零信任实验室
Zero Trust Laboratory

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

TRUSTED SECURITY
可信安全

零信任发展洞察报告

（2022年12月）

版权声明

前　言

近年来，云计算、大数据等新一代信息技术与实体经济加速融合，产业数字化转型迎来发展新的浪潮。数字化在为企业提质降本增效的同时，也为企业 IT 架构带来新的安全挑战，传统安全防护机制遭遇瓶颈，探索适应企业数字化转型需求的新一代安全体系具有重要意义。

零信任理念及架构能够有效应对企业数字化转型过程中的安全痛点，愈发得到行业关注。在此背景下，零信任实验室和云计算开源产业联盟继《零信任发展与评估洞察报告（2021 年）》后第 2 次发布报告。报告基于对重点零信任供应侧企业的调研结果，从零信任发展呈现的四点趋势展开，对我国零信任的发展趋势与供应侧的零信任生态进行观察和分析。一是，在未来，零信任与数字身份密不可分，并向统一整个基础设施的策略管理发展。二是，在零信任供应侧方面，梳理了零信任理念所涵盖的六大能力、供应生态概况、金融行业与电信行业在零信任落地方面的表现，包括：落地零信任用户数量、不同类型的零信任产品应用情况、应用场景与环境等。三是，对零信任产品与身份安全产品、终端安全产品，以及安全管理类产品的联动能力进行调研。最后展望我国零信任产业发展，应从提升技术壁垒避免同质化竞争、强化安全产业供应链间合作、持续强化信创改造、细化实施引导、以及深化行业应用五方面开展。

参与编写单位

中国信息通信研究院、北京蔷薇灵动科技有限公司、腾讯云计算（北京）有限责任公司、联通数字科技有限公司、绿盟科技集团股份有限公司、深信服科技股份有限公司、北京持安科技有限公司、北京芯盾时代科技有限公司、成都云山雾隐科技有限公司、中移（苏州）软件技术有限公司、数篷科技（深圳）有限公司、天翼云科技有限公司、上海派拉软件股份有限公司、江苏易安联网络技术有限公司、贵州白山云科技股份有限公司、北京天融信网络安全技术有限公司、奇安信科技集团股份有限公司、网宿科技股份有限公司、新华三集团、北京从云科技有限公司、广东一知安全科技有限公司、深圳竹云科技股份有限公司、北京指掌易科技有限公司、杭州亿格云科技有限公司、ZTE中兴通信、飞天诚信科技股份有限公司、北京栖安科技有限责任公司、山石网科通信技术股份有限公司、苏州云至深技术有限公司、杭州默安科技有限公司、北京国信融信科技产业有限公司、北京哈希安全科技有限公司、深圳市米特信息科技有限公司、广州锦行网络科技有限公司

编制人员

吴倩琳、栗蔚、孔松、郭雪、陈镇东、熊瑛、王丹、邹艳鹏、谌鹏、张慧莹、杨志刚、姚坤、何艺、季文东、曾帅、杨一飞、严益昌、王肖斌、张羽、王鑫渊、刘羽、左奕航、张丽婷、许博文、汤冰洁、赵菁菁、赵培、程君、秦忠鹏、李沂航、史晓婧、王杰、王璐瑶、侯芳、崔石磊、廉秀苓、张建伟、崔芙蓉、张秀岩、宋园园、亚米、黄佳妮

目 录

图 目 录

表 目 录

一、 零信任发展备受关注

1. 零信任发展呈以下四点趋势

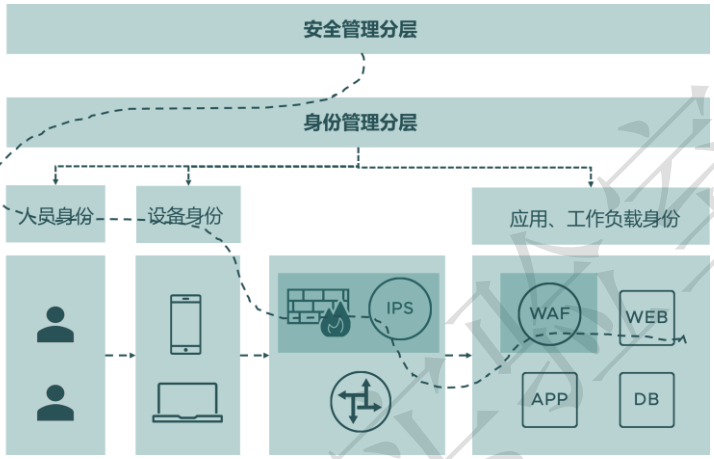
1.1 零信任产品形态向大而全的平台化、集成化演进

零信任从为企业解决部分安全问题向解决整体的网络安全问题发展，向架构性的平台前进。一方面，当下企业选择零信任主要解决数据中心网络安全接入的问题，但随着企业云计算使用规模逐步提升，安全边界的粒度逐步细化，安全风险不再以网络分隔出的安全域为维度划分，而是以访问的业务为维度进行划分，仅解决网络安全接入并不能满足业务安全需求，需要贴合业务的身份以解决业务访问全链路的风险，从而缓解整个企业网络的安全问题。**另一方面，**安全本身在企业中是一种横向的能力，集成的、聚合的安全能力可形成平台化的、中台化的产物，基于零信任理念的架构性平台可在身份安全、终端安全、数据安全、网络环境安全、工作负载安全等方面提供全方位的防护。

1.2 身份管理分层之上与更多安全能力结合

零信任是为了应对基础设施的变化、为了应对无边界化后网络安全威胁而出现的手段，零信任基于访问主体身份为访问过程提供全链路的安全保障，如图 1 所示。**一是建立身份管理分层。**零信任在逻辑上建立了一张基于身份的网络，赋予人、设备、工作负载等实体唯一身份标识，基于身份对访问主体进行动态访问控制。**二是在身份管理分层之上建立安全管理分层，将更多的安全能力进行编排。**传统安全

工具缺乏访问主体身份识别能力，如防火墙仅能识别访问主体 IP，然而 IP 并非访问主体唯一身份标识，因此诸如防火墙一类的传统安全工具无法确定访问主体身份。零信任架构下将传统安全能力与身份管理分层共同编排，通过编排链共享身份信息，实现基于身份的安全管理分层，以针对访问过程实现动态访问控制。

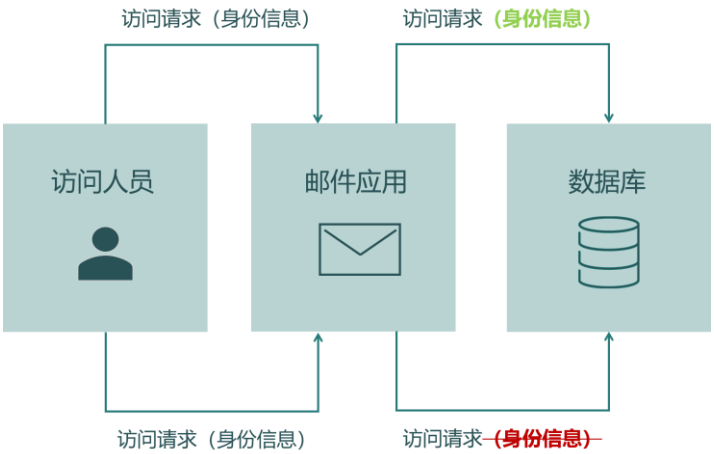


来源：中国信息通信研究院 2022 年 12 月

图 1 身份信息与各类安全工具的事件信息贯通

1.3 身份信息穿透业务访问全程

通过应用改造实现身份信息“穿透”业务访问全程。如图 2 所示，当下应用访问过程中的身份调用是中断的，例如当用户通过零信任网关访问某应用时，前端应用可以识别访问主体的身份，当应用调用后端数据库时，会建立新的会话连接，数据库视角所见是应用在进行服务调用，此时访问过程中的身份调用已中断。零信任架构下，应用应携带访问主体的身份信息对数据库发起访问，数据库的策略决策点将基于身份进行权限和执行策略的判定，默认不信任前端应用。诸如前端应用、后端数据库等检控点都应具备策略执行能力，因此需要对应用进行改造以实现身份信息穿透业务访问全程。

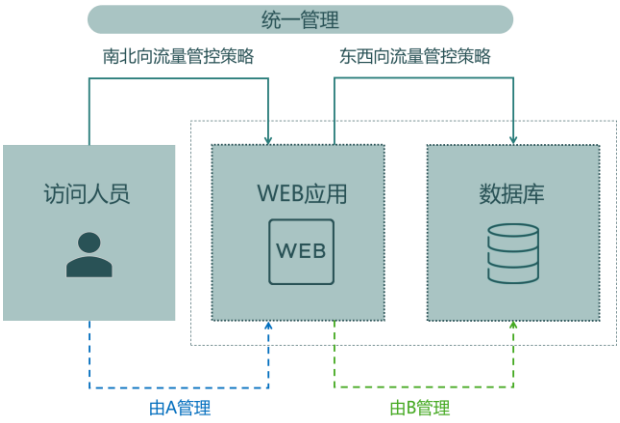


来源：中国信息通信研究院 2022 年 12 月

图 2 身份信息穿透业务访问全程

1.4 南北向流量与东西向流量统一纳管

统一整个基础设施的策略管理，弥补零信任网络访问与微隔离在物理拼接后留下的防护断层。如图 3 所示，物理式拼接易留下潜在安全威胁，例如业务通过零信任网关对外暴露时，Web 服务对外暴露，但后端数据库不对外暴露，所有从外部访问 Web 的流量受零信任网关上相应策略的管控，此处需设计一套面向南北向流量的管控策略；Web 服务与后端数据库通过微隔离进行网络微分段，数据库工作负载需设置限制，仅允许从 Web 服务过来的流量通行，此处需设计一套面向东西向流量的策略。一旦任意工作负载发生变化，两套策略需要同时修改，否则将留下防护断层，为解决上述问题，可统一基础设施的流量策略，通过使用一套策略对全网流量进行管理。



来源：中国信息通信研究院 2022 年 12 月

图 3 统一整个基础设施的策略管理

2. 零信任相关政策与标准涌现，驱动产业规范发展

随着零信任落地及商业模式走向成熟，零信任已逐渐成为政府与企业数字化转型的安全首选战略，各国在近五年都出台了零信任相关政策，以加快零信任部署落地，为数字经济快速发展护航。

以美国为首的发达国家高度重视零信任能力建设。如表 1 所示，自 2019 年起，美国陆续发布零信任指导建议、计划等推动零信任在美落地，其他发达国家也纷纷在零信任领域展开布局，以强化网络空间话语权。2022 年 11 月 22 日，美国国防部发布了 《国防部零信任战略》和《国防部零信任能力执行路线图》，计划在 2027 年之前实施战略和相关路线图中概述的独特的零信任能力和活动。

表 1 国外零信任相关政策

时间	政策发布组织	名称	侧重点
美国			
2019.04	ACT-IAC（美国技术委员会-工业咨询委员会）	《零信任网络安全当前趋势》	对政府机构采用零信任进行评估

2019.07	DIB（美国国防创新委员会）	《零信任安全之路》	指导国防部实施零信任架构
2019.07	DISA（美国国防信息系统局）	《DISA 战略计划 2019-2022》	明确 DISA 网络防御战略重点为零信任
2019.10	DIB	《零信任架构（ZTA）建议》	建议将零信任实施列为最高优先事项
2021.02	DISA	《国防部零信任参考结构》1.0	建议 DoD 下一代网络安全架构基于零信任建设
2021.02	NSA（美国国家安全局）	《拥抱零信任安全模型》	提出渐进式部署零信任方式
2021.05	美国总统拜登	14028 号行政令	发动联邦政府迁移上云使用零信任架构
2021.09	OMB（联邦政府管理和预算办公室）	《美国政府向零信任网络安全原则的迁移》（征求意见稿）	要求各机构在 2024 年前实现具体的零信任安全目标
2021.09	CISA（网络安全和基础设施安全局）	《零信任成熟度模型》（征求意见稿）	细化五个“具体的零信任安全目标”
2021.09	CISA	《云安全技术参考架构》（征求意见稿）	推荐采用零信任辅助迁移上云
2022.11	DoD（国防部）	《国防部零信任战略》、《国防部零信任能力执行路线图》	概述国防部计划如何在 2027 年前在国防部范围全面实施零信任网络安全框架
英国			
2020.10	NCSC（英国国家网络安全中心）	《零信任架构设计原则》	积极响应美国零信任战略，为政企机构实施零信任提供参考
加拿大			

2021.03	加拿大政府部门机构-共享服务部	《网络与安全战略》	采用零信任等新方法支撑未来网络服务
新加坡			
2021.10	新加坡政府	《网络安全战略2021》	要求相关机构实现从边界防护向零信任安全模式转变

来源：公开材料整理

我国加大政策保障，推动零信任落地。目前我国正在从政策、行业实践、产业发展等多个层面对零信任进行积极探索，工业和信息化部通过多种举措引导零信任发展，前期以推动零信任理论研究和技术创新为主，后期加强零信任技术，推动项目落地，具体表现为：**一是，**发布《网络安全产业高质量发展三年行动计划（2021-2023 年）》，重点围绕“加快开展基于开发安全运营、主动免疫、零信任等框架，推动创新技术发展与网络安全体系研发。加快发展动态边界防护技术，鼓励企业深化微隔离、软件定义边界、安全访问服务边缘框架等技术产品应用”等内容展开。**二是，**多个零信任项目在试点示范项目名单上发布，包括“2022 年网络安全技术应用试点示范项目名单”、“2021 年大数据产业发展试点示范项目名单”等。

我国已从多层级启动零信任标准研究，协助建立产业规范。为落实国家网络信息安全相关要求，我国已从多层级开展零信任标准研究。**国际标准方面，**由中国企业主导的 ITU-T（国际电信联盟电信标准分局）零信任国际标准《服务访问过程持续保护指南》正式发布；**国家标准方面**，全国信息安全标准化技术委员会正在开展《信息安全技术零信任参考体系架构》的编制；**行业标准方面**，中国通信标准化协会

正在开展《面向云计算的零信任体系 第 2 部分：关键能力要求》、《面向云计算的零信任体系 第 4 部分：成熟度评价模型》、《面向云计算的零信任体系 第 5 部分：数字身份安全能力要求》与《零信任安全技术参考框架》等标准的研究工作。

二、 供应侧的零信任能力生态逐渐成熟

1. 围绕六大领域能力，建立产品体系

对于网络攻击者，只需要找到整个网络防护的一个脆弱点即可攻破网络，而作为网络安全防护者，需要进行整体的防御。**因此，基于零信任理念展开的安全防护不单独强调技术，而是强调解决了哪个领域的安全问题。**

本报告中，零信任安全能力涵盖六大领域，如表 2 所示：数字身份是基础组件、是核心，联合网络环境安全、终端安全、数据安全、应用工作负载安全和安全管理五个关键能力，共同赋能企业整体安全防御。

数字身份主要解决用户身份不统一，以及 IT 架构中所有对象数字身份缺失、不合法等问题。一是，对接入用户、组织架构、设备、应用赋予唯一身份标识，并对其数字身份进行全生命周期管理，完成身份的自动化管控；**二是**，通过持续的身份认证，确保访问主体在整个资源访问过程中身份的合法性。

网络环境安全主要解决威胁的横向移动，以及传输数据被窃取等问题。一是，将资源划分到一个个微小的网络分段中，分段间通过策

略隔离，阻止威胁的扩散；**二是**，对网络传输链路进行加密，以保证数据传输过程中的安全性。

终端安全主要解决使用移动终端办公难以对设备进行管控，以及不同终端的安全基础不同易引入威胁等问题。一是，加强终端威胁检测，实现终端安全状况可感；**二是**，对所有连入企业网络的移动终端进行纳管，实现 BYOD 可控；**三是**，建立终端基线，对于不符合基线要求的终端可修复。

数据安全主要解决数据资产安全防护无法差异化，以及数据在使用、传输和存储过程中意外泄露等问题。一是，通过数据分类规范化关联关系，再通过数据分级实现数据防护策略的差异化；**二是**，通过数据脱敏、加密、审计等技术手段降低数据泄露的可能性。

应用工作负载安全主要解决两类被访问资源的安全问题，包括容器、虚拟机等基础设施资源，以及应用系统、API 等应用资源。一是，通过安全基线扫描、漏洞管理、入侵检测等技术手段，辅以计算资源纳管清单、供应商名录等管理手段对基础设施资源进行防护；**二是**，在应用研发阶段引入安全检测流程、为已发布应用提供各类恶意攻击防护手段，以及持续验证应用执行的动作是否符合其权限。

安全管理主要解决各安全组件无法联动处置威胁、流量不透明等问题。一是，通过编排将各安全工具的能力以某种逻辑组合在一起，联动进行威胁的检测与响应；**二是**，联动各安全组件并以可视化形式展示监测指标，以便快速定位威胁。

表 2 零信任能力域与能力项

能力域	能力项

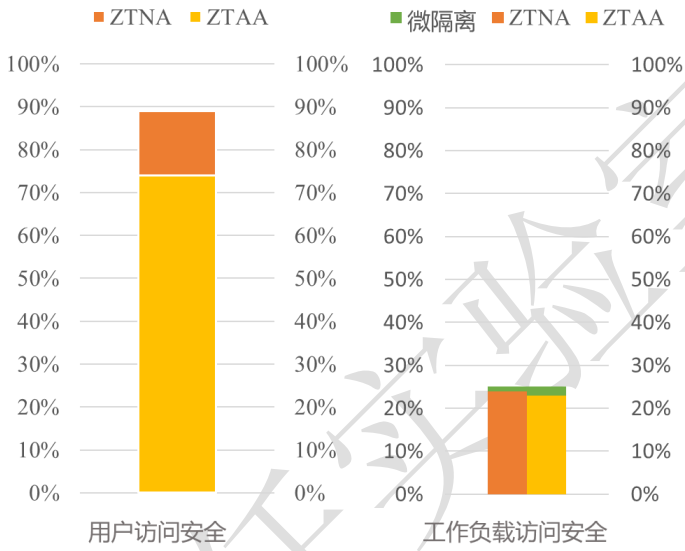
身份安全	身份管理
	身份认证
	访问控制
	身份风险评估
终端安全	终端资产管理
	终端安全基本要求
	终端防护
网络安全	网络隔离
	网络流量加密
	网络威胁防护
应用工作负载安全	计算资源安全
	研发运营安全
	应用威胁防护
	应用访问控制
数据安全	数据分类分级
	数据防泄漏
安全管理	安全编排和自动化
	威胁检测与响应
	安全事件管理

来源：中国信息通信研究院 2022 年 12 月

2. 零信任能力供应生态丰富

用户访问和工作负载访问是产品发展的两条关键路径。用户访问需要对数据中心内外的南北向流量进行访问控制，工作负载访问需要对数据中心内部的东西向流量进行访问控制，两者安全防护位置不同，逐渐形成不同零信任产品。在本报告的调查统计中，如图 3 所示，提供南北向流量安全防护能力的厂商仍占多数，有 89%的零信任供应侧企业可提供 ZTNA（Zero Trust Network Access，零信任网络接入），

对四层流量进行防护；在这些企业中，又有 84%的企业可提供 ZTAA（Zero Trust Application Access，零信任应用接入），可对七层流量进行防护；提供东西向流量安全防护能力的厂商较少，仅有 25%的企业可提供微隔离能力；但是这些企业中，又有 95%和 91%的企业支持以 ZTNA 和 ZTAA 形式提供南北向流量的安全防护。

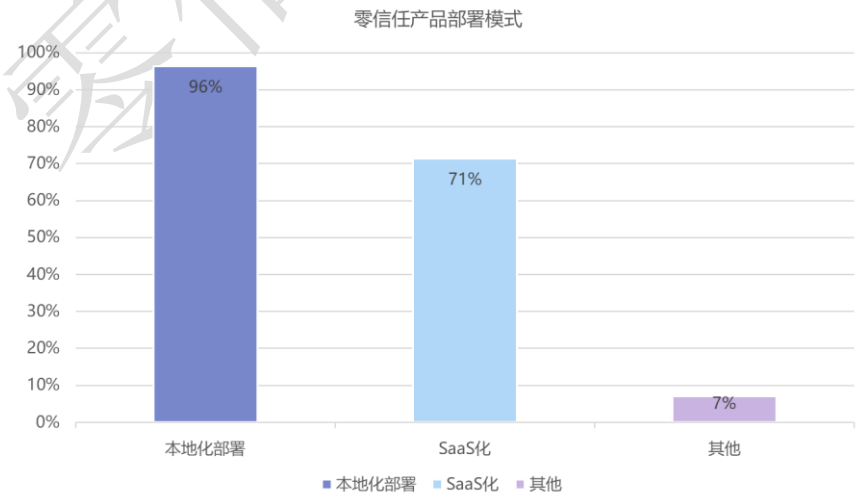


来源：中国信息通信研究院 2022 年 12 月

图 4 我国零信任供应侧发展路径

SaaS 化零信任在国内普及仍面临企业上云比例低等诸多挑战，但已有超七成零信任供应侧企业支持提供 SaaS 化的零信任服务。与本地化部署相比，SaaS 化的零信任有四大优势：**一是标准化交付，**交付更加便捷，普及性更强，适合中小型企业部署，降低用户使用门槛；**二是自身维护成本低，**用户无需部署、维护系统；**三是可利用云网自身优势，**提供安全以外的增值特性，如出海访问加速等；**四是连通性强，**通过云的方式提供接入点，便于对云上业务进行访问。然而，对于国内用户而言，尤其是中小企业，安全需求的刚性尚且不足，“零信任”乃至“安全”都不一定构成“买点”，SaaS 化零信任的推广更

是面临了诸多挑战：**一是国内大部分企业的业务部署在内网，云接入的优势变为劣势，**用户从 POP 点接入再访问数据中心内部业务，存在流量绕圈问题；**二是 SaaS 化产品很难提供业务侧的安全能力，**SaaS 化产品虽然解决了云上业务的网络接入便利性问题，在网络方面提供了安全性，但实际上在安全攻防领域，安全威胁多发生在近业务侧，SaaS 化产品鞭长莫及；**三是无法定制化需求，**企业内部业务环境存在差异性，而 SaaS 化产品提供的标准化产品，在功能适配上难以满足用户个性化需求，尤其在国内头部企业的定制化需求较高。**四是对云上数据安全性有顾虑，**国内多数企业认为公有云上数据不受控难以开展安全保障。本报告对国内零信任供应侧企业的 SaaS 化供应能力进行调查，结果如图 4 所示，有 96.4%的零信任供应侧企业支持本地化部署，有 71.4%的企业支持提供 SaaS 化的零信任服务，即便 SaaS 化零信任产品在国内的普及仍面临诸多挑战，但**国内零信任厂商已有超 7 成在 SaaS 化上进行了投入。**



来源：中国信息通信研究院 2022 年 12 月

图 5 供应侧 SaaS 化情况

自 2021 年起，本报告便已基于选定的六大安全能力，对国内云

厂商、安全厂商以及专精型零信任厂商提供的零信任安全解决方案展开调研，今年是在去年调研的基础上对结果进行了更新，结果如图 5 所示。

企业	产品名称	身份安全	网络和环境安全	应用云工作负载安全	数据安全	终端安全	安全管理
腾讯云计算（北京）有限责任公司	腾讯iOA零信任安全管理系统	●	●	●	●	●	●
北京天融信网络安全技术有限公司	天融信零信任SDP控制器系统	●	●	○	●	●	●
奇安信科技集团股份有限公司	奇安信零信任安全解决方案	●	●	●	●	●	●
绿盟科技集团股份有限公司	绿盟科技零信任安全解决方案	●	●	○	●	●	●
北京蔷薇灵动科技有限公司	蔷薇灵动蜂巢自适应微隔离安全平台V2.0	●	●	●			○
深信服科技股份有限公司	零信任访问控制系统aTrust/零信任安全办公解决方案	●	●	●	●	●	●
华为云计算技术有限公司	应用信任中心ATC	●	○	●	○		○
阿里云计算有限公司	办公安全平台SASE	○	●	●	●	○	●
杭州安恒信息技术股份有限公司	零信任数字化安全接入平台（AiTrust零信任网络安全解决方案）	●	●			○	○
成都云山雾隐科技有限公司	端隐SDP	○	●	○	○	○	
江苏易安联网络技术有限公司	易安联EnIAM零信任身份管理平台	●	●	○	○	●	●
贵州白山云科技股份有限公司	应用可信访问（Access）	●	●	○	○	○	●
浪潮云信息技术股份公司	浪潮云御零信任控制系统	●	○	○	○	○	○
珠海市一知安全科技有限公司	山河零信任云办公系统	○	●		○	○	○
启明星辰信息技术集团股份有限公司	零信任SDP	○	●	○	○	●	○
北京持安科技有限公司	持安零信任平台 持安零信任办公安全解决方案	●	●	○	○	○	○
网宿科技股份有限公司	网宿安达SecureLink	●	●	○	○	●	●
北京芯盾时代科技有限公司	零信任业务安全平台	●	●	○	●	●	○
北京指掌易科技有限公司	灵犀SDP零信任网关	●	●	○	○	●	●
北京火山引擎科技有限公司	零信任安全（内部使用）	●	○	○	○		○
北京百度网讯科技有限公司	零信任安全解决方案	●	○	○	○	○	○
中国移动通信集团浙江有限公司	浙江移动算力网络SASE安全服务	○	○	○	○	○	○
北京京东尚科信息技术有限公司	零信任框架	●	○	○	●	○	○
新华三技术有限公司	新华三零信任安全解决方案	●	●	○	○	●	○
上海派拉软件股份有限公司	一体化零信任安全平台	●	●	○	○	○	●
杭州默安科技有限公司	默安ZTA	●	●	○	○		●
广州赛讯信息技术有限公司	INFOSENSE零信任网关 / SMS安全控制系统	○	●	●			
北京栖安科技有限责任公司	栖安零信任安全访问控制系统	○	●	○	●	●	○
中航金网（北京）电子商务有限公司	航空工业商网安全云	●	○	○	○	○	○
北京安天网络安全技术有限公司	智甲云主机安全系统，智甲容器云安全系统，智甲终端防御系统	○	○	●	○	●	○
深圳竹云科技股份有限公司	竹云零信任安全访问平台	●	○		○	○	●
中孚信息股份有限公司	零信任安全防护	○	○		○	○	
北京哈希安全科技有限公司	哈希安全云	○	○	○	○	○	○
北京华瀛安盛科技发展有限公司	零信任安全互联	●	●			○	○
数篷科技(深圳)有限公司	零信任终端安全工作空间DACS、零信任应用访问网关 DAAG、增强型零信任安全框架HyperCloak（凌界）	○	●		●	●	○
北京志凌海纳科技有限公司	Everoute	○	●	●			○
杭州亿格云科技有限公司	零信任办公一体化解决方案	●	●	○	●	●	●
思特沃克软件（北京）有限公司	零信任架构安全解决方案	●	●		○	●	○
深圳市智安网络有限公司	智安网络零信任安全平台	●	●		○	●	●
肃特（北京）信息技术有限公司	迈格网络即服务MagADN和MagEVN	●	●			●	●
杭州天谷信息科技有限公司	零信任解决方案	●					
山石网科通信技术股份有限公司	山石网科零信任访问解决方案	○	●		○	○	●
北京从云科技有限公司	DAS智能接入/DAS终端微隔离/DAS API访问控制/DAS物联接入安全/DAS数据库访问控制	●	●	○	●	●	○
苏州云至深技术有限公司	零信任安全接入	○	●	○	○	○	○

● 核心产品　○ 涉及产品

来源：中国信息通信研究院 2022 年 12 月

图 6 供应侧零信任安全能力

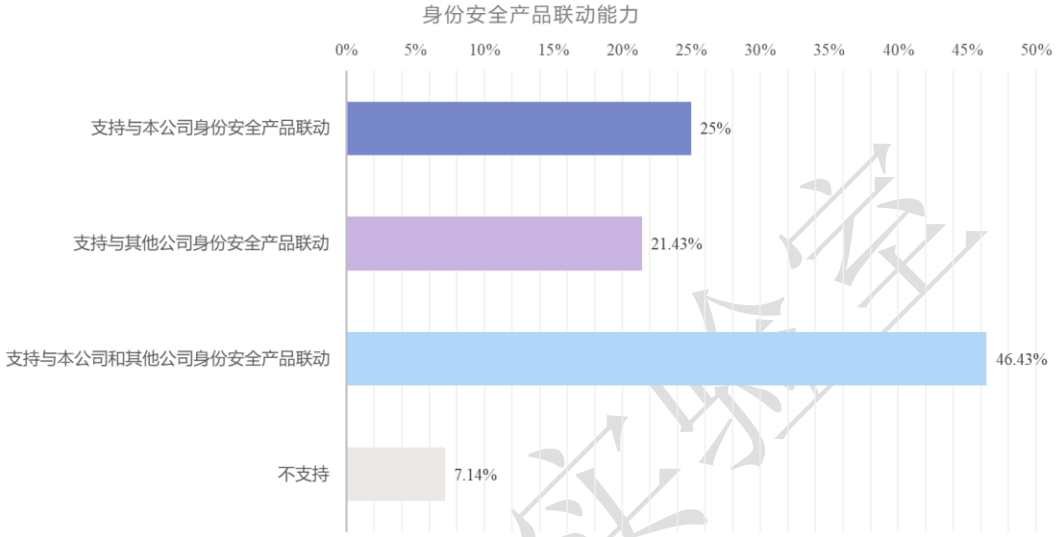
国内零信任赛道竞争激烈，各家都在不同领域寻求新的突破。一是在端上实现更多安全功能。越来越多的客户希望通过一个客户端解决 PC 终端安全的问题，端上安全检测能力、防泄漏、漏洞修复等备受重视。**二是在端上建立可信安全环境以保护数据安全。**疫情之后，远程办公需求增多，移动终端上访问企业业务数据成为刚需，通过软件定义边界与终端沙箱相结合的方式，将零信任的能力延伸至端上成为一种新的解决方案。

3. 持续提升产品联动能力，加快与现有架构融合

零信任与企业已有的安全防护能力应该能相互融合，企业已有的安全工具不应因零信任的使用而失效，而应该得到能力的提升。零信任控制引擎为了更精准地下发策略，应与企业环境中的身份安全类、安全分析类、终端安全类产品进行联动：

身份安全类包含身份管理与身份认证能力，**一方面，**零信任从身份源同步用户身份，建立用户身份与访问过程中使用的设备、访问的资源、访问行为等之间的联系，形成用户画像；**另一方面，**零信任可以将身份认证与多源评估结合实现动态地认证。本报告调研了零信任供应侧企业的产品与用户环境中的身份安全产品联动能力，结果如图 6 所示。**超七成零信任供应侧企业支持与第三方身份安全产品对接。**46.4%企业可提供自研身份安全产品，同时其零信任产品支持与第三方身份安全产品如竹云、派拉、亚信、芯盾、格尔、吉大正元、金智等进行对接；有 21.4%企业不具备自研身份安全产品，但支持与第三方身份安全产品对接；有 25%企业仅支持客户使用自家提供的身份安

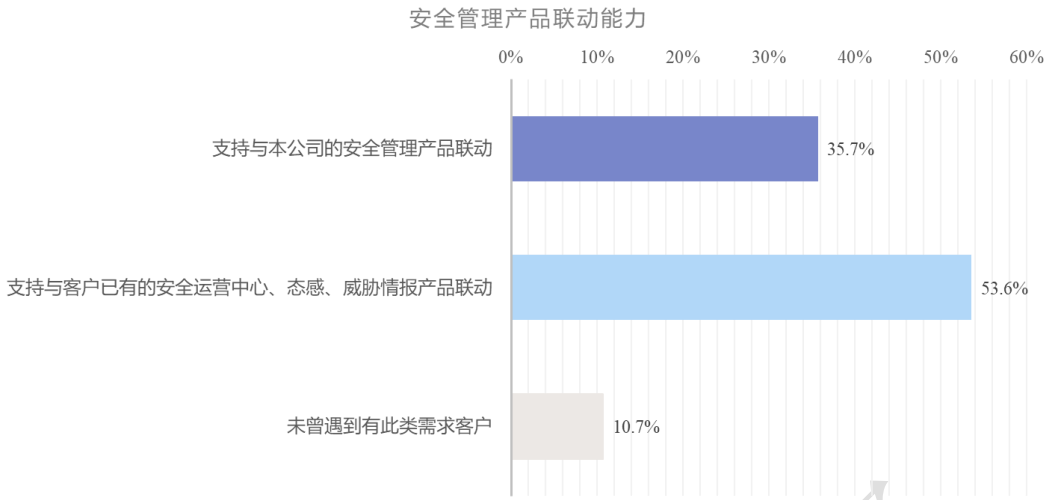
全产品，还有 7.1%企业无法与客户环境中已有的身份安全产品进行联动。在身份安全产品展开投入的零信任供应侧企业占比超过 70%，反向说明同质化竞争激烈，并非每家都能将零信任安全领域做全，各家应避免同质化竞争建立技术壁垒以实现合作共赢。



来源：中国信息通信研究院 2022 年 12 月

图 7 身份安全产品联动情况

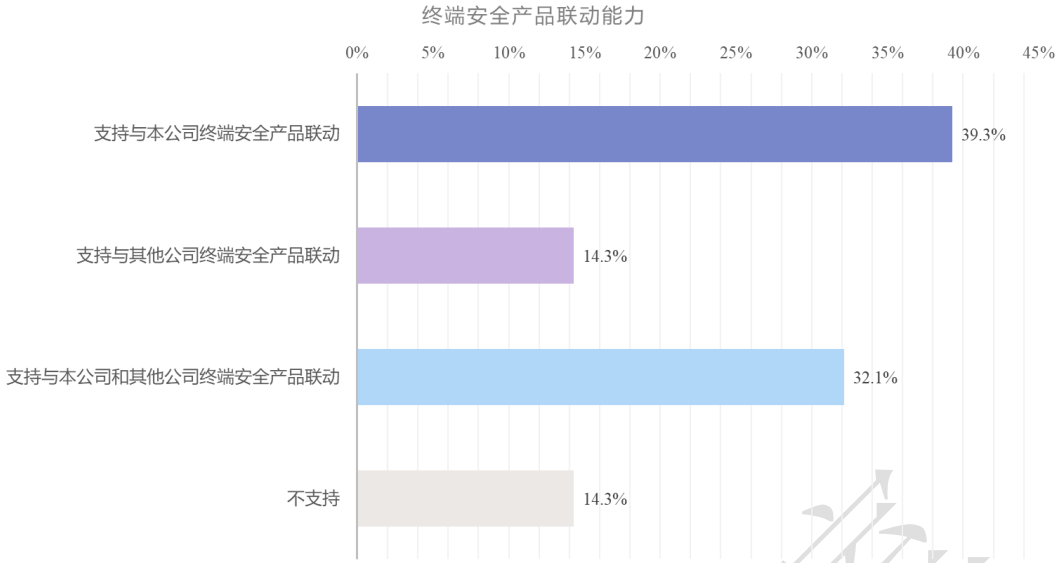
安全管理类包含安全事件和信息的汇聚、实体行为分析、威胁检测与响应等能力，**一方面，**通过与实体行为分析工具结合可获取更多安全风险信息，对访问主体的评估将更加准确；**另一方面，**零信任和威胁检测与响应工具的结合为策略执行提供了更丰富的管控手段。本报告调研了零信任供应侧企业的产品与用户环境中的安全分析产品联动能力，结果如图 7 所示。**超半数企业的零信任产品支持与客户已有的安全运营中心、态势感知、威胁情报等安全分析系统联动**，占比 53.6%，也有 35.7%的企业仅支持与自家的安全分析系统进行联动，有 10.7%的企业尚不支持与安全分析系统联动。



来源：中国信息通信研究院 2022 年 12 月

图 8 安全管理产品联动情况

终端安全类包括终端安全检测与修复、以及数据安全等能力，**一方面，**收集终端环境信息，并根据检测结果对终端进行管控；**另一方面，**通过技术手段实现数据不落地，以保护数据安全。本报告调研了零信任供应侧企业的产品与用户环境中的终端产品联动能力，结果如图 8 所示。**零信任供应侧企业在终端安全展开投入的较多，与第三方对接率较低**。尤为明显的一个数据是支持与自家终端安全产品联动的企业占比 39.3%，这一数据在身份安全领域为 25%，一方面说明终端安全的重要性，供应侧企业纷纷展开投入，另一方面说明与第三方终端安全产品的对接仍面临接口协议无法统一的困境；支持自家与第三方如腾讯、北信源、安天、奇安信、深信服、启明星辰、青藤等企业的终端安全产品进行对接的仅占比 32.1%；此外也有**超七成零信任供应侧企业支持提供终端安全产品**，零信任供应侧企业在终端安全的投入超过安全管理类产品与身份安全类产品，主要原因是身份认证与身份管理所使用协议具有国际、国家标准，然而终端安全领域存在标准协议缺口，有待通过生态间接口互认解决。



来源：中国信息通信研究院 2022 年 12 月

图 9 终端安全产品联动情况

三、 行业应用不断深化，零信任市场步入成长期

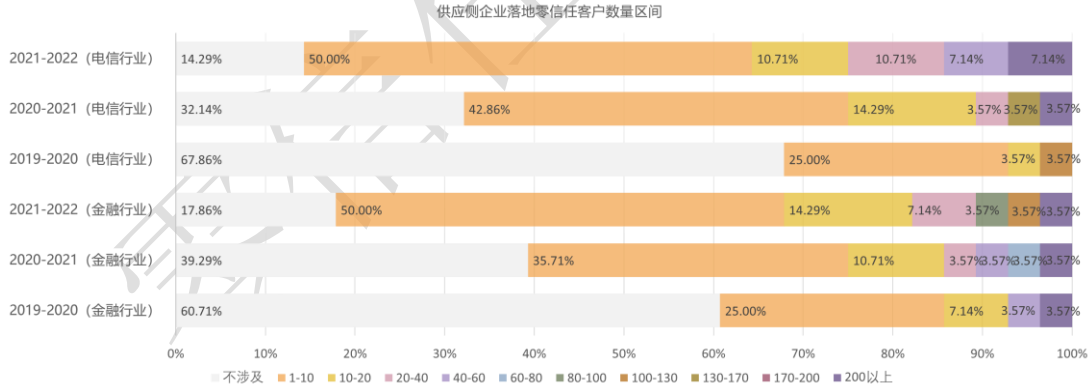
1. 零信任市场近三年呈持续增长态势

经过多年发展，零信任商业模式走向成熟，市场逐步规模化，已经在各个行业进入落地阶段。在 2022 年，以 VPN 替换为主要目标，国内的零信任供应商在用户侧拥有了一个切实落地的卖点。同时，在今年的安全攻防行动中，零信任防护效果优异，得到了众多企业的认可。在未来，会有更多企业选择零信任作为其安全防护架构。

金融与电信行业在近三年落地零信任的客户逐年增长。本报告调研了 2019 年至 2022 年三年间，零信任供应侧企业服务过的金融客户数量区间，结果如图 9 所示。**一方面，在金融行业**，2019-2020 年间仅有 39.2%零信任供应侧企业为金融客户落地过零信任，这一数据在 2020-2021 年间与 2021-2022 年间分别达到了 60.7%与 82.1%，**越来越多的金融机构认可零信任架构所提供的安全防护能力。另一方面，在**

电信行业，2019-2020 年间仅有 32.1%零信任供应侧企业为电信客户落地过零信任，与金融行业相比低 7.1%，这一数据在 2020-2021 年间与 2021-2022 年间分别为 67.9%与 85.7%，**电信行业在近两年落地势头较猛，超过金融行业。**

落地 10 家以内的零信任供应侧企业占据主流，多数行业用户仍处于应用研究探索阶段。据调研，三年间落地用户数量区间 1-10 的企业分别占比金融行业为 25%、35.7%和 50%，电信行业为 35%、42.8%和 50%。也有一些行业专精型的企业存在客户量超过 200 的情况，三年间在金融行业的占比分别为 3.5%、3.5%和 3.5%，电信行业占比分别 0%、3.57%和 7.14%。可以看出，2020 年零信任才开始在国内安全圈中得以普及，产品经过两年的打磨，用户对这个理念有了初步了解，开始积极的在此领域展开采购。

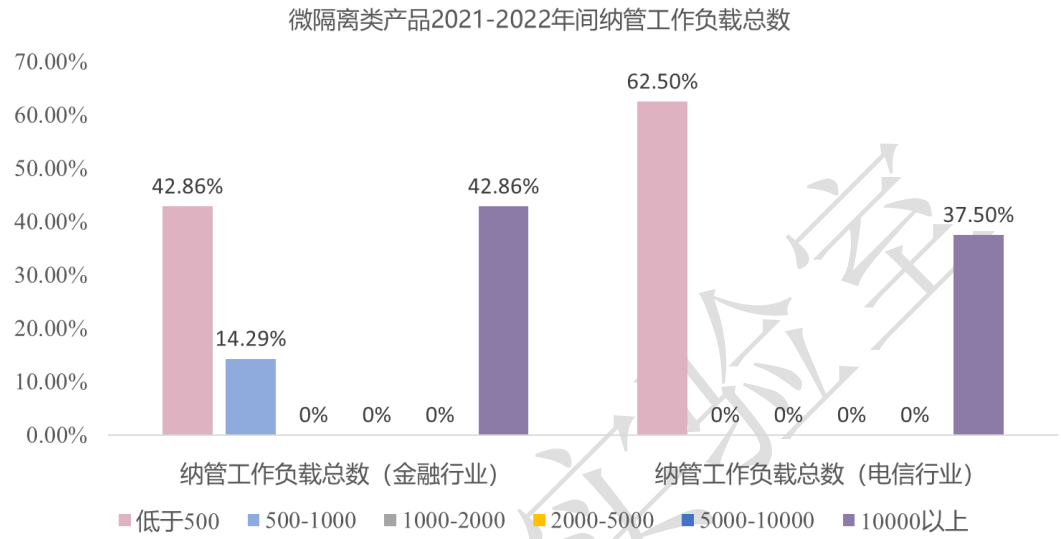


来源：中国信息通信研究院 2022 年 12 月

图 10 供应侧企业落地零信任客户数量区间

微隔离类产品应用情况呈两极分化，与行业相关性较低。本报告调研了 2021-2022 年间，提供微隔离类产品的零信任供应侧企业所纳管用户的工作负载总数，结果如图 10 所示。在支持提供微隔离能力的企业中，金融行业纳管工作负载总数低于 500 的占比 42.8%，高于

10000 的占比 42.8%，电信行业表现类似，纳管工作负载总数低于 500 的占比 62.5%，高于 10000 的占比 37.5%。将近半数供应侧企业的微隔离在行业内仅开展试点工作或未曾开展，同时也有近半数企业在行业内进行了规模化的落地实践。

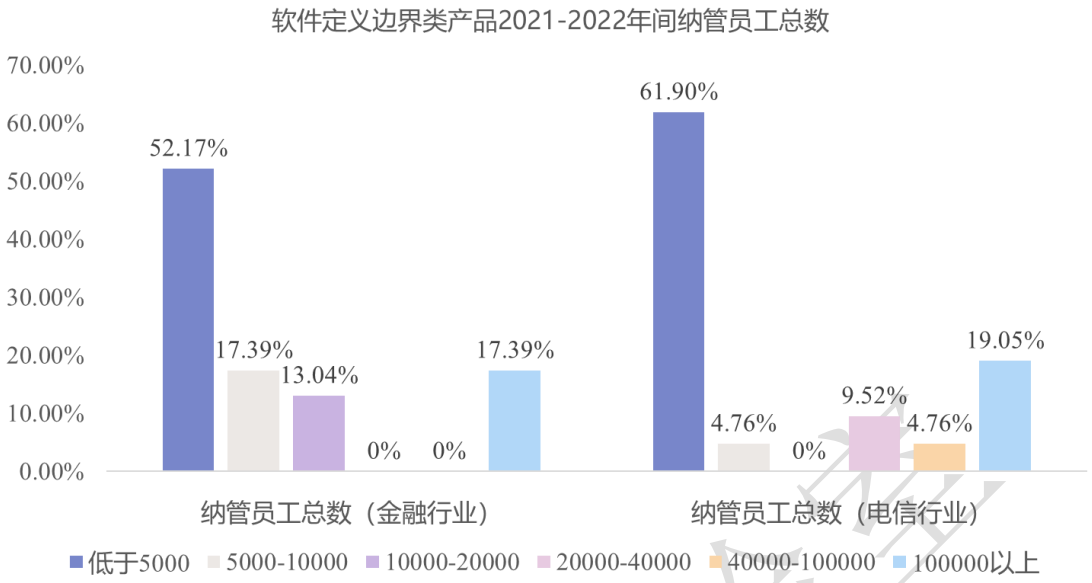


来源：中国信息通信研究院 2022 年 12 月

图 11 微隔离类产品纳管工作负载总数

软件定义边界类产品应用潜力大，头部客户已进入探索阶段。本报告调研了 2021-2022 年间，提供软件定义边界类产品的零信任供应侧企业所纳管用户的员工总数，结果如图 11 所示。在金融与电信行业中，纳管低于 5000 人占比最高，分别为 52.2%和 61.9%，剩余半数涵盖 5000-100000 不等，再结合对零信任落地客户数量的统计结果，即在 2021-2022 年间金融与电信行业均有 50%零信任供应侧企业落地客户数区间为 1-10 家，推算每个客户使用基于软件定义边界纳管员工数量低于 500 人，甚至更低。500 人已属于中型企业，因此各行业内的中型企业应是落地软件定义边界类产品的中流砥柱。此外，在电信行业纳管员工 20000 人以上的占比 33.3%，金融行业仅有 17.4%，

电信行业在零信任领域的投入与落地势头相较金融行业略高一筹。

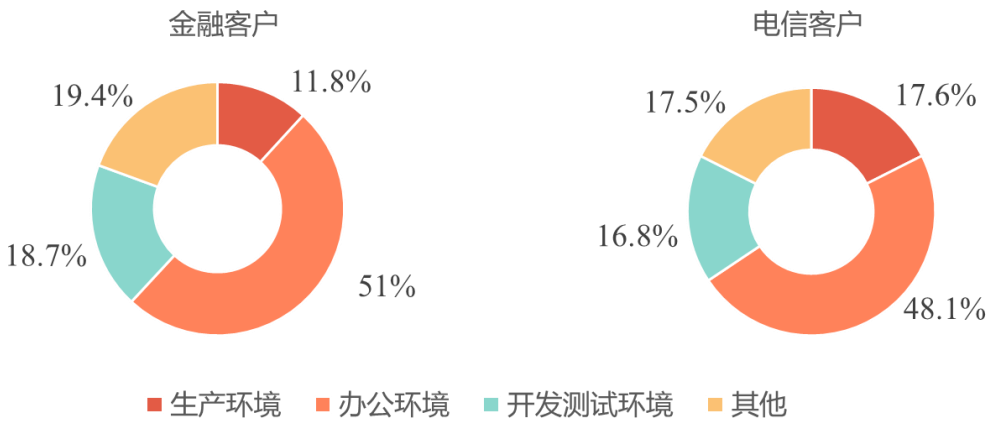


来源：中国信息通信研究院 2022 年 12 月

图 12 软件定义边界类产品纳管员工总数

2. 不同应用场景逐步实现零信任落地

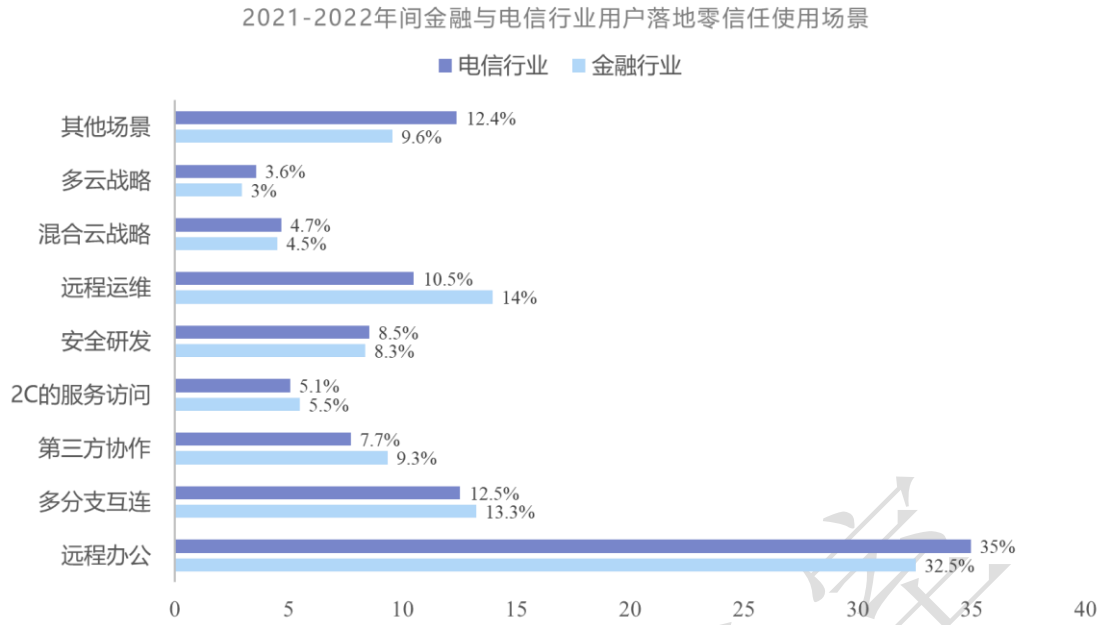
将零信任应用于办公环境是用户主流选择。本报告调研了零信任供应侧企业服务的金融与电信行业客户应用零信任时的环境选择情况，如图 12 所示。金融行业 51%应用于办公环境，18.7%应用于开发测试环境，仅有 11.8%应用于生产环境。电信行业 48.1%应用于办公环境，17.6%应用于生产环境，16.8%应用于开发测试环境。金融行业生产环境承担了核心账务系统的运营，数据资产安全稳定性尤为重要，在生产环境的应用更显谨慎。



来源：中国信息通信研究院 2022 年 12 月

图 13 零信任应用环境情况

远程办公、远程运维、多分支机构互连为用户主要使用的场景，总占比超过半数。本报告调研了金融与电信用户落地零信任时使用的场景，分布如图 13 所示。**一方面，**远程办公场景是当前企业实施零信任的主要驱动和优先选择，在金融与电信行业占比分别达到 32.5%和 35%，其次是远程运维和多分支互连，金融行业远程运维场景占比 14%较多分支互连场景的 13.2%略多一些，电信行业远程运维场景占比 10.5%较多分支互连场景的 12.5%略少，电信行业在多分支互连的需求上较金融行业更高一些。**另一方面，**多云、混合云战略是当前企业实施零信任最少场景，金融行业使用多云、混合云场景占比仅 3%和 4.5%，电信行业分别为 3.6%和 4.7%，大多数企业不具备在云原生环境中的治理能力和安全能力可能是企业迟迟难以大规模上云的主要原因，零信任可以提供此场景下的安全访问，未来多云、混合云场景蕴含较多发展机会。



来源：中国信息通信研究院 2022 年 12 月

图 14 落地零信任使用场景情况

四、 我国零信任产业发展展望

提升技术壁垒避免同质化竞争。当前我国有非常多的零信任供应侧企业，一旦企业提供能力相似，同时针对技术不具备深入突破能力，就会产生泡沫，市场将会在恶意竞争下变得不健康。当下，对于用户的简单场景和轻量需求已经基本可以覆盖，要将零信任向整个企业安全防护架构、向更复杂的业务场景推进，就必须要从底层技术做出深度创新。

安全产业供应链间合作有待强化。目前，我国安全产业内各主体围绕各自擅长的领域发挥着推动产业发展的重要作用，但彼此间的协作尚有欠缺。报告调研的零信任供应侧企业在身份安全与终端安全的对接能力上，在国内已有较多成熟的身份安全与终端安全产品的情况下，现有超七成企业基于自身产品体系研发了相关产品，且有相当大一部分企业的零信任产品只能与自研身份安全、终端安全进行联动，

在产业链的技术合作方面意愿较弱。以零信任为加速引擎，加强我国安全产业主体间的协作，有助于打造繁荣共生的零信任产业生态。

信创改造需持续深入。为提升我国在安全领域的核心竞争力，零信任供应侧企业已持续在国产操作系统适配、国密算法支持等维度开展了改造与适配工作。但存在强调运行环境适配改造，而忽略系统性开源研发框架风险的问题，因此，需针对零信任产品所涉及的开源框架风险应做好预案，梳理潜在的限制供应、停止更新、闭源等风险并找寻替代方案。信创是我国信息化建设的关键环节，而零信任作为网络安全领域的热点，其信创工作的深层次推进将为我国网络安全产业的发展提供有效借鉴。

零信任成熟度评价模型为用户实施零信任提供细化帮助。我国零信任相关标准建设已初步成型，规范零信任应具有的关键能力，但零信任理念的实施不仅是平台工具的建设，更是思维文化的变革。在零信任的落地实施层面，企业需要制定零信任的战略规划，具备可驱动战略的组织力量，以及战略实施所需保障，这与企业整体的经济基础、组织架构规划业务发展等方面强相关，并且是一个分步实施并持续优化的过程，零信任成熟度评价模型对部署过程与目标进行描述，针对零信任的落地提供了更加细化的指引。

鼓励试点示范，深化行业应用。政务、金融、电信、工业等行业业务场景各有特色，如政务通常使用多租户统一接入场景，省级单位管理政务云，下属的若干企事业单位以租户形式入驻，管理自己的用户和安全策略。电信行业通常落地多分支互联场景，通过连接省内多

个分支，从而实现资源共享。金融行业通常落地第三方协作场景，解决第三方运维人员有多账号下的安全接入问题。即便是相同场景，在不同行业落地也具有不同行业特色，为鼓励行业试点示范工作，中国信通院开展了安全守卫者计划，甄选一批成熟度高具有代表性的零信任优秀案例，鼓励零信任供应侧企业结合行业安全需求不断升级产品。

零信任实验室

“2021 年可信云大会”上，中国信通院牵头成立**零信任实验室**，致力于推动零信任标准和测试评估体系建设，引领零信任产业健康有序发展。零信任理念秉持“从不信任，永远验证”，以身份为核心，对所有访问请求进行持续动态的身份验证和最小权限授予，将风险面尽可能收敛，为企业数字化转型安全建设提供思路和手段。

目前，零信任实验室正开展零信任关键技术探索、标准预研、测试评估实施、专家研讨与行业交流等工作。截止于 2022 年末，实验室成员共 66 家单位，包括 1 个理事长单位，8 个副理事长单位，57 个成员单位。

零信任实验室

Zero Trust Laboratory

联系我们：

吴倩琳 | 开源和软件安全部

云计算与大数据研究所 | 中国信息通信研究院

邮箱：wuqianlin@caict.ac.cn

电话：13436559311

可信安全