特殊研究

中国网络安全市场新趋势——零信任市场研究

Austin Zhao

IDC 观点

《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》在 2021 年 3 月 12 日正式发布，纲要中强调“加快数字化发展 建设数字中国 ”，再次彰显了中国政府推动数字化发展的决心，数字化转型已经成为中国各个行业都在加速发展的重要进程。IDC 认为，虽然受全球新冠肺炎疫情影响，2020 年中国数字化转型投资增长有所放缓，但仍保持 12.8%的增长。IDC 预测，到 2022 年，中国 65%的 GDP 将由数字化推动，经济将走上深度数字化之路。

IDC 通过对大量企业 CIO 的调研发现，在应对新冠肺炎疫情过程中，数字化转型较为领先的企业抗“疫”能力明显更强，工作资源转型领先的企业远程协同能力更好，整体工作效率更高。因此，经历此次新冠肺炎疫情后，企业管理者更为直观地感受到数字化转型的重要性，企业预防不可抗力的忧患意识将明显增强。同时，随着云计算、大数据、移动互联网、物联网、5G 等技术广泛应用到企业信息化建设和业务发展中，远程办公、业务协同、分支互联等业务需求快速发展，企业的员工、设备、合作伙伴以及客户需要通过多种方式灵活接入企业业务系统，以提高工作效率、增强用户体验，而无需考虑这些系统是位于企业内部网络、云平台还是开放网络环境，企业原有的网络边界逐渐泛化。

与此同时，全球各行各业不同规模的企业所面临的来自互联网和企业内部的网络恶意威胁从未减少。一旦遭受网络攻击，企业不仅需要花费大量的精力修复网络攻击造成的系统损坏、数据丢失、数据泄露等问题，还要投入大量资源挽回由于遭受网络攻击而失去的企业信誉。如何在提升业务响应速度和敏捷性的同时确保系统和数据的保密性、完整性和可用性是摆在所有企业面前的重要挑战。正因如此，零信任理念在其被业内提出并在谷歌的 BeyondCorp 实践落地后，得到了安全厂商及最终用户的广泛关注和认可。美国国家标准与技术研究院（NIST）发布的《零信任架构》对零信任的概念和逻辑组件进行了详细介绍，并成为国内外企业构建零信任架构时的重要参考。2021 年，美国国家安全局（NSA）发布关于零信任安全模型的指南《Embracing a Zero Trust Security Model》，再次强调零信任的实施不可能一蹴而就，并在零信任成熟度模型中将零信任的发展路线划分为初始准备阶段、基本阶段、中级阶段、高级阶段。

根据 IDC 的调研，疫情期间，因为企业用户开始不断要求工作场所中的 IT 体验可以等同或优于私人环境中的 IT 体验，但是传统 VPN 远程解决方案存在缺陷，所以 VPN 问题成为了企业 IT 投诉的第二大来源。因此，IDC 提出软件定义安全访问（SDSA）的概念。IDC 认为，软件定义安全访问是一种新的访问安全和控制解决方案，包括软件定义边界（SDP）、身份感知代理（IAP）和 Internet Overlay。SDSA 为认证用户和授权应用程序建立基于上下文感知、身份感知和设备感知策略的安全连接。SDSA 解决方案摒弃了静态的网络边界，更适用于数字化转型的组织。SDSA 建立在以应用和用户为中心的分布式完整性原则以及最小权限访问基础之上，从而阻止未经认证的用户连接，或者向未经授权的应用程序发送任何网络流量。IDC 预测，到 2023 年，由于传统 VPN 远程访问解决方案的缺陷在大量居家办公（WFH）场景中暴露出来，针对现代软件定义安全访问解决方案的预算将翻四倍。到 2024 年，安全远程访问解决方案（虚拟专用网[VPN]、网络访问控制[NAC]和软件定义边界[SDP]）将以 260 亿美元价值占据全球网络安全市场 12.5%的份额。

June 2021, IDC

IDC 认为，软件定义安全访问的定义囊括了零信任理念。零信任理念的挑战不在于技术实现，而在于如何从人的视角进行规划和执行。安全专业人员通常从不同的层面提及“信任”——战术、技术层面；“数字化”战略层面；以及传统的人的层面。实际上，信任是数字化转型的客观要求，也就是说，组织/实体必须信任其他组织/实体才能获得成功。IDC 使用以下术语介绍零信任理念：

- **数字信任**是一个重要的战略组织概念，它将组织和最终用户之间的信任从技术层面整合到广泛的感知和基于声誉的层面。
- **数字化转型（DX）安全模型**是一种通用的安全方法，它属于数字信任的范畴，并在身份、漏洞、信任和威胁管理等功能服务下组织数字转换的新技术和流程——所有这些都与 IDC DX 平台模型相关。
- **分布式完整性模型**是网络安全架构模型，它关注的是用户和设备如何访问应用程序和处理数据。在这个模型中，有三种常见的能力——软件定义边界（SDP）、增强身份认证（IAM）和微隔离（MSG）——构成了零信任架构的主要技术能力。

数字化转型要求企业网络安全体系主动求变

科技的进步加快企业网络边界的泛化

自 2007 年开始，IDC 已经预测以云、大数据分析、社交网络和移动为中心的第三平台将成为未来 ICT 产业发展的重要基础。IDC 将数字化转型定义为一种途径，企业通过数字化转型利用第三平台技术建立新产品、新业务模式和新的合作关系，从而增加价值和竞争优势。几乎所有行业的客户都有数字化转型的需求，而新兴科技将成为组织数字化转型的关键，并将聚焦在七个“创新加速器”，即：物联网、机器人、增强/虚拟现实、人工智能、3D 打印、下一代安全、区块链。IDC 预测，2021 年中国 ICT 市场（含第三平台与创新加速器技术）规模达到 7,111 亿美元，将比 2020 年增长 9.3%，恢复到疫情前相对高速的增长。2021-2024 数字化转型总支出将达到 1.5 万亿美元，年均增长率达到 17%。

与此同时，云计算、大数据、移动互联网、物联网、5G 等技术广泛应用到企业信息化建设和业务发展中，企业的业务发展路线和应用模式正在快速转变。一方面，业务的持续健康发展要求企业增强与客户的沟通并及时了解客户的需求变化，因此，Web 应用、移动应用成为企业为客户提供便捷、高效产品和服务的重要选择。同时，云计算在提升业务的高可靠性和可扩展性方面具有独特优势，促使大量企业将核心应用迁移到云计算平台和互联网，新冠肺炎疫情的爆发更是进一步加快了企业上云步伐，企业的服务范围已经远远超出了原有内部网络边界，企业业务系统走向了更开放的生态模式。另一方面，随着业务的发展，企业信息化建设的规模和复杂性逐渐提升，需要打破各个业务系统的信息孤岛，提升数据统一挖掘、分析和利用的能力，因此，业务系统间相互调用和数据交互越来越普遍，数据资产的价值迅速提升。最后非常重要的一点是，传统网络模式下的业务内网、业务外网正在逐渐融合，尤其是新冠肺炎疫情防护常态化的大趋势下，远程办公、业务协同、分支互联等业务需求快速发展，而新兴技术的不断成熟和发展能够很好地满足企业不断涌现的新增需求，帮助企业的员工、设备、合作伙伴以及客户随时随地通过多种方式灵活接入企业业务系统，以提高工作效率、增强用户体验，而无需考虑这些系统是位于企业内部网络、云平台还是开放网络环境。

由此可见，数字化转型使得企业基础网络架构和业务系统发生重要转变，而传统基于边界的网络安全防护手段通常会默认将企业所处网络环境划分为内部的信任区域和外部的非信任区域，人员或设备一旦通过身份认证或利用系统漏洞进入到企业网络内部，便可以在多个业务系统间随意穿梭，畅通无阻。因此，这一传统理念已经无法有效匹配新环境下的网络安全需求，其弊端日益显现，众多企业正在寻找持续补足的方法，或者更为完善的网络安全防护理念。

威胁的增长迫使企业网络防护观念的转变

恶意威胁持续冲击企业网络安全防线

关注新兴技术的不仅仅有全球企业和网络安全公司，还有分布在各个角落的网络犯罪组织。近几十年来全球范围的网络威胁频繁发生，新技术的引入帮助恶意工具进入批量生产、自动化运行的时代，也使恶意攻击越来越隐蔽和复杂，很难被第一时间检测到，尤其是精准投放的高级持续性威胁（APT）和目的明确的勒索软件给众多企业造成了重大损失。同时，人永远是网络安全防护体系中最不可控的因素。企业对于内部员工有意或无意的越权操作，往往缺乏及时有效的检测和防控手段，由此产生的内部网络威胁会使企业防不胜防。一旦遭受网络攻击，企业不仅需要花费大量的精力修复网络攻击造成的系统损坏、数据丢失、数据泄露等问题，还要投入大量资源挽回由于遭受网络攻击而失去的企业信誉。

纵观近几年全球范围频繁发生的各类网络安全事件，我们不难发现，无论是政府、金融、能源等国家重点领域，还是制造、互联网、医疗、服务等其他各个行业均面临着数据泄露、恶意勒索、系统破坏等网络威胁的严峻挑战。而普通民众通过媒体或网络看到的网络安全事件仅仅是冰山一角，还有大量未被大众所知的攻击行为隐藏其后，且新的网络安全事件还在持续发生。另外，2020 年，在新冠肺炎疫情蔓延全球的大环境下，利用疫情话题为诱饵的网络钓鱼攻击和勒索攻击广泛发生，使得企业在疫情环境下的生存和发展面临更多威胁挑战。

聚焦国内网络安全环境，国家互联网应急中心（CNCERT）发布的《2020 年我国互联网网络安全态势综述》报告内容显示，2020 年国家信息安全漏洞共享平台（CNVD）收录的高危漏洞数量达到 7420 个，同比增长 52.1%，“零日”漏洞数量为 8902 个，同比增长 56.0%。勒索病毒持续活跃，全年捕获勒索病毒软件 78.1 万余个，较 2019 年增长 6.8%。勒索病毒攻击活动的目的性继续增强，大型高价值机构成为首要目标。另外，勒索病毒的攻击也伴随着技术的发展呈现快速升级趋势，利用漏洞入侵以及随后的内网横向扩散过程的自动化、集成化、模块化、组织化特点愈发明显。同时，由于攻击成本低、效果显著，DDoS 攻击仍是目前互联网用户面临的较常见、影响较严重的网络安全威胁之一。

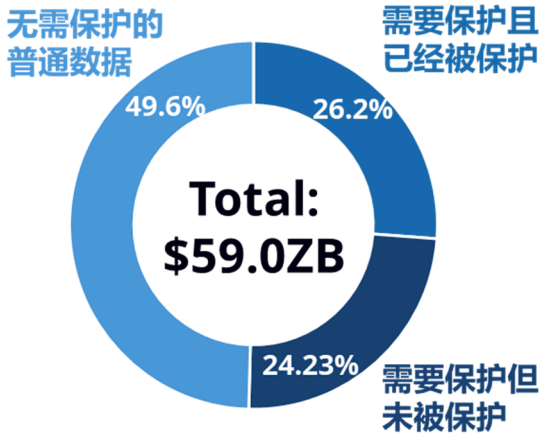
频繁发生的网络安全事件以及上述网络安全态势统计均表明，目前全球的网络威胁局势仍然十分严峻。企业需要在原有网络安全防护的基础上，持续更新优化相关技术和产品，打造更为纵深、动态、智能的防护体系，并通过专业的网络安全服务提升体系的运营效果。零信任理念坚守“永不信任，始终验证”的原则，要求每个访问请求在授予访问之前都应进行完全身份验证、授权和加密，能够有效提升企业网络安全防护的细粒度和动态性，正在成为企业级客户重点关注的网络安全防护防护理念。

数据安全成为企业最关注问题

IDC 认为，全球数字经济正在高速发展，2023 年，由数字化产品和服务驱动的数字经济在全球国内生产总值（GDP）中的占比将达到约 50%。同时，根据 IDC Global DataSphere（专门记录全球数据增长的产品）显示，2020 年全球创造了 59ZB 的数据（Zettabyte，即泽字节，1ZB=1 万亿 GB）；2025 年，全球新产生数据量将高达 180ZB，数据已经无处不在。IDC 发现，一半以上的数据需要一定程度的保护，近四分之一的数据被认为是私人的或通常不向公众提供的，安全级别很高但却缺乏保护。企业核心数据一旦丢失，就如同战场上司令部被对手消灭一样严重。与此同时，我们也清晰地意识到，全球范围的数据安全事件频繁发生，而这些公开的信息仅仅是众多网络威胁的冰山一角。数据必须根据其重要级别得到相应的安全保护，不仅因为它能够帮助企业提高生产力和竞争优势，还因为数据的非法/违规访问和使用可能导致企业由于违反法律法规遵从性而遭受经济和信誉上的严重损失。随着企业在数字化转型过程中 IT 系统日益复杂，网络暴露面不断扩大，企业数据面临的安全挑战也愈发严峻。

图 1

2020 年全球新增数据总量及待保护数据份额



来源: IDC, 2021

从监管层面看，全球各国政府都在积极应对数据安全的问题。从欧盟通用数据保护条例（GDPR）、《加州消费者隐私保护法案》（CCPA）、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法（草案）》等法律法规的颁布来看，同时，多个重点行业也发布了各自的行业要求或规范，例如《电信和互联网企业网络数据安全合规性评估要点（2020 年版）》、《证券期货业数据分类分级指引》、《国家健康医疗大数据标准、安全和服务管理办法（试行）》等，进一步明确了企业在数据安全保护方面的责任和义务，也将广大企业管理者的数据安全防护意识推升到了前所未有的高度。

PB（Petabyte）级的数据系统部署在许多组织中已经很常见，很多数据经常被复制、共享和存储在多个资源库中。随着数据价值的增加，对数据的保护需求也在增加，同时，虚拟化基础设施、云计算的采用以及越来越多移动设备的加入使得企业数据日益分散、可见性和控制力降低，数据安全保护的难度不断增加。当前很多企业正努力通过多种手段获取对敏感企业数据资产的可见性和控制权，以便对于数据在企业内部业务系统间流转，或者来自外部的数据访问进行安全防护，公司的数据安全团队承受着数据风险管理的巨大压力。由此，零信任网络架构正在逐渐成为企业应对数据安全防护需求的重要方案之一。

主动求变，零信任理念落地生根

通常情况下，企业会在网络边界部署防火墙、统一威胁管理（UTM）、入侵检测/入侵防御等网络安全产品，从而构建一个“受信任”内部网络，将企业重要资产与外界的“非信任”外部网络隔离；为了满足企业员工和客户的外部访问需求，又往往需要设置虚拟专用网络（VPN）或隔离区（DMZ）。无论采用何种方式，上述网络基础架构中均存在权限管控过于宽泛的问题，网络攻击者一旦利用产品/系统漏洞、企业非受管 IT 资产、社会工程学等手段进入企业网络内部或者攻破数据中心网络的某台服务器，将获得充足的权限执行进一步的渗透，此时企业的众多网络安全防护产品将形同虚设。

随着数字化转型的不断深入，企业将越来越多的核心应用迁移到云计算平台和互联网，企业的服务范围已经远远超出了原有内部网络边界，企业业务系统走向了更开放的生态模式。同时，基于 IP、域名等传统的管控方式显然已无法适应未来的安全需求，企业很难像过去一样快速找到一条明确的网络边界，从而将不同的风险域明确地隔离开来。

正是由于上述企业数字化转型业务需求以及严峻的网络威胁挑战的普遍存在，零信任理念在其被业内提出并在谷歌的 BeyondCorp 实践落地后，得到了安全厂商及最终用户的广泛关注和认可。美国国家标准与技术研究院（NIST）发布的《零信任架构》对零信任的概念和逻辑组件进行了详细介绍，并成为国内外企业构建零信任架构时的重要参考。2021 年，美国国家安全局（NSA）发布关于零信任安全模型的指南《Embracing a Zero Trust Security Model》，再次强调零信任的实施不可能一蹴而就，并在零信任成熟度模型中将零信任的发展路线划分为初始准备阶段、基本阶段、中级阶段、高级阶段。零信任架构的企业网络安全防护体系坚守“永不信任，始终验证”的原则，不再以访问主体（人/设备/应用）的物理或网络位置作为其是否被信任的主要依据，任何访问主体都需要进行持续权限验证和安全评估才能够获得对企业资源动态的最小化授权访问。

零信任的核心是对企业资源和数据的安全防护，在假定网络环境已经被攻陷的前提下，对每一次访问请求进行可信验证。零信任的实现很多涉及到的是对原有网络安全技术的持续优化和重构，这在很大程度上促进了零信任理念的快速发展和应用。根据 IDC 的观察，我国众多网络安全产品和服务提供商已经纷纷根据自身技术积累和产品优势推出了各具特色的零信任相关解决方案，包括从软件定义边界（SDP）、增强身份认证（IAM）、微隔离（MSG）等维度帮助企业构建零信任理念下的网络安全防护体系，并已经在行业重点客户侧进行落地实践和持续优化。

零信任理念成为中国网络安全市场新趋势

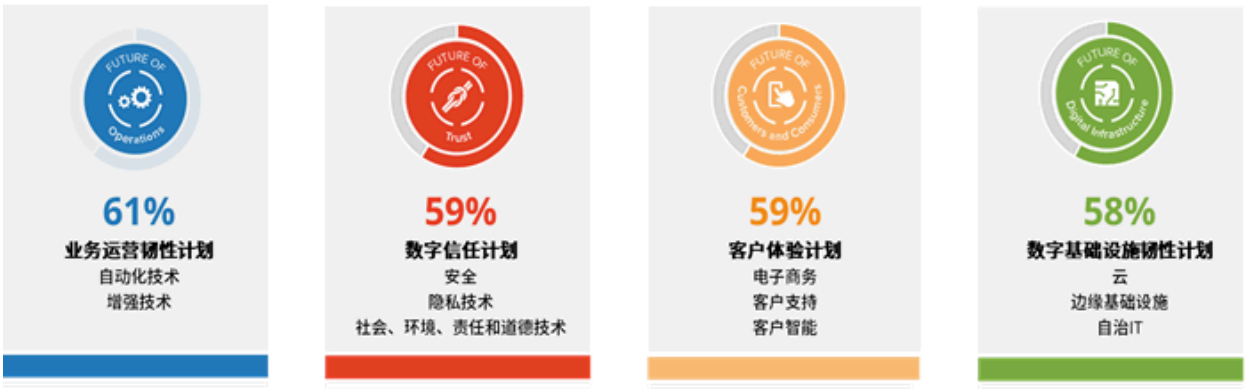
未来信任护航企业持续健康发展

科技的进步推动着社会快速发展，信息化、数字化、智能化成为当今人类社会和几乎所有企业演进的重要方向。随着人们面对的信息爆炸式增长，企业要想持续健康发展，一方面需要从海量信息中准确抽取真实可信的高价值内容，另一方面需要运用综合方案保护自身核心数据并不断提升企业信誉。在这个过程中，网络空间安全的重要性不断提升，并已经成为数字经济发展的基石。IDC 认为，企业正在进入一个“后真相时代”。在这个时代，真相的解释不是由企业控制的，而是被各种利益集团所控制，每个利益集团都会受到其自身的偏见和规划的影响，对真相、事实进行多重解读。企业及其客户、合作伙伴和监管者面临的一个重要问题不是“什么是可信任的”，而是“什么是可以被证明的事实”。换句话说，企业需要判断存在的哪些信息是客观的，且这些信息足以证明企业可以被产业链信任。

2020 年全球爆发的新冠肺炎疫情考验了所有企业的数字化转型成效，后疫情时代，“数字化韧性”成为企业关键词之一。它将帮助企业快速适应业务中断所带来的影响并快速恢复，并能够在不断变化的环境中保持业务的增长与创新。企业要充分利用数字技术，在领导与组织、运营与流程、品牌与声誉、客户与生态、员工与工作、金融与财务 6 大方面打造数字化韧性，迈向全球领军的未来企业。2021 年 2 月，IDC 在《未来企业韧性与支出调查》报告中针对全球超过 700 位技术决策者进行了调研，“数字信任计划”已经成为企业为了确保业务的长期韧性和成功而优先考虑的重要技术。

图 2

问题：为确保业务的长期韧性和成功，对于以下每项计划，贵企业未来 2 年优先考虑哪些技术？



来源: IDC, 2021

IDC 认为，“信任”有两个组成部分：

- 信息被客观地以“风险”来衡量，即信任由“可信任”和“不可信任”的二选一决策转变为对合作伙伴、供应商、客户和监管机构的可信度的衡量评估，这种风险度量提供了未来行动和决策所依据的信息。从概念上可以认为，这种客观的评级分数从 0 到 100，其中 0 表示不可信任，100 表示可信任，而现实很可能介于可信任与不可信任之间。
- 信息被主观地以对海量新闻和信息来源的“看法”来衡量，从“看法”的性质来看，这些信息来源带有个人和群体的偏见。

IDC 认为“信任”是两个或多个实体之间能够做出反映各方之间信任程度（风险和声誉）的决定条件。未来信任是一个首要的战略组织概念，将组织间及其和最终用户之间的信任从技术层面整合到广泛的认知和基于声誉的层面。未来信任是由风险、安全、合规、伦理、社会责任和隐私构成的综合体系，这些要素也构成了未来信任的演化框架，它们将是未来企业进行信任治理的关键。信任的五个要素将从讨论一个企业“必须”做什么来预防负面结果转变为一个企业“应该”做什么来防止负面结果的同时建立正面的信任结果。因此传统的处理安全、风险、合规、和隐私的方式在规模和范围两方面都将面临挑战。

图 3

IDC 未来信任的演化框架

来源: IDC, 2021

在信任的基础阶段，最终用户需要关注风险，即可能影响组织信任度、完整性、可用性、生产力或营业收入的“结果”。最终用户需要定义一组合适的“负面结果”来对风险进行评估并降低风险；在信任的义务阶段，需要最终用户关注安全与合规。在安全层面上，需要政企做到内部的安全建设以及和外部共享数据等资源时的安全防护，这里面包含一系列安全产品与服务。在合规层面上，各国政企需要遵守当地的与安全、信任相关的法律法规，以实现更好的连接与运营。例如，欧盟实施的《通用数据保护条例》（GDPR）从法律层面上保护了个人隐私数据，现在该条例已经被欧盟以外其他司法管辖区用作保护消费者数据的模型；信任的战略阶段需要最终用户将信任提升至战略层面，在降低风险或成本的同时关注资本、资源和工作投资回报的最大化，运用隐私、道德和社会责任的战略规划来创造积极结果。例如，为了满足最终用户的需求，雀巢和亚马逊通过合作建立“原产地链”——Hyperledger Fabric 网络以提高透明度，主动满足了人们对咖啡供应链的信任，消费者可以在区块链上跟踪他们从农场到消费的所有产品，该方式运用新技术提高了最终用户对于产品的信任，进而提高了产品效益。

在商业中，每一项投资都有机会成本，至少会存在由于没有进行投资而错过收益的机会成本。因此，对信任的投资必须以所有投资相同的方式来进行审查，即投资回报率（ROI）。因此，我们在实现信任的同时，也关注信任的结果。由于未来的信任环境引入了超越传统的安全、风险和法规遵从性概念的新元素，IDC 提出了三种新的信任结果：可信任的治理、可信任的生态系统和可信任的商业，它们将对由未来社会、未来行业、未来企业所组成的数字化社会带来深远的影响。

- 可信的治理需要管理者从未来信任的五个关键要素出发，在信任治理层面实施控制，建立信任文化，以确保遵循有助于建立或加强信任的行为和最佳实践。信任的文化源于企业的高层领导，其中，道德和监督实践源于首席执行官（或一名 c 级信任官）和以身作则的董事会。可信的治理侧重于内部，而内部又与企业的信任生态系统相联系，并使该生态系统能够与整个世界进行信任的商业活动。
- 可信的生态系统通过前瞻性地管理合作伙伴、供应商、客户和内部员工之间生态系统中所存在的集体风险来确保交易的完整性。这是在一个难以实现信任的地方建立一个生态系统，因此，区块链技术将在这个生态系统的建立过程中起到非常重要的作用，IDC 将区块链视为实现未来信任的重要技术底座。
- 可信的商业中的一个重要组成部分是组织需要理解客户内部的信任感是在长期的合作中形成的，组织通过提供优质便捷的产品、服务、体验来提高最终用户的信任程度，但也有可能在一瞬间被破坏。此外，“商业”并不一定意味着各方之间的交易，也可能意味着建立在高度定制体验之上的增值服务，这种增值服务可能连最终用户都不知道“商业”正在发生。同时，企业开始将社会责任视为增加用户信任的一种方式。可信的商务是未来信任的最终实现目标，也是成为保障未来智能社会正常商业秩序的基石。

零信任帮助企业打造未来信任

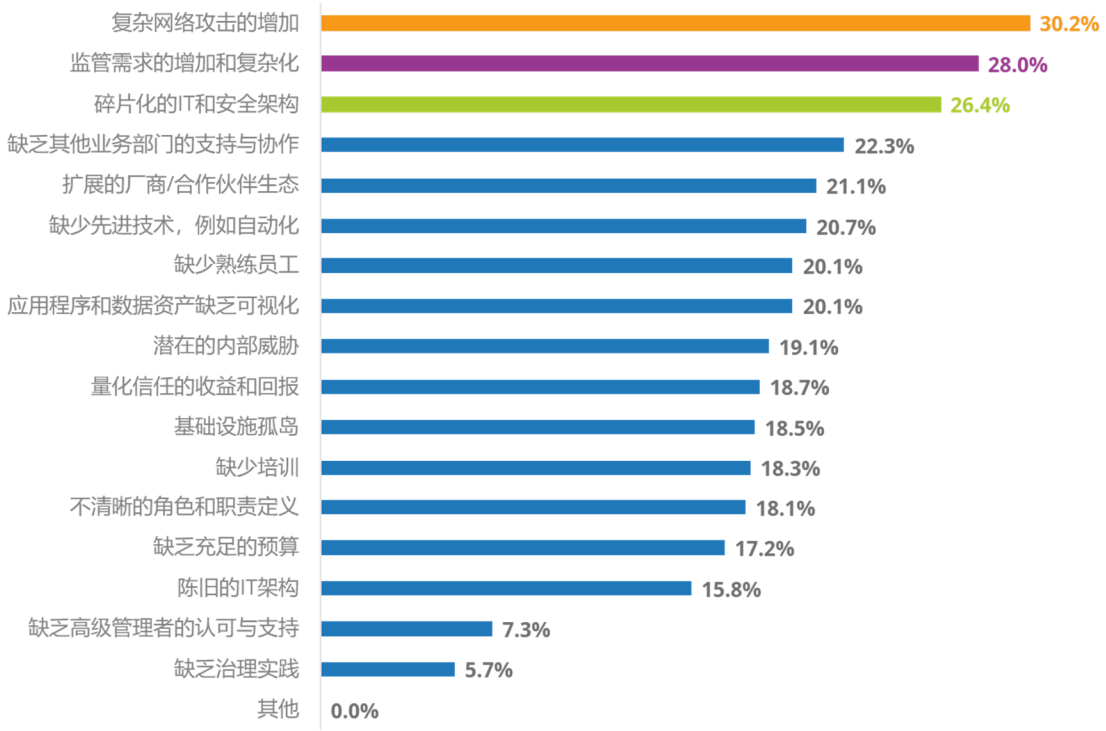
随着企业数字化转型的持续推进，信息化、数字化、智能化已经不可逆地融入到企业整体发展战略，企业管理者越来越清晰地认识到网络安全对保障业务持续发展中的重要作用。保护 IT 资产——无论是数据、应用程序、网络还是设备——已经成为企业基本要求。遵守并符合国际、区域或行业的安全法规或准则是企业业务开展的前提。例如，涉及支付业务的企业必须遵守支付卡行业数据安全标准（PCI DSS），否则将失去通过信用卡或借记卡接收付款的能力。同样，医疗产品相关的厂商也常常受到《健康保险携带和责任法案》（HIPAA）合规性的约束。这些合规性要求可能是某个公司为保护自己免受信任损失而制定的政策，由行业（如 PCI DSS）实施，或被监管机构（如 HIPAA）要求。合规要求不断扩大的一个例子是欧盟实施的《通用数据保护条例》（GDPR）。无论规定来自何处，安全、合规都将持续成为企业打造未来信任的重要组成部分。

聚焦中国网络安全市场， 2017 年 6 月 1 日，中国《网络安全法》正式生效，推动了中国的网络安全法制化进程，成为网络安全法制化建设的重要里程碑。2019 年 5 月 10 日，《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》以及《信息安全技术网络安全等级保护安全设计技术要求》三大核心标准正式发布，标志着等保 2.0 时代的到来。除此之外，2020 年，国家新颁布的《网络安全审查办法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法（草案）》等法律法规的也在不断提升政府、企业对网络安全的重视程度，提升组织甚至国家网络安全综合防护能力，推动整个网络安全产业发展。

企业必须明白的是，云计算、大数据、移动互联网、物联网、5G 等新兴技术的广泛应用不但提升了企业的生产效率、扩大了业务范围，同时也带来了更多的网络安全挑战。根据 IDC 对全球超过 500 家企业的调研结果，关于企业建立信任面临的内外部挑战的全球调研数据，复杂网络攻击的持续增加是企业建立信任过程中面临的最严峻的内外部挑战。企业看待网络安全已经不是询问“会不会被攻击”，而是担心“何时被攻击”。而来自不同国家、地区和行业的各种网络安全、数据安全的强制性要求会随着网络威胁种类、范围、破坏性的扩大而不断增加，企业将面临日益严峻的网络安全挑战。与此同时，我们可以很直观地感受到以往传统基于边界的网络安全防护理念在应对当今多样化的网络威胁时逐渐显得捉襟见肘，恶意威胁一旦突破企业网络的防护边界，即可获取“充足”的内部资源访问权限，可以在网络内轻松的横向移动，从而获取或破坏更多系统和数据。

图 4

企业建立信任时面临的内部及外部挑战



来源: IDC, 2021

正因如此，零信任理念逐渐成为全球网络安全市场最炙手可热的话题之一，已经有众多全球知名企业或依靠自建安全技术团队，或凭借第三方专业安全厂商的支撑开始构建零信任网络架构，并且已经取得了显著的网络安全防护效果。

通过构建零信任的网络架构，打破传统的网络安全防护过度依赖安全边界的架构体系，将保护重点从粗粒度的、静态的网络边界转移到更细粒度的企业资源（包括 IT 资产、数据资产等）。零信任网络另外一个核心能力是实时评估网络中所有操作和资源，以减少非法访问业务数据和敏感资源的风险。同时需要指出的是，IDC 认为，随着零信任将安全防护从“以网络为中心”转移到“以身份为中心”，减少了对网络位置的依赖，但网络的访问控制和边界防护在整体安全架构体系中仍然非常重要。零信任理念与企业现有安全防护体系之间是相互补充，而不是完全替代的关系。

IDC 认为，任何组织都应该意识到，一旦遭受严重的网络攻击，组织要面临的的不仅仅是经济的损失，还包括客户的流失、员工士气的降低、生态合作的重铸，以及监管和合规成本的增加。未来信任是对安全话题的升级，且将对未来数字化社会的发展带来重要影响，零信任网络架构的持续完善能够帮助企业打造愈发智能、动态的网络安全主动防御体系。

数字化转型安全模型为零信任理念的实现创造根基

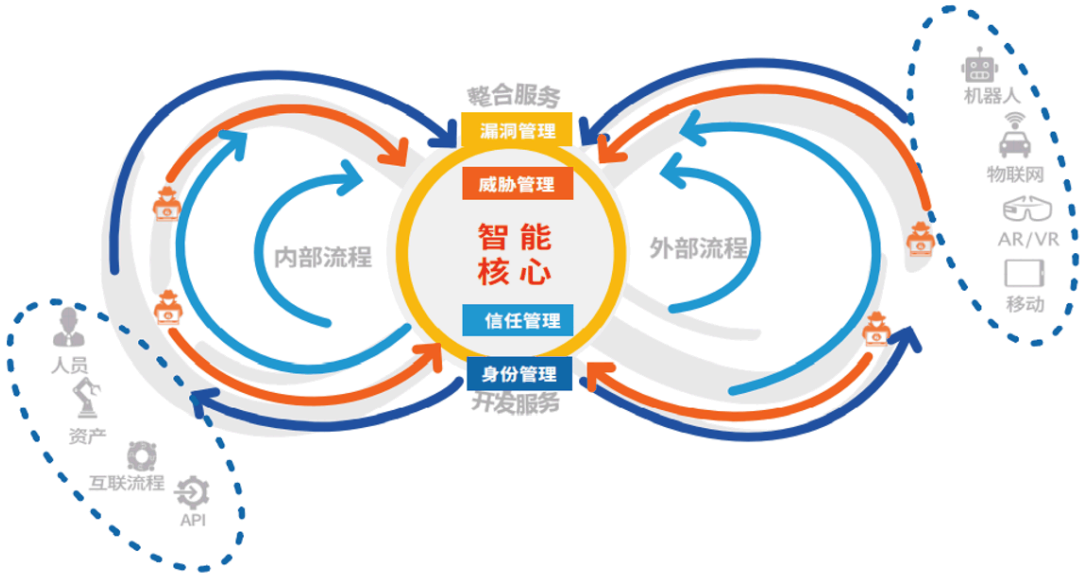
IDC 将数字化转型平台定义为“能够加速企业的数字化转型计划，能够快速打造面向外部的数字产品、服务和体验，又同时可以对内部 IT 环境进行现代化改造，使其成为智能核心的未来的技术架构”。在

过去的几年里，随着 IDC 称之为“第三平台”的下一代技术的到来和部署，数字化业务转型一直是高管们最关心的问题。当这些技术与新的工作实践相结合时，可以使企业从根本上改进其运营模式，甚至创造新的商业模式。IDC 认为，数字化转型的推进促使企业 IT 环境正在发生很大变化。企业的核心资产（终端、业务系统、数据）越来越多地被部署在多云或混合云环境，并广泛地连接到互联网上的其他资源，企业内外网的概念愈发模糊；丰富的企业资产/资源面临着不同级别的安全风险，想要全面监控分析网络活动并准确识别其中的恶意威胁是一项艰巨的挑战；用户、数据和工作负载可能来自远程办公、分支机构、合作伙伴，合作伙伴的合作伙伴，对第三方甚至第四方风险的识别和管理需要得到更多的关注。虽然环境的变化正在使得企业面临的网络威胁复杂度不断提升，安全防护技术和理念持续面临新的挑战，但安全基本原则不变，即：身份管理、信任管理，漏洞管理和威胁管理不变。

主动安全防御体系的建设需要从身份、信任、威胁和漏洞四个方面进行规划。在数据开始进行内外部流通时，首先需要运用身份管理能力来验证用户和设备的身份，从而采取适当的策略进行访问控制。在此之上，不同的 IT 资产将利用信任根来确保数据流动时的机密性和完整性。与此同时，数据将在集成安全分析能力的智能核心中进行传播，通过包含漏洞管理等能力的智能核心来洞察威胁，集成全面的威胁情报来识别并响应威胁，最终维护整个 IT 系统环境的安全。

图 5

IDC 主动安全防御体系建设模型



来源: IDC, 2021

各个环节所需的安全产品能力如下：

- **身份管理：**包括所有人工、自动化流程以及与用户、帐户和凭据相关的技术解决方案（如：配置/取消配置、授权、密码重置、身份认证和访问控制）。
- **漏洞管理：**包括所有人工、自动化流程以及与 IT 系统资源相关的技术解决方案（如：资产清单、配置管理、漏洞扫描与修补、渗透测试、防火墙以及隔离和过滤）。

- **威胁管理：**包括所有人工、自动化流程以及与威胁、攻击、泄露、事件的处置、响应和恢复相关的技术解决方案（如：安全运营和告警、入侵检测、威胁情报、取证和事件管理。其中，威胁情报包括基于云的威胁情报查询系统、本地化威胁情报管理平台等技术解决方案）。
- **信任管理：**包括所有人工、自动化流程以及与治理、风险和合规相关的技术解决方案（如：审计、策略管理、第三方尽职调查、加密通信、数据加密、数字签名）。

从整体视角来看，数字化转型平台将在整个内外部流程中提供“智能核心与数据服务”、“集成与编排服务”、“开发者服务”和“参与服务”。其中，“智能核心与数据服务”将在整个数据流转的过程中提取出可以促进业务良性循环的“真知灼见”，将洞见转化为可采取的行动进行输出；“集成与编排服务”帮助组织连接分散架构中的数据交换与服务，增强 IT 环境的弹性与自动化水平；“开发者服务”帮助组织开发符合业务需求的应用软件；“参与服务”为组织提供与内外部生态交互的必要服务，包括为生态提供产品、数据信息、以及对于生态合作伙伴的支撑服务等等。在实际操作中，四种服务或能力将把身份、信任、威胁和漏洞这四个方面的能力进行集成，从而帮助组织建立坚实的安全底座。

图 6

数字化转型平台的关键安全要素

来源: IDC, 2021

分布式完整性模型提供零信任理念的核心能力

分布式完整性模型是网络安全架构模型，它关注的是用户和设备如何访问应用程序和处理数据。在这个模型中，有三种常见的能力——软件定义边界（SDP）、增强身份认证（IAM）和微隔离（MSG）——构成了零信任架构的主要技术能力。

- 软件定义边界（SDP）是由云安全联盟（CSA）开发的一个安全框架，通过软件的方式提供了一个集成的安全体系结构，利用基于身份的访问控制和动态的权限认证机制实现企业关键资产和基础架构的隐身保护，只有通过身份验证的请求才能够基于最小化授权原则访问相应的应用程序，而非整个企业网络，同时所有的访问流量都通过加密方式传输，且进行双向认证。在过

去的多年，虚拟专用网络（VPN）一直都是企业支撑远程办公、分支互联等业务需求最直接和有效的技术手段之一。但随着网络开放性和复杂性的逐渐提升，企业对于网络接入的灵活性和便利性的要求明显提升，VPN 由于其自身技术限制和管理复杂度的提升，往往成为业务稳定和发展的瓶颈之一。根据 IDC 的调研，疫情期间，因为企业用户开始不断要求工作场所中的 IT 体验可以等同或优于私人环境中的 IT 体验，但是传统 VPN 远程解决方案存在缺陷，所以 VPN 问题成为了企业 IT 投诉的第二大来源。而 SDP 的上述技术特点和防御机制更好地解决了安全接入和资源访问的业务需求，同时能够屏蔽大多数非法用户的网络攻击，例如企业网络端口探测、分布式拒绝服务攻击（DDoS）、中间人攻击等。

- 全面身份化管理是零信任架构的基石，尤其是在业务多云部署、终端种类和数量激增的现代 IT 环境下，企业需要更加敏捷、高效、智能的身份管理能力。与传统基于单因素或多因素认证的一次登录持续信任的静态身份管理不同，零信任理念要求企业为资源的访问制定基于风险的动态评估策略。增强身份认证（IAM）将企业所有数字资产进行有效管理并通过唯一标识进行身份化处理，同时结合权限细粒度划分、网络环境检测等信息对身份进行有效管控和治理。通过零信任理念下的 IAM 实施，企业可以将原有各自孤立的用户管理体系、身份认证体系紧密整合，最终实现以身份为中心的全生命周期的动态信任管理，并根据信任评估结果，判断该身份访问企业关键资产和数据的权限。
- 如果说 SDP 主要解决了企业网络内外部访问流量的安全性，那么微隔离则是通过软件定义的方式对数据中心或业务系统工作负载进行细粒度的策略控制和流量可视化，从而阻止来自企业网络内部的横向攻击，更加有效地防御黑客或病毒持续性大面积的渗透和破坏。特别是随着虚拟化、容器、混合云等技术广泛应用到企业网络环境，原先利用 IP 地址规则的网络隔离防护手段已经失效，一旦在网络内部发生网络攻击或恶意程序感染，将很难做到细粒度的精准防护。同时，由于微隔离会把企业网络进行逻辑细分并基于东西向流量分析执行动态访问控制，该技术的应用往往会对现有业务系统造成较大影响，因此企业对待微隔离技术更为谨慎，通常会采用分阶段实施的策略。

除了上述软件定义边界（SDP）、增强身份认证（IAM）和微隔离（MSG）三项主要能力外，零信任架构还包含其他多项网络安全技术要求，例如行业合规管理、威胁情报联动、安全信息和安全事件的全面记录和关联分析等。同时，在美国国家标准与技术研究院（NIST）发布的《零信任架构》中还指出，零信任架构的网络要求企业必须能够全面识别和管理设备资产及其当前的安全状态，能够持续记录和分析所有网络流量并识别潜在的网络威胁，通过通信加密手段保障任何网络位置的通信都是安全的，这些网络要求保障了零信任架构能够切实的运转和生效。

零信任理念在中国市场的现状与趋势

技术提供商零信任相关方案能力观察

作为实现零信任理念的三种核心方案——软件定义边界（SDP）、增强身份认证（IAM）和微隔离（MSG）成为目前全球安全厂商落地零信任的主要路径。IDC 通过对众多国内安全解决方案提供商的调研和访谈了解到，国内零信任相关解决方案提供商大体分为以下三类：

专业型安全厂商：随着零信任理念的持续火热，国内涌现出大量以零信任为核心能力的创新型专业安全厂商。凭借对市场热点敏锐的嗅觉，对零信任相关技术的快速迭代和企业战略的灵活调整，这些安全厂商紧跟市场需求，推出了各具特色的零信任相关产品和解决方案，并在众多行业用户的应用实践中快速积累经验、树立口碑。其中，由于 SDP 解决方案相对便于落地实践，且能够帮助用户更直观地感受到 SDP 带来的业务访问便捷性和安全性的提升，因此成为专业型安全厂商参与最多、最活跃的零信任技术路径。

综合型安全厂商：此类安全厂商具备全面的产品品类，并在多个技术领域有着深厚的技术积累，同时在重点行业拥有良好的口碑和用户基础。正是由于认识到了零信任理念明确的技术可行性和广阔的市场前景，这些厂商能够集中优势资源快速创建或优化自身解决方案，必要时甚至重构网络防护架构，以满足

用户业务系统对零信任的复杂需求，同时能够凭借长期积累的市场优势实现解决方案的快速试点应用和推广。

云服务提供商：中国网络安全市场的高速发展和广阔的市场前景正在吸引着云服务提供商持续加大网络安全领域的资源投入，并根据云计算环境对网络安全能力的特殊需求不断丰富自身的安全产品和服务。而随着多云、混合云场景的普及，零信任架构已经成为云服务提供商，特别是公有云服务提供商的必备能力之一。这些厂商依靠强大的技术底蕴和创新能力，能够快速响应市场需求，同时凭借云原生优势，深入了解云上系统和业务场景，提供高适配、高弹性、高性能的零信任架构。

IDC 认为，零信任理念在未来几年仍将是全球网络安全市场关注的热点，也将会有更多的安全技术提供商投入到零信任的浪潮中。但零信任理念的实践是一个持续更新优化的漫长过程，没有哪个技术提供商能够通过一套解决方案实现对网络威胁的彻底防御，需要配合不同品类、不同视角的网络安全产品为企业打造全方位的主动安全防护体系，尽可能降低企业遭受恶意入侵的风险，并在发现威胁时及时响应处置，避免威胁的扩散，减小企业的经济、信誉损失。同时，零信任越来越多地在用户侧的应用实践也是一个大浪淘沙的过程，具备领先技术、优质服务，能够高度适配用户业务场景的零信任架构必将脱颖而出，获得越来越多企业客户的认可。

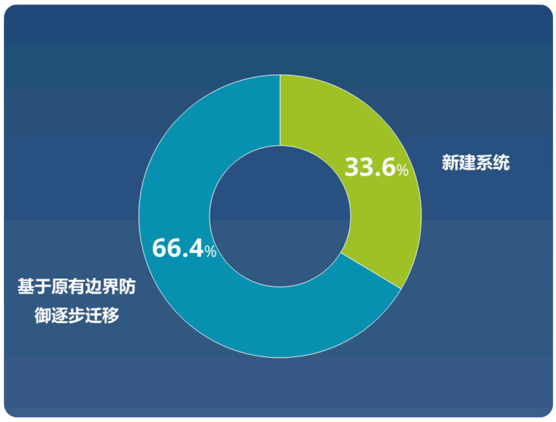
技术买家的零信任落地现状

2020 年爆发的全球范围的新冠肺炎疫情使所有企业都深刻体会到数字化转型在提升企业业务连续性和业务韧性方面的重要性，也进一步促进了例如远程办公、协同办公、业务上云等业务需求的蓬勃发展。企业管理者不禁感叹“我们被疫情改变，再也回不到过去了。”从网络安全角度来看，企业原有严格的网络边界划分以及完全基于 VPN 的远程访问规则已经无法满足新兴业务场景下对网络安全防护的动态、灵活、细粒度等方面的要求。根据 IDC 的调研，疫情期间，VPN 问题成为了企业 IT 投诉的第二大来源。因此，越来越多的企业开启了对零信任架构的调研和学习，并逐步尝试将这一理念应用到不同的业务场景。

IDC 认为，远程办公/协同办公的安全接入与业务访问、数据中心的数据访问与调用、云计算环境下的业务和应用的安全访问等是目前国内企业应用零信任架构的重点领域。IDC 在 2021 年 4 月针对零信任在国内企业中的建设情况，以及建设过程中面临的主要挑战访谈了大量企业网络安全管理者，并获得了大量有价值的信息。调研数据显示，66.4%的国内企业选择基于自身原有网络边界防护体系逐步建设零信任架构。同时无论是政策合规要求驱动，还是网络安全防护连续性考虑，都要求企业在进行零信任建设的同时持续加强对边界防护的资源投入。

图 7

贵司零信任网络架构的建设方式？

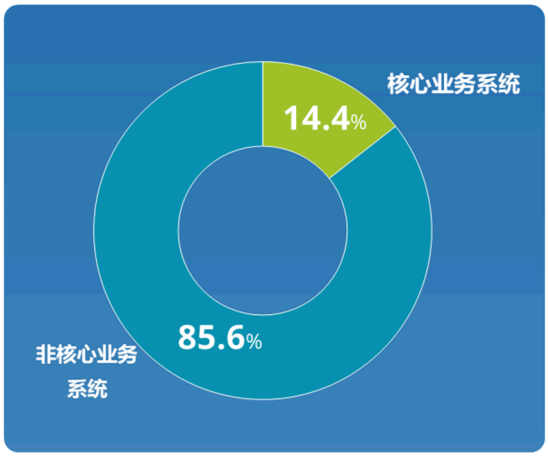


来源: IDC, 2021

IDC 调研数据显示，目前正在实施零信任网络架构迁移的企业基本都能够保持对零信任理念的客观、理性认知，且零信任在企业中的应用大多处于局部试点阶段，并不会盲目扩展。由于零信任理念的实践需要根据企业具体的业务特点进行持续优化和完善，有 85.6%的企业会选择从非核心业务着手零信任网络架构建设，并将在充分的验证和试点后逐步向核心业务拓展。

图 8

贵司零信任网络建设目前涉及到哪些业务系统？

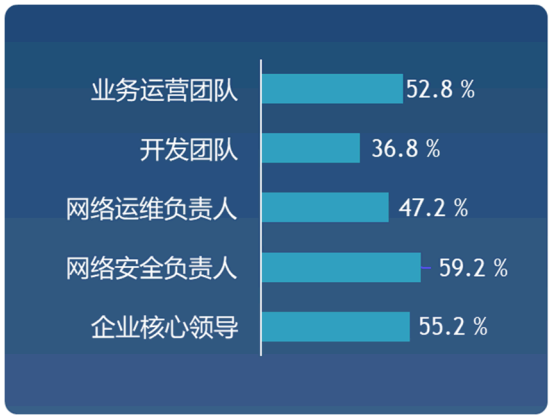


来源: IDC, 2021

零信任架构建设是一项长期工程，将会涉及企业众多业务系统和相关团队的配合，包括企业核心领导团队、网络安全团队、网络运维团队、业务运营团队等。因此，获得企业管理团队的认可和支持必不可少，很多企业会建立自上而下的项目管理体系，以促进零信任架构迁移的顺利进行。

图 9

贵司零信任网络建设过程中的主要参与方式有哪些？

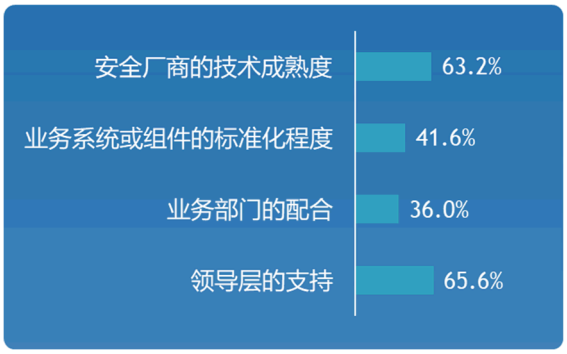


来源: IDC, 2021

当然，向零信任网络的转型对几乎所有企业的网络安全体系建设都是一次严峻的挑战。零信任相关技术仍需要持续的改进，各技术模块间的集成与协同仍需进一步完善，其在企业侧落地过程中不免仍将面对例如技术成熟度、产品和接口标准化，以及人员配合等方面的问题。

图 10

贵司零信任架构建设过程中的主要挑战有哪些？



来源: IDC, 2021

当然，在 IDC 调研过程中，我们也发现部分自身网络安全技术能力和研发实力较强的企业会考虑在零信任架构建设中逐渐增强自研网络安全产品和技术的融入，将零信任架构建设成为具备更强自主研发能力的工程，同时也便于充分利用自有团队对企业自身业务系统流程与规划的深入理解，更好地实现网络安全与业务发展的融合。

零信任市场发展趋势

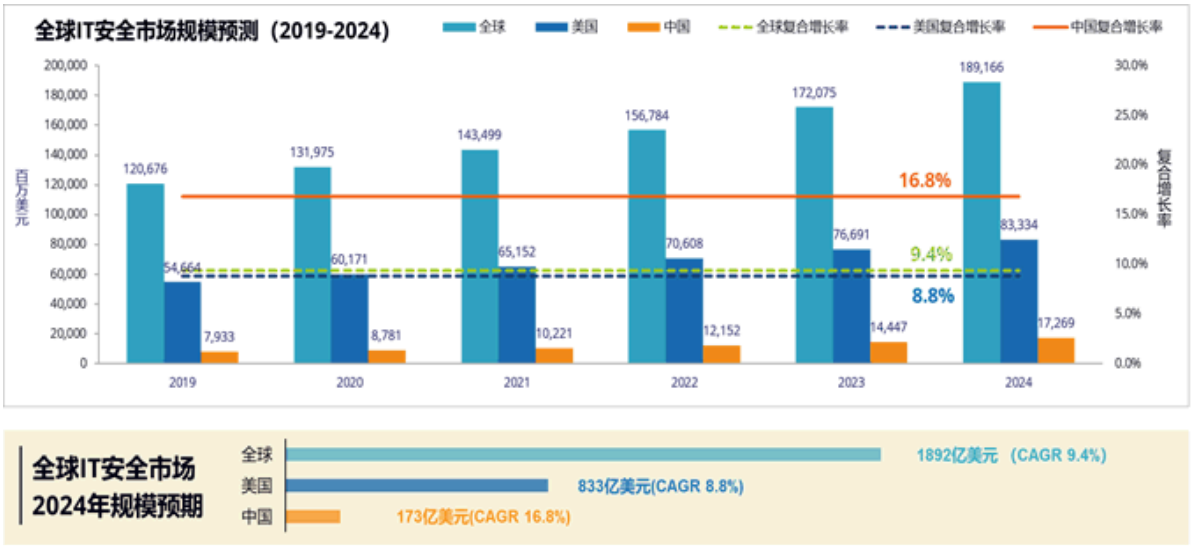
中国网络安全市场的发展主要由政策和威胁形势两大驱动力推动。从政策角度上看，2017 年 6 月 1 日，中国《网络安全法》正式生效，该法律明确了社会各个主体的义务，其内容涵盖了关键基础设施保

护、网络数据和个人信息保护、网络安全应急与监测等方面，保障了网络安全的空间主权和国家安全、网络产品和服务安全，以及网络运行安全，推动了中国的网络安全法制化进程，成为网络安全法制化建设的重要里程碑。2019 年 5 月 10 日，《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》以及《信息安全技术网络安全等级保护安全设计技术要求》三大核心标准正式发布，标志着等保 2.0 时代的到来。除此之外，2020 年，国家新颁布的《网络安全审查办法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法（草案）》等法律法规的也在不断提升政府、企业对网络安全的重视程度，提升组织甚至国家网络安全综合防护能力，推动整个网络安全产业发展。从威胁形势的角度上看，当下全球网络安全事件频发、攻击手段的多样化、智能化不断增强，攻击者隐蔽性的进一步提高使得全球网络安全形势变得愈发严峻，数字化转型平台变得更加“易攻难守”。

在此背景下，根据 IDC 最新发布的《全球网络安全市场支出指南 2021V1》，在政策与威胁形势的共同驱动下，到 2024 年，全球 IT 安全市场规模将达到 1,892 亿美元，2019-2024 年复合增长率达到 9.4%。中国 IT 安全市场规模预计将在 2024 年达到 173 亿美元，2019-2024 年复合增长率达到 16.8%，增速领先全球主要国家和地区。

图 11

全球 IT 安全市场规模预测（2019-2024）



来源: IDC, 2021

从软件、硬件和服务的产业结构发展来看，全球和美国 IT 安全产业结构以服务和软件为主，硬件市场规模仅占总市场不到 20%的比例。与之相反的是，中国 IT 安全的产业结构以硬件为主，软件和服务为辅，硬件市场规模占比在 2020 年达到了 47%。当然，IDC 也同时看到了中国市场产业结构的微妙变化。从 2018 到 2020 年产业结构数据来看，中国硬件市场占比在不断下降，软件和服务市场占比不断上升。IDC 认为，此类产业结构的变化调整主要是由软件平台类产品、云安全以及安全服务市场在中国的不断发展所引起。

根据《IDC 全球网络安全软件和硬件分类，2021》报告中对安全功能市场的定义，零信任理念的实现涉及到包括终端安全（Endpoint security）、身份和数字信任（Identity and digital trust）、网络安全（Network security）、网络安全分析、情报、响应和编排（AIRO）在内的几乎所有功能市场领域。在

零信任理念不断成熟和发展、全球市场持续关注以及中国网络安全整体市场高速发展的综合背景下，中国零信任市场在未来几年将迎来快速增长。

IDC 认为，零信任理念的核心是对企业资源和数据的安全防护，远程办公、数据中心、云计算（特别是多云和混合云）环境等，将成为对零信任网络安全防护体系需求最旺盛的应用场景。结合国内网络安全市场现阶段发展特色，未来几年国内零信任架构建设仍将以本地化和私有云模式为主。但随着企业上云步伐的加快，凭借云计算环境带来的便捷部署、灵活扩展、多租户管理等独特优势，公有云和混合云模式的零信任体系将占据越来越重要的位置。

技术买家零信任架构建设指南

新冠肺炎疫情的爆发客观上促进了各行各业对远程办公需求的提升，同时也更为鲜明地暴露出传统 VPN 方案的不足和隐患。作为零信任架构的关键能力之一，软件定义边界（SDP）迅速成为企业改善远程办公体验、降低互联网暴露面、提升业务安全性的重要选择。虽然 SDP 并不能涵盖所有零信任能力要求，但却能够帮助企业员工更直观地体验到零信任网络架构建设所带来的安全性和便利性，为零信任理念在企业中的快速拓展提供了基础。

IDC 希望提醒正在考虑零信任建设的广大企业级客户，当前声称具备零信任网络建设能力的厂商众多，企业需要认清零信任理念与传统网络安全防护方法的区别。IDC 重点关注零信任模型的三个主要能力，即软件定义边界（SDP）、增强身份认证（IAM）和微隔离（MSG）。零信任模型假设企业网络的失陷是不可避免的，或入侵已经发生，默认不再信任任何一个账户或设备，对所有业务系统和数据的访问都将受到基于安全策略、用户和设备属性等因素的限制，并进行用户和设备安全状态、网络活动和数据访问的持续监控。

IDC 提供以下几点建议，供广大技术买家选择和建设零信任架构时参考：

不因零信任建设而降低传统安全防护投入

零信任架构的建设不是“一键切换”能够简单实现的，需要长期规划和建设，企业因为零信任建设而降低企业原有安全防护体系的投入是不明智的选择，特别是零信任架构建设前期，零信任理念还无法全面覆盖企业所有业务系统和数据。零信任理念并不是对企业原有边界防护的彻底抛弃，而是互相补充和加强。无论是出于网络安全建设合规性还是网络安全防护完整性考虑，大多数企业将在未来几年的时间内保持传统边界防御和零信任架构同时建设的混合运营模式。

IDC 认为，全面梳理企业 IT 资产并进行数据资产的分级分类是实现企业网络安全整体防护的基础，也是零信任架构顺利实施的前提。因此，有较好企业 IT 资产管理和数据资产治理基础的企业在进行零信任架构迁移时，往往会更为顺畅和高效。

零信任的建设与业务紧密结合，需做好长远规划

网络安全管理人员需要通过充分的学习和预研，了解当前网络安全市场主要零信任架构提供商的技术能力和特点。结合企业数字化转型发展现状和业务长远规划评估零信任架构在企业网络安全体系建设中的必要性和可行性，并向企业管理团队汇报，帮助管理团队坚定零信任网络建设的战略，以获取企业整体政策和资源支持。

业务安全和数据安全在企业发展中的重要性迅速提升，企业需要认识到，最先进的零信任建设方案不一定是最适合自己企业的方案，企业应该结合自身业务的独特需求和未来规划选择最适用的零信任建设方案。选择可信的零信任服务商至关重要，企业需要服务商在项目建设的整个生命周期提供可持续的、不断迭代的服务支撑，建设框架或实现路径的变更将带来大量额外负担和资源浪费，降低企业管理团队和业务部门的项目建设信心。

自身网络安全技术能力和研发实力较强的企业，可以考虑在零信任架构未来建设中逐渐增强自研产品和技术的融入，将零信任架构建设成为具备更强自主研发能力的工程，同时也便于充分利用自有团队对企业自身业务系统流程与规划的深入理解，更好地实现网络安全与业务发展的融合。

零信任体系的持续完善需要关注安全生态

企业还需要认识到，零信任的实现是一个复杂的工程，很少有单一的服务商能够提供所有零信任所需的能力或产品，安全服务商围绕零信任框架打造的合作生态能够帮助企业构建更为完善的零信任体系。同时，零信任本身也需要逐步的成熟，企业应清晰梳理服务商目前提供的零信任能力在整体零信任架构中的影响范围，未来还有哪些能力需要持续补充或强化。

IDC 认为，当前大多数企业建设的零信任网络体系中的安全信息仍然相对比较独立，企业在进行了初期的试点应用后，应该充分利用技术提供商及其合作生态的整体方案能力，在零信任网络架构中更多地融入威胁情报、数据安全、网络威胁态势感知等能力，并增强威胁事件的可见性和自动化响应，以有效应对不断涌现的新兴威胁。

关注人的因素

企业应该意识到，人仍然是零信任架构实践过程中最关键的因素。零信任架构迁移是一项长期工程，可能涉及企业众多业务系统的改造，获得企业管理团队的认可和支持必不可少。因此，网络安全团队需要向管理团队明确阐述零信任体系的建设标准和目标，及对企业收益的影响。由企业管理者亲自挂帅，建立自上而下的项目管理体系，促进零信任架构迁移的顺利进行。IDC 认为，采取有效的激励措施奖励主动完成零信任改造的业务团队是个不错的方式，一方面，可以提升业务团队配合迁移的积极性，另一方面也能够提升相关团队的荣誉感和获得感。同时，企业需要对各类员工进行针对性的网络安全意识和岗位技能培训，使员工意识到企业正对其网络行为进行严格的安全审计，使其了解维护网络安全的职责和惩戒措施，降低内部员工有意或无意操作造成的网络违规风险。

企业网络安全防护体系的建设不仅需要实现法律合规，还应有专业的安全人员在熟悉企业各项业务特点和需求的前提下，结合企业整体发展战略帮助企业打造量身定制的网络安全防护体系，并通过专业的安全运营充分发挥体系的应有能力。因此，零信任体系的运营与规划、建设同等重要。零信任体系需要安全运营人员（可能来自专业安全厂商，也可能来自企业自建安全团队）结合企业现实业务的发展和系统使用过程中出现的切实问题持续优化模型和策略，并对攻击事件进行深入分析和溯源。

中国市场零信任理念最佳实践

海信集团最佳实践

海信集团成立 52 年来，坚持“诚实正直、务实创新、用户至上、永续经营”的核心价值观和“技术立企、稳健经营”的发展战略，业务涵盖多媒体、家电、IT 智能信息系统和现代服务业等多个领域。随着集团数字化转型的快速推进，海信正在实现由传统“家电公司”向“高科技公司”的华丽转身。

海信集团是一个全球性集团公司，长久以来对企业系统开放到互联网的必要性十分重视，对信息安全也有着严格的要求。随着数字化转型的不断深入，海信集团将越来越多的核心应用迁移到云计算平台和互联网，企业的服务范围已经远远超出了原有内部网络边界，企业业务系统走向了更开放的生态模式，由此面临的来自互联网的恶意威胁越来越大。2020 年的新冠肺炎疫情更进一步推动了远程办公业务需求的增长，这也加速了企业对这些开放到互联网上的应用的保护进程。以上诸多因素促使该集团一直在寻求更完善的信息安全解决方案，有效防护企业 IT 资产和数据安全，并帮助全球员工安全地接入业务系统，便捷地开展日常工作。因此，海信集团从 2018 年开始调研零信任网络框架相关的技术和管理思路。

海信集团从 2020 年开始与指掌易合作进行 SDP 零信任网络框架的建设，并与集团原有 IAM 系统紧密集成。未来长期建设目标是把企业内部所有开放到互联网的资产进行全面保护。由于该集团业务种类众多、数据资产庞大，且已经构建了复杂的网络体系，面对应用实践仍然较少的零信任理念转型需求，该集团建设规划比较谨慎，并采用分步实施的总体策略，在现有网络架构的基础上进行逐步替代，为用户打造相对无感的网络切换环境。

该集团零信任网络防护理念的转型受到了相关领域领导的重点关注，从顶层设计推动项目顺利开展，并要求业务系统应用部门深度参与，从业务系统面临的实际问题、场景和风险出发，提出零信任建设需求。同时，面对集团数万员工的业务安全访问需求，专业的安全运营非常重要，如何能够帮助员工切实理解网络安全防护的重要性，主动配合信息安全部门完成新安全策略的下发，并真正将部署的安全能力充分利用起来，也是他们一直探索实践的重要部分。

当然，海信集团零信任理念转型的不同阶段也持续面临相应的挑战。例如该集团十分重视企业数据资产的安全防护，随着网络开放性的提升，企业网络安全防护体系需要在满足业务发展需求的同时，保障数据的合法合规访问和使用，这促使网络安全团队主动学习国内网络安全市场的新兴技术和理念；在确定了零信任理念作为企业网络安全建设方向以后，如何选择最贴切集团业务安全需求的方案提供商成为重要挑战，因此，该集团经历了漫长的方案选型和概念验证（POC）测试，对比了众多安全提供商的方案，最终选择了指掌易的 SDP 零信任框架作为零信任理念的实践方案。在零信任建设过程中则需要适配海信集团现有的庞大网络架构和业务流程，与众多品牌服务商提供的业务系统和安全产品紧密集成，减少系统建设过程中对已有业务的影响。今后，在零信任架构的内部应用推广过程中，也必将面临如何说服企业不同级别的业务应用使用者配合落实网络安全防护体系转型的挑战。

通过一年多的持续考察论证，海信集团的零信任网络架构建设思路已经取得了显著的成效。从实施推进的具体路径上，从覆盖的业务系统范围来看，目前该集团的零信任架构重点关注于 OA 系统、邮件系统、移动办公平台等使用范围广泛，用户级别较高的业务，且已经覆盖了庞大的用户群体。未来将不断接入更多数量和种类的 IT 资产和业务系统，例如，把零信任框架扩展到集团的信息开放程度和保密要求都比较高的业务营销域，在帮助经销商、服务商、一线促销员等终端用户做好数据安全防护的基础上，提升网络接入效率和业务访问合规性。帮助企业网络安全防护突破传统内外网边界的限制，有效收缩企业网络暴露面，提升对接入终端的持续认证能力的同时，改善员工远程办公的便利性和安全性。

海信集团信息安全建设核心人员认为：零信任理念是未来企业网络安全防护体系的重要发展方向，希望随着我国网络安全技术的不断完善，未来能够通过一体化的零信任体系建设减少企业信息系统间的信息孤岛，实现企业数据的安全流通。

上海汽车乘用车公司

上海汽车集团股份有限公司乘用车公司，是上海汽车集团股份有限公司的全资子公司。上汽集团作为国内规模领先的汽车上市公司，努力把握产业发展趋势，加快创新转型，正在从传统的制造型企业，向为消费者提供移动出行服务与产品的综合供应商发展。随着上汽集团数字化转型进程的不断推进，企业对移动办公的业务需求迅速增加。数字业务的快速发展促使企业越来越倾向于营造开放式办公环境，鼓励员工携带自有设备办公（BYOD），同时能够帮助企业节约 IT 投资。但这也在很大程度上为企业网络安全的全面有效防护提出了新的技术挑战。

为了弥补上海汽车乘用车公司信息系统原有虚拟专用网（VPN）的多项不足，例如 VPN 服务端口直接暴露在互联网、对接入企业网络的设备和账号缺少安全检测以及持续的认证和访问控制等，上海汽车乘用车公司从 2020 年开始进行零信任网络架构的规划和建设，希望通过网络架构的零信任改造，隐藏企业服务、收窄信息系统互联网暴露面，并实现对接入设备的持续安全验证和细粒度授权管控。

上海汽车乘用车公司通过在原有网络安全防护体系基础上逐步迁移的方式，正在小范围试用由专注于移动业务安全领域的专业安全公司指掌易提供的 SDP 零信任解决方案。利用 SPA 单包授权、最小化授

权、持续信任评估等技术，将企业业务应用从互联网隐身，避免被恶意威胁扫描和攻击，以保障业务访问的安全性。当前，上海汽车乘用车公司零信任网络建设主要集中在移动终端的安全接入，涉及到的业务系统包括企业资源计划（ERP）系统、办公自动化（OA）系统等。

同时，上海汽车乘用车公司零信任网络的建设规划完全以业务需求为核心引导，并尽量减少对相关业务系统的大规模改造。这个过程的主要参与人员包括网络安全团队、网络运维团队、业务研发团队、以及业务使用部门等。由于该公司自有的网络安全团队规模并不大，如何加强各团队间的协同工作变得尤为重要，特别是业务使用部门的密切配合。网络安全团队需要能深入了解各业务的具体需求，才能更顺利地实现零信任理念的落地。

零信任网络的构建需要与上海汽车乘用车公司原有的身份安全管理系统紧密集成。得益于该公司原有身份管理系统建设相对完善，有着明确和细致的权限管控，零信任框架落地过程中可以直接获取原有配置信息并加以优化和使用，减轻了 IT 人员大量工作负载。同时，通过与公司部署的终端安全和准入系统的配合，目前该公司的零信任网络实现了实时获取移动终端的安全状态，并进行信任度评估，从而动态调整终端或账号的权限设置。

上海汽车乘用车公司网络安全负责人认为，零信任理念是未来网络安全建设的大势所趋。当前企业关键应用和数据的使用场景正在发生较大的变化，网络开放性逐渐提升，零信任理念的引入能够有效帮助企业应对越来越复杂的新兴威胁。因此，上海汽车乘用车公司对于零信任网络框架的建设有着较为长远且清晰的规划。在经过充足的应用效果验证后，零信任的应用范围将涵盖更多的终端类型和数量，包括各类移动终端和个人电脑终端等，从而实现更为丰富的 BYOD 能力，并在未来完全替代公司现有的传统 VPN 方案。但作为零信任理念最终的践行者，企业也清晰地认识到，目前国内网络安全市场零信任框架提供商数量众多，且基本都能够满足零信任网络架构的基础能力，但提供商的综合技术能力还需要持续提升，从而帮助企业打造更为完整和专业的零信任网络。

某钢铁集团

某钢铁集团是多元协同发展的集团化企业，构建了钢铁及产业链延伸产业、战略性新兴产业协同发展的产业格局。随着数字化转型进程的持续推进，该钢铁集团正处于加快转型升级、迈向高质量发展的关键时期。

该钢铁集团从 2019 年开始做基础网络改造项目的技术研究和方案设计，网络安全防护体系是该长期项目里非常重要的部分。但随着业务实践中不断的经验积累和技术演进，传统安全防护手段的缺陷和隐患逐渐暴露出来。虽然通过部署多种安全防护产品形成对企业网络环境大而全的保护体系，且覆盖当前国内网络安全技术的众多领域，但面对业务应用的互联网化需求普遍增强，全球恶意威胁、网络攻击的隐蔽性和复杂性逐年提升这一显著趋势，该集团已经越来越直观地感受到传统基于边界的网络安全防护体系已经无法满足企业对防护有效性和实时性的要求。因此，该钢铁集团通过长期和严格的市场调研，最终选择了零信任作为企业未来网络安全防护体系的指导理念，希望利用零信任网络架构的持续验证，永不信任的机制更好的应对新兴威胁对业务的负面影响，同时满足该集团对技术领先性和投资保护的要求。

该钢铁集团最关心的是零信任相关技术的成熟度，因此，在选择服务提供商时会比较关注厂商的典型案例的落地情况、对行业标准的贡献以及与企业现有安全体系的对接能力等。在充分对比分析了中国市场多个网络安全提供商的技术能力和方案特色以后，该钢铁集团结合自身业务特点和网络安全需求选择了腾讯安全的零信任建设方案。零信任网络架构的建设和迁移是一项长期工程，尤其是对于钢铁集团这样的大型企业来说，更是会涉及众多部门的共同参与。安全管理团队通过合理的规划和紧密的沟通，在项目建设过程中形成了自上而下的项目管理体系，得到了企业管理层的大力支持和相关业务部门的充分配合，保障了企业整体零信任体系长远规划能够有条不紊的顺利实施。

当前，该钢铁集团的零信任建设包含了身份安全、终端管控、网络准入等多项网关能力，涉及的系统涵盖集团的各级应用，包括办公系统、生产管理系统和过程控制系统等。通过零信任网络架构建设，该集团不但实现了对接入终端的统一管控，有效隐藏了企业中众多的后台应用，还实现了企业员工权限的最小化、精细化管理。经过长时间大范围的试运行后，零信任网络架构将被应用到包括该钢铁集团工控安全领域在内的全业务领域，并进行零信任体系与网络安全运营平台的对接和联动分析，进一步提升集团网络安全防护体系的整体性和智能化。同时，该钢铁集团还将组织针对性的企业内部攻防对抗演练，从而深入验证零信任理念在企业各业务系统中安全防护的有效性和便利性。

某物流公司 A 最佳实践

某物流公司由于业务特点和商业运营需求，其系统中保存有海量用户数据，因此该企业一方面需要对数据进行严格的访问限制和数据保护，另一方面又需要将数据合理地开放给企业内部员工、快递人员以及外部合作伙伴，以支撑商业的正常运营。传统基于边界的网络安全防护理念已经无法满足该企业数据安全防护的需求。零信任理念基于身份而非网络位置来构建业务访问认证体系，更能贴合该企业的业务场景，因此，该物流公司从 2020 年开始规划针对全栈业务系统的零信任整体网络架构的转换。

目前该物流公司的全栈应用系统都已经部署到华为云计算平台。同时，通过对国内众多零信任服务商的技术能力及业务贴合度评估，该企业最终选择华为云作为零信任网络架构建设服务商。从建设模式来看，该企业的零信任建设是基于原有网络安全防护架构进行逐步迁移，同时保持原有业务系统能够正常运行，不能因为项目建设影响企业日常的商业活动。

该物流公司的零信任架构整体建设将按照身份安全、软件定义边界、微隔离的部署顺序逐步进行。得益于企业比较先进的数字化转型建设基础，零信任架构与其他业务系统对接和数据迁移过程均比较顺利，未带来明显的工作负载压力。当然，目前该企业的零信任系统架构仍然处于全面深入的概念验证（POC）阶段，尚未进行大规模迁移，但很快会将企业中部分易受攻击的业务系统先迁移至零信任架构，并逐渐完成所有业务系统的迁移工作。

目前，该物流公司已经实现了零信任架构与原有数据安全系统的交互，能够对敏感数据访问进行细粒度审计和权限的动态评估。未来还将加强动态访问控制引擎和信任评估引擎的建设，并实现零信任与企业态势感知系统的协同交互，提升企业整体网络安全防护能力。

该物流公司对于零信任理念落地实施后能够实现的能力和系统建设目标有着清晰的认识。与大多数企业的零信任建设需求主要由网络安全管理团队发起不同，该企业零信任项目的发起源于企业核心领导团队。其领导团队深刻了解企业自身业务特点和企业数据面临的各种安全风险，清晰地认识到传统的安全防护手段无法有效应对黑灰产、内鬼等窃取企业数据的恶意威胁，从而建立了自上而下的项目管理体系。除了领导团队的认可与支持，零信任项目还需要企业众多团队的参与和配合。例如，网络安全团队需要重新定义整体网络安全架构，网络运维团队需要进行大量的系统适配、迁移等工作，研发团队需要提供系统开发和系统调整等支持。如果缺少各个团队的积极沟通和密切配合，零信任项目的推进必然将在多个环节遭遇挑战。

该物流公司网络安全负责人认为：目前国内零信任理念的发展仍然处于早期阶段，各类厂商百家争鸣，纷纷借助零信任概念以不同的方式优化自身技术和方案，但整体能力仍有较大提升空间。未来，云计算、移动办公、远程办公、物联网等企业应用场景将在商业运营中普遍应用，企业的 IT 基础设施必将随之日益复杂，传统的网络安全防护方式很难充分应对来自企业内外部的复杂网络攻击。零信任理念通过多维度的持续的身份认证和风险评估，围绕企业关键资产构建动态安全边界，有效抵御外部攻击和内部人员的作恶。

某物流公司 B 最佳实践

作为物流领域的综合性领先企业，该企业已构建了一套面向国内及全球客户的一体化综合物流解决方案基础能力，以客户需求为驱动、以业务数据为牵引，有效利用云计算技术平台和大数据分析平台提供涵

盖从核心配送端到多环节价值链前端的全链路、智能化物流解决方案。随着 2020 年全球新冠肺炎疫情爆发，迫使该企业大范围开启远程办公模式。但受限传统远程办公模式的局限性，面临着非合规终端访问企业内部系统所带来的数据安全挑战。因此，为满足该企业自身随业务快速变化的内外网安全访问需求，该企业开启了对零信任理念的重新思考。

经过严格的市场调研和品牌选型，该企业最终选择了腾讯零信任安全管理系统（iOA）做为该企业的软件定义边界（SDP）零信任解决方案，并与企业自研的身份安全管理系统紧密集成。经过一年的持续建设，该企业的零信任体系已经在企业内迅速推广并得到大规模应用，实现了数十个业务系统的内外网无差别访问，并根据职责权限进行细粒度访问控制。该零信任体系会对接入终端进行合规状况动态检测和评估，例如终端上是否安装了安全防护软件、是否存在高危漏洞、补丁是否及时更新、设备基线配置是否符合企业安全策略要求。同时，这些终端安全检测信息还将发送给对应业务系统的安全模块，进一步分析和判断接入终端的安全级别是否可以访问该业务系统，实现灵活的权限管理和访问控制。

该企业作为物流行业数字化转型践行者，已经构建了扎实的信息系统标准化架构以及配套的安全防护体系，其良好的数字化转型基础为零信任网络框架建设提供了有利的条件。随着零信任能力的不断完善，未来该企业还将实现移动终端、员工自有设备的零信任接入，不但会对所有终端的访问行为执行严格的审计，还将进一步规范终端的数据访问控制，帮助该物流企业数万员工实现一体化的身份管理、终端管理、访问控制等。

该物流企业网络安全管理人员认为，零信任理念目前的应用场景主要集中在各类终端从内网网无差别接入时的可信性认证，但企业的网络安全防护不应仅局限在网络边界的访问控制，还需要关注终端异常行为、数据访问的合规性、潜在的网络安全风险等，通过建设完整的企业安全感知、响应、处置、溯源体系实现网络安全闭环管理能力。

中国零信任架构提供商解决方案介绍

迪普科技

企业介绍

杭州迪普科技股份有限公司（以下简称“迪普科技”）以“让网络更简单、智能、安全”为使命，聚焦于网络安全及应用交付领域，是一家集研发、生产、销售于一体的高科技企业。

自成立以来，迪普科技坚持技术创新。公司拥有一支专业的软件开发及硬件逻辑开发团队，打造了独有的高性能分布式转发硬件架构和 L2-7 融合式操作系统。在此基础上，依托于安全研究团队十多年以来在攻防研究、漏洞挖掘、威胁情报分析、安全事件响应等技术积累，公司开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术，构建了包括自安全网络、安全检测、安全分析、安全防护、安全服务、应用交付在内的产品体系，为客户提供全场景网络安全解决方案。

迪普科技的用户覆盖了政府、运营商、电力、能源、金融、交通、教育、医疗、企业等在内的各行各业，并承担了二十国集团（G20）峰会、亚太经济合作组织（APEC）峰会、世界互联网大会等重大活动的网络安全保障支持。未来，迪普科技将继续在网络安全及应用交付领域持续投入，不断完善产品与解决方案，为客户创造更大价值。

迪普科技零信任解决方案介绍

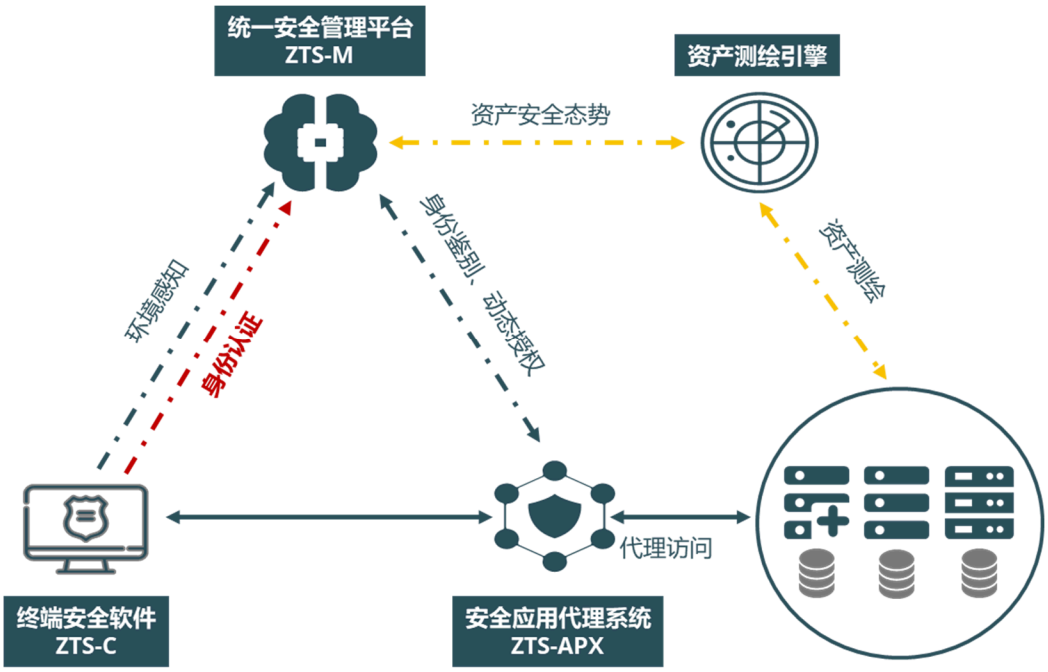
迪普科技零信任相关产品设计以：“彻底消除网络中的默认受信机制，假定所有网络环境均具有恶意性质”为设计理念，严格遵照零信任的基本原则对整体方案进行分解实现组合落地，这种方式不仅能够让零信任的网络架构在客户网络中轻松实践，也能够更好的适用不同的网络环境，最终实现向零信任网络安全架构转型的最终目标。

核心技术和框架

- **双重单包认证（SPA）身份认证技术：**产品采取双重 SPA 身份认证技术，能够实现网络应用真隐身，彻底消除扫描攻击、DDoS 攻击等安全隐患。
- **先认证后连接的接入方式：**通过双重 SPA 身份认证技术的方式，产品可以实现完全的先认证后连接的接入方式，而并非还需要建立连接来传输相关认证数据。
- **前向安全加密隧道技术：**采用一次一密不可逆的前向加密方式，能够保证即使在安全密钥泄露的情况下，也不能够破解、泄露已经发送的信息。
- **双向身份安全认证技术：**访问过程中，不仅仅认证终端的身份，同时也认证工作负载的身份情况，保证合法的身份访问合法的应用。
- **集成基于时间戳算法的一次性密码（TOTP）令牌二次校验：**产品集成了基于 TOTP 的口令分发和校验功能，可通过用户绑定邮箱，动态下发二维码口令，每个用户的二维码口令均是独一无二的。
- **自动识别选择加密方式：**可自动识别终端位置情况，针对不同网络环境，采取不同的加密方式，包括：隧道加密方式、七层应用加密方式等，能够适用更多的复杂和特殊网络。
- **纵深安全风险评估框架：**对访问过程中的主、客体分别进行全方位风险评级，根据安全指数判别访问主客体的访问关系，让风险分析做到实时、动态、可实用，不再仅是一纸定期报告。
- **基于角色的访问控制（RBAC）权限管控：**产品支持 RBAC，融合了基于多属性的角色授权管理机制，可将角色赋予给不同的用户组，用户组可关联多维属性及多维策略，实现健全的以身份为中心的权限管控机制。

图 12

迪普科技零信任核心模块与能力



来源: IDC, 2021

核心模块与能力

- **持续纵深安全风险评估模块：**该功能模块能够对整个访问过程中的访问主、客体进行持续的安全风险评估并动态调整安全指数，为动态策略分析计算调整模块提供条件支撑。
- **动态策略分析计算调整模块：**可根据不同的安全指数结合大数据和 AI 人工智能算法对既有策略进行动态调整，保障系统和终端的双重安全。
- **多维身份信息认证（MFA）能力：**可基于多种信息对访问主客体进行双向的身份认证。
- **多终端安全一体化管理能力：**可对接入的多类型终端进行统一的安全管控。

迪普科技零信任相关产品基于两次 SPA 单包敲门技术，将首次安全访问放入安全缓冲区，极大地缩小了应用的网络暴露面，实现应用真隐身，能够大幅消减端口扫描、DDoS 等多种网络攻击。通过产品功能模块化，实现零信任架构相关产品的无缝对接组合落地。产品除了提供用于认证的环境感知的轻量客户端以外，还可提供集成终端检测与响应（EDR）、终端杀毒、终端管理以及 SDP 功能的融合客户端，可兼容各种主流操作系统，通过融合客户端可更加深层次地检测入网终端的安全性和可靠性。为了适应云计算时代的发展，产品实现了对云原生需求的紧密支持，能够很好地继承云计算环境的诸多优势特性，实现灵活的弹性扩展能力。同时，迪普科技零信任相关产品还可以与第三方云管理平台进行对接，通过云管理平台的接口实现对不同品牌和种类的其他安全产品进行策略下发，帮助企业实现网络安全防护体系的协同联动，打造更为完善的安全生态。

华为云

企业介绍

华为云是华为的云服务品牌，将华为 30 多年在 ICT 基础设施领域的技术积累和产品解决方案开放给政企客户，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”，推进实现“用得起、用得好、用得放心”的普惠 AI。

华为云将围绕零信任，以应用信任中心（Application Trust Center，ATC）服务为核心，打造持续动态信任风险评估与响应的应用安全防护体系。客户安全管理员能够通过 ATC 服务实时地、清晰地了解自己应用的资产拓扑、脆弱性分布、安全事件及风险态势，并依托华为公司多年网络安全防护经验设置静态、动态防护策略，结合华为云安全产品之间联动，实现设备、身份、行为、应用、数据等多层次的持续、细粒度访问控制和权限管控，落地零信任理念。

华为云零信任解决方案介绍

华为云 ATC 服务针对客户在实际安全防护工作中面临的痛点，在应用维度为客户清晰展示应用资产拓扑及安全风险分布，让客户感知安全态势，知其必防。ATC 服务将服务安全状态作为策略因素参与到整体零信任防御体系中，在服务不同的脆弱状态下，利用大数据分析技术动态改变访问控制策略。同时，ATC 服务集成华为云数据安全中心服务，支持获取客户应用资产中的敏感数据分布信息，通过持续监控主体对敏感数据的访问行为，利用大数据分析平台能力识别异常行为，实时提示安全风险并根据客户的策略配置可终止访问或对用户的身份进行增强认证。

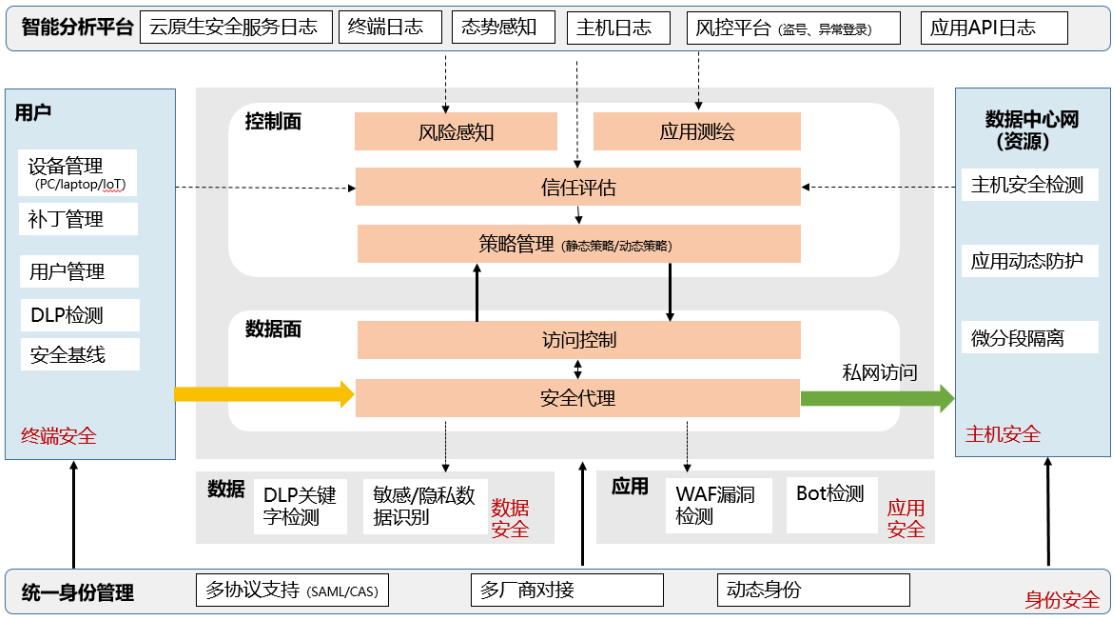
华为云零信任安全体系发挥云原生优势，与虚拟化平台、公有云/混合云/私有云平台的各组件和服务充分集成，并且依托华为公司多年网络安全防护经验，力求为客户提供更全面的应用资产拓扑可视、更精准的安全风险分析、更实时的防护措施联动，解决客户在安全防护中的痛点。华为云零信任安全体系设计本着开放、互联、协作原则，通过标准协议接口与第三方组件集成，与相关产品形成合力，构建更加完整的零信任安全体系。

- 核心模块与能力

华为云零信任安全体系以 ATC 服务为核心，集成云平台其他基础服务、安全服务、运维服务、软件开发平台服务的相关信息，以应用为维度进行关联聚合，并依托零信任安全理念实现细粒度访问控制和权限管控，加固安全防线。 ATC 服务的核心模块如下图所示：

图 13

华为云核心模块与能力



来源: IDC, 2021

- 核心技术或框架

1）应用安全风险测绘

围绕应用维度，全面采集客户业务的资产类型、数量、网络关联组件信息，形成全链路网络拓扑。结合华为云安全服务产品，资产漏洞发现、网络攻击告警等信息，识别应用安全风险，并进行可视化展示，帮助客户一目了然地识别应用风险，持续提高安全水位。

2）应用资产隐身

基于云原生网络服务能力，不需要额外的部署操作即可将原来暴露在公网的服务进行隐藏，仅对通过认证且经过持续信任评估授权的人员和设备可见。

3）多维度信任度量加速

采用快速匹配算法，从人员、设备、行为、应用等多个属性维度，评估访问主体的可信度。基于华为云 AI 平台、机器学习大数据分析技术，持续监控访问主体行为上下文，识别主体异常行为，并进行联动。

4）多重身份管理、认证协议支持

集成华为云 IDaaS 产品，支持密码认证、短信认证、动态口令验证码、微信认证、微博认证、钉钉认证和 Welink 认证等十余种认证能力。客户可以直接创建身份源，也可以将企业微信、钉钉、本地 HR 系统中的身份数据作为身份源导入。

5）多重网络协议支持

安全防护网关同时支持反向代理和软件定义边界（SDP）的模式，支持访问主体客户端与应用资源间三到七层网络连通，支撑 Web 应用、远程运维 SSH/RDP 连接和 C/S 架构访问连接等多种办公场景。

6）多种组合惩罚措施支持

基于 ATC 服务细粒度的控制策略和风险识别能力，配合 IDP（云原生和生态厂商）的多种认证挑战，ATC 实现客户自定义不同条件组合下的灵活惩罚措施。访客在应用、API 等不同粒度下命中规则，可触发针对该维度的响应措施，包括踢下线、要求短信认证、邮箱认证、验证码等。

7）生态伙伴支持

为了将业界优秀的生态伙伴能力注入到 ATC 服务，华为云借力传统安全厂商，共同构筑零信任开放的生态系统。在应用超市引入终端安全厂商、入侵检测/防御厂商、软件定义边界（SDP）厂商，并制定与 ATC 服务联动的接口标准，取长补短，帮助客户打造更加完备、灵活的零信任解决方案。

腾讯安全

企业介绍

腾讯安全作为腾讯立足互联网安全的行业品牌，致力于成为产业数字化升级进程中的安全战略官。依托 20 多年业务安全运营及黑灰产对抗经验，凭借行业知名安全专家、完备的安全大数据及 AI 技术积累，为企业构建“情报——攻防——管理——规划”四维安全战略，并提供紧贴业务需要的安全最佳实践，为政府及企业的数据、系统、业务安全，为产业数字化升级保驾护航。

腾讯安全产品与服务涵盖云计算环境与传统网络环境，帮助企业级客户实现便捷、高效、稳定的安全能力接入。腾讯安全为全行业用户提供包括业务安全、数据安全、身份安全、应用安全、终端安全、网络安全、安全管理、以及安全服务八大模块共计近百种产品与服务，同时根据行业不同属性、不同场景提供更加完整的多元化、多模式解决方案。

网络空间的安全需要有匹配复合网络空间的立体防御系统，任何一张网都是由线构成，腾讯云也会跟更多行业伙伴一起共建安全大生态。腾讯安全将以云管端协同的智慧生态，为用户持续提供安全的、可信的、智慧的安全环境，助力更多企业高效迎接数字化浪潮，实现各行业企业安全发展。

腾讯安全零信任解决方案介绍

腾讯搭建零信任架构的主旨就是实现实现无论员工位于何处（Anywhere）、使用何应用（Any application）、使用何设备（Any device）都可安全访问企业资源以进行任何工作（Any work）。

核心技术和框架

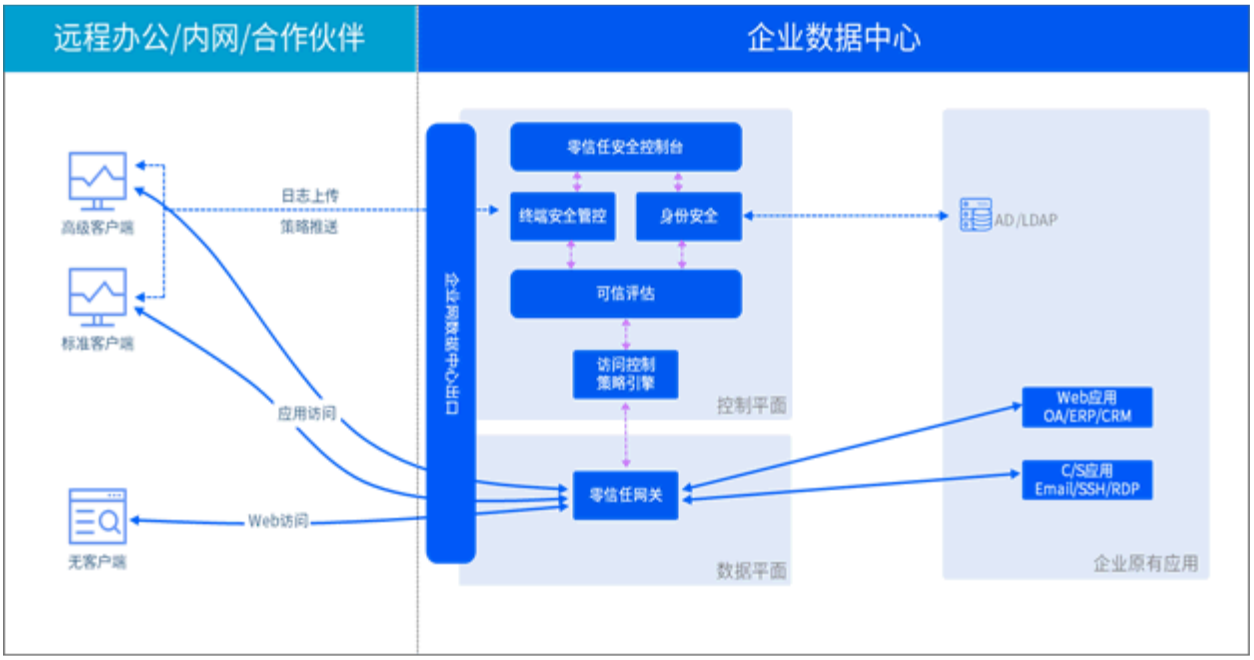
腾讯零信任安全管理系统（iOA）基于终端安全、身份安全、应用安全、链路安全等核心能力，对终端访问过程进行持续的权限控制和安全保护，实现终端在任意网络环境中安全、稳定、高效地访问企业资源及数据的产品。同时， iOA 提供 SaaS 和私有化两种部署方式，并支持有端和无端两种模式，企业可以按需选择。

- 对于终端安全，iOA 集成了全方位的终端管控功能模块，持续检查设备安全状态，限制任何不符合安全要求的设备对企业网络的访问。

- 对于身份安全，iOA 适配多种身份认证方式，针对用户/用户组制定网络访问策略，非授权的应用完全不可见，做到最小特权的需求。
- 对于链路安全，iOA 采用独有的访问链路加密/解密网关，针对设备指定 WEB 或应用程序流量层层加密，对不稳定网络做网络传输协议优化。
- 对于应用安全，iOA 支持细粒度识别应用和进程，远程下发进程黑名单，发现恶意程序即拦截访问，无法建立连接接入。

图 14

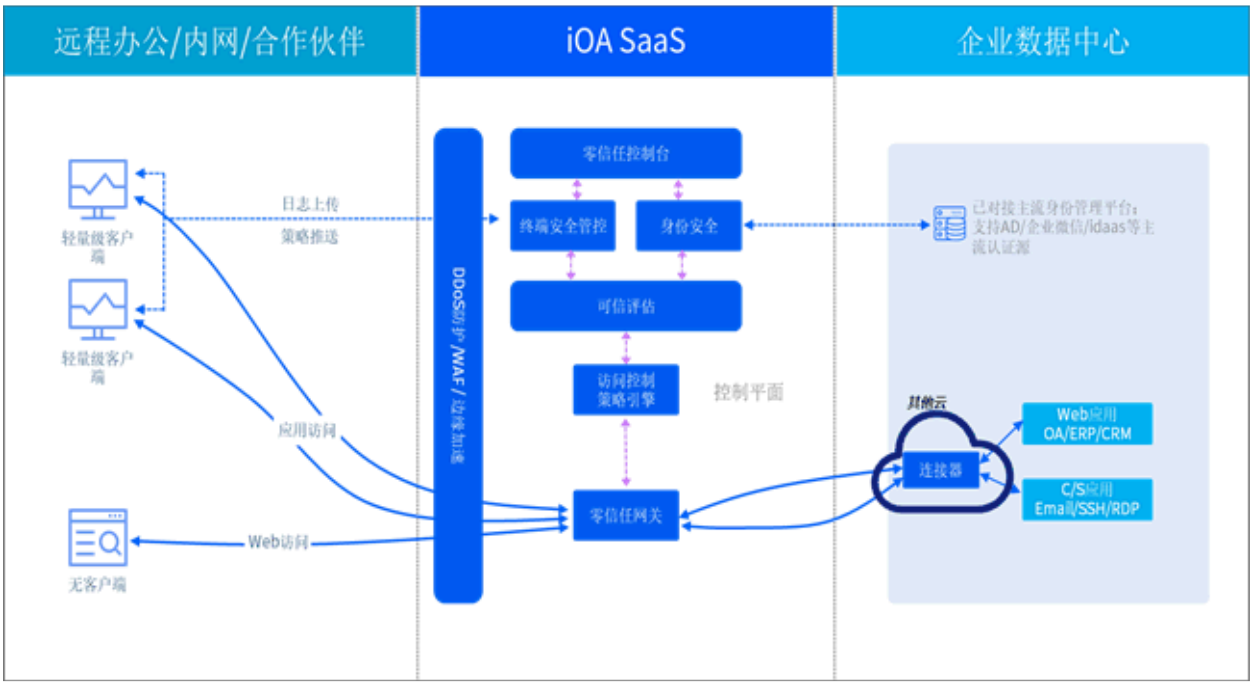
零信任安全部署 —— 私有化部署



来源: IDC, 2021

图 15

零信任安全部署 —— 腾讯云 SaaS 部署



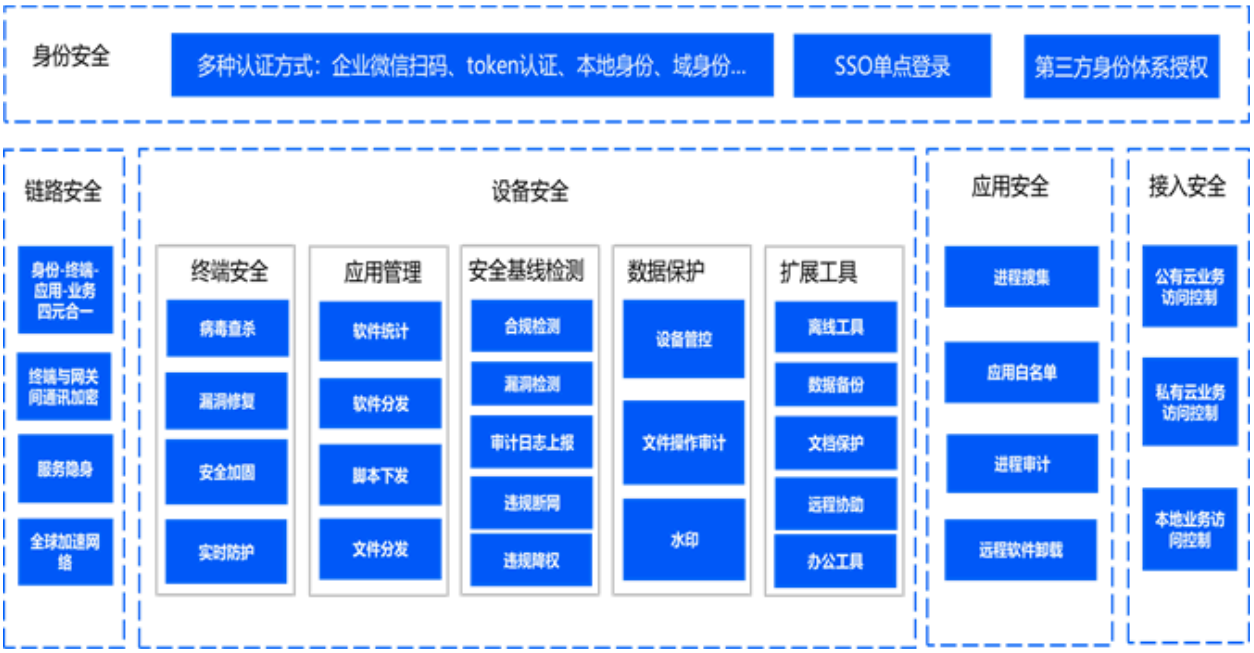
来源: IDC, 2021

核心模块与能力

- 身份安全模块：iOA 对接企业的身份管理系统，以及根据配置的授权管理，通过扫码、密码等方式实现员工的身份认证。
- 设备安全模块：设备可信是安全很重要的一环，也是腾讯长期的能力沉淀，依托腾讯超过 20 年的基础安全技术积累，通过病毒防护、漏洞修复、安全合规等手段实现设备环境的可信。
- 应用安全模块：历史上众多通用工具都爆出过严重的安全问题，正规软件也未必是安全的，iOA 可根据业务情况，指定和控制特定版本的应用对系统的访问权限。
- 链路安全模块：企业业务的互联网接入成为常态，敏感数据在互联网上传播面临诸多安全挑战，iOA 通过严格的链路加密、安全校验保证数据传输不被黑客劫持和嗅探。
- 接入安全模块：iOA 对公有云、私有云以及本地业务访问都有较为完善的访问控制和安全审计功能。

图 16

腾讯零信任产品 iOA 核心模块



来源: IDC, 2021

基于这几大安全原则基础上，整个系统是一个动态监测的系统，持续验证，永不信任，来实现整个职场安全和运营体系的构建。

腾讯 iOA 零信任核心技术创新和优势

腾讯安全通过 20 多年的安全实践，在病毒查杀、漏洞修复以及安全合规策略方面积累了大量的技术和经验。基于多步行为判断的主动防御云引擎可根据样本的系列行为特征进行综合风险判定，并在后台大数据训练集群支持下，对比传统的根据单步行为规则来做监控的方式，获得更高的主防技术安全系数，更强的捕获风险能力。由此实现腾讯零信任安全管理系统（iOA）较为完善的设备安全防御能力。

iOA 对网络访问发起方采用应用白名单模式，仅满足安全要求的进程可以发起内部访问，减少供应链攻击、未知恶意代码执行渗透扫描。iOA 采用按需建立连接的方式保护链路设计，不采用传统的安全隧道模式，从而释放业务系统的并发访问能力。另外，iOA 还具备终端加速和分布式抗 DDoS 能力。

腾讯零信任除了在技术上不断创新和突破，在生态合作以及国内外标准上也在不断突破。2019 年，腾讯主导并起草国际电信联盟电信标准分局（ITU-T）零信任国际标准立项，推动全球零信任标准化应用。2020 年 6 月，腾讯作为中国零信任产业标准发起者，联合公安三所、国家互联网应急中心、中国标准化研究院在内的超二十家中国知名企业和政府机关建立零信任生态联盟，发布适应中国市场的零信任白皮书，该工作组的使命是：以“标准化”为纽带促进零信任产业规模化发展，为用户提供标准、可信赖的零信任产品和服务。

指掌易

企业介绍

北京指掌易科技有限公司（以下简称“指掌易”）成立于 2013 年，总部位于北京，是一家以端点为核心，把端点安全、数据安全、业务安全整合在一起的全栈型解决方案公司。指掌易一直致力于在各行业数字化转型中，帮助行业用户构建可信的运行环境，用安全赋能行业用户开展移动业务，提高业务效率。

指掌易依托自主研发的核心技术，以国家网络安全等级保护标准为依据，从“云——管——端”全方位、多维度地帮助行业用户实现关键业务应用和数据安全保障。凭借先进的技术和优质的服务，已经为包括政府、金融、运营商及企业在内的三十多个行业领域的上千家客户提供了完整的移动安全解决方案，并通过覆盖全国的超过 200 位安全专家为行业客户提供本地支持服务。

指掌易还积极响应和参与国家、产业、行业的各类相关安全标准条例的编制，并通过与高等院校联合成立研发实验室等方式，推动我国网络安全专业人才联合培养以及促进科研成果转化，为网络安全产业的发展和政企客户的数字化转型贡献中坚力量。

指掌易零信任解决方案介绍

指掌易灵犀 SDP 零信任访问控制系统基于“零信任”安全新理念，对传统边界安全架构思想进行了调整，优化了安全接入产品架构思路。产品围绕业务应用访问创建了一种以身份为中心的全新边界，旨在解决“基于网络边界建立信任”这种理念本身固有的安全问题，有效控制针对关键应用服务的可信访问，以提升关键应用服务和数据的安全保障水平。

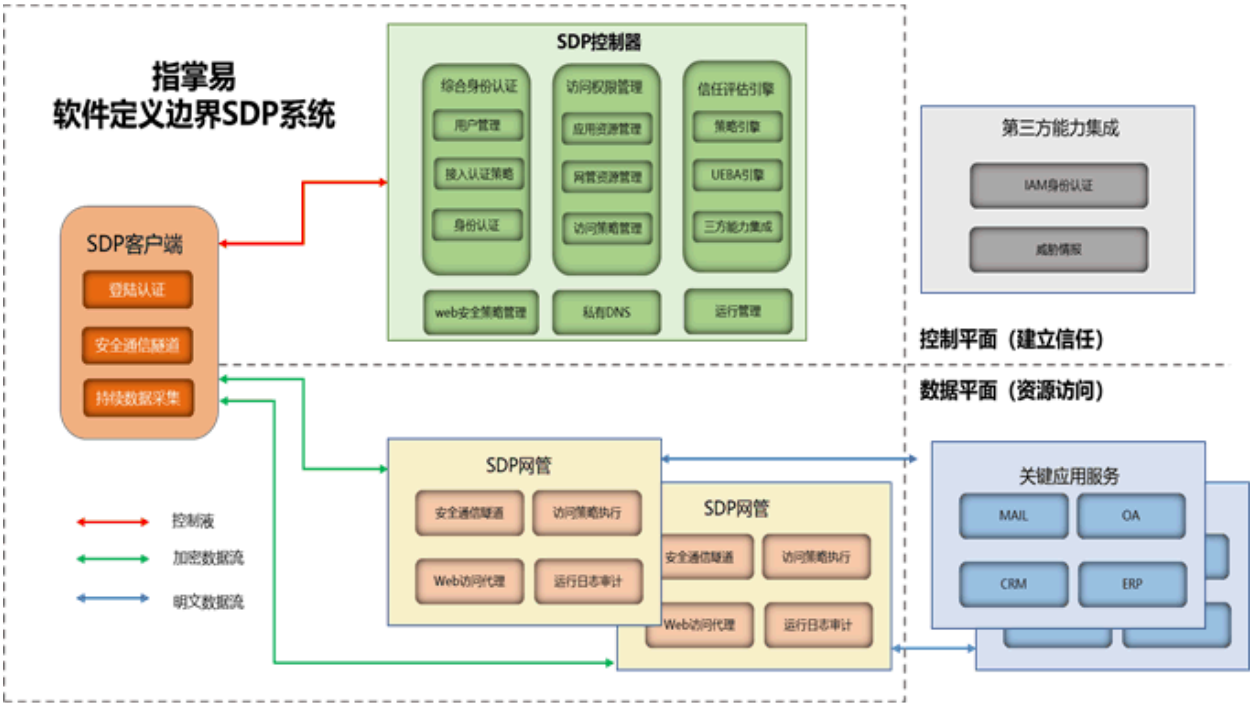
SDP 还兼顾收敛暴露面和安全传输的能力。通过 SDP，将企业对外暴露的应用服务端口进行隐藏，从网络攻击链起始环节限制攻击者收集信息的能力；SDP 同时提供高强度的加密隧道，结合指掌易的终端（移动端、PC 端）数据隔离、加密和 DLP 能力，帮助企业实现从管道到终端的一体化数据安全保护。

指掌易灵犀 SDP 零信任访问控制系统由客户端、安全网关和控制器三大组件构成：

- SDP 客户端负责用户身份认证，周期性地检测上报设备、网络等环境信息，为用户提供安全接入的统一入口。
- SDP 控制器负责身份认证，访问策略和安全策略定义和分发，并持续对用户进行信任等级的动态评估，根据评估结果动态调整用户访问权限。
- SDP 安全网关与客户端建立安全加密的数据传输通道，并执行控制器下发的访问策略。

图 17

指掌易灵犀 SDP 零信任访问控制系统



来源: IDC, 2021

指掌易灵犀 SDP 零信任访问控制系统核心能力：

- 可信接入：指掌易灵犀 SDP 零信任访问控制系统的控制中心对包括用户、设备、网络、时间、位置等多因素的身份信息进行验证，确认身份的可信度。针对异地登录、新设备登录的等风险行为，系统将追加二次验证，防止账号信息泄露而导致的身份冒用。
- 动态信任评估：用户认证通过后，仅设定其可访问的最小业务集。在访问的过程中，对于每次访问会持续监视上下文，基于位置、时间、安全状态和自定义属性进行安全等级评估，按照其安全等级，动态调整业务系统访问权限。
- 服务隐藏：用户认证使用基于 UDP 协议的 SPA 单包授权认证机制，默认“拒绝一切”非法请求。系统实现对外的零 TCP 端口暴露，有效地减少互联网暴露面，预防网络攻击行为。
- 安全加密隧道：数据通信加密隧道采用高安全的加密算法，并采用临时密钥机制，周期性更新密钥，保证通信密钥的安全性。隧道数据报文还具备抗重放和抗中间人攻击的能力。

指掌易灵犀 SDP 零信任访问控制系统严格按照技术规范，实现了控制平面与数据平面的分离，落实先认证再连接的零信任理念。指掌易的零信任架构帮助企业构建新的安全网络边界，形成统一的网络访问安全防护和检测机制，并实现安全策略的快速、有效落地。同时指掌易针对不同用户、不同设备类型、不同网络环境访问内部业务系统的场景，确保业务访问操作策略合规，实现业务核心数据不被篡改和窃取，帮助企业构建全方位动态安全防护体系。

奇安信

企业介绍

奇安信科技集团股份有限公司（以下简称“奇安信”）成立于 2014 年，专注于网络空间安全市场，为政府、企业用户提供新一代企业级网络安全产品和服务。凭借持续的研发创新和以实战攻防为核心的安全能力，已发展成为国内知名的基于大数据、人工智能和安全运营技术的网络安全供应商。同时，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。此外，公司已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展网络安全业务。

奇安信以高投入研发下的技术创新为引领，为客户提供全面有效的网络安全解决方案，推出了“天狗”系列第三代安全引擎，零信任、“天眼”等创新的安全产品。奇安信重点涵盖了网络安全行业多个前沿领域，包括建设云和大数据安全防护与管理运营中心、物联网安全防护与管理系统、工业互联网安全服务中心、安全服务化项目、基于“零信任”的动态可信访问控制平台，以及网络空间测绘与安全态势感知平台。2020 年，奇安信发布面向新基建的新一代网络安全框架，此框架下的"十大工程五大任务"，可以适用于各个应用场景，能指导不同的行业输出符合其业务特点的网络安全架构。

奇安信零信任解决方案介绍

奇安信零信任身份安全解决方案基于“以身份为基石、业务安全访问、持续信任评估和动态访问控制”四大核心特性，应用身份管理与访问控制、访问代理、端口隐藏等技术，基于对网络所有参与实体的数字身份，对默认不可信的所有访问请求进行加密、认证和强制授权，汇聚关联各种数据源进行持续信任评估，并根据信任的程度动态对权限进行调整，最终在访问主体和访问客体之间建立一种动态的信任关系。

奇安信零信任身份安全解决方案的核心特性：

- 以身份为基石：零信任的本质是以身份为基石进行动态访问控制，实现全面身份化是实现零信任的前提和基石。解决方案实现了全面身份化，为用户、设备、应用程序、业务系统等物理实体建立统一的数字身份标识和治理流程。
- 业务安全访问：方案将所有的访问请求（包括用户对业务应用的访问、应用 API 之间的接口调用访问等等）都完成认证、授权和加密。
- 持续信任评估：零信任架构认为一次性的身份认证无法确保身份的持续合法性，即便是采用了强度较高的多因子认证，也需要通过度量访问主体的风险，进行持续信任评估。这种持续的信任评估应基于身份、环境风险判定、以及行为异常发现等。
- 动态访问控制：在零信任架构下，主体的访问权限不是静态的，而是根据主体属性、客体属性、环境属性和持续的信任评估结果进行动态访问控制。传统的访问控制机制下，一次性的静态评估无法保证持续的安全。

基于以上四大核心特性，奇安信零信任身份安全解决方案进一步将安全理念落地为具体的安全能力，为企业提供构建零信任安全体系的基础产品组件和整体解决方案，助力企业迁移到零信任安全架构。

奇安信零信任身份安全解决方案通过全面化的身份认证能力、动态化的用户授权、传输数据的加密与攻击防护能力，智能化的访问行为数据分析能力，全方位、全时地保障企业数据访问的安全性；以自动化的方式实现统一的身份管理、用户认证与授权能力，减少了企业 IT 人员工作量及人为出错几率，大大降低了安全运维成本。解决方案为用户提供了可随时随地访问业务数据能力，同时通过终端环境自动感知、一站式门户访问、单点登录，减少用户访问认证的繁琐操作，实现无缝式的访问体验，有效提高用户工作效率，有效提升了体验与安全的平衡。

奇安信零信任身份安全解决方案重构企业信息安全边界，从根源上解决数据访问的安全性问题，帮助客户树立行业实践标杆。目前，解决方案已经在政府、部委、金融、能源等行业进行广泛落地实施，覆盖典型应用场景，如远程访问场景、数据交换场景和服务网格场景等，为客户的大数据中心、核心业务资产等进行保护，支撑整体安全架构的变革，得到市场、业界的高度认可。

安恒信息

企业介绍

杭州安恒信息技术股份有限公司（以下简称“安恒信息”）成立于 2007 年，于 2019 年登陆科创板，是网络安全行业发展速度最快的上市公司。

安恒信息秉承“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，形成了云安全、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市场战略，凭借强大的研发实力和持续的产品创新，完成覆盖网络信息安全全生命周期的产品、服务及解决方案体系，作为国家级核心安保单位，多次参与全部国家重大活动网络安保，并取得了卓越的成绩。

安恒信息零信任解决方案介绍

安恒信息基于零信任理念，重构资源安全访问框架，推出 AiTrust 零信任解决方案，以可信数字身份为基础，通过持续信任评估、动态访问控制等核心能力，从“零”开始、为政企构建安全可信的业务、数据访问通道。

AiTrust 零信任解决方案理念

- 以身份为基础：所有访问资源的主体必须经过认证及授权。
- 以资源为核心：保护价值数据及资源，构建安全的访问通道。
- 持续信任评估：通过大数据和访问上下文进行持续信任评估。
- 动态访问控制：基于身份、信任、风险等动态调整访问控制策略。

AiTrust 零信任解决方案架构

AiTrust 零信任解决方案由零信任身份服务中心（TAM）、零信任应用代理系统（DSG-APP）、零信任 API 代理系统（DSG-API）、用户与实体行为分析系统（AiThink）等产品组成，可以与第三方风险分析平台、身份及权限基础设施、策略控制服务对接，实现现网向零信任体系的平滑迁移。

AiTrust 零信任解决方案核心能力

- 身份可信

（1）全面身份化：为人、设备、应用、服务等参与访问的实体构建统一的身份标识。

（2）丰富的认证因子：提供账号密码、动态密码等认证方式，可灵活集成、调用第三方认证服务。

（3）多维度身份判别：根据主体访问属性、环境属性、风险事件等判定身份可信状态。

- 通道安全

（1）业务隐藏：通过反向代理方式，实现真实应用、服务的隐藏，减少攻击面。

（2）强制认证授权：只允许持有有效身份凭证、获得授权的请求通过。

（3）全流量加密：全业务流量 TLS 加密，支持双向 TLS、国密 TLS 功能。

（4）流量管控：提供业务健康检查及流量控制，防止业务因异常、超限而过载。

- 信任度量

（1）持续信任评估：基于多时空维度构建访问基线，为每次请求持续进行信任评估。

（2）第三方联动响应：支持对接第三方风险分析平台，实现日志上报和风险联动响应。

（3）日志审计及可视化：提供流量日志、访问日志的记录留存及可视化展示。

- 动态访问控制

（1）细粒度权限鉴别：提供应用、服务、API 颗粒度的权限控制，可灵活集成第三方权限服务。

（2）权限最小化：结合信任度量生成动态最小化权限，并实时转换为访问控制策略。

新华三

企业介绍

新华三信息安全技术有限公司（以下简称“新华三信息安全”）是新华三技术有限公司的全资子公司，成立于 2017 年 3 月，位于安徽省合肥市高新区，致力于为国家信息安全提供安全可信的可靠产品与解决方案、专业的信息安全服务和优质的信息安全人才培养体系，为数字经济发展构筑主动防御、智能免疫的大安全体系。新华三信息安全在云安全、态势感知、高性能综合业务网关等前沿领域有着深厚积累，面向未来打造新一代信息安全产业链，构建信息安全主动防御体系，为中国的数字经济发展保驾护航成为新华三信息安全责无旁贷的历史使命。

基于全球网络安全的最新发展趋势，新华三信息安全在业界明确提出从被动防御向主动防御发展的战略，为业界指明了发展方向。新华三在安全领域拥有超过 18 年的经验积累，拥有 1100 多项信息安全领域专利技术，可提供 35 大类 360+款产品，覆盖网络安全、云安全、工控安全、数据安全和等级保护等细分领域，具备业界最全面的安全产品和解决方案交付能力，为国家提供可信、可控的全系列信息安全产品及完整的”云——网——边——端”一体化安全防护解决方案。

新华三零信任解决方案介绍

新华三以主动安全理念为指导，构建主动安全体系为目标，具体方案以用户需求为主，落地以质量管控为首，以先进的集成产品开发（IPD）流程为支撑，为用户打造适合企业特点的零信任解决方案。新华三零信任安全解决方案基于持续性分析检测、动态授权、最小化原则，利用自身在云、网络、安全、大数据、AI 方面的技术积累，开启了零信任安全架构在不同场景下的落地实践。

新华三零信任安全方案主要由三个部分组成：身份和权限系统、安全统一管理系统、可信业务控制系统。

- 新华三可以为客户自研的提供身份和权限系统，同时可以通过对接和改造客户已有的轻量级目录访问协议（LDAP）、统一安全管理平台解决方案（4A）等系统来满足数字身份管理的建设的需求。
- 安全统一管理系统是零信任的大脑。信任中心通过采集设备的环境信息，设备的日志信息，用户访问应用的行为日志信息等、通过大数据、AI 的技术手段，综合判定用户访问特定应用或业务资源的权限，并给出安全性评分，作为策略系统是否建立用户与资源访问连接的依据。
- 可信业务控制系统属于零信任的信息中枢。可信业务控制包含策略执行点和策略引擎，策略执行点负责完成应用的代理、API 代理、访问策略的执行；策略引擎包含用户的认证、权限的检验。可信业务控制通过和身份权限系统、安全统一管理系统一起实现用户访问应用通路的建立或阻断。

新华三零信任安全解决方案的核心优势在于以身份安全为基础构建可信网络，并辅以 AI 能力实现动态授权，时刻监测异常行为。同时，以攻防为视角提升用户全方位的融合安全防护能力，做到安全问题的及时发现和及时处置，并与整体安全防护体系形成统一策略联动。新华三零信任安全解决方案增加 API 可信系统，基于业务与数据分离的原则，对应用架构进行前后置分离；支持插入式认证模块（PAM），认证服务即插即用；提供高达百 G 性能的运营商级别的硬件平台；具备良好的兼容性和开放性，与第三方系统积极对接。

新华三也在零信任多场景应用方面进行了积极的探索，目前新华三零信任安全方案支持数据中心场景、远程办公场景、智慧园区场景和云场景。

启明星辰集团

企业介绍

启明星辰信息技术集团股份有限公司（以下简称“启明星辰集团”）于 1996 年成立，于 2010 年在深圳 A 股中小板上市（股票代码：002439），是国内极具实力的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。通过不断耕耘，集团目前已对网御星云、合众数据、书生电子、赛博兴安进行了全资收购，成功实现了对网络安全、数据安全、应用业务安全等多领域的覆盖，形成了信息安全产业生态圈。集团始终以用户需求为根本动力，针对客户业务推出了整体安全解决方案及安全专业服务，帮助客户建立起完善的安全保障体系，已成为政府、电信、金融、税务、能源、交通、制造等国内高端企业级客户的重要品牌选择。自成立起，集团经历了不同阶段的跨越式自我升华，目前已迈入“I^3”阶段——独立（Independence）、互联（Interconnect）、智能（Intelligence），并建立“第三方独立安全运营”新模式，立足于云计算安全、大数据、物联网、工业互联网、关键信息基础设施保护、移动互联网等新技术发展，打造专业的安全分析队伍，提供覆盖全行业全技术的安全能力，解决新技术带来的安全挑战，帮助城市全面提升安全能力，从而更大限度保证网络空间的公平与正义。

启明星辰集团零信任解决方案介绍

启明星辰集团是泛 IAM 技术的早期采用者和实践者，应用案例可追溯到 2008 年的电信运营商领域，并持续朝着更加完整的零信任架构演进。同时，启明星辰集团借助在边界安全、云安全领域的长期布局，持续在软件定义边界和微隔离技术上发力。

启明星辰集团零信任包括以下四个关键特点：

融合

启明星辰集团具备长期的信息安全产品线积累基础，其零信任采用了融合扩展架构（Fusion Extended architecture），为用户量体裁衣，既能充分发挥原有纵深防御的建设基础，又能落地零信任理念，化被动防御为主动防御。

在融合扩展架构下，启明星辰集团的零信任架构着力于实现网络内的感知计算、策略判断和动作执行，以及整体的贯通运行，也会对用户原有的安全防护能力进行评估并融合，融合用户原有的主机安全、EDR、态势感知等为其进行安全感知能力；融合用户原有的堡垒机、统一门户（含单点登录）安全准入、VPN 以及安全网关（防火墙、统一威胁管理等）为其安全动作执行能力，在纵深防御体系上进行逐层的访问控制；融合态势感知、IAM 等平台为其进行安全属性，并结合原有的安全闭环机制，进行全网的零信任架构落地。

敏捷

敏捷能力可对传统网络安全动态防御能力不足进行有力补充，它摈弃了传统体系的固化、慢速检查方式。启明星辰集团利用深耕十多年的安全大数据分析优势，对用户的行为、环境检测的评估结果进行分析，迅速调整用户访问权限，使得在攻击发生的初期就能及时识别并处置，最大限度地减小数据泄露的“爆炸半径”。

持续

秉持“从不信任，始终验证”原则，结合业务场景和使用环境实现持续地认证与持续地授权。启明星辰集团将人工智能技术应用于信任评估，不间断地对来源于终端、网络、主体行通过一系列信任评估算法，持续判断主体行为的可信。

弹性

弹性是指从不幸或变化中恢复、调整的能力。一方面，通过“融合”、“敏捷”、“持续”特点的赋能，使得启明星辰集团零信任架构能够快速发现和处置攻击；另一方面，通过其零信任架构的高可用性设计，提升架构中各种组件的服务质量。最终保障业务即使在遭到攻击或组件失效的情况下，依然可为业务提供正常的服务。

绿盟科技

企业介绍

绿盟科技集团股份有限公司（以下简称“绿盟科技”），成立于 2000 年 4 月，总部位于北京，在国内设有 40 多个分支机构，为政府、金融、运营商、能源、交通、教育、医疗及企业等行业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。

绿盟科技高度重视安全研究和技术创新。绿盟科技研究院致力于跟踪国内外前沿网络安全攻防技术，天机、天枢、星云、格物、伏影五大实验室在基础安全研究和前沿安全领域进行积极的探索，为绿盟科技的核心竞争力和持续创新能力提供了有力的保障。绿盟科技依托人工智能、大数据分析和态势感知等专业技术，为用户提供安全态势感知、云安全资源池、下一代威胁防护、威胁和漏洞管理、物联网安全、网站安全监测和防护、工控系统安全防护、智能安全运营等解决方案，帮助用户在领先的研究成果中受益。绿盟“安全运营+”提供安全管理、安全运维和安全技术保障一体化智慧安全运营整体方案，协助客户建设业务驱动的安全运营体系，从静态、被动、基于规则的防御，转变为主动、动态、自适应的弹性防御体系。

作为巨人背后的专家，绿盟科技将一如既往以创新精神、先进技术、优质产品、专业服务，在全球范围内，提供基于自身核心竞争力的企业级网络安全产品、安全解决方案和安全运营服务，成为最受用户信赖的网络安全公司。

绿盟科技零信任解决方案介绍

绿盟科技遵循体系化的安全设计理念，围绕零信任在终端安全，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多个技术领域，为客户提供完整的可落地的零信任安全解决方案。

绿盟科技零信任安全解决方案是主动防御的安全架构，基于设备评估和用户认证，持续集成分析和验证信任关系，以此在不可信网络中构建安全系统，从而降低和消除安全风险。绿盟科技零信任安全架构思路主要包含全面感知、最小授信、持续评估、动态决策四个部分，实现从安全感知、风险决策到资源管控的安全管理闭环，绿盟科技零信任解决方案核心功能包括：

- 全面感知

通过收集认证和权限数据、终端环境感知数据、资产及资产关系数据、应用状态数据、漏洞与配置核查数据、攻击告警数据、历史行为数据以及威胁情报数据等，来进行风险和信任评估，从而实现对设备、用户、数据/应用、网络环境的全面感知。

- 最小授信

通过对用户身份、请求行为、访问资源，以及实时感知的内外部环境信息和历史行为信息，进行实时的风险和信任评估，生成最小访问授权策略，严格控制设备、应用、服务、数据的访问权限。

- 持续评估

在访问活动进行中，应持续对用户设备、网络、系统、应用、数据服务及外部环境进行监测，并进行实时分析，一旦系统受到外部攻击、健康状态出现偏离，应立即采取安全缓解措施，抵御外部威胁，堵塞安全漏洞、持续保障系统运行在稳定、可靠的安全状态。

- 动态决策

在对访问活动持续监测评估过程中，基于终端状态、用户的身份、网络位置、用户行为，动态做出策略决策，一旦发现异常和违规行为，及时执行阻断、二次认证、封堵、隔离等操作，实现基于风险的自适应访问控制，确保访问活动安全、合规、可信。

绿盟科技零信任解决方案遵循零信任原则，提供从安全感知、风险决策到资源管控的体系化安全管理闭环方案。方案支持模块化部署，产品可灵活组合，分层解耦独立部署，可根据客户实际需求分阶段或选择性建设。该方案基于绿盟科技多年的安全积累，提供智能化分析技术，对终端、账号，数据，网络进行全方位多维度综合分析，并基于剧本的自动化响应机制，通过编排调度下发策略，进行动态的访问控制，实现安全响应自动化。

目前，绿盟科技零信任解决方案覆盖了远程安全办公、减少攻击暴露面、统一安全访问、数据安全访问及终端安全接入等典型应用场景，已在公安、政府、教育、运营商、能源行业取得成功案例。

蔷薇灵动

企业介绍

北京蔷薇灵动科技有限公司（以下简称“蔷薇灵动”）成立于 2017 年 1 月，专注于网络安全领域微隔离技术的前沿探索与研究，凭借专业的产品与服务为数据中心用户提供东西向（内部）流量解决方案。蔷薇灵动致力于成为自适应微隔离产品专家，通过自适应微隔离产品与服务为互联网+时代的云端业务体系构建可靠高效的安全基石，助力云计算进入零信任时代。

蔷薇灵动零信任解决方案介绍

蔷薇灵动自主研发的蔷薇灵动蜂巢自适应微隔离安全平台是与基础架构无关，能为混合云提供无差别微隔离服务的软件定义安全产品。产品面向政府、金融、互联网、运营商、能源、大型企业等行业，能够在混合云、容器环境、超大规模网络架构等场景下提供东西向流量的可视化与自适应网络安全策略管理，帮助用户大幅缩短策略部署与调整时间，提升工作效率，构建数据中心内部零信任，让安全跟上瞬息万变的业务需求。

蔷薇灵动帮助企业五步实现数据中心零信任：

- （1）明确要实施微隔离的基础设施，确定管理范围
- （2）利用可视化技术对业务流进行梳理
- （3）根据业务特征，构建零信任网络架构
- （4）生成并配置微隔离策略，对被防护 系统实施最小权限访问控制
- （5）对主机网络行为进行持续监控

蔷薇灵动蜂巢自适应微隔离安全平台核心架构包括：

- 分级授权、分散管理

大型企业规模庞大、分层过多造成管理及运维困难，各部门协同工作效率不高，很难及时作出有效决策。蔷薇灵动蜂巢自适应微隔离安全平台能对不同全向用户提供细致到功能点的权限设置，区分安全、运维与业务部门的权限划分，结合微隔离五步法更好地实现数据中心零信任。

- 高可靠、可扩展集群

微隔离产品属于计算密集型产品，随着点数的增多计算量成指数型增长，在应对超大规模场景时如何保持产品的稳定性、抗故障率等是一种巨大挑战。蔷薇灵动蜂巢自适应微隔离安全平台支持集群模式，支持更多的工作负载接入，降低系统的耦合性，可扩展，解决资源抢占问题，提升可靠性，有更好的抗故障能力。

- 大规模一步通信引擎

随着超大规模场景的需求日益增多，管理中心和客户端之间通信能力迎来巨大挑战。蔷薇灵动蜂巢自适应微隔离安全平台可做到高效并发通信，通过软件定义的方式，从各自为战彼此协商走向了统一决策。

- API 联动、高度可编排

超大规模情况下，资产信息、网络信息、安全信息、管理信息、运维信息等各自独立，不能紧密结合。蔷薇灵动蜂巢自适应微隔离安全平台面向云原生，API 全面可编排，便于融入客户自动化治理的体系结构，将各个信息平面打通并精密编排在一起，促进生态的建设。

- 高性能可视化引擎

随着云计算时代的来临，网络流量不可见就不能对业务进行精细化管控，同时也不能进行更高层的网络策略建设。蔷薇灵动蜂巢自适应微隔离安全平台对全网流量进行可视化展示，提供发现攻击或不合规访问的新手段，为梳理业务提供新的视角。同时，平台可与运维管理产品对接，便于对业务进行管理。

- 高性能自适应策略计算引擎

随着业务不断增长，企业网络架构不断演进、内部工作负载数量也呈指数型增长。超大规模场景下，策略数量大增、策略灵活性不足等问题日益显著，而企业往往缺少有效的应对方式。蔷薇灵动蜂巢自适应微隔离安全平台可以自动适应云环境的改变，面向业务逻辑而与物理实现无关，减少策略冗余，为弹性增长的计算资源提供安全能力。

深信服

企业介绍

深信服科技股份有限公司（以下简称“深信服”）是一家专注于企业级安全、云计算及基础架构的产品和服务供应商，拥有深信服智安全、信服云和深信服新 IT 三大业务品牌，致力于承载各行业用户数字化转型过程中的基石性工作，从而让用户的 IT 更简单、更安全、更有价值。目前，深信服员工规模超 7000 名，在全球有 50 余个分支机构，公司先后被评为国家级高新技术企业、中国软件和信息技术服务综合竞争力百强企业、下一代互联网信息安全技术国家地方联合工程实验室等。

一直以来，深信服十分重视研发和创新。持续将不低于年收入的 20%投入到研发，并在深圳、北京、长沙、南京和硅谷设立 5 大研发中心，研发人员比例约为 40%。深信服坚持以“持续创新”的理念打造省心便捷的产品，获得了市场广泛认可。目前，超过 10 万家用户正在使用深信服的产品。此外，深信服始终重视用户服务，6500 余名认证工程师第一时间响应用户需求，提供专业的技术支持。

深信服零信任解决方案介绍

深信服零信任安全方案基于“以身份为中心，构建可信访问、智能权限、极简运维”的理念，通过网络隐身、动态自适应认证、全周期终端环境检测、动态业务准入、动态访问控制、多源信任评估等核心能力，帮助用户实现流量身份化、权限智能化、访问控制动态化、运维管理极简化的新一代网络安全架构转型。深信服零信任解决方案致力于为广大政府/企业客户提供构建零信任安全体系的基础产品组件和整体解决方案，满足客户内/外网访问、多分支接入、业务上云、移动办公等多种业务场景的安全接入需求，助力政府/企业快速迁移到零信任安全架构。

深信服零信任整体架构基于零信任理念的 SDP 架构实现，核心零信任产品组件为 aTrust 平台，由 aTrust 客户端（可选）、aTrust 安全代理网关、aTrust 控制中心三大部分组成，其中 aTrust 控制中心和安全代理网关参照 SDP 架构，进行控制面和数据面的分离，且 aTrust 也支持无客户端纯浏览器接入的场景。同时 aTrust 平台支持对接桌面云流量接入，也支持对外开放 API 接口，将外部的第三方组件集成到零信任架构来，形成以 aTrust 为中心的统一安全防护体系。aTrust 控制中心负责认证、授权、策略管理与下发，是整体的调度与管理中心，该组件同时负责控制建立连接和切断主体（用户）与客体

（应用）之间的通信连接（通过给网关发送控制指命），生成客户端用于访问应用的身份验证令牌或凭证。aTrust 安全代理网关负责建立、监视及切断访问主体（用户）和客体（应用）之间的连接，它与控制中心通信，从控制器接收策略和指令。aTrust 安全代理网关支持 HTTPS 代理访问和 SSL 隧道代理访问。aTrust 的个人电脑（PC）和移动端均有对应的客户端，PC 客户端和移动端应用程序（APP）支持安全套接字协议（SSL）隧道访问。同时 PC 的客户端提供终端安全检测的能力，对接入的终端当前的环境（如操作系统、防火墙、杀毒软件、应用进程）进行收集和上报，上报给 aTrust 控制中心进行信任评估的策略管理。

深信服零信任安全解决方案系统特色：

- 更安全的身份安全认证能力

深信服零信任安全解决方案以身份为中心，结合多因素身份认证，具备高强度身份认证机制，同时也可与第三方统一身份认证平台平滑对接，采用动态自适应身份认证，实现认证安全增强。

- 动态可信访问保护核心业务

深信服零信任安全解决方案对终端环境实施全周期地实时动态检测，包括用户登陆时、登录后访问业务期间，还可根据业务的重要程度制定高要求的终端准入规则。可设置黑白名单，只允许终端上特定的进程接入访问业务，对终端进行一系列的动态控制，达到高安全终端接入访问。结合用户实时的身份信息、终端环境信息和应用敏感度，能实现对不同安全要求的应用，以及不同范围的用户进行不同安全力度的应用准入，实现动态访问控制。

- 细粒度的智能权限降低异常行为风险

深信服零信任安全解决方案对业务进行智能权限梳理，确保最小化权限的同时，有效减少用户原本权限梳理的管理成本，并设置基于业务系统细粒度准入规则，不同业务制定不同的准入基线，可以灵活地将业务与终端环境、用户行为、认证方式等进行配置，满足企业的安全诉求。当终端环境、身份、行为发生变化时可进行动态访问权限控制，可通过收缩或阻断用户的访问权限，降低被攻击入侵的风险，助力企业从区域边界粗粒度访问控制走向的细粒度访问权限控制，实现最小暴露面。通过用户和实体行为分析（UEBA）、提供 API 与第三方安全能力集成，实现多源信任评估，更准确地识别异常行为和未知威胁，保护业务系统，形成统一的安全防护体系。

- 极简的运维体验降低管理工作量

用户访问浏览器/服务器模式（B/S）业务可以免除客户端登录，通过浏览器即可访问业务，提升使用体验。业务从互联网收缩到内网后不改变用户原有使用习惯，不改变原有访问域名和访问体验，内外网访问一致体验，无论在何地办公，都能获得一致的访问体验，对于用户而言易用性高、上手快，同时也大幅降低 IT 人员在用户终端侧的管理和运维压力。

芯盾时代

企业介绍

芯盾时代创立于 2015 年，基于统一终端安全、智能决策大脑、零信任网络访问等多维技术驱动，通过拥有完全自主知识产权的“智能业务安全产品线”和“零信任企业安全产品线”，保护企业业务系统安全和稳定运行，覆盖移动办公安全、全场景统一身份管理、网络边界安全防护、用户行为风险分析、金融账户及交易安全、交易/信贷/营销风控决策和反欺诈、移动 APP 安全等应用场景。

芯盾时代为金融、政府、运营商、大型企业、互联网等行业近 1000 家用户提供零信任业务安全解决方案，帮助企业防范内外部的业务风险，提供场景化的全生命周期业务安全解决方案，助力客户打造安全、智能、可信的业务体系。在数字时代的发展浪潮中，“人”是网络核心价值点。芯盾时代将继续坚持“以人为核心、以业务安全为基础”的零信任安全理念，为构建安全、智能、可信的互联未来而努力！

芯盾时代零信任解决方案介绍

芯盾时代零信任业务安全解决方案适用于工作无边界、业务无边界、协作无边界的情况，在不改造、不迁移、不影响客户体验的前提下，从身份、设备、行为三个层面进行系统建设，对内帮助客户完善对员工、资源访问等业务管理，避免身份欺诈、越权攻击、信息泄露等风险，对外可快速发现业务系统风险，阻断银身份仿冒、盗转盗刷、交易欺诈、信贷欺诈、虚假交易等手段带来的损失。

芯盾时代零信任安全体系融合软件定义边界 SDP、增强型 IAM 和微隔离三大技术，主要包含可信身份识别、全域风险感知、动态自适应访问控制、资源安全访问的细粒度保护、持续信任评估等五大核心能力，适用于业务系统安全访问、监管合规、数据交换、服务网格、增强优化基础设施安全等场景。芯盾时代零信任安全体系框架分为控制平面、数据平面和管理平面，包含安全客户端、安全应用网关、安全 API 网关、动态访问控制平台、智能安全大脑和安全运营中心五大功能模块，通过复杂的身份治理将用户的权限、认证系统进行统一管理，并对用户的操作行为实行持续分析与鉴别，动态分析可能存在的安全风险。该体系能够灵活支持边界网关、微网关、资源门户三种部署模式，为用户提供跨组织架构、跨区域、跨业务系统的安全保障。

芯盾时代零信任安全体系突出的优势和特点包括：

- 服务隐藏：采用 SPA 机制实现网关和应用的二级隐身。
- 自适应动态授权：对主体身份、设备、行为进行持续动态评估，调整访问控制权限。
- 轻量级设备认证：为设备生成唯一 ID，并以白盒算法避免密钥等信息泄漏。
- 多因子身份认证：通过十余种多因素认证方式提升密码安全性及账号冒用问题。
- 持续身份认证：对前端采集的信息持续进行风险评估，根据评估结果自动匹配认证方式。

关于此项研究

数字化转型促使企业基础网络架构和业务系统正在发生重要转变，云计算、大数据、移动互联网、物联网、5G 等技术广泛应用到企业信息化建设和业务发展中，远程办公、业务协同、分支互联等业务需求快速发展，企业的员工、设备、合作伙伴以及客户需要通过多种方式灵活接入企业业务系统，以提高工作效率、增强用户体验。传统基于边界的网络安全防护手段已经无法对目前愈发复杂的网络环境提供全面保护。零信任理念将网络安全防护从“以网络为中心”转移到“以身份为中心”，凭借其“永不信任，始终验证”的原则，得到了安全厂商及最终用户的广泛关注和认可。IDC 在本次报告中对大量“零信任”相关解决方案的技术提供商和最终实践者进行了深入访谈，并筛选出优秀的解决方案和最佳实践进行详细介绍，以便为同行业企业的零信任架构建设提供参考，同时给出了 IDC 针对零信任理念在中国最终用户落地实践方法的建设指南。

进一步研究

- *Future of Trust: Drivers, Challenges, Perceptions* (IDC #US47653421, May 2021)
- *IDC PeerScape: CIO 视角——中国零信任市场研究*（IDC #CHC46327021，2021 年 4 月）
- *IDC 创新者：零信任之软件定义边界与微隔离技术，2021*（IDC #CHC47362421，2021 年 4 月）
- *IDC 创新者：零信任之身份识别与访问管理技术，2021*（IDC #CHC47364721，2021 年 3 月）
- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions* (IDC #US46912920, October 2020)

大纲

全球各行各业不同规模的企业在数字化转型过程中面临的来自互联网和企业内部的网络威胁从未减少。一旦遭受网络攻击，企业不仅需要花费大量的精力修复网络攻击造成的系统损坏、数据丢失、数据泄露等问题，还要投入大量资源挽回由于遭受网络攻击而失去的企业信誉。如何在提升业务响应速度和敏捷性的同时确保系统和数据的保密性、完整性和可用性是摆在所有企业面前的重要挑战。正因如此，零信任理念在其被业内提出并在谷歌的 BeyondCorp 实践落地后，得到了安全厂商及最终用户的广泛关注和认可。本次报告结合 IDC 定义的未来信任和分布式完整性模型对零信任在中国市场的代表性方案和最佳实践进行了具体介绍，希望帮助广大技术买家了解主要技术提供商的技术特点和各自优势，以及同行业企业零信任实践过程中面临的挑战和应对方案，并为技术买家的零信任架构建设提供 IDC 建议。

关于 IDC

国际数据公司（IDC）是在信息技术、电信行业和消费科技领域，全球领先的专业的市场调查、咨询服务及会展活动提供商。IDC 帮助 IT 专业人士、业务主管和投资机构制定以事实为基础的技术采购决策和业务发展战略。IDC 在全球拥有超过 1100 名分析师，他们针对 110 多个国家的技术和行业发展机遇和趋势，提供全球化、区域性和本地化的专业意见。在 IDC 超过 50 年的发展历史中，众多企业客户借助 IDC 的战略分析实现了其关键业务目标。IDC 是 IDG 旗下子公司，IDG 是全球领先的媒体出版，会展服务及研究咨询公司。

IDC China

IDC 中国（北京）：中国北京市东城区北三环东路 36 号环球贸易中心 E 座 901 室
邮编：100013
+86.10.5889.1666
Twitter: @IDC
blogs.idc.com
www.idc.com