数说安全
CYBERSECURITY REVIEWS

Cyber Security Star Vendors

明星供应商评估报告

中国网络安全 BAS 市场

2026.1

入侵与攻击模拟（BAS）市场分析

一、市场定义

1、市场定义：

该市场聚焦于一类产品及解决方案：以 “主动验证 +（半）自动化” 为核心方式，借鉴攻击者的战术、技术与程序（TTP），模拟杀伤链不同阶段，持续测试并验证现有网络整体安全机制的有效性 —— 包括各安全节点设施运行状态、安全策略配置有效性、检测 / 防护手段预期落地效果等。

市场中对这类方案有多种称谓，如入侵与攻击模拟、安全有效性验证、安全度量等，同时也存在服务形态的 BAS 解决方案。需特别说明的是，尽管 BAS 会应用部分自动化渗透测试技术，但该市场范畴并不包含自动化渗透测试产品及服务。

Gartner 对 BAS 技术定义如下：BAS 是通过不断模拟针对不同资产的攻击，来验证安全防御体系有效性的一种技术。

尽管在许多人看来，BAS（自动化安全验证系统）是一项全新的网络安全技术，但实际上，它是安全验证理念在网络安全不同发展阶段下的产物。安全验证思想最早可以追溯到 20 世纪 80 年代计算机网络的兴起。最初，安全验证的目的是保护计算机系统免受未授权访问和破坏，相关技术主要集中在身份认证和访问控制上。进入 90 年代，随着互联网的普及，安全验证的重点逐渐转向漏洞评估，漏洞扫描工具应运而生。到了 90 年代中期，渗透测试作为一种评估安全性的手段开始广泛应用。

随着 ISO 27001、PCI DSS 等法规和标准的出台，企业需要证明自身安全措施的合规性，安全审计也因此成为企业进行安全验证的重要方式。国内网络安全行业起步后，随着等保 1.0 的发布，安全验证逐步演变为以满足等保要求为核心。进一步发展至 2016 年，

HW 出现，在头部企业中，安全验证的形式又从合规检查升级为实战攻防对抗。

综上所述，安全验证是一种宏观理念和思想，在不同发展阶段和网络安全形势下，呈现出多样化的表现形式，并采用不同的产品和技术。从技术特征上来看，传统安全验证技术的目的是为了保障 IT 与网络资产的安全性，而 BAS 的主要价值是验证保护这些 IT 与网络资产的防护设备的有效性。

2、主流安全验证技术

作为一个创新的安全验证技术，BAS 出现有两个客观因素：

首先，随着国内网络安全产业从建设期迈入运营期，BAS 为安全运营提供了契合的工具，具备明确的应用场景和潜在的市场需求。

其次，BAS 作为积极防御技术，具备风险预测与识别等前置能力，这与当前网络安全领域主动防御和动态防御的总体发展趋势高度契合，因此更容易被客户接受和认可。

主流安全验证技术对比			
安全验证技术	BAS	渗透测试	漏洞扫描
工作实效性	7 x 24	触发式	周期式
交互性	自动	人工+自动	无
验证机制	安全体系风险量化评估	漏洞风险评估	漏洞检测
验证纬度	较广	有限	仅漏洞
验证过程回放	支持	有限	无
回归验证测试	持续性验证	有限	有限
可管理性	高	低	中

二、核心技术：

核心技术	说明
攻击模拟技术	以攻击者视角模拟各种攻击手段和技术，包括传统网络攻击、恶意代码植入、漏洞利用、网络钓鱼、数据窃取等，尽可能多的覆盖主流攻击技术。
自动化技术	基于 ATT&CK 框架，形成对全攻击链上主流攻击技术的验证用例覆盖，包括侦查、执行、持久化、权限提升等，并通过对各场景验证需求的推导，形成自动化验证用例。
场景布防拓扑技术	深入理解各类场景的验证需求，在边界防护、流量安全、端点安全、数据安全等场景中，设计相应的拓扑和布防策略，包括场景的网络拓扑、访问路径、防护预期、响应预期等。
基于业务风险的验证技术	可以提供对一些专项场景的安全验证，包括勒索软件防护、HW 防护、APT 防护、账号安全防护等。
安全知识库	跟踪安全态势的变化，构建安全知识库，包括最新的漏洞信息、攻击手法和防御策略，保证产品能够始终模拟最新的安全威胁。
集成与对接技术	通过与现有产品和工作流集成，保证安全验证结论的准确性，以及闭环验证的能力。

其它技术	1、多维度有效性验证：可基于设备有效性、策略有效性、漏洞与脆弱性、安全运营与响应等多维度进行安全验证； 2、云原生技术：支持云原生环境，能够模拟云环境中特有的安全威胁和攻击手段； 3、分析报告的可读性与可解释性。

三、市场现状：

- **BAS 目前在国内属于起步阶段：**BAS 技术 2017 年由 Gartner 提出，但国内真正起步是 2021-2022 年的时间，市场中陆续出现了商业化的产品。
- **需求侧主要以金融和运营商头部客户为主：**BAS 的客户群体并非聚焦于合规驱动型市场。作为一类具备技术前瞻性的进阶安全方案，其落地应用需以客户较高的安全成熟度、稳定持续的安全投入为前提，且在顶层规划、技术储备等客观条件上，需具备部署 BAS 的基础支撑。因此，当前市场中的核心客户主要集中在两大领域：一是金融领域，具体涵盖国有大行、全国性股份制银行、头部城市商业银行，以及证券、基金、保险行业的头部机构；二是运营商、能源行业的核心央企。从项目规模来看，这类客户的 BAS 相关项目，成交额普遍达到百万级及以上。
- **供给侧主要以初创厂商为主，安全大厂目前很少涉及：**目前国内该赛道厂商数量 10 家左右，以初创、专业型的 BAS 厂商为主，这些厂商大多具备攻防对抗、漏洞研究、自动化渗透测试及企业安全运营等核心技术背景，在 BAS 领域的技术深耕与场景适配能力较为突出。与初创及专业厂商的集中布局不同，目前仅有少部分传统安全大厂涉足该领域，尚未形成大规模入局的态势，整体市场仍以专业型玩家为主导。

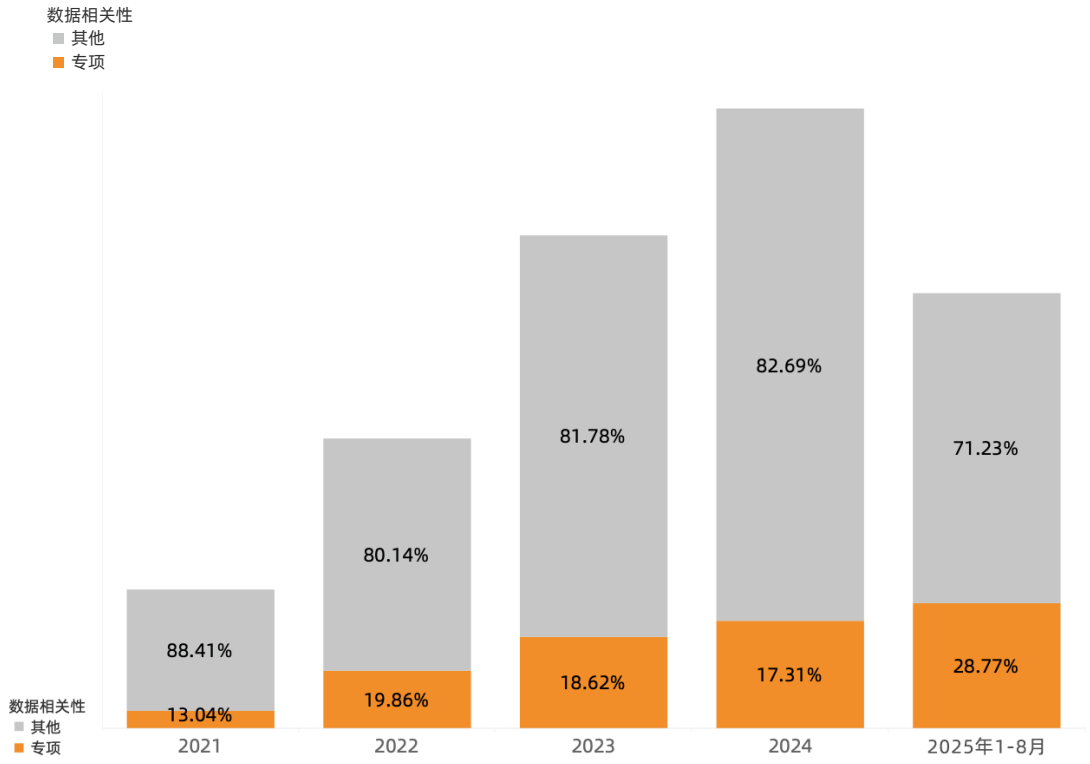
- **国内 BAS 以项目型交付和私有化部署为主：**BAS 以积极防御为核心目标，以实战对抗为核心手段，其落地需与客户的网络环境、业务需求及安全策略深度融合 —— 这一特性也催生了行业内的关键现状：尽管厂商普遍在推进产品标准化研发，试图降低落地门槛，但在实际项目交付中，很难实现高度标准化的落地效果。究其原因，仅提供产品无法确保 BAS 真正发挥价值，必须配套从前期咨询规划、方案定制，到中期实施落地、后期持续运营的全流程服务，才能让技术与客户实际场景深度适配。因此，当前 BAS 多以项目制形态交付，整体实施周期相对较长。在部署模式上，尽管部分 BAS 技术（如边界安全验证）已具备 SaaS 化部署能力，但结合核心客户（如金融、能源领域企业）对数据私密性、业务可控性的高要求，多数客户仍优先选择私有化部署，SaaS 模式暂未成为市场主流。

四、市场规模与发展趋势

1、市场规模：2 亿（2024 年，甲方口径）

2、项目数量分析

整体来看，自 2021 年以来，公开采购的 BAS 项目数量累计近 2000 个，整体项目总量有限，但采购需求呈现逐年增长态势。值得关注的是，BAS 专项采购的占比逐年提升，反映出用户对 BAS 项目的专业化和定制化需求不断增强，也说明 BAS 技术在网络安全体系中的重要性和应用深度持续提升。



图：2021-2025 年 8 月 BAS 项目数量

3、 市场发展趋势

- **BAS 市场短期内（5 年）仍会保持上升趋势**：过去三十年，企业安全体系历经 “安全防护 - 安全运维 - 安全运营” 三步演进，安全验证体系的认可度与关注度逐步提升。BAS 作为从零起步的技术，精准填补安全验证体系的核心空白 —— 验证安全产品实际有效性，且能有效识别安全产品默认配置、SOC 告警遗漏等防御失效点，是未来网安领域的潜力方向。结合国内网安关键客户规模（年持续稳定投入的头部客户约 1200 家）及现有 BAS 市场的客户基数与增速，预计未来 5 年 BAS 市场将持续上升。
- **多类安全验证产品的整合**：网安技术发展中，整合是显著趋势，无论是平台型产品，还是 XDR、SASE、零信任等新技术，多为多产品 / 技术整合，本质创新较少。安全验证领域也可能延续这一融合趋势，集成 BAS、PTE、VA/VPT、ASM 等多维度有效性验证 —— 这契合相关厂商的背景能力与技术发展路径。Gartner 近期提出的持续威胁暴露管理（CTEM）概念，也正体现这一方向。

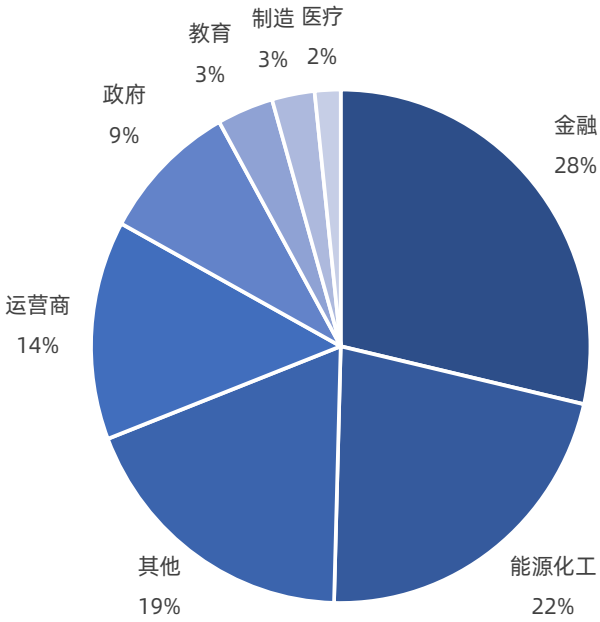
- **BAS 产品具备 SaaS 化的基础**：目前大多数 BAS 产品仅在边界场景支持 SaaS 化安全验证，其他场景仍以私有化部署为主，核心取决于部署位置、应用场景及数据安全敏感性要求。相较于转发或检测网络流量的方案（这类方案较难 SaaS 化），BAS 作为交互攻防流量的方案，在更多场景（如互联网、云场景的有效性验证）中具备 SaaS 化潜力。而 BAS 产品的 SaaS 化订阅，不仅利于简化交付、维护及更新扩展，还可能吸引面临经济压力的潜在客户。

五、厂商分析

1、BAS 明星供应商

2、部分厂商 BAS 产品现状

本次调研共收到 7 份有效问卷，围绕产品基础能力、技术创新能力和服务能力等多个维度，全面了解了各厂商的产品现状。受调研厂商的主要服务对象包金融、能源化工、运营商等客户，调研企业 2025 年的 BAS 收入在各行业分布如下：



2.1 产品基础能力（本部分能力评估等结果均来自调研问卷所收集到的信息，数说安全并未进行实地测评，仅供参考。）

厂商名称	软件部署	虚拟化以及资源池	硬件设备	MSSP
知其安	✓	✓	✓	✓
矢安科技	✓		✓	
华云安	✓	✓	✓	
墨云科技	✓	✓	✓	
灰度科技	✓	✓	✓	
塞讯信息	✓	✓	✓	✓
梆梆安全	✓		✓	

厂商名称	安全设备的..	报表导出	覆盖度评估	离线升级	权限分级	任务模板	审计追踪	稳定性验证	信创兼容	性能监控	用户自定义..	有效性验证	周期任务	自定义攻击..	Agent管理
知其安	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
矢安科技	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
华云安	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
墨云科技	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
灰度科技	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
塞讯信息	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
梆梆安全		✓	✓	✓	✓	✓	✓		✓		✓	✓		✓	

厂商名称	SIEM	SOAR	EDR/XDR	NDR	防火墙/WAF/I..	工单系统(jira/..	威胁情报	邮件安全	云安全平台（C..	ASM/Attack S..	CMDB/资产平台	IAM/AD/PAM
知其安	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
矢安科技	✓	✓	✓	✓	✓		✓	✓	✓	✓		
华云安	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
墨云科技	✓		✓	✓	✓		✓	✓	✓			
灰度科技	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
塞讯信息	✓	✓	✓	✓	✓		✓	✓				
梆梆安全		✓	✓	✓								

厂商名称	SOC	防火墙	WAF	IDPS	其他
知其安	✓	✓	✓	✓	
矢安科技			✓	✓	✓
华云安	✓	✓	✓	✓	✓
墨云科技	✓	✓	✓	✓	✓
灰度科技	✓	✓	✓	✓	✓
塞讯信息	✓	✓	✓	✓	✓
梆梆安全					✓

厂商名称	边界安全	容器/K8s	社会工程	身份&AD	数据安全	数据渗出	网络流量..	应用/API	邮件	云配置	云权限	终端	主机	OT/工控	Web漏洞	其他
知其安	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
矢安科技	✓	✓	✓		✓	✓	✓	✓	✓			✓	✓		✓	✓
华云安	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
墨云科技	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	
灰度科技	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
塞讯信息	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
梆梆安全				✓			✓	✓							✓	✓

厂商名称	日志	告警	流量	其他
知其安	✓	✓	✓	
矢安科技	✓	✓	✓	✓
华云安	✓	✓	✓	
墨云科技	✓	✓	✓	
灰度科技	✓	✓	✓	
塞讯信息	✓	✓	✓	✓
梆梆安全	✓	✓	✓	✓

厂商名称	手动	自动阈值	CI/CD	其他
知其安	✓	✓	✓	
矢安科技	✓	✓		
华云安	✓			✓
墨云科技	✓	✓	✓	✓
灰度科技	✓			
塞讯信息	✓			
梆梆安全	✓			

厂商名称	场景报告	设备报告	整体报告	资产报告	纵深防护报告	ATT&CK报告
知其安	✓	✓	✓	✓	✓	✓
矢安科技	✓	✓	✓	✓	✓	✓
华云安	✓	✓	✓	✓	✓	✓
墨云科技	✓	✓	✓	✓	✓	✓
灰度科技	✓	✓	✓	✓	✓	✓
塞讯信息	✓	✓	✓			✓
梆梆安全	✓		✓	✓	✓	✓

厂商名称	覆盖率	平均检测时间MTTD	稳定性	有效性	整体风险评分	其他
知其安	✓	✓	✓	✓	✓	
矢安科技	✓	✓	✓	✓	✓	✓
华云安	✓	✓	✓	✓	✓	✓
墨云科技	✓	✓		✓	✓	
灰度科技	✓	✓	✓	✓	✓	✓
塞讯信息	✓	✓	✓	✓	✓	✓
梆梆安全	✓	✓		✓	✓	✓

2.3 技术创新能力

厂商名称	沙箱管理	AI智能分析	防御态势大屏	大模型安全有效性验..	OpenAPI	外发配置审核	IPv6	自动复验（修复后触..	指标趋势对比
知其安	✓	✓	✓	✓	✓	✓	✓	✓	✓
矢安科技		✓	✓	✓	✓	✓	✓	✓	✓
华云安		✓		✓	✓	✓	✓	✓	✓
墨云科技		✓	✓	✓	✓	✓	✓	✓	✓
灰度科技		✓	✓	✓	✓		✓		✓
塞讯信息	✓	✓	✓	✓	✓	✓	✓	✓	✓
梆梆安全	✓	✓		✓					

厂商名称	服务模拟	进程模拟	流量回放	模拟命令行	模拟执行	其他	域名解析或IP访问	HTTP仅发包
知其安	✓	✓	✓	✓	✓		✓	✓
矢安科技	✓	✓	✓	✓	✓	✓	✓	✓
华云安	✓	✓	✓	✓	✓		✓	✓
墨云科技	✓	✓	✓	✓	✓		✓	✓
灰度科技	✓	✓	✓	✓	✓	✓	✓	✓
塞讯信息	✓	✓	✓	✓	✓	✓	✓	✓
梆梆安全	✓	✓	✓	✓	✓	✓	✓	✓

厂商名称	自研研究团队	开源社区	客户反馈	情报合作	赛事演练	CVE/漏洞库	其他
知其安	✓	✓	✓	✓	✓	✓	
矢安科技	✓	✓	✓	✓	✓	✓	✓
华云安	✓	✓	✓	✓	✓	✓	
墨云科技	✓	✓	✓	✓	✓	✓	
灰度科技	✓	✓	✓	✓	✓	✓	
塞讯信息	✓	✓	✓	✓	✓	✓	
梆梆安全	✓	✓	✓	✓	✓	✓	✓

厂商名称	自然语言检索	场景生成	风险解读	工单摘要	检测建议生成	其他
知其安	✓	✓	✓	✓	✓	
矢安科技	✓	✓			✓	✓
华云安	✓	✓	✓	✓	✓	
墨云科技	✓	✓	✓		✓	
灰度科技	✓	✓	✓		✓	
塞讯信息		✓	✓		✓	✓
梆梆安全	✓		✓		✓	✓

2.4 服务能力

厂商名称	安全运营演练服务	策略优化服务	定制开发服务	有效性验证服务	驻场服务	咨询规划服务
知其安	✓	✓	✓	✓	✓	✓
矢安科技	✓	✓	✓	✓	✓	✓
华云安	✓	✓	✓	✓	✓	✓
墨云科技	✓	✓	✓	✓	✓	✓
灰度科技	✓	✓	✓	✓	✓	✓
塞讯信息	✓	✓		✓	✓	✓
梆梆安全	✓	✓	✓	✓	✓	✓

厂商名称	客户共创	论坛	门户	FAQ
知其安	✓	✓	✓	✓
矢安科技	✓		✓	✓
华云安	✓	✓	✓	✓
墨云科技		✓		✓
灰度科技	✓		✓	✓
塞讯信息			✓	✓
梆梆安全	✓	✓	✓	✓

2.5 标杆客户案例词云

3、重点供应商产品推荐

3.1 知其安

分析师推荐语：

知其安“离朱安全有效性验证平台”在国内 BAS 市场具备较高的市场占有率，广泛应用于金融、运营商、央国企等行业。平台核心能力在于常态化策略巡检和自动化闭环验证，可持续检测安全设备与策略有效性，降低人工干预，提高安全运营效率。其 7×24 小时自动化验证机制有助于及时发现安全策略失效点，缩短风险暴露周期，为企业防护体系优化提供数据支持。

平台可自动生成防御态势和量化指标，辅助安全团队进行资源投入和策略调整，提升安全建设回报率。针对多分支机构，平台支持多维度量化评估，便于管理层快速掌握各分支防护水平，满足合规和监管需求。

产品设计覆盖“点-线-面”多层次验证，支持自动化报告生成和与主流安全设备日志自动对接，并能联动 SOC/态感平台，实现验证、处置、复验的一体化流程。验证用例覆盖主流攻击手法，响应速度快，具备一定前瞻性和灵活性。

总体来看，离朱平台在自动化验证覆盖面、运营闭环能力和用例响应等方面表现突出，适合有多分支、多场景需求的企业。建议用户结合自身安全架构，评估产品集成能力和实际效果，以实现安全防护水平的持续提升。

主打型号	离朱安全有效性验证平台
核心能力	**常态化策略巡检，为安全运营降本增效：**基于持续性自动化闭环验证，代替人工的每天检查规则策略运转情况；提升有效性检查覆盖面，确保所有安全设备、规则及策略按预期启用并生效。持续7*24 小时全天候验证评估，帮助用户先于攻击者发现安全策略失效点，缩短失效点存在点时间周期，降低失效导致的攻击风险。 **实现防护能力、运营能力精准提升：**第一时间了解最新安全攻击信息并通过安全用例自动化的在企业内复现和验证，检验企业当前的安全防护能力；在掌握当前安全防御能力前提下进行针对性改进，全面提升企业安全防护能力。 **安全防御效能可视化、可量化：**基于执行结果自动生成可视化安全防御态势、量化安全指标，指导辅助安全运营有针对性的、有方向的投入和强化，提高安全建设回报率。 **监管分支机构的可靠抓手：**常态化评估分支机构、分子公司及海外机构安全防护力，以实战化维度快速精准掌握真实情况，及时发现防护失效，输出优化建议。基于量化的数据统计实现对各分支机构的量化多维考评。
产品亮点	**多样化验"点-线-面"多维度验证：**从单点设备到防御链路，再到场景化验证，多层次评估安全防护体系水平。 **自动化验证与智能分析:**无需人工干预，自动执行验证任务并生成详细的分析报告。 **运营闭环能力强:**支持与主流安全设备日志自动化对接，基于验证结果对接SOC/态感进行闭环处置与复验。 **丰富化验证用例:**验证用例覆盖主流攻击手法（ATT&CK战术步骤覆盖度100%，攻杀链阶段覆盖100%）；用例应急响应快（最新的1day等攻击手法出现，4小时之内开发出新的验证用例）。 **灵活自定义编排:**高度灵活自定义编排，可快速验证纵深防御中多设备防护效能。 **客户实践覆盖广:**金融行业（银行业覆盖度超过80%+，证券行业覆盖度超过90%+）；其他行业已覆盖头部运营商、央国企、能源、高端制造、互联网企业等。
典型场景	多年安全能力建设，企业已部署多层安全防护体系，当IT 环境变化、攻击技术演进等导致的防护偏差、安全部署的稳定性、规则策略和预期的一致性、告警的延迟丢失和漏报、特殊事件导致的防护失效等、需统一进行有效性验证与防护水平量化提升。 随着外部网络安全威胁的加剧，基于国家安全监管部门和集团对于网络安全工作的最新要求，缺少统一开展策略有效性专项验证，难以量化已部署安全防护措施的防护水平。
产品展示	 离朱-安全有效性验证平台防御态势大屏  离朱-安全有效性验证平台管理界面

3.2 墨云科技

分析师推荐语：

墨云科技智能攻击模拟验证系统（VackBAS）系列产品，覆盖 VackBAS-SC、AC、XC、VM 等多种型号，广泛应用于网站、端点、数据、容器、邮件、网络、云平台等安全防护场景。系统基于 MITRE ATT&CK 框架，能够模拟各类 APT 攻击的完整杀伤链，进行全链条测试，评估纵深防御能力，精准关联潜在攻击路径，透视全局关键风险。

VackBAS 具备自动化闭环验证能力，自动分析攻击结果并匹配安全设备日志，判定阻断与告警行为，生成可视化报告与修复建议，实现安全运营闭环。平台支持从防御、业务、攻击战术多视角展示安全态势，帮助团队快速定位关键风险，优化安全策略。依托墨云安全实验室持续更新的攻击用例库，覆盖 HVV 高频攻击、TOP100 漏洞利用和最新威胁情报，确保

验证与实战同步。

产品亮点包括基于 ATT&CK 量化安全效能、风险评分与修复优先级，助力安全投资决策。AI 智能体增强功能，可自动生成多样化攻击载荷，智能研判攻击流量，显著提升测试真实性、覆盖率及自动化水平。典型应用场景涵盖重保专项测试、防御态势评估和日常安全运营，适用于有高频安全验证、持续防御评估需求的企业。

总体来看，VackBAS 产品在全方位安全验证、自动化闭环和智能化测试方面表现突出，能够有效提升企业安全防护能力和运营效率，建议有相关需求的用户重点关注。

主打型号	**智能攻击模拟验证系统 Vack-V5.0：VackBAS-SC 版、VackBAS-AC 版、VackBAS-XC 版、VackBAS-VM 版**
核心能力	1）**全方位安全验证：**覆盖网站、端点、数据、容器、邮件、网络、云平台等安全防护能力，通过模拟器间测试、无害化处理等技术，确保测试过程零干扰、零风险。 2）**全杀伤链模拟：**基于 MITRE ATT&CK 框架，模拟各类 APT 攻击完整杀伤链，全链条测试网络业务安全，评估纵深防御，关联潜在攻击路径，透视全局关键风险。 3）**自动化闭环验证：**自动分析攻击结果，匹配安全设备日志，精准分析并判定阻断与告警行为，提供可视化报告与修复建议，形成安全运营闭环。 4）**多维度态势可视化：**从防御视角、业务视角、攻击战术视角等多维度展示安全态势，帮助团队快速定位关键风险，优化安全策略。
产品亮点	1）**实战化验证：**基于墨云安全实验室持续更新的攻击用例库，覆盖 HVV 高频攻击、TOP100 漏洞利用、最新威胁情报等，确保验证与实战同步。 2）**持续自动化运行：**提供自动和持续的安全防御态势评估，增强安全可见性和能见度，及时发现策略及配置缺陷。 3）**量化评估与决策支持：**基于 ATT&CK 框架量化安全效能，提供风险评分与修复优先级，为安全投资提供数据支撑。 4）**AI 智能体增强：**基于百亿级参数大模型与海量攻防数据，VackBAS 可自动生成多样化的攻击载荷，精准打击防护薄弱点；同时智能研判攻击流量，有效识别漏报误报，显著提升测试的真实性、覆盖率和自动化水平。
典型场景	1）**重保场景：**重保前开展信息侦查、渗入等多专项测试，含历年及最新攻击手法，全面测试验证关键风险点并及时修复。 2）**防御态势评估场景：**通过自动化、持续性的攻防模拟，基于全局数据量化评估网络安全水位，提升防御能见度，驱动防御体系优化。 3）**日常安全运营场景：**日常持续验证安全设备策略有效性，判断其能否应对新增威胁，抢先发现修复漏洞，降低入侵风险。
产品图片	 

3.3 灰度安全

分析师推荐语：

灰度安全-先知智能风险评估系统是一款面向企业级用户的智能化安全评估平台，具备实战化攻击模拟、自动化风险评估和纵深防御体系验证等多项核心能力。该系统采用先进的攻击编排技术，能够依据丰富的知识库自动生成多维度攻击向量，对网络安全设备、数据安全产品及 AI 大模型进行全面的防护效果检验。

产品支持网络、邮件、端点、容器、数据库等多种场景，覆盖企业实际运营中常见的安全需求。相较于传统渗透测试，先知系统创新性地采用无损伤评估技术，保障业务连续性，在发现安全短板的同时不会对生产环境造成影响。系统内置自研 BAS 垂直领域大模型，结合 RAG 和微调技术，能够自动生成攻击向量并智能转换，显著降低使用门槛，提升安全评估的智能化和自动化水平。常态化安全运营功能，支持周期性自动验证，帮助企业持续发现防护不足和策略缺陷，辅助安全建设和设备选型。针对新上线资产，系统可提供安全入网测试，从源头杜绝“带病上线”风险。产品还特别适用于攻防演练和重保场景，能够动态验证防护措施的实战效能，提升整体安全防护能力。

通过全场景覆盖和创新技术，灰度安全-先知智能风险评估系统为企业构建了科学、智能、持续的安全评估与风险管理体系，是中大型企业、关键信息基础设施单位和 AI 创新型企业提升安全水平的理想选择。

主打型号	灰度安全-先知智能风险评估系统
核心能力	**1.网络安全设备评估：**采用实战化攻击模拟技术，依据风险评估场景知识库，自动化编排攻击向量，针对安全设备威胁防护和检测进行有效性评估。评估范围涵盖了边界安全、网络安全、邮件安全、端点安全、容器安全、运行时安全、网络策略等多个维度。 **2.数据安全风险评估：**聚焦数据安全评估对象，覆盖企业数据安全管理的各类场景。支持网络DLP、终端DLP、邮件DLP、数据库安全审计、数据库防火墙、API安全网关等数据安全产品，助力组织提升数据安全管理效率与防护水平。 **3.大模型安全评估：**聚焦大模型与智能体安全验证，支持模拟提示词注入、数据投毒、数据泄露、模型窃取等新型攻击，精准适配企业“AI+业务”融合场景下的安全评估与风险防控需求。 **4.纵深防御体系评估：**基于攻击编排能力，定制评估场景，从全局开展专项攻击模拟，以验证评估纵深防御体系的综合防护能力。评估场景包括勒索软件攻击、APT攻击、僵木蠕攻击、重保/HVV等综合模拟，实现对防御体系纵深协同能力的精准度量、防护措施实战效能的动态验证。 **5.可利用漏洞验证评估：**系统提供30+漏洞验证的检测场景，覆盖了安全设备、Web应用、操作系统、编程语言框架、Web中间件、数据库和其它软件等的漏洞利用，以及重大保障和最新热点漏洞的检测。实现对资产漏洞风险优先级评估，辅助组织提升漏洞修复效率。
产品亮点	**1、全维度验证场景创新：**具备全场景安全评估能力，覆盖“网络安全+数据安全+开发安全+大模型安全”四维验证体系。基于ATT&CK实战框架，内置超过40000条经过实战验证的攻击向量，全面覆盖ATT&CK框架中的14个战术层面（如初始访问、执行、持久化等）和200多项技术维度，整体技术覆盖率超过80%。可精准识别从外到内的完整攻击路径，帮助企业构建纵深防御体系。 **2、无损伤评估技术保障业务连续性：**系统采用专利智能评估技术，区别于传统渗透测试，创新性地避免对漏洞的直接利用。通过专有攻击向量模拟技术、风险评估算法和多维验证机制，在确保准确性的同时，不对业务系统造成负面影响。 **3、BAS垂类大模型驱动智能攻防：**基于RAG与微调技术，构建了自有BAS垂直领域大模型，已成功落地多个BAS智能体应用，如攻击向量自动转换与智能生成等，显著降低产品使用门槛，全面提升BAS系统的智能化水平与业务价值。
典型场景	**1.常态化安全运营** 系统开展常态化的周期性安全评估验证，发现安全防护不足、策略缺陷等风险问题。 **2.攻防演练支撑** 实现在攻防演练/重保场景中，进行防护措施优化、防护覆盖度检验等工作，达成全面加固、应急验证等价值收益。 **3.安全建设规划** 系统验证定位防御能力短板，为安全优化建设判断提供支撑，辅助安全采购规划。 **4.设备采购选型** 安全设备采购阶段，通过系统进行安全能力的POC测试验证，为采购选型提供依据。 **5.入网安全测试** 资产/系统上线前，通过系统提供的安全扫描验证完成入网测试，从源头杜绝“带病上线”风险。
产品展示	  先知-产品硬件图  先知-产品管理界面图