头豹 LeadLeo

www.leadleo.com

2021年
中国网络安全集成服务基础能力探析

2021 China Cyber Security Integrated Service Capabilities Research Report

2021年中国ネットワークセキュリティインテグレーションサービス基礎能力の研究

报告标签：网络安全、集成服务、检测响应

报告作者：唐英杰

2021/02

头豹研究院简介

- 头豹研究院是中国大陆地区首家**B2B模式人工智能技术的互联网商业咨询平台**，已形成集**行业研究、政企咨询、产业规划、会展会议**行业服务等业务为一体的一站式行业服务体系，整合多方资源，致力于为用户提供最专业、最完整、最省时的行业和企业数据库服务，帮助用户实现知识共建，产权共享
- 公司致力于以优质商业资源共享为基础，利用**大数据**、**区块链**和**人工智能**等技术，围绕**产业焦点**、**热点**问题，基于**丰富案例**和**海量数据**，通过开放合作的研究平台，汇集各界智慧，推动产业健康、有序、可持续发展

四大核心服务：

企业服务

为企业提供**定制化报告**服务、**管理咨询**、**战略**调整等服务

云研究院服务

提供行业分析师**外派驻场**服务，平台数据库、报告库及内部研究团队提供技术支持服务

行业排名、展会宣传

行业峰会策划、**奖项**评选、行业**白皮书**等服务

园区规划、产业规划

地方**产业规划**，**园区**企业孵化服务

报告阅读渠道

头豹科技创新网——www.leadleo.comPC端阅读全行业、千本研报

头豹小程序——微信小程序搜索“头豹”、手机扫上方二维码阅读研报

添加右侧头豹研究院分析师微信，邀您进入行研报告分享交流微信群


图说


表说


专家说


数说

详情请咨询

客服电话

400-072-5588

上海

王先生：13611634866
李女士：13061967127

南京

杨先生：13120628075
唐先生：18014813521

深圳

李女士：18049912451
李先生：18916233114

摘要

聚焦网络安全：中国网络安全集成服务基础能力几何？

在信息化深入各行业的过程中，网络安全成为首要重要的问题。中国网安市场增长迅速且远未饱和，市场结构也正处于产品向服务转型的过程中。本报告聚焦网络安全服务领域，从中国网络安全集成服务基础能力的角度去分析中国网安行业的发展情况。

处于当前严峻的网络安全形势中，网络安全的防护重心由布置安全产品转向网络安全攻防的能力，防守方安全能力主要体现在威胁检测和应急响应的环节，本报告分别分析了这两个环节里的中国网安行业的技术发展和中国网安厂商的实际应用情况，从而探析安全集成服务理论技术层面及应用层面的能力。

1. 中国网络安全行业处于起步阶段，安全服务未来前景大

- 网络安全总需求提升叠加市场由安全产品向安全服务转型，安全集成服务未来前景大：（1）中国网安行业起步晚，增长迅速且行业还远未饱和，处于行业追赶期，未来整体网络安全需求大。（2）强合规需求、云安全需求、新安全理念三大因素驱动中国网安行业由注重静态硬件部署转为注重攻防对抗能力，从而向主动防御、动态防御、一体化防御的方向发展。这需要覆盖各个细分领域的技术和产品，以及专业网安人员的运营，一般企业无法自己满足这些需求，因此网安行业服务化是大趋势。

2. 网络安全的本质是攻防对抗，攻防对抗能力是网安行业的实际安全能力

- 简单堆叠硬件产品已经无法解决当下的安全问题，购买安全产品在攻防对抗里发挥作用才是关键所在。衡量威胁检测和应急响应能力的关键指标分别是MTTD和MTTR，网络安全厂商们大力发展的威胁情报技术、SIEM、SOAR等均是用于改善MTTD和MTTR两个指标。

3. 中国综合网安厂商和云服务提供商集成服务基础能力较强

- 综合网安厂商技术积累深厚，产品线齐全，有能力覆盖网安各个细分领域，提供安全集成服务，为企业提供一体化、协同、智能的防护；云服务厂商凭借其在自有云端的海量高质量安全大数据及与自身云平台的高度协同，在云安全领域有较强的集成服务能力。

头豹 LeadLeo

目录
CONTENTS

名词解释

- **等保2.0：**全称网络安全等级保护2.0制度,是我国网络安全领域的基本国策、基本制度
- **云计算：**是基于互联网的相关服务的增加、使用和交互模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源。云是网络、互联网的一种比喻说法
- **公有云：**是指第三方提供商为用户提供的能够使用的云。公有云一般可通过互联网使用，可能是免费或成本低廉的，公有云的核心属性是共享资源服务
- **私有云：**私有云的设施只提供给一个包含许多用户的组织单独使用。它可以被该组织、第三方或两者共同拥有、管理和操作，并且可以是内置或外置的
- **MTTR：**Mean-Time-To-Resolution，平均响应事件，网络安全事故从被首次发现到最终被安全运营人员解决之间的时间跨度
- **MTTD：**Mean-Time-To-Detection，平均检测时间，攻击者使用战术和技术在目标网络上首次获得立足到最终被网络或终端安全设备检测出来所持续的时间
- **Kill Chain：**杀伤链，洛克希德·马丁公司开发的“网络杀伤链”模型描述了网络攻击从最早的阶段，从侦察到最终的阶段即数据提取。杀伤链有不同的步骤描述网络攻击的各个阶段生命周期
- **IDS：**Intrusion Detection System，入侵检测系统，是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备
- **SIEM：**Security Information and Event Management，安全信息和事件管理，为来自企业和组织中所有IT资产（包括网络、系统和应用）产生的安全信息（包括日志、告警等）进行统一的实时监控、历史分析，对来自外部的入侵和内部的违规、误操作行为进行监控、审计分析、调查取证、出具各种报表报告，实现IT资源合规性管理的目标，同时提升企业和组织的安全运营、威胁管理和应急响应能力
- **NTA ：**Network Traffic Analysis ，网络流量分析：通过监控网络流量、连接和对象来识别恶意的行为迹象
- **痛苦金字塔：** David Bianco 提出的模型，用于对 IOCs 进行分类并描述各类 IOCs 在攻防对抗中的价值
- **SOAR：**Security Orchestration, Automation and Response ，安全编排自动化与响应，是一系列技术的合集，它能够帮助企业和组织收集安全运维团队监控到的各种信息（包括各种安全系统产生的告警），并对这些信息进行事件分析和告警分诊。然后在标准工作流程的指引下，利用人机结合的方式帮助安全运维人员定义、排序和驱动标准化的事件响应活动

1.1 定义及分类

- **网络安全集成服务将硬件软件及服务有效集成，为客户提供一体化服务，提高客户网络安全性**

网络安全集成服务定义及分类

网络安全集成服务定义

网络安全集成服务是指技术服务提供商按照网络安全工程规范，结合用户业务风险，把安全硬件、安全软件、安全服务等有效集成到用户信息系统，提高信息系统自身安全防护能力的过程和方法

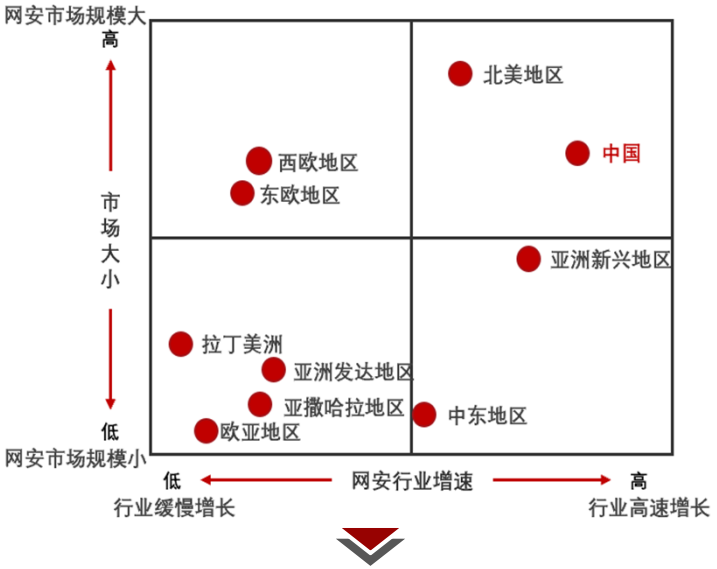
网络安全行业分类

来源：中国信通院，头豹研究院编辑整理

1.2 中国网络安全市场增长速度及规模预测

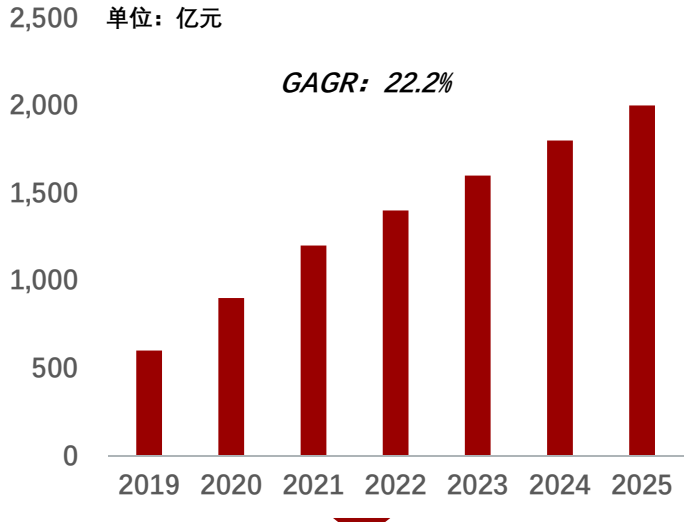
- 中国网安市场处于高增速低饱和的追赶阶段，即将成为世界第二大网安市场，中国厂商未来发展空间辽阔

2016年-2020年全球各地区网安支出增长速度比较



- 中国网安支出低于世界平均水平：目前中国网络安全支出仅占IT总支出的2%，远低于美国的4.5%和全球平均的3.8%
- 中国网安支出增速高且行业空间巨大，发展潜力大：中国网安支出近年来保持着15%的高速增长率，远高于全球平均的8%；市场规模也居世界前列

中国网安市场规模及预测



- 2019年中国网安市场规模为600亿元，保守估计2025年达到2,000亿元，年复合增长率为22.2%：2019年工信部发布的《关于促进网络安全产业发展的指导意见（征求意见稿）》中明确指出到2025年，中国网安市场规模将超过2,000亿元，据此保守估计市场规模到2025年达到2,000亿元，原因有如下3个：

头豹洞察

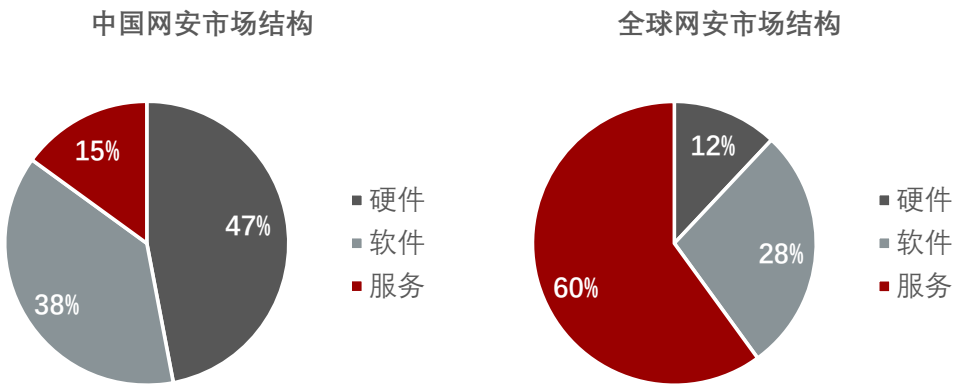
- 从客户层面看，配合完成国家政策目标可能性极高：网安行业是客户驱动型，且下游政企大客户占比超65%，配合政策意愿强，政策目标达成可能性极大
- 从政策层面看，近年颁布的重大网安政策将加速促进行业发展，市场规模增速预计提高：工信部表示2020年中国网安产业规模较2015年翻一倍，复合增长率为15%。但以等保2.0为代表、对网安建设提出硬性要求的政策2019年才开始颁布，且2019年当年网安行业市场规模同比增速就提升至50%，相比之前有明显加速，因此22.2%的增速预测较为保守合理
- 从新应用场景和安全形势看，应用场景的扩张和安全形势的严峻化都将提升网安实际需求：当前网安应用场景在以“云大物移”为代表的新技术驱动下不断扩张，且以APT为代表的高级网络攻击日益增加，安全形势严峻，网安需求将随之增加

来源：头豹研究院编辑整理

1.3 中外市场结构对比

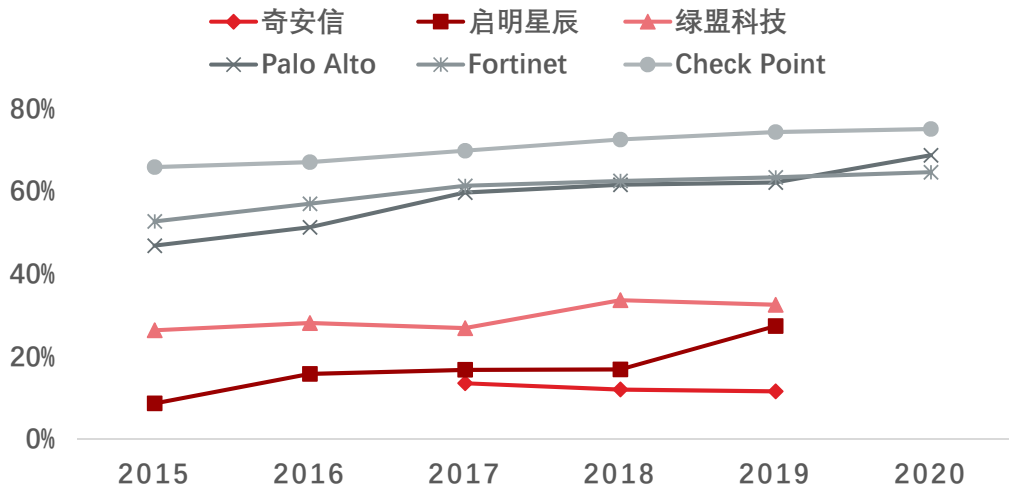
- 中国网络安全行业仍处起步阶段，整体市场和龙头企业均呈现重硬件轻服务的现象，与全球市场结构差异较大

中国与全球网安市场结构对比



- 全球网安市场以服务和软件为主，硬件占比最低：全球网络安全行业起步较早，安全服务市场已非常成熟，服务收入占整个网络安全行业的比重达到60%
- 中国网安市场以硬件为主，安全服务占比低：中国网络安全行业起步较晚，再加上企业对网络安全重视不足，网络安全需求主要为合规需求，在等保2.0实行之前，堆砌网络硬件基本能通过合规要求，有提升真实网络安全能力意愿的企业少，因此造成了中国重硬件轻软件弱服务的局面，网络安全服务占比持续低于国际水平

中国与全球网安公司安全服务收入占比对比



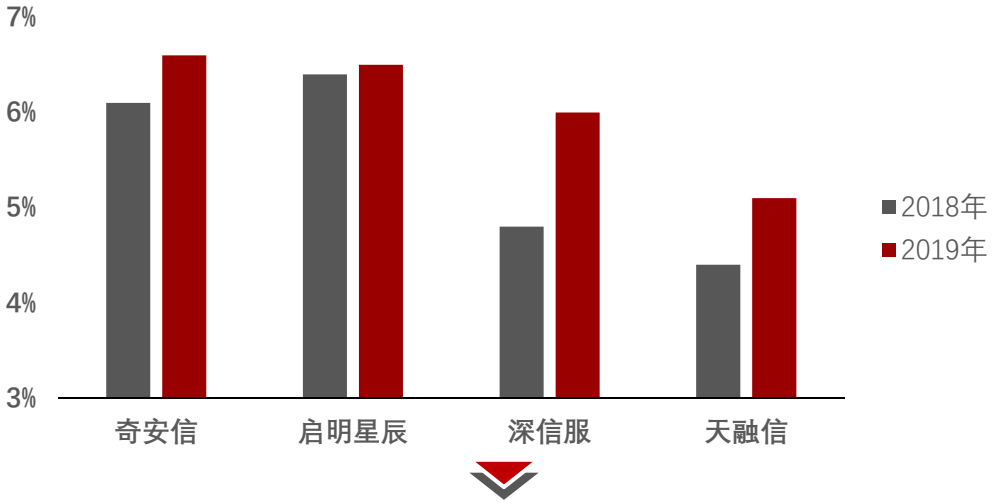
- 全球网安龙头企业安全服务均是主要收入来源，且增长趋势不变：2020年Palo Alto、Fortinet、Check Point三家全球领先网安厂商安全服务收入占比分别为69%、65%、75%，均为主要收入来源，且三家安全服务占比仍在稳步上升
- 中国网安龙头企业安全服务收入占比较低：2019年奇安信、启明星辰、绿盟科技三家中国领军网安厂商安全服务收入占比分别为11.65%、27.45%、32.60%，与国际大厂商相比，安全服务收入占比显著偏低

来源：CCID，Wind，头豹研究院编辑整理

1.4 中国网络安全市场竞争格局

- **中国网安市场集中度低，头部厂商优势渐显，第一梯队的网安厂商均积极布局安服领域**

中国网安行业头部厂商市场份额



- 中国网安市场集中度低，竞争激烈：中国网安市场较为分散，综合性网安企业市占率较高，2019年CR4为24.06%，CR8为39.48%，处于完全竞争型行业
- 龙头安全厂商市占率逐步提升，头部效应逐渐显现：从2016年至2019年，行业CR4从17.83%提升到24.06%，CR8从36.59%提升到39.42%。行业市占率前四的公司开始加速抢占市场，头部效应渐显
- 头部安全厂商纷纷布局安服领域，安服业务增长快，细分领域逐渐覆盖，各厂商均发展出自己的特色

中国网安头部厂商在安服领域的布局及特点

	安服营收及增长	安服领域布局	特点
奇安信	2019年网络安全服务收入3.7亿元，同比增长67.15%	覆盖咨询、风险管控、应急处理、运维、考试与培训业务，提供27项安全服务细分产品	安服人员规模大，居中国第一
启明星辰	2019年网络安全服务收入8.5亿元，同比增长31.67%	覆盖规划咨询、风险管理、运维与应急、合规评价及其他定制服务，提供12项安全服务细分产品	探索第三方独立安全运营模式，建立安全即服务全国业务平台、城市级安全运营中心
深信服	网络安全服务收入没有单独统计口径	覆盖运营类、评估类、培训类、运维类、规划咨询类服务，提供22项安全服务细分产品	以“人机共智”的创新模式为组织提供服务
天融信	2019年网络安全服务收入3.4亿元，同比增长90.35%	覆盖网络安全、大数据、云服务三类服务，提供30项安全服务细分产品	大数据能力强，相关的风险探知系统和态势感知系统行业领先

来源：CCIA，Wind，头豹研究院编辑整理

1.5 供应端：主要厂商分类及优势分析

- **中国网络安服行业主要玩家包括综合型安全厂商、专业技术安全厂商、云服务提供商，其中综合型安全厂商整体实力最强，云服务提供商在云安全领域竞争力较强，专业型云安全厂商在云安全领域也有其独特优势**

主要厂商分类及优势分析

	代表厂商	优势分析
综合性安全厂商	奇安信、启明星辰、深信服、绿盟科技等	❑ 深耕网安领域多年，积累大量的经验、技术、资源 ❑ 产品布局完善，覆盖网络安全的各个细分领域，能够提供一体化、协同化的服务，综合安全实力最强
专业型云安全厂商	安恒信息、山石网科、知道创宇、安全狗等	❑ 专注于云安全细分领域，云安全产品和服务布局完善 ❑ 专业细分领域技术积累高，产品和服务更具针对性 ❑ 专业领域口碑好，客户粘性强
云服务提供商	阿里巴巴、腾讯、百度、华为等	❑ 公有云安全市场有绝对优势，基本占据整个市场 ❑ 云平台积累大量云安全经验和用户，利于未来开展业务 ❑ 大数据资源丰富，技术成熟，能为云安全提供优质的数据源

来源：各公司官网，安全牛，头豹研究院编辑整理

头豹洞察

❑ 行业碎片化严重，综合型网络安全厂商覆盖细分领域多，综合安全实力最强：据安全牛统计，2020年中国网络安全行业共分为15类一级安全领域，88类二级细分领域，产业碎片化严重。综合型网络安全厂商具有完善的服务及产品线。如奇安信，产品覆盖所有15类一级安全领域和71类二级细分领域。这样的综合安全厂商能够提供一体化、协同化的安全服务，符合未来网络安全发展趋势，综合安全实力最强

❑ 云安全是未来网络安全行业最有发展潜力的细分行业，云服务提供商在公有云上占据绝对优势，专业型云安全厂商在私有云也占据独特优势：云安全厂商主要分两类，即云服务提供商和第三方厂商，其中第三方厂商又包括综合型安全厂商和专业型云安全厂商。公有云方面，用户以中小B为主，对非本地部署接受度较高且付费意愿低，因此普遍偏好云服务厂商配套提供的标准化基础安全服务；私有云、混合云方面，客户以政企为主要，注重数据安全、独立性和有效性，通常选择第三方网安厂商进行本地部署。包括综合安全实力最强的综合型厂商和业务最具针对性的专业型云安全厂商

1.6 需求端：主要客户分类及特征分析

- **网安行业是客户驱动型行业，下游政企客户掌握话语权，综合型安全厂商安全服务能力强，最受青睐**

中国网安市场客户结构

https://www.leadleo.com/pdfcore/show?id=603f3e1c20410e5a31957a17

- 政府、电信、金融等大客户是网络安全行业主要客户，且这一趋势将继续延续：政府、电信、金融几大领域目前消费了65%的网安产品及服务，是网络安全行业的主要客户。且政府、电信、金融均是中国政府重点支持信息化建设的行业，网络安全又是信息化的基础，预计未来趋势不改，政府、电信、金融仍会是网络安全产品服务的消费主力，是厂商需要重点攻克的客户

头豹洞察

- 网安行业是客户驱动型行业，下游客户话语权大：政府、电信、金融等网安下游客户通常将安全建设需求汇总后确定建设方案，通过项目招投标的方式确定供应商。而大多数安全产品如防火墙、WAF、堡垒机等，标准化程度都比较高，只有态势感知等少数产品、服务不同厂商之间差异较大，因此总体来说，网络安全行业由客户驱动，特别是政企客户话语权大

- 网络安全行业下游政企客户需要一体化的安全服务和良好的保密性，头部综合型网安厂商拥有完善的产品、服务线，且有国资股东背景背书，是下游政企客户的首选：一方面，安全厂商对下游政企客户的主要交付方式是提供解决方案，以解决客户网络安全需求为目的。因此获得政企客户订单的前提是产品线和服务完备，在碎片化严重的网络安全行业，只有综合型安全厂商满足这一要求。另一方面，政企客户对数据信息极为敏感，因此有国资股东背景的网安厂商更容易受到政企客户的青睐。目前中国上市网安公司中，仅有三家具有国资股东背景，均为综合型网安厂商。奇安信由中国电子信息集团持股17.95%，绿盟科技由中国电子科技集团持股15.5%，天融信由中国电子科技集团持股4.95%

来源：CCID，头豹研究院编辑整理

2.1 强合规需求（1/2）

- **中国网络安全相关政策法规密集落地，网安相关法律体系日渐完善，合规需求旺盛**

中国网络安全相关政策法规及意义

政策/事件名称	颁布/发生日期	颁布主体	政策要点
《个人信息保护法（草案）》	2020-10	全国人大	提升企业网安建设的意识
《数据安全法（草案）》	2020-06	全国人大	提升企业网安建设的意识
《关于促进网络安全产业发展的指导意见（征求意见稿）》	2019-09	工信部	明确了对网安行业发展的扶持态度
《国家网络安全产业发展规划》	2019-06	工信部	明确了对网安行业发展的扶持态度
《信息安全技术网络安全等级保护基本要求（意见稿）》	2019-05	公安部	明确了网安建设的硬性要求
《关键信息基础设施安全保护条例（意见稿）》	2017-07	网信办	明确了网安建设的硬性要求
《中华人民共和国网络安全法》	2017-06	全国人大	建立了整个网安市场的法律体系
《国家网络空间安全战略》	2016-12	网信办	将网络安全上升到国家战略高度
中央网络安全和信息化领导小组成立	2014-02	网信办	将网络安全上升到国家战略高度

来源：头豹研究院编辑整理

头豹洞察

- 网安被上升到国家战略高度：中央网安和信息化领导小组的成立体现了对网络安全的重视，国家领导人提出“没有网络安全就没有国家安全，没有信息化就没有现代化”，将网安上升到国家战略高度
- 网安的基础性法律推出，搭建起网安的法律体系框架：《网络安全法》是中国第一部网络安全管理方面的基础性法律，填补了网安领域的法律空白，让网安发展有法可依
- 网安建设的硬性要求逐渐明确：以等保2.0为代表的政策法规在《网络安全法》的框架基础下，进一步明确了硬性要求，是网安领域的核心法条
- 国家大力促进网安行业的发展：《关于促进网络安全产业发展的指导意见（征求意见稿）》提出，到2025年网络安全产业规模超过2,000亿，培育形成一批年营收超过20亿的安全企业
- 继续提升企业网安建设的意识：以《数据安全法》为代表的法律正在密集制定中，有望进一步提升企业的网安意识

2.1 强合规需求（2/2）

- **等保2.0将网安要求全面提高，传统硬件布置难以满足需求，更注重防护实际效果的网络安全服务受强合规需求利好最多**

等保2.0与等保1.0对比及分析

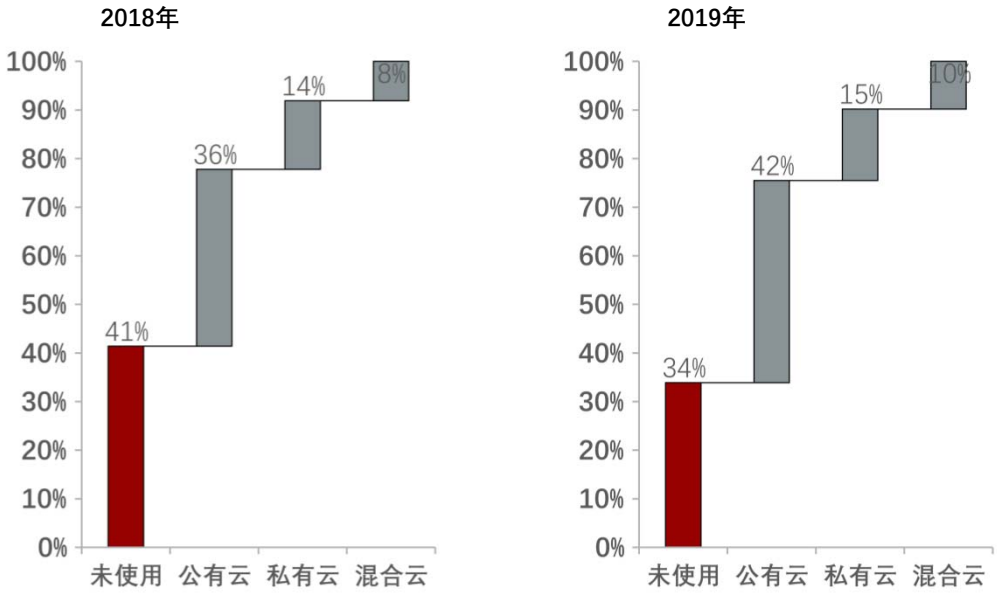
	保护对象	合规内容	保障体系	等级测评要求	定级备案流程
等保1.0	❑ 信息系统	❑ 五个规定性动作	❑ 被动防御：一个中心三重防护（防火墙，入侵检测，防病毒）	❑ 达到60分基本及格	❑ 自主定级、自主保护
等保2.0	❑ 信息系统 ❑ 云计算平台、工业控制系统、大数据中心、物联网系统、移动互联网等关键信息基础设施	❑ 五个规定性动作 ❑ 风险评估、安全监测、通报预警、事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全效果评价、综治考核等	❑ 全方面、一体化的主动防御：感知预警、动态防护、安全检测、应急响应等	❑ 达到75分基本及格	❑ 专家评审、主管部门审核、公安机关备案
分析	覆盖对象范围扩大，对新安全领域提出合规需求	更加注重防护效果，合规内容注重动态的攻防能力	从碎片化硬件布置的要求转为对一体化安全服务的要求	合规要求更严格	

来源：安全内参，头豹研究院编辑整理

2.2 云安全需求（1/2）

- 中国企业加速上云，云计算市场规模快速扩大，其中公有云是主要增长来源

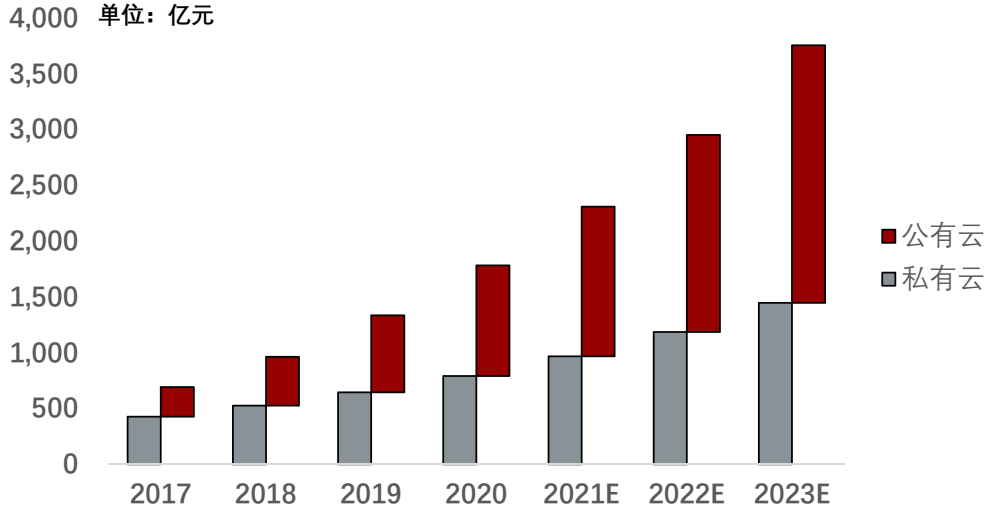
中国企业云计算使用率



- 66.1%的中国企业已经应用了云计算，云计算的渗透率继续稳步提升：2019年中国已经应用云计算的企业占比达到66.1%，相较2018年上升了7.5%
- 中国云计算使用率提升主要源于公有云的使用率提升：中国企业采用公有云的占比41.6%，较去年提高了5.2%；采用私有云的占比为14.7%，与去年相比仅有小幅提升

中国云计算市场规模及预测

以云计算为代表的新IT技术加速进入商业落地期



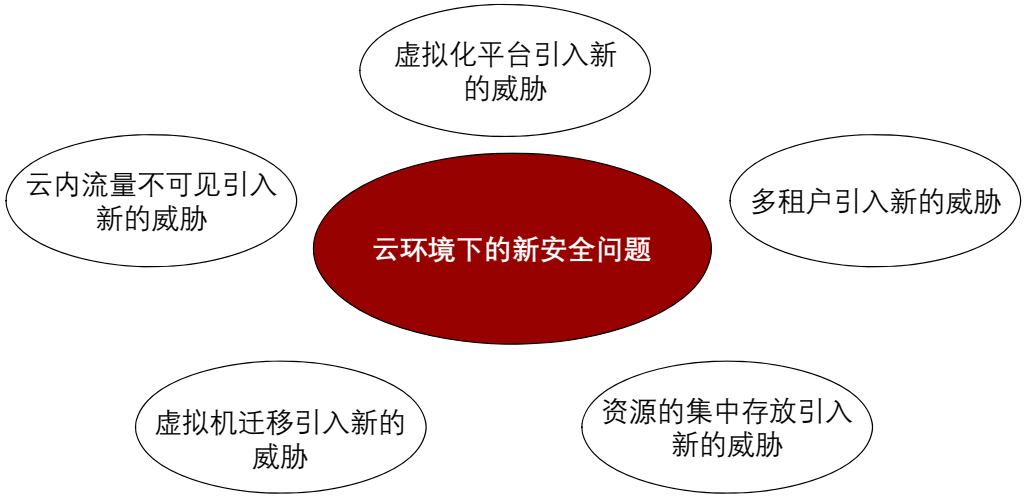
- 中国云计算市场高速增长趋势不变，预计2023年规模达4,800亿元：2019年中国云计算整体市场规模达1,334亿元，增速38.6%，预计未来几年增速保持增长，到 2023年市场规模将接近4,800亿元（不包含混合云）
- 公有云市场规模反超私有云：2019年中国公有云市场规模达到689亿元，私有云市场规模达645亿元公有云首次完成了规模上对私有云的反超。预计到2023年公有云市场规模将超过2,300亿元，私有云将接近1,500亿元

来源：中国信通院，头豹研究院编辑整理

2.2 云安全需求（2/2）

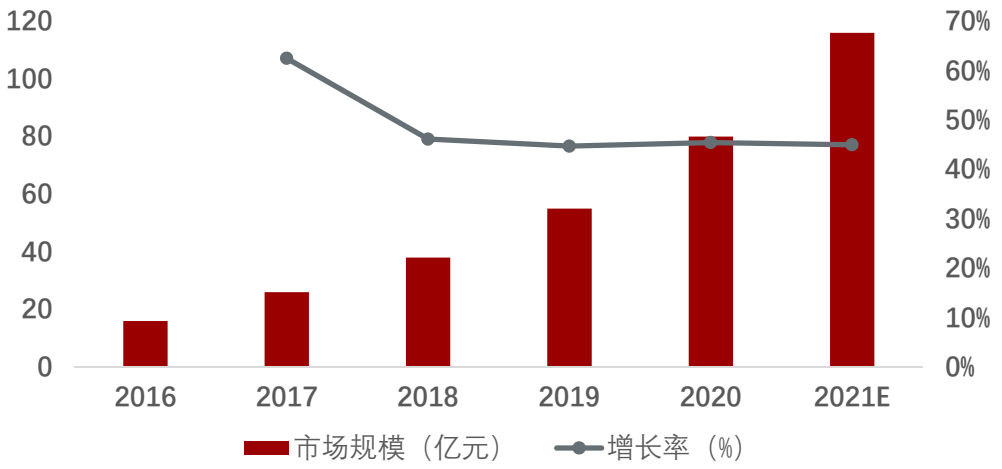
- **云环境带来新网络安全问题，安全配套需求快速增长，市场天花板高**

云环境下的新安全问题



- 虚拟化平台：虚拟化平台的设计漏洞，将成为新的威胁
- 多租户：多租户运行在同一台物理机上，边界消失，传统防护手段失效
- 云内流量不可见：虚拟机之间的互访采用传统手段不可见
- 资源集中存放：针对云计算中心的攻击更有价值
- 虚拟机迁移：安全策略应动态跟随调整

中国云安全市场规模及同比增速



- 云安全市场处于起步阶段，行业天花板高：2018年中国云安全市场规模仅为37.8亿元，市场还远未饱和，未来增长空间大；市场目前保持快速增长，2018年同比增长44.8%，预计未来几年云安全需求将持续快速增长，到2021年，行业规模增速保持在40%以上

来源：深信服，CCID，头豹研究院编辑整理

2.3 新安全理念

- **传统安全理念无法应对当前的网络安全形势，主动防御、一体化防御、动态防御的新安全理念将推进行业由产品向服务转型的过程**

传统网络安全理念与当下安全形势的冲突

传统安全理念

- 边界安全防御：通过防火墙等硬件产品隔离内外网，御敌于外，保证内网安全
- 碎片化的安全能力部署：“创可贴”式的产品形态，基于“差哪补哪”的思路进行网安建设，没有形成体系
- 依赖已知特征库检测威胁：检测网络事件，与已知特征库对照，检测出可能的网络攻击，发出预警

当下网络安全形势

- 网络边界模糊化：随着云计算应用的普及，传统的“内外网”边界越来越模糊
- 网络攻防两方地位不对等：攻击方只需单点突破，因此网络安全程度取决于最薄弱环节，防守方需要全线防护
- 网络攻击手段越来越隐蔽、复杂、多变：攻击手段变形方式多样，未知威胁如APT占据主流，传统基于特征库无法有效检测

新安全理念

打造主动防御能力：基于一体化的安全防护部署获得更全面的安全数据。结合大数据分析、机器学习等技术，主动感知、预测风险

建立体系化的安全能力：内部部件联动响应，打造安全闭环，对安全威胁进行发现识别、理解分析、响应处置的体系化操作

安全服务代替安全产品：布置齐全的安全产品价格不菲，且体系化的防御系统需要专业网安人员实时操作。因此，选择集成安全服务大势所趋

头豹洞察

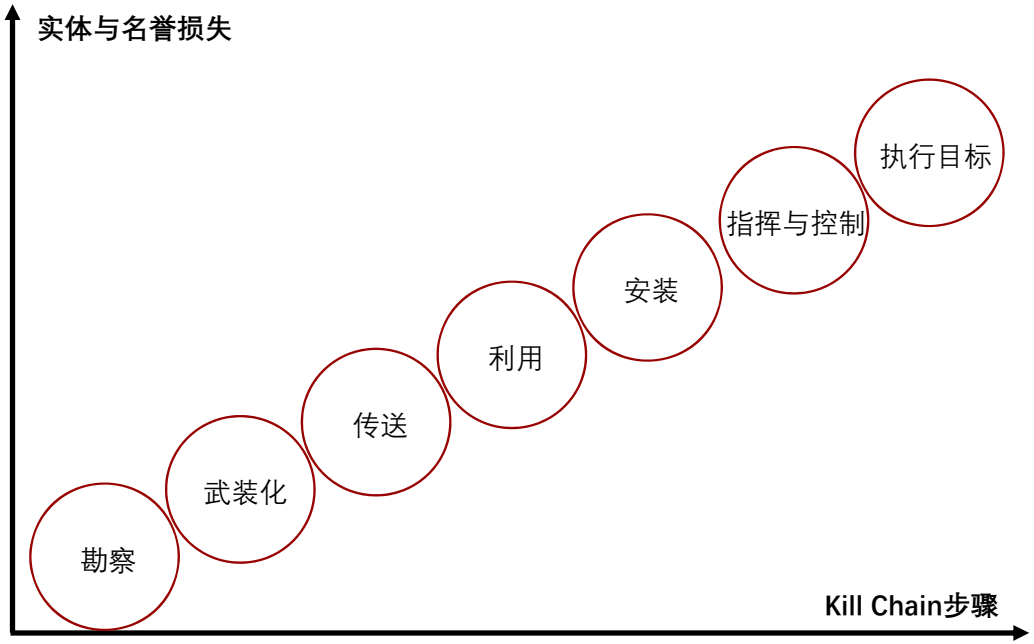
- 基于边界安全防御的防御理念逐渐失效：传统的被动防御多使用边界安全产品，如防火墙、IDS/IPS、防病毒等，但随着网络边界的模糊化，这种看大门式的防护理念逐渐失效
- 碎片化的安全能力部署不能防护网络攻击方协同联动的攻击闭环体系：传统的安全理念习惯根据合规要求，创口贴式的部署安全能力，没有形成安全闭环，内各部件孤立工作，不能实现有效的信息共享、能力共享和协同工作。相反，网络的攻击方却有着从侦察、武装、传送、利用、安装、指挥控制到执行目标的一系列闭环的攻击行动，信息和能力共享，容易找到防守方最薄弱的环节，迅速突破
- 基于已知特征规则的威胁检测不足以应对现在复杂的网络攻击手段：传统的威胁检测只能检测基于已知网络攻击的特征检测威胁，无法检测到APT等未知威胁，且现在网络攻击手段变形多、隐蔽性强，威胁特征库只能在网络攻击发生后总结该威胁特征，难以及时收集，实际防护能力较弱
- 当前新安全理念将推动安全服务替代安全产品

来源：北京网络安全大会，BCS，头豹研究院编辑整理

3.1 检测和响应时间是衡量安全服务能力的关键标准（1/2）

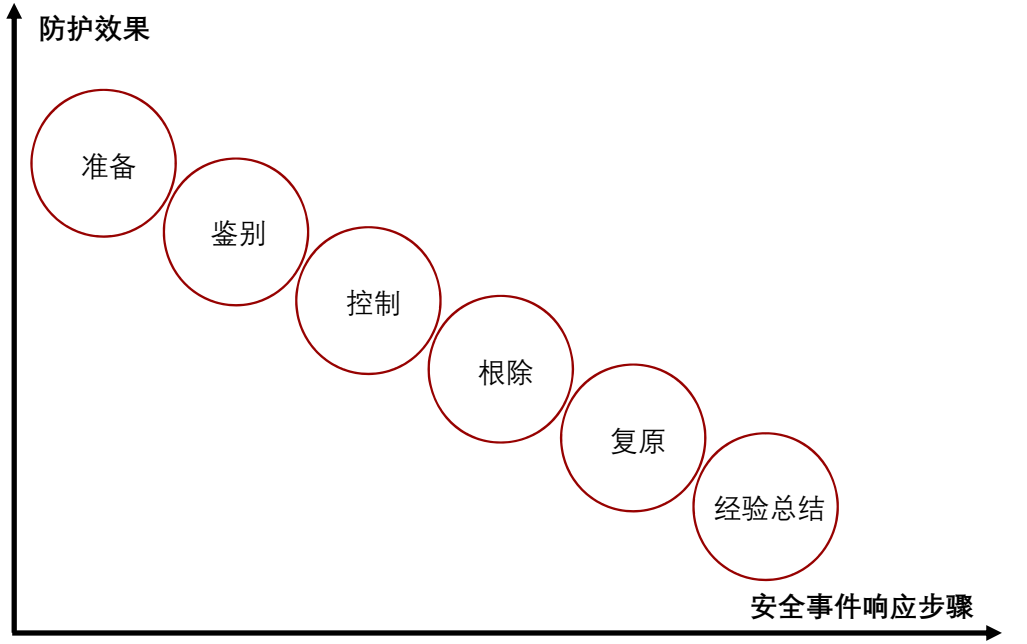
- **安全事件发生后，攻击推进的步骤越靠后，造成的损失越大；响应的步骤越靠前，防护效果越好**

网络攻击步骤与对应损失



- 网络攻击造成的损失程度取决于攻击被检测出的阶段：攻击越早被检测出来，该网络攻击造成的损失就越低
- 从“传送”开始，就是检测与响应的发力点：“传送”和之后的步骤，对应正在发生，和即将发生的威胁

安全事件响应阶段与对应时效性



- 安全事件开始响应所对应的步骤决定了防护的效果：基于攻击生命周期（Kill Chain）的相关信息，安全团队创建相对应的安全事件响应步骤，采取的步骤越靠前，防护效果越好
- 安全事件响应的步骤可以总结为“检测”和“响应”两大部分：“控制”之前的步骤属于检测，“控制”和之后的步骤属于响应

来源：卡巴斯基，头豹研究院编辑整理

3.1 检测和响应时间是衡量安全服务能力的关键标准（2/2）

- **网络攻防中防守方始终滞后于攻击方，优化MTTD和MTTR两个指标是提升防御方安全能力的根本问题**

防守方滞后于攻击方

	攻：攻击启动时间	防：入侵发现时间	攻：数据窃取时间	防：应急响应时间
秒级				
分钟级				
小时级				
天级				
周级				
月级				
年级				
				

威胁检测阶段
安全能力指标-MTTD

威胁响应阶段
安全能力指标-MTTR

头豹洞察

- 防守方相对攻击方，行动均具有滞后性，其中发现入侵环节滞后性尤为严重：以攻防对抗的角度看，防守方与攻击方的对抗主要在发现入侵环节和应急响应环节。在发现入侵环节，攻击方通常在分钟级启动攻击，而防守方主要在月级和周级才发现入侵，中间的时间差巨大。在应急响应环节，攻击方窃取数据的时间通常在分钟级或者天级，防守方主要在周级和天级作出应急响应，防守方在这一环节仍有明显滞后性，但相对及时一些

- 攻防方之间的时间差是网络安全防护的根本问题，同时降低MTTD和MTTR才能提升防守方安全能力：根据PPDR模型，当Pt>Dt+Rt时，系统即是安全的。Pt表示入侵者攻击安全目标花费时间；Dt是MTTD，表示平均检测时间，是指发现一个真正有风险的威胁所用的平均时间；Rt是MTTR，表示平均响应时间，指全面分析威胁并平息任何可能的风险所用的平均时间。因此，MTTD和MTTR共同决定了安全威胁的程度，是衡量防守方实际安全能力的关键指标，安全服务厂商需要同时降低MTTD和MTTR来提高其攻防能力

来源：Verizon，头豹研究院编辑整理

3.2 威胁检测技术能力探析（1/3）

- **主流威胁检测技术有IDS、SIEM、NTA，IDS技术逐渐不能适应当前网络环境，SIEM主要检测内部威胁，NTA是比较新的技术，结合大数据、机器学习等技术，未来发展空间大**

威胁检测主流技术原理及特点对比

	技术原理	特点
入侵检测系统（IDS）	❑ 预先确定特征知识库里的各种攻击模式，对计算机或网络系统中发生的事件进行监视和分析，利用特征检测判断异常或者入侵行为	❑ 威胁检测的重要手段，有近30年的发展历史，但在当下一些网络场景下，并不能有效发现威胁 ❑ 存在主要三个缺陷：一是大量误报，需要安全人员不断对IDS系统进行调整；是二漏检严重，依靠特征库做判断，所以不能判断未知攻击；三是事后检测到，适时性不好
系统跟踪事件（SIEM）	❑ 从广泛的网络硬件和软件系统中获取日志数据，实时分析这些数据，将事件和个别异常或行为模式关联起来，进行威胁检测	❑ 是目前解决内部威胁的主要技术 ❑ 从第三方收集日志和事件信息时，所收集数据的质量是无法预测和控制的，许多信息是碎片的、孤立的、不相关的
网络威胁检测 (NTA)	❑ 融合了传统的基于规则的检测技术，及机器学习、高级分析和特征分析等技术，对正常的流量进行收集和分析，从而建立出正常的企业网络流量模型，用以检测企业网络中的可疑行为，尤其是失陷后的痕迹	❑ NTA通过对实际流量进行分析、对比，发现威胁，因此即使是APT攻击，也能被检测出来 ❑ NTA性能主要取决于行为模型的质量，模型质量依赖于模型训练的能力，这又取决于安全大数据的量级与质量，因此，拥有数据优势的大厂商NTA技术占优势

来源：安全牛，安全内参，头豹研究院编辑整理

3.2 威胁检测技术能力探析（2/3）

- **威胁情报是辅助威胁检测的重要手段，能提高主流威胁检测技术的实际效果，有效性得到高度认同**

主流威胁检测方式与威胁情报形成互补

基于安全传感器

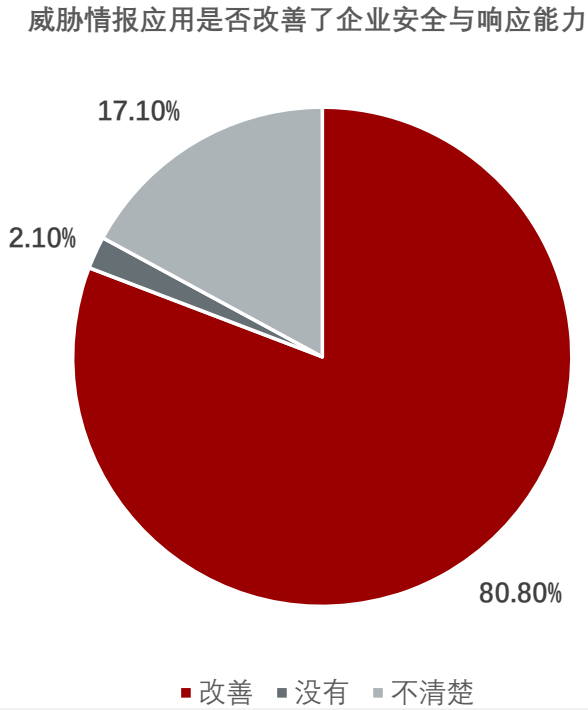
- 原理：试图寻找异常行为或已知的恶意签名活动
- 常见传感器：防火墙、入侵检测系统(IDS / IPS)、应用程序网关防病毒/反恶意软件、终端防护
- 缺陷：安全传感器提供的威胁相关的连续事件流会产生大量噪音，不能凸显真正重要的威胁

基于威胁情报

- 原理：用适当上下文，在正确的时间提供正确的信息
- 优势：显著减少检测时间，过滤噪音，减少误报，发现正在发生和即将发生的重大网络安全威胁

- 威胁情报提高现有威胁检测工具的价值：使用威胁情报与现有的传感器结合，会缩短他们的平均检测时间和平均响应时间，扩展当前的安全工具的价值，并通过攻陷指标的机器分析发现前所未有的威胁

威胁情报的有效性得到高度认同



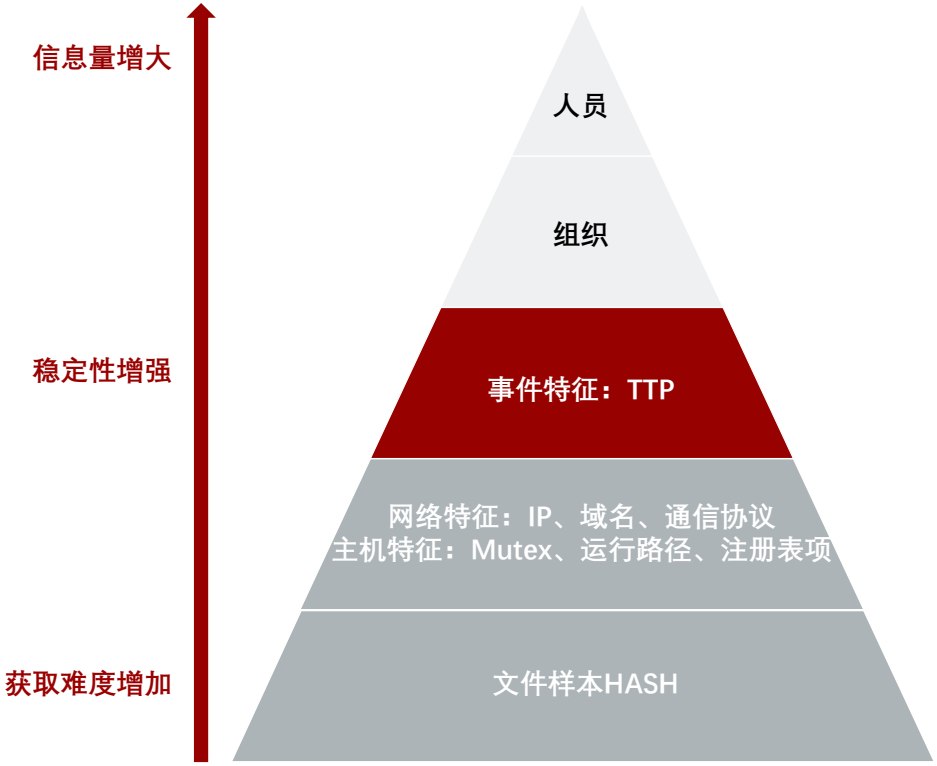
- 大部分企业认为威胁情报有效性高：根据SANS2019年发布的报告，80.80%的受访者认为威胁情报能改善企业的安全状况，仅有2.10%受访者认为威胁情报是无效的

来源：SANS，头豹研究院编辑整理

3.2 威胁检测技术能力探析（3/3）

- **威胁情报目前主要用于检测传统IOC，但TTP情报最有价值，是主动防御体系里的重要组成部分，TTP情报是未来威胁情报发展方向**

威胁情报的分类及用途



进攻反制阶段的前沿技术，在中国未被广泛利用：根据TTP情报，了解攻击对手的的手法，再利用大数据、机器学习等技术，找到相似攻击手法，从而推出攻击人员和组织

主动防御的关键：属于“敌在控我”类情报，是价值高但不易获取的高级情报

最为广泛应用的情报IOC：属于“敌在攻我”类情报，是现实而紧迫的危险，是易于获取但利用价值不高的低级情报

头豹洞察

- TTP情报最有价值：TTP处于痛苦金字塔塔尖，对攻方而言，TTP反映了攻击者的行为，调整TTP的时间和金钱成本最高；于防守方，基于TTP的检测及响应给对手造成痛苦最高，因此TTP是最有价值的一类情报
- TTP情报是主动防御的重要工具，是未来威胁情报的发展方向：比起其他IOC，TTP更能检测未知威胁，在“敌在探我”阶段就检测到威胁，将网络攻击的损害降低到最小，也给安全团队足够时间作出反应，实际的提高防守方的安全能力

来源：奇安信，安全牛，头豹研究院编辑整理

3.3 应急响应技术能力探析（1/2）

- SOAR的核心能力是编排与自动化，通过整合人、工具和流程，提升应急相应能力，弥补了SIEM的短板

SOAR核心特点及优势分析

主要功能	核心特点	优势分析
安全能力编排化	❑ 基于工作流引擎的多模安全编排器 ❑ 可视化安全剧本编组器 ❑ 面向社区的剧本及应用的协作与其享	安全流程化和告警响应自动化的基础
安全流程自动化	❑ 工作流引擎驱动的剧本执行自动化 ❑ 应用及动作执行自动化 ❑ 告警分诊与响应自动化 ❑ 案件调查与处置自动化	减少了人工的干预，大幅提升应急处置的效率：将客户分散的安全能力和响应过程标准化，形成剧本库和应用库，实现团队、工具和流程的整合与协同联动
告警响应自动化	❑ 全方位告警接入 ❑ 智能化告警分诊 ❑ 编排化告警调查 ❑ 自动化告警响应	聚焦关键告警，提高告警质量：自动化聚合告警，自动计算告警的可信度和优先级，聚焦关键告警；对告警信息进行补充调查分析，将低质量的告警变成高质量告警，排除虚假告警

来源：IT168，奇安信，头豹研究院编辑整理

描述

- ❑ SOAR工作原理：将各类安全应急响应过程中的动作进行组合，将原始数据（主要来自SIEM）作为剧本，按照剧本化的方式自动开展应急响应及追踪溯源工作。借助编排好的安全应急响应剧本，当安全事件发生时，系统将通过自动化的手段进行响应，减少人工干预
- ❑ SOAR从全网整体安全运维的角度去考虑，提升整体安全响应效率：SOAR将分散的检测与响应机制整合起来，不仅从单点考虑，而是站在一个安全大脑的位置，调度各种资源，标准化流程，自动响应事件，优化整体效率
- ❑ SOAR针对SIEM对安全人员的高度依赖和告警低质量泛滥两大问题，进行改善：SIEM一大问题是数据来源质量低，进而得出大量低价值告警，将正真有用的高价值告警淹没，SOAR的智能分诊功能解决了这一问题。另一方面，SIEM注重“收集”，响应部分高度依赖安全技术人员，SOAR通过标准化响应过程，将自动化提高，减轻了安全人员的负担，同时提高应急处置的效率

3.3 应急响应技术能力探析（2/2）

- 传统SIEM/SOC应急响应存在明显短板，不能满足网络安全实际需求，SOAR与SIEM互补，改善应急响应能力

传统SIEM/SOC事件响应能力的短板

传统SIEM/SOC响应中的短板

事多人少

- 大量的运维事件/告警
- 有限的运维人员
- 人工无法及时处置

响应时间长

- 在不同系统和工具间切换
- EDR/NDR设备参与
- 人工执行封堵
- 审批不及时

知识累计高度依赖个人

- 运维事件响应处置方式需要人为判断
- 对运维人员的处置经验要求高

自动化

- 将事件响应过程转化为一致的、可重复的工作流

协同化

- 联动多个系统和平台，调动不同的安全工具和技术

案例库

- 固化安全专家经验
- 响应流程可以借鉴案例库

SOAR对传统SIEM/SOC响应的改善

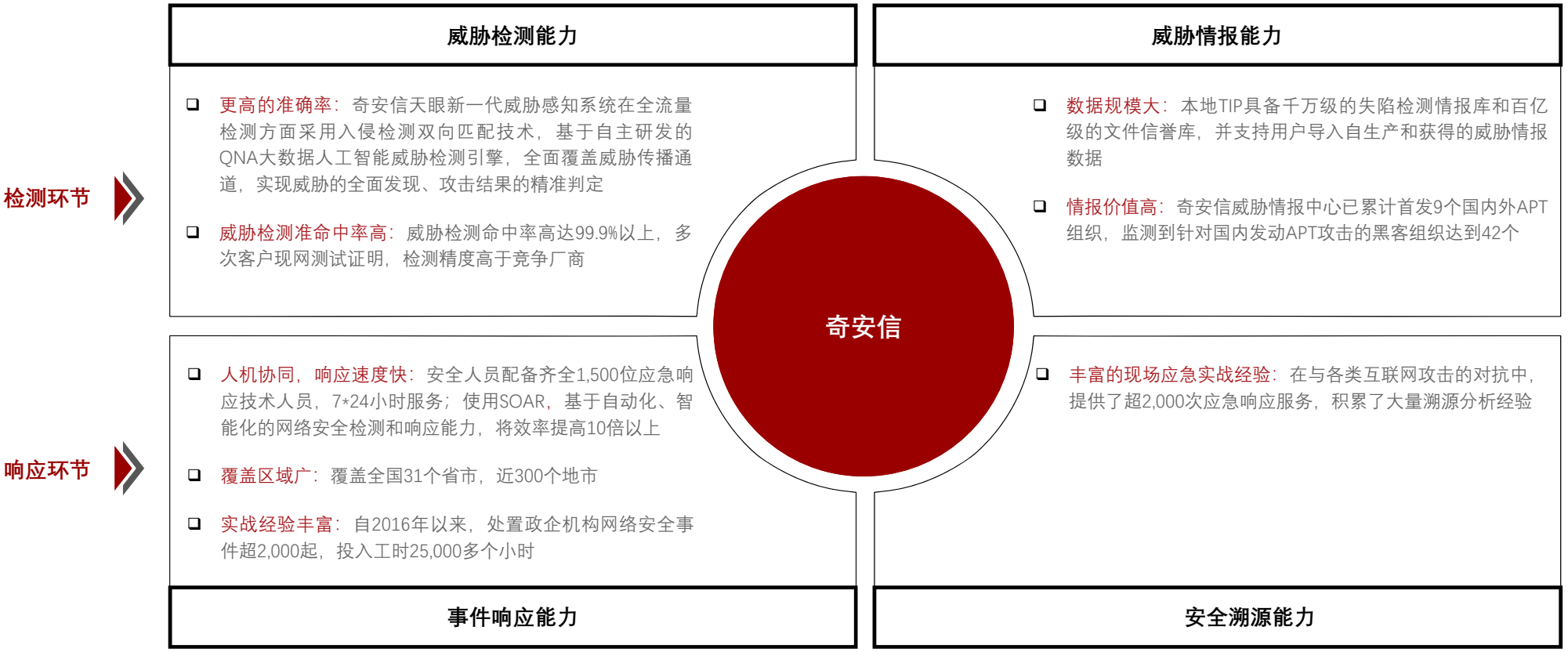
描述

- 传统SIEM/SOC使用反馈不佳：据C.A.沃克调查显示，当被问及其所用SIEM系统的有效性时，只有28％的受访者认为他们非常有效。对已经安装和使用了SIEM的企业，有三分之一的IT部门表示如果有可能，他们宁愿将SIEM拿掉不用
- 传统SIEM/SOC高度依赖人工处理，人与安全工具没有整合，响应效果不佳：传统SIEM/SOC自动化能力偏低、工具之间整合度低，产生的大量告警和响应需要人为处理和决定；且安全工具分散，使得安全人员要在不同工具间切换，响应时间过长
- SOAR自动化强，改善SIEM/SOC的响应能力：SOAR加强了自动化、协同化、和案例库的使用，弥补了SIEM/SOC的短板

来源：绿盟科技，安全内参，头豹研究院编辑整理

4.1 奇安信基础能力分析

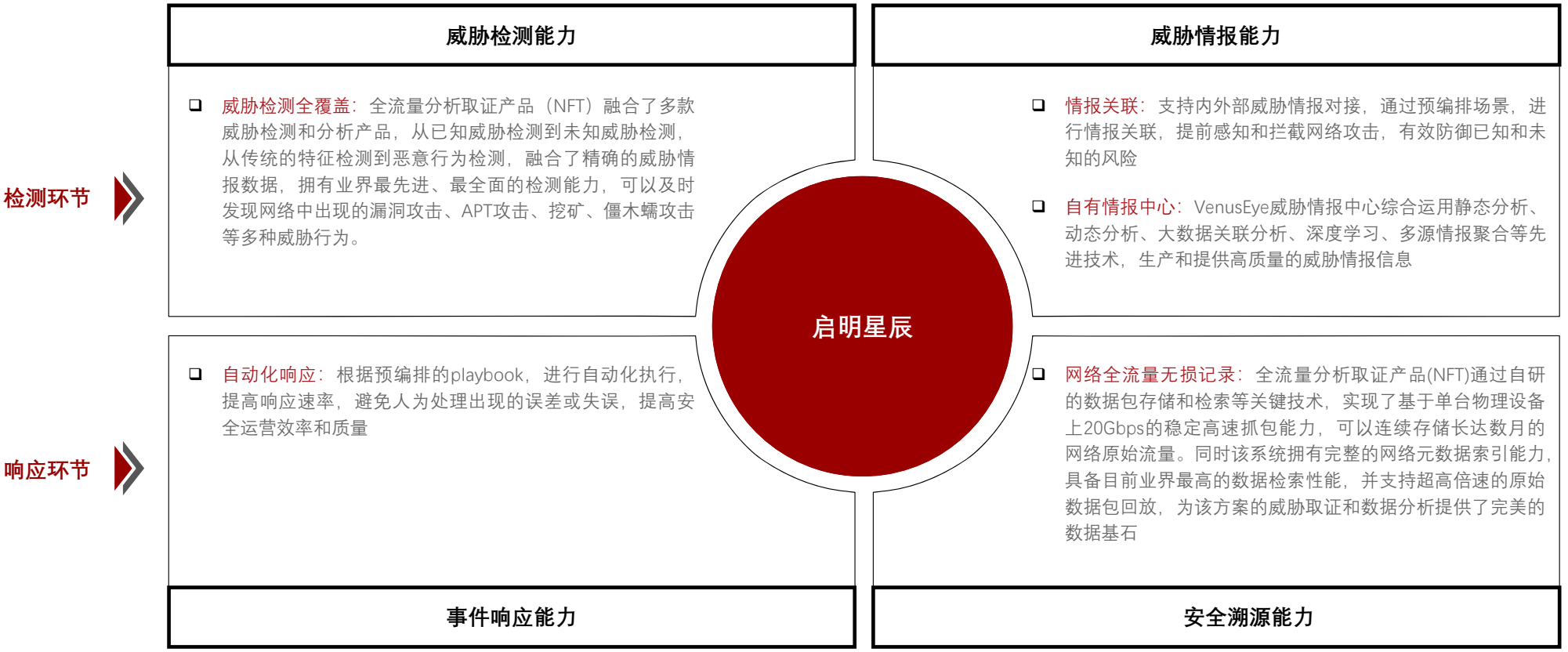
- **奇安信作为传统安全厂商龙头，安全人才充足，覆盖面广，实战经验丰富是其主要优势；在新技术上，奇安信也积极尝试并取得一定成效**



来源：奇安信，头豹研究院编辑整理

4.2 启明星辰基础能力分析

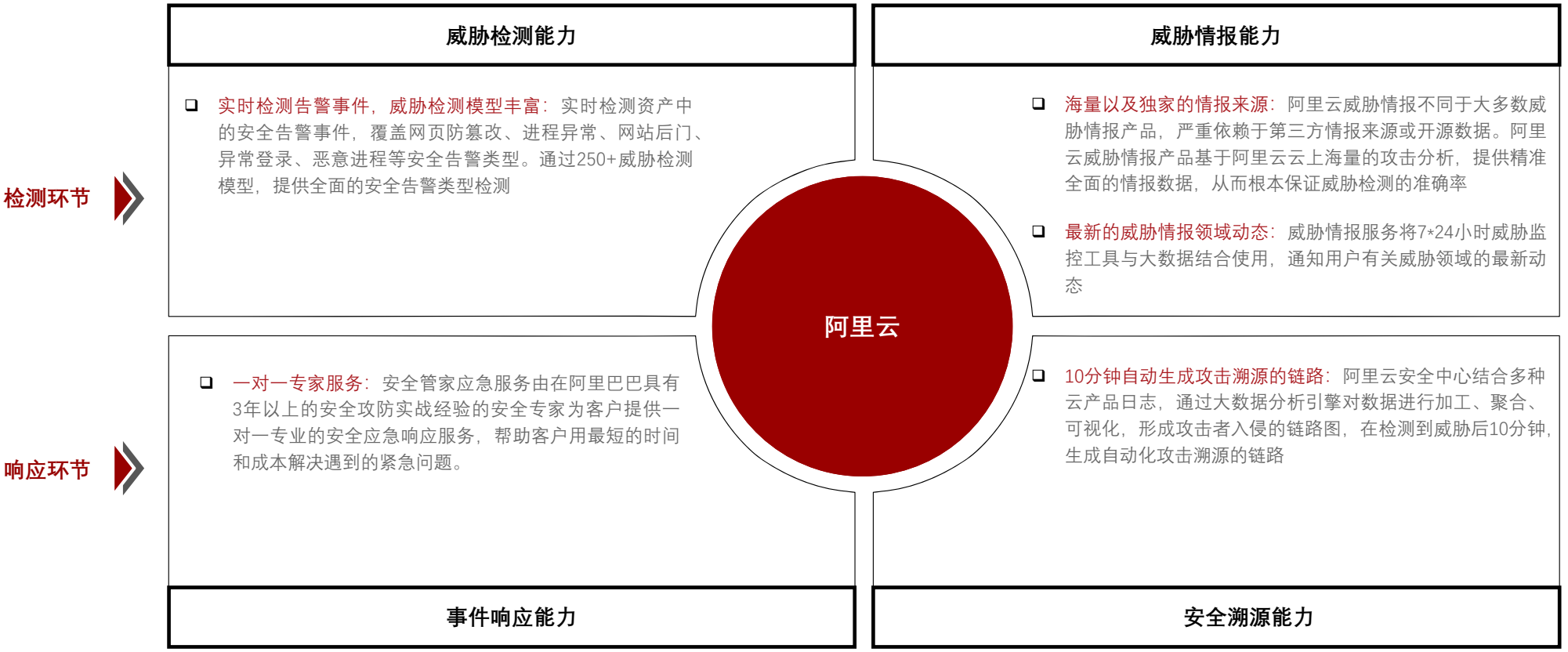
- **启明星辰是传统安全厂商中的领导者，积极研发新技术和新产品，在检测环节和相应环节均有较强能力**



来源：IT168，头豹研究院编辑整理

4.3 阿里云基础能力分析

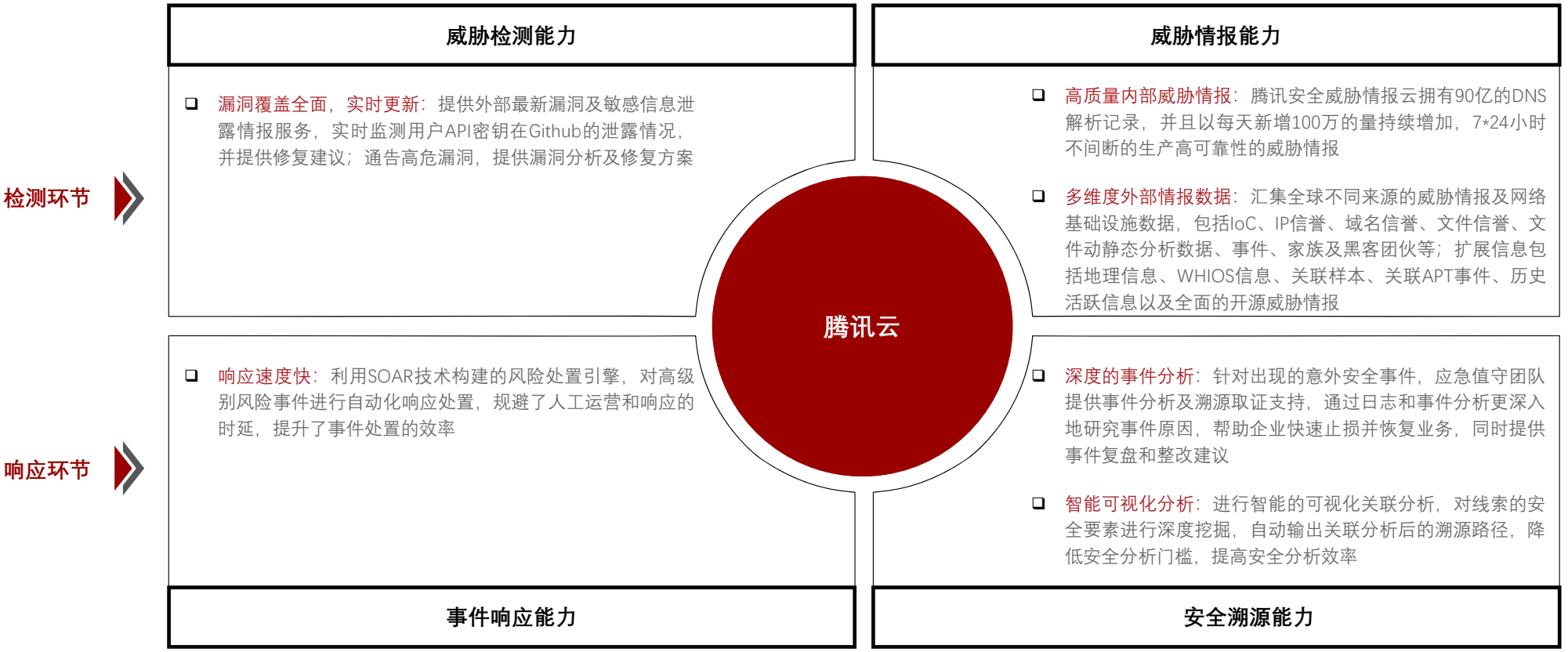
- **阿里云是中国云安全龙头，在电商平台和云平台上积累的独家海量数据是最大优势**



来源：阿里云，头豹研究院编辑整理

4.4 腾讯云基础能力分析

- **腾讯云是中国云安全厂商中的佼佼者，产品线齐全且自有高质量的数据源，在云安全行业竞争力强**



来源：腾讯云，头豹研究院编辑整理

方法论

- 头豹研究院布局中国市场，深入研究10大行业，54个垂直行业的市场变化，已经积累了近50万行业研究样本，完成近10,000多个独立的研究咨询项目。
- 研究院依托中国活跃的经济环境，从网络安全、云安全、攻防对抗等领域着手，研究内容覆盖整个行业的发展周期，伴随着行业中企业的创立，发展，扩张，到企业走向上市及上市后的成熟期，研究院的各行业研究员探索和评估行业中多变的产业模式，企业的商业模式和运营模式，以专业的视野解读行业的沿革。
- 研究院融合传统与新型的研究方法，采用自主研发的算法，结合行业交叉的大数据，以多元化的调研方法，挖掘定量数据背后的逻辑，分析定性内容背后的观点，客观和真实地阐述行业的现状，前瞻性地预测行业未来的发展趋势，在研究院的每一份研究报告中，完整地呈现行业的过去，现在和未来。
- 研究院密切关注行业发展最新动向，报告内容及数据会随着行业发展、技术革新、竞争格局变化、政策法规颁布、市场调研深入，保持不断更新与优化。
- 研究院秉承匠心研究，砥砺前行的宗旨，从战略的角度分析行业，从执行的层面阅读行业，为每一个行业的报告阅读者提供值得品鉴的研究报告。

法律声明

- 本报告著作权归头豹所有，未经书面许可，任何机构或个人不得以任何形式翻版、复刻、发表或引用。若征得头豹同意进行引用、刊发的，需在允许的范围内使用，并注明出处为“头豹研究院”，且不得对本报告进行任何有悖原意的引用、删节或修改。
- 本报告分析师具有专业研究能力，保证报告数据均来自合法合规渠道，观点产出及数据分析基于分析师对行业的客观理解，本报告不受任何第三方授意或影响。
- 本报告所涉及的观点或信息仅供参考，不构成任何投资建议。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。在法律许可的情况下，头豹可能会为报告中提及的企业提供或争取提供投融资或咨询等相关服务。本报告所指的公司或投资标的的价值、价格及投资收入可升可跌。
- 本报告的部分信息来源于公开资料，头豹对该等信息的准确性、完整性或可靠性不做任何保证。本文所载的资料、意见及推测仅反映头豹于发布本报告当日的判断，过往报告中的描述不应作为日后的表现依据。在不同时期，头豹可发出与本文所载资料、意见及推测不一致的报告和文章。头豹不保证本报告所含信息保持在最新状态。同时，头豹对本报告所含信息可在不发出通知的情形下做出修改，读者应当自行关注相应的更新或修改。任何机构或个人应对其利用本报告的数据、分析、研究、部分或者全部内容所进行的一切活动负责并承担该等活动所导致的任何损失或伤害。

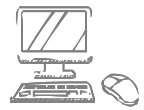
读完报告有问题?

快，问头豹！你的智能随身专家

千元预算的

高效率轻咨询服务

扫码二维码
即刻联系你的智能随身专家



STEP03 解答方案生成

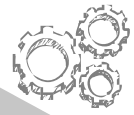
大数据×定制调研
迅速生成解答方案

STEP01 智能拆解提问

人工智能NLP技术
精准拆解用户提问

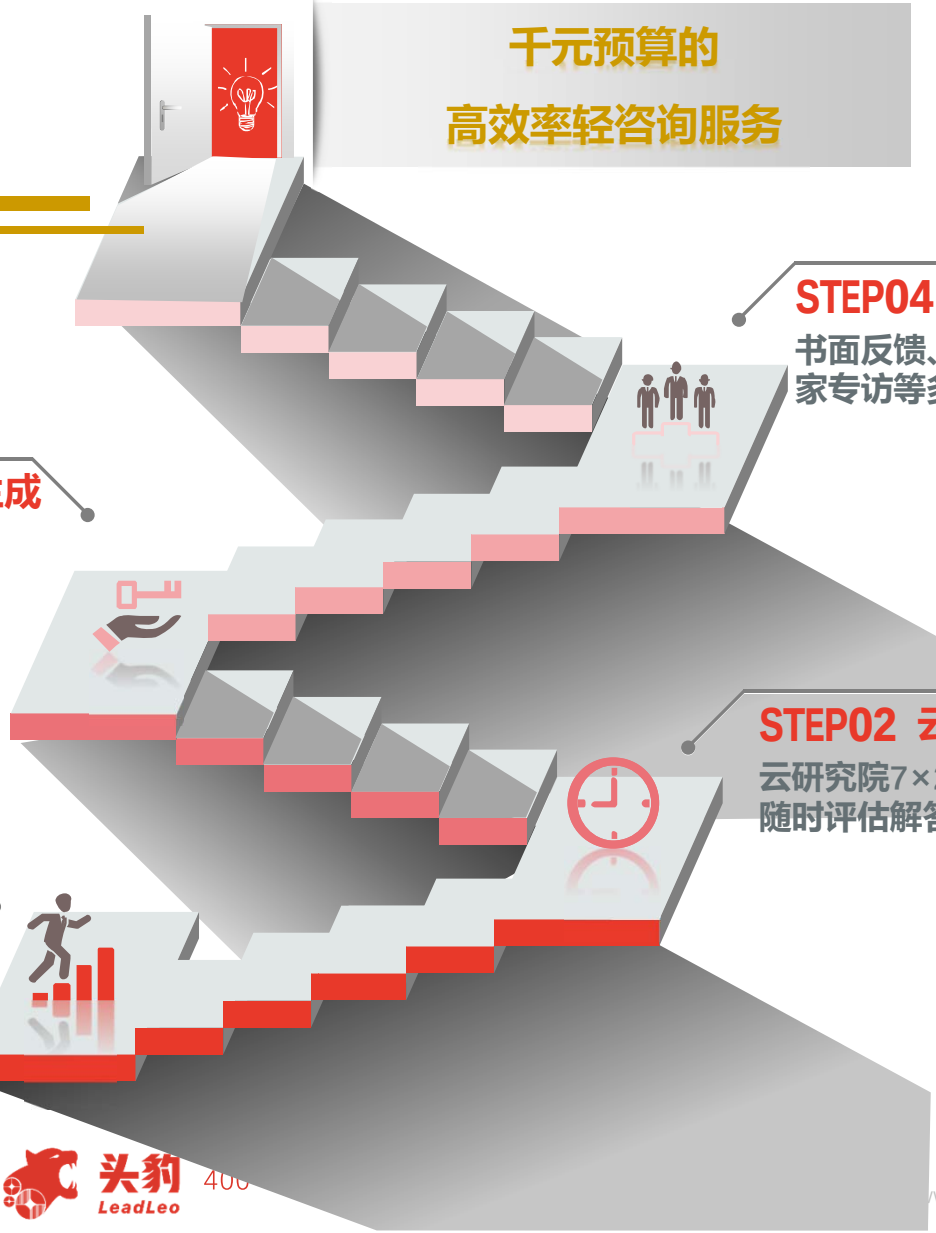
STEP04 专业高效解答

书面反馈、分析师专访、专家专访等多元化反馈方式



STEP02 云研究院后援

云研究院7×24待命
随时评估解答方案



头豹 LeadLeo 400