CSA GCR cloud security alliance GREATER CHINA REGION

ZERO TRUST

中国零信任神兽方阵分析报告（2022年）

扫码解锁
更多行业报告

国际云安全联盟大中华区
2022年11月

CONTENTS

01 摘要

零信任模型于 2010 年由零信任之父、国际云安全联盟 CSA 安全顾问（原 Forrester 分析师）约翰 · 金德维格（John Kindervag）正式提出。新冠疫情的流行促使企业从传统的办公环境转向居家办公模式，加速了企业期待已久的向零信任安全战略的转变。大规模移动、云计算、软件即服务（SaaS）以及自携设备打破了安全边界，组织开始由传统企业环境转型为无边界网络。随着数字化的逐步实现，传统的网络安全边界已经消亡，再也不存在内外之分。在数字技术与新冠疫情推动下，安全威胁发生重大变化。

零信任代表了新一代的网络安全防护理念，关键之处在于打破默认的“信任”，用一句通俗的话概括，就是“持续验证，永不信任”。默认不信任企业网络内外的任何人、设备和系统，基于身份认证和授权重新构建访问控制的信任基础，从而确保身份可信、设备可信、应用可信和链路可信。

零信任给广大企业带来了新一代网络安全的战略理念，零信任的落地和价值的发挥是一项复杂工程。作为全球零信任产业引领组织，CSA 为业界更好地促进零信任实施做了大量的贡献，首先将 SDP 开源贡献给业界，形成了由数百家网络安全厂商构成的零信任生态，其次推广 CZTP 零信任专家认证课程，为业界实施零信任培养了上千名网络安全专业人才，而最近建立 CSA 零信任推进中心，则携手零信任领先厂商们为广大客户们排解落地疑难。此外，国际云安全联盟大中华区每年举办的国际零信任峰会，已成为全球认可的零信任领域的风向标活动。

2020 年开始，国际云安全联盟大中华区为了向业界完整呈现中国零信任的行业生态，让读者对零信任有一个全面的认知，同时提高零信任领域相关厂商和优秀实践者的曝光度和知名度，为打算实施零信任的甲方提供完整的参考，开始发布《中国零信任全景图》，这项活动已经持续了两年。

国际云安全联盟大中华区今年首次推出了《中国零信任神兽方阵报告》，从技术和市场两个维度评估目前零信任市场的主要厂商，帮助广大厂商和对零信任有兴趣的人员和组织进一步了解该市场的趋势。本报告是《中国零信任全景图》的补充，更关注于对零信任厂商的分析，勾勒出这些厂商在市场上的相对位置，进一步推动零信任市场的健康发展。

02 中国神兽方阵简介

中国神兽方阵(China Mythical Creatures Matrix)是在联合国科学技术促进发展委员会和联合国数字安全联盟指导下,由国际云安全联盟大中华区基于中国传统文化创立的分析模型,适用于数字科技各领域的通用分析。神兽方阵将中国的传统元素在数字世界点亮,通过神兽形象树立具有中国特色的科技标杆,助推与加速优秀科技企业的发展,从而带动整体的科技创新。

中国神兽方阵模型以“四象”即青龙、白虎、朱雀、玄武为基础,“四象”又称“天之四灵”,分别是镇守东西南北四方的神兽,其中青龙为东方之神,是四灵之首; 白虎为西方之神,也是战斗之神; 朱雀为南方之神,有浴火重生之职能; 玄武为北方之神,以防守见长。模型的创立旨在为数字安全领域树立具有中国特色科技标杆企业的行业分析品牌。方阵模型图及该模型中各神兽的定位与描述如下:

图2-1:神兽方阵模型图

青龙 - 四灵之首: 企业在零信任领域投入高,且研发能力、产品成熟度、市场营收及知名度方面整体实力强的头部企业。

白虎 - 战斗之神: 企业在产品方面作出快速的调整及创新,且获得市场的认可,在相关领域市场影响力大,占有率高。

朱雀 - 功力之神：企业具有核心竞争力的特定领域的产品，技术研发实力强，产品成熟度高，并有良好的市场占有率。

玄武 - 后起之秀：企业初创或新开设业务线，已在技术研发能力方面具有很强的能力及市场能力，是特地领域崛起的力量，潜力强。

国际云安全联盟大中华区发布的中国神兽方阵系列将涵盖云安全、数据安全、零信任、物联网安全、隐私科技、区块链等数字技术安全领域，从技术先进性与市场影响力两大维度对厂商进行评估，从研发能力、知识产权、营收情况等子维度做出分析与评价，并将具有特色能力的科技标杆企业通过方阵对应神兽进行代表。神兽方阵逐步渗透到数字安全各细分领域，寻找出各领域的科技标杆企业，引领行业企业的整体创新，推动数字安全发展。

03 零信任市场

零信任思想的历史可以追溯到 2004 年成立的耶利哥论坛（Jericho Forum），其重点研究方向之一就是探讨无边界趋势下的网络安全架构和解决方案。零信任（Zero Trust）这个术语最早是由时任 Forrester 分析师的 John Kindervag 于 2010 年提出，目前 John 已经加入国际云安全联盟 CSA 担任安全顾问。

随着云计算、物联网以及移动办公等新技术新应用的兴起，企业的业务架构和网络环境随之发生了重大的变化，给传统边界安全理念带来了新的挑战。新冠疫情以来，远程办公、多方协同办公等成为常态，带来了访问需求复杂性变高和内部资源暴露面扩大的风险，各种设备、各种人员接入带来了设备、人员的管理难度和不可控安全因素增加的风险，高级威胁攻击带来了边界安全防护机制被突破的风险，这些都对传统的边界安全理念和防护手段提出了挑战，亟需有更好的安全防护理念和解决思路。传统边界安全理念先天能力存在不足，新技术新应用又带来了全新的安全挑战。

3.1 零信任定义

零信任架构重新评估和审视了传统的边界安全架构，并给出了三个基本思路：应该假设网络自始至终充满外部和内部威胁，不能仅凭网络位置评估信任；默认情况下不应该信任网络内部或外部的任何人、设备、系统，需要基于认证和授权重构访问控制的信任基础；并且访问控制策略应该是动态的，基于设备和用户的多源环境数据计算得出。

Forrester Research 提出的零信任模型“消除了可信网络的概念”并教导“在零信任中，因为所有网络流量都是不可信的，所以安全专业人员必须验证和保护所有资源、限制并严格执行访问控制、检查和记录所有网络流量”。Forrester 于 2010 年发布了最初版本的零信任模型，在接下来的几年中，Forrester 修订 2010 版零信任模型并最终发布了零信任扩展（Zero Trust eXtended，ZTX）模型。ZTX 模型提供丰富的内容和以数据为中心的完整模型，如图 3-1 所示。ZTX 模型反映了 Forrester 的观点，即将本地环境（On-prem）和云计算环境所面临的“数据大爆炸（Data Explosion）场景”视为保护核心，同时也保护数据管道的周边元素，例如工作负载、网络、设备和人员。

图3-1：Forrester零信任扩展模型

2019 年，NIST 撰写了零信任架构特别出版物（SP 800-207），该文章将零信任理念融入零信任架构（ZTA）的抽象定义，并提出了 ZTA 开发和实施的指导原则，如图 3-2 所示。

图 3-2：零信任原则，NIST SP 800-207

根据 NIST（美国国家标准与技术研究院）关于《零信任》白皮书的定义：

零信任（Zero Trust，ZT）提供了一系列概念和思想，在假定网络环境已经被攻陷的前提下，当执行信息系统和服务中的每次访问请求时，降低其决策准确度的不确定性。零信任架构（ZTA）则是一种企业网络安全的规划，它基于零信任理念，围绕其组件关系、工作流规划与访问策略构建而成。因此，零信任企业是作为零信任架构规划的产物，是针对企业的网络基础设施（物理和虚拟的）及运营策略的改造。

中国通信标准化协会（CCSA）在《零信任安全技术参考框架》中把零信任定义为：

一组围绕资源访问控制的安全策略、技术与过程的统称，从对访问主体的不信任开始，通过持续的身份鉴别和监测评估、最小权限原则等，动态调整访问策略和权限，实施精细化的访问控制和安全防护。

零信任对访问控制进行了安全范式上的改变，引导网络安全架构从“网络中心化”走向“身份中心化”。从技术方案层面看，零信任安全架构是借助现代身份管理技术实现对人、设备和系统的全面、动态、智能的访问控制。零信任是指谨慎地建立信任基础，提升信任，最终在预设的时间内允许合理级别的访问”。零信任“并不是没有信任，而是让信任边界最小化，减少网络攻击的爆炸边界”。零信任“是把安全风险最小化的一种安全范式。国际云安全联盟大中华区概括了零信任的五项基本原则为 ABCDE：

A：Assume nothing 不做任何假定

B：Believe nobody 不相信任何人

C：Check everything 随时检查一切

D：Defeat dynamic risks 防范动态威胁

E：Expect for the worst 做最坏的打算

“零信任”是一种安全战略和思想，其核心理念是“永不信任，始终验证”。SIM（SDP, IAM, MSG）是其三大主流技术。其中，“S”代表的软件定义边界（Software Defined Perimeter, SDP），由 CSA 大中华区提出，旨在使应用程序所有者能够在需要时部署安全边界，以便将服务与不安全的网络隔离开来，更加关注南北向流量的安全。2013 年，国际云安全联盟 CSA 开发 SDP 框架，发布了《软件定义边界（SDP）标准规范 V1.0》，为零信任贡献了首个技术解决方案。“I”代表的现代身份管理和访问控制（Identity and Access Management, IAM），通过建立和维护一套全面的数字身份，并提供有效地、安全地 IT 资源访问的业务流程和管理手段，更加关注南北向流量。“M”代表的微隔离（Microsegmentation, MSG），由 Gartner 提出，更加关注东西向流量的安全，能够在逻辑上将数据中心划分为不同的安全段，一直到各个工作负载级别，然后为每个独特的段定义安全控制和所提供的服务，可以在数据中心内部部署灵活的安全策略。

根据 NIST，通用的零信任抽象架构如图 3-3 所示。

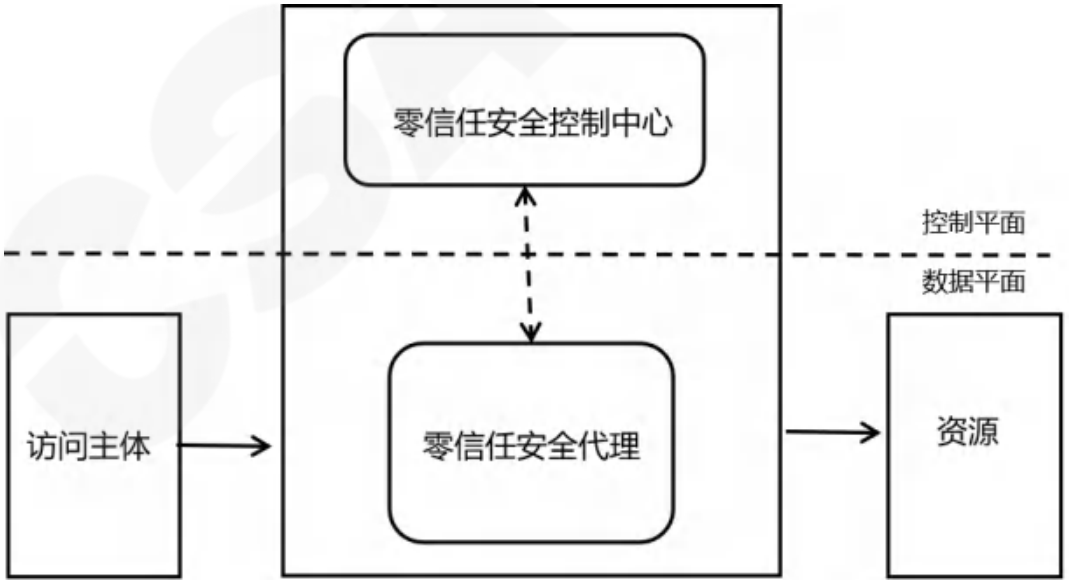


图3-3：零信任抽象参考架构

其中，零信任安全控制中心组件作为 NIST 的 PDP 的抽象，零信任安全代理组件作为 NIST 的 PEP 的抽象。零信任安全控制中心核心是实现对访问请求的授权决策，以及为决策而开展的身

份认证（或中继到已有认证服务）、安全监测、信任评估、策略管理、设备安全管理等功能；零信任安全代理的核心是实现对访问控制决策的执行，以及对访问主体的安全信息采集，对访问请求的转发、拦截等功能。

3.2 零信任产品（三大主流技术SIM）

“零信任”作为一种新安全理念，已经成为全球网络安全的关键技术和大趋势。虽然零信任已成为营销热词，但组织更应该相信零信任背后有着实质的内容和价值。零信任是一种战略理念、一种方法和一套指导原则，这也意味遵循零信任基本理念和通用原则的每套零信任架构我们认为满足 3.1 所述架构和原则的产品都是零信任产品。

目前，海外市场参与者众多，实现路径各有差异。既有谷歌、微软等率先在企业内部实践零信任并推出完整解决方案的业界巨头，有“以身份为中心的零信任方案”的 Duo、OKTA、Centrify、Ping Identity，也有偏重于网络实施方式的零信任方案的 Cisco、Akamai、Symantec、VMware、F5 等。海外零信任市场的商业模式较为成熟，安全即服务（SECaaS）为主流交付模式。

国内“零信任”市场刚刚兴起，包括互联网巨头及传统安全厂商，以及网络安全新锐均结合自身业务推出“零信任”产品和解决方案。从目前进入该领域的厂商来看，主要有 IAM、SDP、微隔离三个方向。当然，真正的“零信任”远不止于此，“零信任”还在发展中。

驱动企业转向采用零信任架构的因素主要包括：

- 合规驱动。近年来，安全形势日益严峻，侵犯个人隐私，攫取、破坏和滥用数据资源的行为时有发生，严重危害社会公共利益乃至国家安全。各行各业都迫切需要寻求新的解决之道，以零信任为代表的安全理念及架构等脱颖而出，成为推动并赋能合规建设的重要方法和指南。

- 合需驱动。数字经济时代，数据已经成为基础性、战略性生产要素，成为决定各国数字经济

发展水平和竞争力的核心资源。因此，数字化伴生的新技术和应用对网络安全技术和管理方式提出了更高要求。因此，需要一个更符合未来安全趋势的理念和架构来开展整体安全建设，也直接驱动了零信任在终端安全、应用安全、访问安全、设备准入、流动数据安全、勒索病毒防护等能力的应用和落地。

国际云安全联盟大中华区于 2020 年开始发布年度“零信任全景图”。从过去两年的调查可以发现，相比 2020 年，2021 年零信任的参与企业和产品有了显著提升，无论是既有安全厂商还是新兴创业公司，都关注到这一市场并有所投入，而相关的成功案例也比前一年有所增长。目前，国内零信任的目标客户主要集中在政府及事业单位、金融、制造业、运营商、互联网、能源、电力和医疗行业。

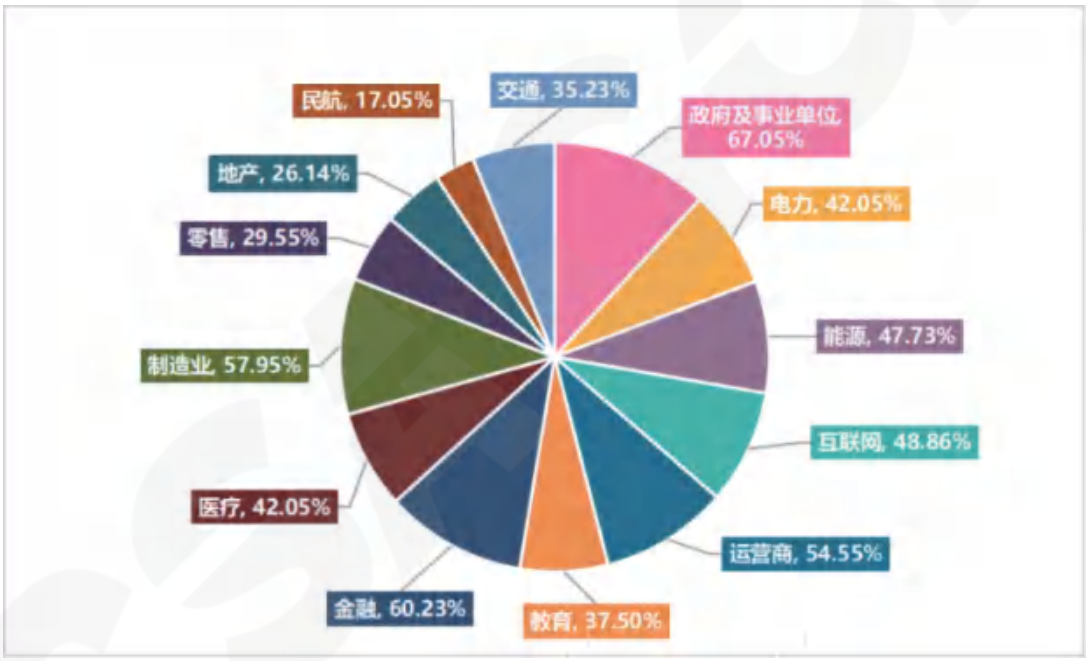


图3-4：零信任应用行业分布图

根据 Research Dive 最新发布的报告显示，全球零信任网络安全市场规模将从 2019 年的 185.0 亿美元增长到 2027 年的 667.413 亿美元，从 2019 年到 2027 年的复合年增长率为 17.6%，而其中零信任整体解决方案的市场份额将会越来越大。零信任从单一产品往平台、整体解决方案发展的趋势越来越明显。

04 中国零信任神兽方阵

4.1
2022中国零信任神兽方阵

CSA 大中华区综合考虑了企业的行业概况、商业模式、企业竞争力等因素，分别对应各神兽方阵数据模型的入选标准，筛选出一批在零信任领域具有一定规模，在业界有一定知名度和影响力，或者处于起步阶段但技术实力强和快速成长阶段的企业，作为 2022 年零信任领域的科技标杆企业。本次共 30 家，其中青龙标杆企业 4 家，朱雀标杆企业 6 家，白虎标杆企业 9 家，玄武标杆企业 11 家。

图4-1：2022中国零信任神兽方阵

零信任科技标杆企业—青龙： 奇安信科技集团股份有限公司、深信服科技股份有限公司、腾讯科技（深圳）有限公司、天融信科技集团股份有限公司（4 家）

零信任科技标杆企业—朱雀： 北京九州云腾科技有限公司、北京蔷薇灵动科技有限公司、厦门服云信息科技有限公司、深圳市联软科技股份有限公司、深圳竹云科技股份有限公司、苏州云至深技术有限责任公司（6 家）

零信任科技标杆企业—白虎：北京神州绿盟科技有限公司、格尔软件股份有限公司、江苏易安联网络技术有限公司、三六零数字安全科技集团有限公司、上海缔安科技股份有限公司、上海派拉软件股份有限公司、数篷科技（深圳）有限公司、亚信安全科技股份有限公司、长春吉大正元信息技术股份有限公司（9 家）

零信任科技标杆企业—玄武：北京持安科技有限公司、北京从云科技有限公司、北京数安行科技有限公司、杭州安恒信息技术股份有限公司、杭州迪普科技股份有限公司、杭州虎符网络有限公司、杭州亿格云科技有限公司、任子行网络技术股份有限公司、上海安几科技有限公司、上海物盾信息科技有限公司、新华三信息安全技术有限公司（11 家）

（按企业名称拼音排序，排名顺序不分先后，下同）

4.2 对入选企业的介绍与点评

北京持安科技有限公司

- 简介：

持安科技成立于 2021 年 4 月，公司核心产品持安零信任产品，在技术架构方面，通过微服务、平台化方式开发的原生零信任架构，所有的组件均可插拔，包括身份与认证中心，零信任终端，零信任网关、决策引擎，构建了从网络层、应用层、应用资源和数据层的全阶全链路零信任能力。当前客户主要集中在互联网、金融、能源、科技、高端制造、新零售领域。

- 点评：

持安科技属于零信任领域的新兴创业公司，创始团队具有甲方背景，对企业业务理解深，其零信任架构从业务出发，保障安全与效率，其主打技术融合 IAM、SDP 等技术，整体解决方案完备度较高，在市场规模上具有较大潜力。另外，其产品经过 CSA 大中华区举办的首届零信任攻防挑战赛，经过数百名白帽子攻击，未能被攻破，进一步验证其产品自身的安全性。

北京从云科技有限公司

- 简介：

从云科技成立于 2018 年，2020 年正式发布零信任安全产品。公司致力于零信任数据安全产品及场景方案的研发，帮助企业解决办公场景中业务直接暴露在互联网、数据在电脑终端主动或被动泄露带来的数据安全问题。公司目前主要产品为 DAS 智能接入系统、DAS 终端微隔离系统、DAS API 访问控制系统、DAS 物联安全接入系统、DAS 数据库访问控制系统、DAS 云主机防护系统。主要解决网络及业务暴露在互联网的安全问题、数据在终端 / 系统被泄露的问题、人员和系统权限精准匹配问题，杜绝越权访问及简化运维。目前服务的客户有中国铁路物资集团有限公司、信通院、公安部第一研究所、中信建投证券等。

- 点评：

从云科技属于零信任领域的新兴创业公司，在微隔离技术方向，已发布上网空间的微隔离产品，聚焦数据安全，尤其在数据安全隔离方面，产品方案完整度较高，在市场规模和技术方案上均有较大潜力。

北京九州云腾科技有限公司

- 简介：

北京九州云腾科技有限公司是一家专门为企业提供统一身份认证 IDaaS 解决方案提供商，同时提供衍生的零信任安全 ZTA 的解决方案。公司专注于解决国家机构、事业单位、各类企业机构的员工、合作方以及其服务对象、客户等人群在访问私有云、公有云、内网自有业务、互联网及移动互联网业务等多种复杂应用场景下的身份认证及零信任安全问题。2019 年 11 月，九州云腾被阿里云全资收购，现为集团全资子公司，保持独立品牌继续运营。

- 点评：

九州云腾属于零信任领域的创新型企业，是零信任泛身份认证的实践者，代表产品是泛身份认证 IDaaS 云服务，包括 IDP、CIAM、EIAM 等子领域。同时也具有 SDP 产品，零信任技术路线比较全面，且拥有较强的技术创新性和专业积累。总体而言在技术研发方面的表现较好，也具备一定的市场和客户规模。此外作为阿里云的全资子公司，可以利用阿里云平台和生态方面的优势。

北京蔷薇灵动科技有限公司

- 简介：

蔷薇灵动成立于 2017 年，主要专注于网络安全领域微隔离技术的前沿探索与研究。其产品蜂巢自适应微隔离安全平台已在大规模工作负载统一纳管、跨域异构混合环境集中部署等方面凸显了一定竞争力，在政府、金融、大型企业、军工、能源、运营商等多领域场景得到运用。2022 年 9 月 8 日正式推出全流量零信任访问控制与安全接入平台——统一微隔离。新产品通过向办公网场景延伸为用户提供覆盖其全部基础设施的微隔离控制与安全运营服务。

- 点评：

蔷薇灵动是国内目前仅专注于微隔离技术研发的创新科技企业，基于多年的的技术打磨及市场需求探究，在微隔离技术创新及突破上具有独特的技术优势；蔷薇灵动产品目前已众多在政府、金融、大型企业、军工、能源、运营商等多领域头部用户核心场景处处成功运用；蔷薇灵动目前已牵头或参与起草国内多个零信任及微隔离相关标准的制定，产品已成为国内微隔离产品方案的事实标准。蔷薇灵动聚焦于微隔离，该细分领域目前市场竞争者较少，近年来营收增速也比较明显。

北京数安行科技有限公司

- 简介：

北京数安行科技有限公司于 2020 年 8 月进入零信任市场，公司主营产品涵盖零信任数据安全、数据安全风险监测与风险评估、个人信息合规与隐私保护、数据安全计算与安全计量和数据运营安全等。数安行以 DataSecOps 为理念，融合零信任数据安全框架，以 AI 人工智能技术为核心驱动，聚焦数据运营安全，助力数字化转型。目前，产品服务于金融、运营商、互联网、教育、高端制造、软件与信息技术服务、工业互联网、能源等各行业客户。

- 点评：

数安行在零信任领域具备数据安全特色，通过零信任助力数据安全，有效平衡数据开发利用与数据安全保障，零信任轻量化部署，对业务架构无改造，较为容易落地实施，在市场发展方面有较好的增长性。

北京神州绿盟科技有限公司

- 简介：

绿盟科技于 2014 年启动零信任关键技术研究，2019 年陆续发布多款零信任产品。绿盟科技零

信任安全解决方案，遵循零信任安全理念，组合终端安全、身份识别与管理、网络安全、应用和数据安全、安全分析协作与响应等模块，构建以用户信任和设备信任为基础，持续评估访问过程的行为可信，自适应访问控制的零信任安全架构。

- 点评：

绿盟属于原有安全厂商新增零信任业务条线，技术完整度较高，涵盖了 SDP、IAM 和 SASE 几大技术路线，具备整体零信任方案建设能力，能支持不同技术基础的公司的零信任建设需求。零信任方案可与绿盟堡垒机产品深度融合，形成远程办公 + 远程运维解决方案。目前，绿盟零信任安全已有一定市场规模和营收，但由于缺少 VPN、终端准入等历史积累，市场拓展相对其主营产品条线略显薄弱。

长春吉大正元信息技术股份有限公司

- 简介：

吉大正元以密码技术为核心，为客户提供涵盖安全基础建设、数据安全、移动互联安全、云计算安全、物联网安全等不同领域的整体安全解决方案。依托多年密码行业的优势，已成功为多个大中型企业建立基于 SDP 技术的远程办公边界防护安全解决方案和基于 IAM 技术的身份与访问控制的零信任案例。已累计服务政府、金融、电信、军工、能源、互联网、教育、医疗、电力、交通、制造等多个垂直领域。

- 点评：

吉大正元基于密码技术的零信任体系建设方案能够合规、正确、有效使用密码，使用自主、安全、可控的密码，方案能力涵盖身份安全、权限安全、终端安全、数据安全、传输安全、网络安全、接入安全等多维度。通过多年的行业积累和技术优势，已经在多个行业应用，并获得客户的认可。产品经云化能力迭代升级后，基于零信任密码核心技术，将会有更强的市场竞争力。

格尔软件股份有限公司

- 简介：

格尔软件成立于 1998 年 3 月，深耕密码行业多年。格尔零信任安全体系坚持以密码为基石、以身份为中心、基于软件定义边界的思想，依托密码服务平台、PKI/CA 基础设施、可信身份服务平台、特权帐号管理、策略控制中心 、终端环境感知、UEBA 等管理控制组件，构建了从终端登陆、网

络准入、应用访问、接口访问、数据访问及特权访问等各个环节的纵深防御体系，确保可信的人通过可信的途径访问可信的数据。格尔零信任体系相关产品具备国密资质，支持国产密码算法，全面兼容国产化硬件 / 软件平台，已在政务、军工等行业领域落地，可应用于智慧城市、云计算、大数据、物联网、车联网、工业互联网等业务场景。格尔零信任项目已成功入选 2020 年工信部网络安全技术应用试点示范项目、2021 年 CSA 云安全联盟大中华区零信任落地案例集。

- 点评：

格尔软件零信任体系全面集成合规的密码产品及服务，全线产品支持信创环境。以及体系全面覆盖终端、身份、网络、应用、数据、可见性及分析、编排及自动化等维度，采用云服务化及开放 API 架构设计，可方便的支持第三方系统及安全产品的集成。目前格尔软件基于原有技术的优势及在军工、政企等方面客户资源优势，加之具有较强的生态集成能力，适用场景广泛，未来在市场发展方面将有更强的爆发力。

杭州安恒信息技术股份有限公司

- 简介：

安恒信息结合以往零信任领域研究成果，分析当前网络安全现状与客户需求，采用 SDP、IAM 等零信任技术，结合商用密码技术，推出零信任解决方案。解决方案以身份安全为核心，具有多源信任评估、动态访问控制、可信业务访问等安全服务能力，同时可扩展移动认证、单点登录、可视化监管等功能。

- 点评：

安恒作为原有安全厂商新增零信任产品线，其零信任安全客户端轻量化部署，通过零信任理念打造 API 身份鉴权安全网关，保障 API 接口安全，将零信任解决方案在其已有政企客户市场深耕，同时关注云市场并完成与安恒云的融合。目前零信任相关产品包括身份服务中心 TAM、DSG-API 和 DSG-APP，零信任市场主要客户为运营商和政府。

杭州迪普科技股份有限公司

- 简介：

迪普科技从 2019 年开始进行零信任产品的研发并于次年正式发布零信任安全解决方案，整体架构由零信任安全客户端、统一安全管理平台及安全应用代理系统组成，结合可扩展的终端环境感知管理平台和统一身份认证中心，可实现基于身份、终端、环境的统一授权以及动态权限调整

等功能。目前产品已广泛服务于运营商、医疗、金融、政府等行业用户。

- 点评：

迪普科技属于原有安全厂商新增零信任产品线，在 SDP 和微隔离技术方案完整程度高，整体解决方案相对较为全面，目前已经有多个行业案例落地的经验，并且已经针对信创改造需求，目前整个产品涉及到的安全组件基本能够适配主流的国产操作系统及硬件架构。

杭州虎符网络有限公司

- 简介：

虎符网络成立于 2019 年，是一家专注于“零信任”安全方向的网络及数据安全厂商。公司聚焦重塑企业安全架构、构建身份与数据安全可信网络，现已推出“虎盾”访问安全产品线、“虎影”数据安全产品线等产品，用于解决远程办公、多云多数据中心接入、开发运维环境数据共享等业务场景下的安全问题。

公司拥有完整的零信任产品研发平台，在可信身份网络、数据隔离等领域拥有多项核心技术，牵头制定《移动办公场景下的攻击面收敛技术规范》等标准。目前虎符网络是浙江省科技型中小企业，中国计算机行业协会数据安全专委会成员单位，杭州市余杭区科技企业研发中心，相关研发成果已成功应用于电商、大数据局、能源、物流、高校等行业头部客户。

- 点评：

虎符网络的零信任产品主要是易落地的轻量级方案，能够很好兼容企业现有 IT 基础设施和安全能力，容易实施现网改造，并且易于和数据安全产品集成对接，形成从终端可信、身份可信、网络可信到数据可信的综合解决方案，发挥整体零信任安全保障体系最大优势。另外，其产品经过 CSA 大中华区举办的首届零信任攻防挑战赛，未能被攻破，产品体验感好，产品安全性都得到验证。

杭州亿格云科技有限公司

- 简介：

亿格云是零信任 SASE 安全服务厂商，主要解决企业数字化转型过程中遇到的多分支统一安全管控 、远程办公、内部应用暴露、数据安全等威胁； 通过自主研发的亿格云枢平台，基于云原生零信任 SASE 架构，15 分钟内即可快速部署上线，为企业构建一张覆盖全球的专有安全网络，为数字化企业提供零信任安全访问、终端安全防护（XDR）、数据安全防护（XDLP）、全球应用加速的一站式办公安全解决方案。团队人员来自阿里云安全的产品和业务骨干，打造过多个亿级安全产品

线，曾服务超过 10 万 + 企业，团队同时拥有 15 年以上的网络安全从业经验和互联网 SaaS 服务经营的实战经验，具备做 SASE 产品的基础和技术能力，公司员工数量近百人，拥有多项技术专利和 18 项 + 软著等资质。公司成立于 2021 年，目前，已服务 AIOT、零售、电商、金融、教育、游戏、汽车等行业的几十家头部企业客户。为客户提供了安全办公一体化解决方案，得到了客户的认可。

- 点评：

亿格云在零信任 SASE 方向具有核心技术能力，专注推进零信任 SASE 安全服务体系零信任领域，其产品扩展性强，各类角色用户体验良好，具有很好的市场潜力。团队成熟，企业向上发展，在市场规模和技术方案上均有较大潜力。

江苏易安联网络技术有限公司

- 简介：

易安联是中国零信任应用场景的探索实践者，专注零信任领域多年，围绕应用访问安全，先后发布 EnSDP（零信任安界防护平台）、EnBox（零信任安全工作空间）、EnCASB（零信任云应用安全接入平台）、EnAppGate（统一资源发布系统）、EnIAM（零信任身份管理平台）、EnNTA（零信任网络流量感知平台）共计 6 款基于零信任架构之下的网络安全产品，目前合作客户已超 500 家，涵盖高校、科研院所、电信运营商、能源、金融、互联网等行业。

- 点评：

易安联定位是一家零信任公司，具备一定规模的零信任研发队伍，主打 SDP 和 IAM 技术路线，覆盖终端安全工作空间、零信任网关和流量分析、零信任身份管理等多个技术维度，有多样的零信任网络安全产品，市场品牌发展好，已取得了较大的市场规模，是零信任领域专注的创新企业。另外，其产品经过 CSA 大中华区举办的首届零信任攻防挑战赛，经过数百名白帽子攻击，未能被攻破，进一步验证其产品自身的安全性。

奇安信科技集团股份有限公司

- 简介：

奇安信成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务，在人员规模、收入规模和产品覆盖度上均位居行业第一。2022 年 3 月 13 日，奇安信圆满完成了北京冬奥会和冬残奥会网络安全保障工作，兑现了北京冬奥网络安全“零事故”的承诺。奇安信零信任安全解决方案以数据为中心，以身份为基石，是奇安信“一中心两体系”内生安全框架的核心要素，助力政企客户应对数字化转型的安全新挑战。

- 点评：

奇安信属于原有安全厂商增加零信任业务，奇安信的“一中心两体系”内生安全框架将“零信任体系”与“实体安全防护体系”有机结合，实现“主体身份可信、行为操作合规、计算环境与数据实体有效防护”。具备强大的生态能力和市场能力，产品及方案已在政府、金融、央企、能源在内的诸多行业全面落地。此外，奇安信在零信任领域产品技术研发、市场营收和用户市场规模等维度表现均较出色。此外在国内零信任布道和标准起草方面表现出色。总体属于零信任安全领域的领军者之一。

任子行网络技术股份有限公司

- 简介：

任子行自主研发的智行零信任解决方案是为政府、军工、医疗、教育、企事业单位提供集身份认证、统一门户、应用防护、安全接入、信任评估、访问控制、端点安全、数据安全、全面审计、安全联动为一体的综合安全防护解决方案。在不改变原有的网络架构下能够轻松应对远程接入、内网安全访问、数据安全运维、数据安全交互、访问内容审计、文档不落地、一机两用、攻防演练等各类应用场景的安全问题。

- 点评：

任子行属于原有安全厂商新增零信任产品线，在企业已有安全技术能力上融入了零信任的理念进行创新，企业在大数据平台方面具有较好的能力优势促进零信任策略智能化，企业在零信任领域研发投入高，在各行业用户积累基础好，能较好将零信任解决方案落地。

上海安几科技有限公司

- 简介：

安几网安创始于 2018 年底，以零信任框架为核心，研发实践了访问端、通道、资源端的“安全端到端”的系列产品 EDR、SDP、安全工作空间以及物联网零信任平台等。公司产品已覆盖金融，制造，能源，医药，交通等各个领域，广泛应用于威胁态势感知、多云办公、远程访问、数据防护、物联网加固等各类场景。

- 点评：

安几网安属于零信任领域的新兴创业公司，主打 SDP 技术，零信任融合 AI 技术，实时动态评估安全风险，制定安全策略，具有安全智能化特色，并且支持多种访问协议，可延展性强，产品理念清晰，成熟度高，具有很强的市场潜力。

上海缔安科技股份有限公司

简介：

上海缔安科技股份有限公司创立于 2007 年，是国内虚拟安全云网络服务的代表企业之一。缔安科技零信任解决方案基于身份这一核心，融合国家商用密码算法，帮助企业用户在零信任网络、身份安全、应用安全管理等模块中的进行更加细致与深入的管控，增强安全防护能力。目前，缔安科技零信任解决方案已在多个行业中实现落地，如政府、电信与互联网、制造、能源、交通等。近年来，缔安科技深度参与行业技术探讨与标准编写制定，参与翻译《SDP 标准规范 1.0》、《软件定义边界架构指南》等零信任理念早期引入国内的相关材料，并参编《网络服务安全与监控》、《零信任网络安全：软件定义边界（SDP）》等书籍。

点评：

缔安科技作为 SD-WAN 安全云网络运营服务提供商，在安全方面始终保持大量的研发投入并保持对技术趋势和市场态势的敏感性，其零信任网络访问解决方案完整覆盖用户接入访问的全过程，在架构安全性、产品的传输安全性、对内网安全的防护性、用户使用时的便捷易用性等方面具有优势，其市场拓展主要采用分销模式，目前已在多个行业中实现落地并树立标杆案例，并取得良好的市场效益和客户反馈，在市场发展方面有较强的优势。

上海派拉软件股份有限公司

简介：

派拉软件成立于 2008 年，拥有完整的零信任产品体系，从以身份为中心的动态访问控制，逐步延伸到联动终端管理、SDP、动态授权、API 网关、用户行为分析、数据访问安全等为一体的端到端零信任安全解决方案。派拉一体化零信任安全可支持远程办公、移动设备接入、远程运维、企业分支机构接入、互联网业务访问等应用场景。

点评：

派拉是国内较早从事身份安全研发的原厂商，在身份安全领域具有丰富的方案落地经验，以及在安全方向的产品多样化，如：IAM、SDP、PAM、IDaas 等，一体化的零信任产品和服务能较好融合支持客户复杂业务环境。依托其多年来积累的行业优势，已将零信任快速落地到各个行业，在市场拓展方面取得较好成绩。

上海物盾信息科技有限公司

- 简介：

物盾安全成立于 2019 年 1 月，聚焦物联网边缘计算网络安全领域，以零信任为核心理念，以物安盾零信任安全防护为核心解决方案，致力于解决“物联网 + 边缘计算”场景下的安全问题，实现工业互联网中“最后一公里 " 的安全管控。

- 点评：

物盾安全在边缘计算技术融入零信任理念，构建自适应边缘计算架构的边原生安全能力；打造统一探针，实现零信任能力技术在物联网设备上的成功验证。物盾在物联零信任产品方向具有技术竞争能力和特色，面对边缘计算和物联网的发展，物盾安全具有很强的市场潜力。

三六零数字安全科技集团有限公司

- 简介：

360 数字安全自 2016 年起，参考 Google BeyondCorp 的落地情况，确立了以 SDP 为演进方向的零信任建设目标。2020 年正式对外推出了 360 连接云安全访问产品，基于“零信任 " 安全理念打造了安全访问控制平台，帮助客户在数字化转型过程中应对各类风险攻击、保障业务安全、满足监管合规等各类安全要求。目前，在多家客户部署落地，主要包括金融、财政、能源、政务、互联网等行业。

- 点评：

360 数字安全属于原有安全厂商增加零信任业务，主打 SDP，集成了第三方的 IAM 和 MSG，开放的生态产品对接能力，支持和各类身份平台、业务网关快速集成对接。可发挥 360 安全大脑获取访问环境风险信息，实现及时的零信任动态权限控制。360 依托小金融（农商、城商行和股份制银行）、能源（电力、重型燃料）和城市产业，在市场上快速拓展落地。总体来看，360 在品牌和市场基础方面具有较强的优势，产品架构集成生态基础好，在大客户场景落地零信任整体解决方案方面有较大潜力。

数篷科技（深圳）有限公司

- 简介：

数篷科技成立于 2018 年，致力于零信任数据安全平台的研发。基于新一代安全沙箱、高性能网

络隧道、软件定义边界、AI 安全策略引擎等核心技术，数篷科技已推出“零信任终端安全工作空间 DACS Pro”、“零信任网络访问控制系统 DACS Lite”、“零信任移动安全工作空间 DACS Mobile”等产品。数篷科技在 2020 年 9 月发布的 HyperCloak 增强型零信任安全框架，已在商业智能（BI）、研发环境、专业服务外包、跨组织协作、远程办公等场景中得到了应用，服务于众多企业。

- 点评：

数篷作为零信任数据安全公司，主打 SDP 技术路线，拥有终端沙箱和零信任网关产品，技术采用微内核 + 轻量可信计算技术，实现对敏感数据的精准访问控制及有效隔离管控，特色在于信创国产软件自主可控。数篷在电力、运营商等行业落地零信任，容易实施和运维方便，得到较好的市场反馈。

深信服科技股份有限公司

- 简介：

深信服是一家专注于企业级安全、云计算及 IT 基础设施的产品和服务供应商。深信服于 2019 年正式发布零信任产品 aTrust，包括零信任平台和零信任组件，以零信任平台为核心，可平滑扩展不同场景下的组件，使用场景涵盖远程办公、移动办公、混合办公等多种访问场景。目前已在企业、政府、金融、教育、医卫等行业落地了上千个项目。

- 点评：

深信服属于原有安全厂商增加零信任业务，零信任方案扩展简便，以统一的 ZTA 平台为中心，通过 SDP 代理网关、DGW 直连网关、CWPP 云主机保护平台、UEM 沙箱等核心组件的叠加，实现业务场景的灵活扩展，帮助用户从单一场景逐步演进到全场景零信任。基于深信服“平台 + 组件 + 服务”的安全战略配套专项服务保障体系能较好得完成零信任整体解决方案的落地，提升用户的使用体验。在技术研发和市场营收方面的整体表现较好，属于零信任安全领域的领军者之一。

深圳联软科技股份有限公司

- 简介：

联软科技于 2004 年从事网络准入控制研发，2019 年推出 SDP 产品，2021 年推出 UEM 的

ZTNA 零信任网络访问产品和方案。在零信任接入与管理方面，企业在接入零信任方案时，只需通过 EMM 系统即可，提升零信任接入效率。联软 SDP 零信任系列产品用户全面覆盖金融、高端大型制造、医疗、政府、运营商、互联网等众多行业。此外，联软 SDP 产品入围了《IDC 创新者：零信任之软件定义边界与微隔离技术》报告；连续两年上榜 CSA 云安全联盟《中国零信任全景图》并荣获 CSA 联盟年度大奖 - 安全创新奖。联软拥有多名 CSA 首批零信任资格讲师，以及 Forrester 零信任认证专家，联软科技作为参编单位参与国内首个零信任技术标准（T/CESA 1165-2021《零信任系统技术规范》团体标准）的发布。

- 点评：

联软属于原有安全厂商新增零信任业务条线，主打 SDP 技术路线，依托其多年来积累的终端安全领域优势，统一内网的 NAC 技术和外网的 SDP 技术，实现内外网全面零信任接入。此外在数据安全方面也具备终端多域安全沙箱能力，实现终端企业数据隔离、终端网络隔离和企业应用进程保护。在零信任领域拥有较强的技术创新和积淀，技术研发能力较强。具备一定的用户规模和市场营收能力。

苏州云至深技术有限责任公司（云深互联）

- 简介：

苏州云至深（云深互联）自 17 年开始研发软件定义边界 SDP 产品，2018 年 10 月“深云 SDP”V1.0 版本发布，正式面世，2019 年入选 Gartner《ZTNA 市场指南报告》，2019~2022 年连续四年入选 Gartner 市场指南报告，牵头编制多个零信任相关的规范和著作。苏州云至深的产品经过多年的开发和完善，已从最初的 1.0 版本开发至 7.0 版本，功能模块也从最初的 DPA（私有应用访问控制），到 DGA（热门应用访问加速）、DIA（公共应用访问控制）、DWA（无客户端模式访问控制）、DMDA（跨域应用访问控制），产品逐渐完善，并在国际 SDP 标准基础上开发出 SmartSPA、SmartDNS、DHR 网络、Linker 连接器等特色技术。苏州云至深（云深互联）多年来为各行业提供网络安全服务，如金融、政府、运营商、互联网、大型央企 / 国企、教育等。

- 点评：

云深互联属于专注于 SDP 领域的新兴创业公司，主打 SDP 技术路线，产品技术方案完整度高，在国际 SDP 标准基础上创新的开发出 SmartSPA 技术，且深云 SDP 目前已经支持无客户端部署和云原生架构部署，拥有较强的技术创新和积淀。此外在推进零信任技术标准化和技术布道等领域也有较突出的贡献。也具备一定的市场营收能力。其产品经过 CSA 大中华区举办的

首届零信任攻防挑战赛，经过数百名白帽子攻击，未能被攻破，进一步验证其产品自身的安全性。

深圳竹云科技股份有限公司

- 简介：

竹云科技专注于 IAM、零信任以及云应用安全领域，具有全栈 IAM 及零信任产品线。竹云零信任解决方案以 IAM 平台为核心，涵盖 SDP 接入服务、权限与策略管理、风险检测与信任评估系统，以全链条持续验证为手段，动态控制应用、URL、角色以及数据是否允许访问。通过单包授权完成设备可信检查、安全接入网关接管用户认证、对应用系统隐身及请求的安全防护，形成完整的零信任网络接入方案。同时提供足够的开放性，融合已有安全系统，如终端安全、态势感知等，形成完整的零信任生态体系。平台应用自适应风险识别机制，对用户、设备、应用、流量进行持续信任评估，根据风险数据建模分析，实时告知企业存在的潜在风险。平台已应用于政府、能源、建筑等行业客户。

- 点评：

竹云属于零任任领域的创新型企业，主打 IAM 和 SDP 技术路线。IAM 的代表产品竹云 IDaaS，涵盖了 CIAM、EIAM 等子领域，致力于保护“人与应用间一切连接”。在零信任领域拥有较强的技术创新和积淀。此外竹云的零信任产品提供足够开放性，可以融合已有的终端安全（EDR）、态势感知等安全系统，快速构建完整的零信任安全架构。具备较强的技术研发能力，市场拓展层面潜力也比较大。

天融信科技集团股份有限公司

- 简介：

天融信成立于 1995 年，于 2019 年正式发布零信任安全产品，可针对远程安全访问、用户业务统一访问、云端业务访问等场景进行具体部署，提供身份管理、终端环境感知、用户行为分析、信任推断、动态访问控制模块等五大技术能力。在采用 SPA 技术实现业务隐身，减少业务暴露面的基础，通过客户端对终端环境的风险评估、控制器进行动态访问控制、网关进行安全防护等技术手段，实现安全的业务访问。在目前在公安、运营商、企业、能源等行业已有众多落地实践。

- 点评：

天融信属于原有安全厂商增加零信任业务，天融信的零信任产品涵盖 SDP 和 IAM 身份服务系统，API 代理系统等，微隔离产品也在落地过程中。行业整合能力较强，覆盖超过 100,000 家政府、

金融、电信、教育、医疗、能源、交通、制造等行业的客户。总体技术路线较全面，在技术研发和市场营收方面的表现均较出色，另外天融信也多次参与零信任相关标准的起草工作。总体属于零信任安全领域的领军者之一。

腾讯科技（深圳）有限公司

- 简介：

腾讯安全作为腾讯立足互联网安全的行业品牌，从 2016 年开始自研并使用自家的零信任安全产品 iOA。腾讯 iOA 基于终端安全、身份安全、应用安全、链路安全等核心能力，对终端访问过程进行持续的权限控制和安全保护，实现终端在任意网络环境中安全、稳定、高效地访问企业资源及数据。同时，iOA 提供 SaaS 和私有化两种部署方式，支持有端和无端两种模式。当前客户主要定位于泛互联网、金融、政府、教育、保险、地产、物流、医疗、工业、能源等行业，终端部署量级上百万。

- 点评：

腾讯安全属于原有安全厂商增加零信任业务，拥有 20 年互联网安全技术和实践经验的积累。其 iOA 零信任架构具备终端安全、身份安全、应用安全、链路安全等多维度安全能力，且可以通过一键连接企业微信进行部署。在技术研发和市场营收方面表现均较出色。具备完善的内外部生态，依托企业微信等天然的 2B 渠道优势和部署实施的便利性，在业界享有较高的知名度。另外在零信任标准制定方面表现突出。总体属于零信任安全领域的领军者之一。

新华三信息安全技术有限公司

- 简介：

2019 年 9 月，新华三推出零信任方案，以 SDP 和 IAM 两个方向作为发力的重点，满足远程办公、分支接入、远程运维、云端管控、移动办公等多个常见应用场景的要求。基于终端安全、身份安全、权限安全、数据安全等安全能力，结合持续信任评估和动态权限管控，为客户提供解决方案。主要客户涉及金融、政府、公安、教育、能源、电力、企业等多领域。

- 点评：

新华三属于原有安全厂商增加零信任业务，具有成熟的终端管理能力和丰富的可信网关覆盖能力等原有优势，在零信任方向上，新华三零信任方案全面自研，在零信任终端安全管理融入零

信任理念，及逐步加大在零信任领域的研发，结合新华三成熟的市场体系优势，其在零信任领域的技术和市场发展都具有很强的发展和突破潜力。

厦门服云信息科技有限公司

- 简介：

厦门服云（安全狗）作为中国云安全 CWPP 的代表厂商，从创立之初就致力于主机安全产品的研发。2017 年启动微隔离产品的设计研发，2018 年 3 月发布云隙自适应微隔离产品，2021 年云隙入选 Gartner CWPP 市场推荐指南清单。2021 年 9 年，安全狗发布了分别基于 SDP 和 SASE 的零信任安全产品，丰富和完善了零信任产品线，为用户提供了不同场景下的零信任安全解决方案。

- 点评：

安全狗属于原有安全厂商新增零信任业务条线，依托其多年来积累的云安全优势，在微隔离领域有一定的技术积累，代表产品是基于 CWPP 技术方案的自适应微隔离系统，具备策略自动识别和配置的能力，以及混合云场景下跨云平台流量识别和统一策略管理能力。此外安全狗兼具 SDP 和 SASE 产品，涉及的零信任技术路线比较全面。在技术研发领域表现较好，同时也具有一定的市场营收能力。

亚信安全科技股份有限公司

- 简介：

亚信安全信磐零信任访问控制系统 AISDP，以零信任理念为客户提供快捷、安全的网络接入能力，保障用户在任意位置安全地访问内部业务资源。通过终端准入基线、MFA 多因素认证、资源访问授权、持续信任评估、威胁流量联动处置为客户打造终端可信、环境可信、身份可信、行为可信、流量可信的净朗网络空间。亚信安全零信任访问控制系统入选 Gartner Toolkit，结合零信任产品打造的电力解决方案获得 2022“闪电杯”能源行业网络安全实践案例三等奖。目前，AISDP 产品已经在政府、运营商、电力等重要行业得到成功应用。

- 点评：

亚信安全属于原有安全厂商增加零信任业务，特色是基于终端融入零信任能力构建大终端零信任一体化安全解决方案，一体化部署。在运营商、电力等行业已经拥有大型客户案例，结合长期服务于运营商行业的技术积累和用户资源，亚信安全零信任方案，市场发展具有很大优势。

05 分析总结

国际云安全联盟大中华区从 2020 年开始发布《中国零信任全景图》，一直在持续关注零信任市场的发展。如果说《中国零信任全景图》是对零信任市场的整体描述，那么《中国零信任神兽方阵》就是对企业的深入探讨。本次调研的内容与《中国零信任全景图》调研的内容相互验证，揭示并验证了一些市场趋势和企业的关注点，可供参考。

5.1 市场现状

2020 年发布的《中国零信任全景图》，参与的企业共 65 家，2021 年收录了 88 家单位，比第一版零信任全景图参加的单位增加了 35%。本次调研关注于零信任产品提供商，与参与零信任全景图的单位相比，剔除了甲方零信任实践者，以及咨询、评估、测评和治理类的乙方企业。参与本次调研的企业数量减少，但提供零信任产品的企业数量显著增长。2021 年，在工信部发布的《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中，“零信任 " 作为需要加快发展的创新安全技术之一。可以预期，在零信任市场，还会有更多的参与者加入进来。

5.1.1 服务对象

目前，国内零信任的目标客户主要集中在政府及事业单位、金融、制造业、运营商、互联网、能源、电力和医疗行业，其中，尤其是政府和事业单位占据了重要地位，这和政府今年来加强数据安全合规的趋势以及数字政务的发展密切相关。与此同时，能源行业关系国计民生，对安全较为重视，因此也比较注重在零信任方面的投入，在所有服务客户中名列前茅。以下为在本次调查中，零信任客户案例在行业的分布情况：

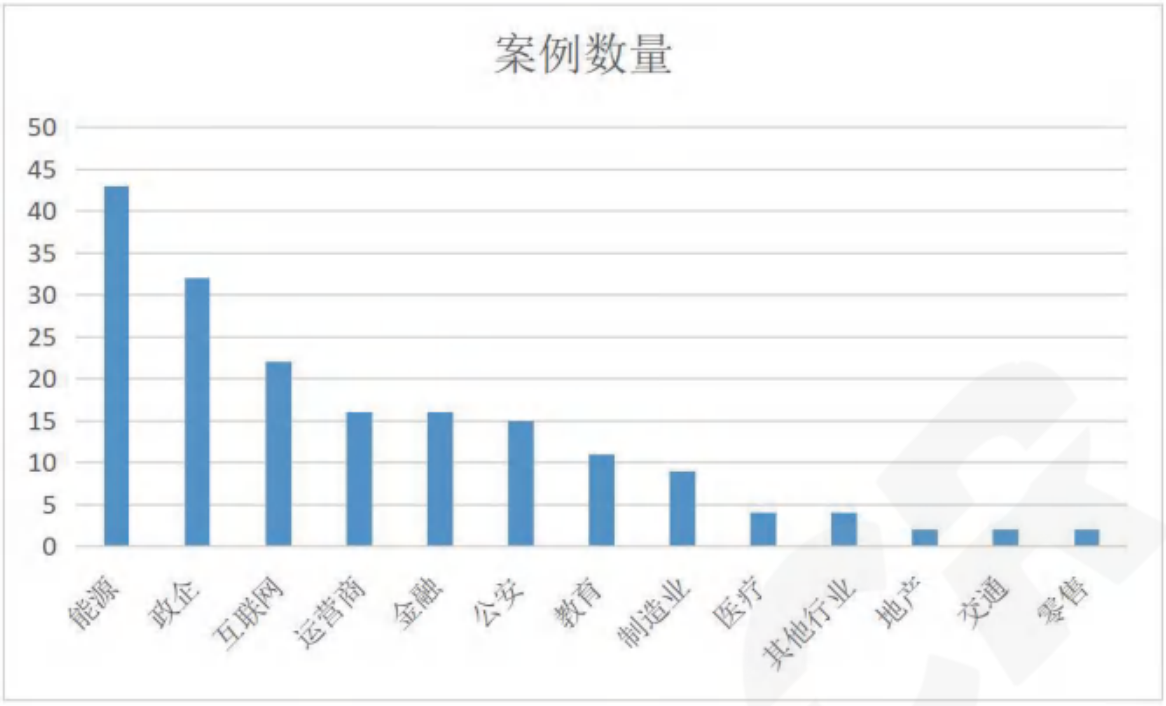


图5-1:零信任客户案例在行业的分布图

5.1.2 应用场景

目前,零信任的应用场景主要聚焦于对企业内部的安全访问,与外部的协助以及安全合规。前二者也可以认为是对传统 VPN 访问的替代,而安全合规更多是伴随着国家对安全监管的加强,要求的明确,责任的追究力度的加大对企业所产生的压力的应对。以下为在本次调查中,零信任应用场景的分布情况:

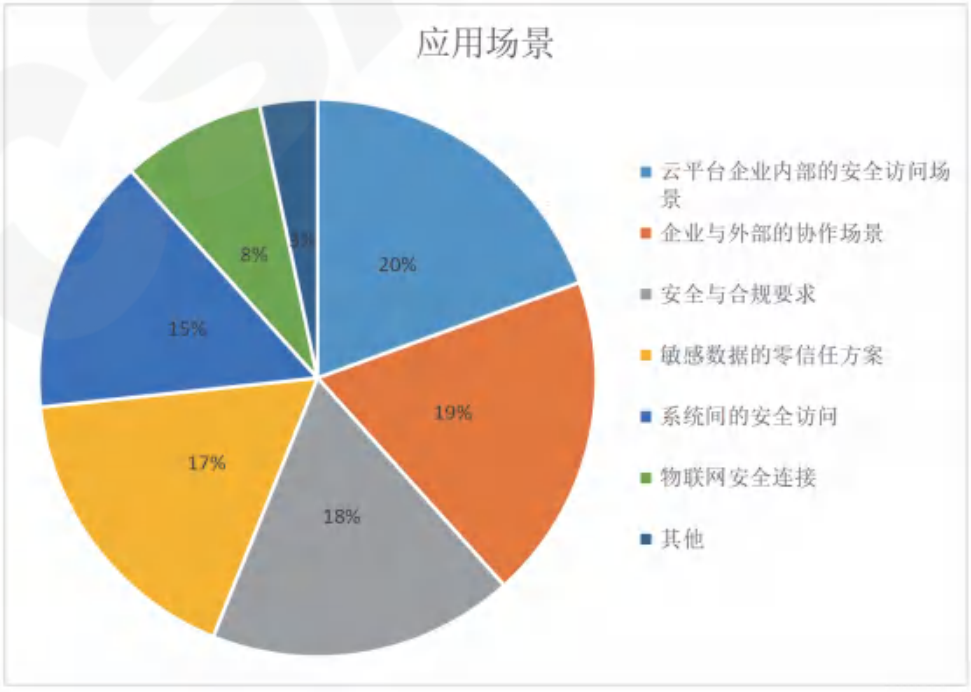


图5-2:零信任应用场景分布图

5.1.3 公司沿革

从调查可以发现，目前的零信任厂商包括传统的安全厂商整合资源，并开拓全新的业务线，也包括专注于零信任领域的安全初创公司。但由于传统安全企业资源较为丰富，资金也比较充裕，相比而言在市场上占据主导地位。

5.1.4 技术路线和产品形式

在市场上的零信任解决方案中，占据主流的仍然是 SDP 解决方案，这与疫情以来的灵活办公需求增长以及对 VPN 的替代密切相关。几乎所有的零信任厂商都提供了自己的 SDP 产品。同时，在企业研发过程中，也发生技术路线的变更，在 SDP 产品中，有四家厂商目前主打的零信任产品不是首次研发的产品。目前，市场上主要的零信任产品既有软件又有硬件，可以满足不同客户和场景的需求。以下为在本次调查中，零信任各技术路线的占比情况。

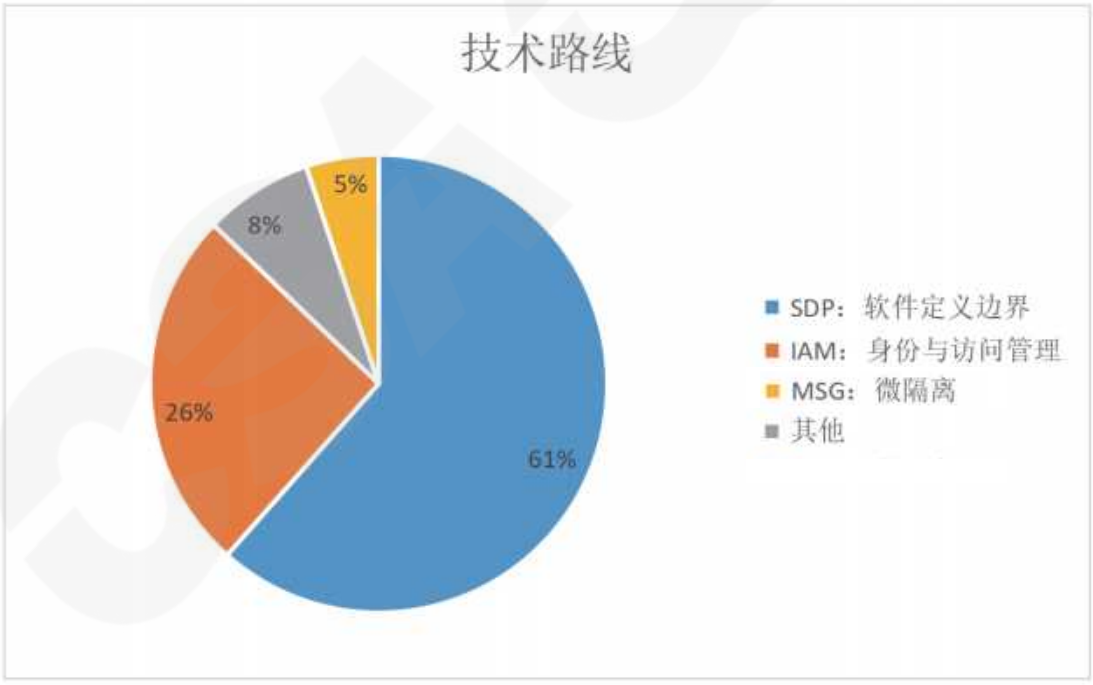


图5-3：零信任产品技术路线占比情况

5.1.5 研发时间

从开始了解零信任理念到着手开发相关产品，再到市场推广，各个厂商经历的时间大不相同。在零信任理念推出不久，就有企业开始着手研发，历时数年。同样，近年来，随着零信任理念的普

及，一些企业的研发速度大大增强，有些企业在不到一年的时间就有零信任产品面市，有企业把一些传统产品加上零信任概念包装，就以零信任的名义在市场上推广，从而导致市场上零信任产品鱼龙混杂，良莠不齐，迫切需要规范化。

从分析可以发现，目前市场上注意主要的零信任产品大部分是在近两年研发的，但也有一些企业在零信任行业研究了多年，某些企业在 2012 年就开始关注零信任，历时 9 年才开发出首款产品。以下为在本次调查中，企业开始研发零信任相关产品至产品上市所需时间。

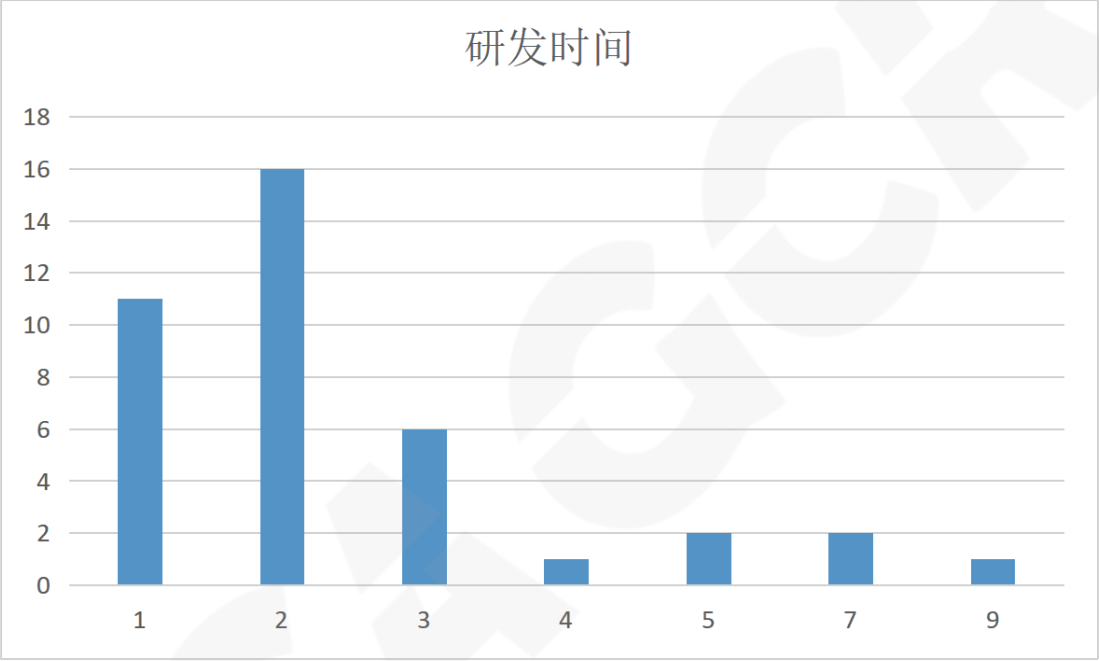


图5-4：企业开始研发零信任相关产品至产品上市所需时间

5.2 技术和市场趋势

在本次调研中，我们发现各个企业都不满足于现有的产品和取得的进展，希望通过进一步研发，提供差异化产品，满足多样化的市场需求。

5.2.1 深入集成

尽管目前大部分的产品都是 SDP、IAM 和微隔离产品，但这些产品很少相通。同时，零信任作为一个独立的产品，与其他安全或 IT 产品缺少集成。因此，一些厂商已经开始规划，提供 SDP、IAM 和 MSG 的一体化零信任方案，从用户端深入细化身份安全权限管理，提升动态授权、持续身份认证的能力，对访问资源的用户身份、设备信息增强合规检测、准入检测等。在服务端对接 MSG，增加策略配置，管控各个服务端流量走向，持续验证流量安全，根本上隔离各个服务间资源，确保企业内部资源防护能力。同时，集成第三方威胁情报系统或终端环境感知平台，更好的做好准入控制和与其它平台的兼容性; 支持将用户行为的日志数据推送给 SOC 或 SIEM 系统进行风险分析，风险信任评估和持续认证将会结合人工智能技术，对用户行为进行持续风险信任分析，利用机器学习技术只能的挖掘用户行为风险，智能的进行风险策略处置，智能的访问控制，实时阻断风险。通过 API 接口和插件引擎可以将更多的安全能力以插件的方式加载到零信任体系里，让安全能力变得像云一样可以生长，可以按需扩展，可以更贴合用户的安全诉求和使用体验。解决方案提供 SDK 实现与已有终端安全体系的融合与集成，实现与企业应用客户端 /App 的融合与集成，减少用户终端客户端的数量。

5.2.2 更多场景

除了常规的企业内部系统接入等应用场景，更多企业开始进入一些目前还没有太多竞争者的蓝海区域。一些企业以数据本体为核心目标，构建数据安全的零信任架构，充分考虑流动数据安全防护，以数据安全治理为前提，形成数据资产清单；结合零信任体系和安全治理成果，基于数据流转路径和现有的数据访问原则和控制策略，规划数据安全策略；继而导入零信任架构，通过全局数据安全态势感知、数据库审计、数据脱敏、数据水印、数据库加密、数据备份恢复等技术手段，对数据全生命周期进行多方位防护，并加强数据防泄漏、云沙箱等细分安全能力。还有一些企业零信任解决方案从满足传统办公应用场景，逐渐向工业互联网、物联网、5G/6G 网络等领域，适配不同网络架构的安全需求，用零信任理念和架构实现目标网络中 IT/OT 的安全闭环。

5.2.3 开放互联

企业在当前产品已有能力基础上，充分开放、实现零信任的融合和扩展能力，建设零信任生态体系，为已有客户提供整体方案能力，保护已建安全系统。通过后端风险检测和信任评估体系，充分将终端安全状态的评估纳入评估体系，研究和建立合理的评估模型，与产业内各合作伙伴深入

沟通，构建完善的零信任业务合作生态产品；尽可能保持开放性和兼容性，能够很好兼容企业现有 IT 基础设施和安全能力，最小化程度的现网改造和安全能力对接，帮助企业在零信任安全底座之上，构建更贴合企业业务和 IT 建设现状及应用场景的专属零信任安全能力。加强业务应用的技术兼容和互联互通，解决互操作性差、兼容率、复用率低的难题。

5.2.4 简洁易用

快速推进“泛端兼容 "，覆盖更多的终端类型。在支持 Windows，macOS，macOS（M 系列芯片），Linux，Android，iOS 6 个平台的各类设备的基础上，扩展覆盖国产芯片与国产操作系统平台。适配更多终端以进行更精准的环境感知，如物联网终端、5G 终端等，提供细致化的识别模型，更精确的定位终端可管控的内容，通过建立终端类型库，分类管理，为动态访问控制提供精准的分类授权，以适配不同类型的终端，拓展零信任理念，从用户终端着手，完善零信任建设，建立全面的零信任防护体系。

通过 AI 与 UEBA 的深度结合，构建以人员、设备、应用、网络、数据为主体的行为建模体系，达成更加细致而全面的持续验证与感知能力。通过 AI 智能推荐各类策略配置，对已生效的安全策略进行评估也优化推荐，实现更精准和灵活的安全策略体系，减轻客户 IT 运维的成本。

将管理平台打造的尽可能的简单易用，让绝大多数 IT 人员都可以轻松上手；另一方面，作为零信任的管理平台，其高可用和稳定性至关重要，结合企业实际应用场景进行安全能力梯度化，真正让零信任管理平台融入到企业的 IT 管理和生产中去，为企业降本提效。

5.3 面临的挑战

- 对数据安全要求较高的用户来说，在实施零信任后，如何评估零信任架构的整体安全性，如何评估零信任架构下的网络安全防护能力，比较难以量化。

- 当前数字化背景下企业大都拥有多个成熟的安全产品堆叠，零信任在被接受和替换的过程中有一定的时间周期，需要与安全产品更好的融合。

- 产品开放性兼容方面还不足，不同厂商产品间存在互操性难、复用率低等问题，产品间兼容性适配性、应用类产品接口的标准化程度均有待提升。

- 在落地一体化零信任理念的过程中，客户需要考虑网络层面、业务层面、IT 层面等多维度的优化需求，落地周期长，复杂度也比较高，因此大多采用分布实施的方式部署零信任方案。实施落地零信任方案周期长。

- 很多资质有企业经营时间、人员规模、营业收入等硬性要求，导致在很多项目中被非技术因素控标，对零信任能力强的中小企业来说也是重要的挑战，限制了部分能力强的中小企业发展。

- 很多甲方客户希望的是大而全的整体方案，采购上以合规为导向而非实际业务需求为导向。

- 市场对于零信任概念的接受程度、对零信任的理解和期望落地后产生的效果千差万别，很难通过一套标准的方案去进行推广落地。

- 外部环境的不确定性逐步提升，不可控的外部因素，如疫情造成的行业整体环境的变化、供需平衡被打破、部分行业发展速度放缓等均对解决方案的落地提出新的挑战。

06 评价方法论

国际云安全联盟大中华区发布的神兽方阵系列遵循相对客观的方法论与评价体制，在本次发布的零信任神兽方阵中，CSA大中华区参考了众多较为成熟的评价方法，同时结合零信任产业在中国国内的实际情况，围绕企业真实数据讨论出客观的评价指标体系，并在此基础上运用模糊综合评价法，建立了综合评价模型。

6.1 公司选择

神兽方阵系列是一套综合企业产品发展路径的体系模型，包括规则分类、象限模型、细分权重等，对企业及企业产品进行发展路径的分级定位，客观评价该企业产品在行业内的状态。

CSA 大中华区综合考虑了企业的行业概况、商业模式、企业竞争力等因素，分别对应各神兽方阵数据模型的入选标准，筛选出具有一定规模，知名度和影响力，或者处于起步阶段但技术实力强和快速成长阶段的企业，进而通过访谈评价分析进一步筛选推荐上榜。

6.2 评价维度

在评价指标上，CSA 大中华区经过多轮筛选，确定了零信任神兽方阵的两个评价维度，多项分类数据模型，并根据分类数据模型下的各个指标因素的重要性，构建了指标判断矩阵。

6.2.1 技术研发评价维度

技术研发能力是零信任领域最主要的竞争因素之一，通过该维度可以反映不同企业对于零信任技术创新的战略趋势，同时也体现了企业的核心技术研发投入程度和产品更新速度，而将技术研发能力作为核心能力的企业，往往具有较强的技术实力，其产主要产品在市场中不断迭代趋于成熟，同样其新产品也往往具有先发优势。神兽方阵在技术研发评价维度中从研发能力、知识产权、产品成熟度等具有代表性的量化指标进行综合评价。

6.2.1.1 研发能力

这一数据模型主要体现企业独立研发的能力以及对零信任产品研发的投入能力，包括研发团队的技术能力、企业在零信任领域的投入情况、零信任产品在公司产品组合中所处的位置，以及公司对该类产品的承诺等因素。此外人员投入情况能够体现企业对零信任产品重视程度，包括了零信任研发人员的数量及占总研发人员的比重等情况。

6.2.1.2 知识产权

这一数据模型主要体现企业在该类产品研发中的技术积累，对于核心技术的掌握程度。知识产权主要包括了专利权、著作权以及销售许可的拥有量，而零信任产品的销售许可更可以有力地证明企业的创新能力，从而获得客户的信任，树立企业品牌。此外企业对于零信任产品研发的专注程度也体现在知识产权与企业的产品（服务）的是否具有强关联性，以及知识产权的迭代路线。

6.2.1.3 产品成熟度

这一数据模型主要体现产品与目前市场的契合程度，包括了企业对零信任产品投入研究的年限、上市时间、产品数量、行业客户及应用场景等众多要素作为参考，其中客户的行业涵盖范围体现了企业产品在各细分市场已具有较高的成熟度。另外对于企业零信任能力后续规划的自述，CSA 将其与企业对于零信任相关技术、应用和产业发展的预测相结合，作为判断企业零信任产品发展潜力的参考依据之一。

6.2.2 市场营销评价维度

零信任技术具有快速迭代的特性，对企业产品更新换代能力提出了更高的要求，能够明锐察觉市场需求并及时推出新产品。所以企业在进行技术研发和产品创新的同时，应重视零信任产品的营销管理，建立完整的产品销售管理体系，并与客户建立长期的战略合作计划，帮助零信任产品适应市场环境，不断提高产品质量和市场竞争力。

6.2.2.1 产品营收

这一数据模型主要体现企业零信任产品上的销售情况，销售情况是最有利证明企业在零信任产品上且能够被量化的竞争力。盈利能力作为市场营销的主要目标之一，企业在零信任产品上的盈利能力与其产品在市场中的竞争水平是强相关的，同样企业零信任产品营收占整体市场的比重以及其所处上下游位置，往往体现了该产品综合能力与市场认可度，另外企业在零信任产品在市场中变化情况作为产品的动态评价能力。

6.2.2.2 客户情况

这一数据模型主要体现企业在零信任产品上的客户管理，主要包括客户满意度、服务能力、新客户开发率、终端持有率等因素。该数据模型主要以使用的组织和用户数两个方面评估企业零信任产品的使用情况，并根据客户的复购率评估产品满足客户需求的程度。此外产品的综合服务能力作为辅助参考依据，体现企业从产品的研发、销售、售后服务等方面为消费者提供的一系列产品增值体验和好感的能力。

6.2.2.3 营销能力

这一数据模型侧面反映企业在零信任产品上的市场投入和重视程度，并结合其他指标反映营销活动的效果。该模型主要包含了企业在零信任产品中的营销投入、营销模式、营销计划等要素，反映了企业在零信任产品品牌建设、产品质量、渠道建设等方面的综合实力。这一模型可以作为分析其他数据指标之间的相互影响的参考依据，进而分析各指标之间的内在相互作用和长期趋势。

6.3 入选标准

根据上述的评价维度，CSA 大中华区首先确立零信任领域中在技术研究、市场产品的被普遍认可的领跑者，以这些头部企业的产品为最高标准，然后建立分级评价体系，将该分级评分纳入四大神兽方阵的入选标准与评价中。

该评价体系将每个维度下的不同数据模型赋予不同分值予以评价。

6.4 评价流程和要求

CSA 大中华区在本次零信任神兽方阵评价过程中遵循严谨、客观的评价流程，以公平、公正、诚信为原则，确保评定结果的合情合理。

6.4.1 专家访谈

为确保问卷质量，由 CSA 专家组与部分头部企业沟通，访谈各企业的管理层、核心技术人员、相关业务人员。从访谈中获取目前企业在零信任产品研发、销售、运维等方面的关注重点，并根据企业对于零信任产品市场的认知与长远认知设计问卷大纲，大纲维度设计由多位行业专家多次讨论最终通过。

6.4.2 问卷设计

问卷设计根据大纲要求进行具体问题的设计与排版，并将不同的问题分开排列，以确保相关问卷结果与相关维度的关联。问卷经过多个企业的先行设测验，CSA 根据测验的反馈与收集的结果对问卷维度包括比较倾向、比较方向、比较动机、比较效果等方面进行了相应的微调，确保数据建模时能够综合体现企业在零信任产品的能力。在上述基础上，采用专家评定法、问卷调查法、内部一致性信度等方法对问卷进行审校，发布最终问卷。

6.4.3 数据收集与评价

通过企业调查和问卷调查，及经过专家讨论分析，将问卷各分指标数据化为数据模型的隶属

度，然后利用数据模型对两个评价维度进行综合评价。同时根据相关企业的实际行业情况对比，结合原始数据验证了模型的可靠性，并对各模型的分类精度进行了比较分析。

6.4.4 情况核实

对所有问卷的结果进行严格复核后，采用双录入的方式将数据（包括数据表与验证文件）录入神兽方阵的计算模型中，形成企业的神兽方阵的初步定位。CSA 根据初步的入选情况对每一家入选企业对数据进行核对与材料的补齐，对未入选企业实际情况的数据及时提出调整意见，并按程序重新提报、修改，确保数据可靠、准确、完整。

07 展望

从调研的反馈可以清楚地看到，零信任的安全优势显而易见，对于运营和安全人员在管理以及便捷性方面具备巨大的优势。从 2010 年零信任概念的提出，到今天已经走过了十二个年头，数字化和新冠疫情推动了零信任市场的发展，市场上越来越多的厂商看到了零信任市场的潜力，积极投身到这一市场中来。这些厂商有的是传统的安全厂商，有的是初创公司，无一例外都推出了自己的产品，各具特点。同时，一些厂商也创造性得将零信任技术用于全新场景，例如利用零信任技术进行数据保护。

现在，轻舟已过万重山，零信任技术已经广为接受，有着广阔的前景。我们希望今后可以看到越来越多的厂商推出直接的产品，也希望更多的组织运用零信任产品保护自己的资产，享受这一技术带来的便捷。同时，我们也希望业界可以探索更多可以发挥零信任技术优势的场景。

作为零信任技术的倡导者，CSA 将继续推动零信任技术的发展。由于本研究报告是国际云安全联盟大中华区的首次尝试，瑕疵不可避免。国际云安全联盟大中华区的研究团队在今后会持续优化，进一步改善。同样，我们欢迎广大读者给予反馈，我们可以更好地提升我们的工作。

零信任是一种理念。希望业界同行共同携手，推动零信任社区的健康发展。

鸣谢

感谢国际云安全联盟 CSA 全球会员单位奇安信及云安全联盟大中华区理事单位天融信对《2022 中国零信任神兽方阵》分析报告的赞助支持，但不影响国际云安全联盟大中华区对本报告的编辑权和所有权。

奇安信

新 一 代 网 络 安 全 领 军 者

奇安信科技集团股份有限公司成立于 2014 年，专注于网络空间安全市场，主营业务为向政府、企事业类客户提供新一代企业级网络安全产品和服务。公司凭借持续的创新研发和以实战攻防为核心的安全能力，已发展成为国内领先的基于安全大数据、人工智能和安全运营技术的网络安全产品及服务提供商，同时公司不断扩展国际市场，已在印度尼西亚、新加坡、加拿大等国家开展网络安全业务。此外，奇安信是 2022 年冬奥会和冬残奥会网络安全服务与杀毒软件的官方赞助商，并圆满完成网络安全保障工作，兑现了北京冬奥网络安全“零事故 " 的承诺。

天融信

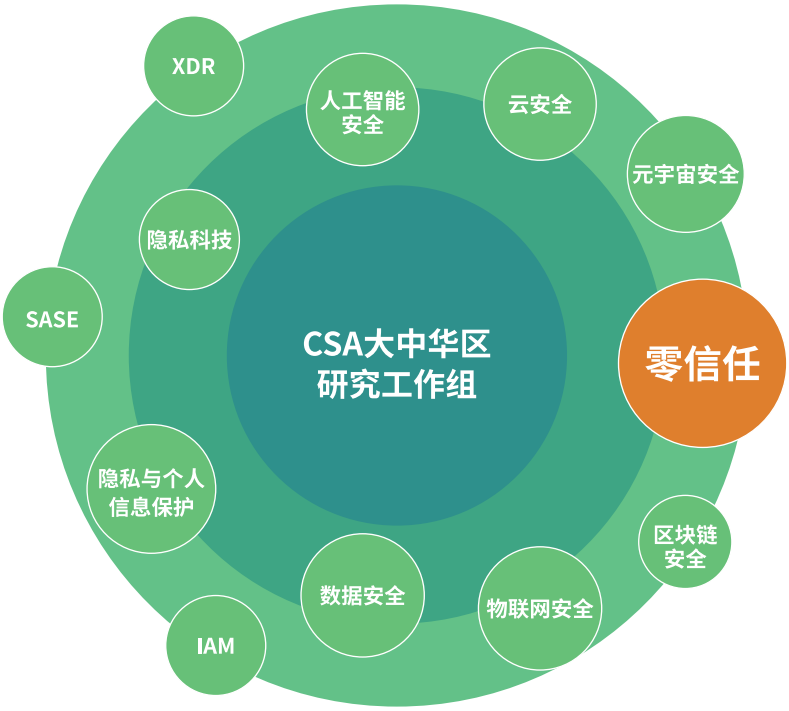
TOPSEC

天融信科技集团创始于 1995 年，是国内首家网络安全企业，亲历中国网络安全产业的发展历程，如今已从中国第一台自主研发防火墙的缔造者成长为中国领先的网络安全、大数据与云服务提供商。天融信始终以捍卫国家网络空间安全为己任，创新超越，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。

关于国际云安全联盟大中华区

国际云安全联盟（CSA）是世界领先的独立、中立、权威国际产业组织，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，以帮助确保安全的云计算和下一代计算环境，是云计算领域的 “ISO”、“ITU”国际标准组织。

国际云安全联盟大中华区（CSA GCR）作为CSA全球四大区之一（其它大区为美洲区、亚太区、欧非区），立足于中国，作为国际桥梁联接世界，致力于构建国际数字安全的生态体系。



10W 个人会员　　**1000+** 企业会员

100+ 国际城市分会　　**6000+** 国际高端专家

企业会员包括：联合国国际计算中心、欧盟网络安全局、中国信通院、美国国家标准和技术研究院等机构，微软、亚马逊、谷歌、华为、腾讯、阿里、IBM、国家电网、顺丰、中兴、工商银行、海尔、联通、奇安信、天融信、深信服、360集团等1000多家企业会员。

中国零信任推进中心

国际云安全联盟CSA作为零信任首个技术解决方案软件定义边界SDP的发明者，零信任倡议者及实践者在构建和传播零信任技术标准 最佳实践和工具方面具有权威性和独特的优势。于2022年，CSA设立零信任推进中心，这对全面提高网络安全基线和消除重大系统性风险具有重大意义。

CSA大中华区在中国设立零信任推进中心，通过研究培训、专业认证、活动、咨询等方式提升企业及人才的零信任实践能力，使企业能够理解并在业务规划、企业架构和技术部署中实施零信任原则。CSA大中华区将联动行业专家 城市分会和学术会议等方面的全球资源能力,助力零信任在中国的创新发展，及输出具有中国的最佳实践。

反馈与合作

CSA大中华区零信任推进中心合作交流

CSA大中华区副秘书长 许木娣 (Melan)
18218024060 melanxu@c-csa.cn

官网地址：https://c-csa.cn

公众号　　视频号

国际云安全联盟大中华区
电话:0755-86548359
官网:https://c-csa.cn
邮箱:info@c-csa.cn

CSA办公室微信　　视频号