Google Workspace

安全拐点已至

为什么不能再依赖增量式修补

2024 年 10 月

Google 寄语

随着人们工作方式和工作地点的变化，业务环境在不断重塑，世界各地的组织都在面临快速增长的安全威胁。最近发布的 Mandiant M-Trends 报告表明，在过去的一年中，以大型政府机构和商业组织为目标、由国家资助的间谍行为和以牟利为目的的勒索软件攻击次数呈现出增长态势，各行各业的数据泄露事件也层出不穷，从电信业到娱乐业都未能幸免。

为了帮助组织更好地了解如何应对新的威胁局势，近期，我们与 Hypothesis Group 合作，委托他们开展了一次全球安全调研。我们与中型机构和大型企业组织的 2,000 多名决策者进行了交流，目的是了解他们如何保障安全、他们发现了哪些变化，以及他们希望将来采取哪些行动。

调研结果表明，未来的工作模式已然形成，新的安全风险也随之来临。但许多组织并未应势而变，而是一味加大力度实施传统策略和工具。后果就是，他们遭遇了越来越多的安全事件，并且付出了沉重代价，导致业务运营中断、客户数据受影响、组织声誉蒙损。在安全方面，维持现状已无法满足需求，是时候彻底转变，采取更有效的方法了。

企业真正需要的是更安全的产品，而不是一味地增加产品数量。我们相信，安全事件和泄露应该只是例外情况，绝非常态。我们希望借助从设计上保证安全的解决方案，让组织对自身主动防御攻击的能力更有信心。

衷心希望这份研究报告能对贵组织有所启发，也希望贵组织从此和我们建立起持续对话，讨论自身安全需求以及 Google Workspace 如何作为您的战略合作伙伴，全程助您打造更安全的工作环境。

Andy

Andy Wen
产品管理高级总监
Google Workspace 安全团队

目录

简介

当今的工作环境仍在不断变化，混合办公已成为数百万员工的常态，AI 也在不断进化。与此同时，安全威胁也快速增多且日益复杂。各类组织逐渐意识到了这些日益严重的新风险，但许多组织仍犹豫不决，未能大胆做出必要决策，来确保环境安全。

本文探究了当今业务环境的核心矛盾：部分领导者对自家策略充满信心，但屡见不鲜的严重安全事件暴露出了其认知与现实之间的重大差距。组织应做出必要的改变，而非加倍投入原有方案，这样才能弥合差距，更好地应对安全形势。

为了帮助组织更好地认清现状，并确定可以采取哪些行动来改善自身的安全状况，Google Workspace 与提供分析洞见、设计和战略服务的机构 Hypothesis Group 合作，开展了一项涉及多个方面的综合研究。这项研究包含：

- 量化研究：访问了超过 2,000 位 IT、业务和安全决策者，受访者来自美国、英国、印度和巴西的中型机构（300-999 名员工）和大型企业组织（1,000 多名员工），调查时间为 2024 年 7 月 22 日至 8 月 8 日。
- 定性访谈：在 2024 年 8 月 22 日至 26 日，访问了六位美国决策者。
- 与下列行业专家对话，探讨当前的安全趋势与未来安全状况：

John McCumber
前 NIST 联合主席及 Gartner 总监；
安全专栏作家

Joshua Scarpino 博士
TrustEngine 信息安全副总裁
Assessed Intelligence 首席执行官

Rachel Tobac
SocialProof Security首席执行官；
Women in Security and Privacy 董事会主席；CISA 技术顾问委员会志愿者

关键分析洞见

安全问题迫在眉睫：现行做法并非长久之计，而且成本高昂；组织迫切需要改变策略，这样才能抢先一步，防范不断演变的威胁。

面对快速发展的威胁形势，必须采取全新的安全防护策略，但鲜有组织进行大刀阔斧地革新。

1. **现行做法难以为继。**尽管组织表示对自身的安全状况满怀信心，但很多行为都存在风险，主管安全的领导者则表示自己的担忧与日俱增。

2. **组织深知提升安全性刻不容缓，但固守旧的解决方案无济于事。**为了增强安全性，很多领导者在实施“加法”策略（添加工具、增加投入、增加保险费）。但安全事件依然频发，且代价不菲。

3. **为了顺应未来需要，变革势在必行。**领导者明确表示希望简化安全措施，并利用 AI 来保护组织。相较于只在事后补救的组织，从根本上解决不足之处的组织表现得更好。

组织应对安全局势的策略因组织规模和所在地区而异，但大家都已经认识到：改变势在必行。

4. **中型机构（300-999 名员工）已为转型做好准备。**考虑到技术陈旧和组织的复杂性，领导者对未来极度焦虑。但大多数领导者在积极反思其安全措施，也乐于做出改变。

5. **在全球范围内，每个地区都面临不同的挑战，因此必须根据安全形势采取不同的做法。**尽管全球各地的领导者都认识到了工作环境会继续发展演变，但只有部分国家/地区的组织实施了长远且有效的安全策略，这意味着许多组织都需要重新评估自己的安全策略。

1

现行做法难以为继

尽管组织表示对自身的安全性与工作方式有信心，但实际行为依然暴露出防御方案的诸多漏洞，这让安全决策者夜不能寐。

组织充满信心，但工作方式的变化导致安全性下降

大多数组织认为自身在安全方面表现较好 - 至少从理论上来说是这样。多达 **96%** 的决策者（包括主管 IT、业务和安全的领导者）相信组织有能力保证数据、应用、设备和新兴技术（如生成式 AI）方面的安全。但他们并没有考虑到人们的实际工作方式已经发生了重大变化。

这些变化涵盖方方面面，从混合办公的日益普及，到不同新工具的引入，其中尤其值得一提的就是生成式 AI。

74%

的受访者表示，其工作方式已经发生了重大变化

> **“我们身处变革的时代，可以使用的工具不计其数。但我非常担心，因为我觉得我们没有适当的政策，而且关于如何妥善运用这些新工具，我们也并没有任何计划。”**
>
> — 某制药企业的研究总监

存在风险的工具和行为非常普遍

大多数决策者表示许多做法会给组织带来风险：

- 只有 **56%** 的受访者表示他们遵循了 IT 政策
- 在组织内使用的工具中，有 **19%** 是未经许可的（即未经过组织的审查和批准）
- 近半数 (**44%**) 受访者相信，未经许可的工具“完全安全”
- 约三分之二 (**63%**) 的受访者表示，他们每周都会使用未经许可的生成式 AI 工具
- 近半数 (**48%**) 的决策者信任未经许可的生成式 AI 工具

组织言行之间的这种差距突显出其当前安全状况蕴含的风险。此外，使用影子 IT 服务的做法十分普遍，而且保护难度极大，这也增加了发生突发事件和违规风险的概率。

> **“组织有时候可能意识不到新技术演变带来的风险，这就给主管安全的领导者带来了挑战，因为他们总是扮演着补救者的角色。”**
>
> **— Joshua Scarpino 博士**
> Assessed.Intelligence 首席执行官

主管安全的领导者变得更加焦虑

安全决策者 (SDM) 并非对这些风险毫无察觉。

63%

的受访者相信，相较于过去，其组织的技术环境安全性有所下降

四分之一的工具被视为存在风险

> “我猜测“人们认为技术环境的安全性有所下降”与缺乏掌控感及相关知识有关。对我们所有人来说，了解所用的全部工具、其使用位置、应用方式以及有心之人如何通过多种方式利用它们对我们行不利之举，都是十分艰难的事情。”

— **John McCumber**

前 NIST 联合主席及 Gartner 总监；安全专栏作家

这种存在风险的行为让人焦虑不安，**93%** 的安全决策者在为安全事件而担忧。导致焦虑的原因很明显。虽然安全决策者最担忧的是漏洞和外部攻击，无论是生成式 AI 攻击还是数据泄露，但他们也担心用户有意或无意的疏忽。

> **“决策者们告诉我，他们忧心忡忡、夜不能寐。技术工具并不完美，需要大量的人工监督，这让决策者倍感压力。”**

— **Rachel Tobac**
SocialProof Security 首席执行官

93%
的安全决策者担心发生安全事件

最担心的攻击/漏洞

生成式 AI 攻击	**31%**
数据泄露	**30%**
网络敲诈	**26%**

最担心的最终用户问题

未经授权的访问	**24%**
员工过失	**20%**
凭据遭盗用	**17%**

2

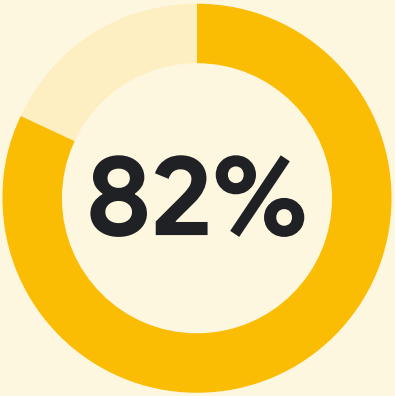
组织深知提升安全性刻不容缓，但固守旧的解决方案无济于事

对增强型安全措施的需求空前迫切。安全决策者已经敏锐地认识到，他们当前的策略有不足之处，也认同有必要作出广泛的改进。但事实证明，许多组织采用的方法不够周全，往往适得其反。

对增强型安全措施的需求明确

82% 的安全决策者表示，他们需要改进安全措施。**超过半数**的安全决策者表示，现代工作环境的复杂性削弱了他们保障组织安全的能力。**59%** 的安全决策者承认，依靠陈旧过时的技术导致他们对未来安全需求的准备不足。

> **“多年来，我们叠加了多种安全解决方案，其中有些工具相当陈旧，需要用新工具取代，至少要重新进行评估。”**
>
> — 某媒体与娱乐业组织的 IT 副总裁



的安全决策者表示，其组织需要改进安全措施

增量式改变不足以满足需求

尽管约半数的安全决策者表示，其网络安全策略在过去两年间经历了重大变化，但那些变化往往属于增量式改变，而非彻底革新。事实上，大多数组织似乎都只是在现有方案的基础上修修补补。

过去两年间的主要安全措施变化

提高网络安全保险费	**37%**
增加网络安全方面的开支	**35%**
升级许可证	**34%**
增加新的网络安全提供商	**31%**

这些调整或许能起到一定的作用，但都没有脱离现有做法，并没有从根本上改变策略。

> “组织会把钱砸在原有的技术上，一层又一层地叠加功能。我从同事和客户的口中都听到过这样的话：‘我们投入了大量资金，但并不解决问题。’他们会把钱花在一些非常昂贵的平台上，但又不会给团队部署密码管理工具。这就好比是花大价钱装了防弹窗，但房门大敞四开。”

— **Rachel Tobac**
SocialProof Security 首席执行官

62%
的安全决策者表示，在需要新功能时，他们会在旧工具的基础上进行扩展（而非替换掉旧工具）

10
种安全工具（大型企业组织平均使用的安全工具数量）

61%
的组织增加了安全工具数量（与两年前相比）

27%
的安全工具是重复的

过犹不及，必须采用统合程度更高的策略

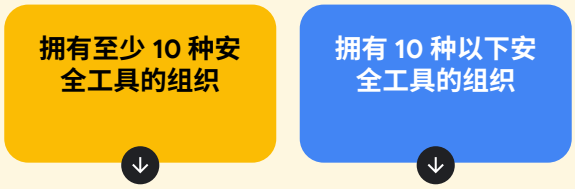
超过三分之二的组织比以往投入更多的时间和资金来保护其环境，但代价高昂的突发事件依然层出不穷。

相比之下，所用工具数量较少的组织表现要更胜一筹。根据受访组织分享的数据，所用安全工具超过 10 种的组织遭遇安全事件的频率更高，付出的代价也更沉重。

81%
的组织每年至少遭遇一起突发事件

8 **起突发事件（平均每年报告的数量）**

488 万美元
2024 年单次数据泄露造成的总体代价，全球平均值[1]



一年中遭遇的安全事件数量

14 对比 6

一年中因安全事件花费 25 万美元以上

34% 对比 19%

> “如果每项安全问题都聘用专门的供应商处理，那么不但管理起来难度极大，而且性价比也低。所以我们需要整合精简。我们目前的供应商过多，不是长久之计。”
>
> — 某媒体与娱乐业组织的 IT 副总裁

1. IBM – Cost of a Data Breach Report 2024 (2024 年数据泄露损失报告)

3

唯有变革才能适应未来

我们的研究表明，安全决策者愿意通过新的方式提升安全性，积极寻求新策略与新技术的安全决策者已经取得了优势。

对变革的渴望

当前大环境促使组织换种方式去思考其安全战略。

78%

的受访者在根据当前网络安全的大环境，重新审视其组织的安全策略

73%

的受访者乐于接受新的安全策略，而且不考虑成本

决策者对精简的安全解决方案越来越感兴趣，**65%** 的决策者表示有意采用统一安全系统。他们认同，在一个界面内整合不同数据源的平台能带来切实可见的好处，包括精简流程、增强运维，消除管理多种工具的负担以及节省时间。

生成式 AI 也赢得了更多关注，**59%** 的安全决策者将其视为关键工具，希望用它来抵御不断发展演变的威胁。

> **“AI 给安全领域带来的最大影响莫过于它让使用者能够响应事件、利用现有工具，并合理调度这些工具去响应事件、生成报告并执行清理。”**

— John McCumber

前 NIST 联合主席及 Gartner 总监；安全专栏作家

59%

的安全决策者将生成式 AI 视为保障数据安全的关键工具

采用生成式 AI 的主要原因

加强数据隐私保护	**43%**
增强威胁情报功能	**37%**
改进安全运维	**36%**
防范威胁	**33%**

实施变革的好处

虽然受访者对新方法表现出了浓厚的兴趣，但只有 **38%** 的安全决策者在积极主动地替换陈旧过时的工具，另外 **62%** 的安全决策者仍然在完善现有的工具。

替换掉陈旧工具的安全决策者（相较于完善现有工具的安全决策者）

…

↓

每年报告的**安全事件数量少 20%**

↓

使用的安全工具数量与 2 年前相比，更可能**相同或更少**

（44% 对比 36%）

↓

表示为保护环境安全而**花费的时间比过去更少**

（33% 对比 28%）

> “团队需要评估其已经购买的工具，了解他们已经拥有哪些功能，避免反复购买功能相近的保护工具。通过了解已经具备了哪些功能，以及哪些方面需要保护，组织即可更好地了解其工具，最终减少安全事件和安全问题。”

— **Rachel Tobac**

SocialProof Security 首席执行官

4

中型机构已为变革做好准备

中型机构（300-999 名员工）未能充分发挥安全潜力，而且他们对此了然于心。面对复杂的现代工作环境，他们的顾虑远超过大型企业组织（超过 1,000 名员工）。

中型机构决策者也表示越来越担心当前的技术环境。生成式 AI 在工作中的迅速应用加重了他们的顾虑。

73%

的受访者表示，生成式 AI 使用的增加导致其组织内的安全事件数量增加

（相比之下，有 58% 的大型企业组织报告了相同的情况）

他们面临的难题是什么

	相较于大型企业组织
71% 的受访者表示，旧技术导致他们对未来的准备不足	高 23 个百分点
63% 的受访者表示，复杂的工作方式导致安全性下降	高 11 个百分点
73% 的受访者表示，生成式 AI 的使用导致安全事件数量增加	高 15 个百分点

他们的感受如何

	相较于大型企业组织
63% 的受访者认为潜在安全事件让他们感觉很焦虑	高 13 个百分点
63% 的受访者表示，相较于过去，技术环境的安全性变差了	高 12 个百分点
36% 的受访者表示，安全威胁导致其安全团队不堪重负	高 16 个百分点

乐于接纳新方法

82% 的中型机构安全决策者表示，其组织在积极重新审视自身的安全措施。对于云原生解决方案的好处，中型机构决策者展现出越来越强的信心，**81%** 的中型机构安全决策者表示，云原生应用比传统桌面应用更加安全。这表明，中型机构不仅注意到了改变的必要，也准备好了采纳更具创新性的解决方案。

> “中型机构情况特殊，因为他们在为快速迈向更大的市场做准备，也在扩大规模。他们需要在这个阶段打好基础，否则，他们就会远远落后，而他们的顾虑也会变为现实。”

— **Joshua Scarpino 博士**
Assessed.Intelligence 首席执行官

82%

的中型机构安全决策者在积极重新审视其自身的安全方法

5

全球不同地区的组织针对安全形势采取了不同的做法

决策者普遍承认，在过去一年间，他们的工作方式发生了巨大变化，但不同国家/地区的组织应对这些变化（尤其是安全方面）的方式存在很大差异。

所有地区的决策者都表示，其工作环境相较于一年前发生了转变，每个市场的安全决策者都在重新考量自身的安全策略。

“与 12 个月之前相比，我们的工作方式发生了极大的变化/发生了一定程度的变化”

印度	85%
巴西	74%
英国	73%
美国	62%

“我们组织正在重新审视自身的安全策略”

印度	83%
巴西	76%
英国	82%
美国	71%

印度

因复杂性而不堪重负，但渴望变革

由于极高的复杂性和工具的激增，印度的安全局势格外引人注意。印度的组织非常渴望变革，也非常愿意提高安全性并探索新方案。印度无疑处于拐点，而印度决策者认识到了必须采用更精简、更高效的安全战略。

安全概况	相较于全球平均值
平均使用 **35 种工具**（例如：产品、服务、应用）	多 11 种
平均使用 **19 种安全工具**	多 9 种
67% 的受访者表示，工作方式的变化导致安全性下降	高 10 个百分点

渴望变革	
82% 的受访者认为，其组织的安全性需要改进	高 8 个百分点
81% 的受访者乐于探索新的安全方法，而且不考虑成本	高 8 个百分点

巴西

存在严重的焦虑心态，但对具体威胁的关注不足

对于安全事件及其后果，巴西决策者表现出了更严重的焦虑心态，但他们没有真正关注安全问题的具体原因。由此可以看出，他们担心的是安全事件造成的后果，而不是害怕造成突发事件的漏洞。巴西组织表明了对于变革的渴望，是对部署生成式 AI 兴趣最浓厚的地区之一（71%，全球平均值为 62%）。

对安全的焦虑感	相较于全球平均值
41% 的受访者一直在为安全事件担忧	高 19 个百分点
42% 的受访者担心（突发事件造成）信任度下降	高 8 个百分点
37% 的受访者担心（突发事件造成）客户流失	高 7 个百分点
39% 的受访者担心（突发事件造成）品牌声誉损失	高 5 个百分点

对特定问题的顾虑较少	
40% 的受访者表示，旧技术导致他们对未来的准备不足	低 19 个百分点
48% 的受访者表示，生成式 AI 的使用导致突发事件数量增加	低 17 个百分点
44% 的受访者表示，复杂的工作方式导致安全性下降	低 13 个百分点

英国

担心新兴技术带来的威胁，但行动迟缓

英国决策者非常担心新兴技术对安全的影响，尤其是在旧系统和生成式 AI 威胁方面。但英国组织在实施政策来缓解这些风险方面一直行动迟缓，英国决策者在这方面表现得比较消极。尽管存在这些挑战，英国组织采用新安全方法的意愿不强，他们更愿意相信安全事故不可避免。

对技术的担忧

	相较于全球平均值
75% 的受访者表示，旧技术导致他们对未来的准备不足	高 16 个百分点
77% 的受访者表示，生成式 AI 的使用导致突发事件数量增加	高 12 个百分点

尽管面临挑战，但仍然不愿实施变革

43% 的受访者表示，其安全团队因安全威胁而不堪重负/精疲力竭	高 15 个百分点
44% 的受访者认为安全事故不可避免	高 14 个百分点
27% 的受访者针对生成式 AI 制定了专门的安全政策	低 14 个百分点
60% 的受访者乐于探索新的安全方法，而且不考虑成本	低 13 个百分点

美国

过度自信可能会掩盖暗藏的风险

美国决策者对其安全状况展现出高度的信心，他们不太担心数据泄露，特别是与生成式 AI 相关的数据泄露。保持乐观的心态固然是好的，但这也引发了问题，即美国组织低估了快速发展的威胁形势，尤其是考虑到美国的数据泄露代价居全球之冠。如果不去明确关注新兴风险，过度自信可能会导致一些组织容易在未来遭受攻击。

对安全环境的信心

	相较于全球平均值
10% 的受访者总是为安全事件而担忧	低 12 个百分点
55% 的受访者表示，生成式 AI 的使用导致突发事件数量增加	低 10 个百分点
52% 的受访者表示，相较于过去，技术环境的安全性变差	低 4 个百分点

数据泄露代价最高

2024 年，一次数据泄露造成的损失平均为 **936 万美元**[1]	高 500 万美元

1. IBM – Cost of a Data Breach Report 2024 (2024 年数据泄露损失报告)

要点总结

“让整个组织了解安全风险至关重要，高管层往往并不了解安全方案的真正价值。但安全专业人员必须能用简单明了的方式给出解释，清楚阐明“风险与解决方案”。

Joshua Scarpino 博士
Assessed.Intelligence 首席执行官

❶ 安全与业务领导者需要携手努力

安全决策者和高级管理者需要相互配合、坦诚沟通，实施有力的风险管理流程，从而制定成功的安全战略。对于安全决策者而言，获得利益相关方的认可并建立更深度的合作关系，有助于推动安全工作高效开展，避免安全问题变成内部的矛盾点。

❷ 不应等到发生数据泄露才去实施转型

危机事件（例如数据泄露）就像强效催化剂，能帮助安全决策者获得批准，更快地实施必要的安全措施。但勒索软件等网络攻击可以在一夜时间让几乎任何企业的运营停摆，因此立即主动实施必要变革愈加重要。对于大多数企业来说，问题不在于安全事件会不会发生，而是何时发生。

❸ 专注于攻击的发起点

根据 Mandiant 最新的 M-Trends 报告，2023 年，72% 的成功入侵事件都是通过盗用身份（例如钓鱼式攻击或盗用凭据）或软件漏洞发起的。因此，在这些方面略微做出改进就有可能帮助组织避免巨大损失。例如，可以使用 Google Workspace 这样的产品。Google Workspace 提供的双重身份验证就可以防范钓鱼式攻击，还可以自动拦截超过 99.9% 的垃圾信息、钓鱼式攻击企图和恶意软件，确保它们不会接触到您的用户，而且它没有需要修补或更新的桌面客户端应用或本地部署。

“人们会想：‘我得买这款庞大又昂贵的程序或工具。只有花大价钱买到的工具才有效。’但实际上，他们能实施的一些最重要的变革，是制定机构政策和调整企业文化。”

Rachel Tobac

SocialProof Security 首席执行官

“AI 将整合到安全工具中，加强我们应对突发事件和威胁的能力。它将会带来一些有深远影响的功能。我认为，它的潜力仍未完全发挥，未来还有太多可能。”

John McCumber

前 NIST 联合主席及 Gartner 总监；安全专栏作家

4 可以分步逐渐实施变革

一次性对整个旧软件生态系统进行现代化改造可能令人望而却步，但逐步改变可以对安全防护带来巨大影响，而且能把对最终用户的影响降到最低。例如，通过部署 Chrome 企业版，您可以为用户提供安全的浏览体验。这款已经声名卓著、广受喜爱的浏览器具备众多安全功能，例如内置的钓鱼式攻击和恶意软件防护、不需要借助 VPN 的零信任访问及数据保护控制措施。

5 生成式 AI 可能会增加风险，但也能加强保护

在选择生成式 AI 工具时，务必使用安全且符合业界标准的工具（例如 Gemini），以降低数据丢失的风险。生成式 AI 还能帮助组织抵御新兴威胁。例如，Gmail 中的 AI 防御机制就已经在使用大语言模型 (LLM)，来更好地防御垃圾邮件和钓鱼式攻击。事实上，借助 LLM 的力量，Gmail 中拦截的垃圾邮件数量增加了 20%。如今，Gmail 每天可以评估的用户报告垃圾邮件数量是以往的 1,000 倍。对于数十亿 Gmail 用户而言，这是 AI 技术为其生活品质带来的重要提升。

研究目标

01
了解当前安全形势（组织各自的首要任务、心态、顾虑、挑战）

02
评估安全和技术对组织的影响，特别是与生成式 AI 的兴起有关的方面

03
探索未来的安全策略，了解有哪些趋势正在涌现，探讨组织未来的投资计划

调研方法

量化研究

于 2024 年 7 月 22 日至 8 月 8 日开展了一次在线问卷调查（填写问卷需要大约 20 分钟），共有来自美国、英国、巴西和印度的 2,025 人回复。

筛选出的回复者符合以下条件：

- 供职于员工人数超过 300 人的组织（涵盖各种规模的组织），并且符合以下两项条件之一：
  - 负责组织或团队的技术/效率提升产品的业务或 IT 决策者
  - 负责组织安全产品的安全决策者
- 各种行业，包括受监管和不受监管的行业

地区	(n=)
美国	501
英国	523
巴西	501
印度	500
组织规模	
中型机构（300-999 名员工）	834
大型企业（超过 1,000 名员工）	1,191
角色	
IT 决策者	673
业务决策者	762
安全决策者	590
总计	2,025

深度访谈

2024 年 8 月 22 日至 26 日，在美国开展了六 (6) 次长达 1 小时的线上深度访谈。参与者均为员工人数在 300 人以上的组织的“首席”级高管及比“首席”级高管低一级的高管（包括 IT 决策者、业务决策者和安全决策者）。

专家访谈

在项目的关键节点，我们咨询了三位安全专家，请他们分享真知灼见和专业知识，并交流想法。这三位安全专家分别是 John McCumber、Joshua Scarpino 博士和 Rachel Tobac。

研究及设计机构 hypothesis