头豹 LeadLeo

FROST & SULLIVAN 沙利文

2020年
中国云主机安全市场报告

2020 China Cloud Workload Protection Market Overview

2020年中国クラウドワークロード安全市場報告

报告标签：自适应、云原生、人工智能、超速响应、架构适配

头豹研究院
弗若斯特沙利文咨询（中国）

报告说明

沙利文谨此发布中国云安全系列报告之《2020年中国云主机安全市场报告》年度报告。本报告旨在分析中国云主机安全产品发展现状、产品特点、技术动向及发展趋势，并识别中国云主机安全市场竞争态势，反映该细分市场领袖梯队品牌的差异化竞争优势。2020年第四季度，沙利文联合头豹研究院对云安全领域核心产品进行了下游用户体验调查。受访者来自泛互联网、金融、医疗、教育、制造、物流等多个行业，所在公司规模不一，细分领域有别。

本市场报告提供的云主机安全趋势分析亦反映出云安全行业整体的动向。报告最终对市场排名、领袖梯队的判断仅适用于本年度中国云主机安全发展周期。

本报告所有图、表、文字中的数据均源自弗若斯特沙利文咨询（中国）及头豹研究院调查，数据均采用四舍五入，小数计一位。

报告摘要

- **功能横向拓展、纵向深化**

主流云主机安全品牌采取“四合一”的产品形态，依托多引擎工具，横向拓展病毒查杀能力，纵向细化资产清点颗粒度，深化信息关联能力。合规基线一键部署能力和基线自定义功能或为用户潜在需求。

- **安全能力精益演进**

技能细化是云主机安全价值提升的核心策略，多元技术集成有助于安全产品实现功能开放和一致性管理；未来10年，中国将诞生一批专精于1-3条产品线的中小型新锐云安全品牌。

- **从零和游戏趋向合作共赢**

新型网络安全环境下，更多厂商从数据孤立、各自为营转向情报互通的数据合作，实现情报数据的最大化价值；此外，厂商可通过产品公测的形式间接实现与攻防领域优秀人才的合作，训练产品，树立品牌口碑。

- **云原生技术实际应用**

用户业务多云部署趋势下，云主机安全能力与云原生技术架构适配的颗粒度将细化，推动多云架构、跨云架构下统一安全管控的实践，最终建成主动适配云原生各项技术的安全运营中心。

目录

- 中国云主机安全市场综述 ---------- 05
  - 云主机安全基础能力 ---------- 05
  - 云主机风险简述 ---------- 06
- 中国云主机安全价值链简析 ---------- 07
  - 云主机安全价值链 ---------- 07
  - 云主机安全能力拓展 ---------- 08
- 中国云主机安全市场结构 ---------- 09
  - 云主机安全市场规模 ---------- 09
  - 云主机安全用户特征 ---------- 10
- 中国云主机安全市场发展现状简析 ---------- 11
  - 云主机安全定价模式 ---------- 11
  - 云主机安全技术特点 ---------- 12
- 中国云主机安全发展趋势 ---------- 13
  - 从零和竞争趋向合作共赢 ---------- 13
  - 云原生技术的实际应用 ---------- 14
- 中国云主机安全市场竞争 ---------- 16
  - 中国市场非本土品牌简析 ---------- 16
  - 云主机安全竞争力评价维度 ---------- 18
  - 云主机安全综合竞争力表现 ---------- 19
  - 中国云主机安全领袖梯队 ---------- 20
- 方法论 ---------- 24
- 法律声明 ---------- 25

Contents

- China Cloud Workload Protection Market Overview ---- 05
  - Common Attacks on Cloud Workload ---- 05
  - Basic Function of Cloud Workload Protection ---- 06
- China Cloud Workload Protection Value Chain Analysis ---- 07
  - Cloud Workload Protection Value Chain ---- 07
  - Core Technology of Cloud Workload Protection ---- 08
- China Cloud Workload Protection Market Structure ---- 09
  - Cloud Workload Protection Market Size ---- 09
  - Cloud Workload Protection User Feature ---- 10
- China Cloud Workload Protection Market Status ---- 11
  - Cloud Workload Protection Pricing Mechanism ---- 11
  - Cloud Workload Protection Technical Feature ---- 12
- China Cloud Workload Protection Market Outlook ---- 13
  - Zero-sum Competition to Win-win Cooperation ---- 13
  - Practical Application of Cloud Native Technology ---- 14
- China Cloud Workload Protection Market Landscape ---- 16
  - Non-local CWP Brands in Chinese Market ---- 16
  - Cloud Workload Protection Brand Rating Index ---- 18
  - China Cloud Workload Protection Competitive Landscape ---- 19
  - China Cloud Workload Protection Leadership ---- 20
- Methodology ---- 24
- Legal Statement ---- 25

中国云主机安全市场综述——云主机安全基础能力

当前云主机安全基础防护功能以监测、检测、告警为主要目的，资产清点、入侵检测2大功能是决定品牌竞争力的核心模块，云主机安全功能颗粒度和稳健性决定用户粘性

■ **资产清点、入侵检测构成核心模块**

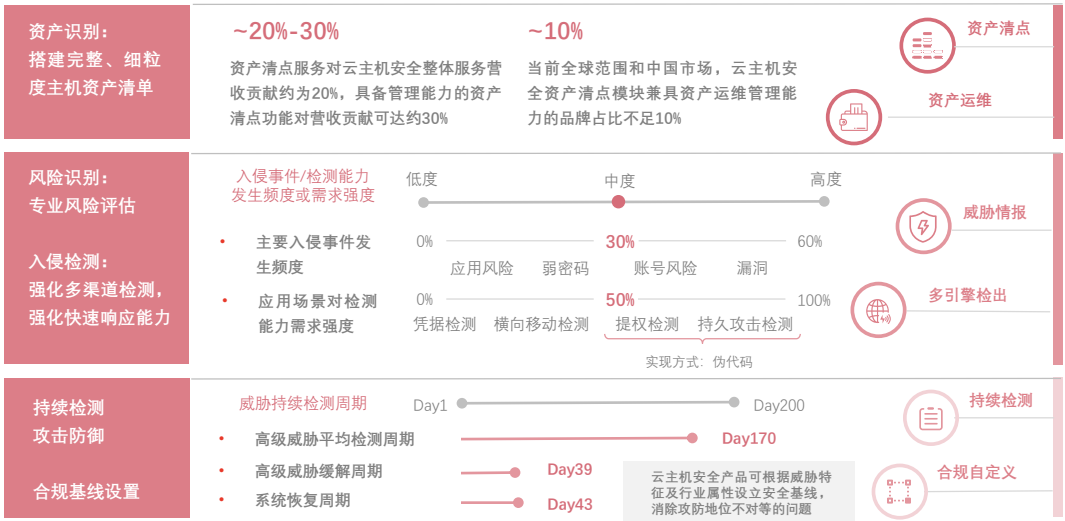
资产清点是云主机安全的核心功能模块，不同品牌资产清点的内核能力呈现较大差异，主要在细粒度、准确度、速度三个维度拉开差距。以青藤云安全为例，其资产清点功能具备出众的向下钻取能力和数据点关联能力，受到下游用户依赖，并推动安全工具向安全管理工具进阶。

入侵检测功能对应黑客攻击行为的颗粒度（检测锚点分类设置）决定检出能力高低。成功的黑客入侵行为平均需要5至8个步骤完成，入侵检测模块对攻击流程设定的检测维度、检测指标颗粒度越细，越能够帮助用户在恶意入侵事件早期实现检出，采取阻断措施。

■ **基于“四合一”主流形态，推动功能演进**

当前，主流云主机安全品牌采取“四合一”的产品形态，并逐步于资产清点、风险分析、入侵检测、合规基线四项模块基础上，结合开源引擎、自研引擎、第三方引擎等，横向拓展病毒查杀能力。在纵向层面，厂商可通过细化资产清点细粒度，提高信息关联度的途经构建安全运营能力。此外，合规基线模块升级配备一键部署能力和基线自定义能力是下游用户潜在需求所在。

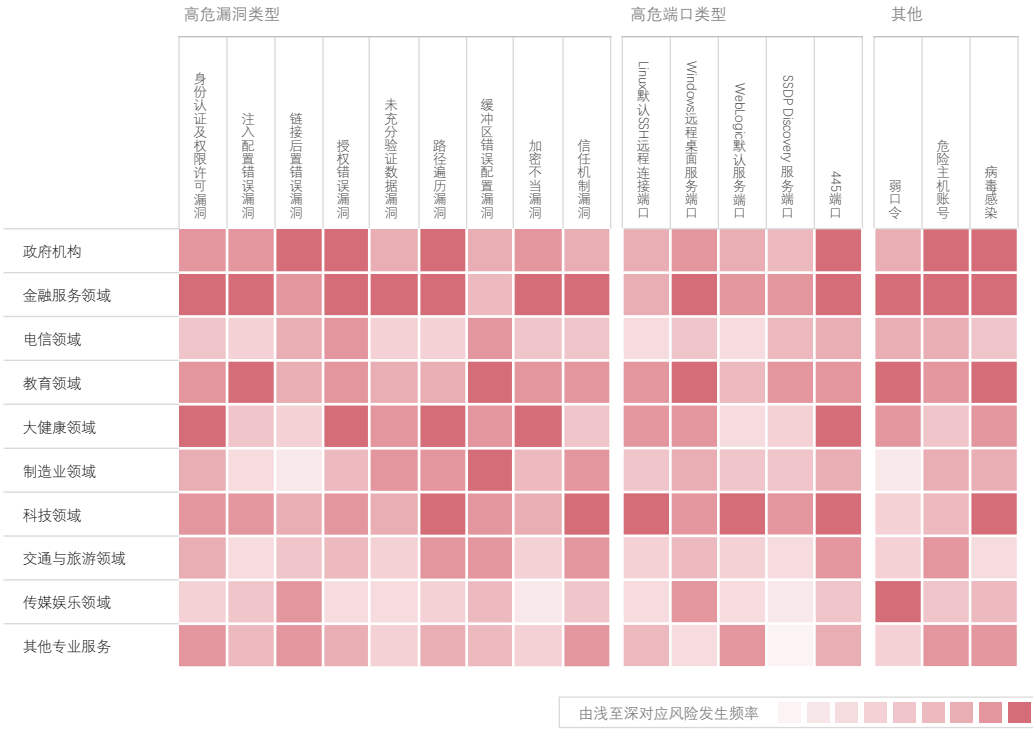
云主机安全基础能力：以资产识别、入侵检测为核心



中国云主机安全市场综述——云主机风险简述

随IT产业和云服务市场快速升级扩容，云端主机、设备端主机面临的攻击面扩大，AI算法的应用显著提高安全产品风险对抗能力，但变种攻击和未知威胁的预测仍为难点

云主机安全应用于下游各类场景面临风险类型及频度



- **多云、跨云（公有云、私有云、混合云）网络环境日趋复杂，云主机攻击面持续扩大**

多云环境下，云主机系统遭受恶意攻击的频率上升，云主机被成功入侵平均时长缩短至约20小时。带有开放端口和漏洞的云端主机成为黑客攻击的首要对象。云主机面临的安全漏洞包括资源管理问题、代码失误、配置错误、代码注入等，补丁修复缺失的资产漏洞成为入侵突破口。

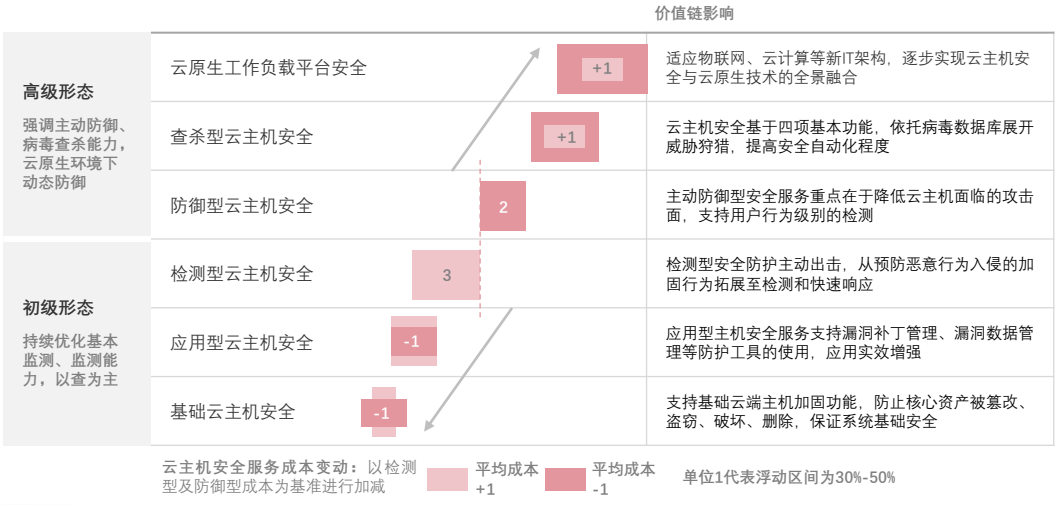
云主机端存在大量易受攻击的资产端口（包括远程连接服务端口、远程桌面服务端口、数据库端口、邮件服务端口等），亦面临较高的勒索病毒及病毒变种攻击风险。此外，云主机软件弱密码、高危账号（开放Root权限）、补丁修复不及时等问题使得恶意网络攻击行为潜在控制面持续扩大。

中国云主机安全价值链简析——云主机安全价值链

传统边界安全防护理念已无法满足安全产业下游复杂业务场景的网络安全运维需求，基于云主机安全构建完整的全端、全场景计算安全产业成为网络安全人的共同目标

云主机安全形态持续演进，融合云原生能力构建产业链生态

- 云主机安全产品形态的持续演进意味着更高成本的产品性能和服务，多元技术集成将推动产业链效应形成，有助于实现安全产品长链价值



■ **多渠道扩容威胁情报数据库，挖掘产业链上游价值**

安全情报数据库是云安全产业价值链上游的"活水之源"，在网络安全厂商独立维护安全数据库之余，第三方安全情报平台的出现丰富了产业链上游的竞争形态，安全厂商情报数据互换的合作方式则让安全数据资产的价值得到最大发挥。

■ **构建完整的计算安全产业链，实现网络层、文件层、应用层全面可信**

未来，网络安全厂商将打造更加丰富的大云主机安全产品形态。鉴于开发场景和真实应用场景存在差异，云主机安全需要实现全端全场景覆盖（传统PC、Serverless PC、IoT等）。

传统被动防护模式（特征匹配、发现病毒）将由具备主动防御能力的多云主机安全模式替代，在主机网络层依托微隔离、IP账户防爆破封禁等机制实现网络级别可信，通过文件完整性保护机制、文件防篡改机制实现文件级别的可信，另外可结合RAAS应用层保护机制实现应用级别的可信，最终构建从网络到到操作系统、文件和应用的全面可信。此外，中游安全闭环需扩大智能运维能力的覆盖面，以应对高级形态的网络攻击（如APT等），降低下游业务场景的安全运维成本。

中国云主机安全价值链简析——云主机安全能力拓展

云主机安全功能演进呈现出以安全管控、稳健部署、用户灵活自定义为导向的特点，且在底层与云原生融合深化、与多云架构全面适配，在应用层呈现态势可视的交互效果

追查攻击外联路径的溯源能力

超过80%的勒索行为利用弱密码、系统漏洞等完成入侵，勒索行为恶意脚本在云主机中隐藏并横向扩散，云主机安全基于ATT&CK检测模型形成勒索追踪能力，溯源链路延伸至勒索行为外联路径。

防容器逃逸检测能力

容器部署环境下，攻击行为从容器逃逸到底层承载节点、宿主机或逃逸到其他容器和节点的行为更为常见，部分高级攻击行为甚至能够穿破多租户，影响所有虚拟机用户。容器逃逸防范工具依赖规模化检测能力和底层I/O数据检测能力。对非云原生安全厂商而言，容器逃逸防范能力实现难度更高。

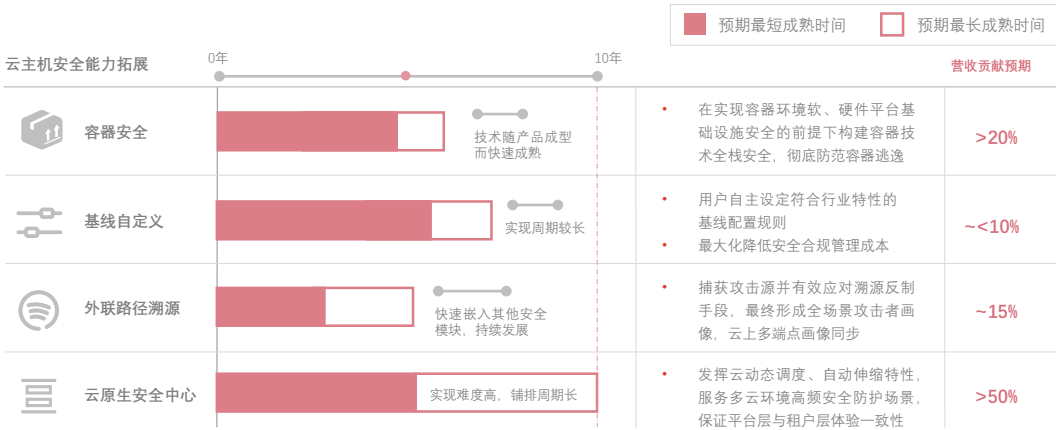
自定义基线检查能力

当前，各大厂商云主机安全基线检查功能基本满足用户遵循等保2.0、CIS等安全规范的需求。对于单一的、带有行业属性的自定义基线需求，厂商可根据用户所属行业政策规定，提供定制化服务。未来，更强的差异化基线检查能力或体现在云主机内置安全规则与安全等级规范匹配的细化程度，高颗粒度的规则自定义部署或耗费安全团队大量时间成本和人力成本。

基于安全防护的安全管理能力

安全运营管理能力是安全防护能力的升级与集成，云主机安全的资产清点功能天然具备管理属性，高级形态的资产清点将帮助用户更加明确网络安全产品与资产的对应关系，提高安全运维性价比。

以云原生技术应用为导向的云工作负载平台能力拓展

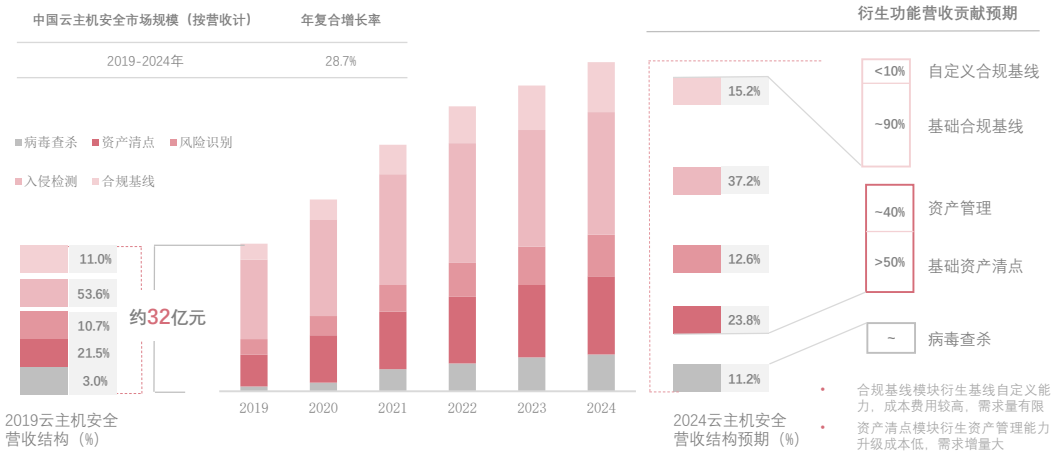


中国云主机安全市场结构——云主机安全市场规模

网络安全市场整体呈现较强的碎片化特征，云主机安全细分市场或成为网络安全领域第二个防火墙赛道，未来5年，云主机安全细分市场规模年复合增长率将保持在约30%的水平

中国云主机安全市场规模构成及衍生功能营收贡献，2019-2024年

- 中国云主机安全市场具备增量扩容空间，商业机会存在于新生用户增长、License付费模式被动收益、运营商合作推广等方面



■ **云主机安全市场规模处于上升增长期**

云主机安全构成云安全市场的核心。2019年起，更多厂商加入云主机安全赛道，推动该细分市场快速扩容，云主机安全将成为网络安全领域第二道防火墙。沙利文数据显示，2020年上半年，云主机安全市场规模在云安全市场整体规模中的占比达到40%以上。未来5年，预计该细分市场将实现约30%的年复合增长率。

■ **下游市场刚性需求显著，云主机安全市场增长潜力高**

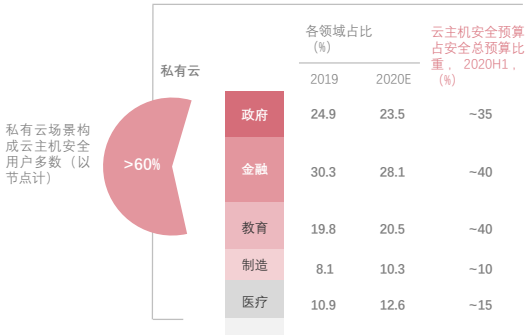
云主机安全市场增长迅速，具备可观的潜在扩容空间。当前，多数下游用户仅在核心资产完成云主机安全的部署，多数用户亦选择层层递进的模式铺排云主机安全能力。未来随IT架构升级和云服务环境更加成熟，中小型企业对更多付费功能的需求将逐步凸显。整体而言，云主机安全市场的增长空间存在于：①下游用户品牌推荐行为和背书效应带来新生用户增长；②用户更多核心业务将完成在云上的部署，核心资产对安全需求升级；③云主机安全模块能力升级，新功能打开新的议价空间；④网络安全等级保护升级，政策层面对安全国产化的引导利好市场份额的保有和提升。

中国云主机安全市场结构——云主机安全用户特征

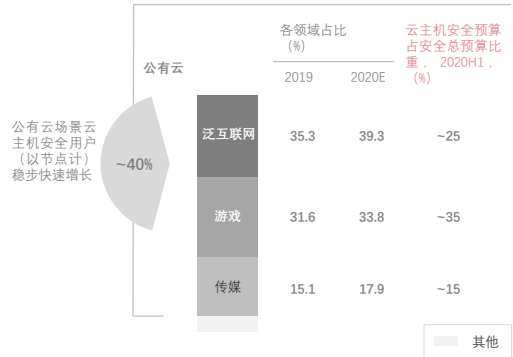
数字化转型背景下，中国市场将出现更多高安全属性、高产品性能需求的政企用户，随着下游业务上云、多云部署并于云上迁徙，用户对安全产品兼容能力的要求或成为核心

中国云主机安全用户结构及用户云主机安全预算占比

中国云主机安全私有云场景节点部署占比



中国云主机安全公有云场景节点部署占比



云主机安全用户共性及特性

下游用户基于行业安全规范、业务安全需求部署云主机安全产品。鉴于主机、云主机承载大量核心业务资产，用户普遍对产品安全性能要求较高。大型企业用户业务场景复杂且实力雄厚，偏好轻量级Agent模式的云主机安全形态，用以应对中上层复杂攻击问题。对中小型企业而言，云厂商提供的云主机自带基础安全功能已基本满足日常业务需求，故而更偏好安全配置管理加固服务。此外，部分行业数字化转型需求更高，对安全属性要求高，是云主机安全服务天然适合铺排的领域。

中国云安全用户应用场景复杂度居全球高位

当前，低成本的恶意攻击行为已形成黑色产业链，并随应用场景持续衍生变种。中国政企机构在遭受各类恶意网络行为攻击后，愈发意识到网络安全范畴的重要性。从安全4层墙至7层墙，后起的中国用户对安全工具的应用复杂度远高于境外市场。同类型交易平台、社交平台面临的安全挑战在中国市场和海外市场不可同日而语。基于应用场景差异，以色列网络安全厂商Checkpoint将中国网络安全市场定义为高增长性、高复杂度市场。基于应用层纷繁复杂的安全需求，厂商需更加注重在研发阶段考虑云主机安全解决方案的适配性，融入DevSecOps的理念。

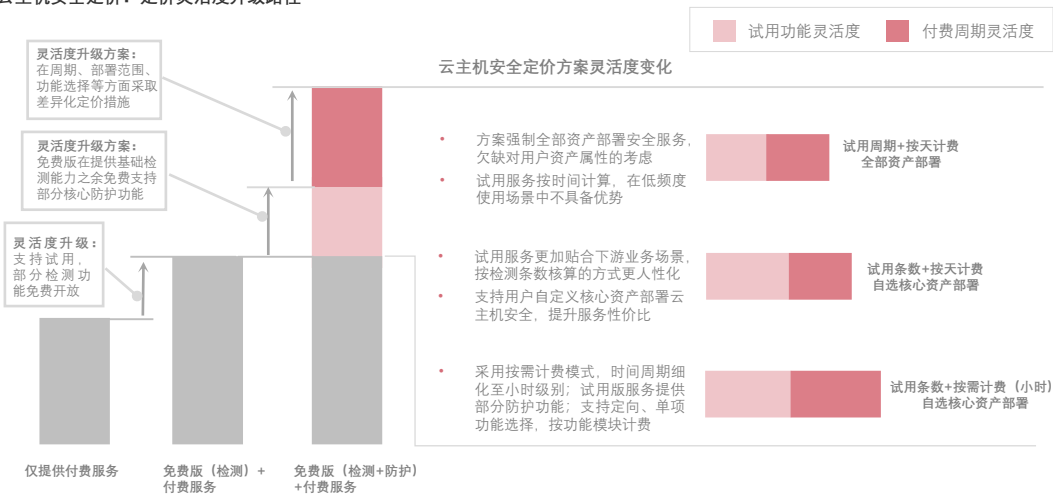
取长补短，为私有云用户提供完整安全解决方案

未来10-20年，网络安全必是IT领域需求增长最显著的领域。随下游用户核心业务接续上云，利用AI能力完成安全自动化部署将成为下游用户刚需。用户关键敏感业务在云上的防护必为关注重点，未来，云厂商可取长补短，以集成商的角色为用户提供完整安全解决方案。

中国云主机安全市场发展现状简析——云主机安全定价模式

云主机安全支持多元计费模式，不同品牌计费灵活度差异较大；提高产品性价比、开放度、兼容性和自定义水平是赢得潜在用户、实现用户转化、保持用户粘性的关键

云主机安全定价：定价灵活度升级路径



■ **厂商定价模式颗粒度不同，用户友好水平显差异**

当前，常见的云主机安全计费模式包括使用周期计费、按需付费、License付费、订阅付费等，不同厂商在云主机安全配置规则、数量、版本等维度也存在计费方式的差异。

就使用周期维度而言，目前腾讯云和华为云支持更加用户友好的付费方案，腾讯云镜主机安全最小时间颗粒度细化至天，华为云推出的按需付费模式则支持以小时为计费单位。此外，用户是否有权自定义云主机安全配置的范围也体现出厂商计费灵活度的差异。

■ **基本模块保持稳定计费，云原生化功能模块或具有更高溢价空间**

根据下游实际情况分析，按套购买模式更能为用户创造成本效应。而License模式、订阅模式则有利于厂商实现持续盈利，获得被动销售保障。

沙利文判断未来3至5年，用户将初步实现云上灵活迁徙，安全产品多形态定价策略有助于吸引多云用户、跨云用户，收割多云环境下用户迁徙红利。远期，为持续提高用户转化率，厂商之间需要加深合作。沙利文判断，厂商云主机安全套餐与其他云环境兼容越高，盈利机会越大。此外，根据用户在既有云上的安全配置方案，厂商可提供客制化兼容分析服务，为用户规划性价比最优且能对既有云主机安全方案实现补短的方案，为用户节省成本，取得规划付费收益及潜在用户转化收益。

中国云主机安全市场发展现状简析——云主机安全技术特点

技术细化是云主机安全核心价值提升的关键所在，多元技术集成有助于安全产品实现功能开放和一致管理；未来10年，中国将诞生一批专精于1-3条产品线的新锐安全品牌

■ **精益：安全防护技能颗粒度细化**

随网络安全业务走向成熟，云主机安全防护技能呈现出由粗粒度向细粒度演进的特点。传统防护模式下，安全工具基于IP进行扫描检测，而随零信任理念的推行，在最小信任原则下，云主机安全从每流、每IP“一检查、一授权”升级为每数据包“一检查、一授权”。此外，基线检查从软件检查发展为版本检查，升级为每版本漏洞检查。在授权层面，使用权限的定义由指定人变为指定时间，再细化至当前“定人+定时+定职”的机制，最大限度发挥身份认证工具的有效性。

■ **多元：技术手段趋于全面**

IP用户对云端和设备端主机安全防护技术手段升级的要求较为明确和显著。云主机安全不断嵌入更加丰富和完善的技术能力。以漏洞扫描为例，传统漏扫行为在主动模式下完成，云主机安全则具备被动扫描手段，在云上实时监控、捕捉网络流量，通过流量识别提高漏洞扫描和监控的效率。再如，云主机安全支持代理扫描技术，支持通过客户端代理扫描流量、发送报告报文，或通过主动发送嗅探包，伪造P2P传输协议等方式主动探索、识别恶意流量。

■ **进阶：防范技术向管控技术过渡**

管控能力是基础安全防护能力的集成和升级。云主机安全可通过将资产清点模块升级为资产安全管理模块的方式实现防范向管控的过渡。多数产品在资产识别层面的能力仅限于判断软、硬件资产的性质，而管控意味着出具全景可视的资产地图（如特定IP区域装载的虚拟机、数据库数量和类别等），对资产损坏率、折旧率、更新率等出具定期报告，在资产盘点环节即可实现对恶意网络行为的防范，最大程度提升安全管理功能在技术层面和用户层面的体验一致性、不同平台安全管配的统一性，加深云安全在不同平面的联动防护。

综合化极化：覆盖下游行业>10

- 多区域云环境安全管理
- 基于态势感知的大屏安全中心

专业化极化：深耕方向>20

文件安全配置、无文件恶意软件识别、事件+情报高级取证、容器安全、内存攻击检测阻断、微服务安全等

■ **综合化能力与专业化能力的两级分化**

- 安全技术的精细化、多样化和技术集成三因素驱动下，云安全产业的发展呈现出综合化和专业化两端极化的趋势，并与此同时趋于标准化。综合化意味着云安全产品形式和种类愈加丰富，专业化意味着单个产品、应用能力的细化，功能更加专一，云平台本身将集成和固化更加广泛的基础安全配置。
- 当前，安全产业仍然以面向大B企业用户开发综合型产品为主，传统边界网络安全厂商多数遵循大产品路线，但未来随更多SME业务上云，多云环境下的专业化安全产品将成为主流，更多新锐网络安全厂商将着眼于1至3个产品线进行深耕。

中国云主机安全发展趋势——从零和竞争趋向合作共赢

新型网络安全环境下，更多厂商从数据孤立、各自为营转向情报互通的数据合作；此外，厂商可通过产品公测的形式间接实现与攻防领域优秀人才的合作，训练产品，树立口碑

■ **多渠道联动协作：安全情报价值最大化**

沙利文数据显示，2020年上半年，全球范围网络安全厂商获取威胁情报的渠道以公开情报源、专业威胁情报供应商为主（超70%的安全团队采用前述两种方案）；采集开源情报的安全厂商占比接近60%；与其他安全厂商达成威胁情报战略互换关系的安全团队、独立构建威胁情报数据库的安全团队数量相较2019年上半年分别有近10%和约5%的提升。

安全厂商通过与各类安全情报供应商（专业情报团队、同业安全团队）能力结合，可助力下游用户间接获取更多威胁情报，实现情报数据价值最大化。此外，在中国网络安全市场，更多本土与非本土安全厂商之间展开合作，非本土厂商加快情报数据库在中国的落地。以色列知名防火墙厂商Checkpoint认为："零和竞争在网络安全行业不再是战略导向，厂商之间达成战略合作成为常态，情报库多渠道实时更新将显著提升云上和云下终端的智慧程度"。

■ **"众人拾柴"：通过公测集成多形态样本，实现品牌效应**

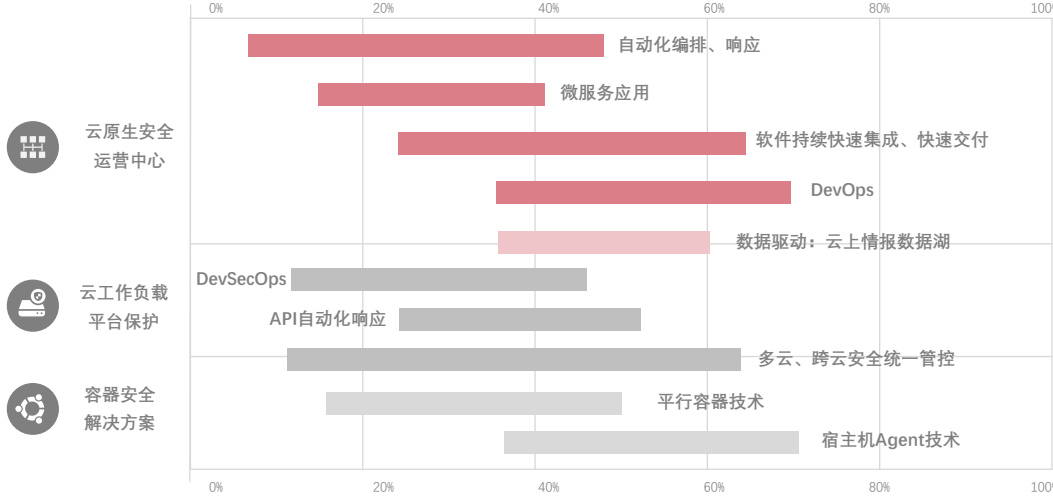
IT行业面临更加复杂的需求，下游应用场景纷繁复杂，网络攻击及其变种形态快速迭代，与此对应，安全厂商的实时防护能力需要更快速地晋升。安全厂商核心产品能力公测以青藤云安全为例，2020年3月，青藤云安全以自研雷火引擎（基于反混淆等价回归算法的Webshell检测引擎）为测试对象，设置100万奖金池，开展为期1个月的公测活动。作为安全防护领域的顽疾，Webshell网页后门形式简单且易于变形，黑客使用成本低，但难以彻底防护。青藤云安全于此次公测汇集22个漏洞响应平台、超1,000名顶级白帽子，完成与超过32,000个Webshell样本的动态对抗，最终检出率为99.54%。出色的检出成绩树立青藤云安全在未知威胁对抗领域的品牌标杆形象。通过公测，厂商收获形态丰富的样本，其安全引擎核心算法（推理运算、虚拟运算等）得到新一轮深度训练，应对攻击样本变形和混淆问题的能力迅速强化。对安全产业整体而言，公测活动带动的行业新风范或倒逼更多的安全厂商专注磨练产品核心技术。

相对第三方评测机构的静态样本检测模式,公测活动营造的安全对抗环境更能凸显"动态对抗"价值。公测活动在助力厂商扩大品牌影响力、获得行业认可的同时，与攻防领域专业人才对抗的实战场景对产品表现带来挑战。

中国云主机安全发展趋势——云原生技术的实际应用

用户业务多云部署趋势下，云主机安全能力与云原生技术架构适配的颗粒度将细化，推动多云架构、跨云架构下统一安全管控的实践，安全产品将主动适配云原生技术

云主机安全应用：可实现商用的云原生技术/功能模块成熟度



注：色块长度代表该项技术从初级到成熟所需花费的周期，长度越短，成熟越快

■ **云主机安全从技术演进、技术环境两个维度适配云原生架构**

云主机安全与云原生架构适配主要体现在两个维度：首先在于技术演进的适配。随着终端服务器向虚拟机过渡，虚拟机升级为Serverless容器，大主机架构持续演进，传统安全管控模式和系统思维不足以支撑云上安全运维系统的全面构建。面对新的基础架构，云安全产品是否能够主动适配并且细化适配颗粒度将成为考量云安全产品性能的指标。

其次在于技术环境的适配。中国国产化操作系统开发取得可见进展，国产化芯片（鲲鹏、昇腾等）快速迭代，相关行业政策更加强调安全自主可控。为适应国产化大趋势下的安全合规要求，满足国产操作系统和芯片深层的安全需求，网络安全产品线要与技术环境全面适配。

■ **云主机安全技术演进，推动云原生安全运维中心的构建**

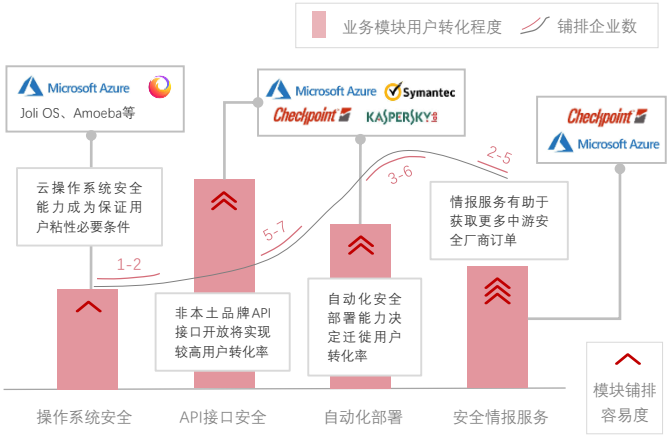
云原生统一安全中心的构建需要安全左移、自动化维护、安全数据同步等能力的支撑，云主机安全产品轻量化Agent自动化部署能力、情报数据汇聚形成的资源池、资产清点模块自带的安全运营属性将对云原生安全运维中心的构建起到对标支持作用。在此基础上，云主机安全协同镜像安全、运行时安全、编排安全等容器解决方案，可全面应对多云架构、跨云架构下的新型安全挑战，主动适配更加复杂的云上、云下业务环境。

中国云主机安全市场竞争——中国市场非本土品牌简析

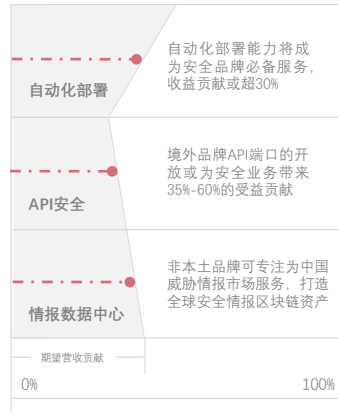
境外网络安全厂商、云厂商面对逐步成熟且更加规范的中国网络安全市场，宜调整竞争策略，拓宽思路，协同中国本土安全品牌，上中游合作打造产业链效应

中国市场非本土品牌安全业务拓展及潜在收益贡献

中国市场非本土品牌云主机安全相关业务铺排方向及品牌示例



非本土品牌中国安全业务营收贡献预期



- **境外网络安全品牌：深化与中国市场的融合策略，调整在安全产业链中扮演的角色**

全球范围内，北美地区云计算业务头部品牌如亚马逊、微软、IBM等依托自身在云原生领域的技术积累和先发优势，快速渗透云安全产品线，意图领导服务器安全、容器安全产业发展路线。头部云厂商的安全战略对全球云主机安全产品形态和发展方式具有参考价值。

全球化趋势演进的背景下，中国云安全市场重要性不可同日而语，中国本土边界安全品牌的进步、中国云厂商的渗透以及新锐优秀品牌的竞争不断挤压境外品牌在中国的网络安全市场份额。

境外厂商遵循中国网络安全规则的程度、与中国本土市场融合的策略，以及境外厂商在中国云安全产业链中扮演的角色将决定其品牌是否可在日趋激烈的竞争中取得一席之地。

传统竞争模式下，境外品牌集中关注中国网络安全产业链的中游市场，未来，中国国产化安全品牌在政策利好、地域就近等方面享有的优势将更加明显，境外厂商或趋向网络安全产业链上游，通过自身在全球范围的安全情报数据积累，依托在云计算领域的技术集成，以上游数据供应商角色、云计算和AI技术供应商角色更加广泛地参与到中国网络安全市场竞争中，协同中国本土安全品牌，实现合作共赢。此外，境外厂商需持续强化自身业务与中国网络安全市场规范的适应力，在业务层面及合规层面同步实现快速响应。

中国云主机安全市场竞争——中国市场非本土品牌简析

在中国网络安全等级保护规则日趋严格的背景下，境外厂商可通过数据库本地部署、参与本土企业间技术联盟、共享安全情报等策略纵向渗透中国云安全产业上下游

Checkpoint：助力中国安全市场打通全球情报数据湖，落实本地快速响应

安全情报服务落地：以色列网络安全厂商Checkpoint认为，海外网络安全品牌在中国市场是否能够长期发展取决于厂商实现本地化落地服务的能力。Checkpoint基于中国政府在数据合规、安全合规层面的要求，做到威胁情报数据库在中国境内落地。Checkpoint通过在全球各地部署的分支机构持续扩容威胁情报数据库，支持安全标识全球同步。其数据库服务在中国市场的落地有助于本地用户快速实现信息查询，原始请求无需转移到境外即可识别数据库覆盖的所有安全情报。

国家政策支持：以色列政府鼓励以色列网络安全品牌在中国市场推进业务本地化，支持同中国本土企业的合作。相较而言，美国品牌因面临不可控政治因素掣肘，在本地化快速响应层面“力不从心”。

当前，Checkpoint是为数不多的在中国市场实现安全情报落地的境外网络安全厂商，自1995年以来积累的海量安全情报让Checkpoint在云主机安全产业上游形成显著先发优势。

多云主机安全：随IT产业和云服务市场的快速进步，以防火墙业务起家的Checkpoint着手布局一整套云上安全服务，在基于web系统的安全服务基础上走向“Cloud World”，意在利用容器技术、自动化编排工具部署多云主机安全系统，依托关键业务自动部署的策略激发市场对云主机安全的需求。

亚马逊AWS：安全能力快速扩展，维持既有用户粘性

安全模块快速扩展：AWS云基础设施在灵活度、安全性方面的扎实表现有目共睹，AWS云安全模块助力用户实现数据存储和应用程序的快速部署。在中国市场，AWS考虑到下游应用场景的复杂性，其云安全模块在保证底层基础设施自动实时监测和检测的基础上，在SaaS层面采用大量自动化部署工具，并采取冗余及分层控制模式，实现基础设施层安全能力、Web层安全能力、应用层安全能力在数据中心、服务中心的快速复制。

保持云用户粘性：云主机安全业务层面，AWS在中国市场的用户更多来自原有云上用户，且面临各类中国本土安全厂商的竞争。提供更加便利、可靠的底层云安全服务是AWS维持云用户粘性的必要条件。

微软Azure：加固操作系统安全，应对潜在威胁

微软Azure在应对操作系统攻击方面具备先发优势。凭借自身在操作系统开发、维护方面积累的超过30年的经验，微软针对云端和设备端主机系统受损问题开发出功能丰富的安全问题分析工具。

在中国市场，微软Azure快速复制全球安全能力，采用AI算法曝光更多潜在威胁，降低云上用户的应用和数据可能面临的风险。在合规方面，微软成为首批通过中国工信部认证的可信云认证成员，并与中国网络安全厂商建立技术层面和业务层面的合作。此外，微软Azure向中国市场提供更加开放的API接口以及混合云操作系统，并以独立的中国数据中心确保中国用户在云上业务的安全。

中国云主机安全市场竞争——云主机安全竞争力评价维度

沙利文设定基础指数、成长指数、服务能力、市场影响力四个评审维度，对中国本土云主机安全品牌竞争力进行多因素分层次评估

	细分指标	指标要点	指标权重(100%)
基础指数	AI云查杀引擎	衡量厂商云主机安全产品应用AI技术搭建云查杀鉴定模型的能力	
	二进制查杀引擎	衡量厂商云主机安全产品对未知二进制木马、病毒等识别与响应处理能力	
	Webshell查杀引擎	衡量厂商云主机安全产品对未知Webshell识别与响应处理的能力	
	攻击及入侵检测	统计厂商云主机安全产品对网络攻击、入侵事件的检出成功率和响应时效性，以及检测能力获得权威评测机构认可的情况	
	安全漏洞预警	统计厂商云主机安全产品对漏洞检测的全面性与响应时效性	

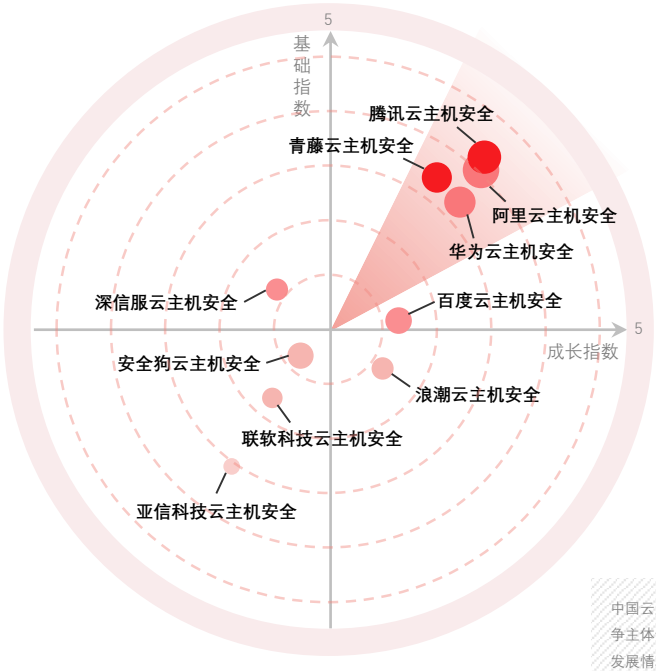
	细分指标	指标要点	指标权重(100%)
成长指数	集成容器安全	衡量云主机安全产品支持云负载平台多场景安全检测、防御能力	
	集成威胁情报	衡量云主机安全接入威胁情报渠道的广泛度，实时检测全网安全动态、判断安全趋势的能力	
	拓展零信任功能	判断零信任安全架构与厂商云主机安全架构集成的进度	
	主机安全云原生化	衡量厂商云原生能力高低，以及云原生能力接入安全模块的水平	
	开放API接入	衡量云主机安全模块增强API安全防护与开放性的能力	

	细分指标	指标要点	指标权重(100%)
服务能力	性能调优	衡量厂商持续优化云主机安全性能、加快用户需求响应速度的能力	
	价格策略	衡量厂商云主机安全产品定价策略的灵活度、价格弹性区间	

	细分指标	指标要点	指标权重(100%)
市场影响力	用户数	统计厂商云主机安全产品在中国境内市场的用户数量	
	市场份额	统计厂商云主机安全业务在中国境内的市场份额占比	
	市场广度	衡量厂商云主机安全产品在下游市场的行业覆盖广度	

中国云主机安全市场竞争——云主机安全综合竞争力表现

腾讯云、青藤云安全、阿里云、华为云入围云主机安全领袖梯队，腾讯云以突出的性价比以及优秀的检测能力赢得迁徙用户认可，青藤云安全以轻量化Agent强稳定性赢得用户忠诚



领袖梯队

- 落于红色扇区的品牌入围云主机安全产品领袖梯队
- 领袖扇区圆环按由内向外递增的逻辑对应由低至高的品牌综合评分。综合评分由“基础指数”（权重35%）、“成长指数”（权重35%）、“服务能力”（权重15%）以及“市场影响力”（权重15%）综合计算得出

中国云主机安全市场初具规模，整体处于上升增长期，本报告对竞争主体云主机安全产品综合竞争力的分析结论仅适用于该阶段市场发展情况。沙利文将持续关注云主机安全市场，更新品牌动向。

- 纵坐标代表“基础指数”：

衡量竞争主体云主机安全产品在基础防护性能方面的竞争力，位置越靠上方，云主机安全产品的基础安全能力越突出

- 横坐标代表“成长指数”：

衡量竞争主体在云主机安全服务中接入和应用新技术的广度、深度，位置越靠右侧，云主机安全产品的成长力越显著

- 色深代表“服务能力”：

衡量竞争主体云主机安全产品在服务跟进、性价比两个细分维度的表现，色深越深，代表厂商云主机安全服务能力越优秀

- 气泡大小代表“市场影响力”：

衡量竞争主体云主机安全产品在市场份额、用户渗透力等细分维度的竞争力，气泡越大，代表厂商市场影响力越强

中国云主机安全市场竞争——领袖梯队：青藤云安全

新锐品牌青藤云安全自研“万相”在约600万服务器中部署，获得下游用户对产品稳健性的一致认可，青藤云安全在与大型云厂商及边界安全厂商的竞争中实现约300%的年复合增长率

■ 主导轻量级Agent模式：稳定运行、低消耗，软件健壮度凸显领先优势

青藤云安全在业界率先实践并推行轻Agent理念，高度稳定的轻Agent部署模式让青藤云安全在云主机安全领域凸显出先发优势和产品性能优势。经历下游百万场景的训练，青藤万相云主机安全已基本实现软件健壮度的成熟。在新基建政策推进、云计算技术升级等时代红利影响下，青藤万相作为平台型产品，具备渗透既有用户全业务场景的潜力，也具备持续渗透潜在市场的品牌实力。

■ 资产清点：从安全防护走向安全运营

青藤万相云主机安全在资产清点模块具有显著的细粒度优势，支持对资产的向下钻取以及数据点深度关联。万相资产清点模块在帮助用户明确资产类型之余，未来或将升级为支持资产合规管控任务的管理级模块。集团型客户、研发人员不仅在基础安全防护领域依赖万相的资产清点功能，更利用其资产识别、归纳、分析能力实现安全运营的目的。资产清点能力的衍生将帮助用户更加明确资产的合规性以及资产与安全防护项目匹配的准确性，对安全产品做出最佳判断，全面提升安全运维性价比。

■ 入侵检测：多锚点检测对应kill chain模型、ATT&CK模型

青藤云安全在入侵检测层面表现出较强的创新能力，设立“入侵锚点”标签对应kill chain攻击链以及ATT&CK模型的12个攻击步骤，并赋予入侵锚点长链检测能力（覆盖暴力破解，Web后门监控，反弹shell，本地提权监控，系统后门监控，挖矿木马检测等）。在Webshell检测环节，青藤云安全单锚点检出率达到**99.74%**，锚点对暴力破解的检出率也**超过99%**。在单锚点绕过几率平均为1%的前提下，多个锚点绕过几率相乘达到整体万分之一甚至更低的绕过几率，显著推高黑客入侵成本。

■ AI技术深度应用：网页后门Webshell高精度检测

AI技术在青藤万相中的深度应用以网页后门检测能力为例。青藤云安全于2020年3月举行的安全引擎公测活动中，在攻击强度等同于或者高于真实业务场景的动态对抗环境下，实现**99.54%**的Webshell入侵检出率，创造当前中国检测领域高峰。

青藤万相引入并实践自适应策略，多维度细化安全指标

主导云主机自适应安全架构、自适应响应机制

- 实时更新产业安全政策、细分领域安全政策
- 持续实现自主安全合规

动态监测：内外流量
针对外部流量攻击进行防护
支持对内部流量的访问保护

主动判断：预防攻击
采取预防外部攻击的措施
建立内部访问适应机制

防护延伸：内外探测
探测可能发生的外部突发事件
实时监督内部使用状态

快速响应：内外安全事件
应对外部突发事件
管理分析内部使用情况

善后：主动判断
预测外部攻击路径并告警
对内发掘防护需求

细化安全指标，安全防护跨越边界

- 面对趋于模糊的网络边界，青藤云安全认为可以放大并发挥业务内生安全指标的价值，通过不断细化的安全指标检测、分析漏洞，早一步于黑客发现问题
- 青藤云安全主导的新型网络安全防护架构覆盖并不限于：
  - 数据中心内部安全
  - 应用安全（应用之间隔离防护）
  - 新一代数据中心虚拟机安全
  - 安全管理策略全网统一
- 青藤云安全是动态防御理念的代表实践者，以云主机安全架构为核心扩大版图

中国云主机安全市场竞争——领袖梯队：腾讯云

腾讯云镜主机安全表现出优越的二进制查杀、多引擎检测能力，在付费周期、部署规则、核心功能开放等方面表现出较强的定价灵活度，凸显用户友好差异化优势

■ **多样化定价策略：周期灵活+功能灵活+部署灵活**

腾讯云镜主机安全主导更加灵活的计费模式。除年、季、月传统付费周期外，腾讯云镜计价颗粒度可细化至天。云镜免费版试用套餐打破时间限制，为用户提供更为友好的试用方案：以检测风险条数为单位。云镜免费版在全面检测功能基础上，开放了相对更多的核心防护功能。此外，云镜推出针对核心资产提供安全防护的模式，不强求云主机安全在用户所有资产的全盘配置。

■ **轻量化部署：兼顾主机业务性能，优化防护时效**

腾讯云镜主机安全支持客户端轻量化Agent模式，轻量化代码部署的方式显著降低安全模块对客户端CPU及内存的占用。轻量化模式下，用户可实现云主机安全能力的一键部署，完成自动化升级，极大降低安全维护成本。此外，腾讯云主机安全具备灵活的告警机制，根据攻击行为、攻击对象设置分层告警，并支持5种以上告警通道，保证安全防护时效性。

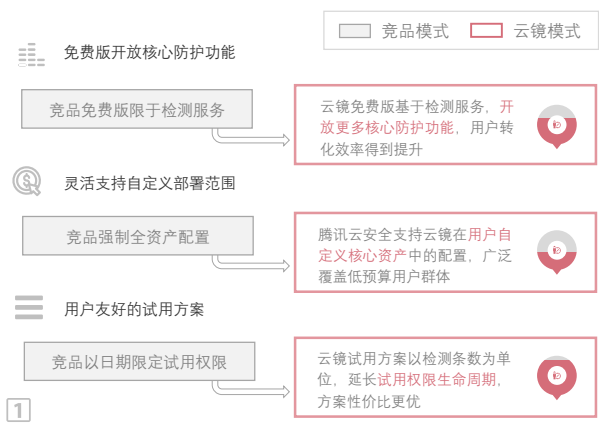
■ **攻击源追踪：7大安全实验室信息同步**

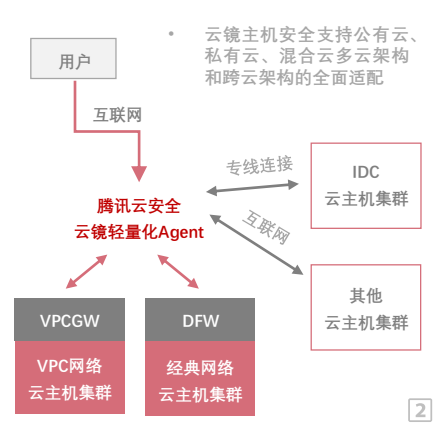
腾讯安全联合实验室为包括云主机安全在内的各大安全产品线持续输出实时威胁情报。7大安全实验室数据同步至云和设备端各类生产生活场景，在应用层、连接层、系统层实现威胁信息的共享。7大实验室能力图谱覆盖威胁情报全生命周期，强大的信息挖掘能力助力腾讯云安全在威胁情报服务市场奠定扎实的资源优势，并助力腾讯云镜提升应对高级持续性攻击（APT）的能力，实现精准响应。

■ **检出能力强化：海量应用场景样本训练**

依托下游业务场景积累的海量攻击样本，腾讯云镜主机安全天然具备训练恶意行为检测工具的数据资源，样本源广泛覆盖病毒、木马、僵尸、蠕虫等形态，并实现对样本源的实时追踪及管理。数据资源加持下，腾讯云Webshell引擎、二进制查杀引擎、AI云查杀引擎等多引擎查杀工具检出率出众（>99.99%）。此外，腾讯云安全与业界合作伙伴建立恶意样本互换合作关系，多渠道强化检出能力。

云镜主导多维度灵活友好计价方案，实现轻量化Agent多云适配





中国云主机安全市场竞争——领袖梯队：阿里云

阿里云安全中心推动云主机安全向安全运维管理能力进阶，优化用户在告警、检索、基线配置、漏洞检测等各项基础服务的体验，并领导安全量化和安全预测的实践

■ 统一轻量级运维

阿里云安全中心集成于阿里云控制台，用户可通过阿里云安全中心直接调用各台云主机数据，并对其安全状态进行查询、监测。云安全中心Agent支持在阿里云服务器和非阿里云服务器的部署，可于不同版本的Windows、Linux系统进行安装。

阿里云安全中心各类进程已实现轻量化部署，控制台统一管理模式极大降低用户维护大规模主机的时间成本和工作强度，减轻安全模块对云主机业务应用的影响。

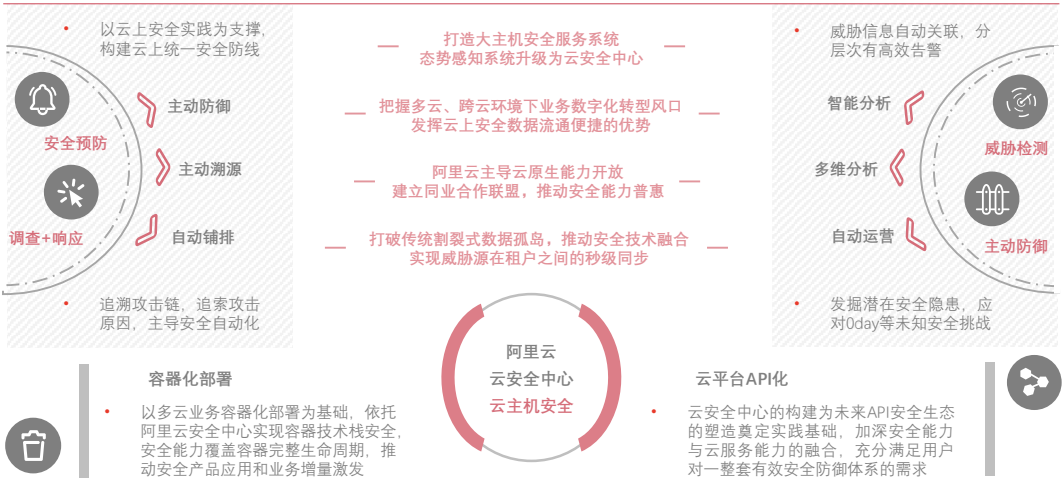
■ 超速响应，主动溯源

阿里云安全中心支持对木马、病毒等攻击的溯源追查，实现Agent轻量级化部署模式下的高效检测。Agent与云端防护中心联动，实时分析木马行为在云主机中的运行模式，及时定位木马文件并即时清理。对于Webshell脚本文件，阿里云安全中心Agent支持即时隔离，以防范对云主机的渗透和控制。

■ 强化分析能力，从防护向管理进阶

阿里云安全中心对记录、阻断、告警、定位等能力完成全盘强化，依托云端防护中心高效威胁识别能力实现管理控制台在云主机安全层面的可视应用，全方位为云主机提供安全防护。云安全中心控制台支持对用户登录信息的精细查询，深度追踪IP源地址，可实现对黑客链接的精准定位，助力用户从传统边界安全向精准安全及安全管理进阶。

以云原生技术为优势，推动阿里云安全中心云主机安全应用增量扩容



中国云主机安全市场竞争——领袖梯队：华为云

华为云快速拓展云主机安全边界，在云主机安全自闭环基础上实践全端、全场景的安全大闭环，支持安全能力在多云环境的快速迁徙，并持续训练和完善攻击样本家族图谱

■ 全端、全场景云主机安全闭环：多方编排调度

华为云基于云主机安全内部闭环，融合态势感知系统实现上下联动、编排、响应，实现云主机安全能力在云上、云下的全端全场景部署。此外，华为云主机安全大闭环支持第三方厂商对云主机安全功能的编排与调度，实现与CIS、Splunk等SIEM厂商的联动。

■ 多云环境下的云主机安全能力：快速渗透

未来随着更多用户核心业务上云，多云部署必然成为主流趋势，华为云专注于多云场景部署安全Agent，为下游用户在华为云上管理其他云场景的安全运行提供便利。此外，华为云主机安全支持广泛的端点类型，覆盖Linux、Windows等操作系统以及国产新创操作系统，并在底层同步实现对X86、ARM架构的支持。

■ AI检测引擎深度训练：家族归属

基于AI算法形成的恶意行为家族图谱构成华为云主机安全恶意程序检出工具的核心。通过对攻击行为特征字段进行提取，并转化成类二维码图像，华为云成功利用AI技术在海量样本中训练出20多类常见攻击行为家族，包括挖矿家族、特洛伊家族、蠕虫家族等。

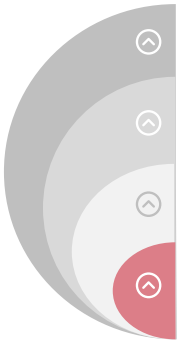
华为云主机安全通过AI图像识别技术，将外部文件转化成的类二维码图像与家族图谱进行比对，进而判断攻击类别。传统网络安全软件在变种攻击层面“力不从心”，而利用AI技术在图像识别层面的优势，华为云主机安全可实现对存在微小特征变化攻击行为的准确判断。

■ 漏洞源实时维护：支持一键修复

华为云安全漏洞库实现对各大标准漏洞网站的覆盖，漏洞库规模达到近20万。华为云还支持对Linux漏洞源的维护，通过漏洞一键修复能力帮助用户在线打补丁。华为云主机漏洞修复功能一方面确保漏洞源的可信，另一方面为用户节省验证、维护漏洞源所需的大量时间成本和经济成本。此外，华为云主机安全在内网安全态势可视方面走在前列，通过对系统漏洞进行大屏重现，将资产态势大屏汇聚于态势感知整体系统中，进一步消除内网安全边界。

华为云主机安全突出智能、全端、主动理念，主导双因子认证机制的实践

多引擎智能检测体系构筑云端病毒查杀能力



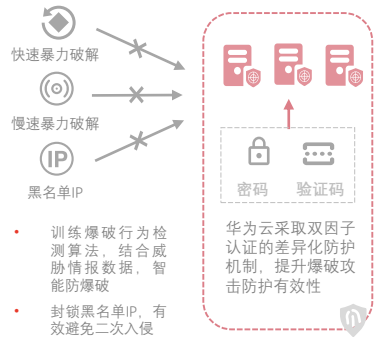
基于文件信誉检测
- 依托文件信誉库安全特征值探测可疑文件
- 基于黑白哈希全面捕捉安全情报

基于基因特征检测
- 参照基因学方法论分析恶意代码，构建特征识别库
- 推动信息安全升级至安全基因检测级别

基于人工智能检测
- 采用虚拟图像指纹算法提炼恶意行为特征码
- 依托机器学习完善攻击行为家族图谱

基于情报+攻击行为分析检测
- 多渠道情报汇聚、关联，大数据分析快速响应
- 利用沙箱训练恶意行为规则，对抗未知威胁

主导双因子认证机制，主动防御账户暴力破解



- 训练爆破行为检测算法，结合威胁情报数据，智能防爆破
- 封锁黑名单IP，有效避免二次入侵

华为云采取双因子认证的差异化防护机制，提升爆破攻击防护有效性

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，从云原生技术、零信任、人工智能等领域着手，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。

www.leadleo.com

https://space.bilibili.com/647223552

https://weibo.com/u/7303360042