2023-2024年

全球应用程序安全测试市场研究报告

《中国信息安全》杂志社 | 武汉金银湖实验室 | 深圳市网络与信息安全行业协会
OWASP中国 | 网安加社区

报告编委

参与编写单位：《中国信息安全》杂志社、武汉金银湖实验室、深圳市网络与信息安全行业协会、OWASP 中国、网安加社区。

参与编写人员：严雪伦、位华、李刚、白健、杨军艳、李宇卉、王颉、宋荆汉、郭露、李婷、罗欣然、谢凌云、韦兆进（排名不分先后）。

版权声明

本文件为首次发布。本调查报告版权属于《中国信息安全》杂志社、武汉金银湖实验室、深圳市网络与信息安全行业协会、OWASP 中国以及网安加社区，并受法律保护。转载、摘编或利用其他方式使用本调查报告文字或观点的，应注明“来源:《2023-2024 年全球应用程序安全测试市场研究报告》”。违反上述声明者，将追究其相关法律责任。

前言

在当今这个数字化时代，随着信息技术的飞速发展，应用程序已成为推动各行各业数字化转型的关键力量。然而，伴随着应用程序的广泛应用，其安全性问题也日益凸显，成为制约其进一步发展的关键因素。应用程序安全漏洞的存在不仅可能导致数据泄露、服务中断等严重后果，还可能对用户的隐私和财产安全构成威胁。因此，确保应用程序的安全性，已成为企业和组织不可忽视的重要议题。

正是在这一背景下，全球应用程序安全测试（AST）市场应运而生，并迅速发展成为保障应用程序安全的重要支撑。应用程序安全测试（AST）是一种专门用于检测、识别和预防应用程序中潜在安全漏洞的技术手段，它通过深入分析源代码、二进制代码或运行时行为，为开发者和安全团队提供发现潜在安全风险的途径，进而提升应用程序的整体安全性。

本报告旨在全面剖析全球应用程序安全测试（AST）市场的现状、发展趋势及未来前景。通过收集和分析大量市场数据、行业报告、专家访谈以及问卷调查，我们对全球 AST 市场的规模、竞争格局、技术趋势、应用领域以及面临的挑战与机遇进行了深入探讨。我们相信，这份报告将为相关从业者、投资者及政策制定者提供有价值的参考和启示。

1 研究概述

1.1 研究背景与意义

随着信息技术的飞速发展和数字化转型的加速，软件已成为现代企业运营中不可或缺的核心部分。无论是金融服务、电子商务、社交网络，还是医疗健康、智能制造等领域，应用程序都扮演着至关重要的角色。然而，随着应用程序的广泛普及，其面临的安全威胁也日益严峻。黑客攻击、数据泄露、恶意软件等安全问题频发，不仅损害了用户的隐私和利益，也给企业带来了巨大的经济损失和声誉风险。

应用程序安全测试（Application Security Testing, AST）作为保障应用程序安全的重要手段，近年来备受关注。AST 可通过模拟攻击、漏洞扫描、代码审查等方式，对应用程序进行全面、深入的安全检测，发现潜在的安全漏洞和风险点，为开发者和安全团队提供及时的安全反馈和改进建议。随着技术的不断进步和市场的不断成熟，AST 工具和方法也日益丰富和多样化，从静态分析到动态分析，从自动化测试到人工渗透测试，为不同场景和需求下的应用程序安全测试提供了丰富的选择。

在此全球化背景下，深入剖析全球 AST 市场具有重大战略价值。洞悉市场现状、把握趋势脉搏、挖掘机遇与挑战，不仅助力企业精准制定战略规划、优化产品布局，共促应用程序安全领域繁荣，携手构建更加稳固可信的数字基石。同时，为政府监管、行业协会等提供决策支持，推动整个行业稳健前行。

本报告核心意义在于为企业提供前瞻性的战略指引。通过深度挖掘 AST 市场需求、竞争格局及未来走向，助力企业精准自我定位，制定既契合市场又具前瞻性的战略蓝图，强化市场竞争力。此外，报告强调技术创新与产业升级的关键作用，鼓励企业通过把握 AST 技术潮流与创新导向，激发创新潜能，加速新技术、新产品的迭代涌现，引领应用程序安全领域实现质的飞跃。

鉴于网络安全挑战日益严峻，用户隐私与数据安全成为全民关切。本报告致力于推动相关企业及机构强化安全测试与防护体系，筑牢用户隐私与数据安全防线，守护社会稳定与公众权益。同时，为政策制定者提供详实市场数据与洞见，确保政策制定紧贴市场需求与行业脉搏，共谋应用程序安全行业的长远发展蓝图。

1.2 研究范围与方法

本报告的统计标准包括，统计口径、统计范围、调查方法和术语解释，供业界相关人员参考指正。

本报告的统计口径包含国内外公开财报的上市企业，以财报披露的营收额为准。本报告包括多种整体市场规模的统计数字，根据不同维度进行划分，分别为全球、地区、我国应用程序安全行业总收入。本报告表格统计数据的时间跨度为 2017 年至 2024 年上半年（不包含并购年份时间），不同维度数据时间上会存在浮动，具体以表格描述为准。

本报告根据原厂能力、营收水平和业务类型，选择了国内外核心厂商以及极具代表性的厂商作为本报告的基础调查对象。

- 本报告的统计范围为全球在应用程序安全测试领域极为突出或者公司核心业务包含应用程序安全测试的企业，其中国内的企业不包含香港、澳门和台湾地区。
- 本报告的 AST 内容仅围绕提供核心测试功能的工具部分，不包含其他各种可选的专用功能。
- 本报告的基础调查对象不包括专门从事分销、代理、代售业务的企业，不具备解决方案能力的集成商，公司产品不具备软件著作权的企业，以及非企业主体，如研究所、测评中心、高校学院等。
- 在调研方面，本报告主要通过企业问卷调查、公开资料收集、日常交流访谈三种形式开展调研工作。截至 9 月份，我国 AST 行业调查问卷主要针对 AST 供应商进行调研，问卷回收量约为 95.7%，覆盖国内 AST 供应商数量近九成。此外，我国软件供应链安全调查问卷面向国内 IT 企业进行发放，回收量为 100%。
- 在统计方面，本报告将统计对象的年营业收入、商业模式、商业逻辑、业务类型、收并购情况、市场招投标数据等数据进行分析整理以及计算后，从各种不同的维度进行展现。
- 在收入方面，因国内暂无主营应用程序安全测试业务的上市企业，因此国内营收数据以及收并购情况并不计入分析，但市场规模方面会将核心业务包含应用程序安全测试有关工具的数据加入统计。

1.3 术语解释

（1）应用程序安全测试（AST, Application Security Testing）

应用程序安全测试是审查和分析应用程序以识别潜在安全漏洞的过程。AST 旨在预测和减轻潜在的安全风险，防止恶意攻击，并确保应用程序的稳健性。它是一种主动的方法，通过识别并修复漏洞和弱点来增强应用程序的安全性。

（2）并购（M&A, Mergers and Acquisitions）

并购是指企业之间的合并与收购行为，即一个企业通过购买股票、资产或承担债务等方式，获得

另一个企业的控制权或全部资产，以实现企业的扩张、资源整合或战略转型。并购是企业重组的一种重要形式，涉及企业法人权利的转移和重新安排。

（3）静态应用程序安全测试（SAST, Static Application Security Testing）

SAST 是一种通过静态分析技术对源代码或编译后的中间码进行扫描、检测、分析，以发现潜在安全漏洞和代码缺陷的技术。SAST 工具可以在不执行程序的情况下，检查代码中的安全问题和漏洞，如跨站脚本攻击 (XSS)、SQL 注入等。

（4）动态应用程序安全测试（DAST, Dynamic Application Security Testing）

DAST 是在应用程序处于运行状态或生产环境中，通过模拟攻击来发现安全漏洞的过程。DAST 测试者通常无需了解应用程序的内部架构或代码，而是从外部攻击者的角度，利用自动化工具或手动测试来识别应用程序中的安全弱点。

（5）交互式应用程序安全测试（IAST, Interactive Application Security Testing）

IAST 是一种结合了 SAST 和 DAST 特点的安全测试技术，也被称为灰盒测试。IAST 通过插桩技术收集、监控应用程序运行时的函数执行和数据传输，实时与服务器进行交互，从而高效、准确地识别安全缺陷及漏洞。它可以在开发和测试阶段无缝集成到现有的开发流程中。

（6）软件成分分析（SCA, Software Composition Analysis）

SCA 是一种对二进制软件的组成部分进行识别、分析和追踪的技术。它专注于分析开发人员使用的各种源码、模块、框架和库，以识别和清点开源软件组件及其构成和依赖关系，并识别已知的安全漏洞或潜在的许可证授权问题。

（7）自带设备办公（BYOD, Bring Your Own Device）

BYOD 是一种允许员工使用个人设备（如智能手机、平板电脑和笔记本电脑）进行工作的政策或实践。它提高了员工的工作灵活性和效率，但也带来了数据安全和隐私保护方面的挑战。

（8）产品主导增长（PLG, Product-Led Growth）

PLG 是一种以客户为中心的增长策略，通过产品的自我推销和用户体验来吸引和留住用户。PLG 强调产品的易用性、价值和用户体验，旨在通过口碑传播和用户自发推荐来实现增长。

（9）年复合增长率（CAGR, Compound Annual Growth Rate）

CAGR 是复合年增长率，用于衡量某项投资、资产或收入在一段时间内的平均增长率。CAGR 考虑

了增长率的复利效应，是评估长期增长趋势的重要指标。

（10）软件开发生命周期（SDLC, Software Development Life Cycle）

SDLC 是软件工程中的一个通用性名词，它描述了软件从产生到报废的整个生命周期。SDLC 是一种逐步推进的方法论，旨在通过一系列明确定义、有序执行的阶段来提高软件的质量。

（11）人工智能（AI, Artificial Intelligence）

人工智能是一个以计算机科学（Computer Science）为基础，由计算机、心理学、哲学等多学科交叉融合的交叉学科、新兴学科，研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学，企图了解智能的实质，并生产出一种新的能以人类智能相似的方式做出反应的智能机器，该领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。

2 应用程序安全测试定义与分类

AST 是一个综合性的过程，旨在通过审查和分析应用程序来识别并预防潜在的安全漏洞。这一过程不仅关注应用程序的代码层面，还涵盖其基础设施和整体架构。AST 的核心目标是在漏洞和弱点被恶意攻击者利用之前，通过主动的方法识别并减轻它们带来的安全风险，从而确保应用程序的稳健性和安全性。

AST 由四种提供核心测试功能的工具维度（静态应用程序测试、动态应用程序测试、交互式应用程序测试和软件组成分析）以及各种可选的专用功能（API 测试、应用程序安全状况管理 ASPM、容器安全、开发人员支持、模糊测试、基础设施即代码测试 IaC 以及移动应用程序安全测试 MAST）组成。

可选功能提供更专业形式的测试，并且通过根据组织的应用程序组合或应用程序安全程序成熟度来补充核心功能。它们包括：

- **API 测试：**API 已成为现代应用程序（例如，单页或移动应用程序）的重要组成部分，但传统的 AST 工具集可能无法完全测试它们，从而导致对专用工具和功能的需求。典型功能包括在开发和生产环境中发现 API 和测试 API 源代码的能力，以及引入记录的流量或 API 定义以支持正在运行的 API 的测试的能力，都是典型的功能。
- **应用程序安全状况管理（ASPM）：**ASPM 通过检测、关联和确定整个 SDLC 从开发到部署的

安全问题的优先级，持续管理应用程序风险。他们从多个来源摄取数据，然后关联和分析其发现，以便更轻松地进行解释、分类和补救。它们充当安全工具的管理和编排层，支持安全策略的控制和实施。通过提供应用程序安全发现的统一视角，ASPM 工具有助于管理和修复单个发现，同时提供整个应用程序或系统的安全和风险状态的全面视图。

- **容器安全：**容器安全扫描在部署之前检查容器映像或完全实例化的容器是否存在安全问题。容器安全工具专注于各种任务，包括配置强化和漏洞评估任务。工具还会扫描是否存在机密，例如硬编码的凭据或身份验证密钥。容器安全扫描工具可以作为应用程序部署过程的一部分运行，也可以与容器存储库集成，因此可以在存储映像以供将来使用时执行安全评估。
- **开发人员支持：**开发人员支持工具和功能支持开发人员和工程团队成员创建安全代码。这些工具主要侧重于安全培训和漏洞修正指导，无论是独立使用还是集成到开发环境中。
- **模糊测试：**模糊测试依赖于向程序提供随机、格式错误或意外的输入，以识别潜在的安全漏洞，例如，应用程序崩溃或异常行为、内存泄漏或缓冲区溢出，或其他使程序处于不确定状态的结果。模糊测试，有时称为非确定性测试，可以与大多数类型的程序一起使用。
- **基础设施即代码（IaC）测试：**Gartner 将 IaC 定义为软件定义计算（SDC）、网络和存储基础设施作为源代码的创建、配置和配置。IaC 安全测试工具有助于确保符合通用配置强化标准，识别与特定操作环境相关的安全问题，查找嵌入式机密，并执行支持组织特定标准和合规性要求的其他测试。
- **Mobile AST（MAST）：**这解决了与测试移动应用程序相关的特殊要求，例如在使用 iOS、Android 或其他操作系统的设备上运行的应用程序。这些工具通常使用传统的测试方法（例如，SAST 和 DAST），这些方法已经过优化，以支持通常用于开发移动和 / 或物联网（IoT）应用程序的语言和框架。他们还测试这些环境特有的漏洞和安全问题。

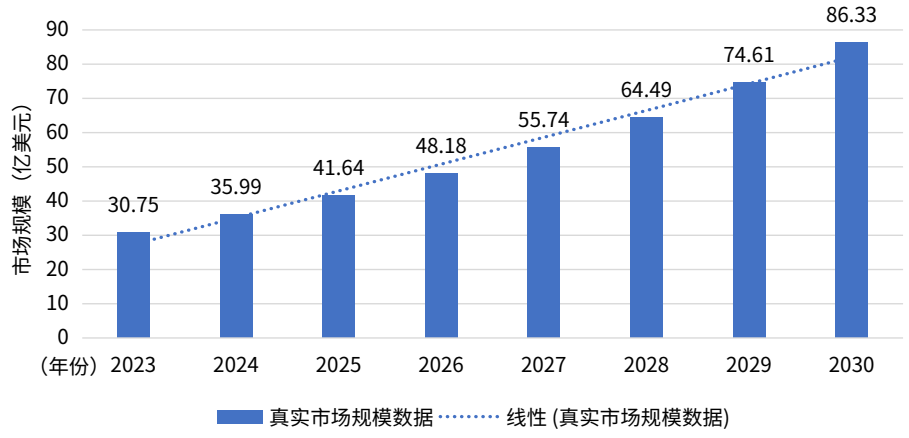
3 全球应用程序安全测试市场现状

3.1 全球 AST 市场规模与增长趋势

2023 年，全球 AST 市场规模增至 30.75 亿美元。预计 2024 年全球 AST 市场规模将达到 35.99 亿

美元并且在 2024—2030 年预测期间内，该市场将以 15.7% 的 CAGR 于 2030 年增长至 86.33 亿美元 [1]。

图 1.2023 年全球应用程序安全测试市场规模及预测

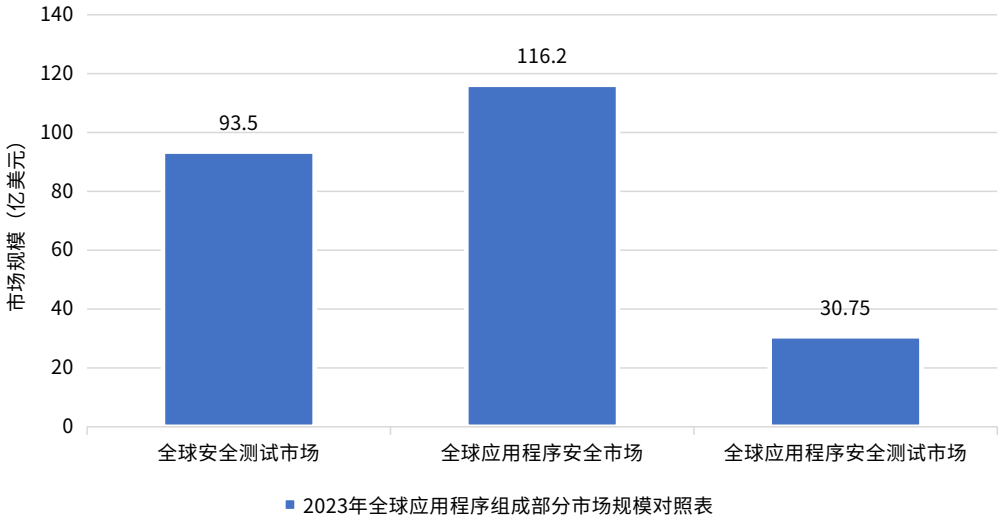


【数据来源于 QY Research】

3.2 全球相关市场规模比对

2023 年全球安全测试市场规模约为 93.5 亿美元，预计复合年增长率为 26.76%，在预测期内的未来五年将达到 375.5 亿美元 [2]。物联网设备和 BYOD 的日益普及刺激了市场的增长。2023 年全球应用程序安全市场规模约为 116.2 亿美元，预计在 2024—2029 年的预测期内以 17.39% 的 CAGR 于 2029 年达到 259.2 亿美元 [3]。

图 2.2023 年全球相关市场规模比对



【数据来源于 Mordor Intelligence】

从上述信息可以看到全球 AST 市场分别占全球应用程序安全市场规模的 26.5% 以及全球安全测试市场规模的 32.9%，占比之高凸显出该市场的重要程度极高，未来待发掘体量大，前景较好。

3.3 区域市场分析

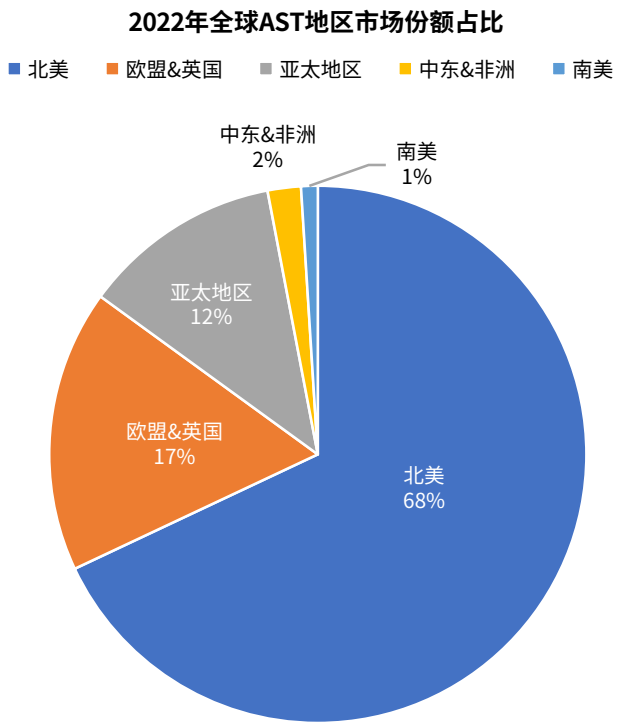
3.3.1 区域市场构成部分

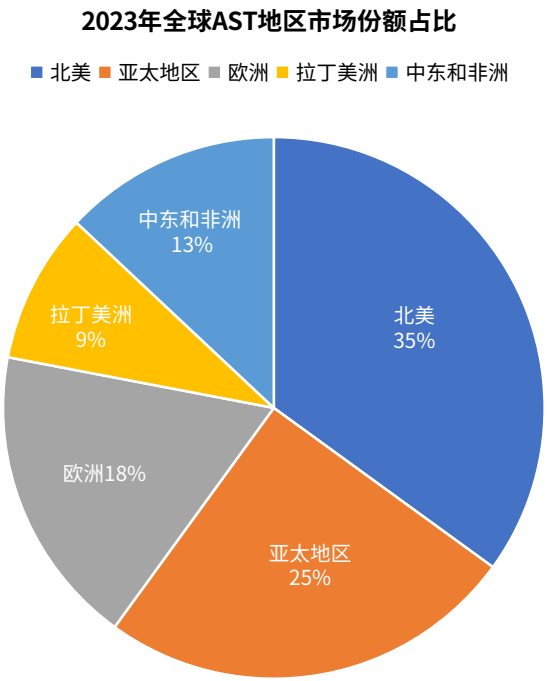
根据网安加社区调研的数据显示，在 2023 年的全球市场份额分布中，北美地区凭借其技术领先优势与强劲的市场需求，稳居榜首，占据 35% 的市场份额。亚太地区紧随其后，以 25% 的份额展现强劲势头，这一增长主要归因于数字化转型的加速、复杂 IT 架构的广泛应用以及网络威胁的不断增加。而欧洲市场则因云端安全测试需求的激增及政府对于安全问题的日益重视，位列市场第三。

2022 年全球 AST 市场各地域总支出占比相较于 2023 年区别较大：

- 北美仍是最大的整体市场，约占总支出的 68%，高于 2023 年 ..3美市场份额占比接近一倍；
- 欧盟和英国排名第二，占 17%，相较于 2023 年未有明显波动；
- 亚太地区占支出的 12%，仅达到 2023 年市场份额占比的半数；
- 中东和非洲（2%）和南美（1%）目前仍属于新兴市场，但正展现出积极的增长态势。

图 3.2022 & 2023 年全球 AST 市场地区市场份额占比





【数据来源于网安加社区】

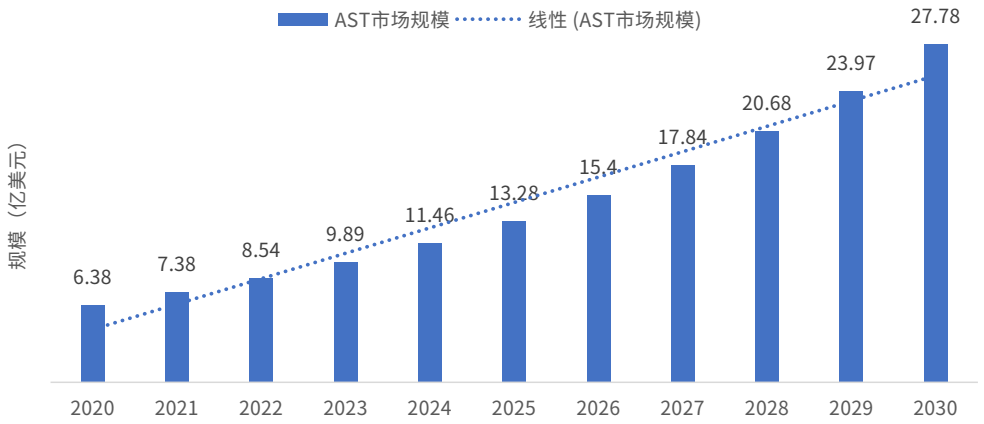
显然，2023 年全球 AST 市场份额分布经历了显著变化。北美地区虽持续作为整体市场的领头羊，但其市场份额却缩减了 33 个百分点。与此同时，亚太地区实现了显著增长，市场份额提升了 13 个百分点，成功从全球第三大市场跃升至第二大市场。中东与非洲地区在 2023 年也迎来了显著增长，市场份额攀升了 11 个百分点。相比之下，欧洲地区市场需求相对稳定，而亚太地区、中东及非洲等区域则展现出对 AST 市场需求的迅猛增长态势。

3.3.2 北美地区

（1）北美地区及美国 AST 市场规模与增长趋势

根据 Grand View Reseach 的研究结果显示 [4]，2023 年北美地区 AST 市场规模约为 10.76 亿美元（北美地区市场份额占比约为 35%）。其中，美国 2023 年应用程序安全测试市场达 9.89 亿美元，占全球 AST 市场规模的 32.16%，并且几乎独揽北美 91.9% 份额。预计美国 AST 市场在 2024—2030 年的周期内将以 15.9% 的年复合增长率持续增长，并在 2030 年达到 27.78 亿美元。下图展示了美国应用程序安全市场的规模情况以及未来增长预测：

图 4. 全美应用程序安全测试市场规模及预测



【数据来源于 Grand View Research】

（2）美国主要企业与竞争格局

北美地区汇聚了众多知名的 AST 厂商，这些厂商在技术创新、产品性能、市场份额等方面均表现出色，详见第四章节。典型代表包括但不限于 Synopsys、Rapid 7 等知名企业。尽管北美 AST 市场的份额分布相对分散，但一些行业领头羊凭借其深厚的技术底蕴与独到的市场策略，成功占据了市场的显著份额。该市场的竞争核心在于持续的技术革新，各厂商竞相加大研发投入，不断推出融合创新功能与卓越性能的新产品，同时灵活运用差异化竞争策略，精准捕捉并满足市场日益多元化的需求。

3.3.3 欧洲地区

欧洲主要企业与竞争格局

在欧洲 AST 市场中，Snyk 于 2022 年以 74 亿美元的估值占据了核心地位，其领先地位体现在诸多方面。尽管该区域不乏其他具有 AST 业务或产品的优秀企业，如 CAST Software 和 Invicti Security，它们在各自领域内均展现出一定的实力与潜力，但与 Snyk 相比，这些企业在产品能力、市场估值、竞争力、市场热度及占有率等方面均存在一定差距。欧洲 AST 市场的竞争格局中，市场集中度高，市场竞争不激烈。

3.3.4 亚太地区

（1）亚太地区 AST 市场规模情况

2023 年全球 AST 市场规模为 30.75 亿美元，亚太地区 AST 市场规模（亚太地区市场份额占比为 25%）总值为 7.69 亿美元，约合人民币 56.12 亿元。

（2）我国 AST 市场占比与全球持平

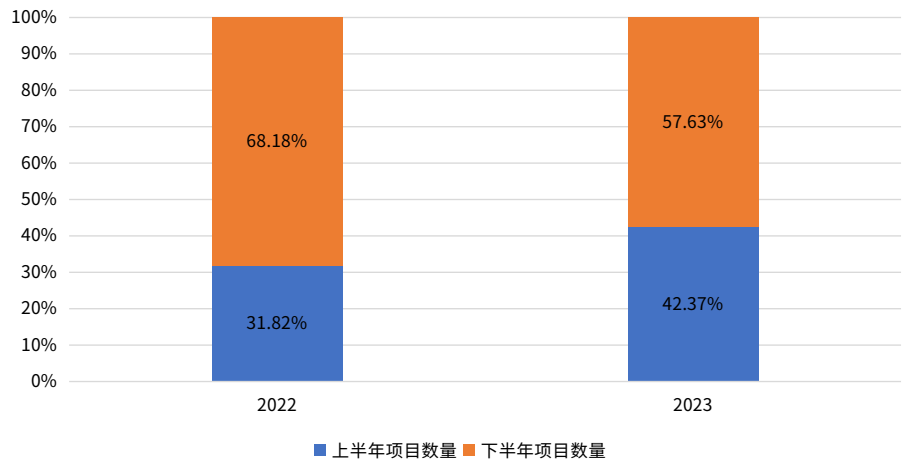
2023 年，全球网络安全市场蓬勃发展，规模高达 2150 亿美元[5]（约 15695 亿人民币）。其中，应用程序安全测试（AST）市场表现抢眼，市场规模达 30.75 亿美元（约 224.48 亿人民币），占比约 1.43%。值得关注的是，我国网络安全市场中 AST 占比已达 1.41%，与国际水平仅差 0.02%，几乎持平，彰显出我国对 AST 技术的高度重视与快速发展。这一现象预示着 AST 市场在我国拥有巨大潜力，市场被高度看好。

（3）中国 AST 招投标项目市场情况分析

依据深圳市网络与信息安全行业协会和网安加社区的联合调研结果显示，在 2022 至 2023 年的持续观测期间，我国产品类项目市场展现出稳健的发展态势，尽管招标项目数量呈温和增长趋势，但市场总体保持相对平稳。从 2022 年上半年至 2023 年，该领域项目占比实现了显著提升：2022 年上半年占比为 31.82%，而到了 2023 年，这一比例已跃升至 42.37%，显示出市场对 AST 产品需求的强劲增长动力。

然而，观察年度内下半年数据，情况则出现了一定程度的反转。与 2022 年下半年高达 68.18% 的占比相比，2023 年下半年 AST 相关产品类公开项目的占比有所回落，降至 57.63%，显示出 10.55 个百分点的降幅。这一变化可能反映了市场需求的季节性波动或是行业内出现部分调整的影响，同时也提示企业在布局市场时需更加关注长期趋势与短期波动的结合分析。总体而言，尽管面临短期波动，但 AST 产品类项目市场的长期增长潜力依然值得期待。详情见下图所示：

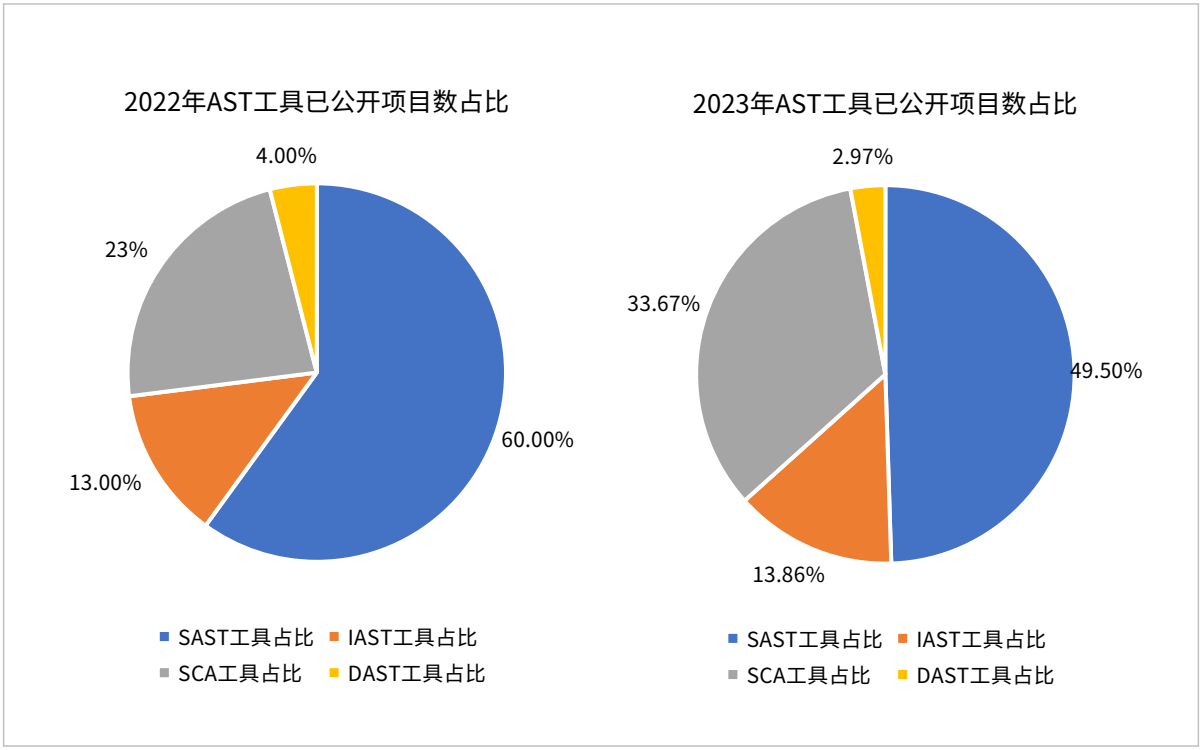
图 5.2022—2023 年中国 AST 产品类目公开招标项目上半年、下半年数量占比情况



【数据来源于招标网】

我国招投标市场所有已知公开项目数据中，2023 年 AST 产品类项目上半年数量占全年项目的 45.9%，下半年占比为 54.1%，其中上半年以及下半年各工具维度的占比如下所示：

图 6.2022 & 2023 年中国 AST 工具已公开项目数占比



【数据来源于招标网】

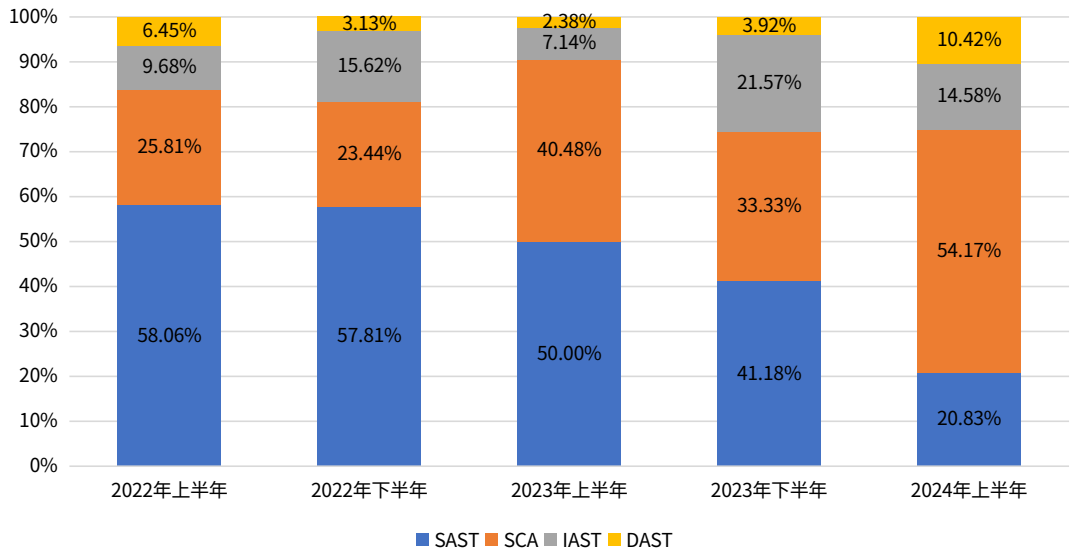
对比两年数据，我国 AST 市场需求显著变化：2022 年 SAST 主导市场，份额达六成，凸显其在应用安全中的核心地位。至 2023 年，SAST 份额缩减，反映出市场需求微调。随着开源代码广泛应用，开源风险凸显，SCA 工具凭借优势迅速崛起，填补市场空白，成解决之道。

SAST 与 SCA 持续领跑，体现企业“安全左移”战略，即在开发初期识别并低成本治理风险。SCA 因全面管理组件、漏洞及许可证风险而备受青睐。

从半年度维度来看，SAST 曾独领风骚，但 2023 年起逐步让位于 SCA。至 2024 上半年，SCA 招标项目占比超五成，跃居首位，标志着市场需求向开源风险管理倾斜。

开源代码依赖加深，风险随之增加，企业开源治理意识增强。SCA 工具精准应对此需求，有效管理开源风险，预示其将成为软件安全领域新趋势。具体情况如下图所示：

图 7.2022—2024 年中国 AST 招标市场公开工具采购数量占比

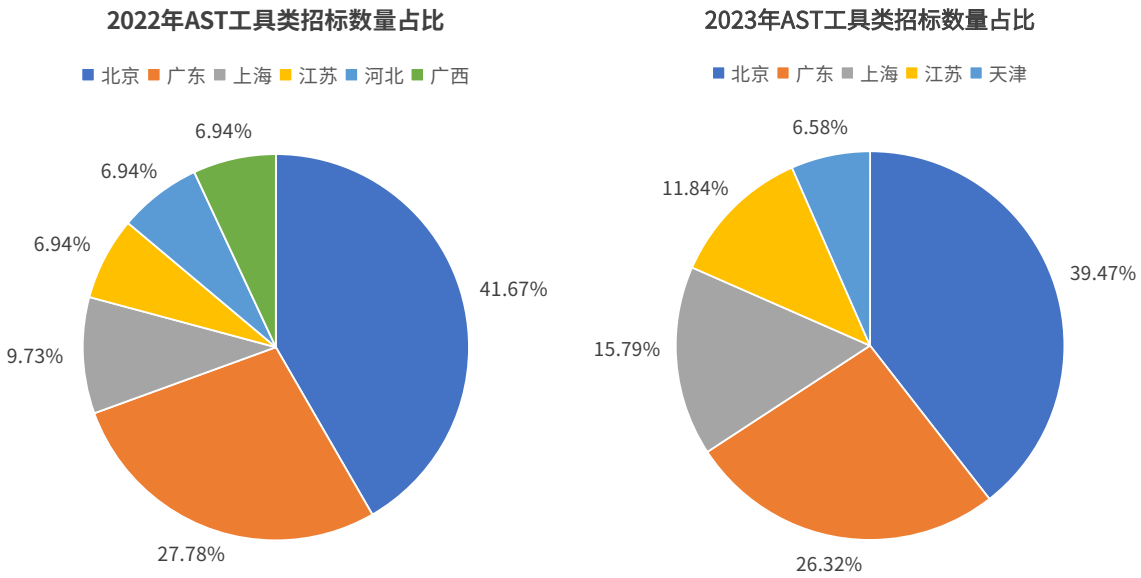


【数据来源于招标网】

（4）中国 AST 市场客户分布情况对比

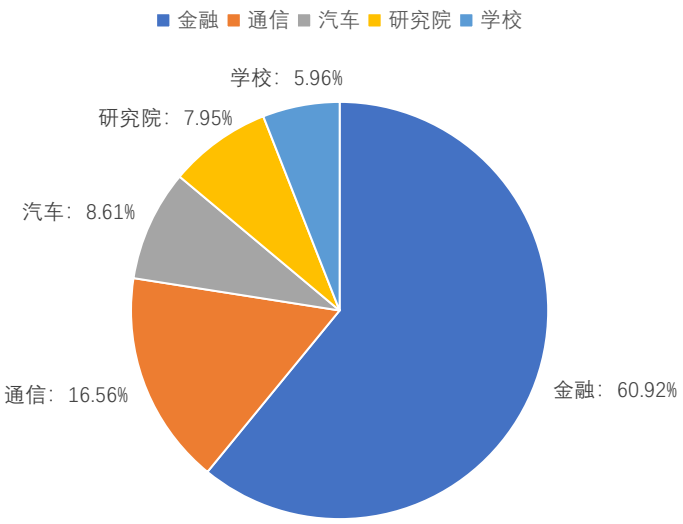
从真实年度数据来看，北京、广东、上海是对应用程序安全测试类产品需求最高并且较为稳定的地区，其他省份如江苏、广西、河北、天津、湖南等需求也在逐渐攀升。

图 8.2022 & 2023 年 AST 工具类招标数量占比



【数据来源于招标网】

图 9.2023—2024 年采购人行业 Top5 占比



【数据来源于招标网】

从 2023—2024 年采购人行业数据前五名占比情况来看，金融行业（银行、证券、保险等）仍旧是核心主需求方，其次是通信行业。

（5）中国本土 AST 企业与竞争格局

中国 AST 市场本土厂商众多，竞争格局多元化且分散，各厂商依据自身专长，在业务方向与产品线覆盖上展现独特风采，形成百花齐放之势。深圳市网络与信息安全行业协会协同网安加社区针对我国 AST 供应商，分别从行业影响力、产品能力、年销售额、是否具备产品著作权这四个核心维度进行综合评选，评选出 31 家企业，清单如下（排名不分先后）：

- **IAST 方面包括：**开源网安、悬镜安全、爱加密、南北科技、海云安、安全共识、水木羽林、国舜、四维创智、默安科技、基调听云、孝道科技；
- **SAST 方面包括：**开源网安、悬镜安全、酷德啄木鸟、HDSEC、鸿渐科技、默安科技、梆梆安全、思客云、南北科技、国舜、海云安、华为、奇安信、中科天齐、安天、孝道科技；
- **DAST 和模糊测试方面包括：**梆梆安全、安般科技、默安科技、海云安、悬镜安全、开源网安、水木羽林、南北科技、云起无垠；
- **SCA 方面包括：**开源网安、悬镜安全、奇安信、比邻科技、思客云、软安科技、清科万道、探巡、腾讯安全、默安科技、安天、安般科技、安势、梆梆安全、HDSEC、海云安、南北科技、孝道科技、爱加密、鸿渐科技、国舜、棱镜七彩、墨云科技、酷德啄木鸟。

3.3.5 中东地区

中东地区主要企业与竞争格局

中东地区的 AST 市场竞争格局呈现出鲜明的特点，即以 Checkmarx 为代表的领军企业占据主导地位。Checkmarx 凭借其深厚的行业积累、先进的安全测试技术和广泛的客户基础，在中东市场树立了极高的品牌知名度和市场认可度。该企业不仅提供全面的 AST 解决方案，还持续投入研发，以适应不断变化的威胁环境和客户需求，进一步巩固了其市场领先地位。

然而，这并不意味着其他国际企业被完全边缘化。相反，众多国际知名 AST 供应商如 Synopsys、Fortify、Veracode 等，也纷纷在中东地区布局，通过本地化策略、定制化服务以及技术创新等手段，努力争夺剩余市场份额。这些企业凭借自身在全球市场的成功经验和技术优势，为中东地区的客户提供多元化的 AST 选项，促进了市场竞争的多元化和活力。

值得注意的是，尽管竞争激烈，但中东地区的 AST 市场并非零和博弈。国际企业与本土企业之间，以及不同国际企业之间，都在探索合作的可能性。通过技术共享、联合研发、市场拓展等形式的合作，共同提升整个市场的技术水平和服务质量。这种合作模式不仅有助于降低企业的运营成本和市场风险，还能加速创新成果的转化和应用，推动整个行业向更高水平发展。

3.4 全球市场机遇分析

3.4.1 数字化转型需求增加与安全挑战并存

随着云计算、大数据、人工智能、物联网等技术的快速发展，企业越来越倾向于通过数字化转型来提升业务效率和竞争力。这些技术为企业提供了更多的创新机会和可能性，但同时也带来了复杂的安全挑战，要求企业加强信息安全方面的投入和保障。

新技术普及双刃剑效应显著，云计算虽便利生活与工作，却也拓宽了安全攻击面。云端存储用户数据若保护不力，易遭窃取。数据传输、共享、迁移中的加密缺失加剧泄露风险，未加密敏感数据更易遭黑客觊觎。容器镜像作为云核心，其漏洞风险亦不容忽视，基础镜像问题可波及所有相关容器，让攻击者有机可乘控制服务。恶意镜像上传至仓库，诱导使用后可植入恶意软件，危害深重。因此，通过 AST 能力对云安全与容器镜像管理进行强化迫在眉睫。

此外，人工智能技术在编码领域的广泛应用也相应带来了不容忽视的风险，尤其体现在编码层面。GitHub 的一项权威开发者调研数据显示 [6]，高达 92% 的开发者在编写代码过程中已采纳 AI 工具作为

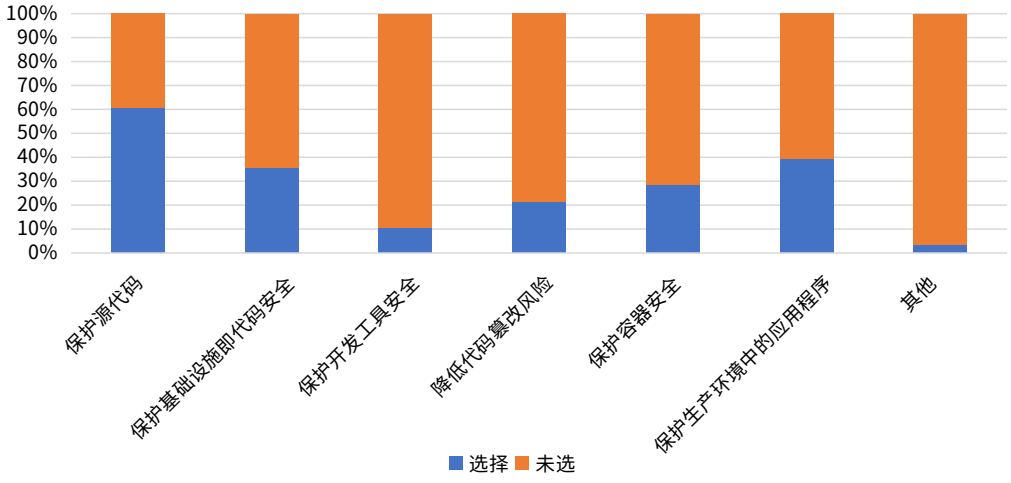
辅助手段，这一趋势凸显了 AI 在软件开发中的普及程度。然而，AI 辅助编码虽便捷高效，却也暗藏风险，其生成的代码安全性问题可能较人工编译更为复杂且难以预测，风险等级有时甚至更高。AI 生成代码安全性的核心在于训练数据的纯净。掺杂高风险漏洞或开源许可冲突的数据将隐患引入 AI 代码，威胁安全并可能引发法务问题。企业数字化转型加速下，AI 工具的高频使用成 AST 市场增长关键。面对 AI 编码新挑战，企业对 AST 工具需求激增，既求高效检测，又盼精准识别并应对 AI 编码引入的安全风险。

3.4.2 企业软件供应链安全意识提高促进 AST 需求增加

网安加社区近期发布的软件供应链安全问卷调查深刻揭示了企业安全投资的重点倾向。在探讨企业于哪个应用安全领域倾注最多资源（包括时间与资金）的问题上，数据表明，高达 60.7% 的企业将首要关注点放在了源代码保护上，这充分显示了源代码作为企业核心资产的重要地位。与此同时，39.3% 的企业则将最大比例的资源投入到了生产环境中的应用程序保护上，凸显了保障业务运行安全性的迫切需求。值得注意的是，另有 35.7% 的企业也强调了基础设施即代码安全性的重要性，体现了企业在现代化 IT 架构下对自动化部署与配置安全性的深刻认识。

这一系列数据不仅映照出当前企业在安全战略部署上的优先次序，也清晰传达了一个信息：源代码、生产环境中的应用程序以及基础设施即代码，这三者构成了企业最为珍视的资产组合。企业正以前所未有的决心和力度，在这三大关键领域加大安全投入，以确保其核心业务的连续性与数据的完整性，从而在日益复杂的网络威胁环境中稳固前行。

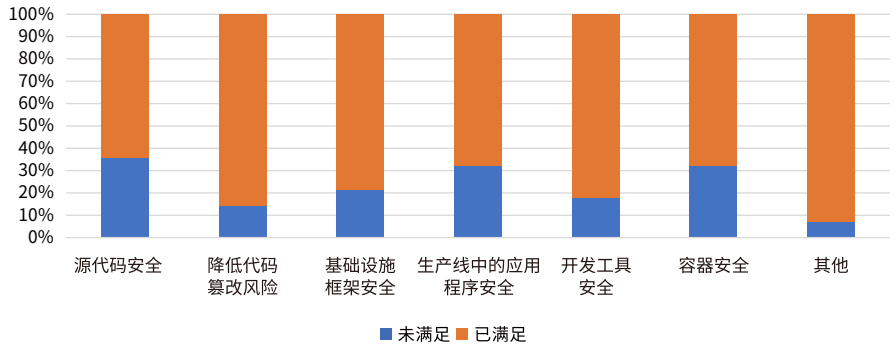
图 10. 企业资源投入情况



【数据来源于网安加社区】

然而，现实的安全状况却呈现出显著的落差。尽管有 6 成的企业高度认同源代码作为企业最宝贵的资产，但令人震惊的是，竟有 35.7% 的企业在源代码安全这一关键环节上尚未采取任何实质性的保护措施，显然未能充分满足该领域迫切的安全需求。更令人忧虑的是，对于生产环境中应用程序安全的保护，同样存在显著疏漏，高达 32.1% 的企业未能达标，这直接暴露了企业在保障业务连续性方面所面临的严峻挑战。综上所述，当前企业的真实安全状况令人堪忧，亟需引起广泛重视并采取紧急措施加以改善。

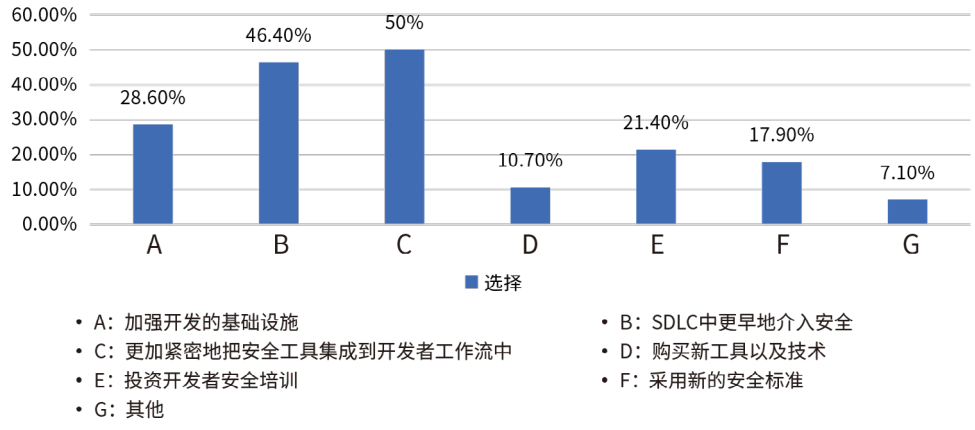
图 11. 企业未满足的安全需求情况



【数据来源于网安加社区】

现阶段企业核心选择通过更加紧密地把安全工具集成到开发者工作流中（50%）和在 SDLC 中更早地介入安全（46.4%）这两种方式来对软件供应链攻击进行有效防范。然而，这两种方式的成功实施均离不开 AST 工具。

图 12. 企业防范软件供应链攻击的核心应对方式



【数据来源于网安加社区】

3.4.3 中小企业市场崛起

应用程序安全漏洞可能导致数据泄露、服务中断等严重后果，直接威胁到企业的业务连续性和声誉。因此，中小企业开始更加重视应用程序安全测试，以确保其应用系统的稳定性和安全性。法规遵从方面，随着网络安全法规的不断完善，如 GDPR（欧盟通用数据保护条例）等，中小企业需要确保其应用程序符合相关法规要求，以避免高额罚款和法律风险。业务需求方面，随着市场竞争的加剧，中小企业需要不断提升其产品和服务的质量，包括安全性，以赢得客户信任并扩大市场份额。此外，由于云计算、AI、自动化测试等技术的发展降低了 AST 的门槛和成本，使得中小企业也能负担得起专业的安全测试服务。因此中小企业对 AST 市场需求近年来增速飞快，但是不同于大型企业，中小企业市场具有以下三个维度的特点：

- **定制化需求增加：**全球中小企业由于业务规模和行业特点的不同，对 AST 的需求往往具有定制化特点。他们希望安全测试服务能够针对其特定的应用场景和业务流程进行优化。
- **性价比要求高：**与大型企业相比，中小企业对成本更为敏感，因此他们更加关注 AST 服务的性价比，即希望在保证测试效果的同时，降低测试成本。
- **智能化水平提升：**随着 AI 技术的不断发展，中小企业对于智能化 AST 工具和服务的需求也在增加。他们希望通过自动化和智能化的手段提高测试效率，降低人力成本。

3.4.4 行业政策与标准的支持

近年来，我国及全球范围内对数据保护和隐私安全的重视程度不断提高，出台了一系列相关法律法规（如 GDPR、中国的《网络安全法》《数据安全法》等）。这些法规要求企业加强对其应用程序的安全管理，确保用户数据的合法、合规使用。这为 AST 市场提供了巨大的市场需求和发展空间。企业需要借助 AST 工具来确保其应用程序符合法规要求，避免因违规操作而面临的法律风险和经济损失。随着 AST 市场的不断发展，相关行业标准也逐渐完善和推广。这些标准不仅规范了 AST 工具的性能指标、测试方法等关键要素，还为企业选择和使用 AST 工具提供了明确的指导。通过遵循行业标准，企业可以更加科学、合理地实施应用程序安全测试，提升整体安全防护水平。同时，行业标准的推广也有助于促进 AST 市场的规范化发展，提高市场的整体竞争力。

3.5 市场挑战与应对

3.5.1 技术复杂性与成本问题

AST 技术涉及多个领域的知识，包括网络安全、软件开发、系统架构等。尽管我国核心主要 AST 需求方为 IT 软件、央国企、政府、金融机构等大型企业，但是近年来中小企业对安全性的重视度和需求量急速增长，因此中小企业逐渐成为了 AST 市场需求的又一大主力军。然而，中小企业往往缺乏专业的技术人员来实施和管理 AST 项目，这增加了技术应用的难度。此外，随着技术的不断进步，新的安全漏洞和攻击手段层出不穷，AST 技术需要不断更新和迭代以应对这些新的威胁。这对企业的技术能力和资源投入提出了更高的要求。

不同行业的中小企业在业务需求和安全要求上存在差异，这要求 AST 解决方案提供商能够提供更加灵活、定制化的服务。然而，定制化服务往往需要更多的技术投入和时间成本，这进一步增加了技术实施的复杂性。

成本方面，在项目初期，引入 AST 解决方案需要购买相关的软件、硬件和服务，这些初期投入成本对于中小企业来说可能是一笔不小的开支。此外，还需要投入人力和时间进行培训和实施，进一步增加了成本负担。在项目成功实施后，企业需要进行持续维护，因此企业需要持续投入资金来购买升级服务或更新软件版本。同时，还需要投入人力进行日常的维护和监控工作，确保 AST 系统的正常运行。

以下是对核心技术难题的详细分析以及相应的解决方案：

（1）测试的全面性不足

传统单一的 AST 工具无法全面覆盖应用程序的所有代码路径和交互场景，导致一些潜在的安全漏洞被遗漏。企业可以通过采用多种 AST 技术相结合的方法，如 SAST、DAST、IAST 以及 SCA 等，以提高测试的全面性。同时，利用自动化工具进行持续集成和持续部署（CI/CD），确保在应用程序的整个生命周期中都进行安全测试。

（2）误报率和漏报率较高

现有的 AST 工具在检测过程中还无法达到极低的误报率和漏报率，从而影响测试结果的准确性和可靠性。企业应通过引入人工智能和机器学习技术，对 AST 工具进行智能优化，提高其识别安全漏洞的准确性和效率。同时，建立和维护一个全面的漏洞数据库，以便对检测结果进行验证和比对，降低误报率。

（3）测试效率低下

随着应用程序规模的扩大和复杂度的增加，传统的 AST 工具可能需要较长的测试时间，影响开发

效率。AST 供应商应当优化 AST 工具的算法和逻辑，提高其处理速度和效率。同时，采用分布式测试架构，以缩短测试周期。此外，还可以利用增量测试技术，只对更改过的代码部分进行测试，进一步提高测试效率。

（4）合规性问题

随着数据保护和隐私安全法规的日益严格，AST 工具需要确保测试结果符合相关法规要求。然而，现有的 AST 工具在合规性检测方面能力可能存在不足或者缺失。企业应在 AST 工具中增加合规性检测模块或者购买具备合规性检测的 AST 检测工具，对应用程序进行合规性审查。同时，与专业的合规性咨询机构合作，提供合规性指导和解决方案。此外，还可以建立合规性数据库，收集和分析相关法规要求，以便在测试过程中进行比对和验证。

（5）技术门槛较高

AST 技术涉及多个领域的知识和技能，包括网络安全、软件开发、系统架构等，导致技术门槛较高，中小企业难以自行实施有效的 AST。供应商应提升 AST 工具和服务的易用性，降低技术门槛。同时，企业自身须加强内部 AST 技术的培训和普及工作，提高开发人员和安全人员的技能水平。此外，供应商可以提供专业的技术支持和咨询服务，帮助企业解决在实施 AST 过程中遇到的问题。

3.5.2 专业人才短缺

在全球 AST 市场呈现出快速增长的态势之时，对 AST 专业人才的需求也同样大幅增长。尽管市场需求旺盛，但 AST 专业人才的供给却出现结构性失衡的局面。这主要是由于 AST 领域的技术门槛较高，需要掌握网络安全、软件开发、系统架构等多方面的知识，且需要不断学习和跟进最新的安全威胁和攻击手段。教育体系滞后以及攻防实践经验的缺乏也导致专业人才培养的周期过长。除了人才培养难度极高以外，该行业自身知名度也较为匮乏，从一定程度上也影响了人才的流入和行业的发展。

我国围绕 AST 行业开展人才培养与引进，是确保行业持续发展和提升国家网络安全水平的关键。以下是一些具体的策略建议：

（1）构建完善的教育培训体系

加强与高校的合作，鼓励高校开设与应用程序安全测试相关的课程和专业，培养具备扎实理论基础和实践能力的专业人才。组织定期的职业培训和技能提升课程，针对在职人员进行新技术、新方法的培训，提升其专业技能和应对新挑战的能力。

（2）强化实战训练

建立实战化训练平台，模拟真实环境下的安全测试场景，让学员在实践中学习和掌握安全测试技能。鼓励学员参与实际项目，通过解决实际问题来提升其综合能力和实战经验。

（3）跨学科融合培养

推动网络安全、软件开发、数据分析等多学科的交叉融合，培养具备综合素质的复合型人才。加强与国际先进教育机构的交流与合作，引进国外先进的教育理念和技术手段。

（4）建立人才认证体系

建立完善的人才认证机制，对学员的学习成果和实战能力进行评估和认证，提升其职业竞争力。推动行业认证与学历教育的互认，为学员提供更多的职业发展机会。

（5）制定优惠政策

出台一系列人才引进的优惠政策，如提供住房补贴、子女教育优惠等，吸引国内外优秀人才加入。对在应用程序安全测试领域取得突出成果的人才给予奖励和表彰，激发其创新活力。

（6）加强校企合作

鼓励企业与高校建立长期稳定的合作关系，共同培养符合企业需求的应用程序安全测试人才。企业可以通过设立奖学金、实习基地等方式，吸引更多优秀学生参与企业的研发项目。

（7）拓宽引才渠道

利用国内外人才招聘平台、专业论坛等渠道，广泛发布招聘信息，吸引更多优秀人才关注。加强与国际知名企业和研究机构的合作与交流，引进具有国际视野和丰富经验的高端人才。

3.6 我国 AST 市场存量大趋势向好

在当前全球科技竞争格局下，中美关系因素促使部分外国 AST 工具面临市场准入挑战，逐步退出中国市场，这一态势却意外地为中国本土 AST 工具的发展开辟了前所未有的广阔空间。外国品牌市场份额空间缓慢释放这一趋势为国产 AST 工具提供了更多的发展机会和市场份额。这不仅是对国产技术实力的一次考验，更是推动其快速迭代、创新升级的重要契机。

中国作为全球经济的重要引擎，其数字化经济的蓬勃发展正以前所未有的速度改变着各行各业，为 AST 市场注入了强劲的增长动力。随着企业数字化转型的深入，对应用程序安全性的需求日益迫切，AST 成为保障这一进程顺利进行的关键环节。因此，中国 AST 市场不仅处于持续增长阶段，而且展现

出巨大的发展潜力和丰富的想象空间，预示着未来市场的无限可能。

从长远来看，中国 AST 市场的向好趋势不仅体现在市场规模的持续扩大上，更在于其投资属性的日益凸显。随着政策支持的加强、技术创新的加速以及市场需求的不断释放，国产 AST 工具将迎来前所未有的发展机遇。对于投资者而言，这意味着 AST 将是充满吸引力的投资领域，一个能够分享中国数字化经济增长红利的优质赛道。

综上所述，中国 AST 市场整体未来趋势向好，发展空间巨大，投资属性优越。无论是从市场需求、政策支持还是技术创新等角度来看，都预示着该领域将迎来一个黄金发展期。对于行业参与者而言，把握这一历史机遇，积极应对挑战，创新求变，将是实现跨越发展的关键所在。

4 AST 供应商竞争力分析

4.1 供应商竞争力分析

本部分供应商将通过 Gartner 魔力象限入围的核心国外供应商以及中国信息通信研究院（后简称信通院）AST 各维度产品全景图数据进行划分与选择 [7]。本部分国外供应商厂商多维度能力数据选自 Gartner 官方数据。鉴于国内厂商官方各维度综合评分数据的空缺，本报告不对国内供应商竞争力进行数值以及梯队分析。未来，OWASP 中国将会对外发布中国 AST 供应商能力情况分析。全球 AST 系列产品核心客户所在行业包括但不限于：IT 服务、银行、金融、软件、通讯、医疗保健和生物技术、能源、政府等。客户公司量级主要分为三类：

- **全球购买 AST 系列工具需求占比最高的公司平均估值所在区间为：**$5000 万—$10 亿（3.65 亿—73 亿人民币）；
- **全球购买 AST 系列工具需求占比第二高的公司平均估值所在区间为：**$100 亿以上（730 亿人民币以上）；
- **全球购买 AST 系列工具需求占比第三高的公司平均估值所在区间为：**$10 亿—$100 亿（73 亿—730 亿人民币）

各产品评分表主要从评估和签约、集成和部署、服务与支持、产品能力这四个核心维度获取数据并且进行分析，每个维度以 0—5 分为分数区间，且该部分数据计算方式为计算出各能力维度评分的四

分位数并且通过评分数进行分组：

- 当分数 >75% 分数线时，隶属于第一梯队；
- 当分数在 50%<X<75% 的区间时，隶属于第二梯队；
- 当分数在 25%<X<50% 的区间时，隶属于第三梯队；
- 当分数 <25% 分数线时，隶属于第四梯队

注：IAST 和 DAST 部分由于供应商数量较少不足以支撑计算出四分位数，因此按照分数高低进行梯队排名。

4.1.1 SAST 厂商竞争力情况分析

Gartner 给出的 2023 年 SAST 核心产品包含 Veracode、CheckmarxSAST、Fortify Static Code Analyzer、Snyk Code 和 Coverity SAST。

表 1.SAST 产品评分表

产品名称	评估和签约	集成和部署	服务与支持	产品能力
Veracode	4.6	4.6	4.7	4.6
CheckmarxSAST	4.5	4.5	4.6	4.6
Fortify Static Code Analyzer	4.3	4.3	4.2	4.4
Snyk Code	4.5	4.5	4.7	4.5
Coverity SAST	4.4	4.3	4.5	4.5

【数据来源于 Gartner】

（1）评估和签约能力与梯度划分

- 第一梯队（分数超过 75% 线 -4.550）：Veracode
- 第二梯队（分数超过 50% 线 -4.500）：CheckmarxSAST、Snyk Code
- 第三梯队（分数超过 25% 线 -4.350）：Coverity SAST
- 第四梯队（分数未超过 25% 线）：Fortify Static Code Analyzer
- 偏度 -0.405<0，右偏，**整体 SAST 产品在评估和签约维度能力偏强**

（2）集成和部署能力与梯度划分

- 第一梯队（分数超过 75% 线 -4.550）：Veracode
- 第二梯队（分数超过 50% 线 -4.500）：CheckmarxSAST、Snyk Code
- 第三梯队（分数超过 25% 线 -4.300）：Coverity SAST、Fortify Static Code Analyzer
- 第四梯队（分数未超过 25% 线）：无
- 偏度 -0.166<0，右偏，**整体 SAST 产品在集成和部署维度能力偏强**

（3）服务与支持能力与梯度划分

- 第一梯队（分数超过 75% 线 -4.700）：Veracode、Snyk Code
- 第二梯队（分数超过 50% 线 -4.600）：CheckmarxSAST
- 第三梯队（分数超过 25% 线 -4.350）：Coverity SAST
- 第四梯队（分数未超过 25% 线）：Fortify Static Code Analyzer
- 偏度 -1.447<0，右偏，**整体 SAST 产品在服务与支持维度能力偏强**

（4）产品能力与梯度划分

- 第一梯队（分数超过 75% 线 -4.600）：Veracode、CheckmarxSAST
- 第二梯队（分数超过 50% 线 -4.500）：Snyk Code、Coverity SAST
- 第三梯队（分数超过 25% 线 -4.450）： Fortify Static Code Analyzer
- 第四梯队（分数未超过 25% 线）：无
- 偏度 -0.512<0，右偏，**整体 SAST 产品在产品能力维度能力偏强**

表 2.SAST 工具综合能力梯队分布排名

<table>
<tr><th></th><th>评估和签约</th><th>集成和部署</th><th>服务与支持</th><th>产品能力</th></tr>
<tr><td rowspan="2">第一梯队</td><td rowspan="2">Veracode</td><td rowspan="2">Veracode</td><td>Veracode</td><td>Veracode</td></tr>
<tr><td>Snyk Code</td><td>Checkmarx SAST</td></tr>
<tr><td rowspan="2">第二梯队</td><td>Checkmarx SAST</td><td>Checkmarx SAST</td><td rowspan="2">Checkmarx SAST</td><td>Snyk Code</td></tr>
<tr><td>Snyk Code</td><td>Snyk Code</td><td>Coverity SAST</td></tr>
</table>

	评估和签约	集成和部署	服务与支持	产品能力
第三梯队	Coverity SAST	Coverity SAST Fortify Static Code Analyzer	Coverity SAST	Fortify Static Code Analyzer
第四梯队	Fortify Static Code Analyzer	无	Fortify Static Code Analyzer	无

【数据来源于 Gartner】

从上表数据分析，Veracode 在 SAST 工具的综合能力上表现尤为突出，其在评估的四个关键维度上均稳居第一梯队，展现出全面领先的优势。而在产品能力维度上，Checkmarx SAST 与 Veracode 并驾齐驱，两者均被视为 SAST 领域内产品能力最强的代表，各自以卓越的性能和丰富的功能赢得了市场的广泛认可。

4.1.2 IAST 厂商竞争力情况分析

Gartner 给出的 2023 年 IAST 核心产品包含 FortifyWebInspect IAST 和 Seeker IAST。

表 3.IAST 产品评分表

产品名称	评估和签约	集成和部署	服务与支持	产品能力
FortifyWebInspect IAST	4.5	4.0	4.0	4.0
Seeker IAST	4.0	4.5	4.7	4.4

【数据来源于 Gartner】

（1）评估和签约能力与梯度划分

- 第一梯队（分数超过 50% 线 -4.250）：Fortify WebInspect IAST
- 第二梯队（分数超过 25% 线 -4.000）：Seeker IAST

（2）集成和部署能力与梯度划分

- 第一梯队（分数超过 50% 线 -4.250）：Seeker IAST
- 第二梯队（分数超过 25% 线 -4.000）：Fortify WebInspect IAST

（3）服务与支持能力与梯度划分

- 第一梯队（分数超过 50% 线 -4.350）：Seeker IAST
- 第二梯队（分数超过 25% 线 -4.000）：Fortify WebInspect IAST

（4）产品能力与梯度划分

- 第一梯队（分数超过 50% 线 -4.200）：Seeker IAST
- 第二梯队（分数超过 25% 线 -4.000）：Fortify WebInspect IAST

表 4.IAST 工具综合能力梯队分布排名

	评估和签约	集成和部署	服务与支持	产品能力
第一梯队	Fortify WebInspect IAST	Seeker IAST	Seeker IAST	Seeker IAST
第二梯队	Seeker IAST	Fortify WebInspect IAST	Fortify WebInspect IAST	Fortify WebInspect IAST
第三梯队	无	无	无	无
第四梯队	无	无	无	无

【数据来源于 Gartner】

从上述数据可见，Seeker IAST 在集成和部署、服务与支持、产品能力方面均胜于 Fortify WebInspect IAST。

4.1.3 DAST 厂商竞争力分析

Gartner 给出的 2023 年 DAST 核心产品包含 WhiteHat Dynamics、Appscan 和 FortifyWebInspect。

表 5.DAST 产品评分表

产品名称	评估和签约	集成和部署	服务与支持	产品能力
WhiteHat Dynamics	4.5	4.5	4.6	4.5
AppScan	4.5	4.4	4.5	4.5
FortifyWebInspect	4.2	4.3	4.3	4.5

【数据来源于 Gartner】

（1）评估和签约能力与梯度划分

- 第一梯队（分数超过 50% 线 -4.500）：WhiteHat Dynamics、AppScan
- 第二梯队（分数超过 25% 线 -4.200）：Fortify WebInspect

（2）集成和部署能力与梯度划分

- 第一梯队（分数超过 50% 线 -4.400）：WhiteHat Dynamics、AppScan
- 第二梯队（分数超过 25% 线 -4.300）：Fortify WebInspect

（3）服务与支持能力与梯度划分

- 第一梯队（分数超过 50% 线 -4.500）：WhiteHat Dynamics、AppScan
- 第二梯队（分数超过 25% 线 -4.300）：Fortify WebInspect

（4）产品能力与梯度划分

- 产品能力相同

表 6.DAST 工具综合能力梯队分布排名

	评估和签约	集成和部署	服务与支持	产品能力
第一梯队	WhiteHat Dynamics	WhiteHat Dynamics	WhiteHat Dynamics	持平
	AppScan	AppScan	AppScan	
第二梯队	Fortify WebInspect	Fortify WebInspect	Fortify WebInspect	持平
第三梯队	无	无	无	无
第四梯队	无	无	无	无

【数据来源于 Gartner】

从上表信息可见 WhiteHat Dynamics 和 AppScan 在所有维度均稳定处于国外 DAST 市场产品第一梯队，等级划分较为明显稳定。

4.1.4 SCA 厂商竞争力分析

Gartner 给出的 2023 年 SCA 核心产品包含 Sonatype LifeCycle、Mend.io、BlackDuck SCA、Snyk Open Source、Checkmarx SCA。

表 7.SCA 产品评分表

产品名称	评估和签约	集成和部署	服务与支持	产品能力
Sonatype LifeCycle	5.0	4.7	5.0	4.3
Mend.io	4.3	4.1	4.4	4.1
BlackDuck SCA	4.4	4.4	4.5	4.5
Snyk Open Source	4.7	4.7	4.7	4.5
Checkmarx SCA	4.4	4.6	4.9	4.7

【数据来源于 Gartner】

（1）评估和签约能力与梯度划分

- 第一梯队（分数超过 75% 线 -4.850）：Sonatype Lifecycle
- 第二梯队（分数超过 50% 线 -4.400）：Snyk Open Source、BlackDuck SCA、Checkmarx SCA
- 第三梯队（分数超过 25% 线 -4.350）：无
- 第四梯队（分数未超过 25% 线）：Mend.io
- 偏度 1.083>0，左偏，**整体 SCA 产品在评估和签约维度能力偏弱**

（2）集成和部署能力与梯度划分

- 第一梯队（分数超过 75% 线 -4.700）：Sonatype LifeCycle、Snyk Open Source
- 第二梯队（分数超过 50% 线 -4.600）：Checkmarx SCA
- 第三梯队（分数超过 25% 线 -4.250）：BlackDuck SCA
- 第四梯队（分数未超过 25% 线）：Mend.io
- 偏度 -1.207<0，右偏，**整体 SCA 产品在集成和部署维度能力偏强**

（3）服务与支持能力与梯度划分

- 第一梯队（分数超过 75% 线 -4.950）：Sonatype Lifecycle
- 第二梯队（分数超过 50% 线 -4.700）：Checkmarx SCA、Snyk Open Source

- 第三梯队（分数超过 25% 线 -4.450）：BlackDuck SCA
- 第四梯队（分数未超过 25% 线）：Mend.io
- 偏度 =0，正态分布，**整体 SCA 产品在服务与支持维度能力持平**

（4）产品能力与梯度划分

- 第一梯队（分数超过 75% 线 -4.600）：Checkmarx SCA
- 第二梯队（分数超过 50% 线 -4.500）：BlackDuck SCA、Snyk Open Source
- 第三梯队（分数超过 25% 线 -4.200）：Sonatype LifeCycle
- 第四梯队（分数未超过 25% 线）：Mend.io
- 偏度 -0.405<0，右偏，**整体 SCA 产品在产品能力维度能力偏强**

表 8.SCA 工具综合能力梯队分布排名

<table>
<tr><th>产品名称</th><th>评估和签约</th><th>集成和部署</th><th>服务与支持</th><th>产品能力</th></tr>
<tr><td rowspan="2">第一梯队</td><td rowspan="2">Sonatype Lifecycle</td><td>SonatypeLifeCycle</td><td rowspan="2">Sonatype Lifecycle</td><td rowspan="2">Checkmarx SCA</td></tr>
<tr><td>Snyk Open Source</td></tr>
<tr><td rowspan="3">第二梯队</td><td>Snyk Open Source</td><td rowspan="3">Checkmarx SCA</td><td rowspan="2">Checkmarx SCA</td><td rowspan="2">BlackDuck SCA</td></tr>
<tr><td>BlackDuck SCA</td></tr>
<tr><td>Checkmarx SCA</td><td>Snyk Open Source</td><td>Snyk Open Source</td></tr>
<tr><td>第三梯队</td><td>无</td><td>BlackDuck SCA</td><td>BlackDuck SCA</td><td>SonatypeLifeCycle</td></tr>
<tr><td>第四梯队</td><td>Mend.io</td><td>Mend.io</td><td>Mend.io</td><td>Mend.io</td></tr>
</table>

【数据来源于 Gartner】

从上表信息可见 SCA 厂商综合能力较为接近，各有千秋。其中 Sonatype Lifecycle 在产品能力方面表现较为弱势，但是其他维度均处于行业领先水平。Checkmarx SCA 和 Snyk Open Source 从各维度来看并无明显短板，属于综合实力拔尖的产品。Synopsys BlackDuck SCA 产品综合能力排名相较于 2022 年其处在第一梯队的表现而言出现下滑，竞争力明显减弱。

4.2 全球供应商战略及并购情况分析

根据网安加社区的深入调研数据，Synopsys 单一企业即斥资高达 88.11 亿人民币用于收购 AST 工具供应商，若综合考量其他核心供应商的收购金额，整体投入已远超百亿人民币规模，专注于并购杰出的 AST 解决方案提供商。这一巨额投资不仅凸显了 AST 供应商在业界的核心价值与不可替代性，更预示着 AST 领域正迎来前所未有的发展机遇与广阔前景。

4.2.1 Synopsys

Synopsys 产品决策路线选择以收购为主。其市场远见性高，执行能力强。其对 AST 市场发展的布局早，收购行动迅速。此外 Synopsys 对市场的反应速度也较快，2021 年起全球市场客户重点购买 SaaS 形态产品，Synopsys 于 2022 年完成 SaaS 形态产品能力提升相关收购行动。

表 9.Synopsys 历史收购动态

年份	被收购公司以及收购核心能力	收购金额
2022	WhiteHat Security（提升 SaaS 以及 DAST 能力）	$3.3 亿（约￥24 亿）
2021	Code Dx（加速软件漏洞的发现，优先级排序和修复）	未披露
2020	Tinfoil Security（DAST 和 API 安全测试解决方案）	未披露
2017	Black Duck Software(SCA、保护和管理开源软件的自动化解决方案）	$5.47 亿（约￥39.8 亿）
2017	Forcheck*(检测 Fortran 应用程序中的编码缺陷和异常的 SAST）	未披露
2016	Codiscope（产品简化 & 转型）	未披露
2016	Cigital（识别、修复和防止软件应用程序中的漏洞的托管服务）	未披露
2015	Goanna Software（SAST）	未披露
2015	Protecode（SCA）	未披露
2015	Seeker* (from Quotium)（IAST）	未披露
2015	Codenomicon（专注于芯片和设备中嵌入的软件的安全）	未披露
2014	Kalistick（基于云的软件解决方案提供商）	未披露
2014	Coverity（SAST）	$1.34 亿 (约 ¥9.75 亿) 以及 $2 亿 (约 ¥14.56 亿）债务组合，合计 3.34 亿美金（¥24.31 亿）

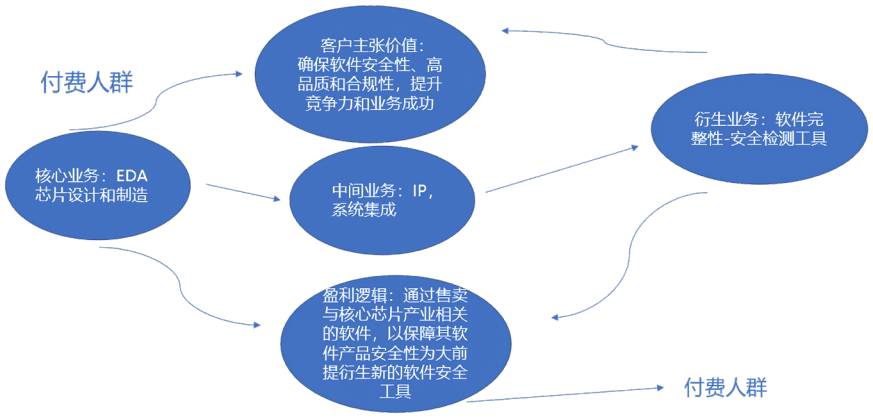
【数据来源于 Synopsys】

（1）商业逻辑

通过收购方式扩充旗下产品线完整性，强化自身的产品能力，并扩大市场的规模及用户基数；

通过硬件、系统软件以及安全检测工具三大核心业务形成闭环产业、优化价值链、赋能营运、提高效率。

图 13.Synopsys 商业逻辑

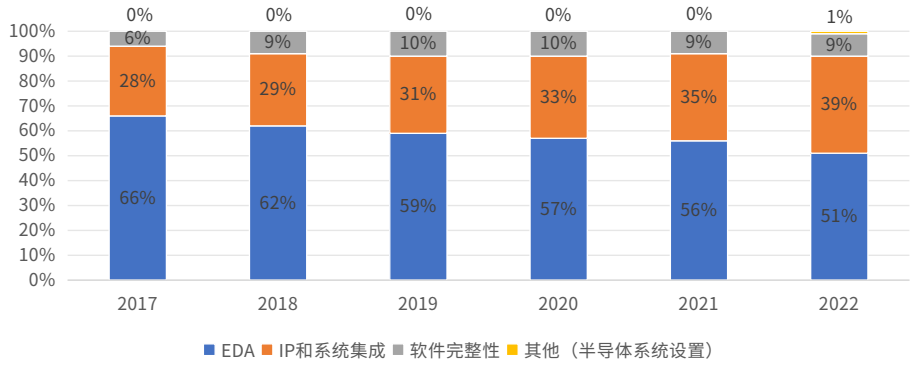


（2）主要营收板块

Synopsys 主要营收板块有三大部分：EDA、IP 和系统设计、软件完整性。其中软件完整性包含其公司应用程序安全测试类产品的静态应用程序安全测试、软件成分分析和动态应用程序安全测试工具以及解决方案帮助客户在软件开发周期的任何阶段，以及在整个供应链中，把安全性和质量编入其软件代码中，从而使风险最小，并最大限度提高应用开发的速度。

Synopsys 主营业务收入占比方面，EDA 软件是公司的核心业务，占比近六成，IP 授权和系统集成、软件完整性业务增长较快，占比有所提升。

图 14.2017—2022 年 Synopsys 各产品类目收入占比



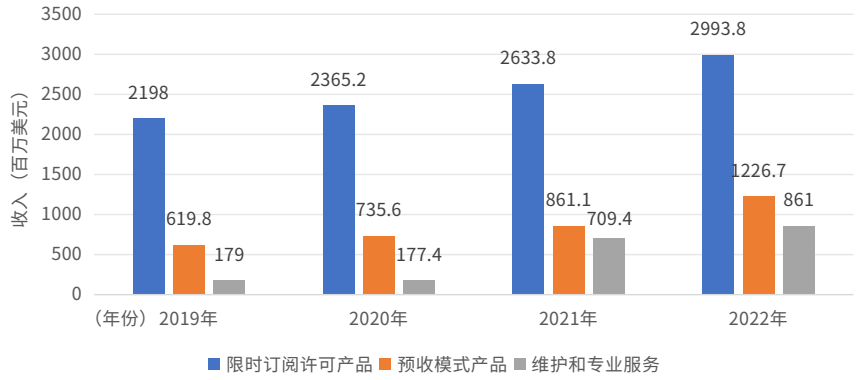
【数据来源于 Synopsys】

（3）盈利模式

根据不同业务的特点，Synopsys 采取了以下三种盈利模式：

- 限时许可模式：通过发放 license 的方式，根据合同履行时间的比例进行确认，通常合同期限为 3 年。2022 年这种方式收入确认占比 59%；
- 预收模式：针对 IP 和硬件的销售，通过预收的方式进行确认。2022 年这种方式收入确认占比 24%；
- 维护和专业服务收费模式：维护和服务通过合同进行确认。2022 年这种方式收入确认占比 17%。

图 15.Synopsys 不同收费模式的收入对比

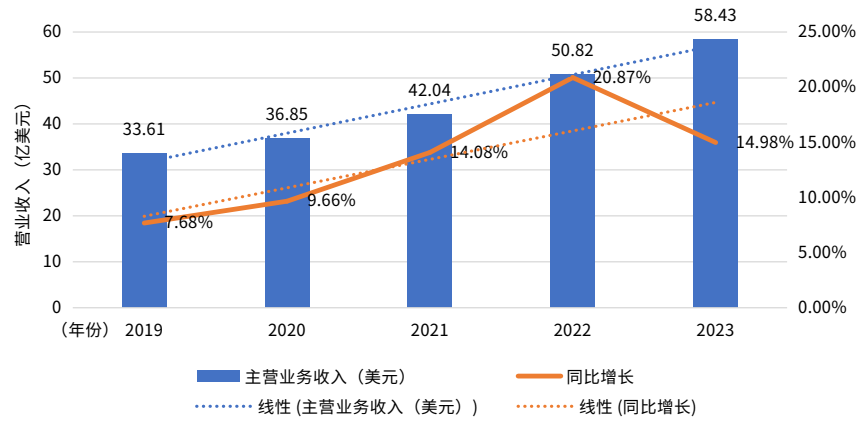


【数据来源于 Synopsys】

（4）盈利情况分析

Synopsys 2023 年营收超过 58 亿美元（约 426.5 亿人民币），长期保持稳定增长，2019 年到 2023 年同比增长分别为 7.68%、9.66%、14.08%、20.87% 以及 14.98%。从下图的趋势线可看出，无论是年营收总额还是同比增长率均呈上升趋势。此外，Synopsys 2024 年第一季度（截至 4 月 30 日）的总营收额为 14.55 亿美元，同比增长 15.2%。

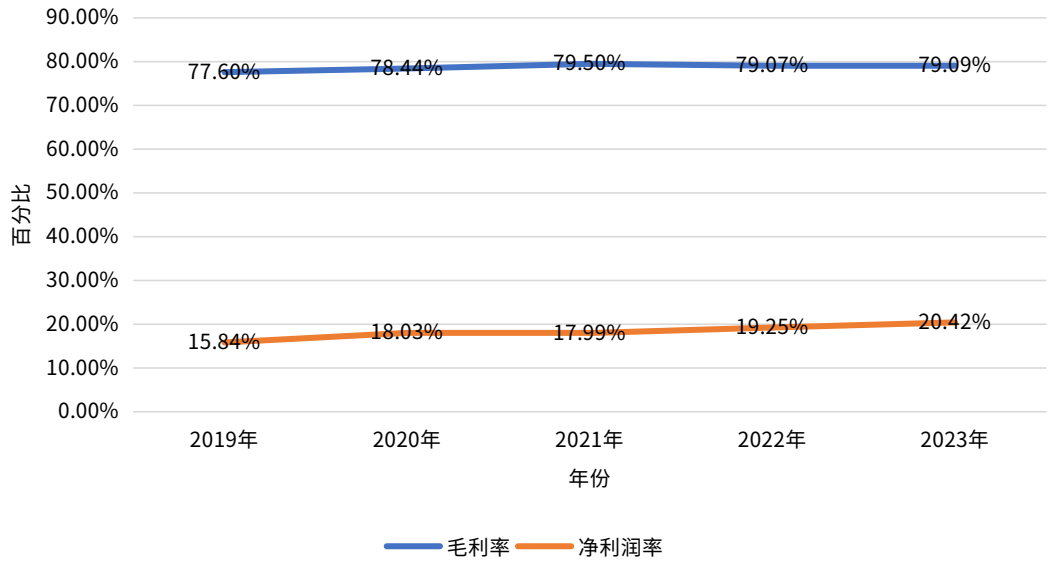
图 16.2019—2023 年 Synopsys 营业收入



【数据来源于 Synopsys】

Synopsys 毛利率稳定在 79% 左右，整体十分稳定并且保持较高水平。净利润率整体稳中有升。

图 17.Synopsys 2019 年—2023 年盈利能力



【数据来源于 Synopsys】

4.2.2 Snyk

Snyk 主要产品决策路线以收购为主，并且具备极强的市场判断力和执行力。Snyk 并未将业务线拓宽到覆盖大部分 AST 领域，而是选择最核心的四块领域进行投资发展，因此可以将投入资源做到集中最大化。Snyk 不同于 Synopsys 的战略思维在于其通过收购的方式对自身已有产品本身以及解决方案的能力进行进一步提升。

表 10.Snyk 历史收购动态

年份日期	被收购公司以及收购核心能力
2023/06/07	Enso Security（Application Security Posture Management 应用程序安全状况 ASPM）解决方案商
2022/05/07	TopCoat Data（数据分析）
2022/02/17	Fugue（云安全以及合规）
2021/10/28	CloudSkiff（IaC）
2021/05/12	FossID（SCA）

年份日期	被收购公司以及收购核心能力
2021/01/27	Manifold.co（构建和自动化安全开发者工作流）
2020/09/23	DeepCode（机器学习技术 & 实时语义代码分析，加深 SCA、容器安全、IaC 安全的漏洞识别准确性）
2019/07/24	DevSecCon Limited（DevSecOps）

【数据来源于 Snyk】

（1）商业逻辑

Synk 的客户价值主张在于提供自动化漏洞发现和修复、持续安全性和合规性、降低开发时间和成本以及客户支持和咨询服务。通过价值主张帮助客户保护其应用程序免受开源组件漏洞和风险威胁，并提高其开发效率和软件质量。Snyk 通过收购强化自身的产品能力，并扩大市场的规模及用户。Snyk 采用 PLG 自下而上的销售模式，使产品易于提供给终端用户，当用户采用产品时，会将其传播给组织内外的其他组织，因此其产品是销售增长的主要驱动力。

（2）主要营收板块

- **许可和订阅：**Synk 提供许可和订阅服务，让客户可以使用他们的软件和工具进行开源软件的安全评估和漏洞管理这些许可和订阅费用是主要收入来源。
- **安全验证和漏洞管理：**Synk 提供用于对开源软件进行安全验证和漏洞管理的工具和服务。他们的产品可以帮助企业发现和修复开源软件中的漏洞和安全风险，以保护其应用程序和系统的安全。
- **安全咨询和支持：**Synk 提供安全咨询和服务，帮助客户制定和实施开源软件安全策略，并提供专业知识和指导。咨询和支持服务可以根据客户需求进行定制，并为 Synk 提供额外的收入来源。
- **漏洞情报和威胁情报：**Synk 提供有关开源软件漏洞和威胁的情报和警报。这些情报可以帮助客户及时了解并应对开源软件的安全问题，提供更全面的安全保护。
- **企业制定解决方案：**Synk 提供定制化的开源软件安全解决方案，以满足客户特定的安全需求。这些解决方案可以根据客户的业务和技术要求进行定制，为 Synk 带来额外的营收机会。

（3）盈利模式

Synk 的商业盈利模式主要基于以下几个维度：

- **安全风险以及资产管理：**开源软件漏洞检测服务、漏洞管理平台和安全顾问服务的销售和订阅，通过帮助企业提供开源软件安全性的可视化和管理，Synk 致力于提高企业的软件安全性和减少潜在的风险。
- **订阅服务：**Synk 提供基于订阅的服务模式，客户可以按照不同订阅级别选择订阅 Synk 的产品和解决方案。
- **企业许可证：**Synk 为企业客户提供定制化的许可证，使其能够在内部部署和使用 Synk 的软件管理工具。
- **数据和情报服务:** Synk 提供数据和情报服务，为客户提供有关软件漏洞和安全风险的实时信息。

（4）盈利情况分析

- 2020 财年结束时 Snyk 收入同比增长 200%；
- 2021 年 Snyk 总收入为 0.58 亿美元；
- 2022 年 Synk 总收入为 1.47 亿美元，相较于 2021 年总收入达到了 153% 的收入同比增长。Snyk 于 2022 年实现了 130% 的净留存收益率和 90% 的毛留存收益率。

4.2.3 Checkmarx

Checkmarx 主要产品决策路线以自研为主。不通过收购产品的方式，以自研产品为主，产品形式以 SaaS 模式为重心，核心主攻 AST 系列产品以及软件供应链安全。

表 11.Checkmarx 历史收购动态

年份日期	被收购公司以及收购核心能力	收购金额
2021/08/05	Dustico（基于 SaaS 的解决方案，可检测开源软件供应链中的恶意攻击和后门 & 机器学习技术）	未披露

【数据来源于 Checkmarx】

（1）商业逻辑

- **市场需求：**随着软件在各行各业的广泛应用，软件安全问题日益突出，企业和组织对其保护关键业务数据和用户隐私需求不断增加，利用这一市场需求，提供全面的软件安全解决方案。

- **技术优势：**Checkmarx 用于 SAST、DAST、SCA 等技术通过深入的代码分析和漏洞检测，快速准确地发现潜在的安全问题。技术优势让 Checkmarx 在软件安全领域具备竞争优势。
- **客户价值主张：**Checkmarx 的产品和解决方案帮助客户提升软件安全性，减少安全漏洞的风险，并保护企业的信誉和品牌形象。通过使用 Checkmarx 的工具和服务，客户可以更好地满足法律法规的要求，提高软件开发效率，避免业务中断。

（2）主要营收板块

Checkmarx 的核心营收板块包括静态应用安全测试（SAST）工具、动态应用安全测试（DAST）工具、软件成分分析（SCA）工具以及云原生安全解决方案。

（3）盈利模式

- **软件许可和订阅：**Checkmarx 通过销售软件许可和订阅模式来获取收入。客户可以购买软件许可或者按照一定周期进行订阅，以使用 Checkmarx 提供的安全测试和分析功能。
- **专业服务和咨询：**除了软件产品，Checkmarx 还提供专业服务和咨询，为客户提供实施、培训、定制化开发和技术支持等服务。
- **云服务：**Checkmarx 提供基于云的软件安全解决方案，客户可以通过订阅模式使用这些云服务。这种模式可以帮助客户简化部署和维护的工作，同时提供更加灵活和可拓展的解决方案。

4.2.4 Rapid 7

Rapid 7 主要产品决策路线以收购为主，并且市场主攻方向不同。其核心发展云安全、容器安全、威胁情报分析处理、网络流量监控、安全编排以及自动化等，以应用程序动态安全为主。核心相关产品为 DAST 以及 RASP。

表 12.Rapid 7 历史收购动态

年份日期	被收购公司以及收购核心能力	收购金额
2023/03/15	Minerva Labs（反逃避和勒索软件预防技术的领先提供商）	$3800 万
2021/07/19	InSights Cyber Intelligence Ltd.（情境化的外部威胁情报和主动威胁修复）	$3.35 亿
2021/04/21	Velociraptor（用于端点监控、数字取证和事件响应的领先开源技术和社区）	未披露
2021/01/31	Alcide（K8s 安全）	$5000 万

年份日期	被收购公司以及收购核心能力	收购金额
2019/04/02	NetFort（一家跨云、虚拟和物理网络提供端到端网络流量可见性和分析的公司）	未披露
2018/10/15	tCell.io（Web 应用程序威胁防御和监控 RASP）	未披露
2017/07/18	Komand（安全编排以及自动化）	$5000 万
2015/10/13	Logentries（基于云的日志管理和机器数据搜索技术）	$6800 万
2012/10/09	Mobilisafe（移动风险管理）	未披露
2009/10/20	Metasploit（渗透测试）	未披露

【数据来源于 Rapid 7】

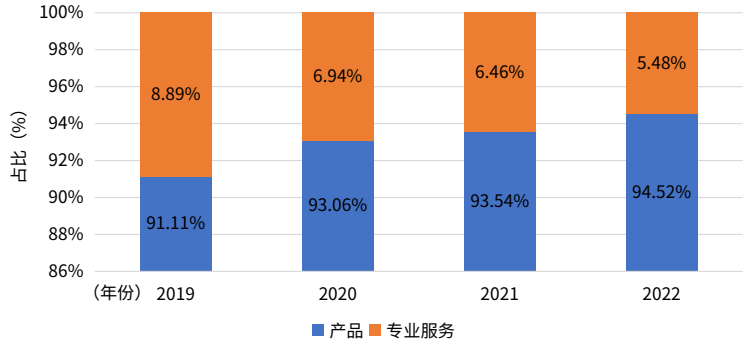
（1）商业逻辑

- Rapid 7 基于综合安全解决方案、创新的技术和工具、数据驱动的安全分析以及优质的客户服务。通过整合这些要素，为客户提供全面的安全保护，帮助他们发现和应对威胁，保护关键资产和业务安全。
- 通过收购强化自身的产品能力，并扩大市场的规模及用户。
- Rapid 7 的客户价值主张体现在综合的安全保护、实时的安全洞察、高效的安全管理以及个性化的支持与服务上。通过提供这些价值，Rapid 7 帮助客户降低安全风险、保护关键业务数据和用户隐私，并提高安全运营的效率与效果。

（2）主要营收板块

- Rapid 7 主要营业收入中产品占据九成以上，主营业务收入逐年上升，营业利率呈缓慢上升状态。

图 18.2019—2022 年 Rapid 7 主营业务收入占比



【数据来源于 Rapid 7】

（3）盈利模式

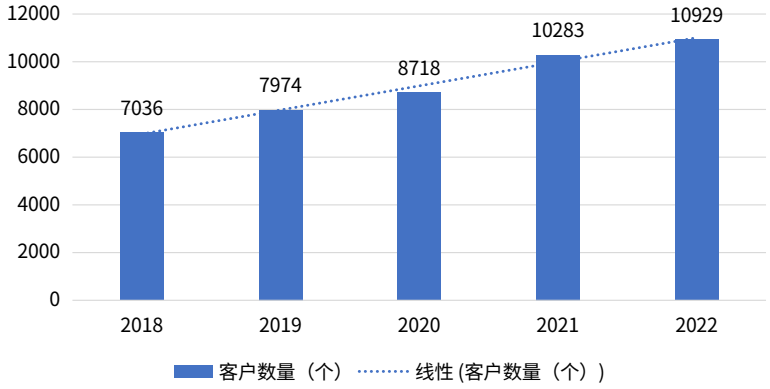
Rapid7 的商业模式通过许可和订阅服务、云服务、专业服务、增值功能和附加产品以及合作伙伴关系来为公司创造收入。公司积极满足客户对网络安全的需求，并持续创新和改进其产品和服务以适应不断变化的威胁环境。

- **订阅服务：**Rapid7 提供基于订阅的软件服务，客户可以基于自身解决方案的需要选择 Rapid 7 的不同订阅级别。
- **云服务：**Rapid 7 通过云平台提供托管的安全解决方案。
- **专业服务：**Rapid 7 提供专业服务包括咨询，实施和培训等。

（4）盈利情况分析

在 2018—2022 年期间内，Rapid 7 客户数量以 12% 的年复合增长率进行增长，如下图所示：

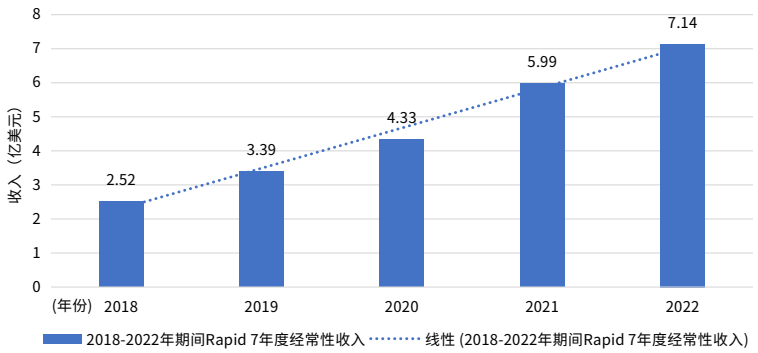
图 19.2018—2022 年期间 Rapid 7 客户数量



【数据来源于 Rapid 7】

Rapid 7 年度经常性收入年复合增长率为 30%。

图 20.2018—2022 年期间 Rapid 7 年度经常性收入



【数据来源于 Rapid 7】

5 应用程序安全测试行业技术发展趋势

5.1 AI 与机器学习在 AST 中的应用

AI 技术的普及，智能化测试已经不再是新鲜概念，而是成为软件安全测试行业的常态。通过集成先进的算法和模型，AST 工具能够学习历史数据，预测并识别潜在的软件缺陷，提高测试的准确性和效率。AI 和机器学习技术的应用有助于降低 AST 过程中的误报率和漏报率。通过智能分析和学习，工具能够更准确地识别真正的安全漏洞，减少无效警报的干扰，提高测试结果的可靠性。同时，AI 驱动的 AST 工具能够实时适应新的安全威胁和攻击模式。随着网络攻击手段的不断变化，AI 技术能够自动更新和优化测试策略，确保应用程序的安全防护始终保持在最前沿。AI 技术同样可以适用于自动化测试，这种测试方式能够自动化完成更多的测试任务，减少手动测试的需求，提高测试效率并降低成本。

5.2 新型测试工具与方法的涌现

（1）多模态测试

随着多模态人工智能技术的发展，多模态测试方法将逐渐兴起。这种测试方法能够处理多种类型的数据输入，提高测试的全面性和准确性。多模态测试将结合文本、图像、视频、音频等多种模态的信息，对应用程序进行全面、深入的测试。这种测试方法能够更真实地模拟用户行为和环境，提高测试的全面性和有效性。随着技术的发展，多模态测试将更加注重不同模态之间的融合和协同，以实现更高效的测试覆盖和更准确的漏洞发现。

（2）区块链测试

区块链技术以其去中心化、透明性和不可篡改性等特点，在金融科技、供应链管理等领域得到广泛应用。区块链测试则是针对区块链系统进行的专项测试，以确保其安全性、稳定性和性能。随着区块链技术的广泛应用，区块链测试将成为 AST 领域的一个重要方向。区块链测试将重点关注区块链系统的安全性、稳定性和性能，确保区块链应用在各种场景下的可靠运行。

（3）无代码 / 低代码测试平台

为了降低测试门槛并提高测试效率，无代码 / 低代码测试平台将得到更广泛地应用。这些平台提供直观的界面和易用的工具，通过图形化界面和预配置的测试模板，降低了测试门槛和复杂度，使非

技术人员也能轻松进行应用程序安全测试。在未来，这些平台将更加注重用户体验和易用性，提供更多定制化的测试模板和案例库，以满足不同企业和组织的需求。同时，它们还将加强与其他测试工具和流程的集成化，提高测试的自动化水平。

（4）自动化渗透测试技术

自动化渗透测试系统被无缝集成到公司的持续集成 / 持续部署（CI/CD）流程中，成为开发周期中不可或缺的一环。每当有新的代码提交或功能更新时，系统便自动启动，模拟真实世界中的黑客攻击场景，对应用程序进行全面的安全扫描和渗透测试。

这些测试不仅覆盖了传统的 Web 应用漏洞，如 SQL 注入、跨站脚本（XSS）等，还深入探索了 API 接口、微服务之间的通信协议以及新兴技术如区块链集成等方面的潜在安全弱点。通过集成 AI 和机器学习算法，系统能够智能分析历史渗透测试数据，不断学习和进化，以预测并识别新出现的攻击模式。

随着测试的进行，自动化渗透测试工具迅速发现了应用中的几个关键漏洞，包括未经验证的输入处理不当、敏感信息泄露以及不当的权限管理。得益于与 CI/CD 流程的紧密集成，这些问题被即时反馈给开发团队，促使他们迅速响应并修复漏洞。

更值得一提的是，这款自动化渗透测试工具还具备自我优化能力。在每次测试后，它都会根据测试结果自动调整测试策略和参数，确保下一次测试更加精准高效。这种智能化的迭代机制，不仅极大地提高了测试效率，还使得安全测试更加全面无遗漏。

6 结论与建议

6.1 对行业发展的建议

在加速 AST 行业发展的征途上，我们应紧扣三大核心策略。首先，加强技术创新，积极进行产学研合作。通过加大科研投资，积极引入人工智能、机器学习等前沿技术，提升 AST 工具的智能化与自动化效能。同时，构建产学研紧密合作的桥梁，促进技术交流，携手制定统一行业标准，增强系统间的互操作性，打破技术壁垒。

其次，需拓宽应用领域，精准对接市场需求。针对金融、医疗、电商等各行业独特的安全挑战，

定制化 AST 解决方案，确保应用安全无虞。紧跟云计算、物联网等新兴技术步伐，挖掘 AST 在新兴领域的新机遇，拓展服务边界。此外，深化市场教育与推广，提升行业知名度，激发更广泛的市场需求。

最后，严守法规红线，确保合规运营。紧密跟踪国内外数据安全与隐私保护法规的最新动态，确保 AST 服务严格遵循法律框架。在测试流程中嵌入合规性验证环节，保障应用程序的安全与合规双重达标。构建全面的合规管理体系，将合规理念深植于产品研发生命周期的每一环节，为企业提供坚实可靠的合规后盾。

6.2 对投资者的建议

6.2.1 投资价值

全球 AST 市场规模正以稳定且较快的速度增长，展现出强劲的市场活力。尤为显著的是亚太地区，特别是中国市场，其市场份额显著提升，已跃居全球第二大市场地位，彰显出该地区对应用程序安全测试需求的蓬勃增长。在中国，AST 市场呈现出多元化与竞争激烈的态势，众多企业竞相角逐，市场集中度相对较低，这种百花齐放、百家争鸣的现象正是 AST 市场健康发展的良好兆头。此外，国外厂商的缓步退出所让出的市场份额以及待发掘的巨大市场空间，无一不预示着市场潜力的进一步释放和行业的持续繁荣。

此外，新技术的不断涌现为 AST 行业注入了新的活力，为解决长期以来困扰行业的难题提供了更多创新思路和解决方案。这些技术不仅提升了测试的准确性、效率与全面性，还推动了 AST 工具与流程的智能化、自动化发展。因此，从投资角度来看，AST 市场蕴含着巨大的潜力与机遇，对于寻求高成长性的投资者而言，无疑是一个值得深入挖掘的宝藏之地。

6.2.2 投资方向

投资者可将目光聚焦在技术创新型企业，投资那些将 AI 和机器学习技术深度集成到 AST 工具中的企业。这些技术能够显著提升测试的准确性和效率，是未来 AST 市场的重要发展方向。另外支持持续集成与持续部署（CI/CD）流程的自动化 AST 工具具有广阔的市场前景，投资这类工具可以帮助企业提高开发效率和产品质量。此外，投资者可以关注核心客户为金融和医疗行业的供应商，这些行业对应用程序的安全性要求极高，且市场规模庞大，并且存在法律法规等强监管要求。

随着云计算和物联网技术的普及，相关应用程序的安全性问题日益凸显。投资于针对这些新兴技术领域的 AST 工具或解决方案供应商也将会是较好的投资方向，具有较大的市场潜力。此外，在数据

保护和隐私安全法规的不断完善、企业对合规性解决方案的需求日益增加的大趋势下，具备提供全面合规性测试和安全咨询服务的 AST 企业也将是较佳的投资选择。

6.2.3 风险控制

在投资前，务必深入了解企业的技术实力、研发团队和核心专利等情况，确保所投资的企业在 AST 领域具有核心竞争力，以避免技术风险。分析市场竞争格局，了解主要竞争对手的市场份额、产品特点和发展战略。选择具有差异化竞争优势的企业进行投资，以降低市场竞争风险。确保所投资的企业在产品开发和服务提供过程中严格遵守相关法规要求。避免因合规性问题导致的法律风险和财务损失。密切关注 AST 行业的最新动态和政策变化，及时调整投资策略以应对潜在的市场风险。同时，保持与行业协会、研究机构等组织的联系，获取最新的行业资讯和趋势分析。

不要将所有资金集中在单一企业或单一领域上，通过多元化投资组合来分散风险，确保整体投资回报的稳定性。AST 行业属于高技术壁垒和高成长性的行业，需要耐心等待企业的成长和市场的成熟。建议投资者保持长期持有的心态，关注企业的长期发展潜力和价值创造。

7 参考文献

[1]《Application Security Testing (AST) Tools - Global Market Share and Ranking, Overall Sales and Demand Forecast 2024-2030》，QY Research

[2]《安全测试市场规模和份额分析 - 增长趋势和预测，2024 - 2029》，Mordor Intelligence

[3]《应用程序安全市场规模和份额分析 - 增长趋势和预测，2024 - 2029》, Mordor Intelligence

[4]《Application Security Market Size, Share & Trends Analysis Report》,Grand View Research

[5]《IDC 全球网络安全支出指南》，IDC

[6]《Survey reveals AI's impact on the developer experience》，GitHub

[7]《2024 中国 DevOps & BizDevOps 现状调查报告》，中国信通院

8 编写单位介绍

《中国信息安全》杂志社

中国信息安全杂志社是由中国信息安全测评中心主办的部级期刊，创刊于 2010 年，出版周期为月刊，出版地为北京。该杂志主要栏目包括卷首语、网际时政、网事焦点、网域前沿、网境纵横、网络空间战略论坛、网业创新、网安测评等，涵盖了信息安全领域的各个方面，包括国内外信息安全战略政策、法规和标准的发展动态，以及信息安全领域的研究报告与白皮书。此外，杂志还关注信息安全技术前沿，介绍最新的安全技术和解决方案，并分享企业和机构在信息安全管理方面的成功经验和教训。

中国信息安全杂志社注重学术质量，努力吸引高质量论文，为信息安全与技术领域的发展建设与科研成果传播做出贡献。该杂志被中国知网、万方数据库、维普网等收录，具有一定的学术影响力和社会认可度。此外，中国信息安全杂志社还面向全国高校招募优秀实习生，成功入选的实习生将直接参与重点课题研究、策划国内重要网络安全会议等活动，为有意从事信息安全领域工作的学生提供了宝贵的实践机会。

武汉金银湖实验室

武汉金银湖实验室成立于 2022 年 11 月，位于国家网络安全人才与创新基地，是由武汉市人民政府批复设立的独立事业法人单位，举办单位是武汉临空港经济技术开发区管理委员会、武汉市东西湖区人民政府，委托华中科技大学牵头管理运行，武汉大学和中国船舶集团有限公司第七〇九研究所参与管理，是网络空间安全领域的新型研发机构。截至目前，武汉金银湖实验室已经确立了智能化软件安全、光通信安全、密码理论与应用以及云系统安全四个重点研究方向。

武汉金银湖实验室聚焦国家网络空间安全领域的重大使命和战略需求，以提升网络空间安全领域原始创新能力、突破网络安全产业发展关键技术瓶颈为使命，打造战略性、前瞻性、基础性科技创新的综合性网络空间安全领域科研平台，建成具有国际一流水准的创新高地，形成支撑网安产业可持续发展的核心能力。通过发挥高校学科集群优势、加强前沿基础理论探索、提升核心技术研发能力，打通人才—创新—产业链，提升网安原始创新能力，助力网络安全产业升级，加快国家网络安全人才与创新基地发展。

深圳市网络与信息安全行业协会

深圳市网络与信息安全行业协会（Shenzhen Network and Information Security Trade Association，缩写 SNISA）是 2014 年 7 月 25 日经深圳市民政局批准成立，具有独立法人资格的非营利性社会团体。

协会宗旨是以深圳市网络与信息安全领域企业为主体，以平等互利、优势互补、资源共享、合作共赢为原则，推动产业发展资源整合，优化环境，倡导行业自律，推动协会会员单位间信息沟通、业务合作，推进深圳市网络与信息安全保障体系的建设，协调与市业务主管部门的交流与沟通，促进网络与信息安全行业发展，提高深圳网络与信息安全行业的国际化水平。

协会业务范围包括：行业管理、信息交流、市场调查、组织调研、国际合作、教育培训、行业认证、商务会展、编辑出版等，咨询和中介服务，承办政府委托事项等。

OWASP 中国

OWASP 作为一个全球性的非营利性组织，致力于推动软件安全性的前沿发展。OWASP 构建了一个由社区驱动的开源生态系统，涵盖代码库、详尽文档及标准化框架，旨在为全球用户提供坚实的安全基石。目前，OWASP 拥有超过 250 个分会，汇聚了数万名安全领域的专业人士与爱好者。OWASP 专注于提供专业论坛与培训活动，通过知识的共享与技术的交流，能够赋能更多组织，助力他们在构思、开发、采购、运维及保障应用程序的全生命周期中，构建出值得信赖的、安全的数字环境。OWASP 中国是中国大陆本地分会，旨在推动了安全标准、安全测试工具、安全指导手册等应用安全技术在中国的发展。

网安加社区

网安加社区，是网络安全技术爱好者们交流与分享安全技术的社区。致力于安全赋能软件开发，让开发者更懂安全。通过组织线上线下沙龙、峰会，多维度进行技术分享，促进行业交流，赋能行业交付可信、客户满意的软件产品。

我们集聚业内资深专家，共同传播安全技术与理念，帮助行业在源头上消减软件安全风险，推动国内软件供应链安全生态建设，保障国家的网络安全政策的落地和实施。