头豹 LeadLeo

www.leadleo.com

2020年
中国云安全产品及技术概览

概览标签：网络安全、云计算、人工智能、态势感知、数据安全、密码技术

报告主要作者：贾雁

2020/04

概览摘要

云安全是用于保护云计算数据、应用和相关结构的安全服务，是基于云计算商业模式应用的安全软件、硬件、用户、机构、安全云平台的总称。云安全作为云计算领域的重要细分市场，中国云安全行业的整体市场规模随着云计算市场规模增长而快速崛起。伴随企业上云步伐不断加快，企业数据向云端迁移，及新的网络安全等级保护制度的落地，企业对数据库加密的要求变成“关键信息基础设施”的刚性需求，用户对易部署、性能影响小、透明性好的数据库加密产品需求逐步上升。云服务用户对数据安全的关注度日渐提升，促使云安全企业不断优化数据安全产品，满足云服务用户对数据安全产品的需求。

- **机制展望：基于角色的访问控制**

传统访问控制管理机制具有模板化、套路化特征，基于既定规则决定授权，相对而言，角色访问控制管理机制较为灵活，可实现基于角色（普通访问、管理访问）的高效授权管理。

- **技术展望：云端加密**

数据加密需求从服务器转向云端，云存储应用程序需支持用户在企业网络、移动系统、云端建立安全链路，实现加密主动化、前置化。

- **流程展望：DevSecOps安全一体化**

DevSecOps将安全程序嵌入开发、运营、生产全生命周期（配套工具柔和嵌入DevOps开发体系），安全工作在软件供应链中实现前置化。DevSecOps“黄金”流水线理念着重强调持续集成、持续部署的自动化工具链技术，为威胁建模、威胁发现、威胁模拟、响应检测等关键环节赋能。

- **功能展望：云上开发**

全球超85%的企业表示愿意在未来选择基于云端开源环境搭建软件开发系统，云开发生态下，软件持续集成、持续部署能力量化提升。

主力厂商分析：

腾讯、阿里巴巴、华为、启明星辰

目录

名词解释（1/3）

- **DevOps：**Development and Operations，一组过程、方法与系统的统称，用于促进开发（应用程序、软件工程）、技术运营和质量保障部门之间的沟通、协作与整合。
- **DevSecOps：**Development、Security and Operations，一套基于DevOps体系的全新IT安全实践战略框架，糅合开发、安全及运营理念的新型安全管理模式。
- **ZTNA：**Zero Trust Network Access，零信任网络访问，在不依赖网络传输层物理安全机制的前提下，有效地保护网络通信和业务的访问。
- **Proxy：**代理软件或代理服务器，一种网络访问方式，用来进行用户不想或不能进行的其他操作。
- **WAF：**Web Application Firewall，Web应用防护系统，网站应用级入侵防御系统，通过执行一系列针对HTTP/HTTPS的安全策略专门为Web应用提供保护的产品。
- **SDK：**Software Development Kit，软件开发工具包，为特定软件包、软件框架、硬件平台、操作系统等建立应用软件时的开发工具的集合。
- **API：**Application Programming Interface，应用程序接口，软件系统不同组成部分衔接的约定，可提供应用程序与开发人员基于软件或硬件得以访问一组例程的能力，无需访问原代码或理解内部工作机制的细节。
- **DDoS攻击：**Distributed Denial of Service Attack，处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。
- **IP：**Internet Protocol，网际互连协议，目的在于提高网络可扩展性，解决互联网问题，实现大规模、异构网络的互联互通，分割顶层网络应用和底层网络技术之间的耦合关系，以利于两者的独立发展。

名词解释（2/3）

- **HDFS：**Hadoop Distributed File System，分布式文件系统，适合运行在通用硬件上的分布式文件系统。
- **IaaS：**Infrastructure as a Service，基础设施即服务，把IT基础设施作为一种服务通过网络对外提供，并根据用户对资源的实际使用量或占用量进行计费的一种服务模式。
- **SaaS：**Software as a Service，软件即服务，通过网络提供软件服务，云厂商将应用软件统一部署在自己的服务器上，客户可根据工作实际需求，通过互联网向厂商定购所需的应用软件服务，按定购的服务多少和时间长短向厂商支付费用，并通过互联网获得Saas平台供应商提供的服务。
- **PaaS：**Platform as a Service，平台即服务，把服务器平台作为一种服务提供的商业模式。
- **AST：**Abstract Syntax Tree，抽象语法树，源代码语法结构的一种抽象表示，以树状形式表现编程语言的语法结构，树上每个节点表示源代码中的一种结构，语法不表示出真实语法中出现的每个细节，而采用条件跳转语句，可用带有两个分支的节点表示。
- **DAST：**Dynamic Application Security Testing，动态应用程序安全测试，在测试或运行阶段分析应用程序的动态运行状态，模拟黑客行为对应用程序进行动态攻击，分析应用程序的反应，从而确定该Web应用是否易受攻击。
- **SAST：**Static Application Security Testing，静态应用程序安全测试，在编码阶段分析应用程序的源代码或二进制文件的语法、结构、过程、接口等来发现程序代码存在的安全漏洞。
- **IAST：**Interactive Application Security Testing，交互式应用程序安全测试，DAST和SAST结合的一种互相关联运行时安全检测技术，通过代理、VPN或者在服务端部署Agent程序，收集、监控Web应用程序运行时函数执行、数据传输，并与扫描器端进行实时交互，高效、准确识别安全缺陷及漏洞，同时可准确确定漏洞所在代码文件、行数、函数及参数。

名词解释（3/3）

- **RASP：**Runtime Application Self-protection，运行时应用进行的自我保护机制，RASP将自身注入到应用程序中，与应用程序融为一体，实时监测、阻断攻击，使程序自身拥有自保护能力，应用程序无需在编码时进行修改。
- **P2P：**Peer-to-peer Computing，一种在对等者（Peer）之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。
- **Web：**全球广域网，万维网，一种基于超文本和HTTP的、全球性动态交互、跨平台的分布式图形信息系统，为浏览者在网络查找和浏览信息提供图形化、易于访问的直观界面。
- **主体：**访问操作中的主动实体，包括所有能够发起访问操作的实体，如人、进程、设备等。主体是访问的发起者，并造成信息流动或者系统状态的改变。
- **客体：**访问操作中的被动实体，是包含信息或接受信息的被动接受访问的资源，如文件、设备、信号量、网络节点等。客体在信息流动中处于主体作用之下。
- **策略：**主体对客体的访问规则集，定义主体对客体的动作行为和客体对主体的条件约束，是允许某个主体可以被授予一组特权或者（与特权对应的）安全属性的行为。
- **动作：**访问模式，信息在主体和客体之间流动的交互方式，常见动作主要包括读、写、读写执行等。
- **冒烟测试：**将代码更改嵌入到产品的源树中之前对更改进行验证的过程，用于确认代码中的更改会按预期运行，且不会破坏整个版本稳定性。
- **白盒检测：**基于代码的测试，使用该方案时，测试者必须检查程序的内部结构，从检查程序的逻辑着手，得出测试数据。

头豹 LeadLeo

FROST & SULLIVAN 沙利文

招聘 行业分析师

我们一起“创业”吧，开启一段独特的旅程!

邮箱：fs.recruitment@frostchina.com

工作地点：北京、上海、深圳、香港、南京、成都

云安全产品与技术综述——全球云安全产品概览

全球头部云厂商寻求差异化竞争空间，云安全产品向高度可视化、精细化管理、高度集成方向发展

全球头部云厂商云安全产品概览

厂商及云安全产品	产品差异化特点	产品优劣势	
Google Cloud 谷歌：谷歌云安全	• API及管理员控制台采用精细安全配置策略 • 风险仪表盘统一部署，可视化程度较高	○	访客系统、IaaS容器具备原生资源、自动扩展机制支持；拥有较为完善的安全认证体系、合作伙伴生态系统
		✕	基于身份控制的角色访问系统较为复杂，用户目录同步存在困难；谷歌云平台硬件安全模块尚未到位
aws 亚马逊：AWS云安全	• 虚拟机管理程序安全、操作系统及容器安全能力较强 • 安全服务定价条款较为灵活	○	管理员控制台身份配置灵活，访问管理方案多样化，私有云网络隔离措施有效可靠，“Macie”工具简化工作数据发现和分类工作
		✕	亚马逊云安全系统安装量数据尚不透明，影响客户对其安全产品的客观评估和采集，AWS平台密钥管理服务操作难度较高，风险仪表盘配置存在难度
Microsoft Azure 微软：Azure云安全	• 部署无密码验证环境，改善开发者集成机制 • 在操作系统、容器安全等方面具备强基础	○	提供强化版加密密钥保险柜管理、防火墙配置，管理员可获取控制台多数安全功能，特权用户可获取访问审核权利
		✕	管理员控制台配置管理难度高（多因子验证、角色身份认证），控制台浏览界面待优化，内置帮助功能待完善
Alibaba Cloud 阿里巴巴：阿里云安全	• 具备云迁徙认证服务能力，安全服务覆盖数据全生命周期 • 具备自动代码审计、渗透测试能力	○	访客操作系统加密功能简单高效，提供分布式拒绝服务机制、防火墙机制，系统具备深度学习功能、仪表盘功能完善
		✕	尚未建立全面的安全合作伙伴关系，对IaaS容器原生云技术支持不足，以中文为主要使用语言，其他语言支持相对欠缺
IBM Cloud IBM：IBM云安全	• 推出“蓝色巨人计划”，于管理配置模块深度融合机器学习技术 • 支持容器和DevOps工具的集成	○	建立较为全面的合规认证系列，具备广泛合作伙伴生态，推动传统安全分析工具与云功能的高度集成
		✕	定价透明度低，市场势力范围不明晰，尚未公布基于角色访问控制以及虚拟机管理程序的安全服务

来源：各企业官网，头豹研究院编辑整理

头豹 LeadLeo

云安全产品与技术综述——云安全技术发展简析

身份认证、虚拟机监控、标记化技术等主流云安全技术已达到生产力成熟期，效益得到企业客户验证，私有云技术、灾难恢复技术、IaaS加密技术将攀至成熟高峰

云安全技术成熟度曲线（部分技术发展阶段）

https://www.leadleo.com/pdfcore/show?id=5ff7bc7220410e79fc954c31

来源：Gartner，头豹研究院编辑整理

➢云安全技术是整合全网资源的主动防御技术

云安全技术以云计算、云存储功能为基础，由网络技术、P2P对等技术等发展而来，主要针对网络计算问题、病毒判断问题等提供解决方案，集中应对移动时代信息安全需求。

云安全技术工作流程：云平台中心对大量客户端网络软件运行情况进行监测，采集各类恶意活动路径并将信息传送至云安全中心完成分析，最终将病毒、木马解决方案发送至客户端。

云安全技术在用户电脑终端、安全厂商之间建立密切联系，形成规模化病毒查杀体系。现阶段处于**成熟度峰值**的云技术已渗透移动设备数据丢失保护、软件边界定义、密钥管理等领域。

➢处于发展阶段的云安全主流技术

- **灾难恢复技术：**该项技术有助于防止敏感数据意外披露，助力用户有效识别导致数据意外泄露、损坏的业务流程，并衍生出改善流程的培训服务；
- **私有云计算技术：**公有云在监管、知识产权等方面无法实现对不同领域企业的全效辅助，私有云技术可通过提高IT资源利用率、提升运维效率等方式协助企业提升效益、驱动增长；
- **IaaS容器加密技术：**该项技术可为存储在云端的整体业务流程、应用程序数据提供保护方案，针对云服务供应商提供给企业用户的数据建立低成本保护机制（如微软为linux免费提供容器加密工具）。

中国云安全产品技术挑战简析——虚拟化对云安全构成挑战

传统数据中心采取物理隔离措施保证数据安全，云端虚拟环境面临攻击面扩大（漏洞传递、共享环境、远程威胁等），需采取严密部署、监控措施应对恶意活动挑战

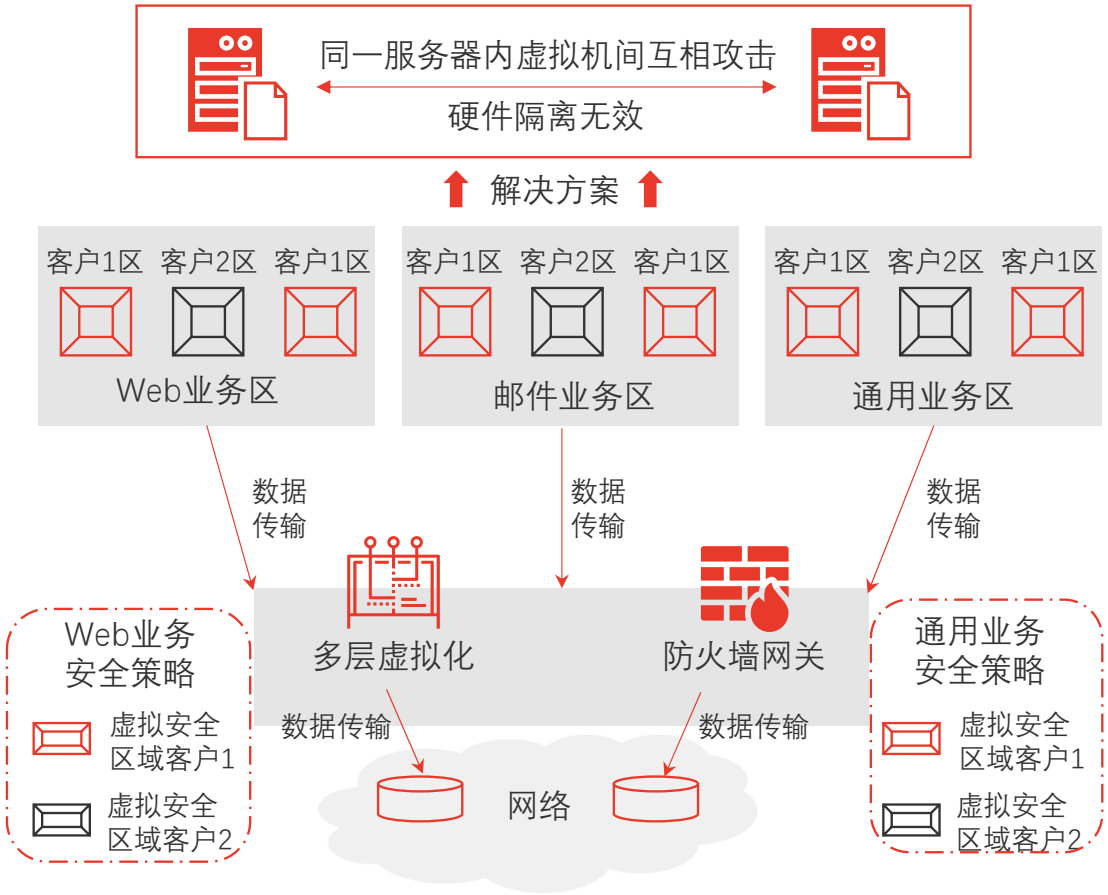
➢虚拟访问增加数据暴露风险

相对传统数据中心对现场或直接连接的控制，虚拟环境依托互联网技术管理用户的访问行为，入侵风险、数据暴露风险控制难度提升，厂商需于云端建立监控体系，实现对服务期内虚拟机间攻击的控制。虚拟化对云端构成的安全挑战如下：

- **一致性挑战：**虚拟机具备动态特征和移动性特征，较难保证数据记录可审计性、安全策略一致性。此外，服务器之间虚拟机克隆、发布易导致安全漏洞传递，对整体系统安全状态确认造成挑战；
- **量级挑战：**云环境下虚拟机数量激增，系统面临攻击面扩展，风险量级提升等问题，虚拟机在云环境中的位置各异，对系统在不同水平的恶意活动检测和防御能力提出挑战；
- **远程威胁挑战：**全球范围超64%的企业用户开始使用云服务器环境、应用程序，现阶段本地化虚拟机多采用与终端服务器相同的操作系统，增加了恶意软件利用系统漏洞、应用程序漏洞远程攻击的可能性；
- **共享环境挑战：**企业数据在公有云和私有云环境之间迁徙频度提高，随云环境共享度提升，系统攻击面扩大，虚拟机相对专用资源环境更容易遭受攻击风险。

虚拟化环境下，企业使用云资源应合理部署物理安全、虚拟化安全模块，并针对威胁性质对不同租户、部门共享安全设备行为做出规划，注重数据中心内部区域安全以及边界安全，提升安全模块可视化水平。

云端虚拟化业务模块结构及云安全策略



来源：头豹研究院编辑整理

中国云安全产品技术挑战简析——云上开发环境安全保障

云上开发模式集成大量源代码、计算模型、基础开发模型以及服务器端功能，移动应用开发行为向云上迁徙在代码兼容、日志传输、功能迭代等方面存在挑战

➢云上移动开发成为趋势

基础设施、应用程序、业务流程服务持续向云端迁徙，截至2019年上半年，全球约超**21%**该类服务市场总收入由云端贡献。预计2021年，该比例或达**28%**。SaaS和PaaS业务在实现高速市场增长的同时，开发模式呈现出本地模式向云模式转换的特征。依托云端算力、SaaS计算模型及较为成熟的PaaS服务器端功能，云上程序开发相对本地开发模式可节约**30%**以上时间成本，大幅压缩代码开发工作量。此外，云端追踪有助于提高移动应用项目开发工作的可控性，并支持功能快速集成。

➢云端开发模式在兼容度、适应性等层面面临挑战

- **多元代码兼容挑战**

云端开发模式下，用户将企业内部开发代码迁移至云端，多种代码云端运行或导致代码组合、兼容挑战，现阶段云端混合技术尚不成熟，多元代码迁入行为或面临多重未知安全漏洞；

- **日志信息安全挑战**

随更多关键开发任务向云端迁徙。云厂商需为云用户管理员或终端应用客户提供实时日志，内部日志在传输过程中面临盗取、滥用问题；

- **云应用功能适应挑战**

云开发环境功能迭代迅速，云厂商需确保用户及时跟进应用改进以确保数据安全，云端功能迅速迭代或导致软件开发生命周期内旧版本安全功能无法正常运行等问题。

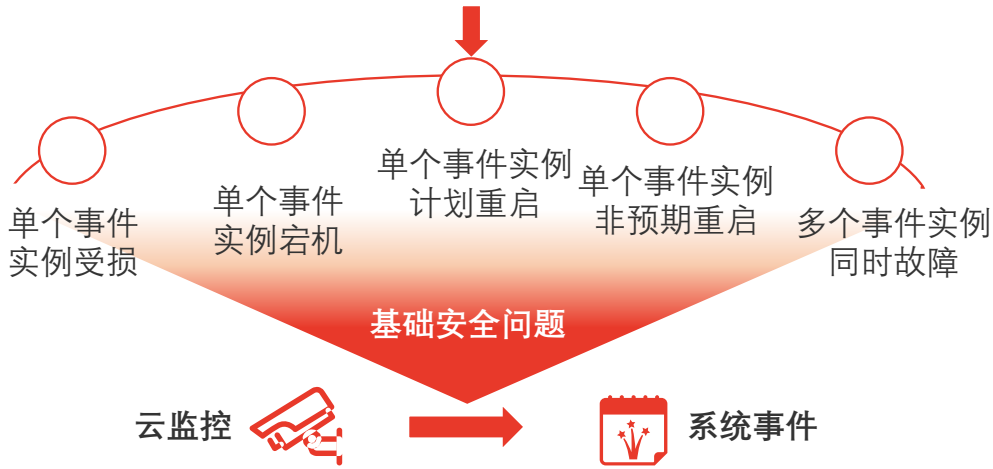
云上开发需求及基础安全问题

①敏捷开发需要
- 传统模式难以满足批量巡检需求，运维人工成本、时间成本高
- 人工运维难以满足实时交付需求

需求来源

③日常管理需要
- 传统模式缺乏运维积累及运维规范，难以形成标准化流程
- 运维权限及操作影响面过大，造成安全生产风险

②代码管理需要
- DevOps管理方式在云端运维提出批量代码管理需求



来源：Gartner，头豹研究院编辑整理

中国云安全产品市场挑战对策——混合云统一安全策略

企业用户期望混合云功能强大且便于管理，数据迁徙可视化、云生命周期主动管理是混合云架构下企业虚拟化资产安全需求的具体应对策略

➢ 混合云统一部署安全策略确保企业虚拟化资产安全

截至2019年上半年，全球约**80%**以上企业采取混合云战略，多云架构下企业资产虚拟化复杂度提高，促发云端数据迁徙安全服务需求，需求具体表现在数据迁徙可视化、云生命周期主动管理两方面。

- ✓ **数据迁徙可视化：**针对公有云、私有云环境各类存储、联网、配备活动提供可视界面，快速识别威胁并提供应对方案；
- ✓ **云生命周期管理：**将安全控件模块纳入原生云应用设计流程中，于应用、数据库、终端设备、用户之间实施综合性安全策略。

➢ 企业部署混合云：4个云端虚拟资产安全管理对策

企业虚拟资产基础架构入驻混合云，需采取多元安全管理对策：①**数据合规：**企业在向云端转移数据、应用程序之前，需保证客户数据（财产、健康等）符合地区合规标准；②**跨云安全管理：**采用集中性的基础设施策略（统一防火墙、入侵防御等）以减少云平台间安全传输造成的IT人工处理成本；③**数据加密：**密切监控敏感数据存储位置、流动路径，为迁徙中、程序操作中的数据寻找合适的加密方法；④**云伸缩空间：**针对潜在爆炸性增长的云计算需求建立可伸缩的安全架构，提高云安全开发工具的可扩展性。

混合云安全策略：统一部署具有针对性的安全管理方案

23亿

2019年，全球范围因云服务器及其他系统配置不一致或失误导致数据记录泄露事件频发，达到23亿

74%

全球约74%以上盈利组织、非盈利组织表示因缺乏统一的云迁徙流程遭到数据泄露

400%

全球范围企业组织因内部人员疏忽导致的云安全风险同比增幅超过400%

混合云部署策略应对云安全问题

来源：IBM官网，Gartner，头豹研究院编辑整理

头豹 LeadLeo

中国云安全产品市场挑战对策——动态基础架构整合安全策略

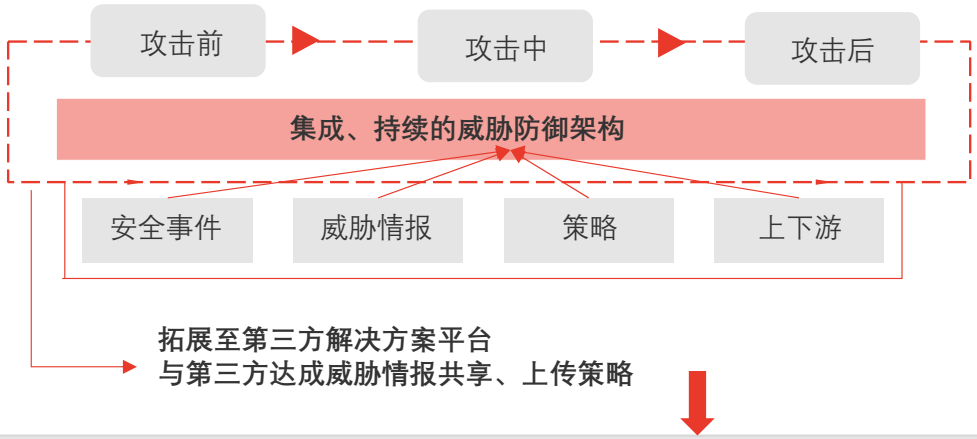
全球超60%企业在网络环境中部署至少6种安全产品（最多达50种以上），动态基础架构下的整合安全策略可提升安全投资效率，满足云端开发环境安全性需求

➢ **全球化业务驱动端到端的安全、合规、风险管理需求：催化基于动态基础架构的通用安全服务**

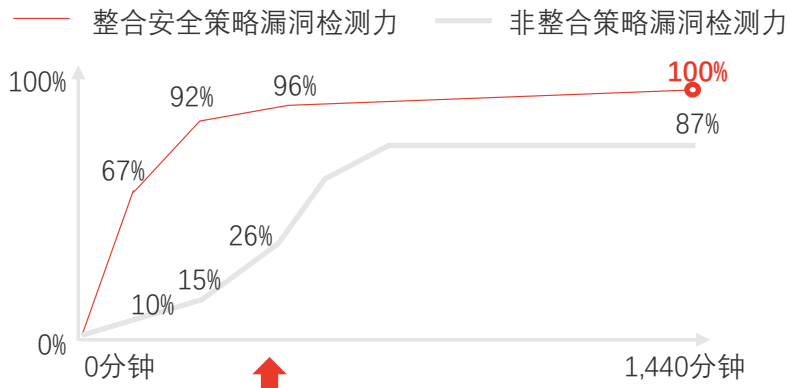
作为通用性IT基础设施平台，动态基础架构下的整合安全战略有助于企业降低风险监控成本，并支持风险量化分析，节约数据安全维护成本。整合性量化分析具备双重效力：**①本地安全模型全球共享：**全球设备可基于本地安全数据情报（流量威胁量化分析、终端威胁量化分析）生成动态安全策略，进行预先防护；**②优化安全投资策略：**基于漏洞对业务影响的量化分析，企业可对安全控制措施设置优先级，优化安全策略投资成效。

云端动态基础架构环境：整合安全模式服务

整合安全产品架构



漏洞检测率线性表现



整合安全产品范例				漏洞检测率		吞吐量结果	
以Cisco高级恶意软件防护服务为例				100%		1,000Mbps	
误报率	路过式漏洞攻击	社交媒体漏洞攻击	域名恶意软件	恶意软件	离线感染	逃避技术	稳定性
<0.5%	100%	100%	100%	100%	100%	100%	通过

来源：Cisco官网，头豹研究院编辑整理

头豹 LeadLeo

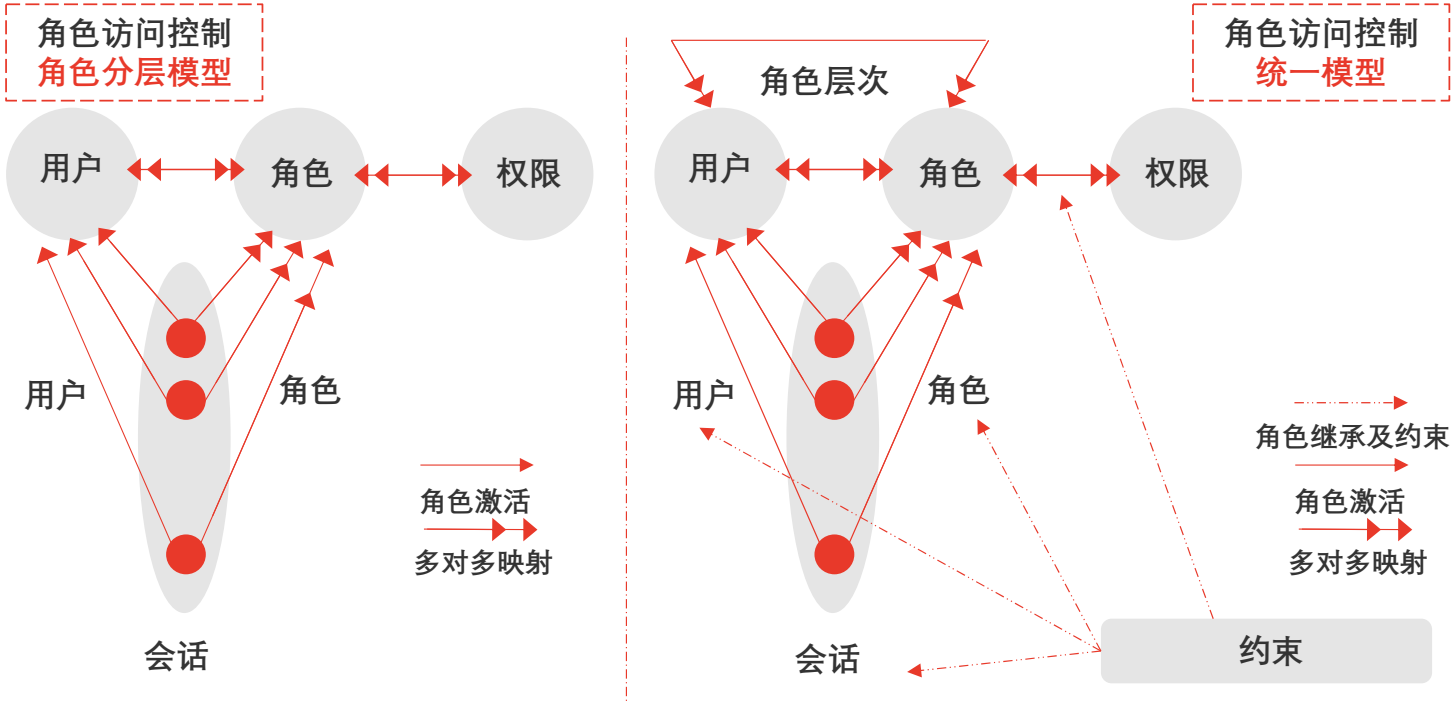
中国云安全市场展望——机制展望：基于角色的访问控制（身份认证）

传统访问控制管理机制具有模板化、套路化特征，相对而言，角色访问控制管理机制可实现基于角色（普通访问、管理访问）的高效、灵活授权管理

角色访问控制管理机制

- 基于角色的访问控制模型由4个基本要素集合构成

- 用户：可以独立访问系统中数据或数据资源的主体
- 角色：可以完成某种特定工作活动的工作位置
- 会话：对应于用户和角色，表示用户角色激活过程
- 权限：对系统中的数据或其他资源进行访问的许可



来源：计算机与网络安全公众号，头豹研究院编辑整理

➢灵活分配权限是角色机制的核心优势

角色访问控制机制下，用户访问权限与访问角色强相关。不同于传统模式“针对用户分配权限”，该模式引入角色概念，**先授予访问对象角色，再“针对角色赋予权限”**。

基于角色的安全机制大幅简化权限管理工作，相对传统权限分配模式节省约**50%**运算资源。现阶段，角色访问控制模型包括基本模型、角色分层模型、角色约束模型以及统一模型等**4**种。

➢看好零信任安全产品市场前景

- **零信任产品核心思路：**在默认情况下，不信任任何网络内部和外部的用户、设备以及系统，只基于**身份认证、角色授权**建立信任基础，进行访问控制。
- 零信任机制引导云安全体系向身份中心化发展（以角色为中心重建信任）。预计2022年，全球约**76%**以上数字应用程序将支持合作伙伴通过零信任网络ZTNA实现访问。2023年，全球**60%**企业或由远程访问虚拟专用网络转向使用ZTNA。

头豹 LeadLeo

中国云安全市场展望——技术展望：云端加密

数据加密需求从服务器转向云端，云存储应用程序需支持用户在企业网络、移动系统、云端建立安全链路，促进云端加密主动化、前置化

➢ **以静态数据保护为中心，做好加密数据隔离、数据与密钥隔离**

企业接入云端存储、处理程序需对传输过程中、使用过程中以及静态数据进行安全保护，并以静态数据保护为重点。

- **创建即保护：**企业应从源头实现对静态数据的保护，在创建敏感数据同时完成加密，以保证本地数据中心、云端数据中心安全。
- **加密模块隔离：**加密数据与加密密钥分布式管理的保护措施已被全球约**40%**的企业接纳。云端自动加密应用程序通过提供SaaS服务（如云加密机服务）实现数据隔离，在保护数据的同时减轻安全任务对企业日常业务流程可能造成的负担。

全球范围 **51%**
企业认为云端数据加密技术将显著提升公有云可信度

49%企业认为应建立并执行安全政策

41%企业认为应对密钥模块建立数据边界

41%企业认为API应具备审计、告警模块

41%企业认为虚拟机应被隔离、保护

来源：云计算D1net公众号，头豹研究院编辑整理

云端加密技术及服务模式

云加密要素	挑战及建议
• 加密密钥定时、频繁更新，对密钥本身进行加密 • 对主密钥和恢复密钥采取多因子验证	尚未获取解密密钥的移动或远程设备只能于云端下载无意义的加密数据，对企业（不愿分享密钥）及其合作伙伴数据共享造成阻碍
• 依托自动加密应用程序中软件即服务应用程序隔离数据	相对由公司内部IT部门管理密钥的模式，客户企业可考虑由服务提供商、第三方代理提供商管理加密密钥（如**云加密机**服务）

腾讯云加密机服务标准及赔偿方案

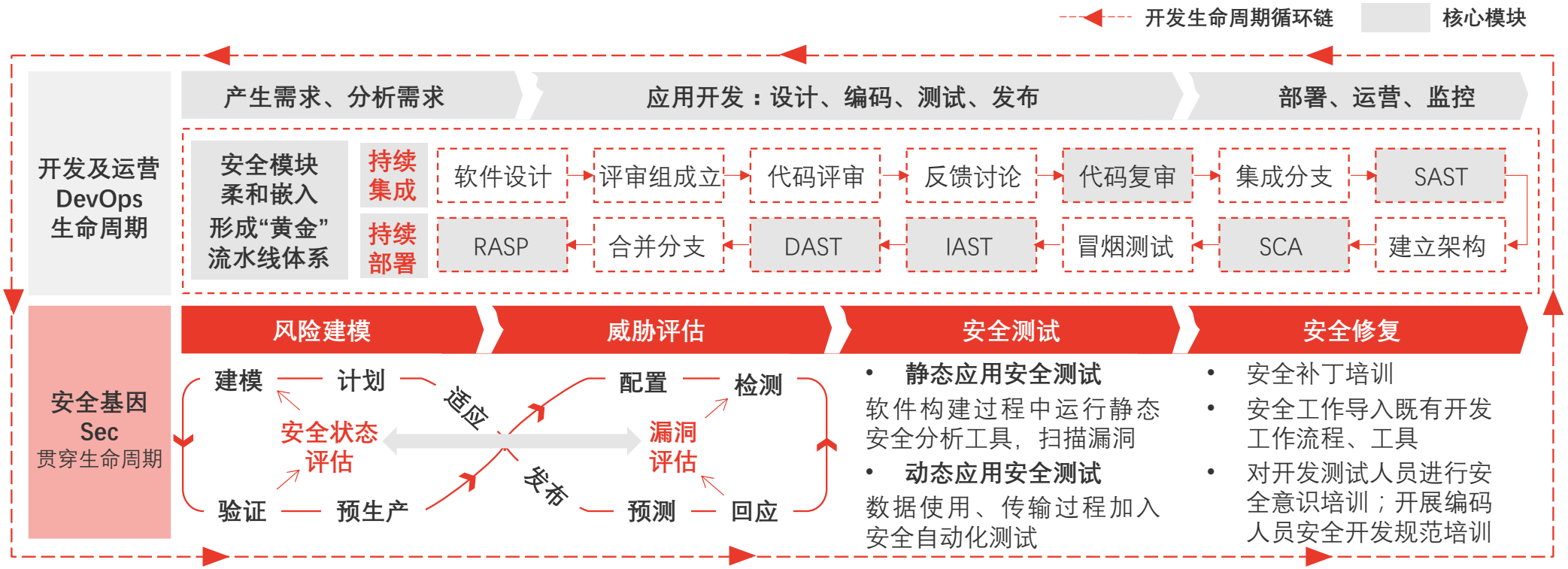
服务可用性=（服务月度总分钟数-服务月度不可用分钟数/服务月度总分钟数）*100%	
按照单实例服务月度内的总天数×24（小时）×60（分钟）计算	
月度服务可用性	**赔偿代金券金额**
<99.90%且≥99%	月度服务费10%
<99%且≥95%	月度服务费25%
<95	月度服务费100%

头豹 LeadLeo

中国云安全市场展望——流程展望：DevSecOps安全一体化

DevSecOps将安全程序嵌入开发、运营、生产全生命周期（配套工具柔和嵌入DevOps开发体系），安全工作在软件供应链中实现前置化

云安全模块嵌入开发及运营全生命周期



- **持续防护降低安全成本：**DevSecOps可确保基础架构、应用程序全生命周期持续安全防护。安全检测前置有助于企业降低近**50%**安全投资成本。
- **“自动化”是DevSecOps的关键：**自动化技术在安全与运营之间建立连接。DevSecOps“黄金”流水线理念着重强调持续集成、持续部署的自动化工具链，为威胁建模、威胁发现、威胁模拟、检测响应等关键环节赋能。

来源：头豹研究院编辑整理

头豹 LeadLeo

中国云安全市场展望——功能展望：云上开发

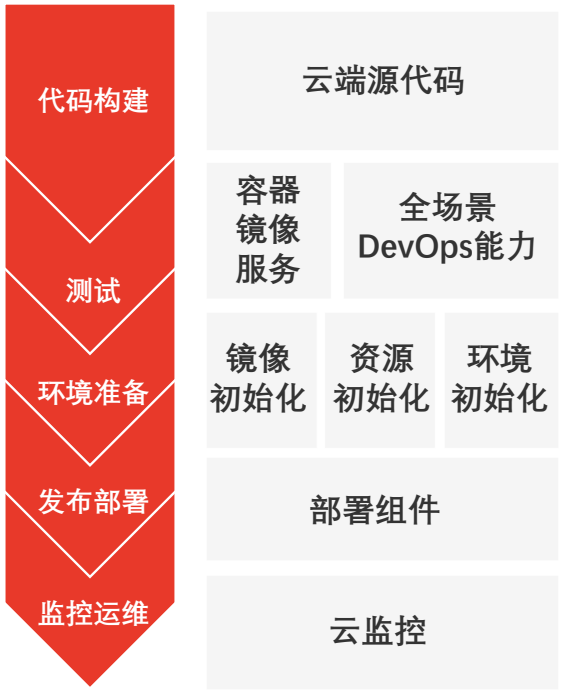
全球超85%的企业表示愿意在未来选择基于云端开源环境搭建软件开发系统，云开发生态下，软件持续集成、持续部署能力量化提升

➢ **云上敏捷开发将成为软件应用开发新范式："一键迁徙+平滑上云+毫秒级延迟"**

有助于企业专注于业务研发工作，减少传统模式下开发环境搭建、测试、差异处理等环节产生的成本。远期，云厂商可协助企业搭建前后台双模DevOps，覆盖前端（舆情分析、动态部署等）、后端（合并主干代码、自动构建集成包等）全部研发周期，计算时延低至毫秒级别。

云上敏捷开发生态环境优势

云上敏捷开发架构示例



云上敏捷开发优势

1. **工具整合 利用率提高**
   - 云端高度虚拟化和共享基础架构实现规模经济
   - 自动化提供更多工具整合机会
2. **交付能力 量化提升**
   - 云端算力延伸，"云边端"协同
   - 全域边缘节点可实现1分钟全国范围边缘算力下发
3. **编程范例 辅助开发**
   - 协助开发者掌握方法，厘清思路，实现自动化部署
   - 范例按技术、行业做详细分类
4. **开发环境 灵活切换**
   - 云端预置多种开发环境，支持用户自行配置开发环境
   - 终端用户可按偏好安装软件包

云上开发影响力

10%-15% 提升1倍以上

数据中心利用率提升1倍或更多

1-2个月 →

传统节点交付周期

云端节点 **分钟级**交付周期

以IBM云端开发服务为例

英文范例接近300个

中文范例约100个

单一开发环境 → Java Hexo Nobe.js PHP C/C++

来源：CSDN官网，头豹研究院编辑整理

头豹 LeadLeo

中国云安全行业竞争格局——品牌结构分析

差异化竞争时代，云服务厂商云安全产品从聚焦公有云市场领域逐渐转向私有云市场领域，其中阿里云与腾讯云营收规模共计占公有云安全市场比重超过50%

中国云安全市场品牌呈现金字塔结构，头部参与者是以阿里云、腾讯云、华为云为代表的云服务厂商，中间层是以绿盟科技、启明星辰、深信服为代表的传统网络安全企业，底层是以青藤云安全、极御云安全和安全狗为代表的初创云安全企业。

- **头部企业：**云平台厂商在云安全领域具有原生云计算资源与技术优势，依托原有客户流量及大数据技术、AI技术，为用户提供DDoS高防、云WAF、加密服务和主机安全等云安全产品及服务，产品体系较为完善；
- **传统网络安全内企业：**传统安全企业产品研发专业度较高，多聚焦于私有云安全与混合云安全领域，围绕云安全监测、防护、管理等需求，推出安全合规、态势感知、虚拟化防火墙、微隔离、安全评测等多个方面的云安全产品及服务；
- **初创类企业：**初创云安全企业通过客户需求为导向开发云安全产品，多以垂直类产品切入云安全市场，如青藤云安全以主机安全为业务核心。

中国云安全品牌结构

- **优势：**在云计算服务阶段，积累了众多客户资源，且云服务研发实力较强，其云安全应用场景覆盖面广
- **优势：**凭借多年网络安全服务经验，客户资源丰富且安全产品开发经验较为成熟
- **优势：**以客户需求为导向云安全产品，细分领域实力较为强劲，能有效提升客户云安全体验

来源：头豹研究院编辑整理

中国云安全行业主力厂商表现——腾讯云安全

腾讯云安全：位居行业头部区间，依托近20年积累的互联网安全经验，通过云平台构建安全城墙，为用户提供众业务场景全链路解决方案

评价维度1：安全能力

- **全方位防护部署能力**

腾讯云针对网络活动事前、事中、事后各层面部署多元化安全产品，覆盖安全防护，安全体检、安全防御、安全监控、安全审计等细化功能。

- **一体化服务能力**

腾讯云安全整体架构深入结合终端安全技术，服务器一体化安全服务依托AI技术，可做到7*24实时告警、智能分析并定期发送状态报告，保障云中租户数据安全。

评价维度2：安全战略

- **网络层与终端对接**

差异化战略：腾讯安全联合实验室以“从网络层到终端”为路径规划并持续输出安全分析技术和安全防护技术。

- **简易接入、全面防护**

简单接口支持登录、注册、用户内容、营销等多元场景，T级分布式DDoS防护节省用户带宽资源。

腾讯云安全服务功能成熟度

安全功能	成熟度	差异化竞争优势
数据安全		研发使用抗量子密码算法的抗量子签名服务，抵抗传统攻击以及量子计算机攻击
网络安全		主动维护企业大规模网络活动，人工智能WAF、网页防篡改、DNS劫持检测等表现出众
主机安全		AI技术支持云镜快速完成预警信息推送（5秒内），AI检测引擎检出率超90%
金融风控		“星云风控平台”高度集成风控方案，提升网络带宽效率，聚焦反欺诈、支付安全、设备指纹
流量风控		“一物一码解决方案”为企业大型运营活动护航，反欺诈AI过滤恶意刷码行为，优化营销效果
终端安全		应用加固方案：将APP防护工作深入到源代码层面，对第三方SDK、小程序进行安全管控

来源：腾讯官网，头豹研究院编辑整理

头豹 LeadLeo

中国云安全行业主力厂商表现——阿里巴巴云安全

阿里巴巴云安全：阿里云持续升级全球云盾高防网络服务（防御力升至约10Tbps），阿里DDoS高防IP服务所需防护带宽较小，为用户节省购买成本，提高网络稳定性

➢ **从DDoS高防IP服务出发，全方位部署安全资源**

阿里云DDoS高防IP服务覆盖基础服务、代码审计、应急响应等全环节，支持包括传统业务、视频直播等场景在内的大规模DDoS攻击防御，其分布式安全资源部署功能以阿里云全球清洗中心能力为支撑，采用智能调度技术、多机房自动容灾技术，实现对大规模DDoS攻击流量的自动牵引。

来源：阿里巴巴官网，头豹研究院编辑整理

➢ **差异化服务：趋于敏捷化和智能化的云安全服务**

阿里云基于既有云盾产品，协助用户跟踪全网恶意IP，排除威胁。

精细化：DDoS防护渗透session级别、域名级别，支持双向流量分析

智能化：依托机器学习、行为识别等算法提高防御效率和精准度

1 **全方位API网关服务**

针对安全隐患较高的API环节，阿里云依托API防护、身份安全等技术，在公有云层面实现流量限制、认证授权、病毒防护等功能，认证层面支持身份认证

2 **推行云安全责任共担模式**

阿里云负责云基础设施层面安全（骨干传输网、地域网），用户负责虚拟化层敏感数据、日志、访问数据等安全，推动厂商与用户共同应对风险的安全服务模式

3 **DDoS高防可视化**

阿里云DDoS高防服务支持对大流量攻击的实时监控，可提供对攻击的完整记录，有助于企业对攻击进行有效实时分析并改进防护效果，保证后续取证、溯源等工作顺利进行

中国云安全行业主力厂商表现——华为云安全

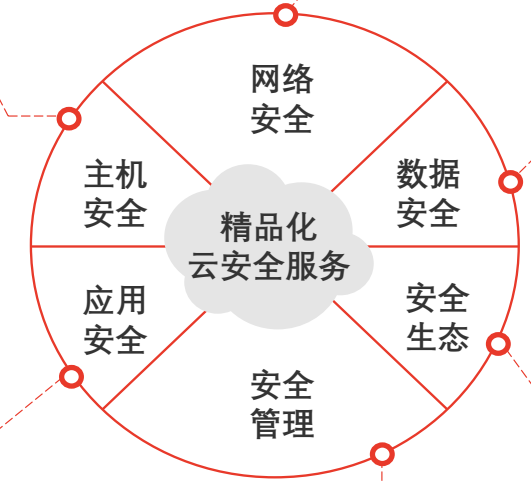
华为云安全：华为搭建具备世界一流水平的云安全合规认证体系，将密钥交付给客户，深度利用AI技术，为用户提供超值易用的云安全工具

华为云安全服务优势

加固弱密码等不安全配置**>10万个**
隔离查杀全球恶意程序**>2万个**

抵御最大攻击流量**1.16Tbps**
识别全球**39.2亿次**DDoS攻击

华为云WAF防御能力覆盖境内外**5个**区域
日均拦截**4,000万次**Web应用层攻击
Web2.0爬虫技术漏洞扫描准确率高于**95%**



推出系列化数据传输、数据存储安全服务
数据库安全服务支持GDPR审计报表

与国际头部安全公司合作，共建云安全测试、云风险管理全球服务体系

RAPID7 SPIRENT Inspired innovation RSA McAfee

态势感知建立威胁检测模型**>30种**
云上资产风险监控日均告警**>百万条**

来源：华为官网，头豹研究院编辑整理

➢云安全服务精品化

截至2019年底，华为于网络、主机、应用、数据、安全管理5个层面推出11款安全服务（覆盖定制化安全配置），部署Anti DDoS、WAF等安全设备以确保云平台自身安全。2018年，华为云通过超10个权威安全合规认证，打造世界一流云安全认证合规体系。同时推动租户按照国家、区域、行业要求采取安全防护措施以实现合规（安全责任共担）。

➢差异化服务动向

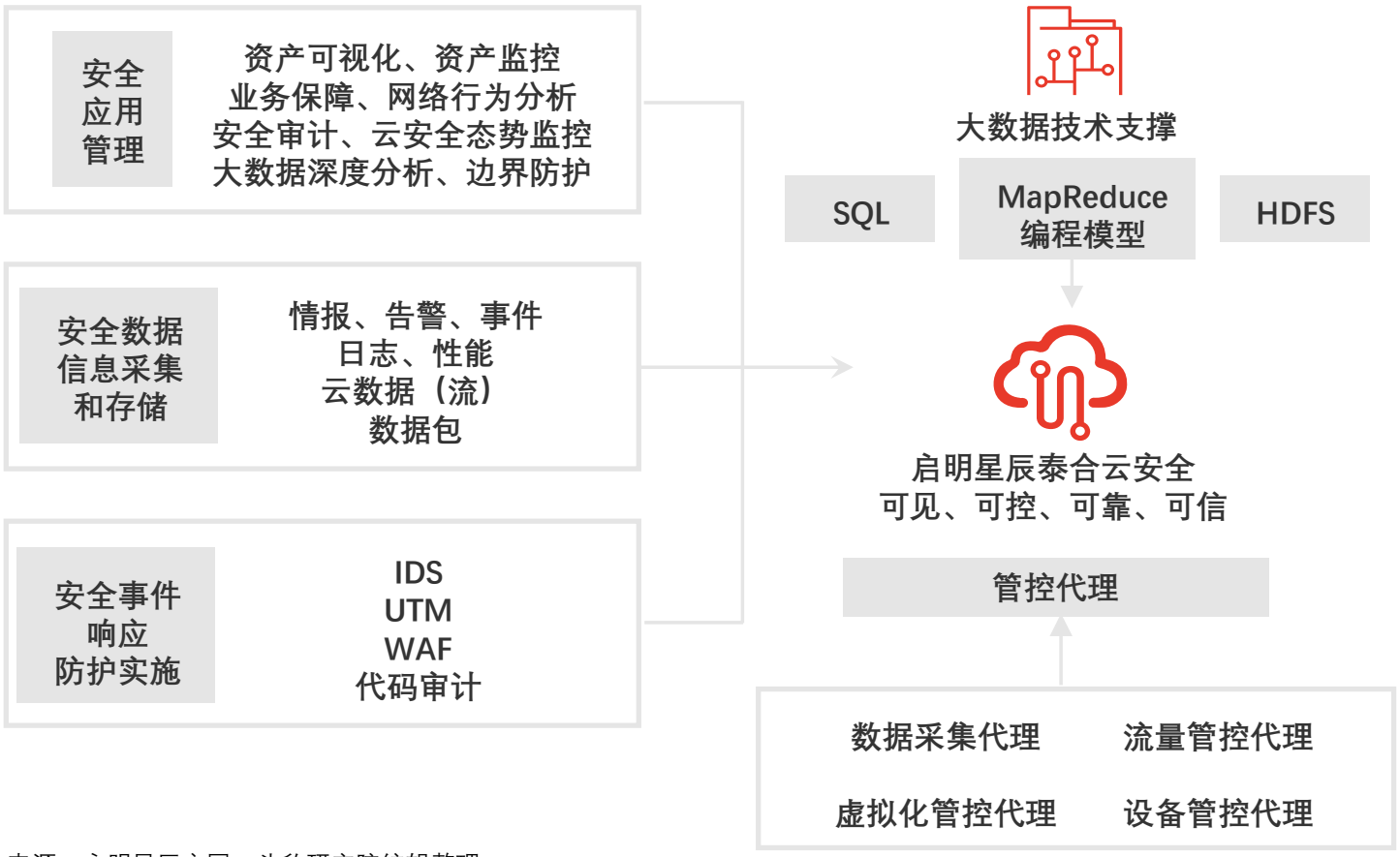
- **技术支撑服务原则：**坚持"上不碰应用，下不碰数据，不做股权投资"的原则，提供从软件到硬件到芯片的技术支撑；
- **全栈安全战略：**针对物理、网络、主机、应用、数据各环节，实现华为自身安全积累与安全服务的融合；
- **超值服务策略：**依托AI技术，华为扭转安全产品参数多、配置难的困境，部分安全服务可自动完成云上部署（DDoS高防、WAF等）。

头豹 LeadLeo

中国云安全行业主力厂商表现——启明星辰云安全

启明星辰云安全：看好云边界安全产品差异化服务能力，大数据技术与云安全多维度结合，产品服务维度、粒度持续提升

启明星辰云安全服务架构



➢多维度、多粒度安全管理

启明星辰泰合云安全管理平台结合物理环境及虚拟化环境信息采集技术，监控和防护云环境中资产、业务等各类知识信息，服务维度广，产品功能粒度高。泰合云安全平台广泛接入现有物理安全产品，对其他品牌安全产品兼容度高

➢敏捷调度、部署的管理平台

依托大数据智能分析技术，泰合云安全全面掌握云环境宏观安全态势、细分安全事件，针对不同时点、地域以及具体软件、硬件、虚拟安全产品需求进行调度、部署，减少云计算资源抢夺现象

➢云环境边界安全差异化服务

泰合云安全拆解传统物理安全产品（细分为安全管理、数据采集、安全防控三个环节），深度结合物理、虚拟数据采集方式，提高对云环境边界数据的监控、审计和保障，从不同等级、不同力度出发提供差异化安全防护方案

来源：启明星辰官网，头豹研究院编辑整理

头豹 LeadLeo

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，从态势感知、DevSecOps、安全等领域着手，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。