全球数据保护指数 — 2024 年特别版

主要调查结论 — 2023 年 10 月

VansonBourne

DELL Technologies

主要调查结论

1
数据保护风险形势

2
网络攻击威胁日益增多

3
多云的使用

4
保护云环境

五个要点

网络攻击继续呈上升趋势

网络攻击的成本不断增加

保险单无法完全支付因攻击而造成的成本

随着生成式 AI 的使用越来越广泛，可能会产生更多高价值的数据

网络攻击带来更大的风险和更多的财务影响

受访者有哪些?

2023 年 9 月和 10 月期间采访了 1,500 名 IT 和 IT 安全决策者

受访组织来自各类公共和私营行业

拥有 250 名以上员工的组织

4 个地区:

美洲 (300)
欧洲、中东和非洲 (675)
亚太及日本地区 (375)
中国 (150)

1. 数据保护风险形势

不仅普遍担忧其数据保护措施的担忧，而且缺乏信心 — 组织发现自身处于弱势地位

60%

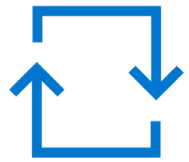
的受访者对其组织能够实现**备份与恢复服务级别目标 (SLO) 不是很有信心**

79%

的受访者**担心**他们将在未来 12 个月内**经历中断性事件**

75%

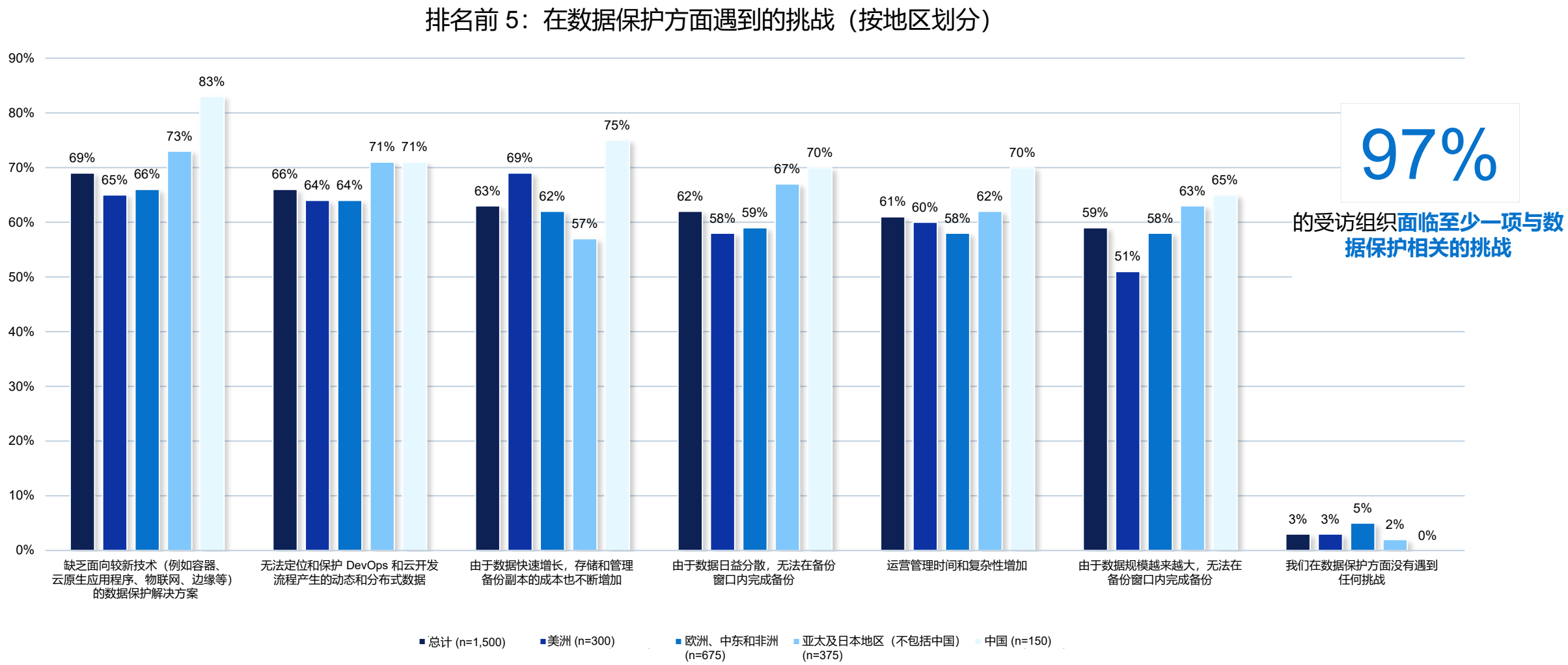
的受访者**担心**其组织现有的数据保护措施**可能不足以应对恶意软件和勒索软件威胁**



65%

的受访者对于在发生数据丢失事件时**能否让所有平台的系统/数据完全恢复不是很有信心**

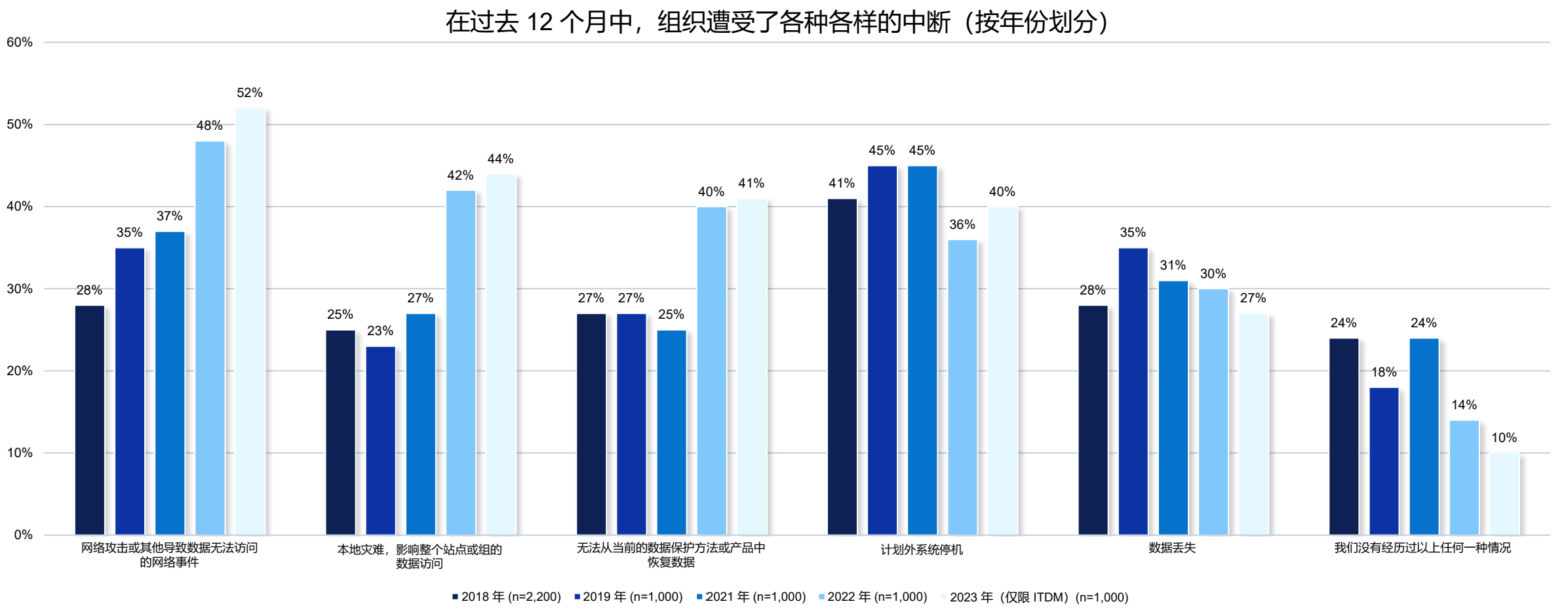
除了对数据保护的担忧之外，许多组织还面临着以下挑战



97%

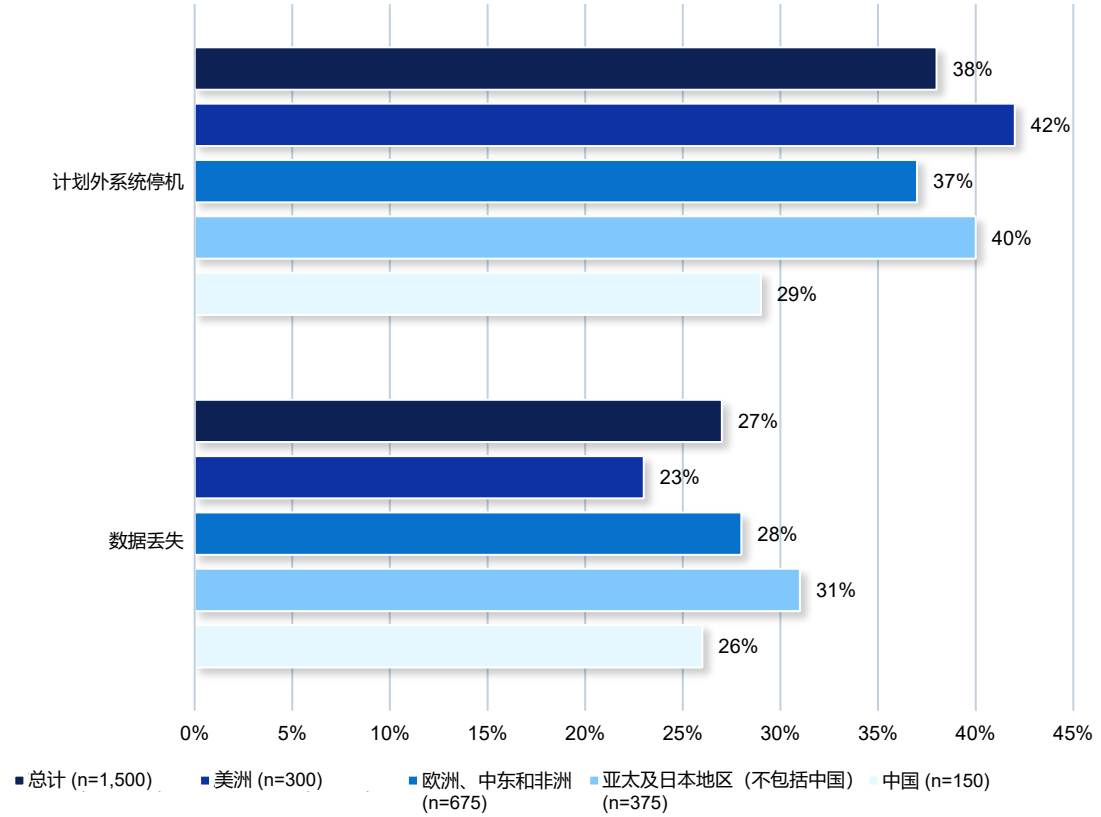
的受访组织**面临至少一项与数据保护相关的挑战**

在过去 12 个月中，由于网络攻击带来的威胁持续存在且不断增加，组织因此面临严重的中断风险



数据丢失不仅导致中断，而且还影响收入

在过去 12 个月中，经历过计划外系统停机或数据丢失的组织百分比（按地区划分）



在过去 12 个月中：

26 小时

平均经历的**计划外系统停机时间**

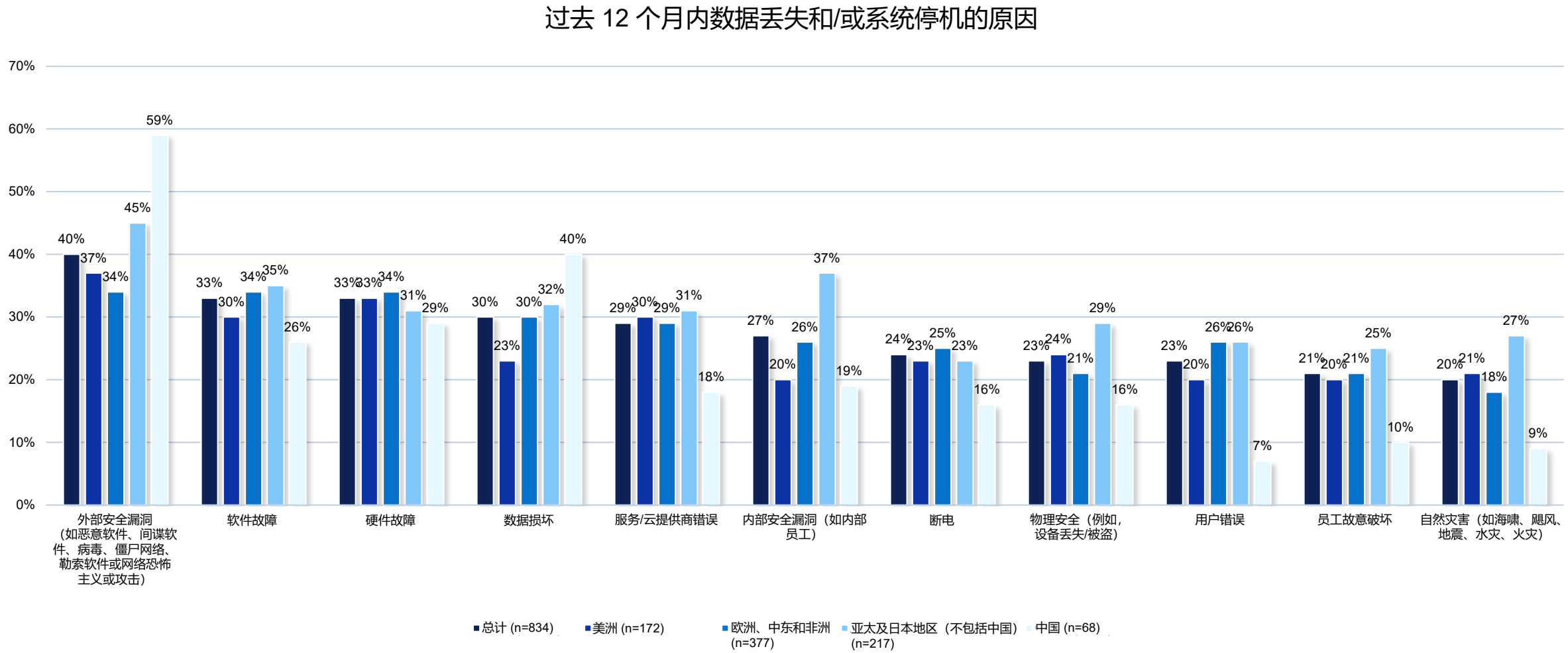
2.45 TB

丢失的**数据量**（平均而言）

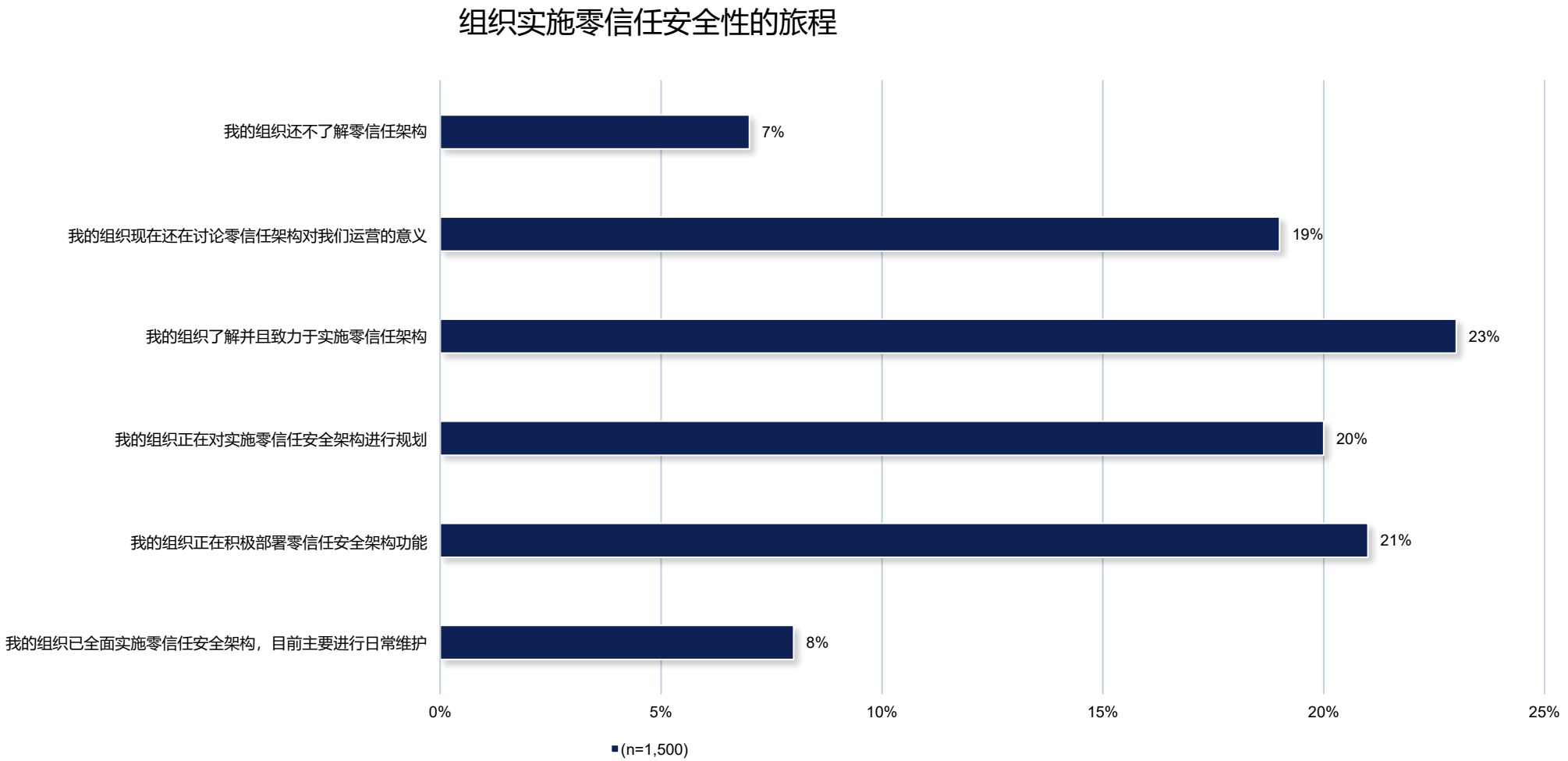
261 万美元

因**数据丢失而产生的**平均成本

在过去 12 个月内，外部安全威胁是导致数据丢失和/或计划外系统停机的最常见原因



尽管存在数据保护方面的挑战和顾虑，但很少有组织完全实施了零信任安全性

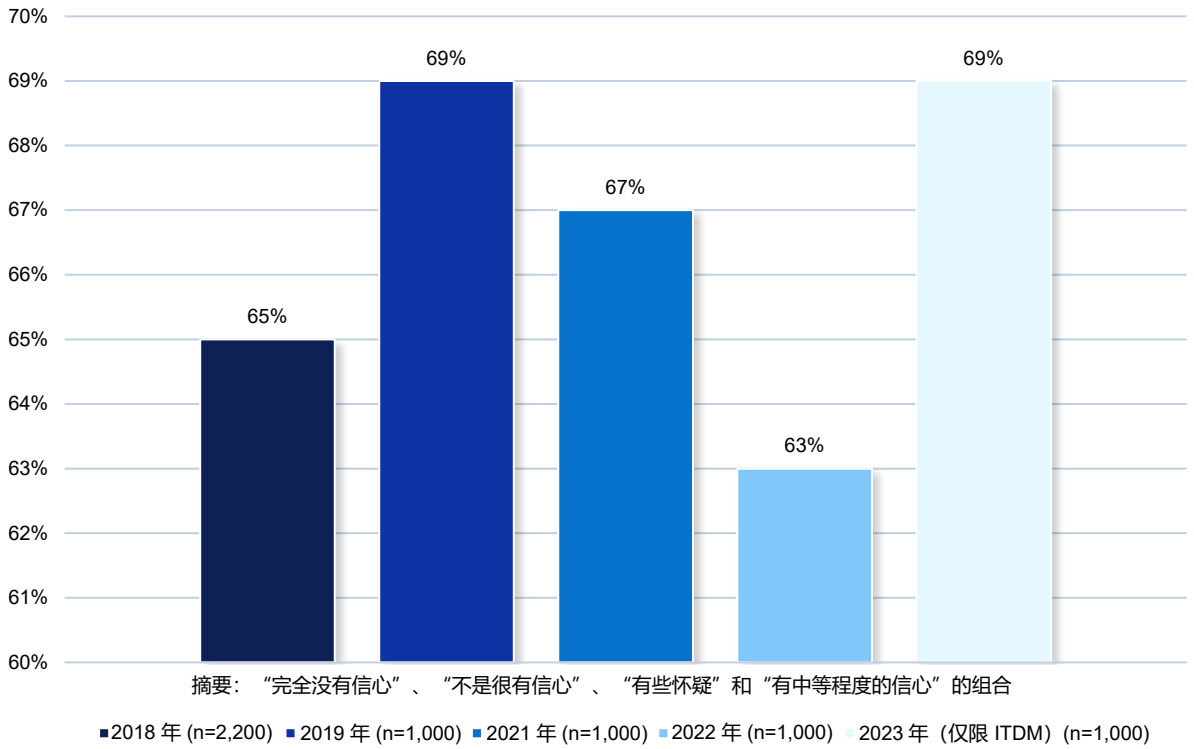


筛选器：数据划分：地区 = 总计

2. 网络攻击威胁日益增多

不仅普遍担忧其数据保护措施的担忧，而且缺乏信心 — 组织发现自身处于弱势地位

对于在发生破坏性网络攻击时妥善恢复所有业务关键型数据表示“不是很有信心”（按年份划分）



81%

的受访者一致认为，随着居家办公员工数量的增加，**其组织因遭受网络威胁而导致数据丢失的风险更高**

74%

的受访者**担心**他们的备份数据可能会被**勒索软件攻击感染或损坏**

人们对勒索软件攻击所造成的后果有一种被误导的过度自信，这进一步加剧了风险

72%

的受访者认为，他们的工作和组织内的员工**不会受到勒索软件攻击的影响**

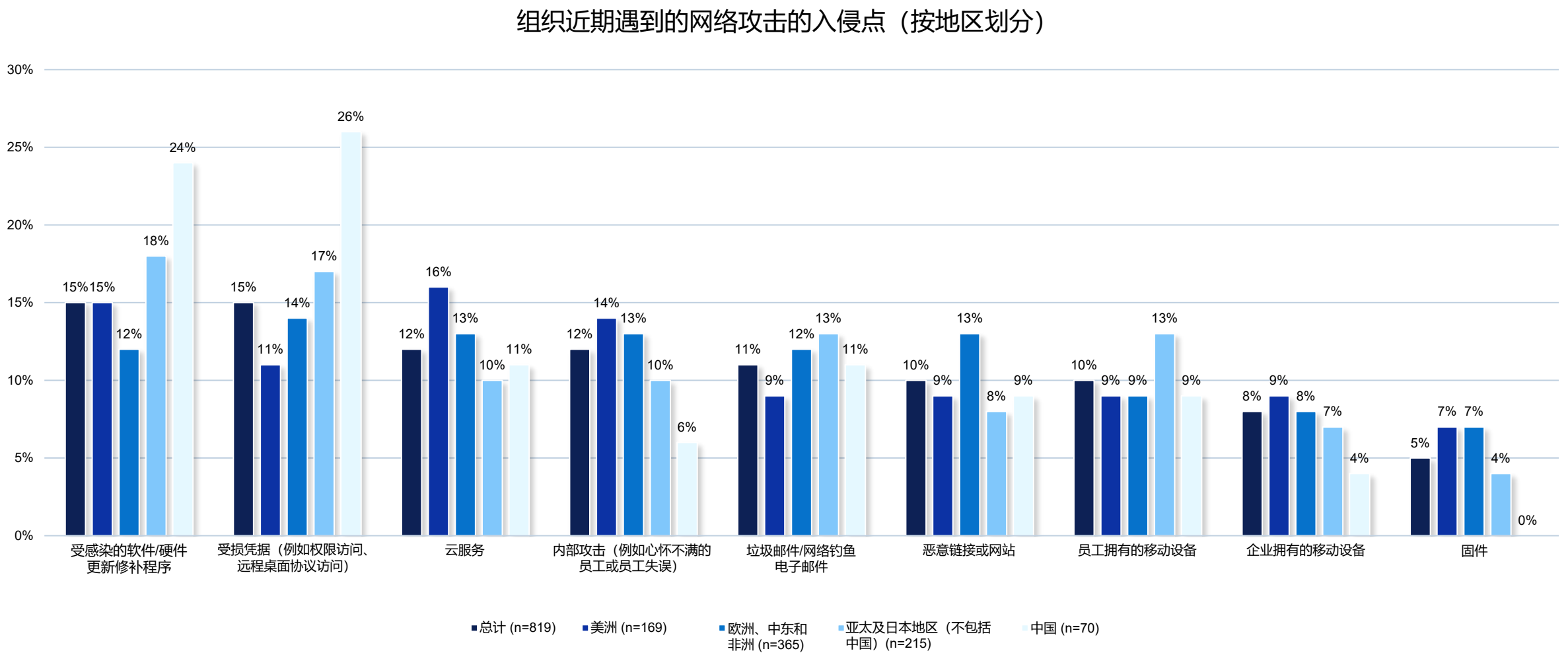
74%

的受访者认为，如果其组织受到勒索软件攻击，只要他们**支付赎金**，就会**赎回所有数据，从而恢复业务运营**

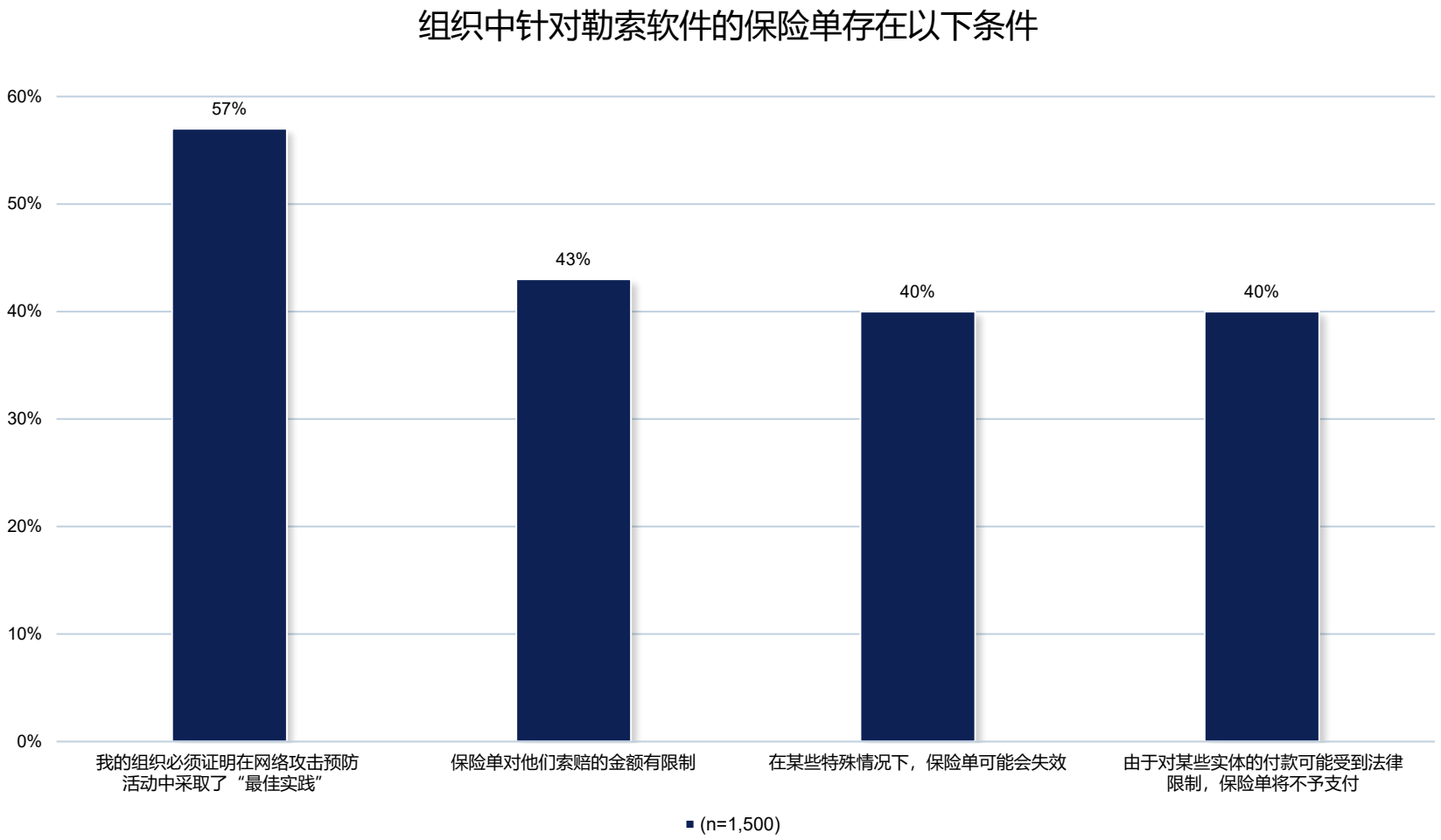
66%

的受访者认为，如果其组织受到勒索软件攻击，一旦他们支付了赎金，**就不会再次受到攻击**

网络犯罪分子以各种入侵点为目标，攻击更有可能来自外部来源



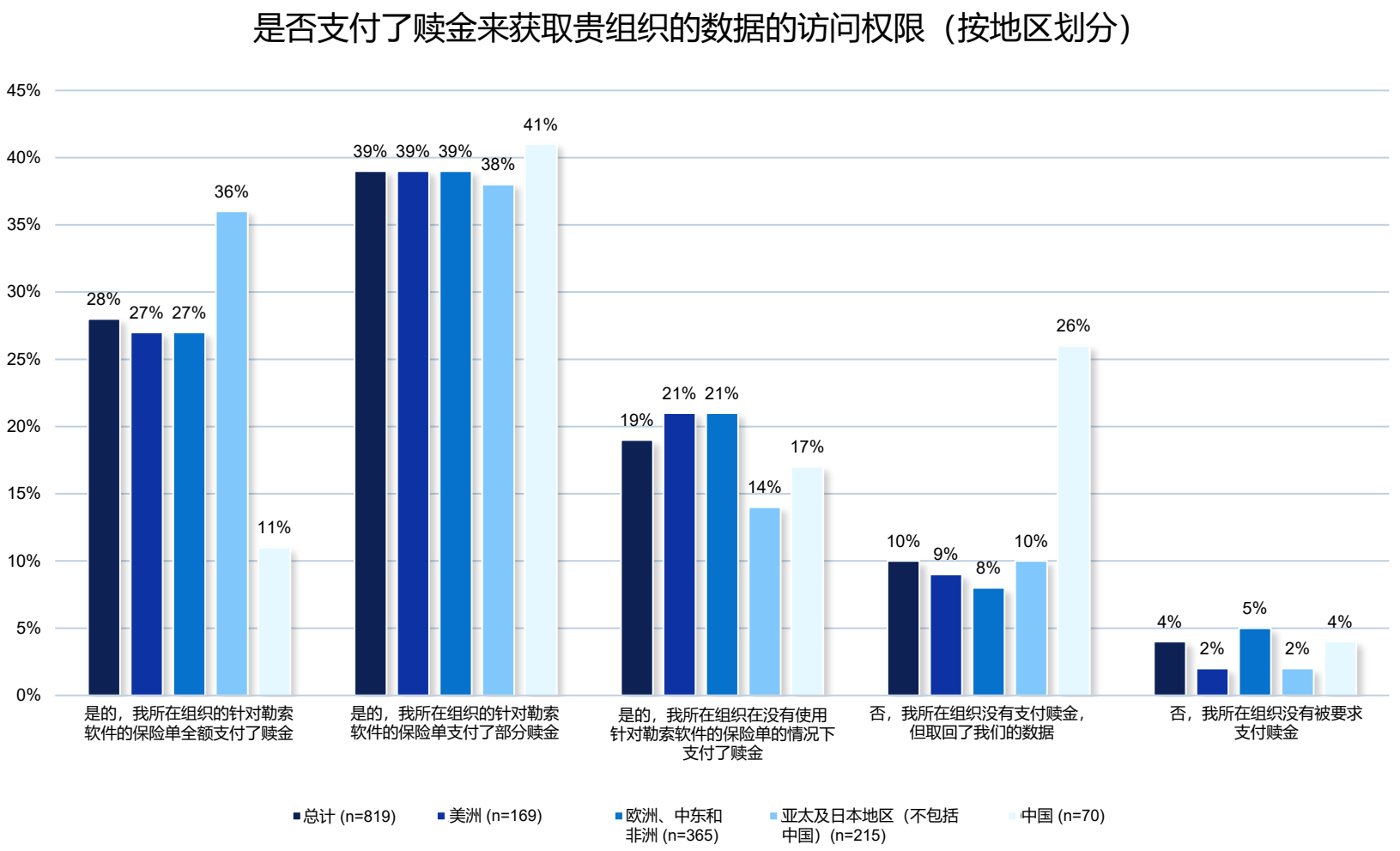
尽管为勒索软件投保在组织中司空见惯，但这种保险单有很大的局限性



93%

的组织**拥有针对勒索软件的保险单**

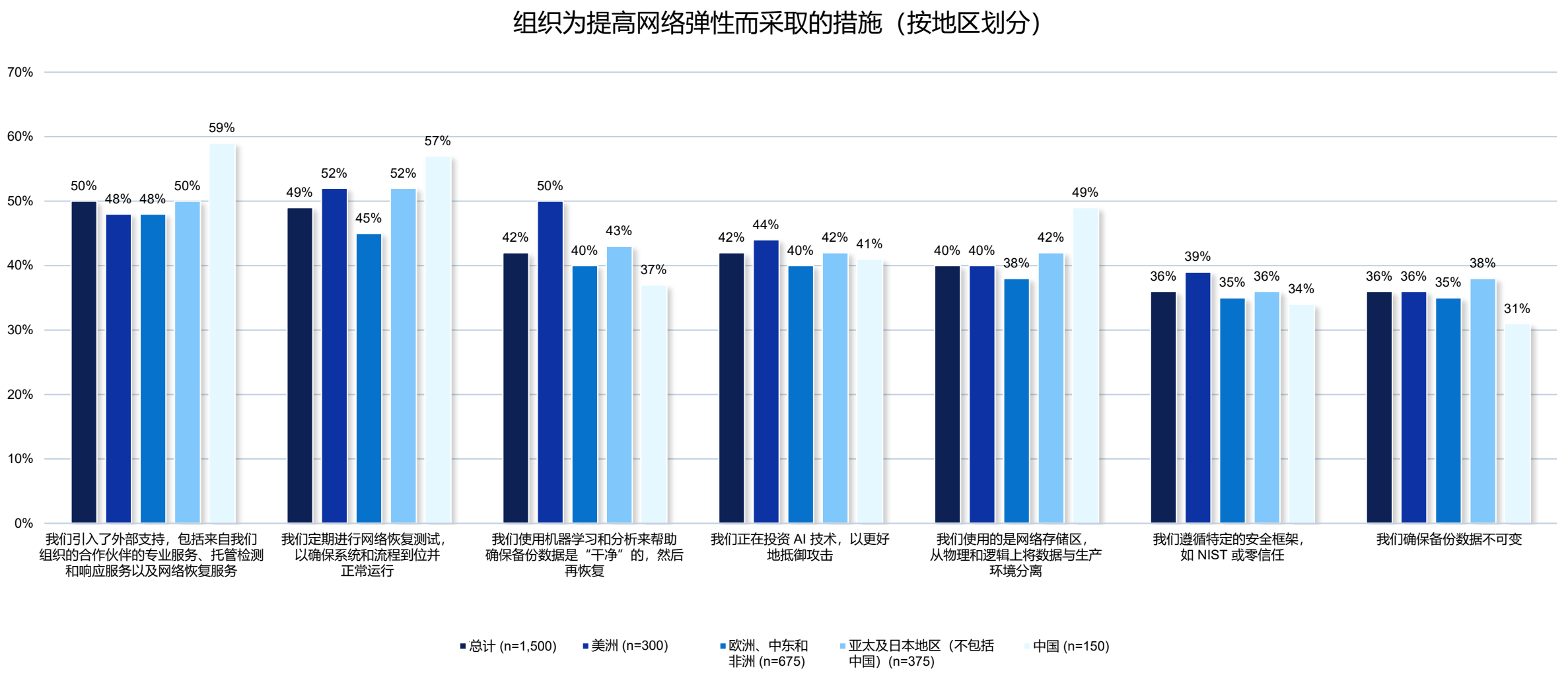
尽管许多组织为勒索软件投保，但仍然面临财务风险



192 万美元

— 过去 12 个月内因**网络攻击和其他网络相关**事件给组织造成的平均成本

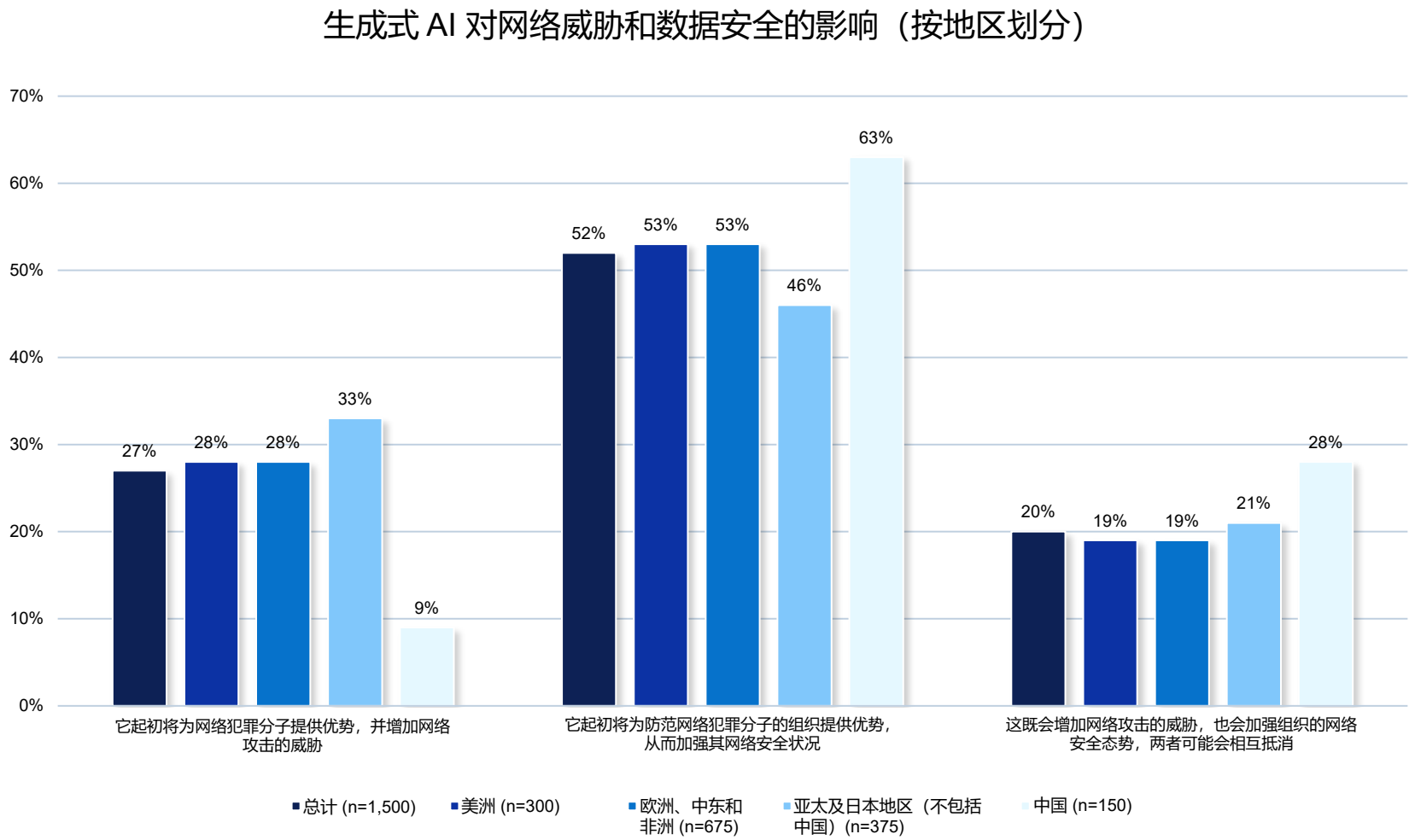
令人鼓舞的是，组织正在采取措施来提高网络弹性



但是，并非所有人都认为生成式 AI 有利于网络弹性受益

81%

认同新兴技术（如 AI、物联网、边缘）**给数据保护造成了风险**



事实上，随着组织开始关注数据保护，许多人认为生成式 AI 将带来新的挑战

88%

的受访者认同，生成式 AI 将产生大量新数据，**需要采取保护措施来确保其安全无虞**

88%

的受访者认同，生成式 AI 将提升某些数据类型的价值，这类数据需要**更高的数据保护服务级别**

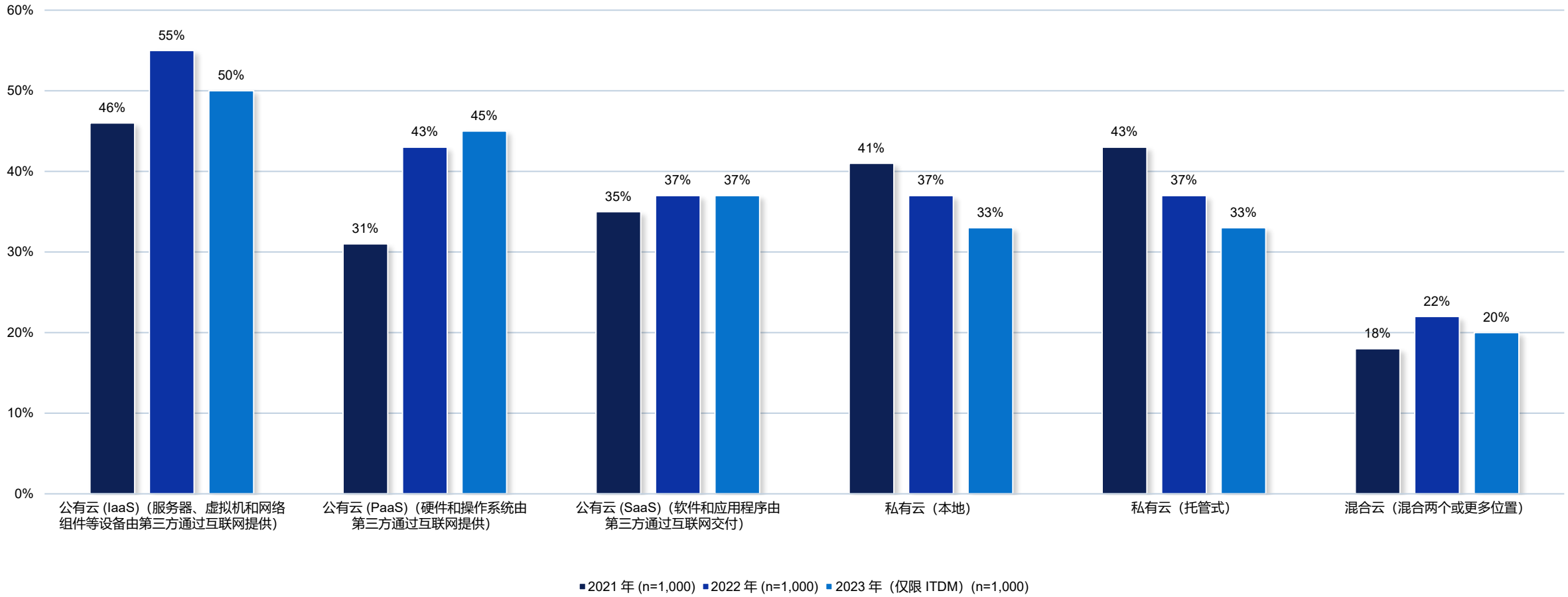
85%

的受访者认同，如果用于生成式 AI 的数据集**受到损坏**，将会**影响生成式 AI 的输出**

3. 多云的使用

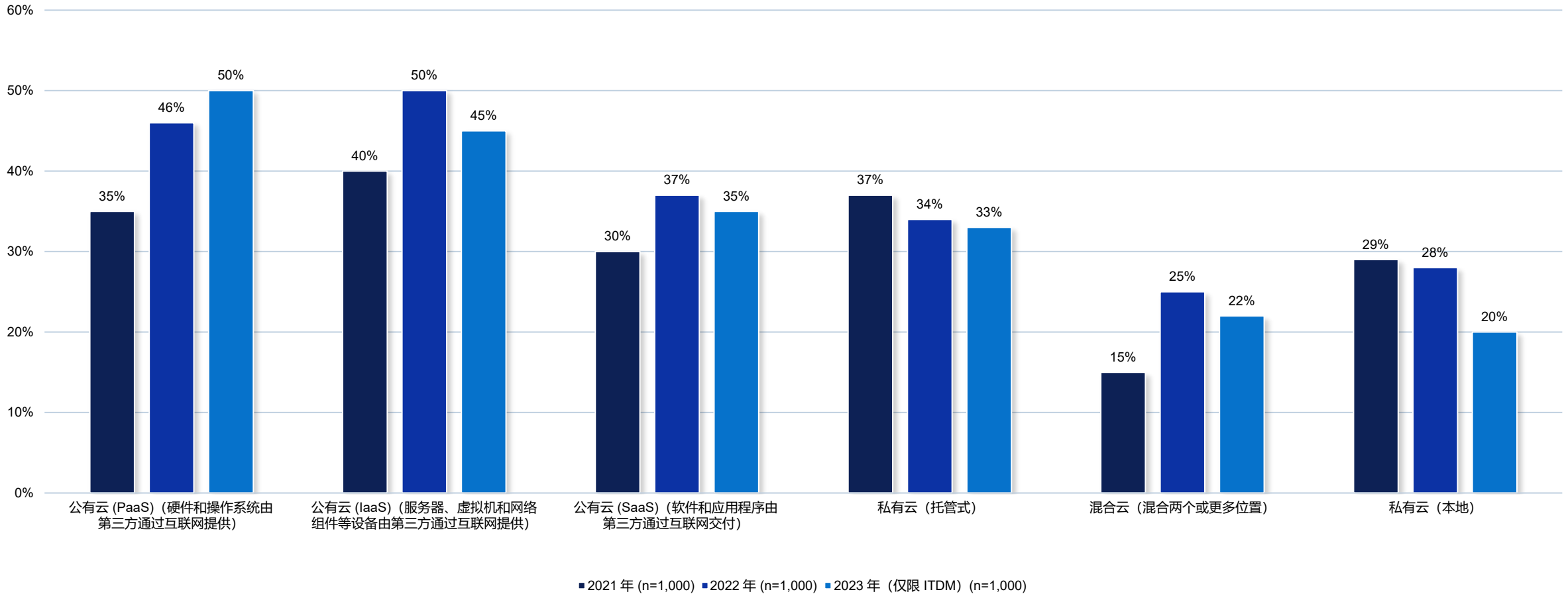
在更新现有应用程序时，公有云仍然是热门选择，而对私有云的偏好正在下降

更新现有应用程序时采取的指导（按年份划分）

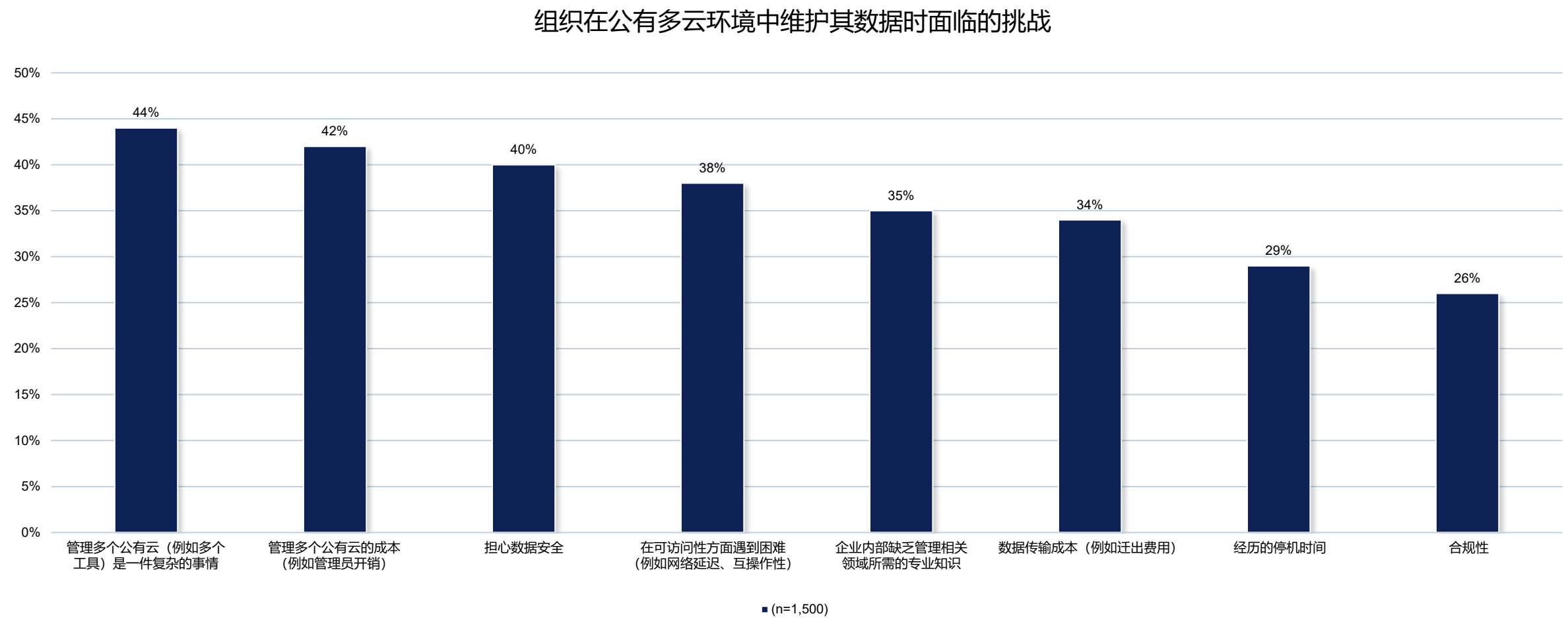


公有云仍然是部署新应用程序的热门选择，但对它的支持可能在下降

部署新应用程序时采取的指导（按年份划分）

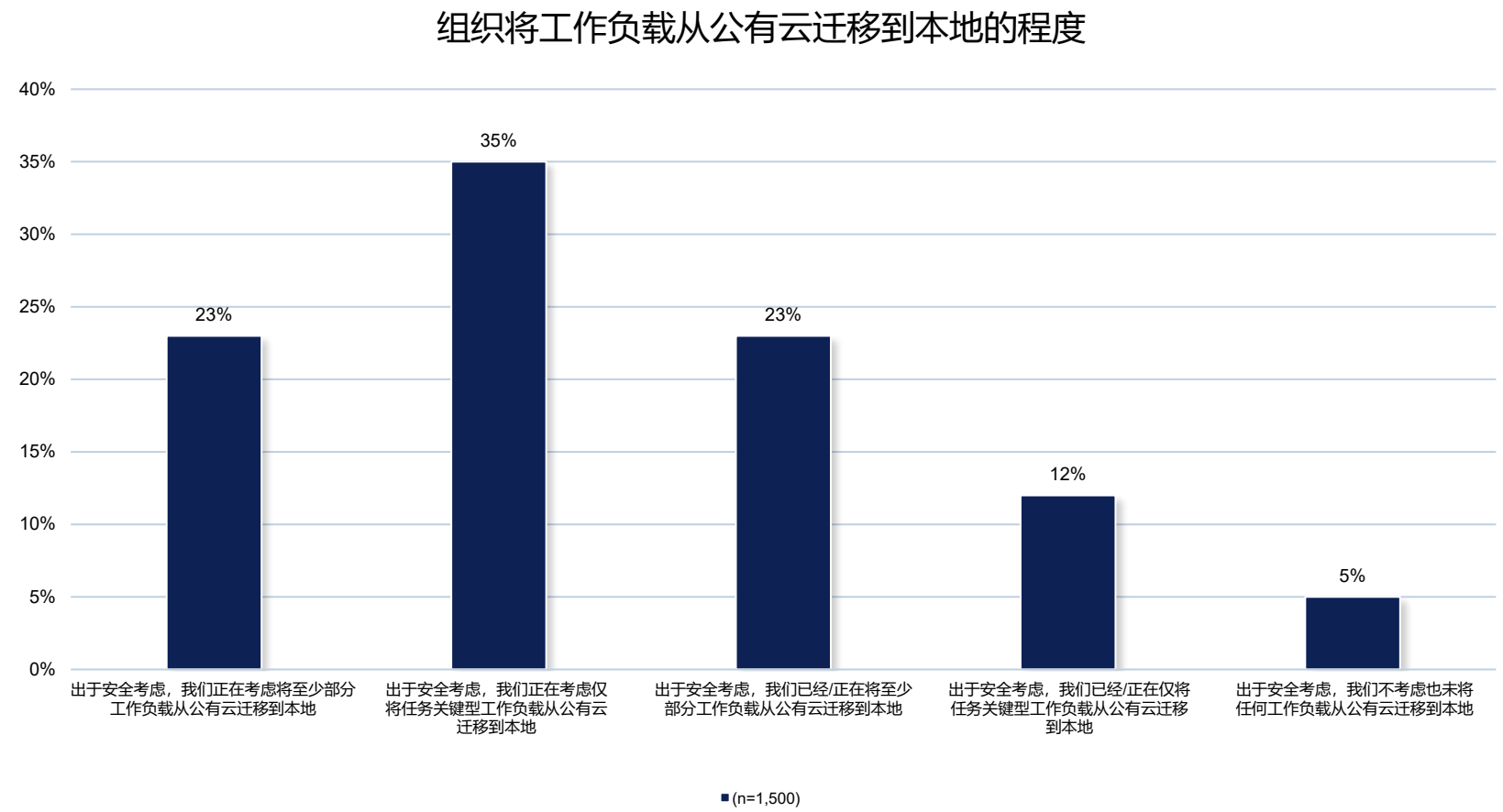


尽管公有云很受欢迎，但许多组织在维护其数据时仍面临挑战



筛选器：数据划分：地区 = 总计

出于安全顾虑，许多组织正在或正在考虑将部分本地工作负载从公有云迁移到本地

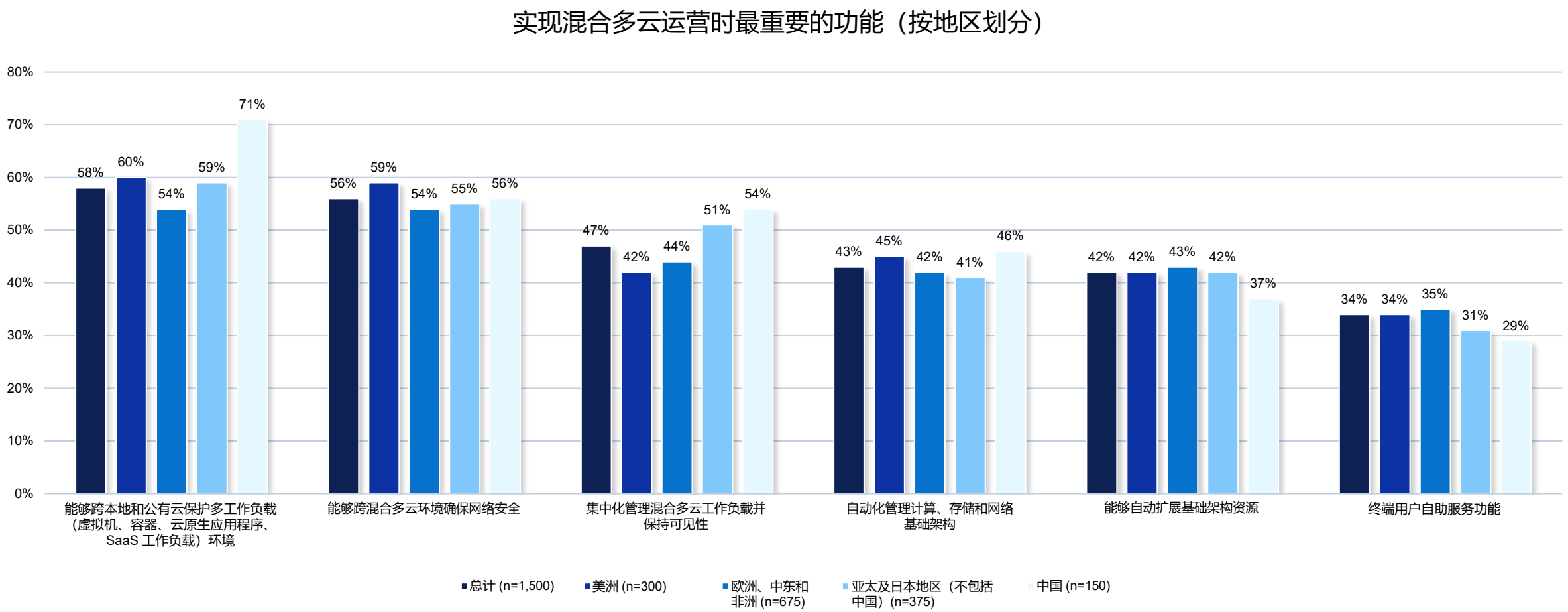


筛选器：数据划分：地区 = 总计

79%

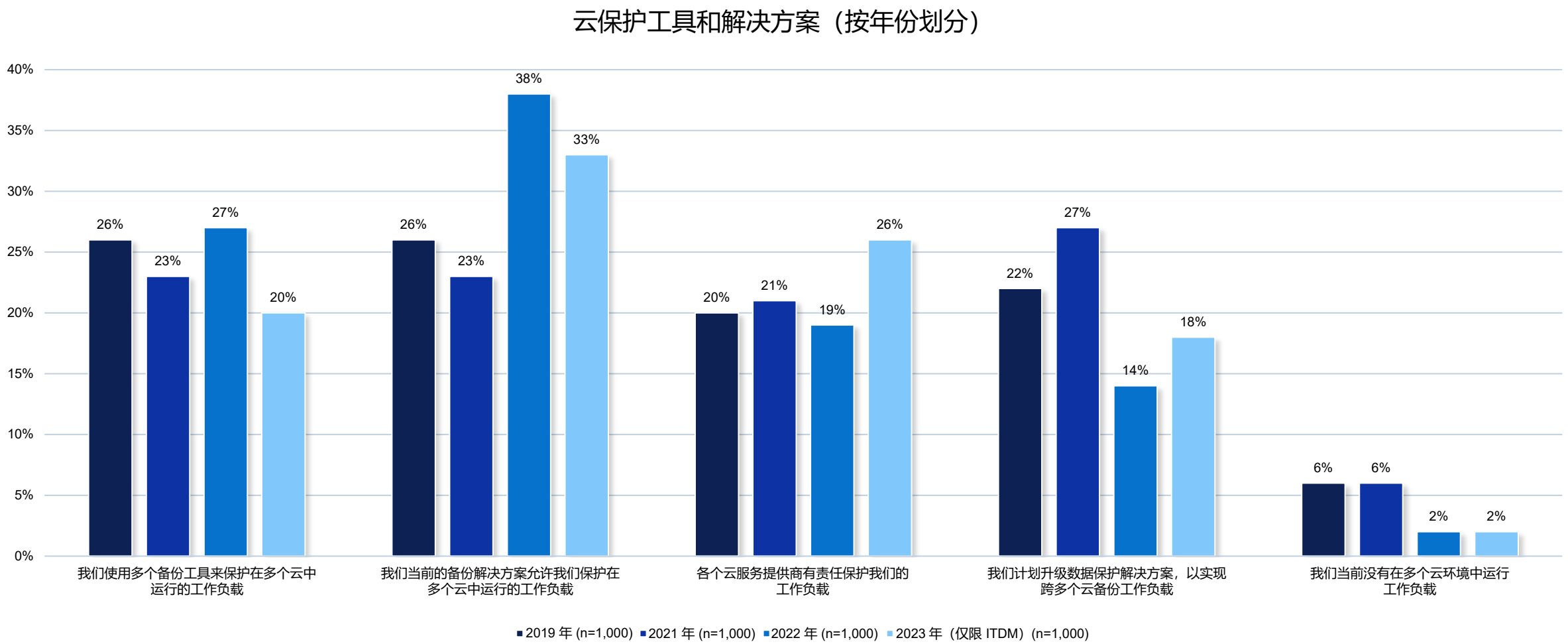
的受访者对组织跨公有云环境**保护其所有数据的能力“不是很有信心”**

随着网络相关事件的增加，以及对数据保护战略的信心降低，许多人将安全性视为实现混合多云运营时最重要的功能



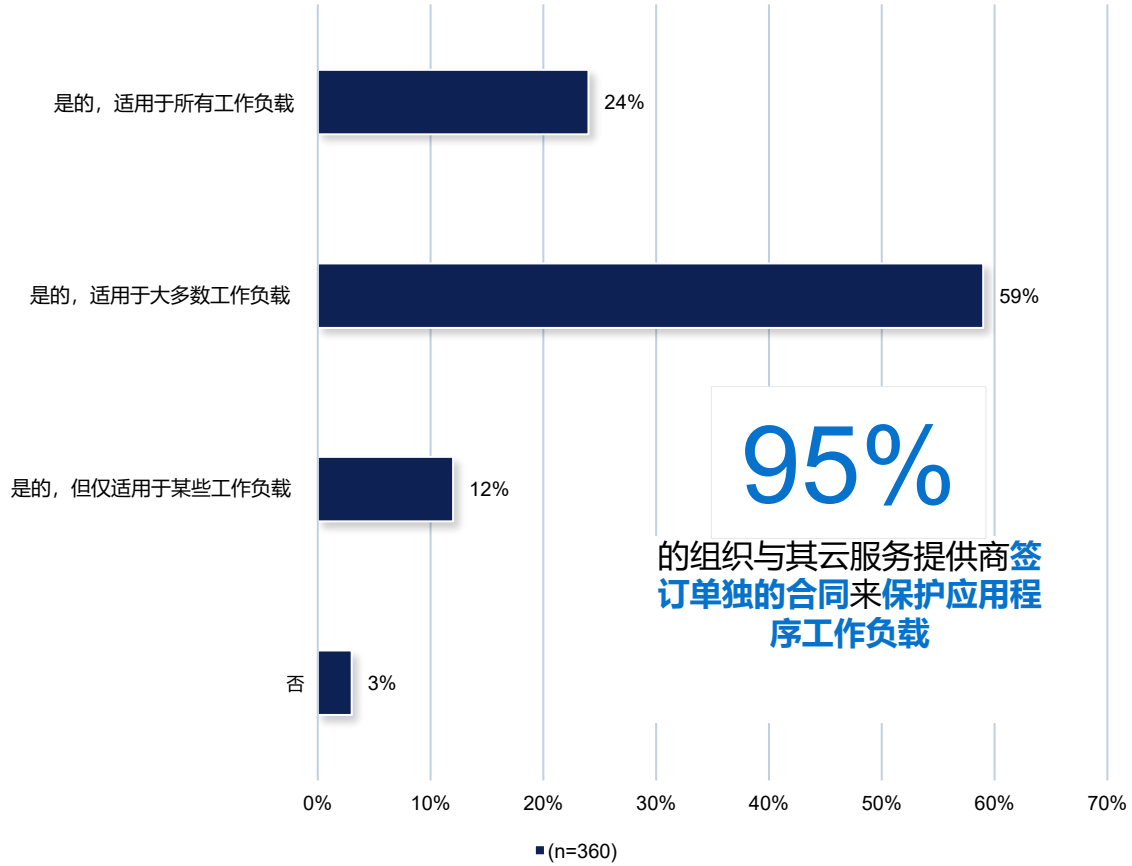
4. 保护云环境

组织当前使用各种备份工具和解决方案来保护其工作负载，但注意到需要升级



组织越来越依赖云服务提供商在不同云环境间保护其工作负载

与 CSP 签订单独的合同来保护其应用程序工作负载

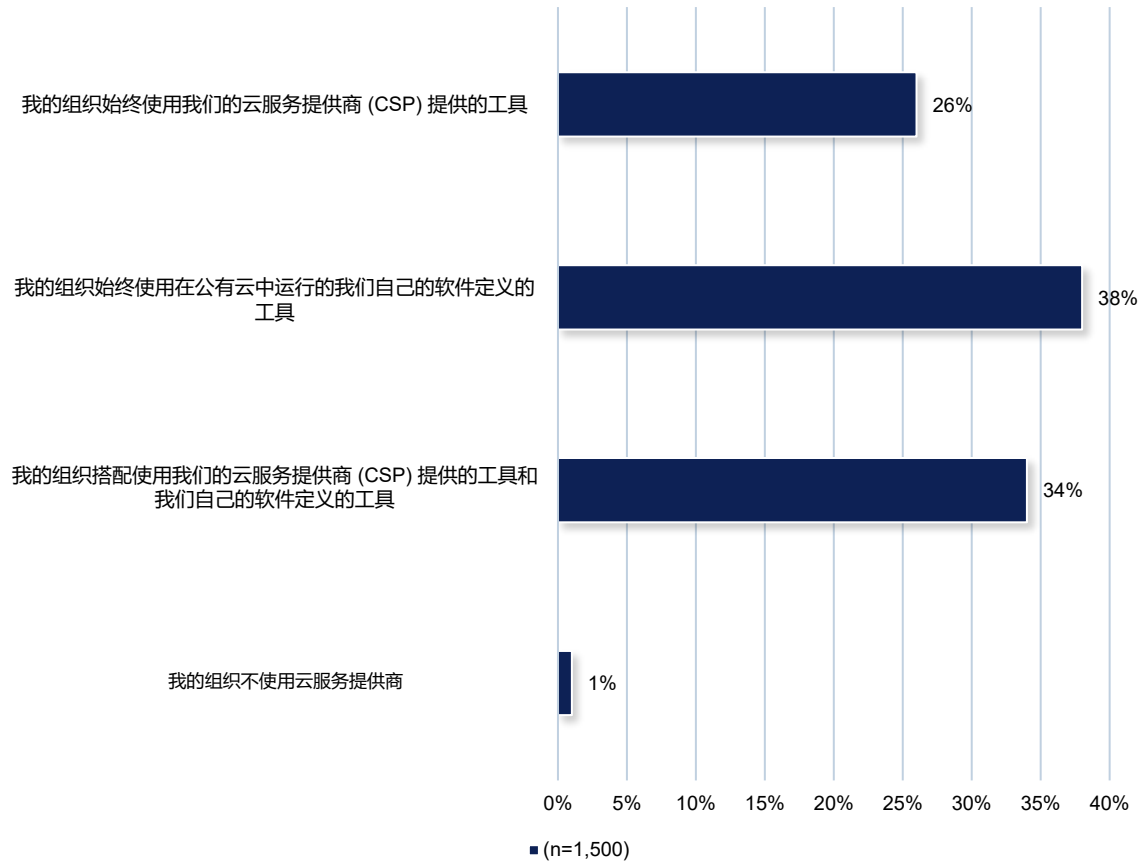


95%

的组织与其云服务提供商**签订单独的合同**来**保护应用程序工作负载**

筛选器：数据划分：地区 = 总计

云服务提供商提供的备份和恢复工具



筛选器：数据划分：地区 = 总计

主要调查结论 — 总结

数据保护风险形势

- 不仅普遍担忧其数据保护措施的担忧，而且缺乏信心 — 组织发现自身处于弱势地位
- 几乎所有组织在数据保护方面都面临着挑战，在过去 12 个月中，许多组织还因数据丢失和/或计划外系统停机而遭遇重大中断
- 在过去 12 个月中，外部安全威胁一直是导致数据丢失和/或计划外系统停机的最常见原因
- 尽管存在数据保护方面的挑战和顾虑，但很少有组织完全实施了零信任安全性

网络攻击威胁日益增多

- 在过去 12 个月中，遭遇网络攻击或事件的组织数量有所增加，致使企业平均损失达 192 万美元
- 许多组织担心他们的备份数据可能会受到勒索软件攻击的感染或损坏
- 人们对勒索软件攻击所造成的后果有一种被误导的过度自信，这进一步加剧了风险
- 尽管针对勒索软件的保险单在组织中间普遍存在，但它们有很大的局限性，使得组织在财务上很脆弱

多云的使用

- 在更新现有应用程序和部署新应用程序时，公有云仍然是热门选择，但存在对数据安全性的顾虑
- 出于安全顾虑，许多组织正在或正在考虑将部分本地工作负载从公有云迁移到本地
- 随着网络相关事件的增加，以及对数据保护战略的信心降低，许多人将安全性视为实现混合多云运营时最重要的功能

保护云环境

- 组织当前使用各种备份工具和解决方案来保护其工作负载，但认识到需要升级
- 组织越来越依赖云服务提供商在不同云环境间保护其工作负载