中国云安全行业研究报告

概念界定

融合云技术，采用云交付，保护云资源及云应用的安全产品

云安全是传统信息安全行业技术的升级，产品的丰富，也是云计算部署的焦点，服务的关键。因此，云安全是云计算与信息安全相互赋能所孵化的新概念。其一，云安全是云计算技术在安全领域的应用，即云安全应用。目的是利用云计算特征，将传统安全产品云化，来提供更能满足个人或行业需求的网络安全解决方案或安全服务。其二，云安全是安全技术在云计算领域的应用，即云自身安全。目的是应用安全技术，解决云计算的安全问题，包括云基础设施安全，云计算资源安全，云计算操作系统安全，云计算应用软件安全，用户信息安全等，提升云服务的可靠性，促进云计算行业的健康良性可持续发展。

云安全概念界定

防护目标

保护云计算基础设施，或防护部署在云平台的相关应用

技术能力

结合云计算技术，融合数智化工具，具备云计算弹性、敏捷等特征

交付模式

采用云交付模式，可按需、按量、按时长付费，并可根据云服务形式和部署模式不同灵活提供选择产品

来源：艾瑞咨询研究院自主研究及绘制。

云安全与传统安全差异

内深外宽、边界模糊、数智工具、责任共担

不论是云安全应用还是云自身安全，云安全与云计算紧密相连。云计算与传统计算在理念与技术上存在显著差异。系统平台开放化，计算网络存储虚拟化，数据所有权与管理权分离化等云计算的显著特征，导致传统的安全措施并不能满足云安全的需要。虽然云安全与传统信息安全相似，均是为了保护计算资源与信息数据的安全性。但是云服务提供商与传统安全厂商在设计云安全产品或提供云安全解决方案时应着重考虑云安全威胁的多样性与需求的独特性。

云自身安全与传统安全比较

	云安全	传统安全
安全内容	云计算相关安全内容更加广泛，需要格外关注虚拟化技术带来的安全挑战（网络，存储，服务器虚拟化等）	传统的安全解决方案不考虑虚拟机安全
安全规模	云计算系统部署在包括大规模物理基础设施数据中心中，其复杂性使安全问题并不局限在单一设施，而是完整的系统安全	传统的安全解决方案关注单机安全
安全边界	云计算的发展使云计算的应用场景不断拓展，产品界限不断模糊，安全解决方案往往不局限某一模块，而是根据用户需要提攻供合解决方案	传统的安全方案可以清晰划分出物理与程序的安全边边界
安全技术	云自身安全技术需要考虑云计算的分布式计算与存储，网格式网络以及虚拟化与虚拟化管理平台等	传统的安全方案主要关注安全软件技术和安全硬件技术面对安全风险，往往采用后期升级或者补丁的形式，安全技术并不复杂
安全管理	云自身安全管理复杂灵活，需要根据部署模式与服务模式差异进行调整，同时需要与租户及监管等多方配合	传统的安全解决方案实施与管理相对简单清晰，安全管理往往是用户承担主要责任

来源：艾瑞咨询研究院自主研究及绘制。

云安全行业发展历程

由独立产品到综合解决方案，由通用安全功能向定制化发展

与云计算行业当前的“云网端”业务发展模式相反，云安全行业的发展可以概括为“端网云”。1）围绕主机安全为主的单机安全阶段，安全防护措施主要以主机病毒查杀软件为主；2）伴随互联网的出现，网络安全逐步成为安全行业关注焦点，网关类安全产品陆续出现，安全防护重点从局域网逐步拓展至广域网；3）云计算时期，早期行业安全建设相较于云计算发展相对滞后，产品类型仍以网关类为主，主要依靠升级传统安全工具来适配云计算安全需求；4）产业互联网时期，云计算广泛渗透，云安全伴随企业上云加速成为关注焦点。在技术上，云安全产品更立足于云计算特性，并融入数智化工具。在实践中，产品能力进一步打通，可根据行业特征及企业业务特性提供更强定制化能力。

云安全发展历程

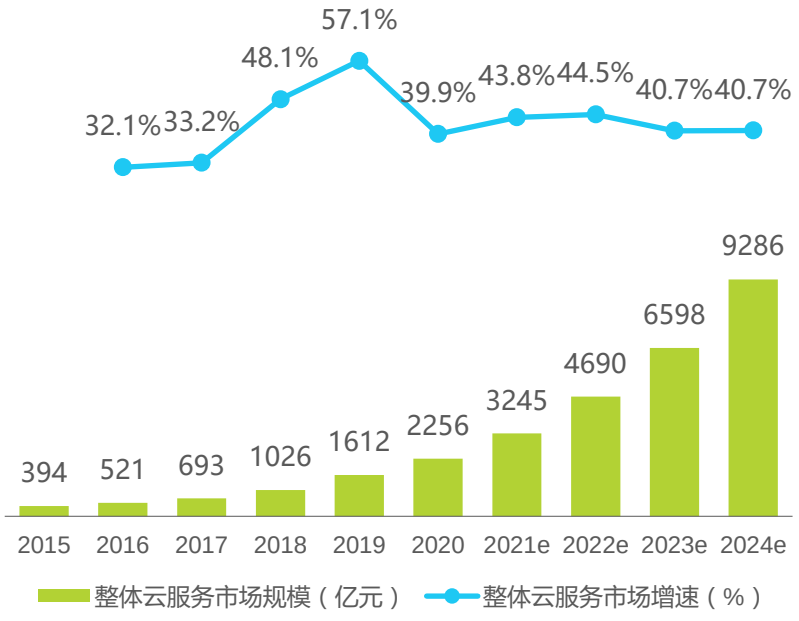
来源：艾瑞咨询研究院自主研究及绘制。

云安全发展特征——供给

中国云服务行业加速发展，云安全较云行业增长存在滞后性

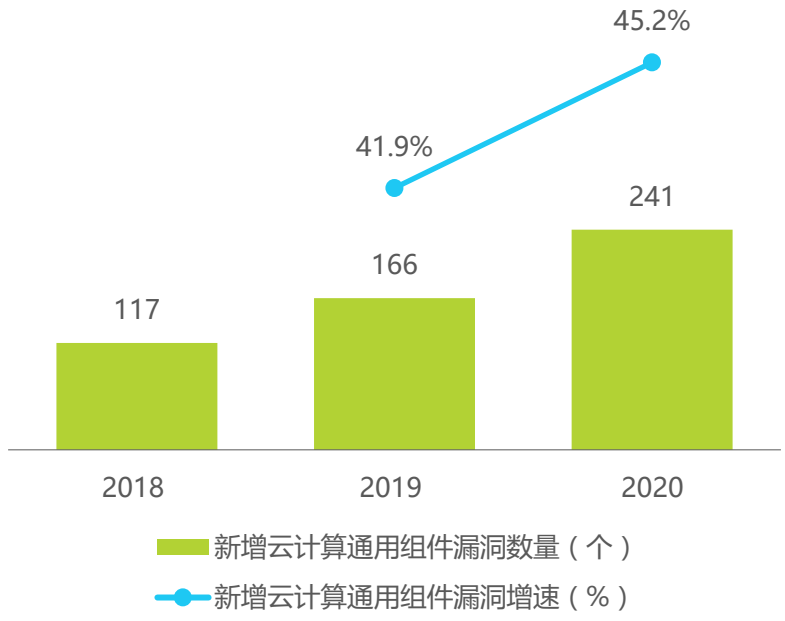
伴随产业互联网发展，中国云计算行业整体迎来发展加速期，市场规模屡创新高，行业应用不断落地。伴随着云计算逐步成为数字经济的技术底座、企业数字化转型的关键基础设施，云计算所面对的潜在风险也显著提升。从2019至2020年，新增云计算通用组件漏洞增速达到45.2%，漏洞数量的增多主要源于云计算已走出互联网行业，向更多传统行业加速渗透，应用场景更丰富，导致所面临的安全威胁和攻击手段更加多元。

2015-2024年中国整体云服务市场规模及增速



来源：艾瑞咨询研究院自主研究及绘制。

2018-2020年中国新增云计算通用组件漏洞数量及增速



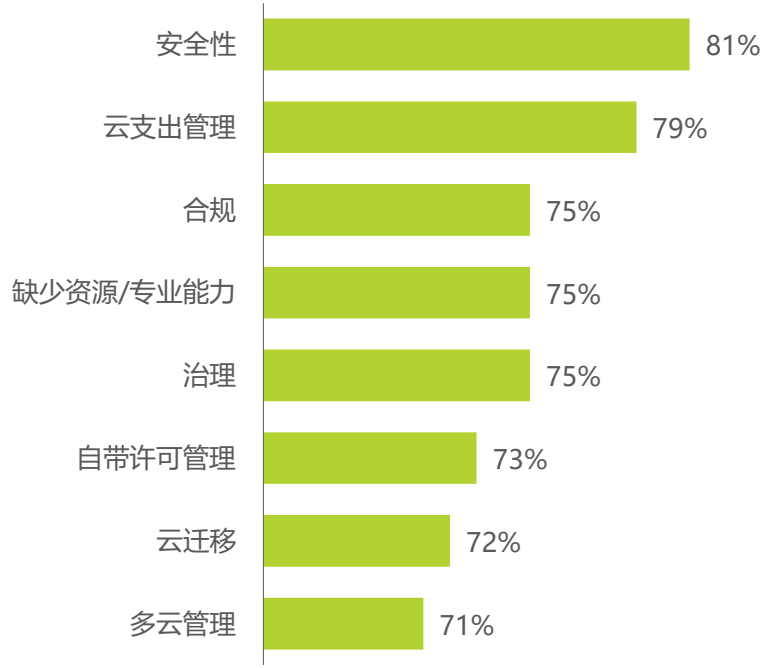
来源：CNCERT，艾瑞咨询研究院自主研究及绘制。

云安全发展特征——需求

伴随企业上云、用云深化，云安全关注度显著提升

安全性长期是企业上云、用云必须要考虑的内容，在用户调研中位列企业上云挑战首位。根据企业上云阶段不同，在上云早期，虽然企业首先聚焦于如何搭建和使用云计算，但对其他云模块关注较为平衡；但在企业用云扩张阶段（上云中期）和在完全上云后，企业对云安全的关注显著提升。由此可见，云安全既是企业实现快速业务拓展的有效支撑，也是保障业务顺利推进的可靠保障，坚实的安全底座是企业助力企业更好发挥云服务能力的关键。

2021年全球不同规模企业上云挑战



2021年全球不同上云阶段企业用云挑战

上云早期		上云中期		完全上云	
治理	79%	缺少资源/专业能力	87%	云支出管理	81%
缺少资源/专业能力	78%	**安全性**	86%	**安全性**	81%
云迁移	77%	云支出管理	78%	治理	75%
安全性	76%	治理	77%	合规	75%
云支出管理	75%	自带许可管理	77%	缺少资源/专业能力	72%

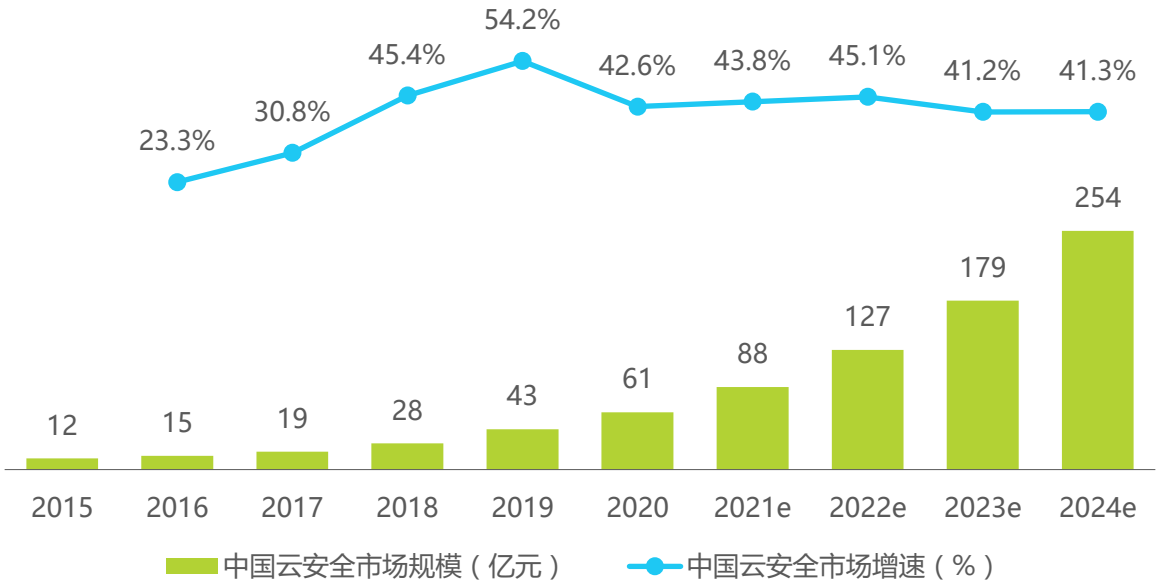
来源：Flexera, N = 750, 艾瑞咨询研究院自主研究及绘制。

云安全市场规模

云安全市场空间广阔，产业升级、政策利好提供增长机遇

中国云安全市场相较于整体云市场体量较小，增长空间广阔。在云计算发展早期，云安全发展相较云资源与云能力产品发展存在滞后性，且安全产品及安全服务提供者集中于云服务厂商。伴随产业互联网深化，云计算广泛渗透带动云安全产品布局加快。一方面，“云+行业”推动云安全产品与时俱进，适用场景扩大、用户需求提升；另一方面，传统安全厂商陆续开始布局云安全领域。最后，中国云安全产业具有较强政策导向，近年来《网络安全法》、网络信息安全等级保护2.0、《数据安全法》的出台，驱动企业关注、提升安全能力，扩大安全领域支出。

2015-2024年中国云安全市场规模

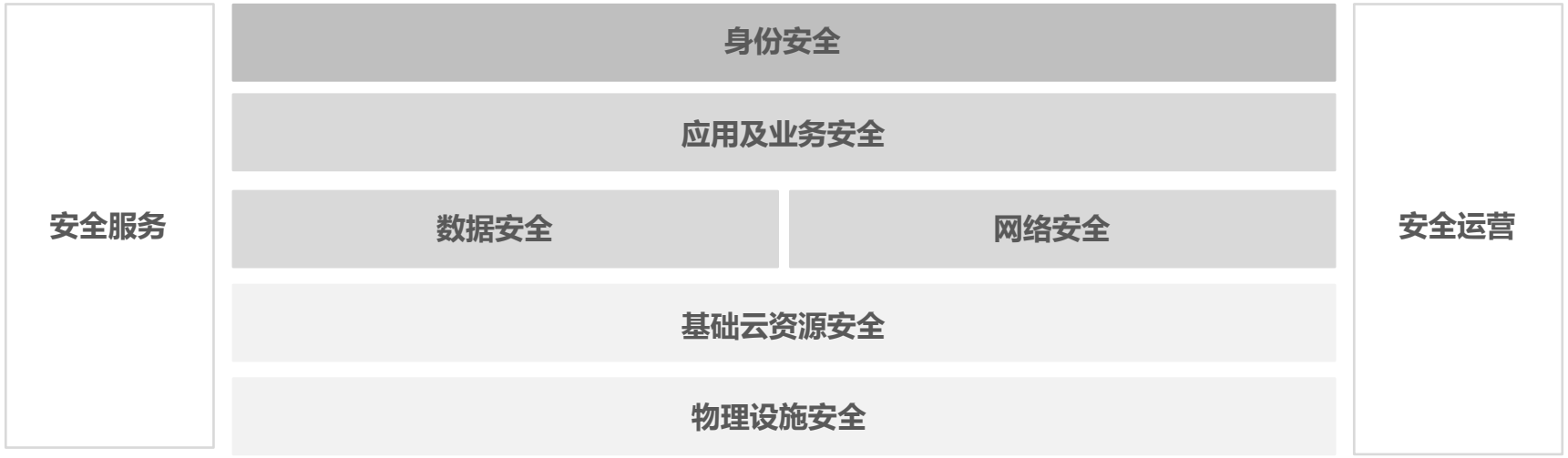


备注：市场规模主要以狭义的云安全产品为主，主要包括：云基础资源安全产品：云主机安全、云原生安全、云堡垒机，网络安全产品中：云DDoS，云网络防火墙，业务安全中：云WAF，云厂商所提供的安全产品模块中：数据安全产品，业务安全产品，安全服务。除以上的泛云安全领域的产品及服务并未计入市场规模统计中。

来源：互联网公开资料、专家访谈，艾瑞咨询研究院自主研究绘制。

中国云安全行业洞察——产品服务

云安全产品结构



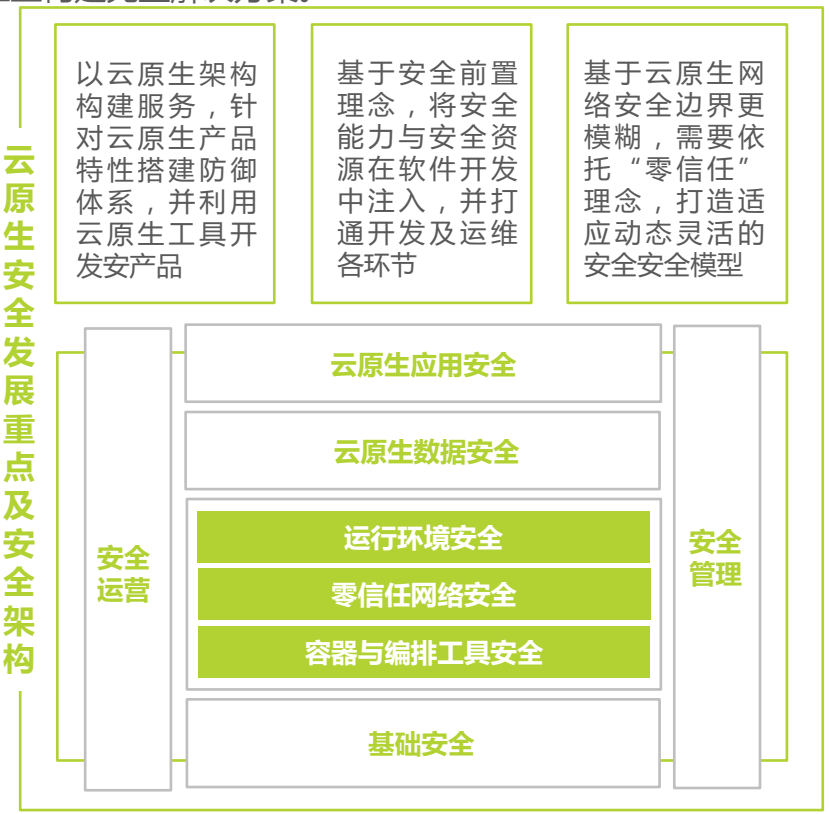
备注：由于物理设施安全主要由安全厂商/云厂商或企业自行负责建设，因此不作为独立云安全产品在本报告中讨论。
来源：艾瑞咨询研究院自主研究及绘制。

云基础资源安全

伴随云原生应用下沉，云原生安全逐步成为云基础安全重点

云原生技术经过长足发展，已逐步被广泛应用，并逐步突破容器、微服务、DevOps等领域，开始形成更完整的云原生产品架构，云原生的应用在显著提升云计算产品能力的同时，也带来的更为复杂的安全需求。传统的安全防护理念，“非原生化”的安全产品与服务均不能满足云原生安全需求。为保障云原生安全，需要更深刻理解云原生架构，熟悉云原生特点，针对针对云原生不同产品特性，提供针对性安全对策，并从下至上构建完整解决方案。

来源：艾瑞咨询研究院自主研究及绘制。



来源：艾瑞咨询研究院自主研究及绘制。

云基础资源安全——产业图谱

云主机安全

Hillstone 山石网科 | 天融信 TOPSEC | 青藤云安全 | ultrapower 神州泰岳 | 网宿科技 | SANGFOR 深信服科技
奇安信 QI-ANXIN | AsiaInfo 亚信安全 | 安恒信息 DAS-security | Neusoft | NSFOCUS 绿盟科技 | 360 政企安全
安天 | H3C | 安全狗 | 志翔科技 ZSHIELD INC
HUAYUN 华云 | 移动云 | 联通云 Unicom Cloud | 中国电子云 CECLOUD | UCLOUD 优刻得 | inspur 浪潮 | 紫光云

容器安全

天融信 TOPSEC | Hillstone 山石网科 | 安全狗
NSFOCUS 绿盟科技 | 奇安信 QI-ANXIN | 安天
AsiaInfo 亚信安全 | 青藤云安全
移动云

堡垒机

奇安信 QI-ANXIN | 天融信 TOPSEC | 知道创宇 | AsiaInfo 亚信安全 | H3C
任子行 SURFILTER | NSFOCUS 绿盟科技 | 北信源 VRV | 安恒信息 DAS-security | 观安
inspur 浪潮 | 中国电子云 CECLOUD | 联通云 Unicom Cloud
UCLOUD 优刻得 | 紫光云 | 移动云

综合云厂商

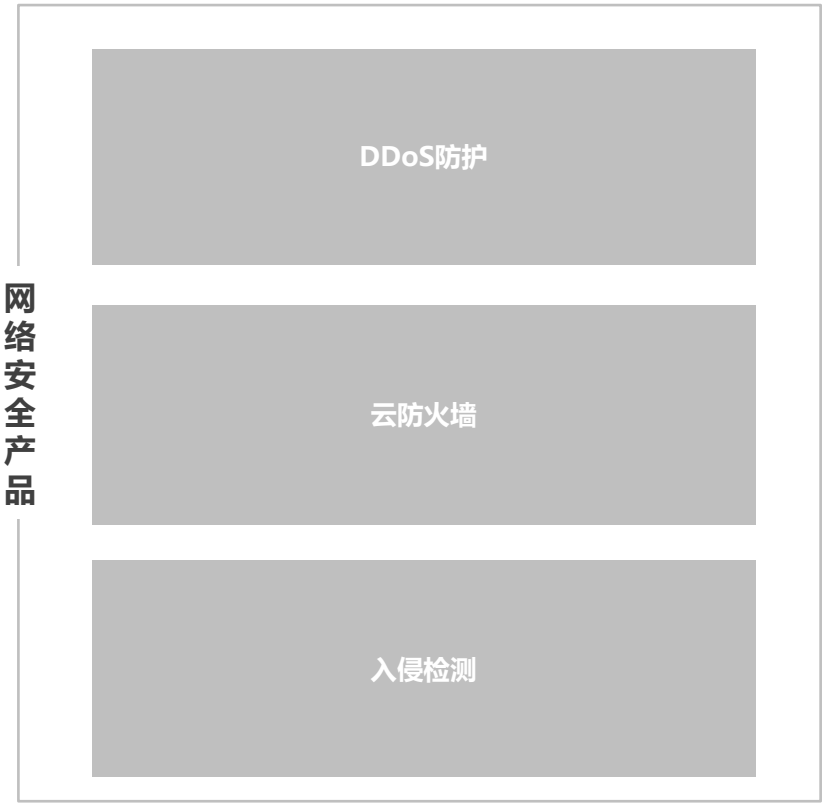
HUAWEI 华为云 | 腾讯云 | 阿里云 | 百度智能云 | 亚马逊云科技 | 京东云 | 金山云 | 天翼云

备注：图谱中综合云厂商表明该厂商针对该领域业务场景均提供广泛的产品与服务支持，其他业务板块中云厂商表明该厂商更专注于某一细分业务场景。
来源：艾瑞咨询研究院自主研究及绘制。

网络安全

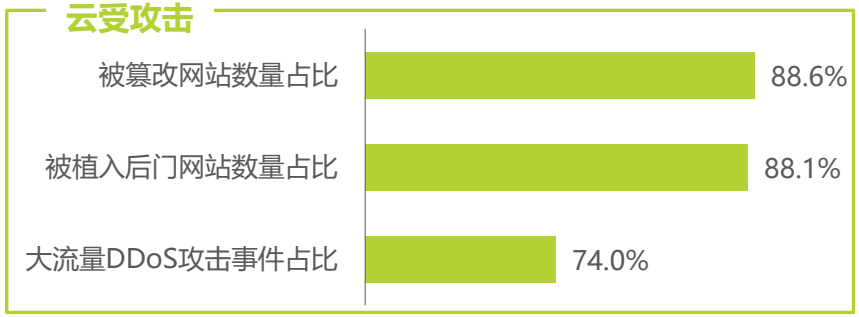
用“云化”的方式解决“云生”的网络安全威胁更行之有效

从传统网络安全时代，DDoS攻击便因为效果显著，难以抵御和追踪，成为黑客进行网络攻击的主要选择。伴随云计算的普及，一方面云平台成为新的攻击对象，另一方面云也被利用作为扩大网络攻击效果的工具。面对以云平台为媒介发起的DDoS攻击，传统抗D方式受限于资源性能，很难化解突发大流量攻击，而为抵御DDoS攻击而投入的设备和人员成本也非常高昂。因此，在云计算时代，针对“云生”的网络安全风险，企业应该选择云上的安全工具应对，才能事半功倍。

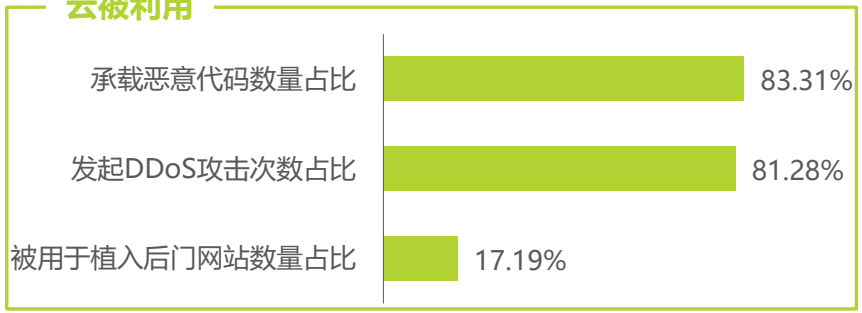


来源：艾瑞咨询研究院自主研究及绘制。

2020年中国境内云平台遭受各类网络安全事件占比



2020年中国境内云被利用发起各类网络攻击事件占比



来源：艾瑞咨询研究院自主研究及绘制。

网络安全——产业图谱

DDoS防护

安恒信息 DAS-security 网宿科技 H3C 360 政企安全 奇安信 QI-ANXIN
知道创宇 天融信 TOPSEC 安全狗 NSFOCUS 绿盟科技 云弈科技
UCLOUD优刻得 QingCloud Technologies 移动云 七牛云 白山云科技 BAISHANCLOUD
inspur 浪潮 HUAYUN 华云 联通云 Unicom Cloud 紫光云

云防火墙

Hillstone 山石网科 SANGFOR 深信服科技 Neusoft
AsiaInfo 亚信安全 天融信 TOPSEC H3C
安恒信息 DAS-security NSFOCUS 绿盟科技 奇安信 QI-ANXIN
inspur 浪潮 联通云 Unicom Cloud 中国电子云 CECLOUD
白山云科技 BAISHANCLOUD 移动云 QingCloud Technologies

网络入侵检测

SANGFOR 深信服科技 默安科技 Hillstone 山石网科
Venus 启明星辰 知道创宇 青藤云安全
安恒信息 DAS-security AsiaInfo 亚信安全 Neusoft
NSFOCUS 绿盟科技 安天 H3C
UCLOUD优刻得 QingCloud Technologies 白山云科技 BAISHANCLOUD

综合云厂商

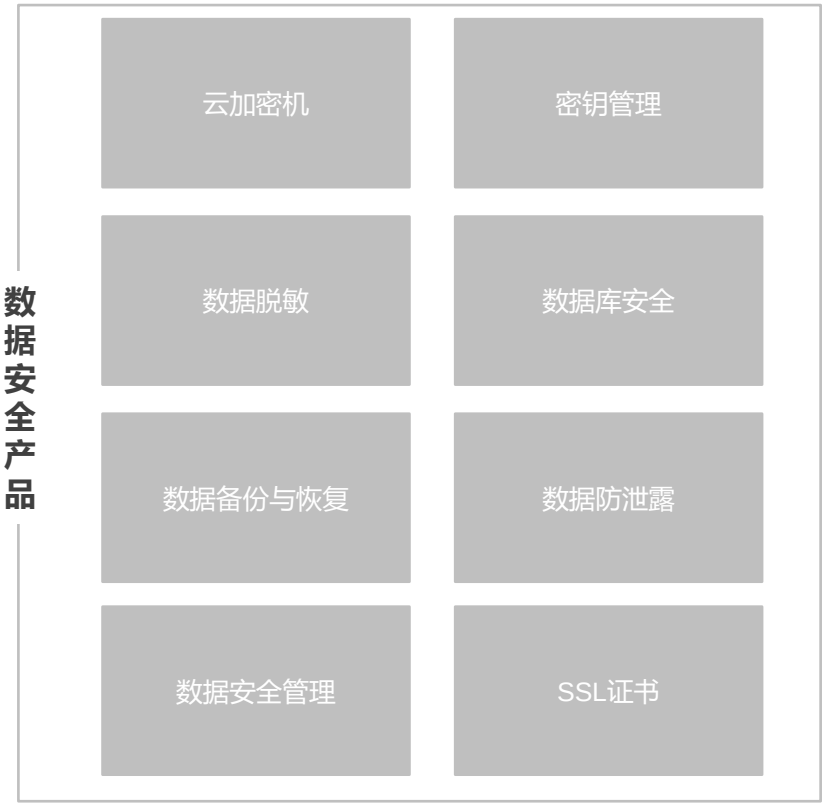
HUAWEI 华为云 腾讯云 阿里云 百度智能云 亚马逊云科技 京东云 金山云 天翼云

备注：图谱中综合云厂商表明该厂商针对该领域业务场景均提供广泛的产品与服务支持，其他业务板块中云厂商表明该厂商更专注于某一细分业务场景。
来源：艾瑞咨询研究院自主研究及绘制。

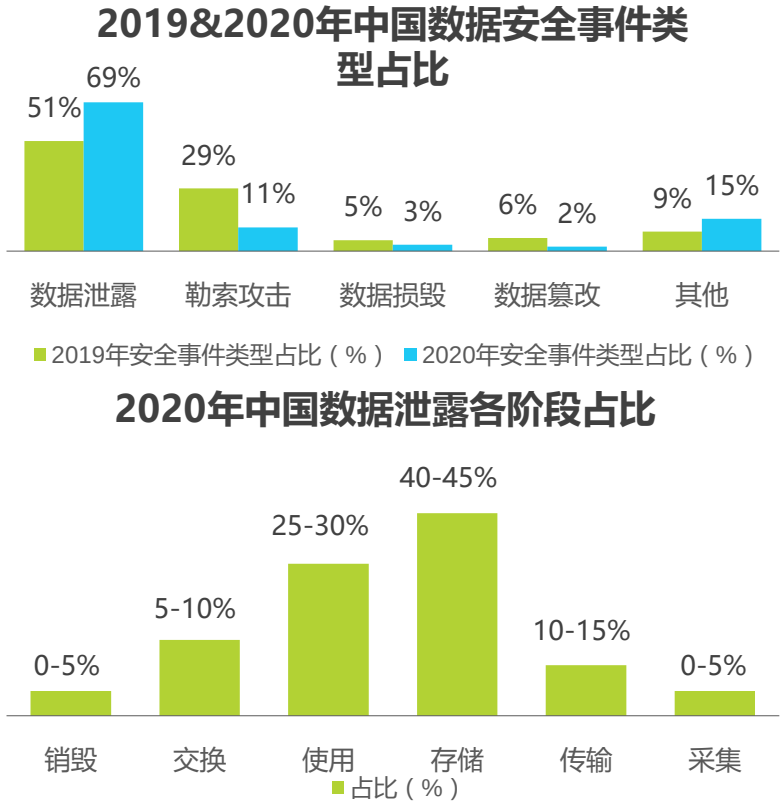
数据安全

数据风险具有普遍性，需针对数据全生命周期构筑安全防御

在产业互联网背景下，数据已经被定义为新一代生产要素。伴随着《网络安全等级保护大数据基本要求》，《中华人民共和国数据安全法》等相关法规的出台，数据安全已成为企业和个人在提供和使用信息技术产品于服务是着重考虑的要素。在数据体量庞大，种类复杂的大数据时代，单一数据安全产品很难有效解决数据安全问题，需要搭配多种数据安全工具，围绕数据生命周期各环节构建数据安全解决方案，才能有效降低数据安全风险。



来源：艾瑞咨询研究院自主研究及绘制。



来源：SECSMART，艾瑞咨询研究院自主研究及绘制。

数据安全——产业图谱

云加密机

inspur 浪潮
移动云

秘钥管理

安恒信息
QingCloud Technologies
移动云
UCLOUD优刻得

数据安全管理

SANGFOR 深信服科技
明朝万达 Wondersoft
安恒信息
奇安信 QI-ANXIN
天融信 TOPSEC
NSFOCUS 绿盟科技
AsiaInfo 亚信安全
志翔科技 ZSHIELD INC
inspur 浪潮

数据防泄漏

安恒信息
北信源 VRV
天融信 TOPSEC
明朝万达 Wondersoft
奇安信 QI-ANXIN
NSFOCUS 绿盟科技
启明星辰
观安

SSL证书/证书管理

知道创宇
Westone 卫士通
启明星辰
江南信安
通付盾 Pay Egis
QingCloud Technologies
七牛云
UCLOUD优刻得
紫光云
inspur 浪潮
HUAYUN 华云
白山云科技 BAISHANCLOUD

数据库安全

知道创宇
Hillstone 山石网科
天融信 TOPSEC
安恒信息
启明星辰
H3C
观安
NSFOCUS 绿盟科技
中国电子云 CECLOUD
inspur 浪潮
紫光云
UCLOUD优刻得
移动云

数据脱敏

天融信 TOPSEC
AsiaInfo 亚信安全
安恒信息
明朝万达 Wondersoft
奇安信 QI-ANXIN
NSFOCUS 绿盟科技
观安
北信源 VRV
inspur 浪潮
移动云

数据备份与恢复

网宿科技
天融信 TOPSEC
北信源 VRV
inspur 浪潮
联通云 Unicom Cloud
UCLOUD优刻得
移动云
HUAYUN 华云
紫光云
QingCloud Technologies

综合云厂商

华为云 HUAWEI
腾讯云
阿里云
百度智能云
亚马逊云科技
京东云
金山云
天翼云

备注：图谱中综合云厂商表明该厂商针对该领域业务场景均提供广泛的产品与服务支持，其他业务板块中云厂商表明该厂商更专注于某一细分业务场景。
来源：艾瑞咨询研究院自主研究及绘制。

应用和业务安全

结合业务场景特性，融合数智化工具，有效打击黑灰产业

业务安全主要用于解决由于企业某些业务场景中存在逻辑漏洞，导致被不法分子利用，获取利益的行为。业务安全相较于基础安全产品，与企业业务场景与业务需求耦合的更为紧密。因此，有效的业务安全产品需要以深入理解业务场景为前提。此外，相比于其他“黑客”攻击更多是技术类风险，“黑产”更多是针对资源类的威胁。因此，针对企业上云后用户资源，数据资源等更分散，需要更好的结合人工智能与大数据工具进行有效管理。

来源：艾瑞咨询研究院自主研究及绘制。

来源：艾瑞咨询研究院自主研究及绘制。

应用和业务安全——产业图谱

云WAF

启明星辰 | 安恒信息 | SANGFOR 深信服科技 | 知道创宇 | 网宿科技 | 观安 | 天融信 TOPSEC | Hillstone 山石网科 | H3C | 360 政企安全 | NSFOCUS 绿盟科技 | 长亭科技 CHAITIN | 奇安信 QI-ANXIN | Neusoft | 昂瑞 | 安全狗 | 云弈科技 | QingCloud | 联通云 | inspur 浪潮 | HUAYUN 华云 | UCLOUD优刻得 | 移动云 | 白山云科技 BAISHANCLOUD | 紫光云 | 中国电子云 CECLOUD

漏洞扫描

安天 | SANGFOR 深信服科技 | NSFOCUS 绿盟科技 | 安恒信息 | 360 政企安全 | 天融信 TOPSEC | H3C | 奇安信 QI-ANXIN | HUAYUN 华云 | 移动云 | 中国电子云 CECLOUD | 联通云 | inspur 浪潮 | 紫光云 | 白山云科技 BAISHANCLOUD

网页防篡改

网宿科技 | 安全狗 | SANGFOR 深信服科技 | H3C | NSFOCUS 绿盟科技 | 360 政企安全 | 安恒信息 | 安天 | 启明星辰 | 奇安信 QI-ANXIN | inspur 浪潮 | 移动云 | 白山云科技 BAISHANCLOUD | 紫光云

内容安全

知道创宇 | 任子行 SURFILTER | 同盾科技 www.tongdun.cn | 数美 NEXTDATA | 网易易盾 | 奇安信 QI-ANXIN | AsiaInfo 亚信安全 | 七牛云 | UCLOUD优刻得 | 白山云科技 BAISHANCLOUD

欺诈检测和识别

通付盾 Pay Egis | 数美 NEXTDATA | 知道创宇 | 网易易盾 | 同盾科技 www.tongdun.cn | 芯盾时代 TRUSFORT.COM | 奇安信 QI-ANXIN | 白山云科技 BAISHANCLOUD

综合云厂商

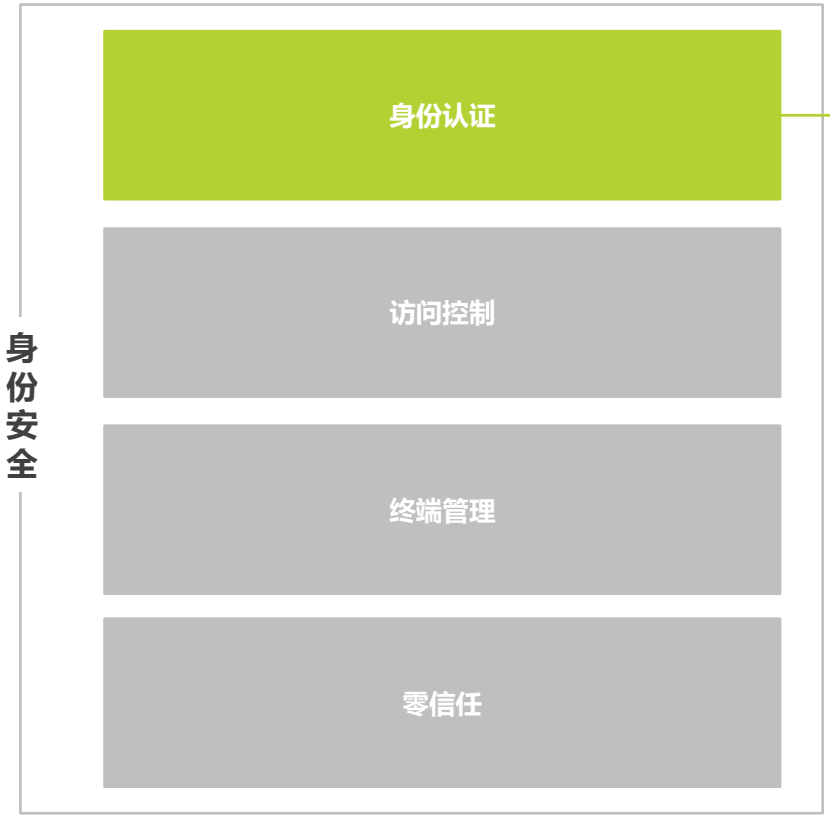
华为云 HUAWEI | 腾讯云 | 阿里云 | 百度智能云 | 亚马逊云科技 | 京东云 | 金山云 | 天翼云

备注：图谱中综合云厂商表明该厂商针对该领域业务场景均提供广泛的产品与服务支持，其他业务板块中云厂商表明该厂商更专注于某一细分业务场景。
来源：艾瑞咨询研究院自主研究及绘制。

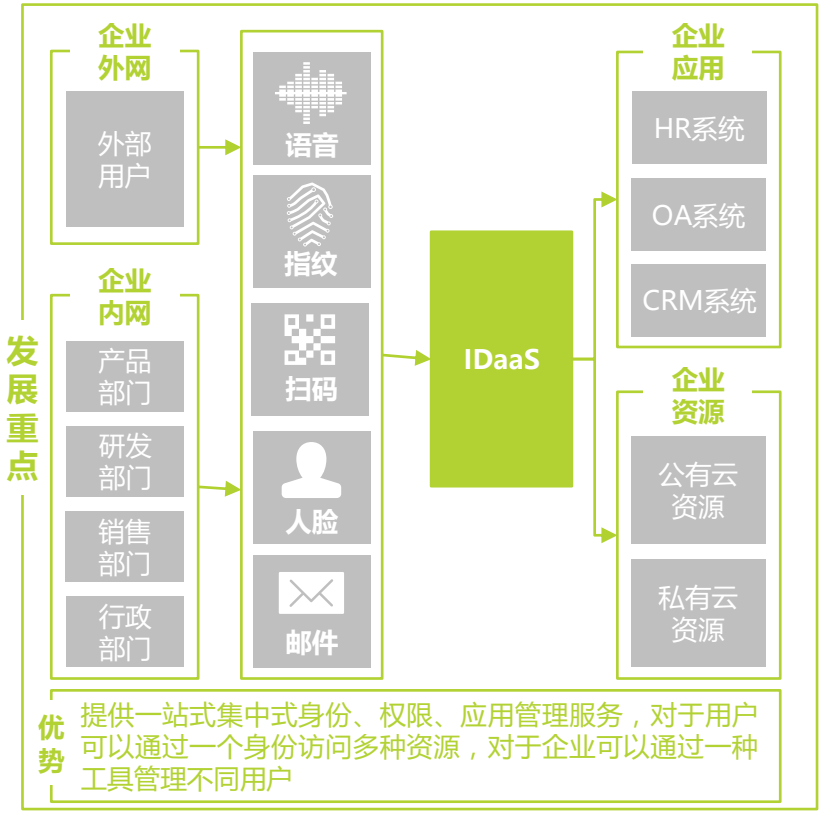
身份安全

针对用户身份生命周期各环节特征，构筑全面安全解决方案

相较于传统的本地部署，企业上云后将面对更多来自企业内部、外部不同类型的用户通过各种媒介对不同资源的访问需求。针对上述场景，IDaaS产品通过覆盖用户身份生命周期各个环节的统一身份管理，支持多种认证协议的统一认证能力，有效帮助企业统一本地及云端的身份管理及多云间的身份管理，兼顾访问效率及访问安全的平衡。



来源：艾瑞咨询研究院自主研究及绘制。



来源：艾瑞咨询研究院自主研究及绘制。

©2021.12 iResearch Inc. www.iresearch.com.cn

身份安全——产业图谱

IDaaS

SANGFOR 深信服科技
网宿科技
NSFOCUS 绿盟科技
UCLOUD优刻得
中国电子云 CECLOUD
联通云 Unicom Cloud
inspur 浪潮
HUAYUN 华云
移动云
QingCloud Technologies
紫光云

零信任

SANGFOR 深信服科技
网宿科技
Hillstone 山石网科
安恒信息 DAS-Security
天融信 TOPSEC
奇安信 QI-ANXIN
安天
NSFOCUS 绿盟科技
H3C
QingCloud Technologies
白山云科技 BAISHANCLOUD

终端安全

SANGFOR 深信服科技
安恒信息 DAS-Security
知道创宇
AsiaInfo 亚信安全
明朝万达 Wondersoft
安天
启明星辰
天融信 TOPSEC
H3C
奇安信 QI-ANXIN
北信源 VRV
NSFOCUS 绿盟科技

综合云厂商

HUAWEI 华为云
腾讯云
阿里云
百度智能云
亚马逊云科技
京东云
金山云
天翼云

备注：图谱中综合云厂商表明该厂商针对该领域业务场景均提供广泛的产品与服务支持，其他业务板块中云厂商表明该厂商更专注于某一细分业务场景。
来源：艾瑞咨询研究院自主研究及绘制。

安全服务与运营

传统行业云上安全管理运维经验缺失驱动云托管服务发展

传统行业虽然受数字化转型驱动，上云、用云热情高涨，但受制于有限的IT运维成本和IT运维团队规模，其网络安全运营管理能力较难匹配云计算安全运营需求。尤其是对价格敏感的中小企业，为兼顾业务需求和用云成本，必须更谨慎地分配预算。而云安全托管平台的出现，有效地帮助中小企业解决上述困境。由云厂商或传统安全厂商提供的安全托管服务，有效帮助中小企业减轻了用云成本负担，并保障业务在云上的安全可靠。

来源：艾瑞咨询研究院自主研究及绘制。

来源：艾瑞咨询研究院自主研究及绘制。

安全管理和运营——产业图谱

iResearch 艾瑞咨询

态势感知

SANGFOR 深信服科技 | 网宿科技 | Westone 卫士通 | Hillstone 山石网科 | ultrapower 神州泰岳

知道创宇 | NSFOCUS 绿盟科技 | 奇安信 QI-ANXIN | 安全狗 | 安恒信息 DAS-security

天融信 TOPSEC | H3C | 观安 | 安天 | 360 政企安全

inspur 浪潮 | QingCloud Technologies | 白山云科技 BAISHANCLOUD | 联通云 Unicom Cloud | 移动云 | HUAYUN 华云

安全运营中心

SANGFOR 深信服科技 | 知道创宇 | AsiaInfo 亚信安全 | 安天

启明星辰 | 安恒信息 DAS-security | 默安科技 企业信赖的安全伙伴 | NSFOCUS 绿盟科技

天融信 TOPSEC | 奇安信 QI-ANXIN | 360 政企安全 | H3C

inspur 浪潮 | UCLOUD 优刻得 | 白山云科技 BAISHANCLOUD | 联通云 Unicom Cloud | 移动云

威胁情报

Hillstone 山石网科 | 安恒信息 DAS-security

NSFOCUS 绿盟科技 | 安全狗

H3C | 安天

启明星辰 | ThreatBook 微步在线

综合云厂商

HUAWEI 华为云 | 腾讯云 | 阿里云 | 百度智能云 | 亚马逊云科技 | 京东云 | 金山云 | 天翼云

备注：图谱中综合云厂商表明该厂商针对该领域业务场景均提供广泛的产品与服务支持，其他业务板块中云厂商表明该厂商更专注于某一细分业务场景。

来源：艾瑞咨询研究院自主研究及绘制。

安全服务——产业图谱

备注：图谱中综合云厂商表明该厂商针对该领域业务场景均提供广泛的产品与服务支持，其他业务板块中云厂商表明该厂商更专注于某一细分业务场景。
来源：艾瑞咨询研究院自主研究及绘制。

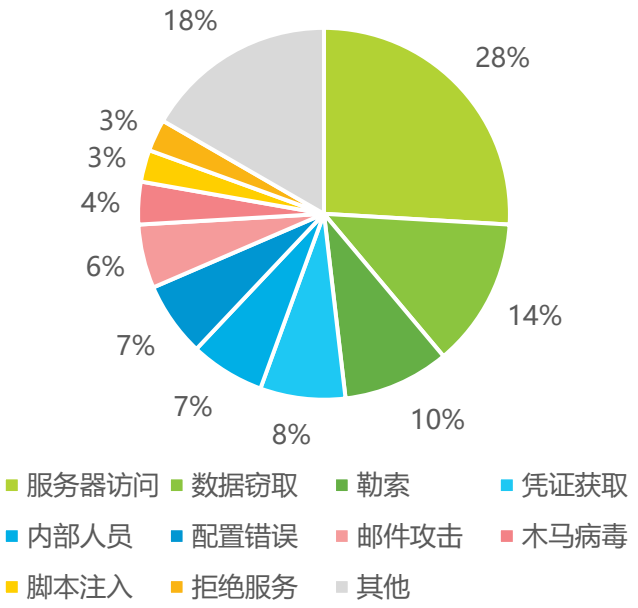
中国云安全行业洞察——应用实践

金融——安全现状

安全威胁类型多样，数据安全是建设及投入重点

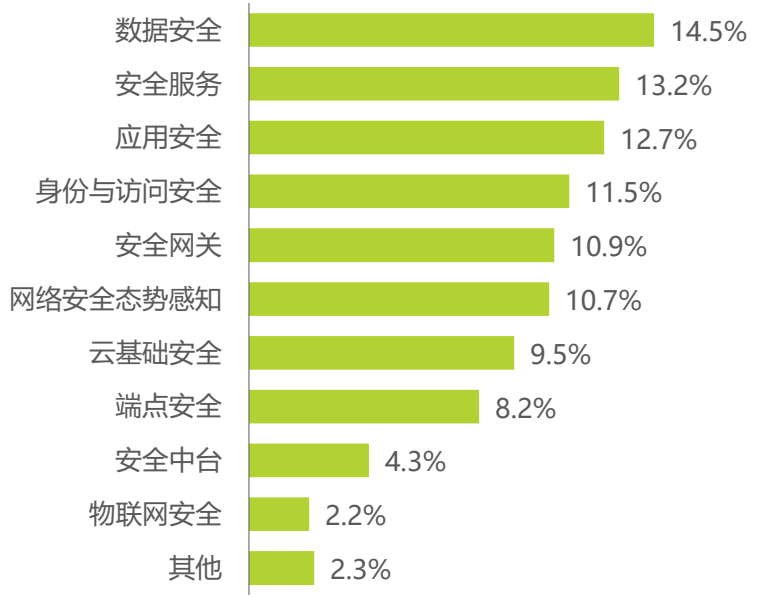
金融行业伴随数字化转型加速，金融科技与金融创新能力加强，金融企业云化程度显著提升。伴随业务上云后，随之而来的是风险暴露面积增多，安全威胁呈现多样化趋势。敏捷开发工具的应用带来产品的快速迭代，为金融企业安全运维管理带来压力。此外，多样化的业务场景下多终端设备间数据的传输和流通也带来更多潜在数据安全风险。近年来，个人身份信息泄露事件在金融行业时有发生，暴露出金融企业数据安全管理能力仍需加强。

2020年全球金融行业主要安全威胁类型占比



来源：IBM X Force，艾瑞咨询研究院自主研究及绘制。

中国主要金融企业未来三年网络安全领域主要投资领域



来源：《金融行业网络安全白皮书》（2020年），艾瑞咨询研究院自主研究及绘制。

金融——安全特征及需求

严格遵循监管要求，以数据安全为核心，完善安全管理体系

金融行业作为数字经济的重要构成，国家推出相关政策强化金融行业监管，引导金融行业信息化建设。而在金融行业信息安全建设中，首先需要关注数据安全问题，内部加强监管，外部强化认证，并引入数智化工具进一步强化数据风险检测效率。此外，为更好地发挥安全工具的效果，在企业组织架构上，安全管理制度上均需要形成配套措施，通过健全的安全管理体系，构建专业的安全管理团队，实现高效的安全管理运营。

金融领域主要安全特征

兼管要求逐渐规范

随着网络安全等级保护2.0相关标准的实施，中国人民银行发布《金融行业网络安全等级保护实施指引》，为金融行业网络安全建设提供更清晰的方法指引。并配合数据安全、网上银行，个人信息保护等相关政策，共同规范金融行业安全建设

组织体系日益完善

金融企业内部合规部门、风控部门，安全管理部门等均逐步成为企业独立部门，且与信息技术部门合作日渐紧密，共建权责分明，管理完善的安全体系。并配套各项管理技术标准，确保从总体战略到流程到执行的安全合规。

安全场景日益多样

金融科技发展及金融云渗透，加速金融创新，线上金融业务场景显著提升。因此，金融行业安全威胁包括传统威胁及云端威胁，总体趋势呈现多样化、复杂化趋势，管理难度提升

安全投入仍需加强

金融行业网络安全投入，相较于金融科技及金融云的投入，仍处在较低水平。引入的安全技术及安全产品仍以终端安全，适配多云环境的云安全管理平台为主，在身份安全，态势感知、安全运维等领域投入稍显滞后

来源：艾瑞咨询研究院自主研究及绘制。

金融领域主要安全需求

数据安全	1）强化安全内容，减少内部人员对用户个人信息、征信信息的泄露。 2）强化大数据工具，有效协调管理用户基础数据，交易、产品数据，经营数据等各类信息
组织升级	1）从上至下建立健全安全防范体制，明确安全责任，深化安全意识。 2）在云安全体系建设中，适当改变组织形态，引入“零信任”DevOps等理念。
人才培养	1）加强金融服务人员安全能力培训。 2）拓展安全人员岗位储备机制，拓宽安全人员招募渠道，提高安全人员薪资待遇。
安全运营	1）强化安全运维、安全运营管理可视化能力，建立安全评估量化标准。 2）强化安全对外包服务机构管理，明确安全权责界限。

来源：艾瑞咨询研究院自主研究及绘制。

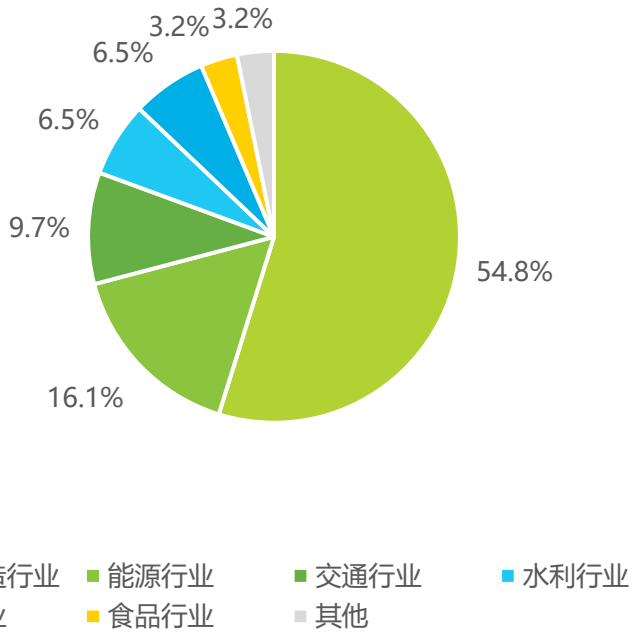
©2021.12 iResearch Inc. www.iresearch.com.cn

工业——安全现状

工业领域安全风险类型复杂，影响行业广泛

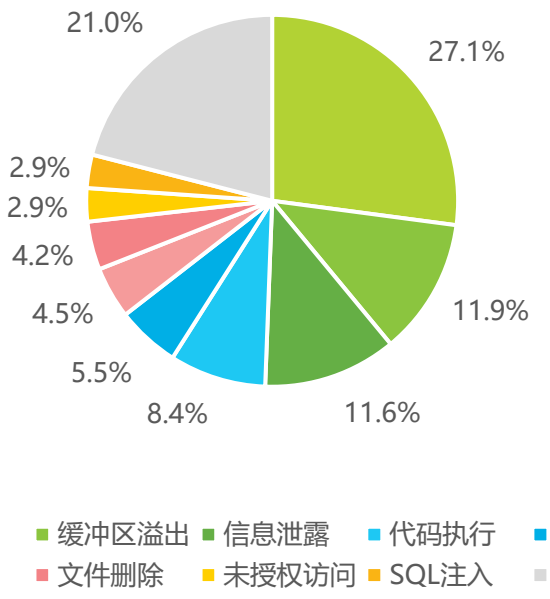
工业行业本身具有覆盖企业多、业务场景杂、信息化基础设施弱的特点。伴随产业数字化的驱动，工业企业开始陆续引入工业云平台，建立工业物联网等方式，尝试进行数字化转型。其中，在数字化转型进程中启动较早，数字化工具引入较多的行业，相应的安全风险敞口也较为明显，如智能制造行业，能源行业，交通行业。此外，工业领域中业务场景广泛，企业安全技术水平层次不齐，导致攻击方式及安全威胁类型也多样，因此，工业企业更需要建设可定制化的专属解决方案。

2020年中国工业控制安全事件涉及行业占比



来源：CNCERT，新华三技术有限公司，艾瑞咨询研究院自主研究及绘制。

2020年中国工业控制系统漏洞类型占比

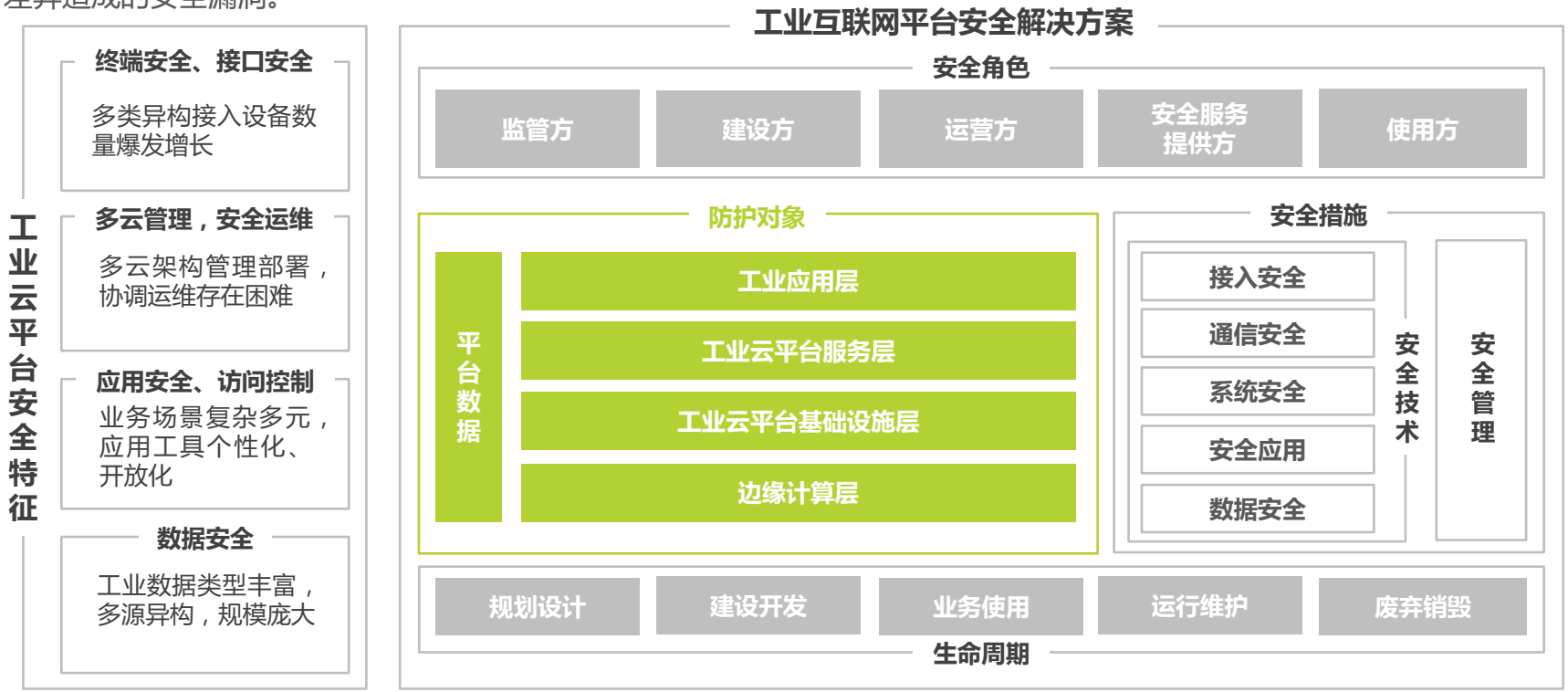


来源：CNCERT，新华三技术有限公司，艾瑞咨询研究院自主研究及绘制

工业——安全特征及解决方案

明确主次，协同厂商，共建安全解决方案及安全生态

工业领域覆盖行业及企业非常丰富，从行业整体角度看，在构建解决方案过程中，首先应该明确主次。1）安全风险的主次，集中精力优先解决根本性质的安全问题。2）建设路径的主次，根据企业信息技术安全现状，优先升级薄弱环节。其次要协同厂商，工业产业链中厂商类型丰富，需要明确不同厂商所扮演的角色，所提供的服务边界，并协同各个厂商共同构建较为适用的安全行业标准，多方共建形成稳固安全生态，以此来屏蔽厂商因为技术能力参差不齐，安全产品标准要求差异造成的安全漏洞。



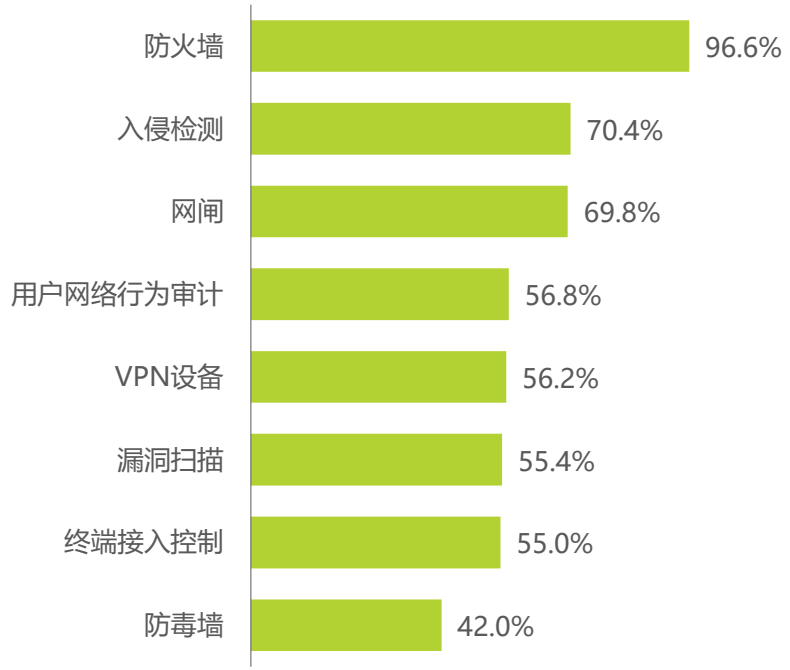
来源：国家工业信息安全发展研究中心，工业信息安全产业发展联盟，艾瑞咨询研究院自主研究及绘制。

医疗——安全现状

网络安全防护设备较为单一，数据保护措施需要提升

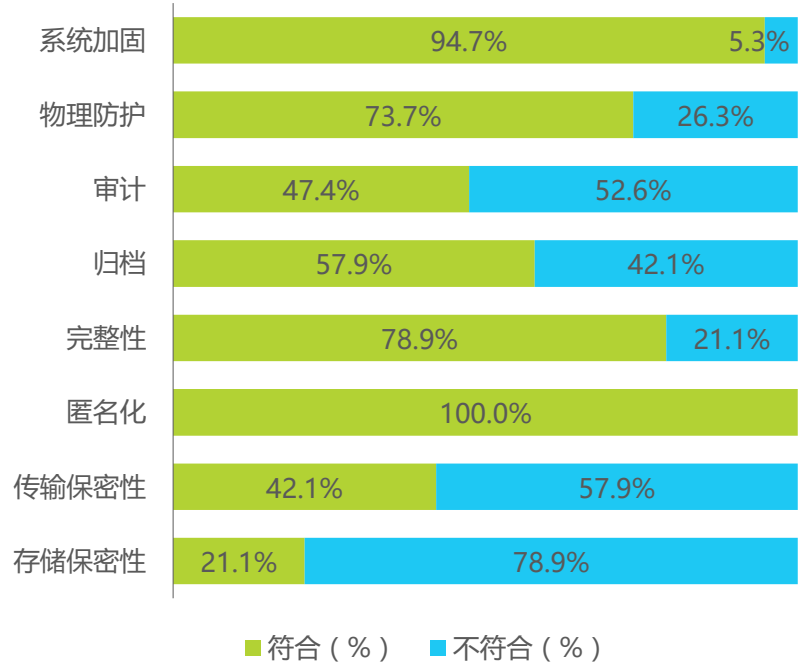
我国医疗行业数字化进程开始提速，部分医院已经开始陆续上云，并引入数智化工具。目前，我国医疗行业信息化焦点，主要集中在升级医疗信息化系统，如医院信息管理系统，电子病例系统等。但由于医疗行业本身信息技术基础设施薄弱，导致安全系统升级相较于业务系统升级存在滞后性。在安全产品领域，我国医院网络安全防护措施主要集中在网关类安全设备及主机安全类设备，针对数据安全管控不足。在安全管理领域，医疗系统整体安全管理理念以及安全管理部门建设有待进步。

2020年中国医院网络安全防护措施



来源：中国医院协会信息专业委员会，艾瑞咨询研究院自主研究及绘制。

2020年中国医疗器械安全测评结果

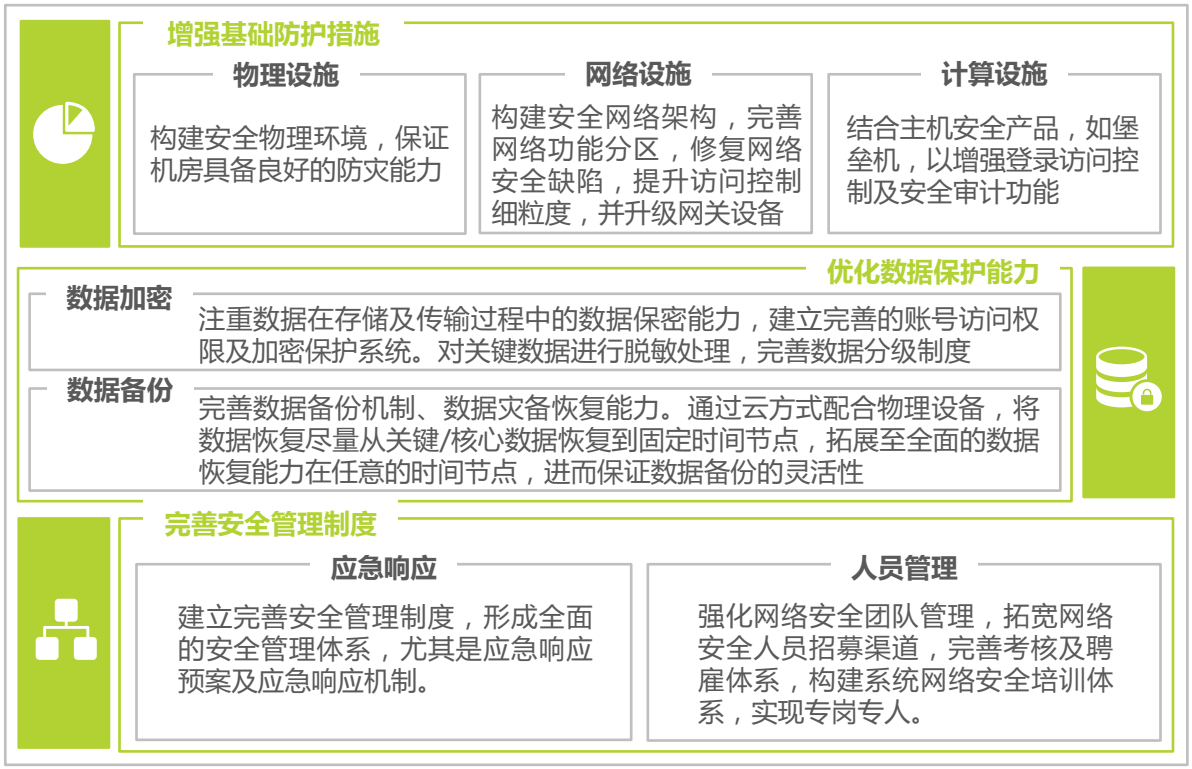


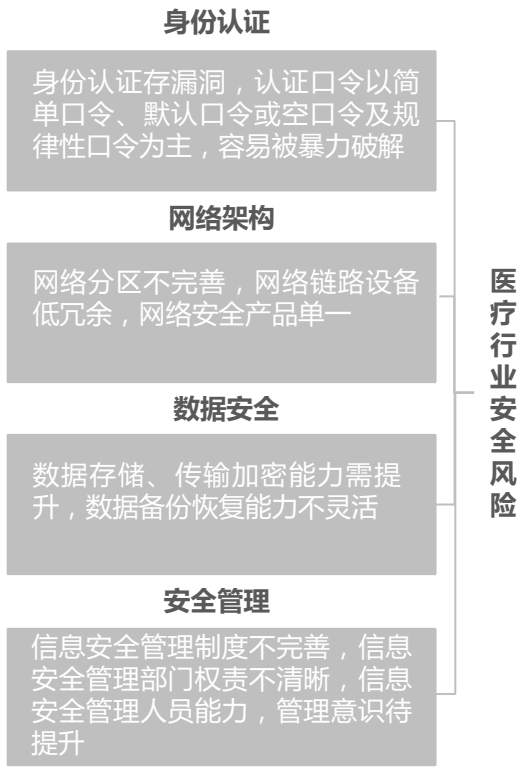
来源：中国医院协会信息专业委员会，艾瑞咨询研究院自主研究及绘制。

医疗——安全风险及解决方案

强化基础设施安全，从下至上构建系统安全防护体系

医疗行业安全解决方案建设需要强调系统化，以强化基础设施安全能力为主，稳步向上形成系统的安全防护体系。在基础层面，需要保证物理设施安全和基础IT资源安全，搭建安全的物理环境并指定稳妥的灾备方案。在基础IT资源安全构件中更需注重均衡，在升级网关设备同时，兼顾计算设施。在顶层应用方面优化访问控制及身份管理，可采用IDaaS等方式更好地实现统一身份管理。最后，在引入安全工具的同时，完善安全管理制度，通过专业的安全部门统一负责管理安全运营，如没办法很好的平衡成本，也可在合规的前提下，利用云安全托管服务。





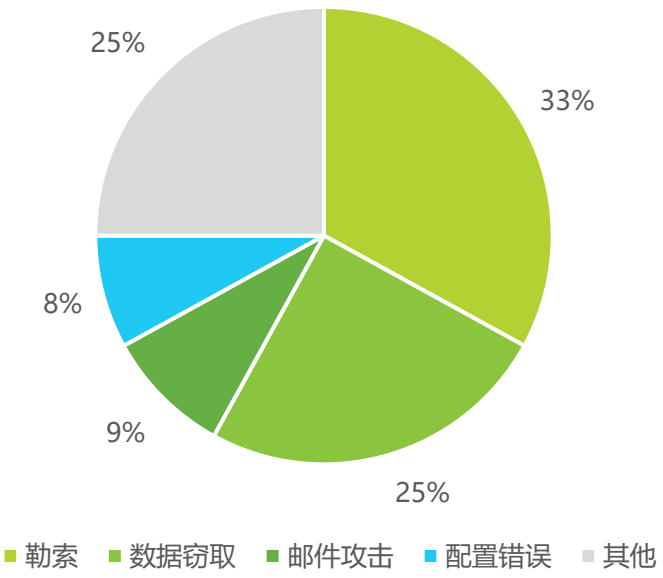
来源：艾瑞咨询研究院自主研究及绘制。

政务——安全现状

安全威胁类型较为集中，安全威胁管理控制效果稳定

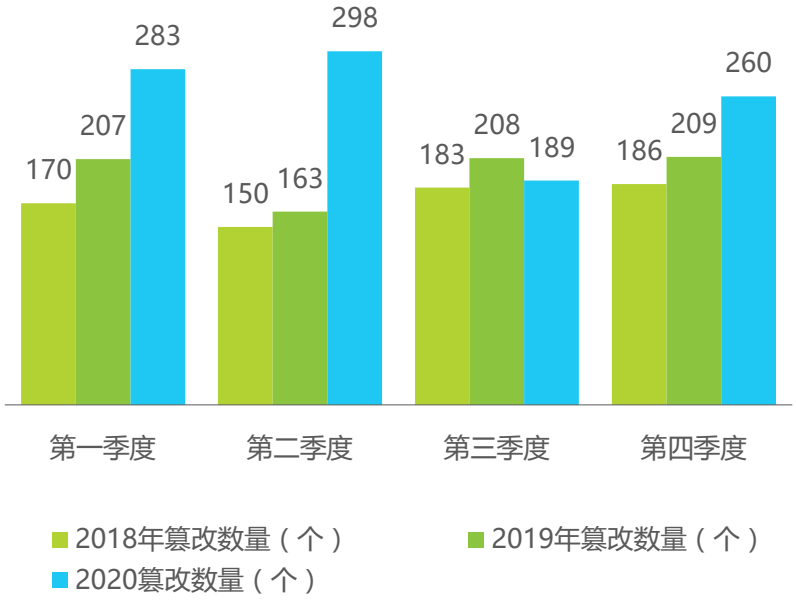
政务行业云平台在建设中围绕自主可控、提升安全能力为重点，并陆续引入PaaS能力，提升平台服务能力。政务领域的安全威胁类型较为集中，主要以勒索与数据窃取为主。虽然政务上云后导致安全威胁数量提升，如网站篡改数量有上升趋势。但从比重看，占据国内被篡改网站整体的数量不足1%，整体安全管控效果较为稳定。政务上云与政务发展相较于其他行业更显得稳中求进，仍以奠定坚实基础为“主旋律”。

2020年全球政务领域主要安全威胁类型占比



来源：IBM X Force，艾瑞咨询研究院自主研究及绘制。

2018-2020年中国境内被篡改政府网站数量

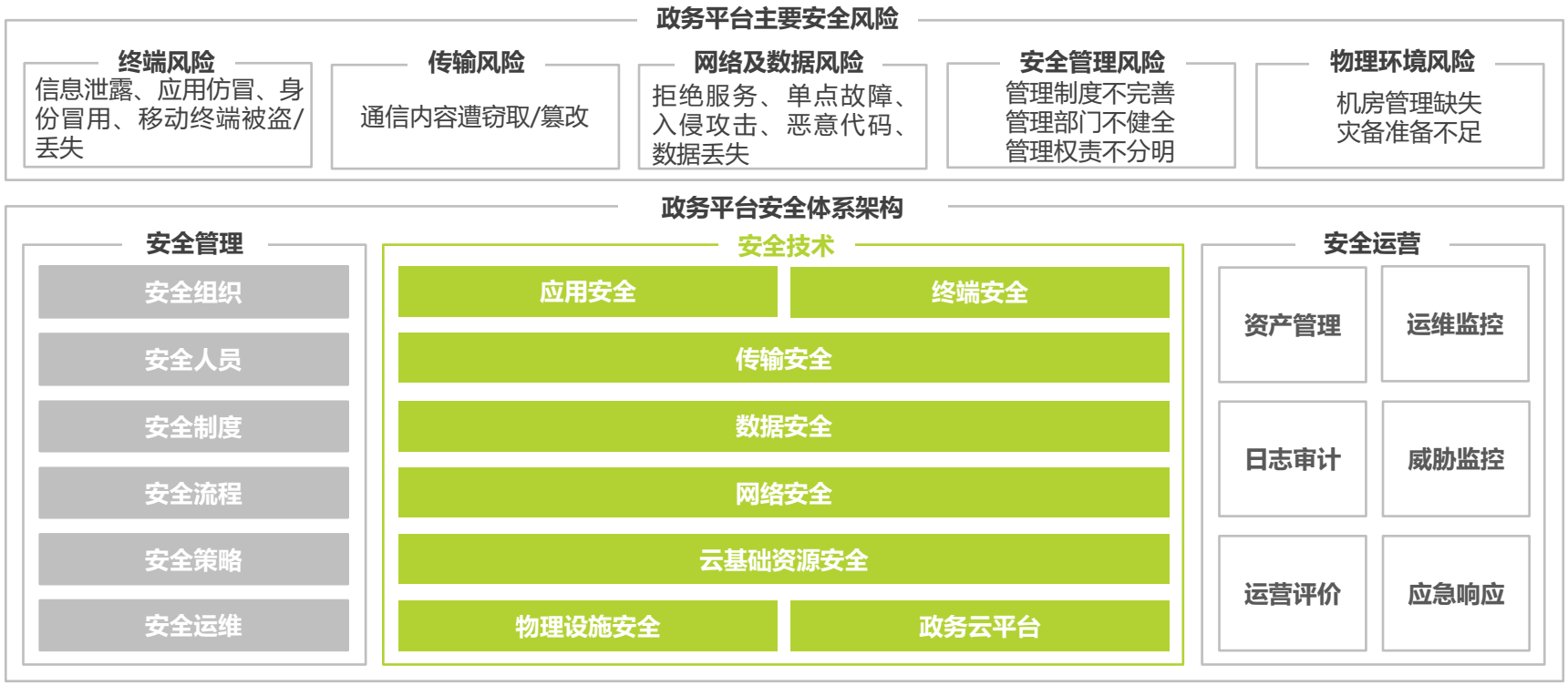


来源：国家互联网应急中心《互联网安全报告（月度）》，艾瑞咨询研究院自主研究及绘制。

政务——安全风险及解决方案

构建完善安全管理体系，有效协同管理、运营与技术

在政务平台建设中，由于提供的服务内容并不复杂，产品功能和服务场景相对有限。因此，政务平台安全技术架构整体比较完善。但技术能力仍集中在维护云基础资源安全为主，在后期升级过程中需要更好地引入PaaS层能力，从而进一步提升平台安全保障能力。在政务平台管理中，重点在于完善相关制度和体系，成立专业的管理部门，制定完善的管理制度，清晰权责。咱安全运营领域，由于运维成本较高，可采用部分安全托管，核心安全资产自管的混合方式更好地实现专业化的安全运营。



来源：艾瑞咨询研究院自主研究及绘制。

百度智能云 | 云安全

以AI为核心构建安全生态系统，赋能全业务场景

百度安全是以AI为核心、大数据为基础打造的安全品牌，是百度21年安全实践的总结与提炼。目前，百度安全拥有TB级防护能力、超亿级别手机号黑库。依托20余年的黑产对抗经验，百度安全每年拦截恶意网页与用户搜索风险超千亿次，在国内国际上参与制定标准90+项、体系认证70+项、获得荣誉25+项。百度云安全是百度安全的五大安全领域之一，其结合AI领域的技术优势与云计算领域的长期服务经验，逐步建立了完善、全面的多类安全产品矩阵以及适应多种业务需求的安全解决方案，形成安全可靠的云基座，有效保护政企资产安全。

百度云安全产品架构

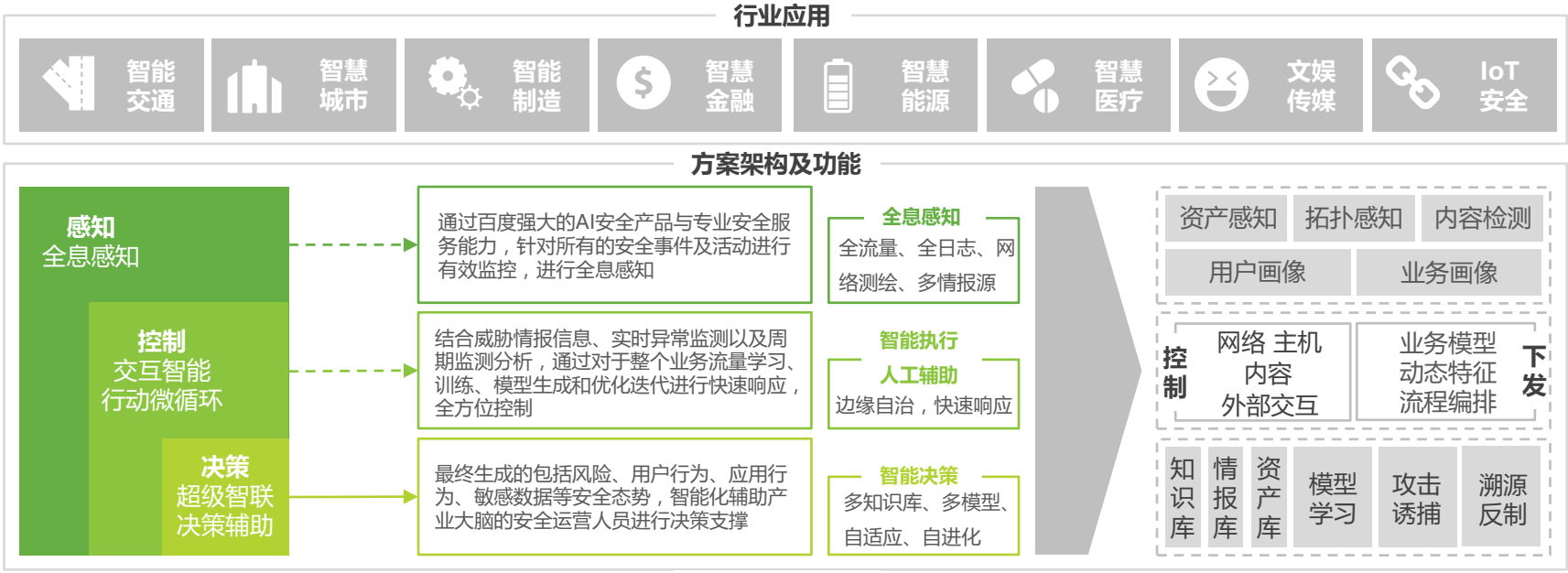
来源：艾瑞咨询研究院自主研究及绘制。

百度智能云 | 云安全

AI赋能产业安全大脑，集运行、决策、管理、指挥于一体

百度云安全通过AI赋能，重点打造了百度安全大脑解决方案，是集安全管理、运营、决策的中枢。基于大数据和机器学习的纵深防御体系，百度安全大脑显著提高安全在数据层、感知层和执行层的效率。在实践方面，百度安全与北京市海淀区携手打造的“海淀城市大脑”荣获 “2020年智慧城市十大样板工程”。此外，百度安全大脑已在桐乡产业大脑、宇信科技智慧金融、上海市爱护健康智慧养老等多个行业落地应用。

百度安全大脑解决方案



来源：艾瑞咨询研究院自主研究及绘制。

华为云

产品丰富，服务专业，生态繁荣，共建安全可信云服务

华为云提供满足一般客户需求的通用安全解决方案，以及满足客户特殊业务场景的专业解决方案。华为云通用安全解决方案，以数据安全为核心构建全栈防御，提供丰富的安全产品选择及配套安全服务。华为恪守“上不做应用，下不碰数据”的业务边界，不以数据变现为盈利方式，帮助客户保护数据安全，与客户共生共荣。同时，其提供的安全产品支持根据客户安全痛点定制专属解决方案，并提供专业安全服务及完善的安全生态体系，以责任共担模式为客户打造安全可信云服务。

华为云安全产品及优势

多项自主研发云安全服务以及多类合作开发安全服务 **技术突出**	累计获得多项全球安全合规认证，安全能力或行业认可 **合规保障**	参与指导和制定多项云安全行业标准，输出多份安全报告 **产业共享**	专业安全团队，7X24小时专业服务，，安全事件高度自动响应 **能力可靠**

安全产品矩阵

应用安全	工作负载安全	数据资产安全	安全态势服务
DDoS高防	企业主机安全	数据库安全服务	漏洞扫描服务
云防火墙	容器安全服务	数据加密服务	态势感知
Anti-DDoS流量清洗	云堡垒机	数据安全中心	管理检测与响应
Web应用防火墙		SSL证书管理	威胁检测服务
应用新人中心		云证书管理服务	
		安全治理云图	

来源：艾瑞咨询研究院自主研究及绘制。

华为云

立足安全实践，构建纵深安全服务体系，匹配用户业务需求

华为云致力于提供稳定可靠、安全可信、可持续创新的云服务，赋能应用、使能数据、做智能世界的“黑土地”。在安全领域，华为云把可信作为第一优先级，放在功能、特性和进度之上。华为云作为数字化转型践行者，通过总结其服务的大中小不同类型企业的业务实践，积累不同企业在安全领域的共性需要和特殊诉求，并基于华为在安全、隐私、合规领域多年的技术和治理能力，为用户建立完善的安全解决方案建设策略，为客户提供安全、可靠、可信赖的基础设施和服务。

华为云安全解决方案及建设策略

华为云上云安全建设理念

身份认证与管理	基础设施保护	数据保护	威胁检测	安全响应与恢复	合规与隐私保护
华为云OneAccess服务提供应用身份挂你了服务，具备集中式的身份管理、认证和授权能力。	根据用户创建的规则对web业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御位置威胁	将数据分级分类，具备数据安全风险识别，数据水印溯源，数据脱敏等安全能力。对数据全生命周期各阶段进行安全防护。	持续发现恶意活动和未经授权的行为，从而保护账户、工作负载。通过集成AI智能引擎等检测模型，识别潜在威胁并输出结果。	提供华为安全标准的运维运营服务，帮助企业与机构对安全事件进行有效监控，并采取必要措施。	基于最佳实践和行业标准，帮助企业全面了解安全合规状况，并使用自动合规性极限检查，呈现出全局安全态势。

安全解决方案

数据安全解决方案	等保合规安全解决方案	网站安全解决方案	移动应用安全与隐私合规	云主机防暴力破解安全方案	通用安全解决方案

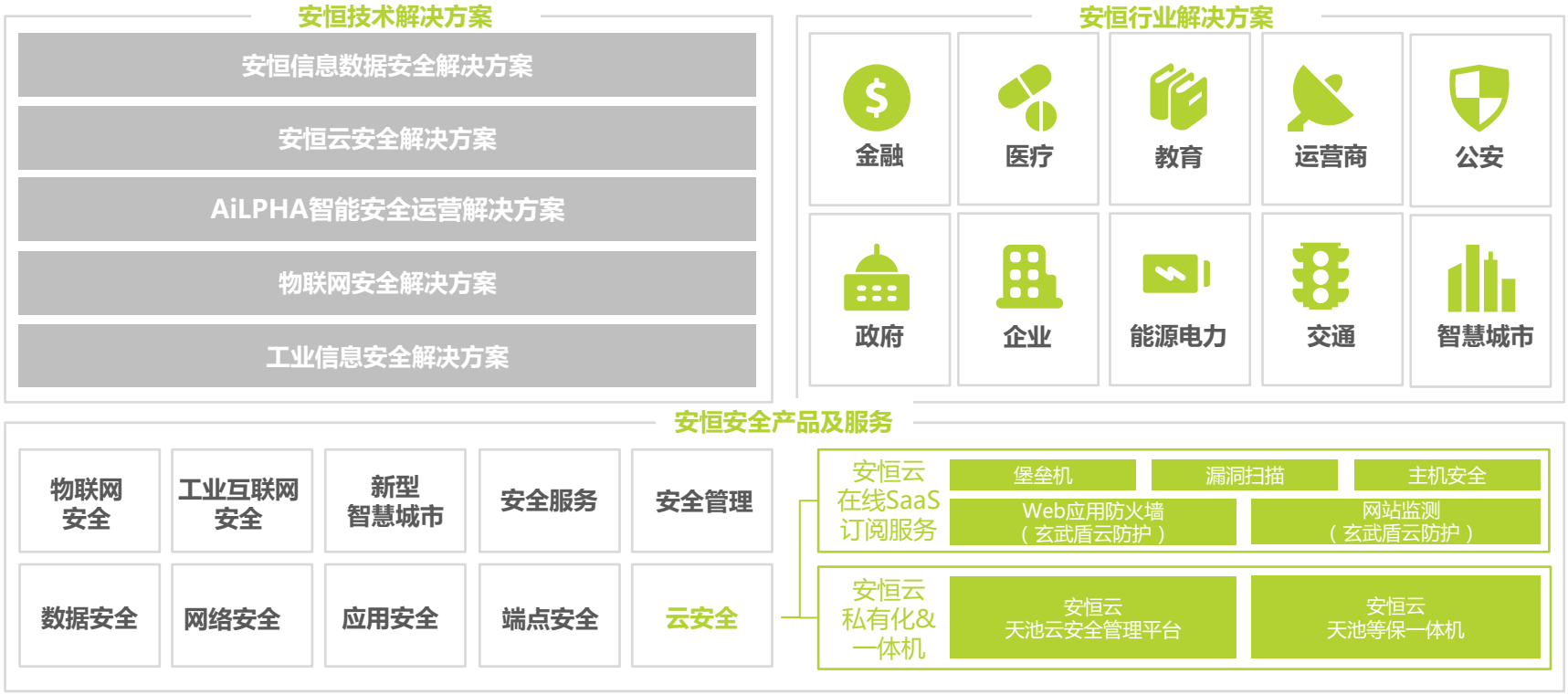
来源：艾瑞咨询研究院自主研究及绘制。

安恒信息 | 安恒云

覆盖网络信息安全全生命周期，向云上解决方案迈进

安恒信息自成立以来一直专注于网络信息安全领域，公司秉承“助力安全中国，助推数字经济”的企业使命，以“数字经济的安全基石”为企业定位。安恒信息以云安全、大数据安全、物联网安全、智慧城市安全、工业控制系统安全及工业互联网安全五大方向为市场战略，构建覆盖网络信息安全生命全周期的安全产品，专业的技术解决方案及多样的行业解决方案。

安恒信息产品及解决方案



来源：艾瑞咨询研究院自主研究及绘制。

安恒信息 | 安恒云

契合多云管理现状，构建完整全面的多云安全管理平台

伴随云计算的发展，安恒信息与时俱进推出集多云管理和多云安全于一体的一站式平台级产品：安恒云，致力于为用户打造一个安全、平等的多云管理和多云安全管理平台。通过结合安恒信息在网络信息安全领域的经验和对云用户安全需求的洞察，安恒云安全解决方案，借鉴传统安全产品的优势及特征，并着重弥补传统安全无法覆盖的，云环境下新的安全需求。同时，为云上安全组件提供统一管理工具，明确责任主体，优化用户用云体验，构建完善安全体系。

安恒云安全解决方案

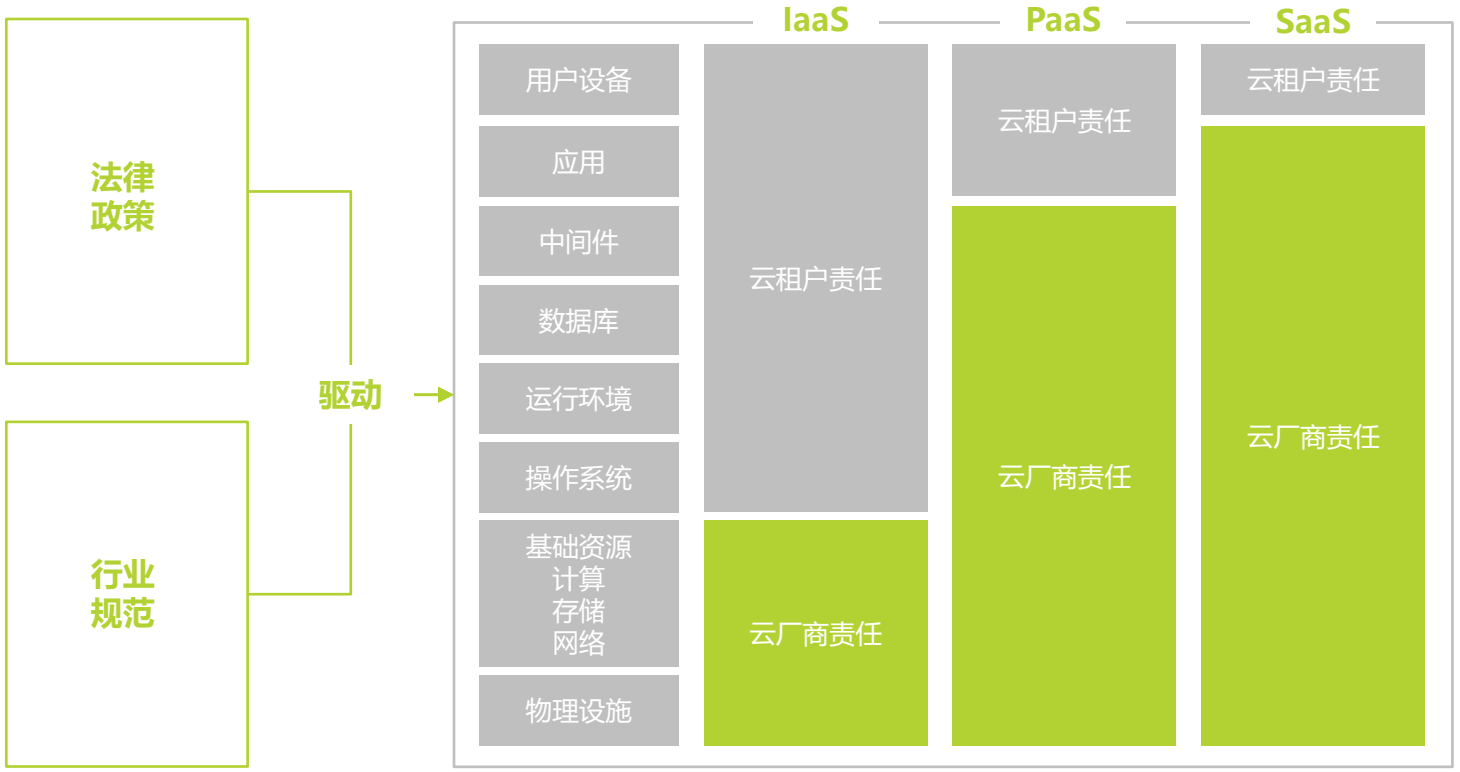
来源：艾瑞咨询研究院自主研究及绘制。

中国云安全发展趋势（1/2）

法律全面，规范健全，权责清晰，助力构建安全可靠云服务

虽然责任共担模型并不是新概念，但在中国云服务市场的落地效果并不理想。伴随企业上云走向“精耕细作”，法律政策与行业规范日渐完善，责任共担模型将更好地指导云厂商在推动“云+产业”结合的进程中，明确其安全责任。同时，清晰的权责划分在云服务边界日渐模糊的发展趋势下，让云用户关心的数据资产，IT资产等所有权问题可以得到更好地保障，进而提升云用户对云服务，尤其是公有云的可靠性、可信性的理解。

云安全责任共担模型



来源：艾瑞咨询研究院自主研究及绘制。

中国云安全发展趋势（2/2）

传统行业上云加速，围绕云安全产品升级驱动云安全服务发展

产业互联网建设要求云厂商在业务布局中更多考虑将技术能力与业务场景结合，云安全产品的发展也将遵循产业互联网发展趋势，配合云服务行业解决方案，将通用云安全能力转为专业云安全能力。同时，根据行业易受安全威胁情况分析，云安全需求将更多集中在金融，制造等传统领域。此外，传统行业不仅安全产品面临升级，安全理念与安全组织架构也需要更新，由此带动云安全咨询、云安全托管等衍生需求。为此，云安全产品在能力上将走向专业化，内容上将走向生态化。

2018-2020年全球易受网络安全威胁行业排名

	2020	2019	2018
金融	1	1	1
制造	2	8	5
能源	3	9	10
零售	4	2	4
专业服务	5	5	3
政务	6	6	7
医疗	7	10	8
传媒	8	4	6
交通	9	3	2
教育	10	7	9

来源：IBM X Force，艾瑞咨询研究院自主研究及绘制。

艾瑞新经济产业研究解决方案

iResearch 艾瑞咨询

行业咨询

市场进入	为企业提供市场进入机会扫描，可行性分析及路径规划
竞争策略	为企业提供竞争策略制定，帮助企业构建长期竞争壁垒

投资研究

IPO行业顾问	为企业提供上市招股书编撰及相关工作流程中的行业顾问服务
募投	为企业提供融资、上市中的募投报告撰写及咨询服务
商业尽职调查	为投资机构提供拟投标的所在行业的基本面研究、标的项目的机会收益风险等方面的深度调查
投后战略咨询	为投资机构提供投后项目的跟踪评估，包括盈利能力、风险情况、行业竞对表现、未来战略等方向。协助投资机构为投后项目公司的长期经营增长提供咨询服务

关于艾瑞

艾瑞咨询是中国新经济与产业数字化洞察研究咨询服务领域的领导品牌，为客户提供专业的行业分析、数据洞察、市场研究、战略咨询及数字化解决方案，助力客户提升认知水平、盈利能力和综合竞争力。

自2002年成立至今，累计发布超过3000份行业研究报告，在互联网、新经济领域的研究覆盖能力处于行业领先水平。

如今，艾瑞咨询一直致力于通过科技与数据手段，并结合外部数据、客户反馈数据、内部运营数据等全域数据的收集与分析，提升客户的商业决策效率。并通过系统的数字产业、产业数据化研究及全面的供应商选择，帮助客户制定数字化战略以及落地数字化解决方案，提升客户运营效率。

未来，艾瑞咨询将持续深耕商业决策服务领域，致力于成为解决商业决策问题的顶级服务机构。

联系我们 Contact Us

400 - 026 - 2099

ask@iresearch.com.cn

企 业 微 信

微 信 公 众 号

法律声明

版权声明

免责条款

本报告中行业数据及相关市场预测主要为公司研究员采用桌面研究、行业访谈、市场调查及其他研究方法，部分文字和数据采集于公开信息，并且结合艾瑞监测产品数据，通过艾瑞统计预测模型估算获得；企业数据主要为访谈获得，艾瑞咨询对该等信息的准确性、完整性或可靠性作尽最大努力的追求，但不作任何保证。在任何情况下，本报告中的信息或所表述的观点均不构成任何建议。

本报告中发布的调研数据采用样本调研方法，其数据结果受到样本的影响。由于调研方法及样本的限制，调查资料收集范围的限制，该数据仅代表调研时间和人群的基本状况，仅服务于当前的调研目的，为市场和客户提供基本参考。受研究方法和数据获取资源的限制，本报告只提供给用户作为市场参考资料，本公司对该报告的数据和观点不承担法律责任。

为商业决策赋能

EMPOWER BUSINESS DECISIONS

iResearch

艾 瑞 咨 询