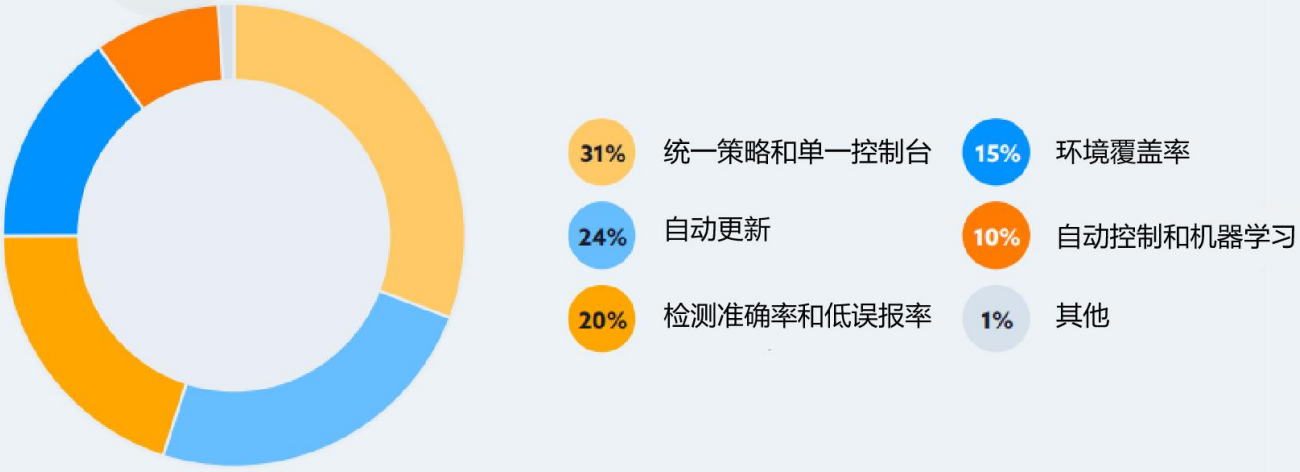
查找策略模板的难度级别



关键发现 4:

组织应优先考虑可简化管理的 DLP 解决方案

组织正在寻找能够解决这些问题和管理难题的 DLP 和数据保护解决方案。统一策略和单一控制台解决方案(31%)将帮助组织解决管理难题和部署复杂性。自动更新(24%)避免了额外的手动工作，并减少了管理难度。此外，检测准确率(20%)减少了误报率。总而言之，组织正在寻找更易于管理和满足云需求的数据保护解决方案。



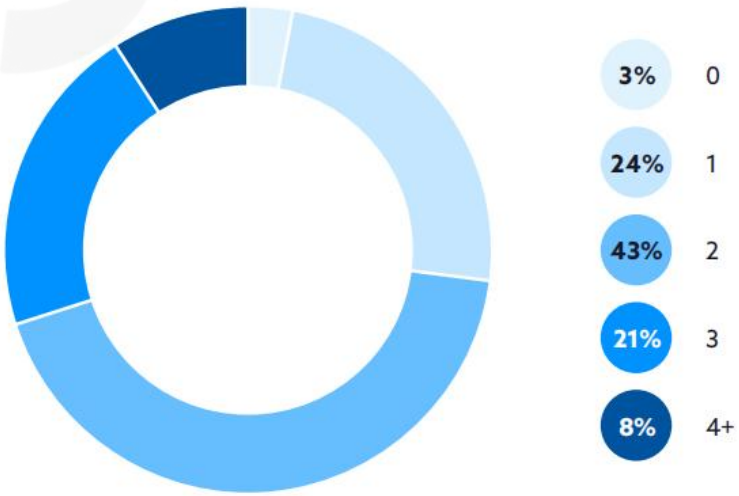
DLP 策略概述

共享和传输数据的方法

员工主要通过云来传输和共享数据。最常见的方法是云存储应用（46%），如 OneDrive，Box 或 Dropbox。其他常见的方法包括云到云（39%），其使用量略高于电子邮件（38%），或云协作和消息传递应用程序（31%），如 Slack 或 Teams。无论采用哪种方法，组织对云及其数据表示信任。

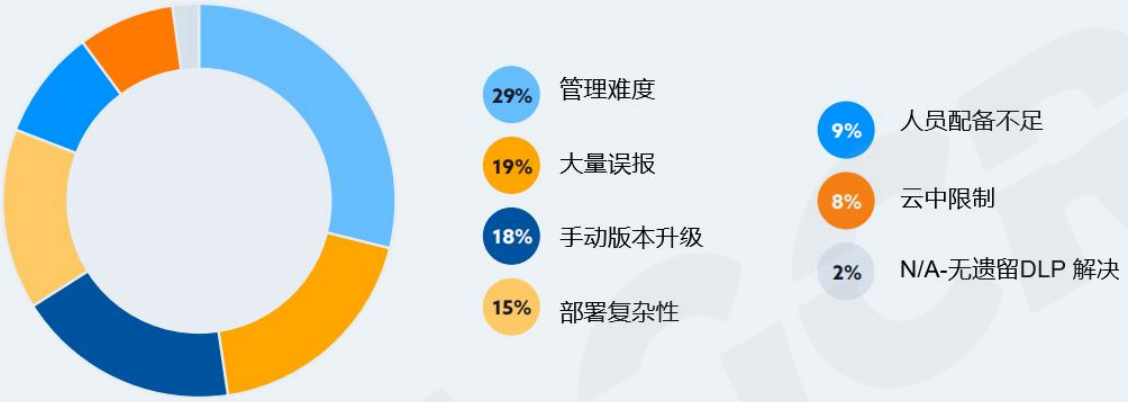
DLP 解决方案数量

大多数组织（72%）使用两个或多个 DLP 解决方案作为其战略的一部分。对于大型组织，即员工数超过 5001 的，50%使用三个或更多个 DLP 解决方案。原因可能是由于组织需要覆盖各种业务环境。无论如何，组织必须将多个解决方案组合在一起以满足他们的需求。



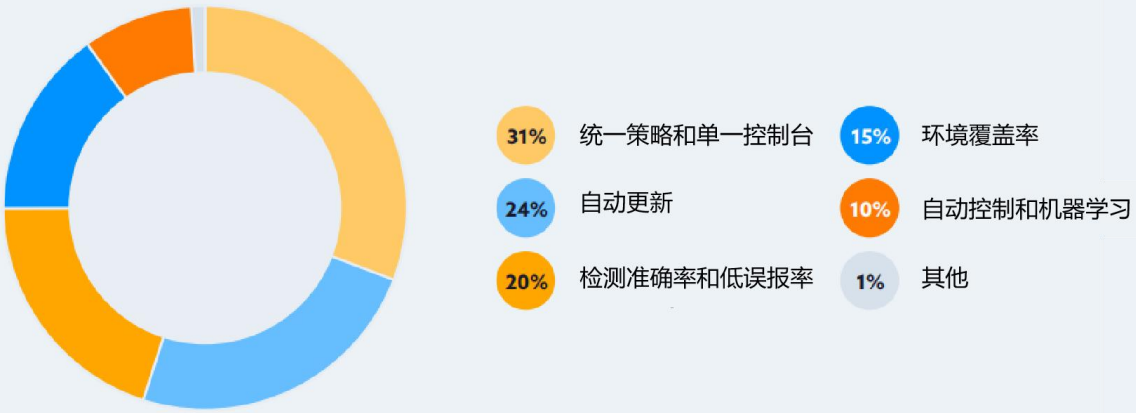
传统企业 DLP 面临的主要挑战

在传统企业 DLP 解决方案方面，组织面临的最大挑战是管理（29%）。这并不奇怪，因为组织经常使用两个或多个解决方案。另一个常见的挑战是收到太多的误报（19%），这里的主要问题是如何微调产品来满足组织需求。手动版本升级（18%）是第三大最常见的挑战，这可能会在管理产品时造成额外的压力。部署复杂性则是15%的组织面临的挑战，这可能是由使用多种解决方案引起的，并进一步增加前文所提到的管理困难挑战。



新数据保护解决方案所需的功能

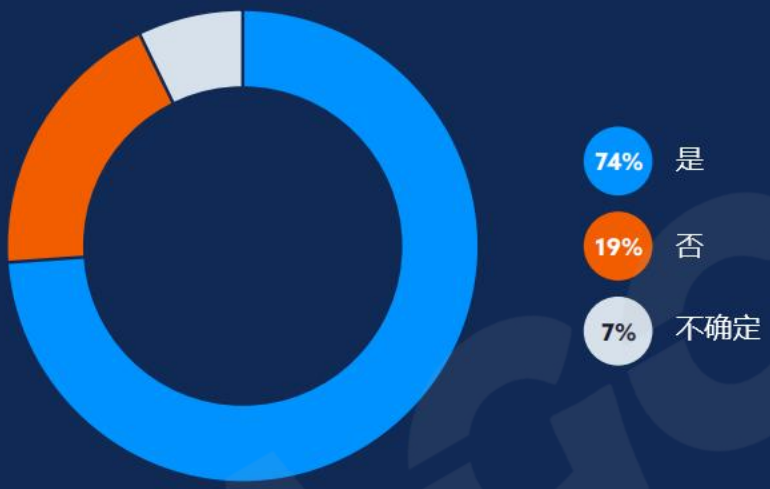
作为对其所面临挑战的直接回应，组织正在寻找解决这些问题的 DLP 和数据保护解决方案。统一策略和单一控制台（31%）将帮助组织解决管理困难和部署复杂性。自动更新（24%）避免了额外的手动工作，减少了管理难度。此外，提高检测准确率和降低误报（20%）的数量。总之，组织正在寻找能够解决其当前痛点的数据保护方案。



零信任和 DLP

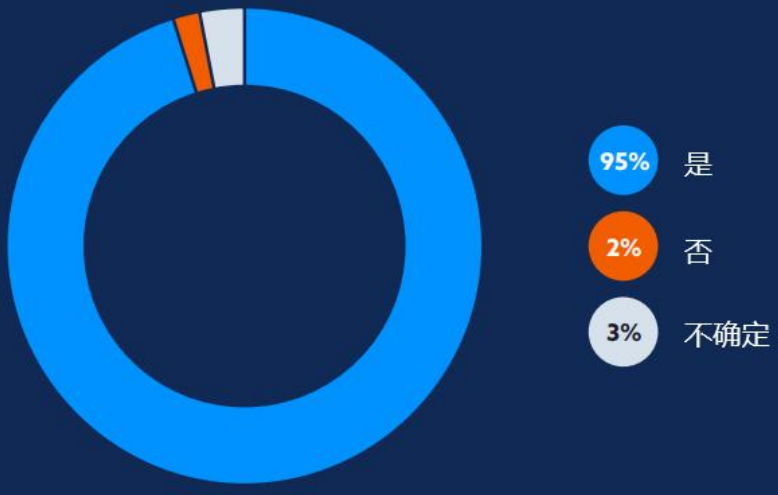
使用零信任策略

在过去几年中，零信任一直是该行业的趋势。不出所料，组织对实施自己的零信任策略非常感兴趣（74%）。这并不意味着所有这些组织都已经完全实施了他们的战略，他们可能只是仅仅创建了一个战略。



DLP 集成到零信任策略中

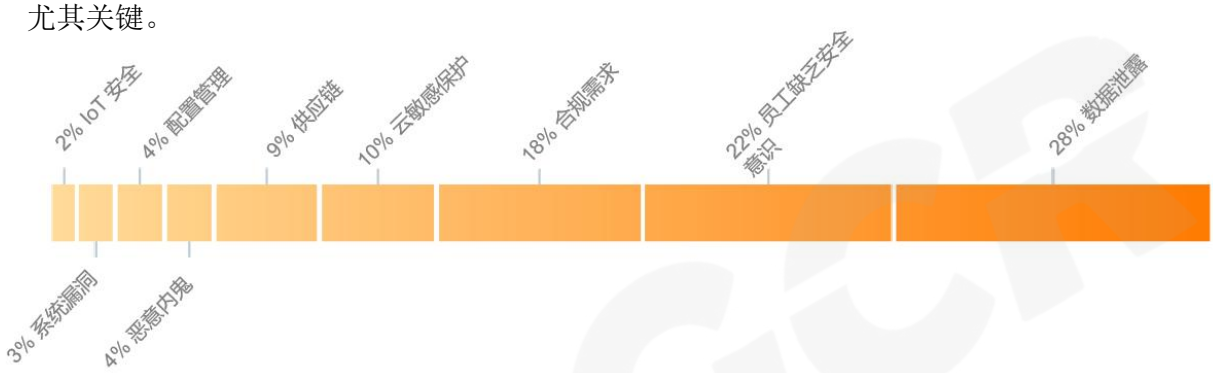
数据保护是任何零信任策略的关键支柱。因此，许多组织将其 DLP 解决方案作为其整体零信任策略的一部分也就理所当然了（95%）。



痛点和挑战

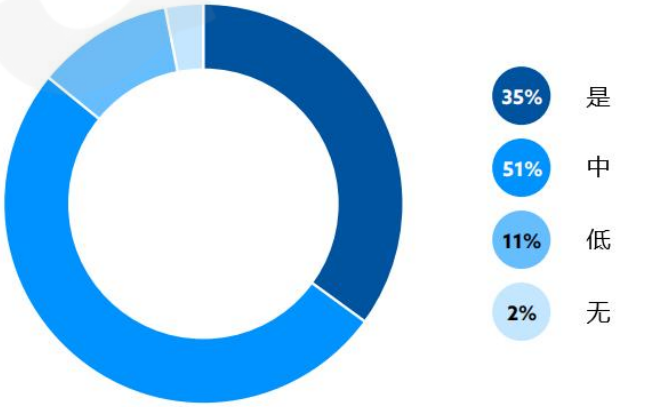
首要安全问题

组织的三大首要安全问题并不让人意外。最常选择的是数据泄露（28%），其次是员工缺乏安全意识（22%），再就是合规需求（18%）。几十年来，数据泄露一直是人们最关心的问题，但随着云优先环境中攻击面的增加，防止数据泄露只会变得更加复杂。现在安全已成为组织中每个人的责任，所以提升安全意识和减少人为错误变得更加重要。这一点随着整个供应链中员工和承包商对敏感数据的访问量增加而变得尤其关键。



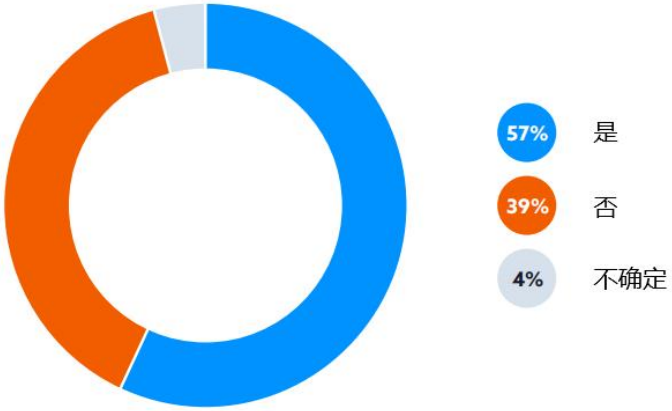
难以找到策略模板

大多数员工很难为其组织找到策略模板（86%）。超过三分之一的人报告说这是非常困难的，超过一半的人报告说这项任务是中等难度的。只有 13%的受访者表示查找政策模板的难度较低或没有难度。当然，寻找的困难，本身可能来自于不常使用。



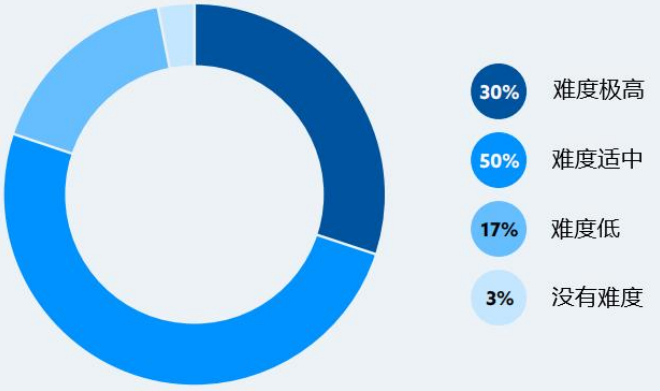
过去一年的安全事件

大多数组织（57%）表示在过去一年中经历了重大安全事件。需要注意的是，这里说的是安全事件，不一定是数据泄露等破坏行为。39%的人没有经历任何事故，只有 4%的人表示他们不确定。



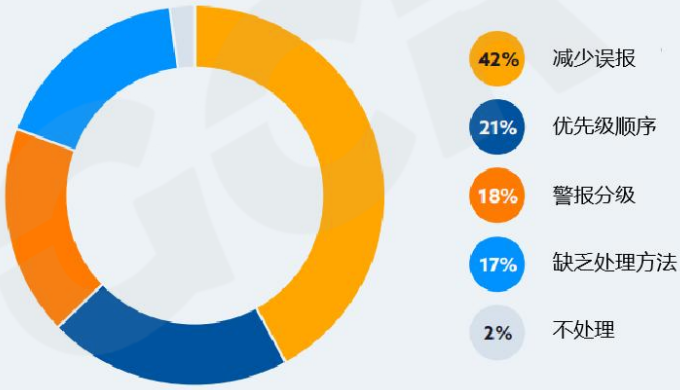
误报管理困难

大部分员工（80%）认为难以对现有 DLP 方案的误报 进行有效管理。 其中不足三分之一的人认 为这项任务难度极高，半数人则认为难度适 中，仅有 20%的人表示难度低或没有难度。这些难度描述与传统企业 DLP 的最大挑战相一致。



减少误报的挑战

目前，组织在应对误报问题时主要通过微调 DLP 工具的方式直接减少误报（42%）。其他常见的办法包括优先级排序 （21%）告警分级管理（18%）， 还有 17%的组织不知道 如何处理。此外，只有 2% 的组织认为不需要 处理。这反映出市面上众多 DLP 产品的复杂性。



数据治理的挑战

组织发现当数据治理涉及到图像、链接和移动数据等不同的数据类型时，是最具挑战性的，其次是数据分类（如个人身份信息、财务数据）、数据位置和数据风险的确定。上述挑战的排序遵循数据治理的自然进展，即，组织需要先了解数据类型和分类，才能准确划定数据风险。

远程工作者的 DLP 策略

远程办公人员占比

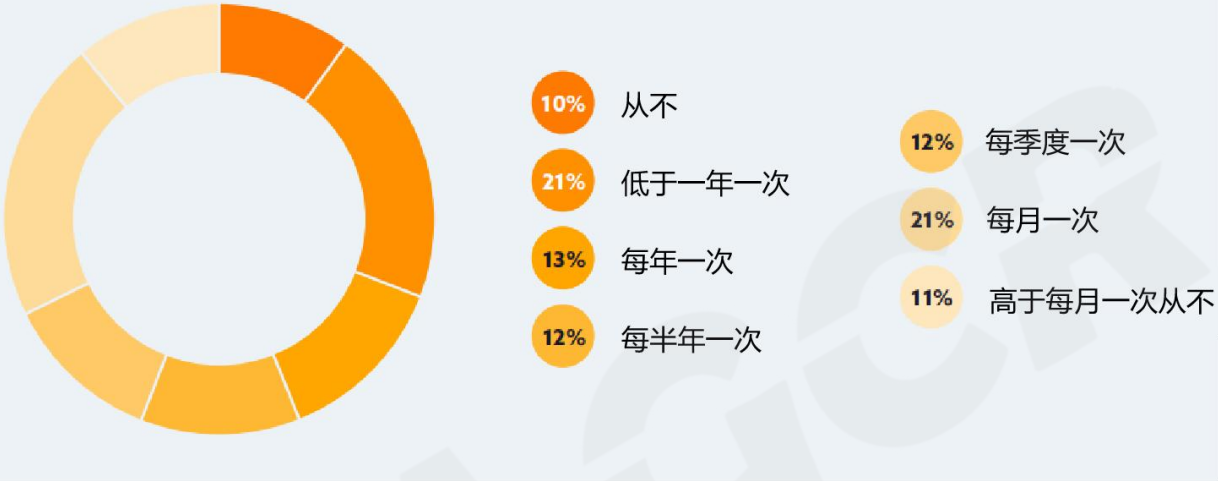
平均而言，远程办公人员占比为 51%。由于近期的公共卫生安全问题，远程办公的趋势已经日益明显，但是对于大约一半的员工来说，远程办公已经几乎成为永久方式。

远程办公者面临的首要安全问题

在远程办公方面，组织最关心的安全问题是员工采取的网络安全措施有限（44%）。由于远程工作人员不再位于公司网络上，因此网络安全成为整体安全的关键；远程办公者也许可以在工作时更加方便的操作个人设备访问个人账户，但这同样会导致未经批准的数据传输行为的发生，并以 42%的比例成为组织关注的第二个问题。其他常见问题包括 网络钓鱼诈骗（33%）、设备 被盗（30%）、用户行为透明性差（30%）以及 未经授权的设备访问（30%）。

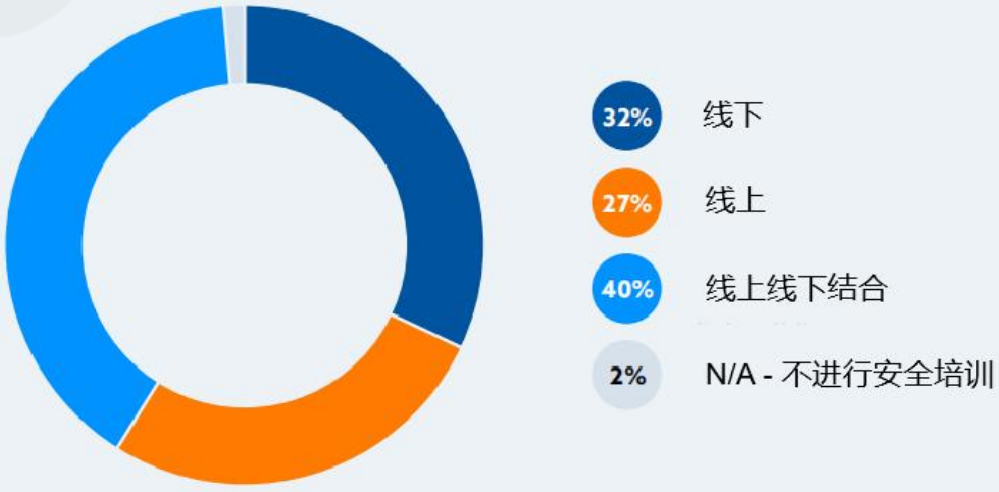
安全培训的频率

近 1/3 的组织（31%）对员工进行安全培训的频率低于一年一次或从不进行培训。其次常见的频率是每月一次（21%）。 安全培训频率在每年一次、每半年一次和每季度进行一次的较为不常见，占比分别是 13%、12%和 12%。 此外，还有 11%的被调查者每月进行一次以上的安全培训，但这可能是因为这些培训并不需要员工每次都参加。



安全培训的交付方式

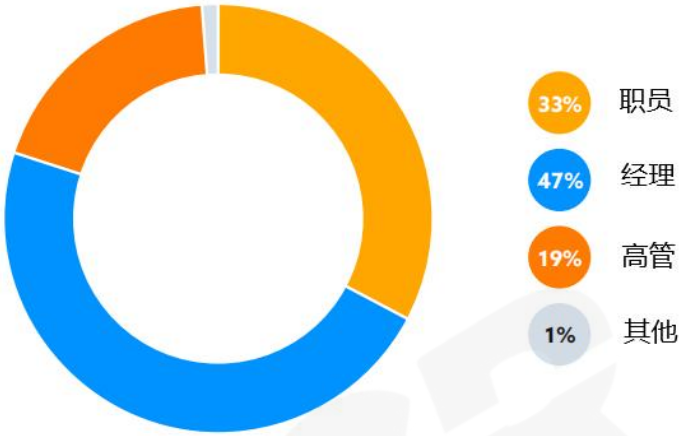
安全培训提供方更倾向于采取线上线下相结合的方式进行安全培训（40%）。对于只提供一种方式培训的组织，只提供线下培训的占比为 32%，稍高于只提供线上培训的占比（27%）。



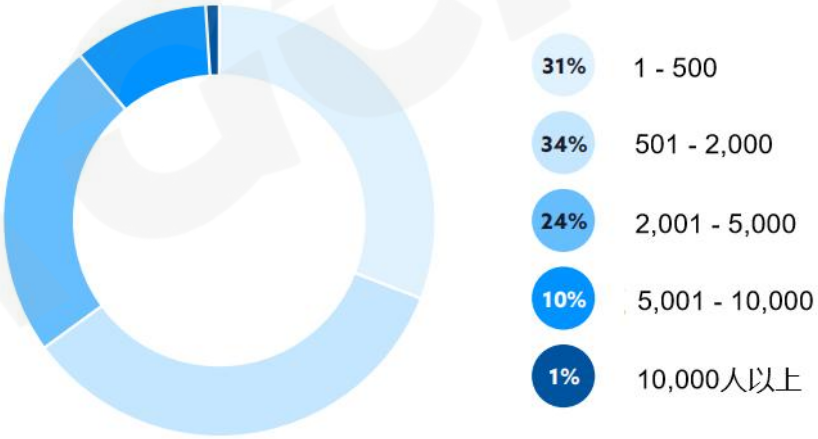
统计数据

该调查由 CSA 于 2022 年 10 月和 11 月通过在线方式开展，共收到 2673 份回复，这些回复来自不同地区和不同规模的组织中的 IT 和安全专业人员。

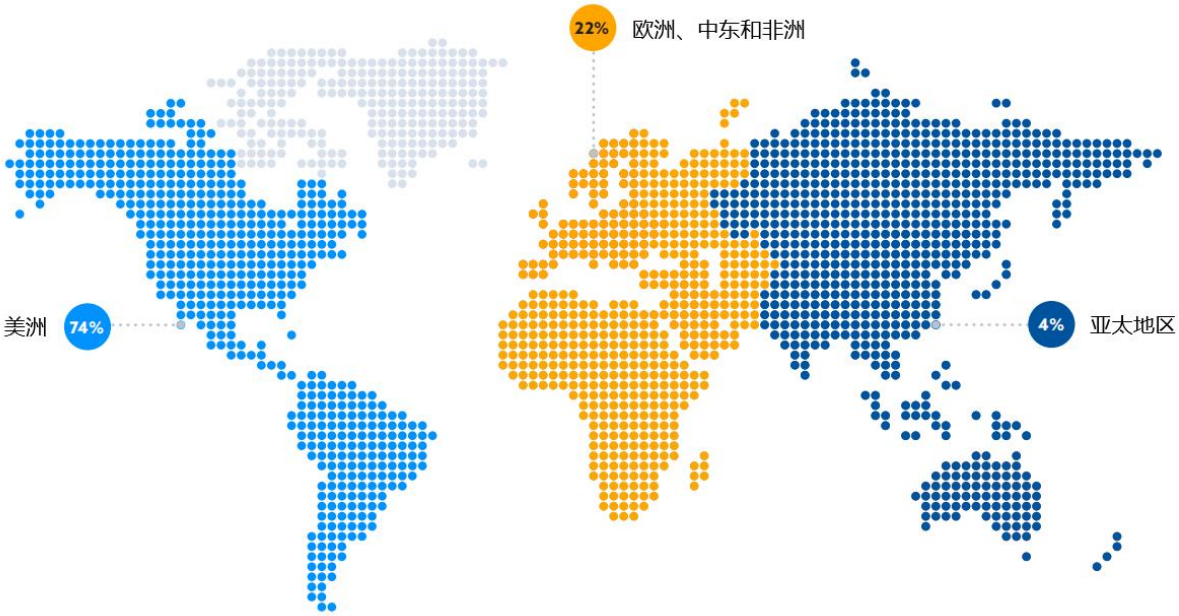
你的主要角色是什么？



你供职于何种规模的企业？



以下那一项最准确描述了您所居住的地区？



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