CAICT 中国信通院

中国通信标准化协会
China Communications Standards Association

云安全全景观察

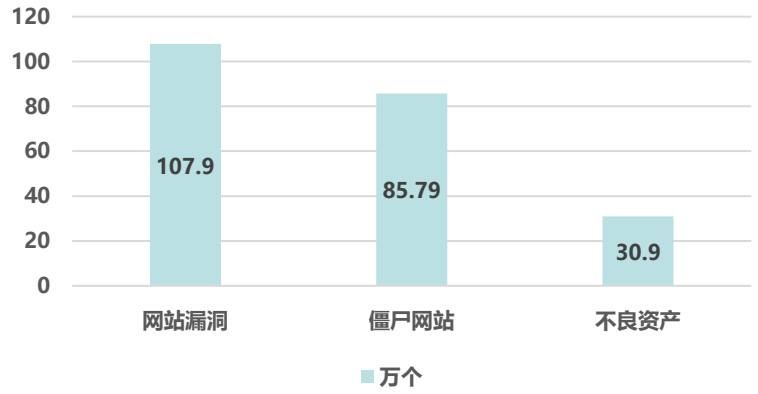
郭雪
中国信息通信研究院云大所云计算部副主任

2021 可信云大会
2021 TRUSTED CLOUD SUMMIT
数字裂变 可信发展

云计算安全备受关注
云安全产业亟待开展全景观察

云计算安全态势严峻

云平台成黑客攻击重要目标

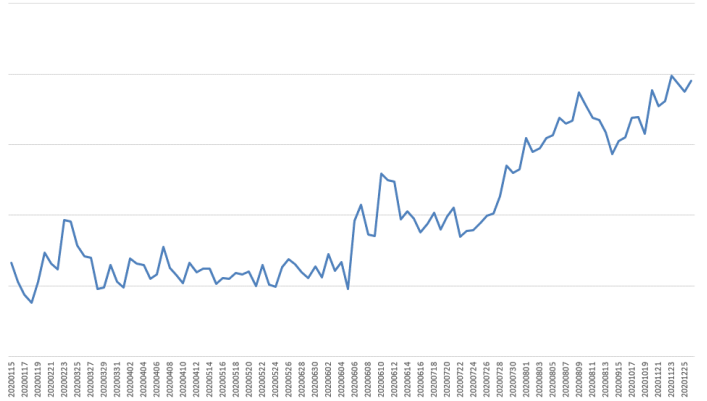


2021年上半年安全事件统计

数据来源：安恒信息玄武盾云监测服务平台

云平台将承载越来越多的重要数据与关键业务，黑客利用云计算提供商技术和管理上的漏洞，或利用云计算客户在云计算使用上的疏忽，**对云平台进行破坏**

云主机是黑灰产争夺主要资源



2020年挖矿木马增长趋势

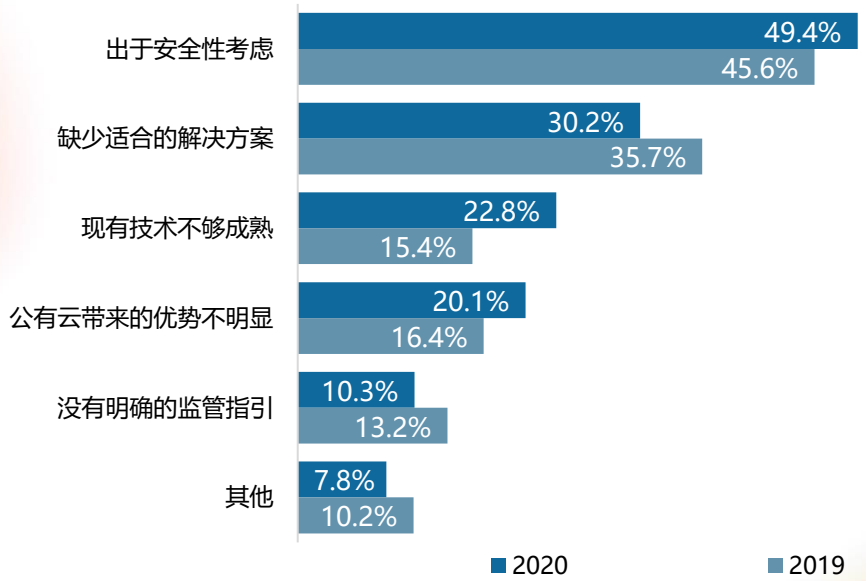
数据来源：《2020挖矿木马年度报告》腾讯安全

恶意客户利用云资源，进行**多种违法违规活动或云资源滥用行为**，如刷单、对外发起网络攻击等；随着近两年数字加密货币价格的暴涨，挖矿和利用僵尸网络分发挖矿木马急剧增加

安全性是企业选择云部署模式的重要考虑因素

安全性是企业暂未使用公有云的主要原因

《中国公有云用户发展调查报告（2021年）》显示，在尚未应用公有云的企业中，出于安全性考虑而未使用公有云的企业占比为**49.4%**

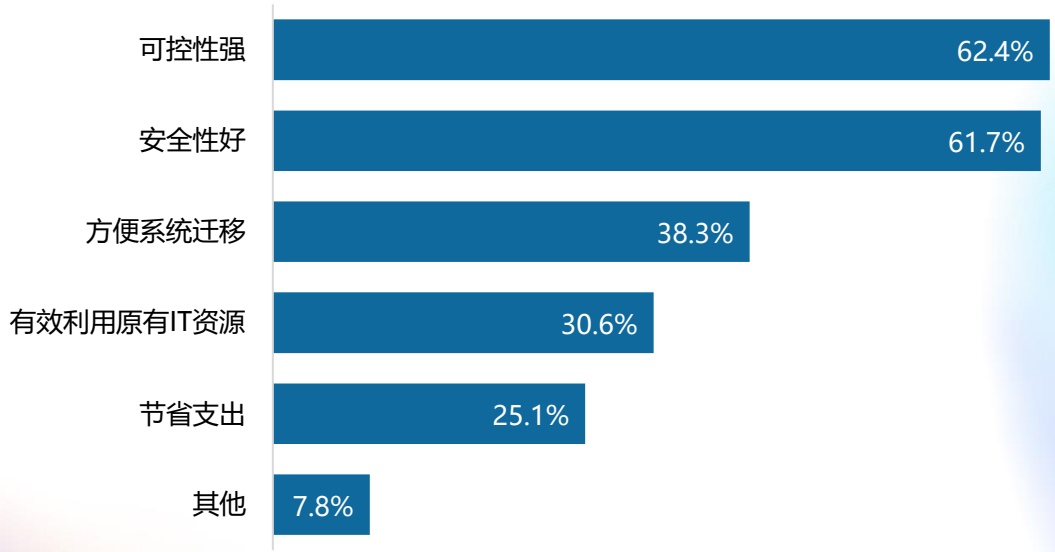


企业尚未应用公有云的原因

数据来源：中国信息通信研究院

企业因安全性好而倾向使用私有云

《中国私有云用户发展调查报告（2021年）》显示，**61.7%**的企业认为私有云拥有更好的安全性进而选择使用私有云

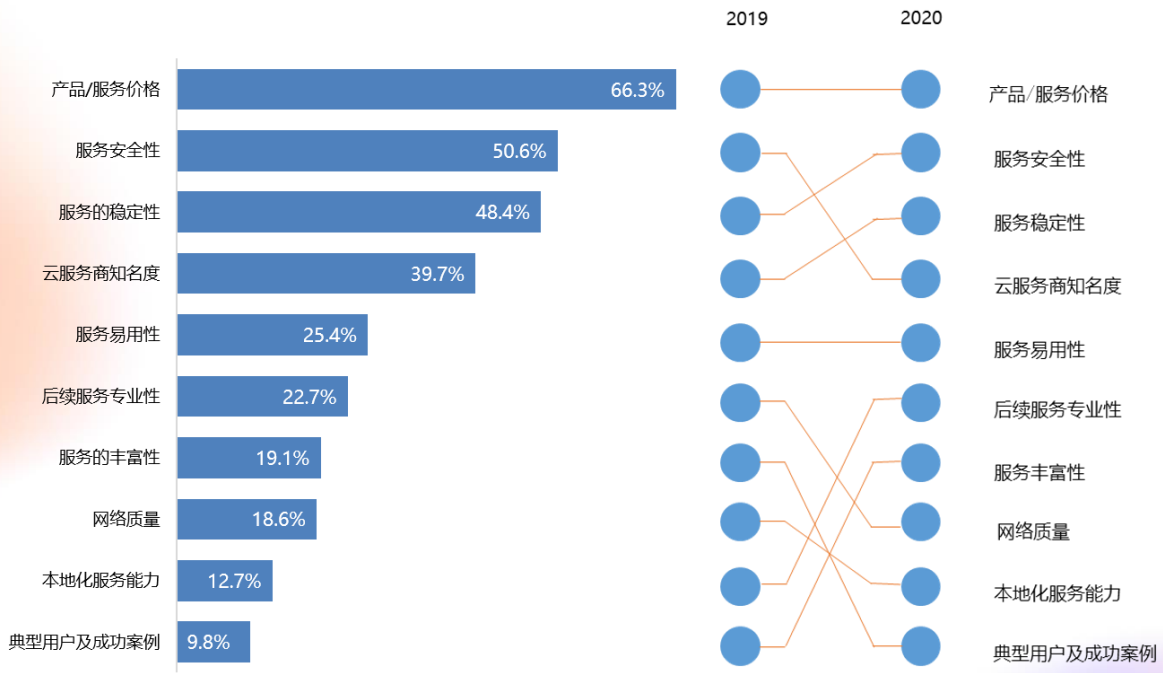


企业选择使用私有云的考虑因素

数据来源：中国信息通信研究院

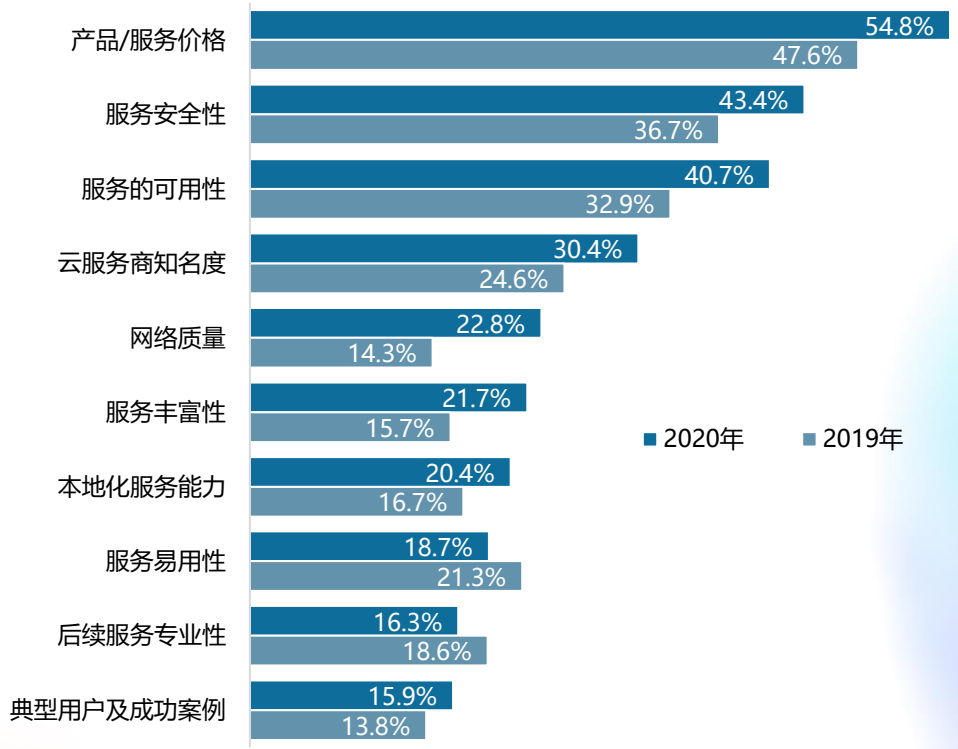
企业选择云服务商时重点关注服务安全性

无论是公有云还是混合云，企业在选择云服务商时都越来越将服务安全性放在优先考虑的位置，成为仅次于价格的**第二大关注因素**



企业选择公有云服务商的考虑因素

数据来源：中国信息通信研究院



企业选择混合云服务商的考虑因素

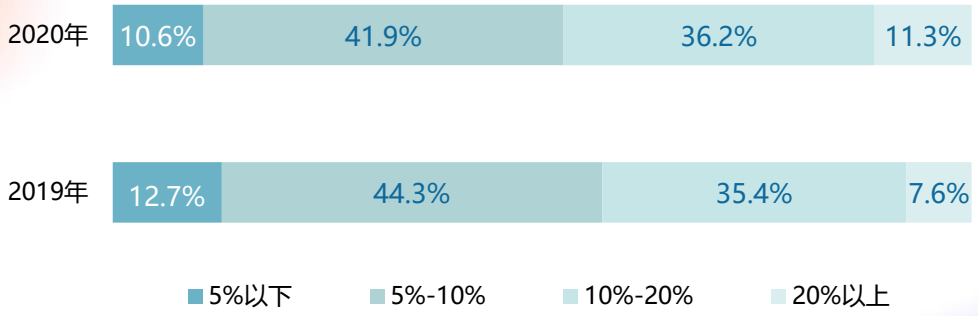
数据来源：中国信息通信研究院

用户侧云安全建设不断提升

企业云安全建设投入力度加大

据《中国私有云用户发展调查报告（2021年）》显示：

- 47.5%的企业在云安全上的投入占IT总投入10%以上
- 11.3%的企业私有云安全投入占IT系统总投入的两成以上



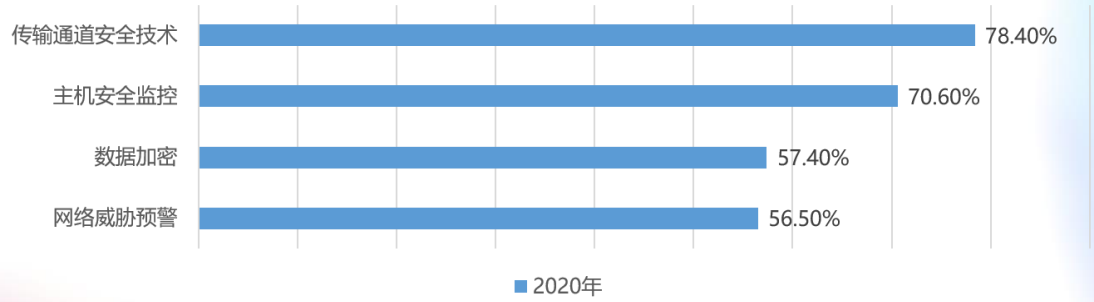
私有云安全投入占IT系统投入的比例

数据来源：中国信息通信研究院

企业云安全防护措施不断完备

据《中国私有云用户发展调查报告（2021年）》显示：

- 78.4%的企业采用了传输通道安全技术
- 70.6%的企业使用了主机安全监控



私有云安全防护措施采用情况

数据来源：中国信息通信研究院

开展全景观察：云安全产品供应侧和云计算供应侧安全

云安全全景图

梳理云安全产品供应情况

分析云安全产业供应侧发展现状与趋势

为云用户侧安全建设提供帮助

云计算供应侧安全

分析云服务商安全能力

分析云平台与云服务安全能力

为云计算供应侧安全能力提升提供指引

云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

零信任实验室
Zero Trust Laboratory

牵头

云服务商、安全厂商和云用户联合编写《云安全全景观察》

中国信息通信研究院、杭州安恒信息技术股份有限公司、腾讯云 计算（北京）有限责任公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、绿盟科技集团股份有限公司、北京蔷薇灵动科技有限公司、北京安天网络安全技术有限公司、甲骨文中国、浪潮云信息技术股份公司、贵州白山云科技股份有限公司、新华三技术有限公司、北京青云科技股份有限公司、中国铁塔股份有限公司、深圳华大生命科学研究院、杭州天谷信息科技有限公司

云安全产业全景图不断丰富
为云用户提供有力安全保障

云安全全景图：七大细分领域，三十六种安全产品

产品收录遵循：

以云服务形式提供

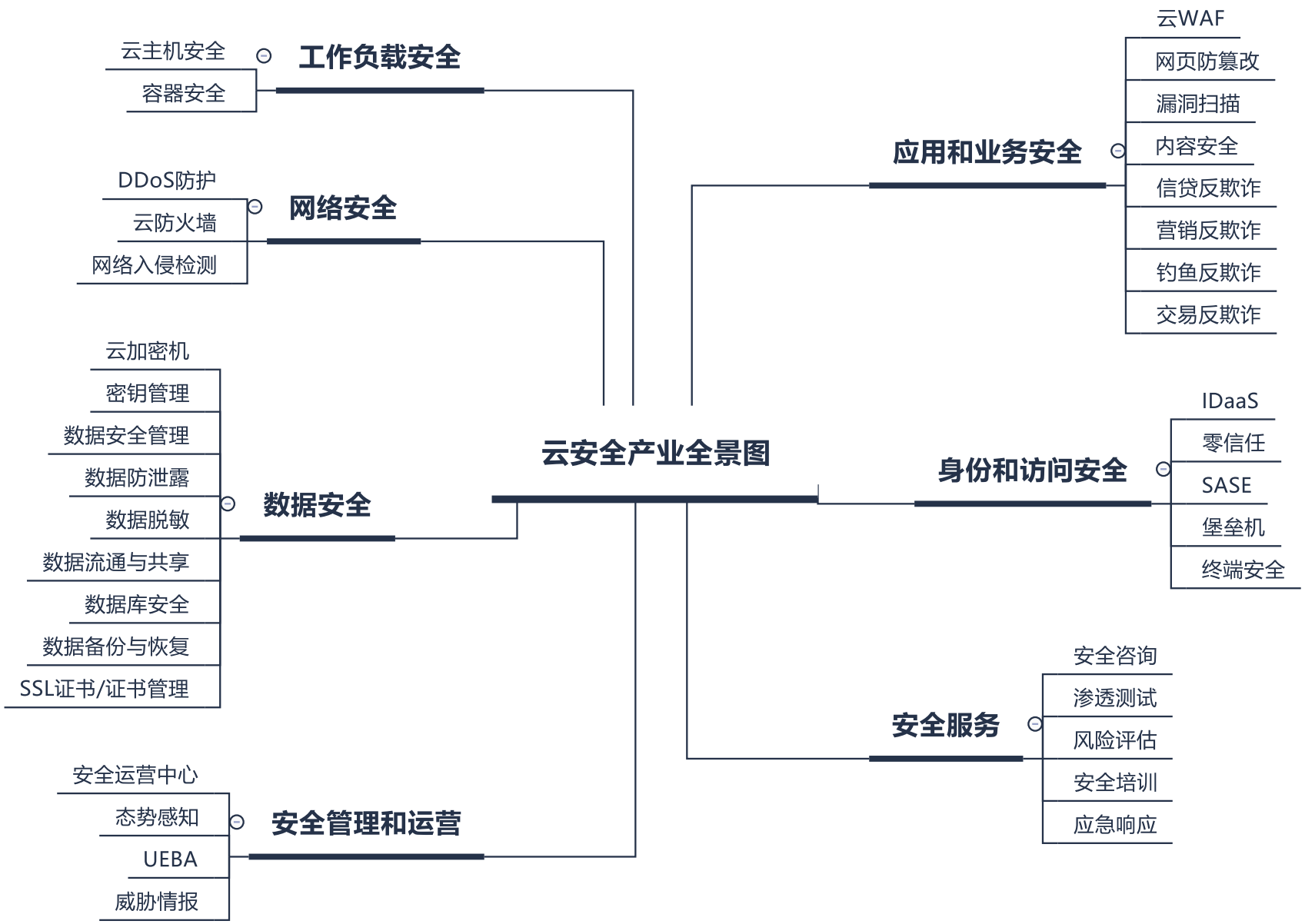
OR

以私有云部署的形式提供

OR

解决云面临的特殊安全风险

安全产品可以是物理设备，或部署于物理设备



工作负载安全：由主机向容器聚焦

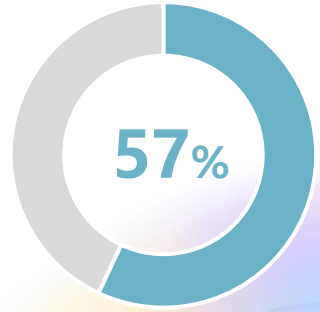
云主机安全发展成熟

云主机作为企业最核心的资产之一，如何保障其安全是企业安全建设时首要考虑的要素，在用户需求推动下，**供应数量在36种安全产品中居于首位。**

容器安全由功能模块向独立产品转变

供应商扩展已有安全产品以兼容容器应用场景

越来越多的供应商提供专门的容器安全产品，在本次全景图统计中，占比57%



独立容器安全产品占比

网络安全：原生安全优势突显

原生集成云网络设施

与云网络服务融合，无需改变业务架构，流量自动牵引，实现透明部署

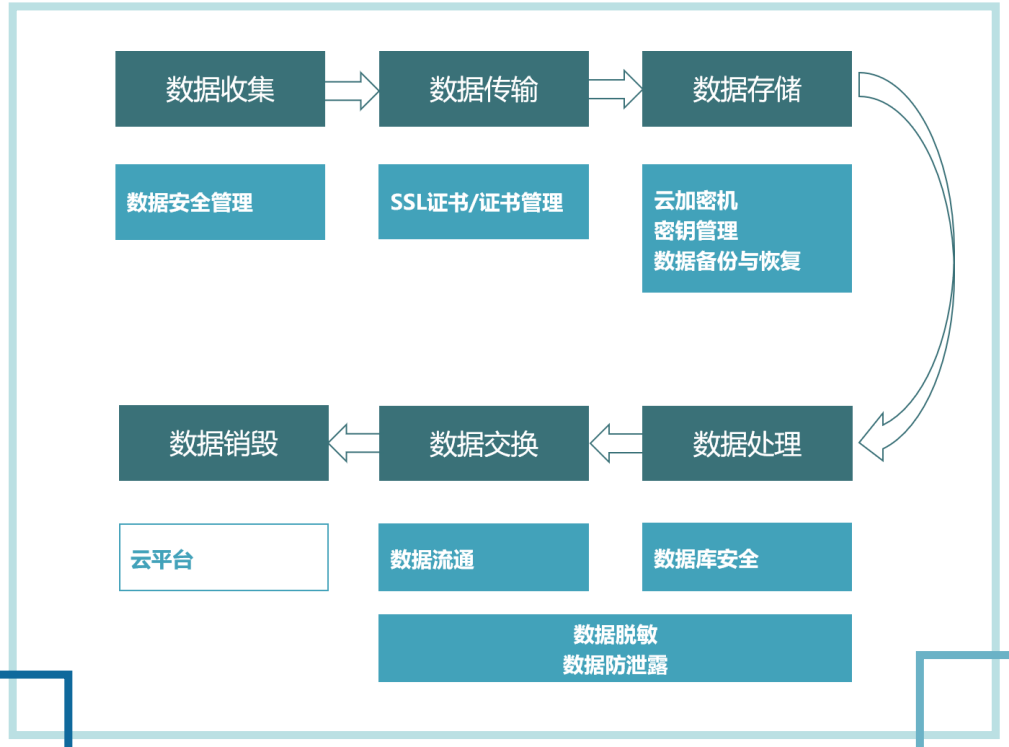
利用云平台原生资源实现性能提升

基于云平台计算、存储、网络等资源，集群化高可靠部署，安全防护性能平滑扩展

安全产品有效联动

各网络安全产品之间协同，联动处置安全事件，实现安全能力整合和纵深防御

数据安全：细分种类丰富实现全栈保护



- 数据作为企业的核心资产，丢失、泄露等安全事件的发生将严重影响企业业务运营，带来不可估量的损失
- 《数据安全法》等法律法规的发布对企业数据处理活动提出更加明确的安全要求

数据安全部分覆盖9种安全产品，**是产品种类最多的领域**，不同安全产品能够满足用户不同场景的数据保护需求，覆盖数据从收集、处理到交换的各个关键环节。

应用和业务安全：云WAF和内容安全为先行者

云WAF通过对云上Web应用的恶意流量、访问行为进行检测和拦截，实现Web应用的安全防护，是企业安全建设的基本选择，产品供应数量多

内容作为法律法规监管的重要对象，内容安全产业成为业务安全领域的先行者

- 数据处理能力强，能够对大流量数据进行实时采集和分析；
- 内容识别能力强，对经过特殊处理的目标仍然能够准确识别

身份和访问安全：零信任理念将成为发展核心

随着企业数字化转型进程的不断深化，以数据中心内部和外部进行划分的安全边界被打破。**零信任理念以身份为基石，能够打破边界安全架构下对信任的假设和滥用，成为可信安全访问的主要选择和趋势。**

用户访问

工作负载访问

安全厂商依靠技术积累提供侧重不同的零信任安全解决方案

云服务商侧重零信任SaaS服务

SD-WAN供应商推出零信任与SD-WAN结合的SASE产品

安全管理和运营：威胁感知与防御全局化

企业云上资产数量和构成日益复杂，海量安全信息难以整合利用，高效的安全管理和运营成为痛点，**依托安全运营中心、态势感知构建安全管理和运营体系成为企业的首要选择：**

A 对云上资产进行统一管理

自动化动态盘点全局资产、检查配置风险

B 安全事件关联分析和统一运营

对分散的资产、安全、日志等数据进行统一处理，通过关联分析发现潜在的安全风险

C 安全策略统一管理与编排

策略进行统一配置和下发；通过自定义编排策略实现安全产品的联动协同

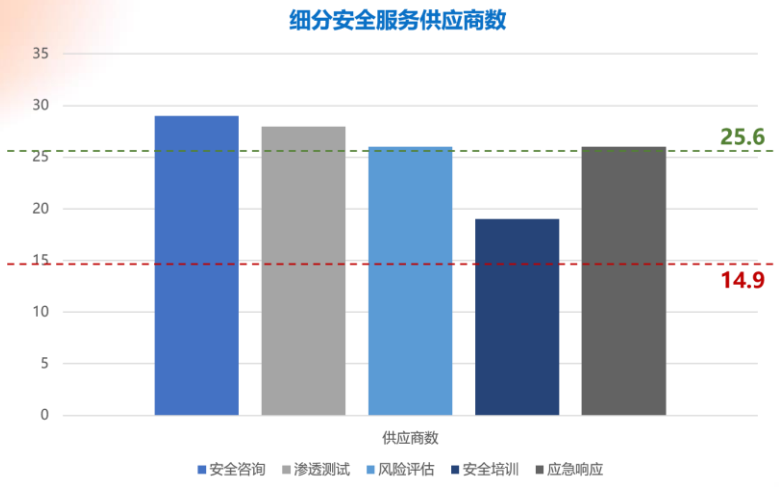
D 安全态势总览可视化

直观、形象的掌握全局安全态势

安全服务：各细分产品发展呈均衡向好态势

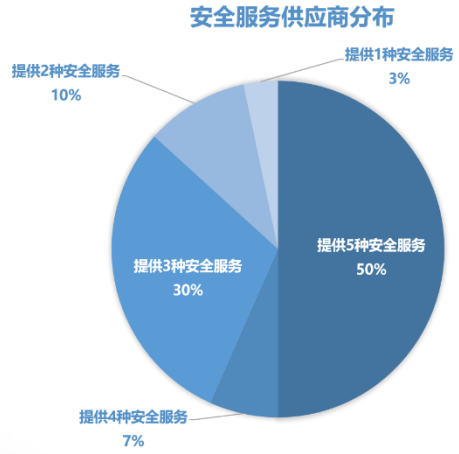
各安全服务供应丰富，数量超全景图均值

行业客户缺少专业的安全团队或安全人员不足，同时，因自身业务发展特性，安全定制化需求强烈；供应商**从产品导向向服务导向转变**，纷纷提供专业的、定制化的安全服务



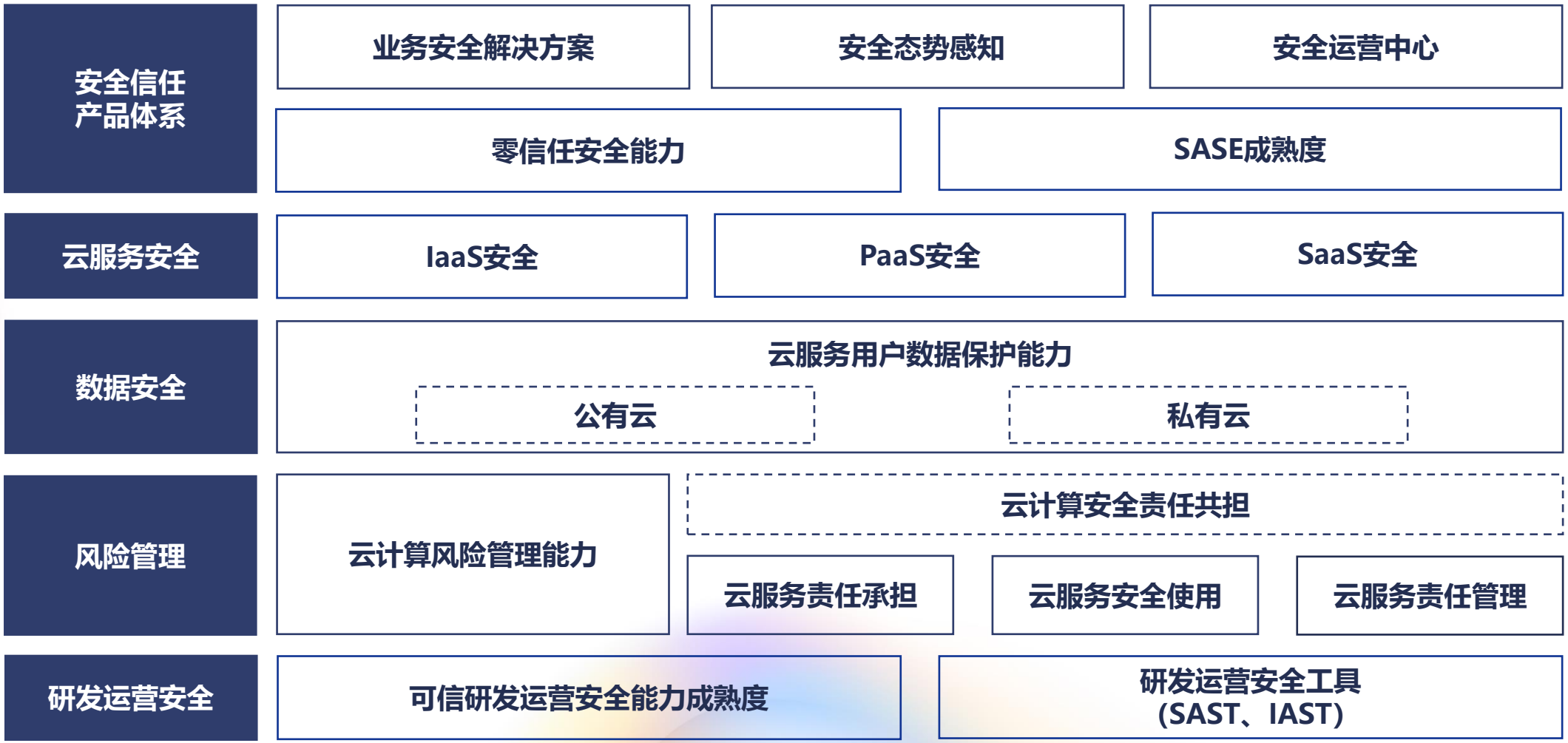
主流供应商能够提供较全面的安全服务

15家供应商提供全部（5种）安全服务，占安全服务类供应商数量的50%；
11家供应商提供3-4种安全服务，占安全服务类供应商数量的37%



云计算供应侧基本安全能力较完备
距高水平仍有提升空间

“可信云”安全评估全景图


安全信任产品体系
业务安全解决方案
安全态势感知
安全运营中心
零信任安全能力
SASE成熟度
云服务安全
IaaS安全
PaaS安全
SaaS安全
数据安全
云服务用户数据保护能力
公有云
私有云
风险管理
云计算风险管理能力
云计算安全责任共担
云服务责任承担
云服务安全使用
云服务责任管理
研发运营安全
可信研发运营安全能力成熟度
研发运营安全工具
(SAST、IAST)

云服务商风险管理能力：已有机制待进一步优化

网络流量安全管控能力待提升

一部分云服务商南北向流量的安全检测和防护手段较为健全，但存在一定的局限：

- ✓ 云内东西向流量安全情况难以把控
- ✓ 缺少由云平台对外发起攻击的检测

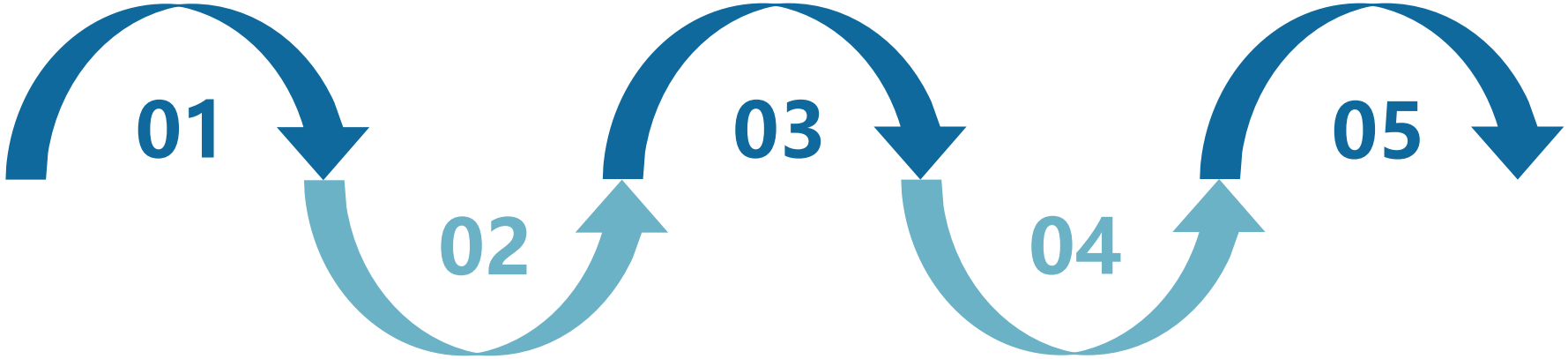
缺少统一、系统的安全管理和运营

一部分云服务商在安全管理和运营中涉及众多平台和工具，使用过程复杂，安全管理和运营效率不高

- ✓ 资产管理较为分散
- ✓ 安全策略独立配置
- ✓ 安全事件告警与处置孤立

机房建设标准掌控程度不够

租用第三方的数据中心，或作为子公司使用集团建设的数据中心，云服务商往往对数据中心建设标准掌握不足，管控能力较为薄弱，不了解安全指标情况。



研发阶段安全机制建设不足

一部分云服务商仍然采用传统研发运营安全模式,安全介入相对滞后：

- ✓ 需求分析重业务而轻安全
- ✓ 代码层面安全覆盖度不够
- ✓ 开源及第三方组件风险管理未成体系

安全责任划分需进一步明确

大部分云服务商通过在SLA中添加免责条款告知不在云服务商责任范围内的风险事件，缺少系统化、精细化的安全责任划分：

- ✓ 免责条款难以覆盖全部云计算安全责任
- ✓ 免责条款颗粒度不够细化

云服务商数据保护能力：安全措施缺少特性化场景支持

加密算法可配置性不足

- ✓ 不支持用户**自主选择加密算法**、设置密码长度,内置的算法可能无法满足用户在强度、安全性、效率等方面的需求
- ✓ 缺少对**国密算法**的支持,难以满足部分行业用户的特殊合规需求

异常行为预警与审计能力待提升

- ✓ 缺少**异常行为的自动审计**，更多的是被动的进行事后追溯
- ✓ 缺少**异常行为的实时预警**，因缺少自动审计，无法对审计发现的异常行为进行及时告警，数据的违规访问和操作不能及时被处置

缺少专门针对数据安全事件的应急管理

- ✓ 在**安全事件分类分级**方面，不同数据安全事件的响应与处置方式存在较大差异，通用应急管理机制中的手段难以有效应对
- ✓ 在**应急演练**方面，侧重业务中断演练，缺少安全类事件的演练
- ✓ 在**用户售后**方面，缺少系统性、标准化的补偿机制，服务商与用户双方对数据价值的界定存在分歧

内部账号存在滥用风险

- ✓ 存在**多人共享同一账号**的现象，通过日志记录仅能追溯至责任账号，而无法定位到具体的账号使用人员
- ✓ 存在**非授权人员使用高权限账号**的可能，缺少高权限账号临时授权机制，授权结束后仍然可以使用或分发高权限账号

云服务安全能力：云控制台基础安全能力

云服务的一部分安全能力由云控制台实现，同一云平台的各云服务通用，云控制台作为云服务访问和管理的基础

敏感操作保护措施与用户体验难以平衡

- 因二次权限认证可能影响用户体验，**仅开启二次确认功能**
- 支持敏感操作二次权限认证，但短时间内进行大量操作时均需进行认证，**影响用户体验**

日志管理功能完备性不足

- 不支持用户**自主设置日志存储时间**
- 日志导出后的数据格式过于简单很多**原始信息无法获得**，不利于用户进一步的日志分析

增加用户自定义功能

二次权限认证策略智能化

云服务安全能力：IaaS/PaaS安全能力

缺少不同加固等级的云主机镜像

不同用户对云主机操作系统安全等级要求存在差异，通用的云主机镜像模板无法满足用户不同等级的安全要求

快照等备份数据删除机制存在优化空间

在用户删除云主机时，其关联的快照、镜像等默认不删除，用户无法选择自动删除关联的副本，副本数据遗留，未来可能存在数据安全风险

账户临时授权能力有待提升

PaaS需要根据业务需求按最小权限原则为用户授权，自定义策略能实现不同资源粒度访问，但对时间的限制能力不够，不利于对临时人员访问权限进行回收，账号安全存在风险

云服务安全能力：SaaS安全能力

后疫情时代，SaaS服务从协同办公、CRM等企业管理领域，逐渐向金融、医疗、教育、政务、工业等行业**垂直领域深入**，企业上云用云**向SaaS层上移**，迎来全新阶段。**SaaS服务的安全性**亦逐渐成为企业关注的重点，当下数据至上的时代，隐私的安全也已经成为诸多企业逐渐重视的课题。

安全管理体系化程度不高

SaaS企业的安全管理体系化程度普遍不高，应加强安全团队的组建、安全管理规范的制定、整体安全体系的建设，更大程度地解决安全风险及挑战，保证业务的连续性和安全性。

身份鉴别能力与用户体验平衡难度高

以下安全要求与对用户体验产生影响的矛盾普遍存在。

1. 身份鉴别中加入二次身份验证机制以保证高安全性的要求。
2. 为防止密码被黑客盗取，一定周期内要求用户对登陆密码进行修改以保证更高的安全性的要求.。

数据保护问题仍任重道远

用户隐私数据泄露的问题仍层出不穷，对于SaaS的数据安全问题仍任重而道远。

1. 需要保证数据的实时加密，且具有备份以及灾备策略。
2. 应用体系架构应能确保数据的隔离性。

DDoS安全防御应用程度较低

SaaS服务商对抗DDoS产品的应用程度较低。SaaS企业应通过防护攻击行为进行精准识别和自动加载防护规则，保证网络的稳定性和安全性。

安全产品的碎片化问题亟需改善

SaaS企业普遍采购和使用的安全产品存在着碎片化的问题，网络安全工作呈分散化，未来产品的集成化发展将有效解决碎片化问题。

“可信云”安全评估全景图

云计算风险管理能力

阿里云计算有限公司
中国电信集团有限公司
腾讯云计算（北京）有限责任公司
华为云计算技术有限公司
北京百度网讯科技有限公司
北京京东叁佰陆拾度电子商务有限公司
中国移动通信集团有限公司
优刻得科技股份有限公司
深圳平安通信科技有限公司
浪潮云信息技术股份公司
曙光云计算集团有限公司
北京金山云网络技术有限公司
联通云数据有限公司
上海浦东发展银行股份有限公司
中国银联股份有限公司
中国联合网络通信有限公司软件研究院

云主机安全

北京金山云网络技术有限公司
中国银联股份有限公司
中国电信集团有限公司
中国移动通信集团有限公司
优刻得科技股份有限公司
浪潮云信息技术股份公司
万达信息股份有限公司
北京京东叁佰陆拾度电子商务有限公司
深圳平安通信科技有限公司
阿里云计算有限公司
腾讯云计算（北京）有限责任公司
华为云计算技术有限公司
联通云数据有限公司

云服务用户数据保护能力

腾讯云计算（北京）有限责任公司
阿里云计算有限公司
华为云计算技术有限公司
北京金山云网络技术有限公司
中国电信集团有限公司
北京百度网讯科技有限公司
中国移动通信集团有限公司
佳讯飞鸿（北京）智能科技研究院有限公司
优刻得科技股份有限公司
华云数据控股集团有限公司
深圳平安通信科技有限公司
浪潮云信息技术股份公司
深圳国家基因库
联通云数据有限公司
中国移动通信集团福建有限公司

SaaS安全

用友网络科技股份有限公司
华为技术有限公司
中国移动通信集团有限公司
上海微盟企业发展有限公司
北京知道创宇信息技术股份有限公司
杭州天谷信息科技有限公司
北京同创永益科技发展有限公司
杭州点智连科技有限公司
财智共享（北京）技术服务有限公司

PaaS安全

腾讯云计算（北京）有限责任公司
中国联合网络通信有限公司软件研究院

零信任安全能力

腾讯云计算（北京）有限责任公司
北京蔷薇灵动科技有限公司
北京天融信网络安全技术有限公司

SASE成熟度能力

深信服科技股份有限公司
贵州白山云科技股份有限公司

安全态势感知

阿里云计算有限公司
北京金山云网络技术有限公司
华为云计算技术有限公司
腾讯云计算（北京）有限责任公司
中国移动通信集团有限公司
中国联合网络通信有限公司浙江省分公司

安全运营中心

华为技术有限公司
腾讯云计算（北京）有限责任公司
深信服科技股份有限公司
阿里云计算有限公司
联通云数据有限公司
浪潮云信息技术股份公司
北京奇虎科技有限公司
北京启明星辰信息安全技术有限公司
上海浦东发展银行股份有限公司
北京天融信网络安全技术有限公司
杭州安恒信息技术股份有限公司
北京知道创宇信息技术股份有限公司

GPU云主机安全

中国电信集团有限公司

物理机安全

中国电信集团有限公司

块存储安全

中国电信集团有限公司

负载均衡安全

中国电信集团有限公司

堡垒机安全

浪潮云信息技术股份公司

内容安全

腾讯云计算（北京）有限责任公司
同盾网络科技有限公司
阿里云计算有限公司
华为云计算技术有限公司

研发运营工具能力

奇安信科技集团股份有限公司
深圳开源互联网安全技术有限公司北京安普诺信息技术有限公司
深圳开源互联网安全技术有限公司

THANKS!

2021
TRUSTED CLOUD
SUMMIT