Enterprise Strategy Group | Getting to the bigger truth.™

一往无前：GitOps与安全左移

可扩展且以开发者为中心的供应链安全解决方案

Melinda Marks，ESG高级分析师

2022年8月

研究目标

随着企业开始采用现代软件开发流程，开发人员可以通过将应用部署到云端而快速开发和发布应用。这给安全团队带来了挑战，要求他们必须跟上持续集成/持续部署 (CI/CD) 周期及其动态组件的增长和速度。

虽然业界一直在讨论通过安全左移来帮助解决问题，实现安全能力的扩展和和应用程序的快速开发，但企业在将其付诸实践时面临着挑战。大多数云原生安全事件都是由不当配置引起的，这给安全团队带来了很大的压力，迫使他们寻找将安全性纳入开发流程的方法，以便在部署之前发现并修复编码问题。企业还需要聚焦于寻找与开发团队更好的协作方式，从而快速修复检测到的任何安全问题。为了洞察这些趋势，ESG对来自北美（美国和加拿大）中型企业（100至999名员工）和大企业（1,000名或更多员工）中负责评估、购买和使用以开发者为中心的安全产品的350名IT (30%) 和网络安全 (40%) 决策者以及应用开发人员 (30%) 进行了调研。

本研究旨在：

确定企业将安全纳入开发者工作流的程度。

洞察哪些类型的解决方案能够最有效地保护软件，同时又不会减慢开发流程。

了解企业在速度更快的云原生开发生命周期中面临的挑战。

评估买家对供应商解决方案的偏好、解决方案的部署方式、以及这些解决方案如何能够减少团队的工作量。

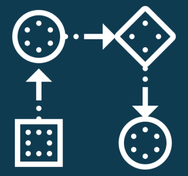
Back to Contents

目录

点击查看

4.

现代应用开发提升了速度，也加剧了安全风险



9.

安全需要纳入开发流程

13.

云原生网络安全威胁形势越来越严峻

17.

安全必须在不中断运行的情况下融入到开发流程中

21.

企业已经开始将监控和安全测试纳入开发流程，以降低风险

24.

企业已经开始在开发流程安全方面投资

现代应用开发提升了速度，也加剧了安全风险

开源软件 (OSS)日益普及

受访者认识到，OSS组件在应用开发中的使用日益广泛。事实上，80%的受访企业指出，他们在编写云原生应用时使用了开源软件。开发者通过在应用开发中使用现成的开源代码来节省时间，从而能够腾出更多时间为软件的独特功能构建定制代码；但他们必须确保这种做法不会引入安全风险，这一点非常重要。鉴于开源软件是由强大的云原生开发社区以及共享和贡献代码的供应商提供的，因此，OSS在软件代码成分中占比很高也就不足为奇了。

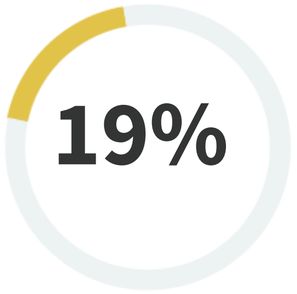
8 IN 10

80%的受访企业指出，**他们在编写云原生应用时使用了开源软件。**

» 开源软件在云原生应用中的使用情况。

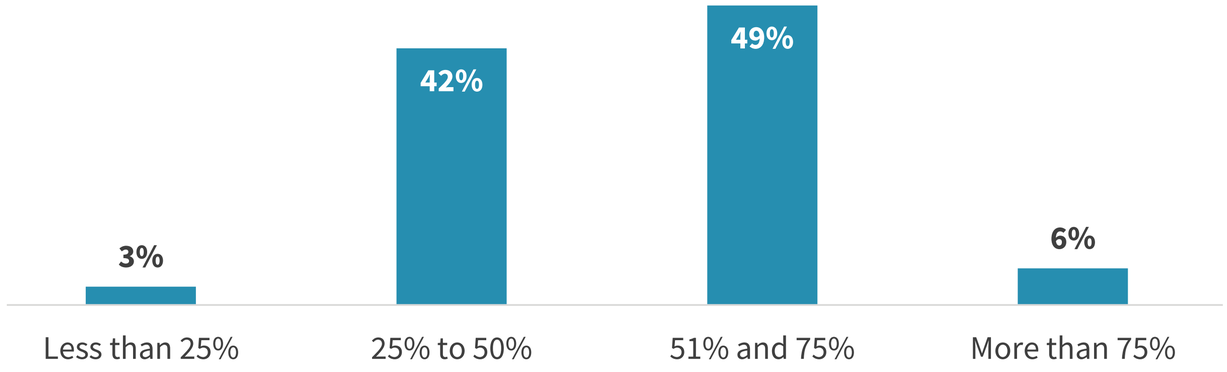
我们目前正在使用开源软件

我们计划在未来12个月内使用开源软件



另有1%的受访者对使用开源软件**感兴趣**。

» OSS在代码组成中的占比。



返回目录

使用开源软件的主要安全隐患

虽然使用开源软件（OSS）可以节省开发人员的时间，但企业也很担心其安全隐患。黑客热衷于寻找常用的开源软件（OSS）的漏洞，因为一旦找到它们的弱点，攻击者便可以对使用它们的任何公司发动攻击。

因此，企业寻找各种办法来确保全面了解其使用的开源组件（OSS），并能够在发现漏洞时快速做出响应。

> 企业寻找各种办法来全面了解其OSS组件，**并能够在发现漏洞时快速做出响应。**”
>
> *- Melinda Marks，ESG高级分析师*

» 开源软件的挑战和担忧

54%
拥有高比例的开源应用代码

41%
成为黑客攻击大众化/常用开源软件的受害者

40%
信任代码来源

39%
识别出代码中的漏洞

39%
了解代码组成并生成软件材料清单

39%
迅速使用新发布的补丁

38%
快速修复漏洞

返回目录

基础架构即代码的使用量日益增加

基础架构即代码 (IaC) 使开发人员能够配置自己的基础架构，不必等待IT或运营团队为其进行配置。他们通常使用模板中的代码，以声明方式来编写所需的云基础架构，用于管理网络、计算服务和存储等资源。超过三分之二 (69%) 的受访企业目前正在使用IaC模板来配置云基础架构，另有27%的受访企业计划在未来12个月内采取这种做法。虽然目前的使用率不高，但61%的受访企业预计，他们会在未来两年内对超过一半的云原生应用使用IaC模板。

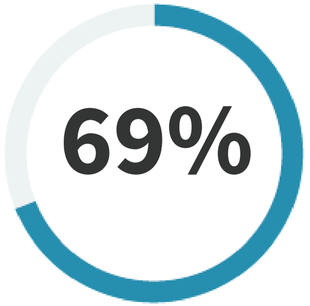
未来两年内，

61%

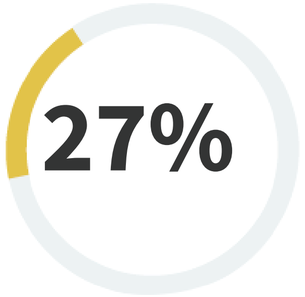
的受访企业预计他们会对**超过一半的云原生应用**使用IaC模板。

» IaC模板的使用情况

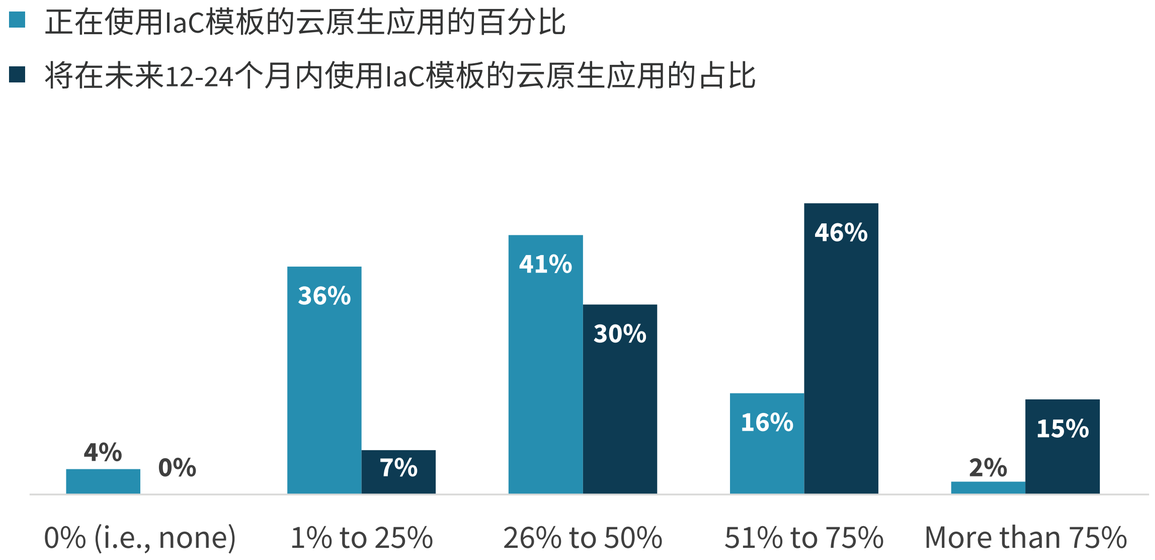
我们目前正在使用IaC模板来配置云基础架构



我们计划在未来12个月内使用IaC模板



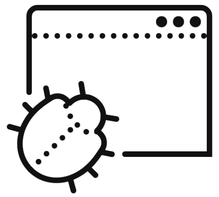
另有4%的受访企业对使用IaC模板**感兴趣**



返回目录

与IaC使用相关的不当配置和突发事件

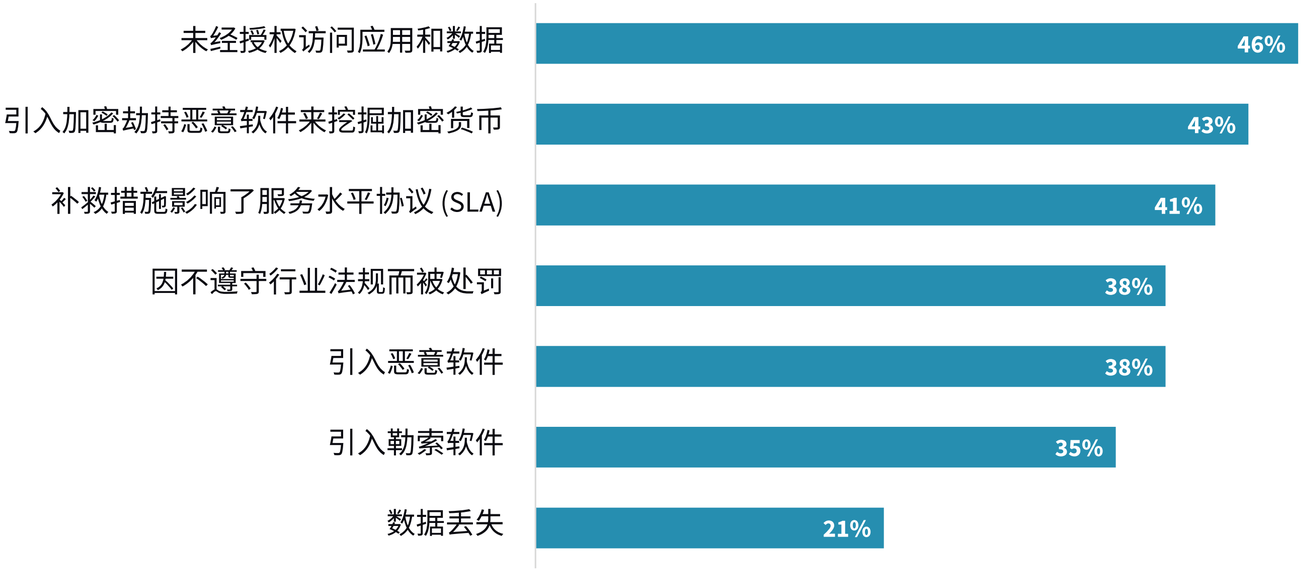
随着开发人员越来越多地使用IaC，出错的几率也越来越大。错误配置可能导致无法检测到编码问题，但由于编码控制着资源访问，因此，错误配置可能会带来严重后果。大多数（83%）的受访者表示，使用IaC导致不当配置有所增加，给他们带来了一系列不良后果，包括未经授权访问应用和数据、引入恶意软件、影响服务水平和数据丢失等。



83%

的受访者表示，他们因**使用IaC而导致不当配置**有所增加。

» IaC模板导致不当配置增加而产生的影响



返回目录

安全需要融入开发流程

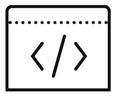
将安全纳入开发流程

企业正在努力将安全流程纳入到软件开发中，从而不会因为发布周期的缩短而面临无法控制的安全风险，例如敏捷软件开发流程、安全即代码 (SaC) 和GitOps中的网络安全用户故事。尽管只有59%的受访者表示他们已经实施了SaC，但受访者认为，这种方法在未来两年内将成为一种高度流行的网络安全方法。尽管大多数受访者都认可采用SaC带来的效果，但鉴于其成熟度和持续的网络安全技能短缺，企业仍然无法确定其如何实施，或者说如何跨项目和团队进行实施。

» 当前用于保护云原生应用的安全流程

定义敏捷软件开发过程中的网络安全用户故事

63%



安全即代码

59%

GitOps恢复到以前的配置

55%

» 受访者对安全即代码的看法

未来24个月内，安全即代码将成为一种高度相关的网络安全方法

72%

我的网络安全团队缺乏足够数量的安全分析人员具备实施“安全即代码”的能力

56%

安全即代码目前还不够成熟，无法纳入我们的网络安全计划

51%

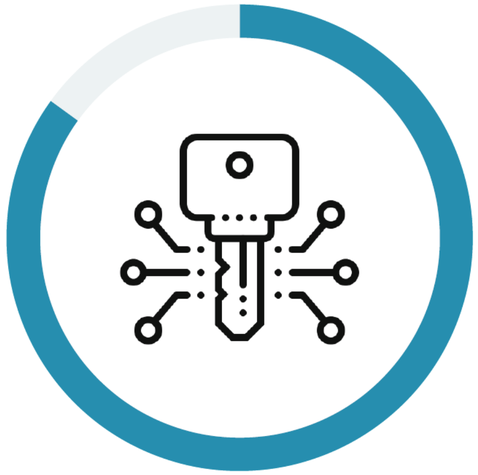
返回目录

Git存储库中的机密信息扫描

开发人员通常将机密信息（即包含密码、API密钥和令牌的凭据）硬编码到代码中，以便于使用。据调查，85%的企业已经开始通过扫描Git存储库来查找并找到了大量的机密。扫描显然是一种不错的做法，但不能保证机密信息得到保护。风险的降低取决于安全团队能否确保采取补救措施。事实上，虽然大多数企业都会通过扫描Git存储库来查找机密信息，但近三分之一 (31%) 的受访者表示，这个源代码存储库发生过机密信息窃取事件。

31%

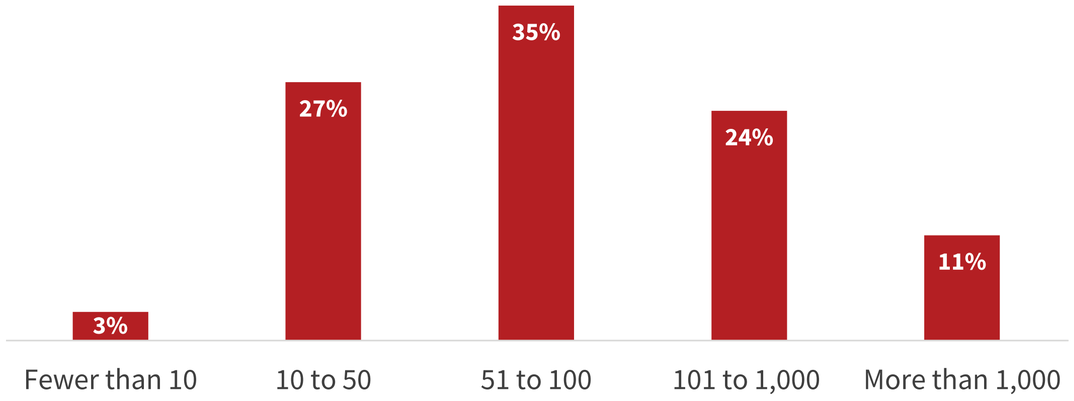
的受访企业表示，这个源代码存储库在过去12个月内发生过机密信息窃取事件。



我们目前通过扫描Git存储库来发现有风险的机密信息

85%

» 通过Git存储库扫描获得的机密信息估值



返回目录

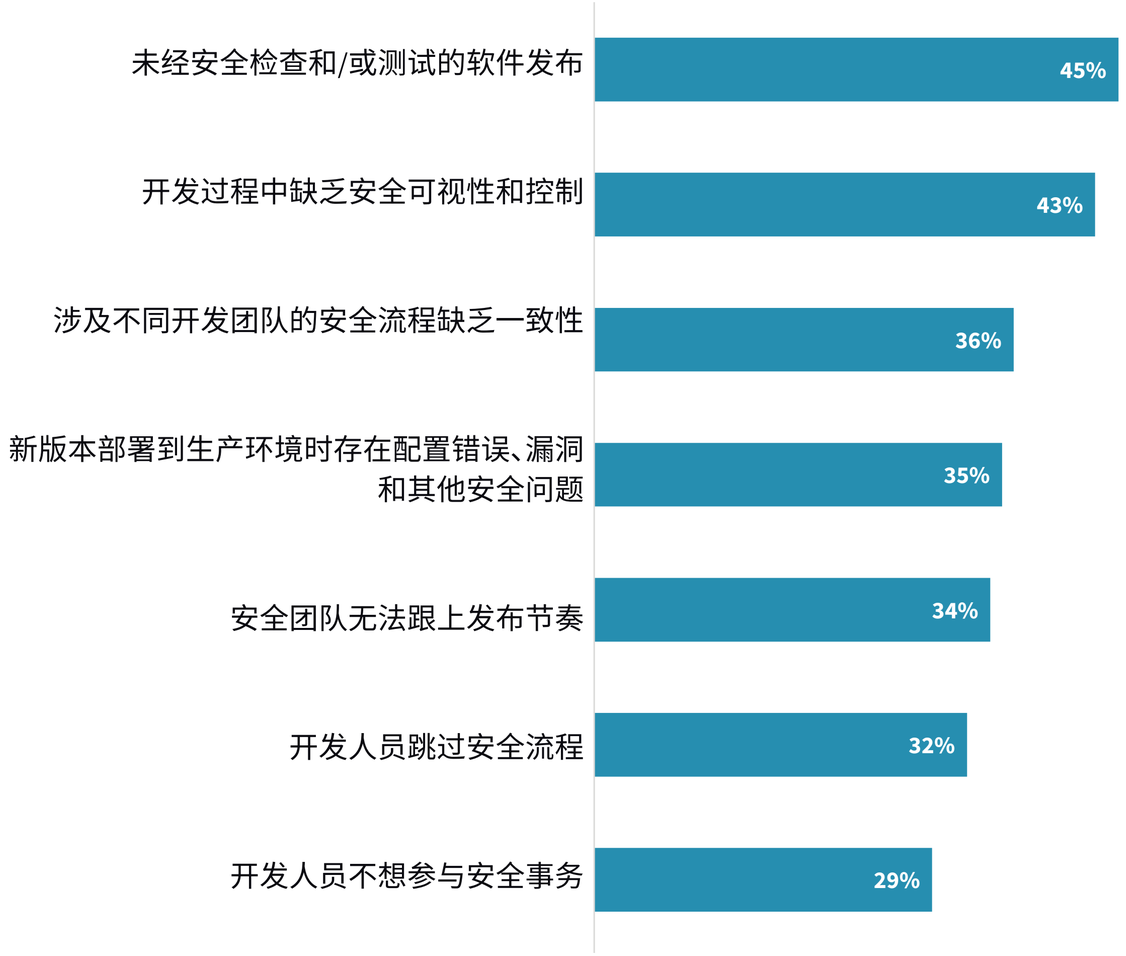
加快开发周期的同时落地应用安全实践的挑战

随着安全团队努力将安全纳入开发流程，为了能够与CI/CD的发布速度和数量保持同步，他们需要应对诸多挑战。据调查，最严峻的挑战是未经安全检查和测试的软件发布（45%）以及开发过程中缺乏安全可视性和控制（43%）。此外，近三分之二的受访企业拥有超过50个Git存储库，这进一步加剧了这些挑战。

65%

的受访企业拥有**超过50个Git存储库。**

» CI/CD开发周期缩短带来的安全挑战



返回目录


云原生网络安全威胁
形势越来越严峻

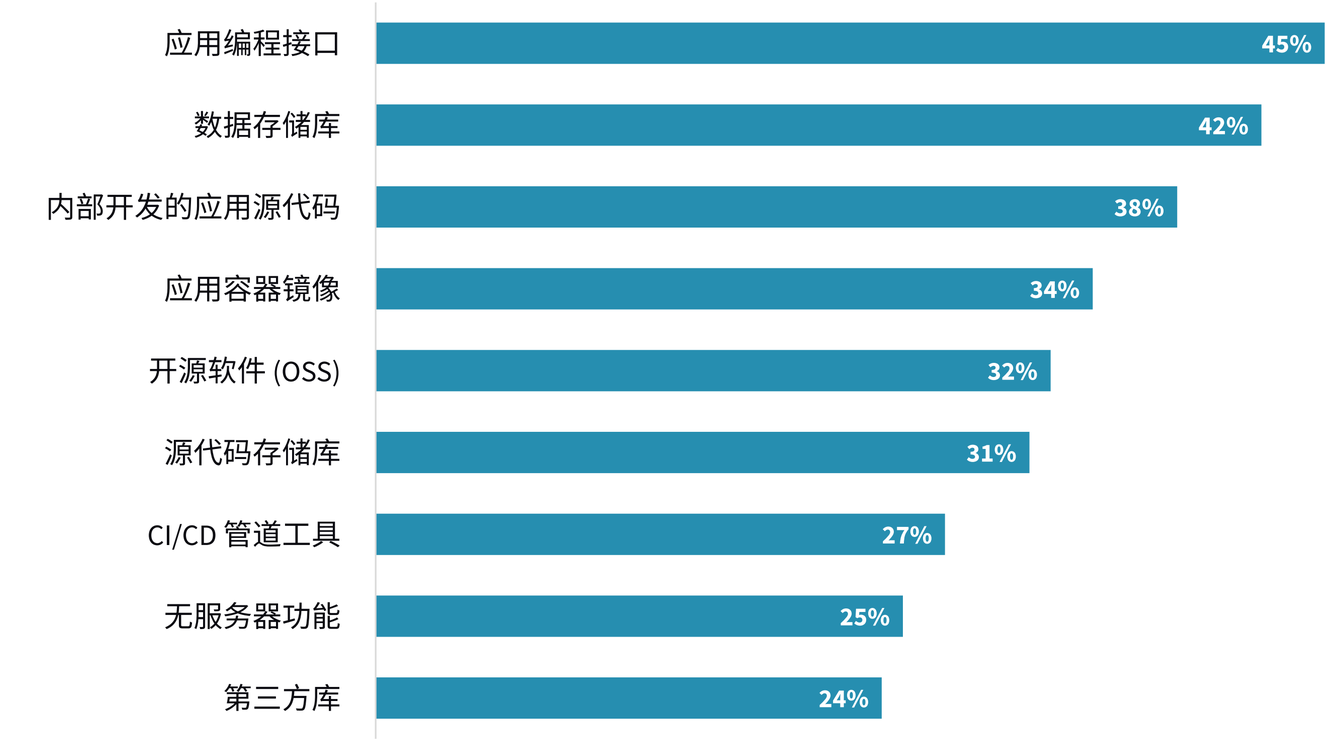
最容易受到攻击的云原生元素与近期发生的安全事件一致

受访企业对其认为最容易受到攻击的软件栈和工具链中的元素进行了评级。API首当其冲，其次是数据存储库和内部开发的应用源代码。

绝大多数受访者都表示，内部开发的云原生应用可能给公司带来各种相关的安全事件和后果。据受访者表示，最常见的三类事件涉及API的不安全使用、代码漏洞和受损的账户凭据，这恰好与两个最易受到攻击的软件栈元素相一致。

> “**API是最容易受到攻击的元素，**其次是数据存储库和内部开发的应用源代码。”

» 云原生应用栈中最容易受到攻击的元素



Back to 返回目录

» 云原生应用导致的网络安全事件

由于API的不安全使用而导致数据丢失的攻击

38%

利用内部开发代码中的已知漏洞的漏洞利用攻击

37%

受损的服务账户凭据

35%

利用开源软件中已知漏洞的漏洞利用攻击

34%

利用配置不当的云服务的漏洞利用攻击

33%

从源代码存储库中窃取的机密信息

31%

利用开源软件中以前未知的新漏洞进行的“零日”漏洞利用攻击

28%

利用内部开发代码中以前未知的新漏洞进行的“零日”漏洞利用攻击

27%

受损的特权用户凭据

26%

返回目录

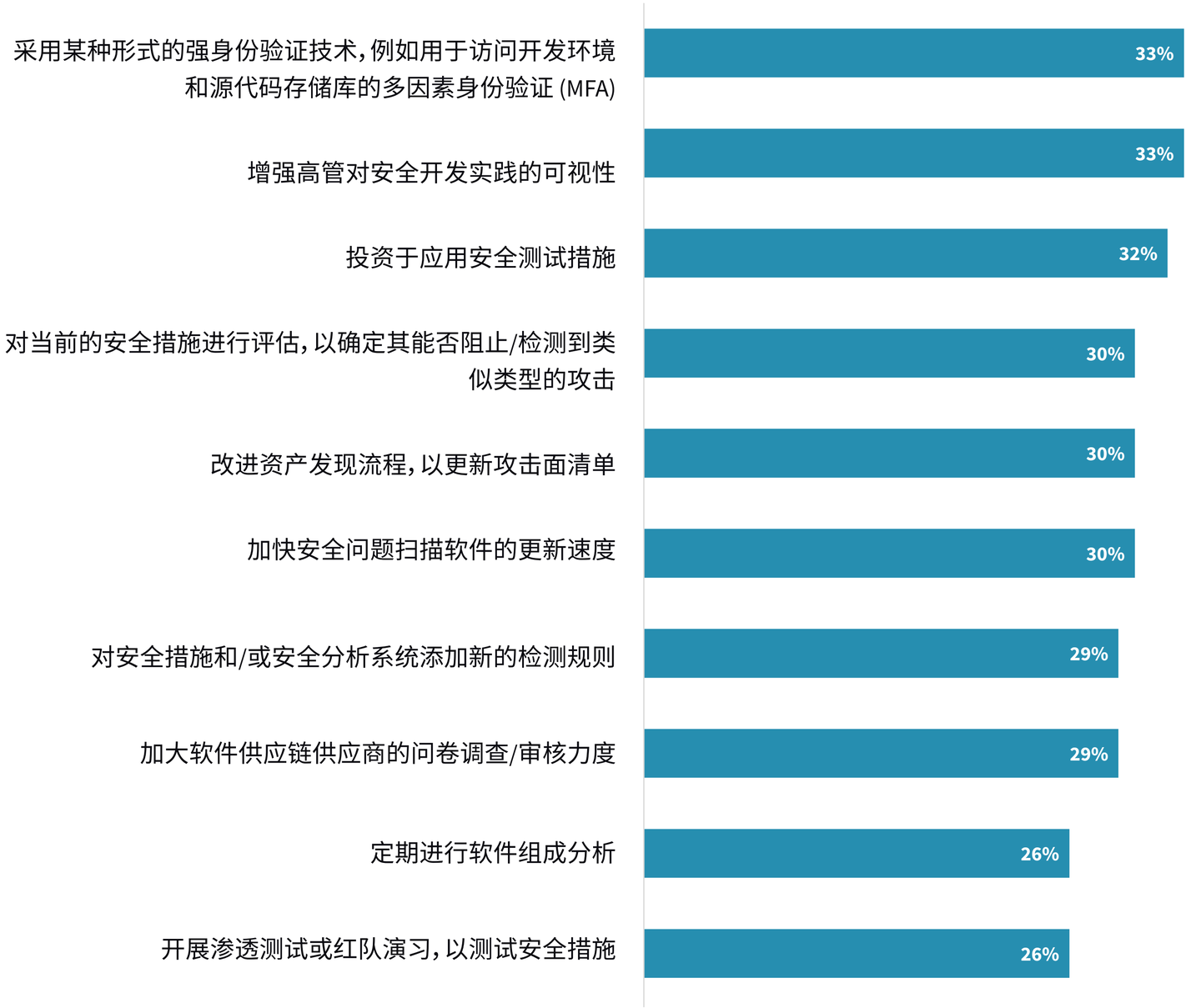
在备受关注的攻击事件之后，企业加强对软件供应链安全的措施

为了消除顾虑，防止云原生应用攻击事件真正发生，企业应尽量采取先发制人的措施来控制这些问题。事实上，受到近期软件供应链攻击的影响，近四分之三（73%）的受访企业显著加大了对开源软件、容器镜像和第三方软件组件的保护力度。企业正在积极采取广泛的措施来降低与这些攻击相关的风险。

73%

的受访企业表示，受到近期软件供应链攻击的影响，他们显著加大了对开源软件、容器镜像和第三方软件组件的保护力度

» 企业因受到近期软件供应链攻击影响而采取的十大措施



返回目录

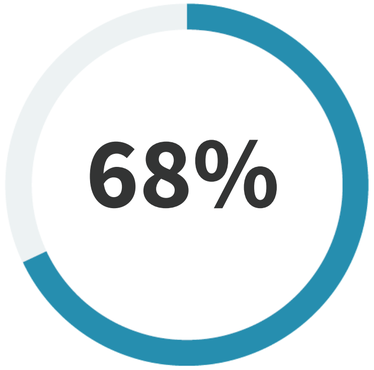
安全必须在不中断运行的情况下融入到开发流程中

企业通过左移进行扩展

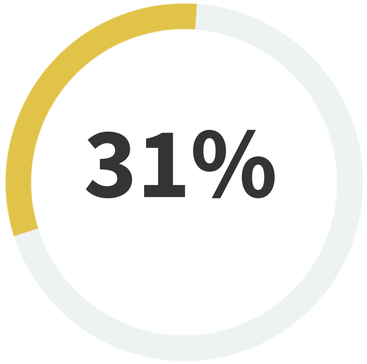
大多数企业都优先考虑以开发者为中心的安全解决方案，甚至将一些安全责任转移给开发人员，因为这是他们实现扩展的唯一方式。事实上，几乎所有的受访者都表示这很重要，超过三分之二 (68%) 的受访者将其视为重中之重。尽管36%的受访企业表示他们完全接受将安全责任转移给开发人员，但大多数受访企业 (49%) 对此表示基本接受，另有部分受访企业 (15%) 对此表示不太接受。

» 企业对采用以开发者为中心的安全策略的重视程度

这是重中之重（即，它将对我们的安全计划产生重大影响）

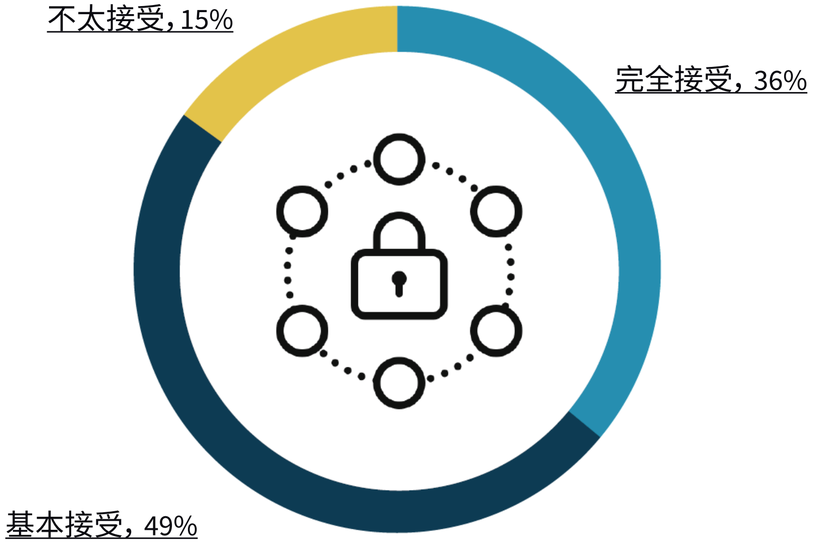


这很重要，但不是重中之重
（即，我们有更重要的安全及/或应用开发项目）



另有1%的受访企业表示，**这根本不重要**
（即不将责任转移给开发人员，照样可以做好安全工作）

» 安全团队对企业采用以开发者为中心的安全策略的接受程度



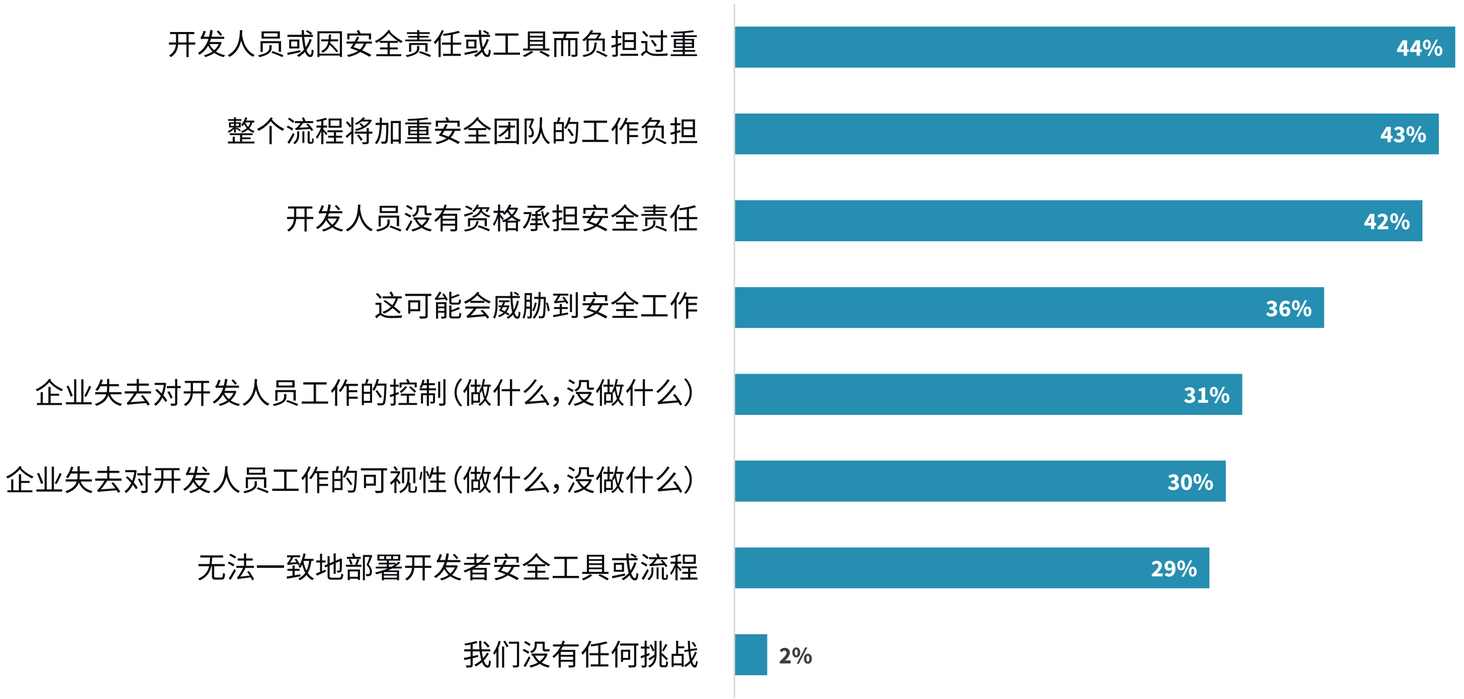
返回目录

将安全责任转移给开发人员的挑战

让开发人员更多地参与安全活动和流程虽然优势明显，但也有一些障碍需要克服。调查显示，在开发人员承担更多的安全任务方面，最大的挑战包括开发人员负担过重 (44%) 或没有资格接管安全责任 (42%)，以及这些努力最终将加重网络安全团队的工作负担 (43%)。

“这种做法虽然优势明显……**但也有一些障碍需要克服。**”

» 让开发人员接管更多安全责任存在的挑战

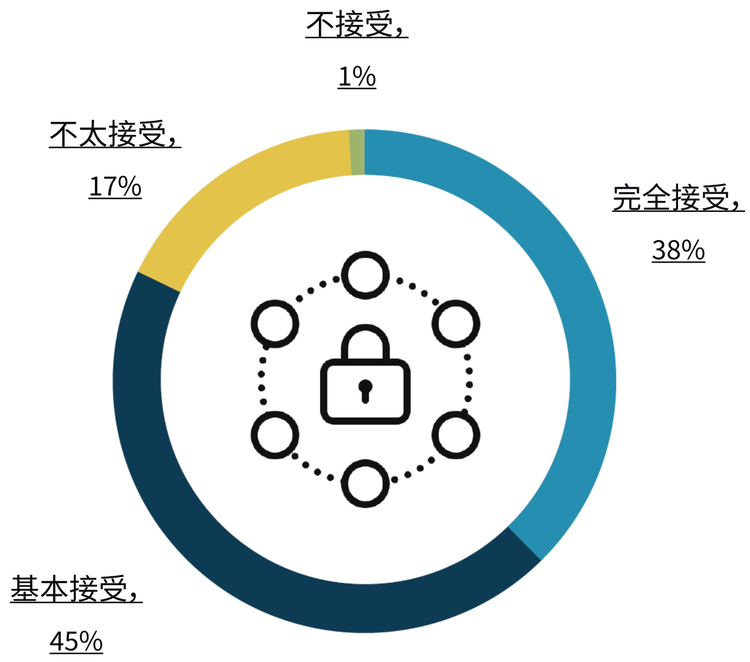


返回目录

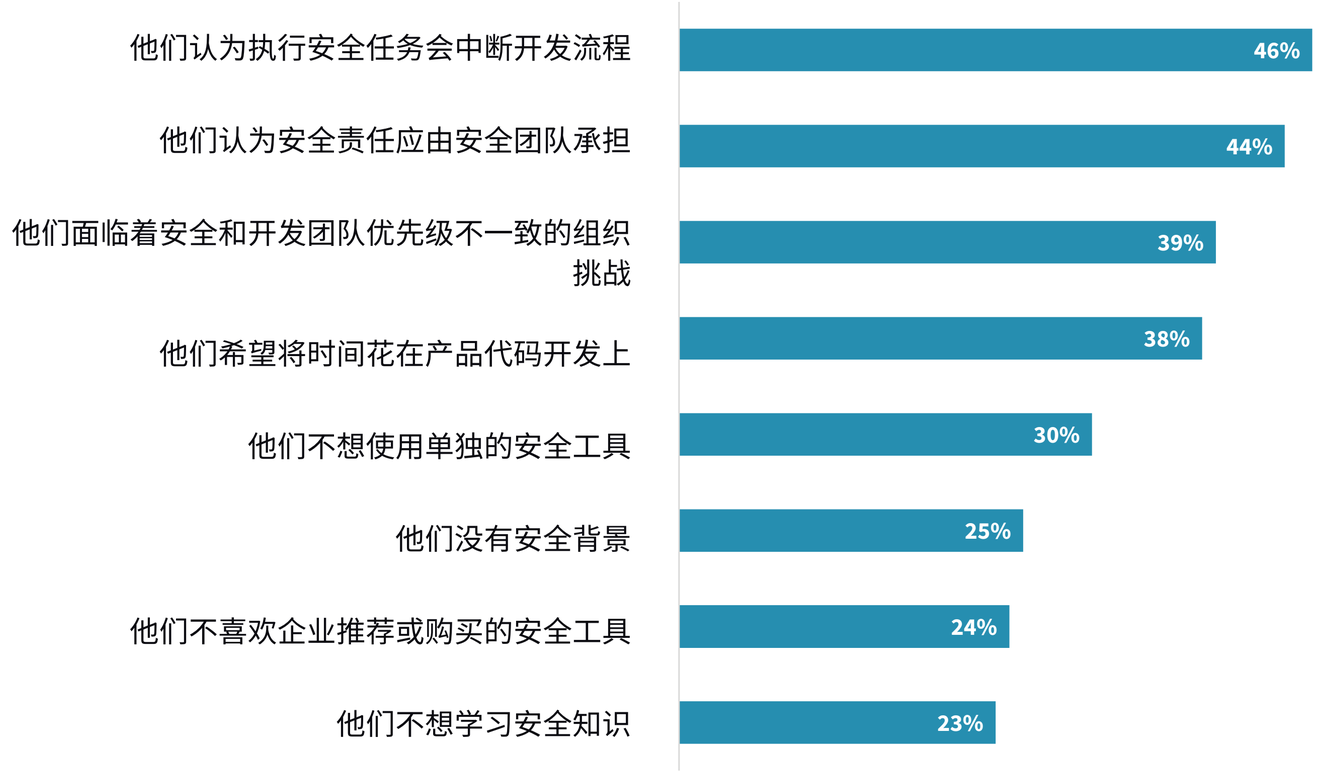
开发人员面临的挑战

从开发人员的角度来看，大多数受访者完全 (38%) 或基本 (45%) 愿意承担更多的安全责任。对于不完全接受这种左移策略的开发人员来说，他们主要担心执行安全任务会导致开发流程中断，并且他们认为安全团队应保持对安全生态系统的完全自主控制。

» 开发人员对进一步参与安全事务的接受程度



» 开发人员对承担安全责任不能完全接受的原因



返回目录

企业已经开始将监控和安全测试融入开发流程，以降低风险

开发人员工作流之外的安全工具

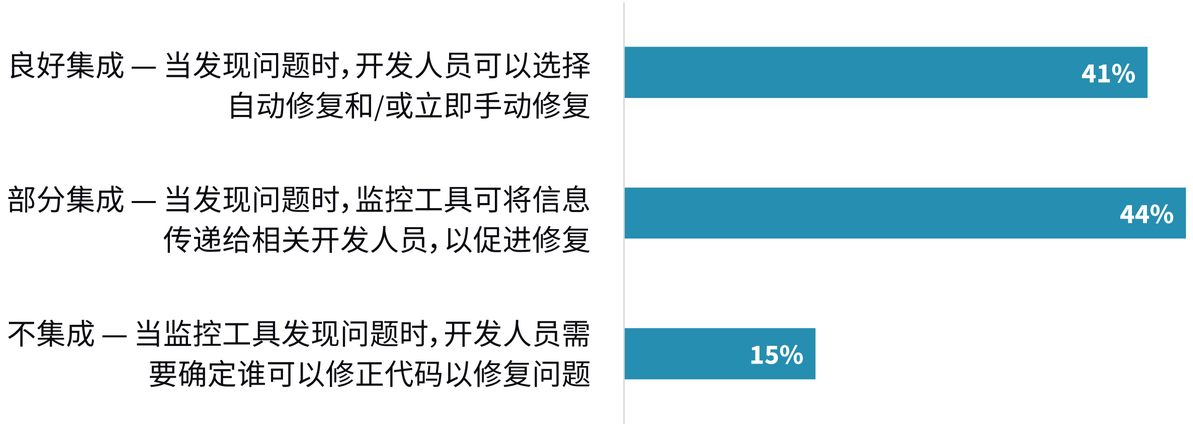
尽管仍有44%的企业依赖单独的安全工具进行测试，但已有超过一半 (56%) 的企业开始使用可以集成到开发者工具中的安全工具。为了提高开发人员的接受度，企业应寻找可以融入开发人员工作流的安全工具，从而无需切换上下文即可修复编码问题。

» 安全工具在开发人员工具和工作流中的工作方式

安全监控工具与开发流程的集成

企业致力于将监控解决方案与以开发者为中心的安全工具相集成，以加快修复速度。这是一种很好的做法，可确保有效修复运行时发现的安全问题，无需安全和开发团队花费太多时间。成功集成后，开发人员将能够有效地修复问题，而无需安全团队提供帮助。

» 云安全监控解决方案与开发流程之间的集成水平



返回目录

将安全测试融入开发流程的主要挑战

企业采用多种工具，作为以开发者为中心的新兴安全战略的一部分，包括使用第三方渗透测试工具或咨询服务来帮助确保应用安全。虽然安全团队试图将安全测试责任左移至开发人员，但他们在此过程中面临诸多挑战，主要包括如何获得所需的可视性和控制权来确保顺利完成测试，以及开发人员如何在不中断开发流程的情况下对安全测试做出必要的调整。

» 使用第三方渗透测试解决方案或咨询服务来确保云原生应用的安全性

是，对于所有应用

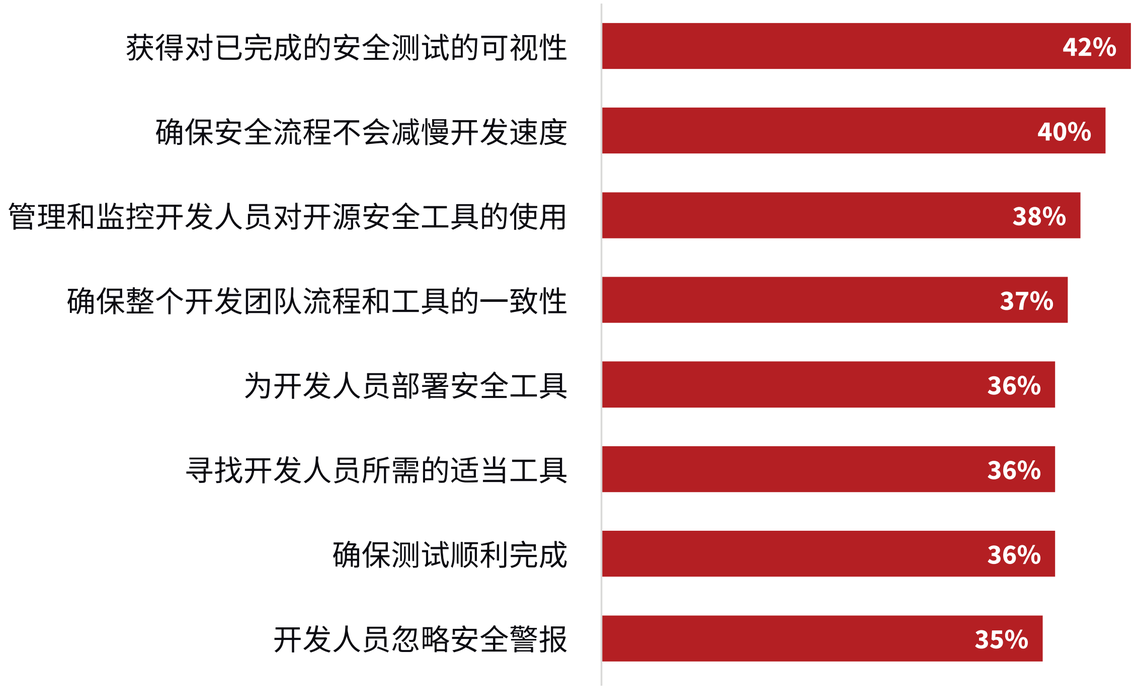
71%

是，但仅限关键业务应用，

27%

An additional 1% said they don’t use these services.

» 开发团队的安全测试挑战



返回目录

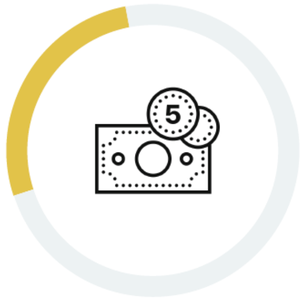
企业已经开始投资安全开发流程

企业已经开始在安全开发流程方面投资

展望未来，超过三分之二 (69%) 的受访企业计划对可以集成到云原生软件开发流程中的安全解决方案进行重大投资。就这些投资的方向而言，超过三分之一 (34%) 的受访企业表示，其投资重点是改进应用安全测试；31%的受访企业表示，其投资重点是检测存储在源代码存储库中的机密信息和/或应用运行时API的安全措施。

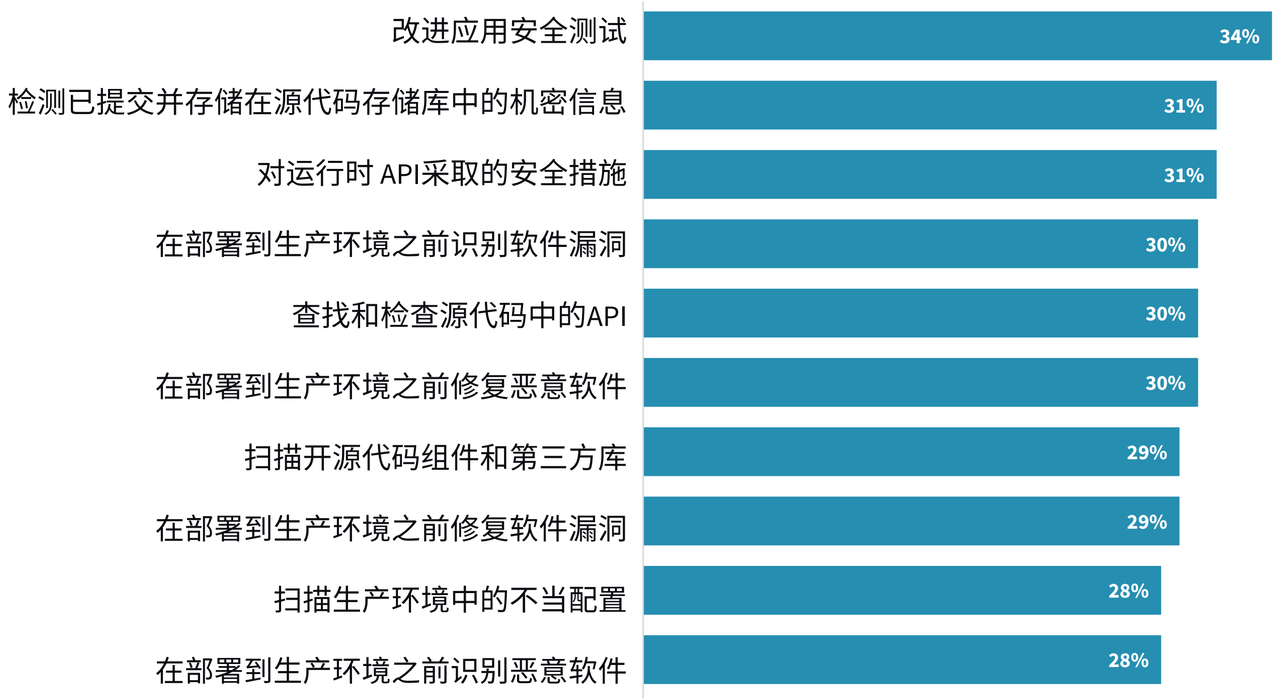
» 投资可以集成到云原生软件开发流程中的安全解决方案的计划

我们预计将
进行重大投资
69%



我们预计将
进行适度投资
31%

» 旨在保护云原生软件开发流程的十大重点投资领域



返回目录

SYNOPSYS® · 新思

新思科技帮助开发团队构建安全的高质量软件，最大限度降低风险，同时提高速度和生产力。新思科技是应用安全领域公认的领导者，致力于提供静态分析、软件组成分析和动态分析解决方案，助力团队快速发现和修复专有代码、开源组件和应用中的漏洞和缺陷。

了解更多信息

关于ESG

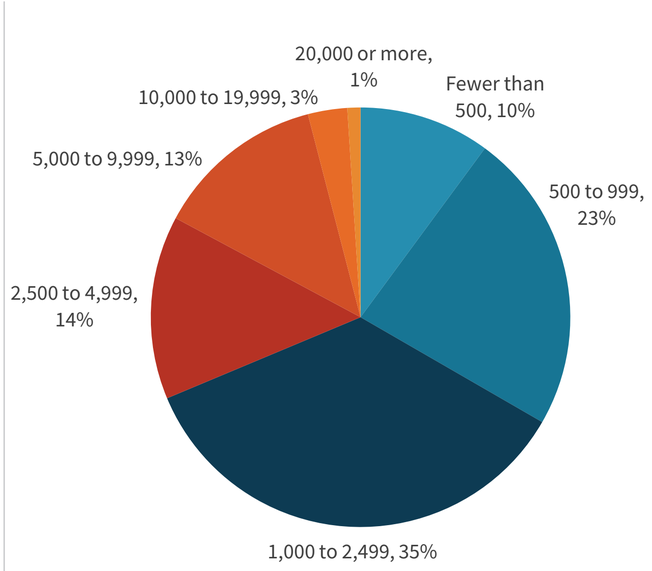
Enterprise Strategy Group是一家综合性的技术分析、研究和战略公司，致力于为全球技术社区提供市场情报、可行的洞察和上市内容服务。

研究方法

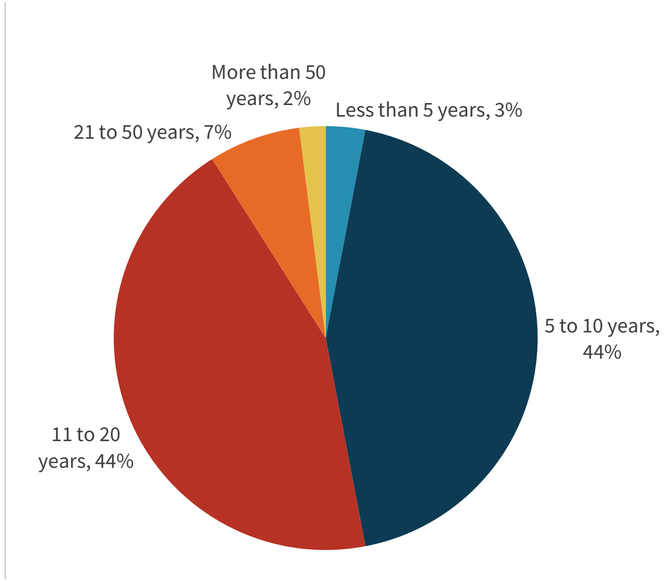
为了收集本报告的数据，ESG在2022年5月18日至2022年6月10日期间对北美私营和公有企业的IT和网络安全专业人员以及应用开发人员进行了全面的在线调查。参与该项调查的受访者必须是负责评估、购买和使用以开发者为中心的安全产品的人员。完成调查的所有受访者均可获得现金和/或现金等价物形式的奖励。

在过滤掉不合格的受访者，去除重复的回答，并根据若干标准对剩余的已完成的回答进行筛选以保证数据完整性后，我们最终得到了350名IT、网络安全和应用开发专业人员的回答样本。

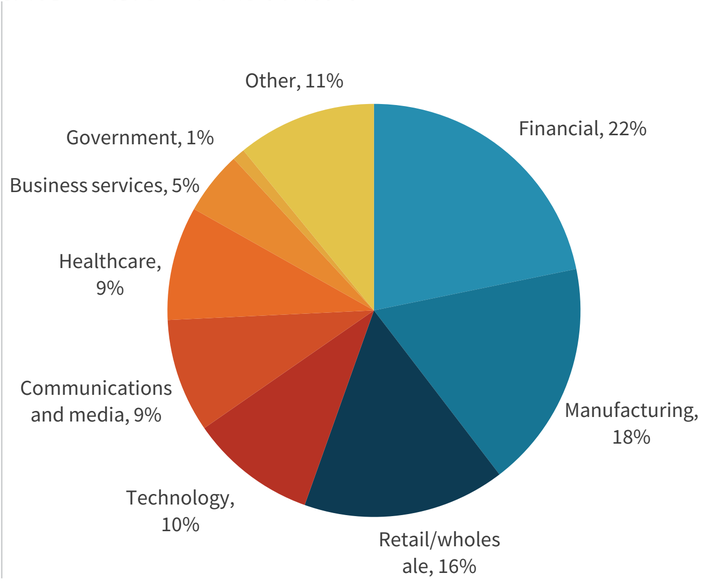
按公司员工数量划分的受访者饼图



按公司年龄划分的受访者饼图



按行业划分的受访者饼图



返回目录

Enterprise Strategy Group是一家综合性的技术分析、研究和战略公司，致力于为全球技术社区提供市场情报、可行的洞察和上市内容服务。