CAICT 中国信通院

腾讯安全

数字化时代
零信任安全蓝皮报告
（2021 年）

中国信息通信研究院云计算与大数据研究所
腾讯云计算（北京）有限公司
2021 年 5 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浪潮，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安全需求的新一代安全体系具有重要意义。

零信任安全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，越来越得到行业关注。本蓝皮报告聚焦零信任安全，通过分析零信任安全理念基本原则，以及基于零信任理念的安全架构形态和核心组成，探究其在企业数字化转型过程中对安全建设的作用及意义。首先，蓝皮报告从基本原则、核心组件、关键技术等方面阐明零信任安全理念及架构内涵，分析零信任安全如何解决企业级用户数字化转型中的安全痛点；继而，围绕无界办公、混合云、企业异地分支接入和第三方接入多个通用场景，以及银行、通信等重点行业场景，探究零信任安全作用和优势；最后，分析了未来零信任的发展趋势。

本蓝皮报告的核心观点与重要发现:

- 数字化转型浪潮下，企业传统安全架构面临挑战。一是上云、应用架构升级等技术转型带来新的安全风险；二是数字化工作空间和供应链协同引入更多的安全隐患；三是新零售、物联网等产品服务创新面临多样的安全威胁。
- 零信任安全理念打破了网络位置和信任间的默认关系，能够最大限度保证资源被可信访问，提升企业数字化转型中新 IT

架构的安全性，基本原则包括：默认一切参与因素不受信，最小权限原则，动态访问控制和授权，持续的安全防护。

- 零信任安全架构核心包括两大平面和三大逻辑组件：控制平面和数据平面将策略与资源访问时的数据交互进行分离；策略引擎、控制引擎和安全代理逻辑组件协作，实现资源访问的信任评估和权限授予，控制访问主体和被访问资源间的连接建立与否。
- 零信任安全和企业数字化转型相互促进，协同发展。一是零信任安全能够解决企业级用户数字化转型的安全痛点，迎接技术转型中的新安全挑战，满足数字化工作空间中用户更高的体验需求，应对产品服务创新后的海量网络威胁；二是数字化转型为零信任安全应用落地提供支撑，技术转型通过提供资源支持助力零信任高性能发展，制度转型鼓励安全架构向零信任变革。
- 零信任安全能够满足企业一些通用场景的安全需要，包括无界办公、混合云、企业异地分支接入、第三方接入等。同时，零信任安全还可以满足不同行业的特殊安全需求，如银行行业、互联网行业、通信行业、物流行业、能源行业、地产行业等。
- 零信任未来发展趋势，呈现与其它领域相融合的特点。一是与原生安全理念相融，助力企业建设高防护性能、组件协同

连通的全因子信任安全架构；二是与广域网络融合，为企业提供端到端安全。

目 录

图 目 录

表 目 录

一、数字化转型不断深入，以信任为核心的安全理念迎来发展机遇

（一）外力与内需共同推进企业数字化转型

1. 国家政策纷现，为企业数字化转型筑良基

数字化转型是数字经济时代社会基座的重要组成，国家高度重视和支持数字经济发展。中国正步入数字经济发展新时代，尤其自疫情爆发以来，数字经济爆发出了强大的活力，加速数字化转型推进十分必要。在国资委发文的《国有企业要做推动数字化智能化升级的排头兵》中，重申数字化转型升级的国家性和紧迫性，并将我国经济社会的中坚力量国有企业，放置在推动数字化转型的排头兵角色。

共性技术筑基础，夯实数字化转型技术支撑。数字化转型的实现技术具有共性，政府加大对共性开发平台、开源社区、共性解决方案以及基础软硬件的支持力度，从而促进共性技术的发展。十四五规划对加快数字化发展做出了重要部署，提出推进新型基础设施建设，加快信息领域核心技术突破，以及建设国家数据统一共享开放平台等建议。大数据、人工智能、云计算、数字孪生、5G、物联网和区块链等技术是支撑数字化转型的新一代共性数字技术，通过高质量建设共性数字基础设施，夯实数字中国基础支撑，全面提升产业链竞争力。

上云用数赋智，大胆探索数字化企业打造之路。全球在新冠疫情的影响之下，云上工作生活成为“新常态”，国家政策涌现加深企业

充分发挥新一代信息技术在后疫情时代的影响。**一是国家发展改革委、中央网信办研究制定了《关于推进“上云用数赋智”行动培育新经济发展实施方案》，**鼓励大胆探索普惠型的云服务支撑政策，推进与大数据技术的融合运用，加大对企业智能化改造的支持力度。**二是国家发展改革委、工信部等 17 部门联合发起了“数字化转型伙伴行动”，**通过上云用数赋智，借助以数据、计算力、算法为驱动的数据智能技术，赋能各行业的数字化转型。**三是地方政府也不断加大对数字化转型的政策支持，**各地积极构建多方联动机制，推动数字化生态共同体建设，从而降低数字化转型成本、缩短转型周期并提高转型成功率。

2. 用户需求升级驱动企业变革，数字化转型是良机

企业数字化转型的内驱力来自用户需求的升级，用户的个性化需求越来越强烈，用户体验要求越来越高，企业需要借助新一代信息技术提供的能力来满足用户需求，新技术在企业的落地与用户升级的需求共同驱动了企业业务的转型、创新和增长。

根据海德思哲联合科锐国际的调查报告[1]显示，企业期望通过数字化转型带来的改进中，“优化客户体验”占比最高，达到 96%，其次是期望“改进现有业务流程运营的效率”，还有超过半数的企业希望“提高企业的业务拓展速度及走向市场的能力”和“推出创新产品及服务”。

1 《从蓝图到伟业：中国企业数字化转型的思考与行动》

营销数字化助力消费者数据打通，致力优质客户体验。移动互联网与营销的结合使得数据、产品与用户之间的固有边界消失，企业通过收集消费者数据绘出全景用户画像，助力精准营销。营销数字化时代，企业通过技术革新将营销与科学结合，让营销数据推动运营战略调整，根据运营战略确定研发方向投入，令消费者作为主体间接参与至决策中，从而实现用户体验升级。

业务流程自动化需求加速企业数字化转型步伐，助力企业实现降本增效。企业中业务流程较为冗杂的两大部分分别为人力资源管理与财务管理，具有业务处理流程长、涉及人员范围广以及审核精确度要求高的特点。企业可以在数字化转型过程中建立集中化资源管理平台，以及分、子公司的集中管控机制，令自动化流程运用其中，自动化代替人工降低成本提升办事效率。

供应链数字化转型助力上下游企业协同发展，为企业业务拓展与创新创造新环境。供应链数字化转型的特殊性在于变革共同性，大数据、物联网和人工智能等信息技术的发展使得供应链从传统的链条式向网状结构变化，使得企业与外部合作伙伴的对接数量大大增加，信息化平台的安全对接变得尤为重要。企业需要主动与其供应链中的上下游合作伙伴的数字化进程配合，从单一生产趋向协同，通过协作实现优化和共赢。

（二）企业数字化转型为传统安全架构带来挑战

1. 技术转型面临安全挑战，传统安全架构有局限

云计算成为数字基础设施重要支撑，弱化传统安全边界防护能力。数字经济时代，云计算作为数字经济的基础设施，安全防护问题是重中之重。然而，**一方面随着虚拟化和容器技术的不断发展，传统网络边界消失。**虚拟化和容器技术的使用使得企业纳管的资源粒度细化，边界的概念从内外网分界处到主机边界处，再到容器之间，传统网络安全边界逐渐消失。**另一方面，混合云模式的广泛采用，弱化了传统安全边界的防护能力，一是公有云与私有云的交付点连接安全尤为脆弱，**攻击者可以通过攻击进入更为开放的公有云，并从公有云渗透入私有云中，在内网中横行，传统的安全边界无法形成有效的防护；**二是多云异构平台无法使用统一安全策略，**异构云平台具有异构技术堆栈，对资源有不同的定义、标签、分类，企业安全策略无法直接从云下平滑迁移至云上，以及在多云之间迁移。

应用架构随基础架构升级不断演进，安全边界模糊。随着基础架构从物理服务器向虚拟机、容器变化，应用架构的升级迎来新契机，从单体应用架构向微服务架构变化，从应用架构形态上来看，微服务化的形态促进了分布式部署模式的发展，应用系统的分布式部署打破了传统单体架构部署于数据中心内的模式，传统网络安全边界逐渐消失。

互联网向网络空间演化，防护性能要求更高。随着科技发展，网络安全的内涵和外延不断扩大，互联网时代企业拥有明显网络边界，

仅需关注边界以外网络本身的安全，例如数据的破坏、泄露和网络瘫痪等威胁。而网络空间安全时代，网络边界模糊，需要关注基础设施、用户、数据和应用等所有资源面临的威胁，面临威胁显著增多，对安全防护能力的要求随之提升，传统安全防护的劣势凸显。**一是传统安全措施多以购置第三方软、硬件为主，**因此多外挂式部署，外挂部署通常基于代理实现，代理本身存在一定的安全和稳定性风险，同时代理的部署也可能对云上 IT 系统造成影响；**二是无法充分利用数字基础设施原生的资源和数据优势。**传统安全产品与已有 IT 基础设施割裂，难以获取云平台内数据，缺少整合、关联分析，无法深度挖掘潜在安全风险；**三是传统安全产品孤立，不具备协同工作能力。**传统安全产品使用复杂、成本高、相对孤立，增高了中小企业的应用门槛，安全效果不能达到预期。

2. 数字化空间扩展引入新风险，传统安全架构难招架

数字化工作空间提升员工生产力，资源安全有隐患。传统的办公设备由企业 IT 统一提供，而数字化工作空间为员工提供了现代化的、个性化的办公环境，企业 IT 能向使用任意设备的员工交付其工作所需的应用和数据，为员工提供跨平台、位置和设备即时可用的体验。企业为实现数字化工作空间，做出变革同时面临安全隐患。**一是使用 BYOD（Bring your own device）办公的数据安全隐患。**随着移动计算设备日益风行，越来越多员工使用 BYOD 办公，设备上的企业应

用与未知下载路径的私人应用同时存在，使用 BYOD 办公具有关键数据所有权模糊和低安全防护等隐患。**二是 VDI(Virtual Desktop Infrastructure)后端资源池共享的安全隐患。**企业的敏感数据需要始终保存在服务器上，因此需要给员工提供远程访问桌面，从而实现数据不落地，最大限度保证数据安全。但是除了专属桌面，池桌面仍是多个共用一个 IP，出现问题难溯源，因此需要时刻确认使用者的身份。

供应链协作扩大数据共享空间，跨边界关键数据位置模糊。在加速信息融合共享的数字化时代，企业与供应链上下游资源协同，面临多数据中心、多云之间的数据融合。传统的数据安全威胁主要来自端点和网络，安全厂商的端点解决方案致力于预防关键数据被拷贝至外部，网络解决方案致力于防止关键数据通过网络流到外部。数据跨数据中心、跨云流动，企业无法准确知道关键数据的存储位置，无法完全控制数据的移动，这就导致传统的边界安全无法对关键数据进行有效的安全管控。

3. 产品服务创新带来特性威胁，传统安全难以覆盖

新零售涌现，新的威胁难以捕捉。新零售是以互联网为依托，优化整合线上线下资源，全方位提升用户体验的零售模式。新零售的模式令其拥有海量用户敏感数据，且涉及资金交易等关键数据，相比于 DDoS 攻击、SQL 注入等传统攻击，新零售更易遇到如刷单、撞库、

恶意下单和虚假注册等威胁，同时新零售网站的数据库盗卖已成为黑色产业，黑客通过黑市出售或网络欺诈等方式获利，这些安全问题不可控也不可见。

物联网推进产品智能和服务变革，安全覆盖难以到位。随着企业发挥物联网智能互连的潜力，智能产品产业链衍生出一系列相关产品或服务市场，智能产品与人类的生活变得更加紧密。然而安全问题十分严峻，早如 2007 年时任美国副总统心脏病发作，调查部门怀疑是心脏除颤器无线连接功能遭暗杀者利用；2017 年的勒索病毒入侵智能联网电视，导致受害者支付勒赎款项；2018 年台积电遭受病毒入侵，导致生产线停摆等。**一方面，物联网有自己的组网方式，使得网络异构复杂，通信协议安全性差。**相比于互联网，物联网的通信传输体系更为复杂，针对其特性的攻击层出不穷，导致对终端设备的入侵和劫持。**另一方面，智能产品处于网络边缘，终端的安全防护能力差异较大。**终端设备种类、体积和功能都非常多样和丰富，然而计算和存储能力非常有限，高度复杂的加解密算法会增加运行的负担，同时终端移动性强的特点使得传统网络边界消失，边界安全防护无法覆盖到位。

（三）以信任为核心的安全理念兴起，弥补传统安全机制缺陷

传统安全机制失效背后的根本原因是信任，传统网络边界由防火

墙、WAF、IPS/IDS 等安全产品防护，凡是通过边界的检查便可进入内网，默认内网中一切均可被信任。随着内网基础设施愈发复杂和流经网络流量种类的增加，内网面临的威胁愈发增多，内网已不可被无条件信任，基于边界的网络安全架构难以应对当下的网络威胁。同时，随着云大物移技术的发展和混合云的大规模落地，企业也无法确立明确的网络边界。在此背景下，零信任应运而生，发展历程如图 1 所示。

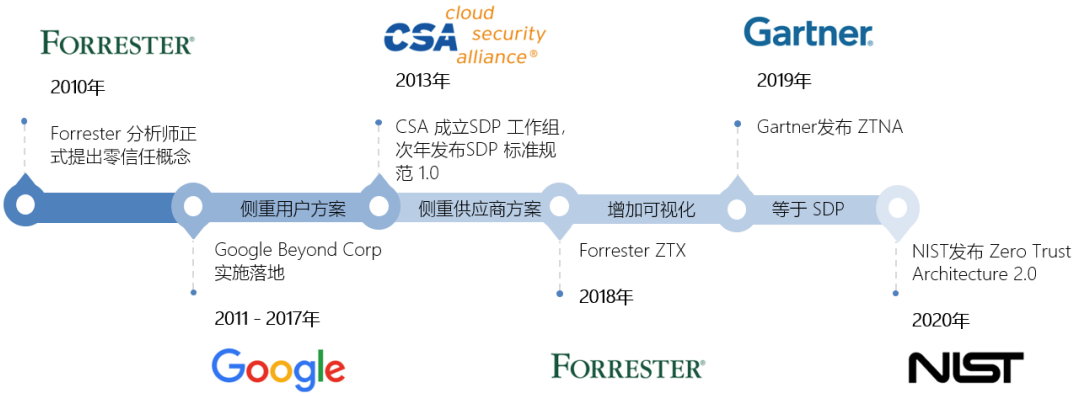

图 1 零信任发展历程

2010 年 Forrester 分析师约翰金德维格正式提出零信任模型[2]，关注点在网络安全架构变革，其核心思想是去网络边界，认为任何流通于网络中的流量在未经过验证之前都不予信任；2011 年-2017 年 Google Beyond Corp[3]实践落地，相比于零信任模型，Beyond Corp 最初的目的是令员工在不受信任的网络环境中不接入 VPN 就能获得内网资源，其关注点在于网络的不可信性；2013 年 CSA 提出 SDP 软件定义边界，作为零信任的第一个解决方案，其核心思想是隐藏核心网络资产与设施，使之不直接暴露于互联网下，使得网络资产与设施免

[2] Kindervag, John. "Build security into your network's dna: The zero trust network architecture." *Forrester Research Inc* (2010): 1-26.
[3] Ward, Rory, and Betsy Beyer. "Beyondcorp: A new approach to enterprise security." (2014).

受外来安全威胁；2017 年 Gartner 在安全与风险管理峰会上发布 CARTA 战略，赋予零信任动态审计的特性，信任不再是绝对的，而是相对的，是根据实际情况动态变化的关系；2018 年 Forrester 提出 ZTX 架构，为零信任扩展其生态系统框架，增加了可视化及分析、自动化和编排等内容;2019 年 Gartner 发布了等同于 SDP 理念的 ZTNA;2019 年-2020 年 NIST 发布 Zero Trust Architecture[4] 草案 1.0/2.0，进一步明确和细化零信任安全理念。

在零信任发展历程中，可以发现各组织提出的不同维度的观点一直在持续发展并融合，最终趋向一致。

二、零信任安全护航企业数字化转型

（一）零信任安全理念：永不信任，持续验证

目前，以零信任为代表的新一代网络安全理念不断衍生和应用，理念打破了网络位置和信任间的潜在默认关系，致力于降低企业资源访问过程中的安全风险。为最大限度保证资源被可信访问，提升企业 IT 架构安全性，零信任的核心思想是：默认情况下，企业内外部的任何人、事、物均不可信，应在授权前对任何试图接入网络和访问网络资源的人、事、物进行验证。

零信任的基本原则归纳如下:

默认一切参与因素不受信: 零信任的信任关系源自于对所有参与

4 Rose, Scott, et al. *Zero trust architecture*. No. NIST Special Publication (SP) 800-207 (Draft). National Institute of Standards and Technology, 2019.

对象和行为的动态验证，所有参与对象和行为共同构成一次端到端的资源访问，这些参与对象包括网络、应用、终端、访问主体、数据、工作负载，行为包括访问请求、连接建立、策略下发等。零信任不为任何参与因素预制信任条件，所处位置无法决定信任关系。

最小权限原则：零信任强调资源按需分配，仅授予各行为所需的最小权限。对每个行为单独授权，对一种资源的授权不会自动作用于另一种资源的访问权限。

持续动态访问控制和授权：对资源的访问控制由动态授权策略决定，动态授权策略依据参与对象的主体信息和行为信息，通过对多源信息进行分析获得授权策略，一旦动态授权策略依据发生变化，将重新计算授权策略，这一动作将在一次端到端的资源访问的全生命周期中持续进行。

持续安全防护：确保进行资源访问的参与对象处于安全状态，通过安全产品/工，及时发现安全问题，并采取措施降低安全风险。

相比于传统的边界防护安全，零信任在护航企业数字化转型过程中能够提供更灵活、更优质的安全能力，表 1 列出了零信任安全与边界防护安全的主要区别。

表 1 边界防护安全与零信任安全对比

	边界防护安全	**零信任安全**
安全信任的范围	信任网络边界内部	网络边界内外均不信任
安全产品关联性	产品孤立	产品联动
安全策略	固定策略	实时调整策略
安全防护方式	以网络为中心	以身份为中心

传统的边界防护认为数据中心的内部是安全的，可以将数据中心

视为一座城，安全防护产品就是一条护城河，作用于网络边界，网关是城门由重兵把守，用户携带身份证在网关处由士兵进行认证，认证通过后放行，城内的商户提供各类资源（虚机、容器、应用等），用户可以去任意商户放置、拿走、破坏其中的物资，意味着用户一旦通过网关接入内网，其所有操作都被信任和接受。

而零信任没有任何预设条件，无论用户在城内城外，如果想要获得某一商户提供的资源，都需前往统一办事处进行身份验证，并经过信用评级后获得官方文书，文书中规定用户可以前往的商户和获取的资源，商户依据文书为用户提供资源，如文书明确去城西买米，用户就不能去城东买米，城西也不能向用户卖面，用户被限制了在单家商户中最小的物资获取权限，去往其他未授权商户也将被拒绝。如果用户在一个商家有了失信行为，相关信息会通告办事处和全城，提醒大家时刻警惕，实现全城共享安全信息共享，联动进行安全防护。

（二）基于零信任安全理念的逻辑架构进一步明确

基于零信任基本原则，企业可建设或改造已有网络安全体系以实现零信任安全架构，利用零信任安全架构为 IT 系统提供持续的安全保障。架构如图 2 所示，由零信任核心逻辑组件和内部或外部数据源组成。

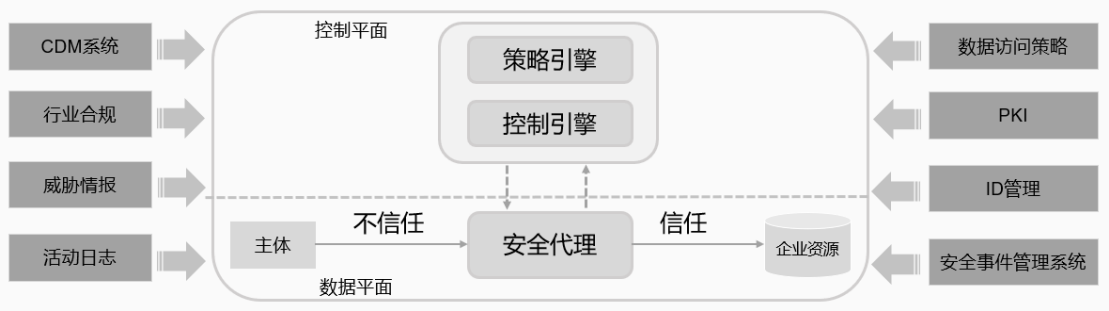

图 2 零信任安全架构

零信任安全架构对访问参与对象和访问资源之间的所有行为进行处理，零信任核心部分分为控制平面和数据平面。访问主体发起访问请求，由控制平面的策略引擎进行多源信任评估计算，由控制引擎对计算结果进行判定，决定授权策略，一旦授权访问，控制引擎将通知数据平面的安全代理，为该次访问建立安全连接。策略引擎仍持续进行评估，一旦参与对象或其行为发生变化，策略引擎将依据新的评估源进行信任评估，控制引擎随时依据评估结果判定授权策略是否需要改变，随时通知安全代理执行相应操作，最大限度保障资源安全。

零信任安全架构核心逻辑组件主要分为三部分:

策略引擎: 该组件负责信任评估，通过收集和分析参与对象和行为等多源信息，对访问主体进行持续的信任评估。

控制引擎: 该组件作为策略控制点，依赖策略引擎的信任评估结果，持续判定授权策略。

安全代理: 该组件作为策略执行点，为授予权限的访问主体，建立其访问主体和被访问资源之间的安全通道。在实际架构中，该逻辑组件可能由两个不同的组件构成: 客户端 (如用户终端设备上的代理

插件等）和资源侧网关（如 Web 网关、API 网关等），或单个代理组件。

零信任架构除了核心逻辑组件，还包括内部和外部信任源，与策略引擎协同，将收集并分析参与对象和其行为的安全信息，传递给策略引擎，为其进行信任评估提供依据。信任源主要包括：**CDM(连续诊断和缓解系统)、行业合规系统、威胁情报源、数据访问策略、PKI(企业公共秘钥基础设施)、ID 管理系统、网络和系统活动日志、安全事件管理系统**等。

（三）零信任安全与企业数字化转型相互促进与协同发展

1. 零信任安全解决企业级用户数字化转型安全痛点

迎接技术转型面临的新安全挑战。技术转型作为企业数字化转型的重要一环，以云计算技术为承载，融合大数据、人工智能、区块链、5G 等新一代数字技术形成综合数字化平台底座，以促进企业生产力提高。同时，因新技术的引入，企业 IT 架构在不断革新中面临新的安全挑战。**一是资源粒度不断细化**，云计算通过虚拟化、容器等技术实现了 IT 资源的细粒度隔离，资源承载着不同类型、不同级别的业务，这要求安全防护策略也随之精细，零信任能够对物理设备、云服务、接口等所有层级的资源进行防护，在访问主体身份验证和权限判定成功后，仅为其提供满足需要的最小粒度的资源；**二是数据融合导**

致内部流量大幅增加，企业数字化转型中大量数据电子化存储，同时基于大数据进行价值挖掘，数据融合与处理促使企业内部（东西向）流量大幅增加，传统的安全产品大多对南北向流量进行控制，难以实现东西向流量异常检测与防护，零信任不为任何参与对象预制信任条件，企业内部资源间的访问也需要进行身份验证和权限判定，能够有效抵御东西向流量存在的安全风险。

满足数字化空间中用户更高的体验需求。一方面企业内部员工生产方式多样化发展，一些生产活动不必局限于企业内网进行，远程办公常态化；另一方面，企业与企业之间将开展更多的合作，进行资源与信息共享，企业内部资源面临更频繁的外部访问。VPN 等传统远程访问方式在稳定性、灵活性等方面存在不足，零信任强调组件原生化发展，分布式、弹性扩展等特性能够为用户提供更优质的使用体验。

应对产品服务创新后的海量网络威胁。企业进行业务转型，促进传统产品向智能产品、智能服务、一站式服务平台等升级，以数字化平台打造更多的新型商业模式。伴随着产品服务转型，企业需要维护管理的数字化平台增多，海量用户和各类终端通过互联网访问平台，企业资源在互联网中暴露程度大幅增加，为黑客攻击提供了更多可能。在零信任安全中，安全代理默认不对外映射任何端口，资源对外隐身，只有访问主体通过认证后才能访问授权资源，同时访问主体仍不能访问未授权的资源，零信任降低了互联网端的攻击面。

2. 数字化转型为零信任安全应用落地提供支撑

技术转型助力零信任高性能发展。一方面，云计算作为数字化转型基础设施，能够为零信任安全提供计算、存储、网络等丰富、可扩展的基础设施资源，零信任安全中各逻辑组件部署于云上，安全防护能力可弹性扩展，分布式部署能够保证组件高可用；另一方面，人工智能技术的应用为零信任安全海量数据智能分析提供可能，零信任策略引擎可以利用人工智能技术建立信任评估算法，同时零信任安全中心也可基于人工智能技术更加深入的挖掘潜在安全风险。

制度转型鼓励安全架构向零信任变革。制度转型强调企业人员、组织架构、文化、管理制度等的变革，网络安全作为企业运营过程中的重要组成，同样需要进行制度转型，零信任正契合了制度转型的宗旨和目标。一方面，零信任实现了安全理念的变革，更加适应企业数字化转型后的新安全需要；另一方面，零信任便于企业进行统一、集中的数字化安全管理，降低管理成本；同时，零信任不要求企业从零构建新的安全架构，可以基于已有安全架构渐进式升级，有效利用已有资源，减少建设成本。

（四）关键技术助力零信任安全架构落地应用

零信任安全架构涉及多个核心技术：一是策略引擎基于多源数据的信任评估技术；二是实现访问行为安全控制的安全代理技术；三是细粒度访问控制的网络隔离技术；四是用于身份认证和访问的身份安

全技术；五是为多样化终端提供安全防护的终端安全技术。

同时，零信任核心组件与内外部信任源协同，也将覆盖多种较为成熟的安全技术，如数据防泄漏检测等数据安全技术，应用防篡改等应用安全技术，容器安全等工作负载安全技术，态势感知等安全管理技术。因相关技术已发展较为成熟，本报告将不再赘述。

1. 多源数据信任评估技术实现更可靠的用户授权

零信任策略引擎为访问主体提供多源的持续信任评估，并将结果传递给零信任控制引擎，由其决定最终授予访问主体对资源访问的权限。

策略引擎具有多评估源，由内部和外部数据源提供：一是访问请求，访问请求包含请求主体的信息，包括使用的操作系统版本、应用研发公司和交互协议等信息；二是用户主体的标识信息，包括用户的账户状态、权限、历史用户行为模式等信息，以及根据时间、用户地理位置和接入网络等信息推算出来的置信度水平；三是资产状态，记录企业资产的物理（位置）和虚拟（运行时间、补丁程序级别、操作系统）状态，用以与请求的资产状态进行对比；四是资源访问要求，包括资源敏感级别、访问者级别、IP 黑白名单和存储方式等定义访问资源的最低要求，用以快速排除完全不符合要求的访问者；五是威胁情报，主要指当下系统中可能运行的威胁和恶意软件的信息。

2. 安全代理关键技术完成访问行为的统一管控

安全代理负责执行策略，通过拦截访问请求，从控制引擎处获得访问主体的权限判定，对认证成功并具有权限的访问主体建立相应安全访问通道。

根据用户访问场景的不同，安全代理可使用以下几种部署模式：

（1）Web 代理网关

Beyond Corp 使用的安全网关即为 Web 代理，Web 代理网关仅支持 Web 网站的接入，不支持 C/S 架构的应用，其功能包括：一是请求转发，根据访问域名转发至相应服务器；二是身份获取，从访问请求中获取用户身份；三是身份验证，联合策略引擎进行动态验证；四是操作执行，根据控制引擎的结果决定授权或拒绝访问。

Web 代理网关具有预判断和持续监控两大优势，一方面该网关可视为在信任资源外侧的一层防护，预先对接入企业资源的用户进行验证，拦截未授权访问；另一方面，所有流量通过网关转发，网关可以持续监控流量，并进行分析和状态检测，发生异常时可以及时响应。

（2）隐身网关+Web 代理网关

SDP 架构中将隐身网关放置于 Web 代理网关前端，其作用与防火墙类似，首先对访问主体进行身份验证，面向合法访问开放端口并与 Web 代理网关建立通信，面向非法访问保持端口关闭，具有隐式防护能力，有效避免非法访问主体对 Web 代理网关进行漏洞扫描或 DDoS 攻击。

（3）网络隧道网关

网络隧道网关主要面向 C/S 架构的应用，弥补 Web 代理网关仅面向 B/S 架构应用能力的缺失，以实现全场景覆盖。通常使用 VPN 实现网关能力，完成请求转发、身份获取、身份验证和操作执行。可以与隐身网关和 Web 代理网关三者配合使用。常用的 VPN 协议有: WireGuard，IPsec 和 OpenVPN 等。

（4）API 网关

随着业务与技术发展，单体应用微服务化，微服务需要具有统一接口实现微服务间的调用，API 网关应运而生。API 网关实现了统一接入、负载均衡、协议转换，具备限流、降级、熔断等措施以保护网关的整体稳定，同时具备统一鉴权能力。

3. 网络隔离关键技术保障东西向流量安全

微隔离是实现东西向流量安全的重要技术，实现方式有多种，究其本质均为防火墙的访问控制能力。一是代理防火墙模式，每台服务器安装防火墙代理，代理通过调用主机防火墙控制服务器间访问；二是原生防火墙模式，使用云平台自身的虚拟分布式防火墙实现访问控制；三是第三方防火墙模式，使用购置的防火墙实现访问控制。原生防火墙具有天然优势，**一方面可以实现统一的安全策略下发，精细化网络安全管理。**安全策略可以根据不同微分段的要求定制，统一下发到每台虚机或容器上，也可以根据应用环境动态分组并统一下发策略；**另一方面可以实现基于身份的分布式防火墙，针对业务访问进行认证。**

安全策略可以基于 AD 域对用户访问业务权限的划分完成设置，令同一服务器上的不同业务实现安全隔离，脱离了传统基于 IP 或位置的安全部署方式。

4. 身份安全关键技术支持高效用户管理

身份安全作为零信任安全重要的组成部分，是对资源提供可控安全保证的核心，核心能力主要包括:

IAM（Identity and Access Management）：主要目标是保障用户从登录系统到授予其权限，再到登出系统的整个过程中，在适当的情况下赋予准入用户对企业内资产的访问权。随着云时代的到来，IDaaS（Identity as a Service）将传统 IAM 作为一项云服务，由第三方服务商构建、运维并实现服务托管。其 SaaS 的本质天然具有云上弹性，支持比传统 IAM 承载更高用户量级，以及天然连接云上云下的统一身份认证能力。

SSO（单点登录）：可以实现一次登陆多次访问，有权限用户在约定期内无需为每个应用单独做身份认证，SSO 服务器会代表用户完成验证。

目录服务（如 OpenLDAP，Microsoft AD，第三方认证源）:可以维护资源与地址的映射关系，可以提供高性能的身份管理，并配合 SSO 使得用户使用一套身份即可访问企业内服务，从而便于用户遵循企业现有用户管理规范，例如定期修改密码、密码使用频次，以及

离职员工的身份注销等。

MFA（多因子认证）：辅助建立了多层次的防御，通过多种身份验证方式验证未授权人员，从而加强身份验证的安全性。常用 MFA 通常有三类：一是知识型验证，通过计算图片中等式结果或圈出某些文字等方式验证并非机器人登陆；二是安全令牌或智能卡，每个令牌仅与唯一用户账号绑定；三是生物识别式验证，利用用户指纹或面部特征来识别唯一用户，安全不易伪造。

5. 终端安全关键技术为多样化终端提供全方位防护

通过对多类型终端进行统一纳管，从应用运行、设备管理等方面进行全方位防护。

随着 BYOD 的普及，BYOD 与传统办公设备统一管理成为企业难题。BYOD 具有移动性，其管理难度较传统个人电脑更高，比起企业统一派发设备，BYOD 更难控制设备上的自有软件，尤其破解设备更易受到恶意软件入侵。因此需要通过一些手段保证终端设备的安全：**一是应用安全沙箱，保障企业应用在 BYOD 上安全运行。**沙箱是一个由容器提供的隔离环境，BYOD 设备可将企业应用运行在安全沙箱中，即便设备中了病毒，企业应用仍然可以在安全沙箱中正常运行。**二是数据不落地，保障特殊工作信息安全。**对于合规性要求较高的工作例如涉及知识产权的图纸、客户的商业机密等信息按规定均不能携带离开办公区，但因不可抗原因如疫情、会议展示等必须携带出去。若要

彻底保证企业关键数据安全，可以将企业应用和数据保留在数据中心，通过远程应用投射和虚拟桌面在移动终端渲染展示，从而实现“数据不落地”。**三是 MDM（移动设备管理）系统构建，助力员工开箱即用。**对于企业派发设备应包含员工所需办公软件，例如 ERP, CRM, HR, OA 系统等，若要实现企业设备集中管理，需要在采购设备后将设备的管理权限转交企业，登记至企业 MDM 系统，即便离职员工设置了用户账号，企业仍具有权限一键抹除。批量应用软件的购置同理，软件的权限属于企业，由企业控制软件许可的分配和回收。

三、零信任安全应用场景

（一）通用应用场景

1. 零信任促进无界办公安全便捷

无界办公打破传统以物理网络为边界的办公模式。办公不再局限于固定地点和设备，大大弱化了办公中对外部环境的依赖，从而最大化提升办公效率。目前常见的无界办公包括但不限于远程办公平台、远程开发、远程运维等。

无界办公提升便捷性，安全风险随之提升。现阶段无界办公带来的安全风险主要有三个方面：**一是接入类别复杂化带来的安全风险。**接入人员和接入设备的多样性大大增加，接入人员的身份和权限管理难度大，接入设备的参数和性能参差不齐，从而带来弱密码、接入程序漏洞等一系列问题；**二是服务与提供服务的基础设施二者之间关系**

的复杂化带来的安全风险。随着云概念在企业运营过程中的深入，企业资源不再局限于内部服务器，还有可能被托管在云端服务器，在这种情况下，资源信息基础设施与应用服务之间的关系复杂度大大提高，引入了更大的系统风险；**三是数据难以管控带来的安全风险。**无界办公导致企业数据在不同设备、内外网之间频繁流动，也需要在个人终端留存，大大增加了数据泄露的风险。

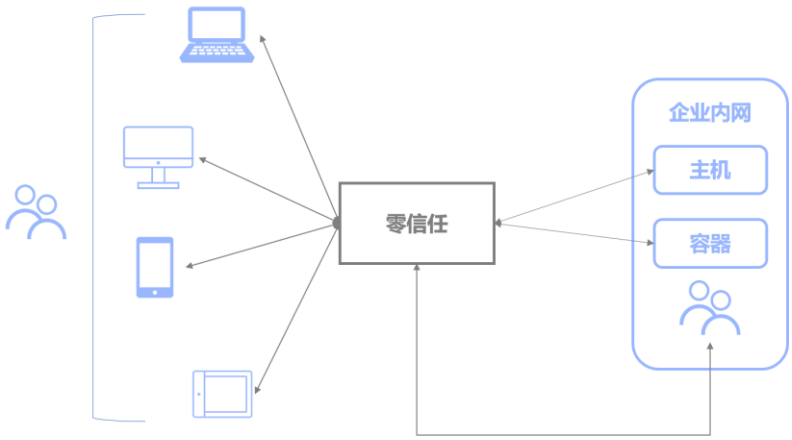

图 3 零信任无界办公应用场景

在零信任安全中，**一方面，不再根据网络位置来验证身份和提供权限，为所有访问主体赋予数字身份，完美地规避了无界办公中物理网络安全边界被瓦解的问题。**其秉承的主旨是对内网和外网的一切设备默认均不可信，在访问主体向安全代理发出访问资源的请求时，基于访问主体、受访资源、访问日志、环境信息等一系列相关多源数据作为判决依据，对访问主体的行径做出动态的身份验证和行为判定，从而决定是否对授权该操作，这一行为伴随每一次操作的始终。**另一方面，零信任安全架构强调按需分配和最小权限原则。**利用端口隐藏等技术手段，在访问主体通过验证之前，受访资源对其隐身，验证通

过后仅对其授予所需的最小权限，大大降低了资源的可见性，大面积减少了攻击暴露面，从根本上降低了互联网可发现和内部威胁的攻击面，保障了无界办公的安全。

2. 混合云推动零信任价值进一步发挥

混合云组建方式多样化，业务灵活具有弹性。混合云可以是云和云的组合，也可以是云与传统 IT 的组合，企业上云可以利用云的弹性使得业务灵活扩缩，利用云的无处不在使得多分支机构互连互通，利用云的便捷进行云上灾备等。

混合云释放红利，企业仍踟蹰不前。主要原因来自**技术堆栈异构，增加企业上云后管理的难度。**不同云之间、云与传统 IT 均拥有不同技术架构、运维流程和管理工具，技术架构的差异为企业上云增加难度，上云后面临异构平台难以统一管理、安全策略不具有一致性的问题，增加企业管理成本和运维成本。企业需要适配不同云服务商提供的访问控制策略接口，实现统一接入，从而进行统一资源安全访问管理。

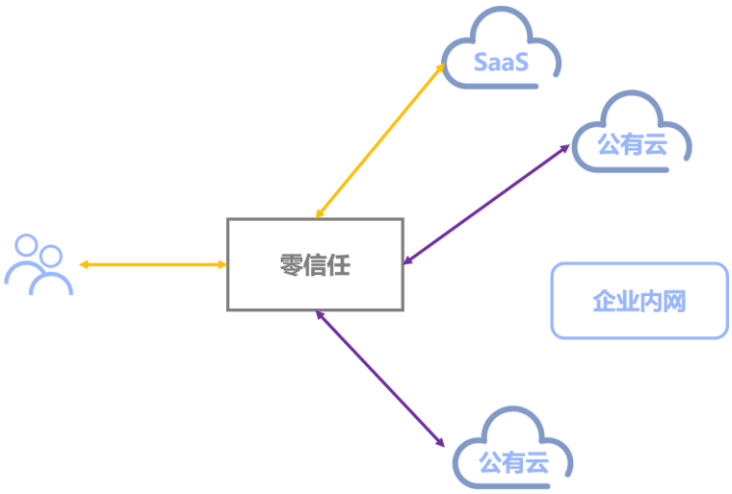

图 4 零信任混合云应用场景

在零信任安全中，通过零信任安全代理将不同环境的业务接口统一纳管。**一方面，隐藏真实业务。**利用其隐藏网关将系统的端口和真实 IP 隐藏，有效防御 DDoS 攻击等安全威胁，实现安全访问转发；**另一方面，统一安全访问策略。**利用零信任策略引擎全方位地动态评估访问主体的信任等级，获取零信任控制引擎下发的决策结果，以身份为中心，实时地、持续地进行访问鉴权，解决了混合云网络边界的脆弱性，用户可以灵活便捷且全地访问处于不同云上的业务系统。

3. 零信任保障企业分支机构安全接入

适应企业业务发展，多分支机构成为常见组织形式。一是金融、通信、电力等为全民提供服务的大型集团公司，在全国各省市设立分公司；二是互联网等迅速扩张业务的企业，在全国多省市设立办公地点；三是在全球化浪潮下，积极拓展海外业务的企业，在全球重点区域开设办事处或分公司。无论何种场景，分支机构员工都有安全访问

集团内部资源的需求。

分支机构体量增大，专线或公网 VPN 无法满足当下访问需求。为实现分支机构员工的访问需求，目前通常利用专线或公网 VPN 的方式实现安全连接，但上述方式存在一定问题，**一方面搭设专线价格昂贵，**集团与分支机构间搭设专线价格昂贵，若分支机构规模较小、访问集团资源的需求不频繁，专线方式将导致资源浪费，无论自建或托管均耗费较高成本；**二是连接稳定性不够好，**分支机构通过公网 VPN 连接至集团内网，但 VPN 稳定性不足，尤其对于跨国访问的场景，丢包率高，访问体验差，同时 VPN 性能扩展存在瓶颈，难以适应大规模的异地接入。

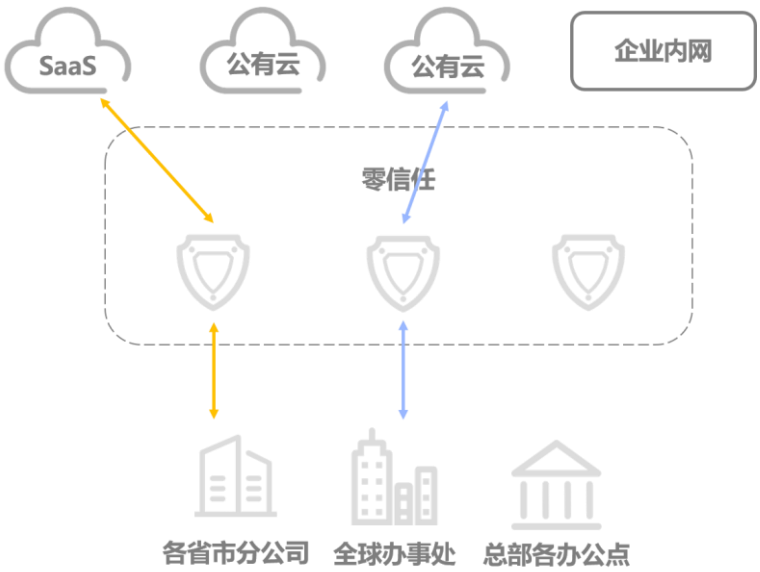

图 5 零信任企业分支机构接入应用场景

在零信任安全中，核心组件呈原生化特性，能够有效避免传统安全连接方式的问题。**一是服务组件化、SaaS 化。**安全代理、控制引擎等以组件形式部署于服务器、容器等基础设施，或以 SaaS 形式交付，

能够有效利用底层计算、存储、网络等资源，在面对大规模异地接入时，组件迅速扩展，防护能力得到提升；**二是组件高可用部署，**且可在全国或全球范围内多节点部署，组件自身稳定性得到提升，用户也可就近接入零信任安全代理，访问体验得到改善。

4. 第三方协作为零信任发展提供机遇

数字化转型推进产业链不断优化提升，企业协同互惠成为趋势。一是企业之间在技术资源、市场资源等关键资源上进行共享，实现跨地区、跨系统、跨组织的连接；二是供应链全链条的优化协同，贯通从原材料/设备供应到产品交付销售的全流程；三是不同行业之间进一步合作融通，实现行业级的互惠发展。在企业协同过程中，面临大量的第三方人员访问和第三方系统连接企业内部资源的需求。

各企业安全体系存在差异，第三方接入带来安全风险。与企业内部员工和系统相比，第三方接入面临更高风险，**一是各企业管理机制和能力有差异，安全能力不对等。**各企业具备自己的身份和权限管理机制，且管理能力有差异，难以保证第三方的身份与权限管理水平与企业自身要求相匹配，弱密码、不合理的权限分配等问题屡禁不止；**二是接入设备和系统的安全能力参差不齐，**漏洞、木马等为黑客带来可乘之机。

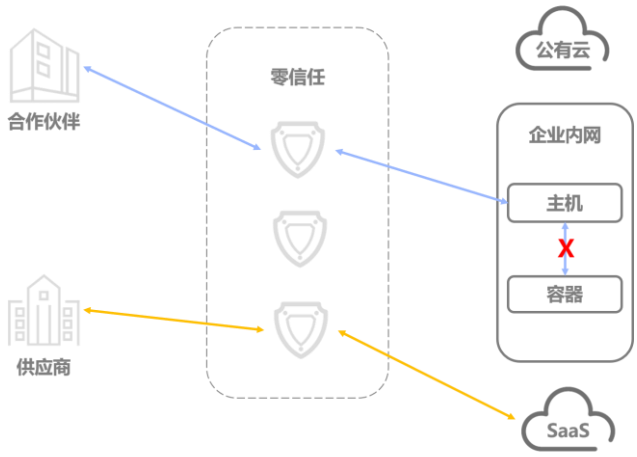

图 6 零信任第三方协作应用场景

在零信任安全中，**一方面，限制最小访问权限。**通过微分段实现资源细粒度的隔离，访问控制策略可下发至具体的服务器、容器，甚至应用，访问主体仅能访问权限内的资源，有效防止主体的越权访问，将风险影响限制到最小范围。**另一方面，终端安全建立统一的安全基线。**仅在第三方设备满足基线要求下控制引擎才允许设备接入企业内部资源，降低接入设备可能引入的安全风险。

（二）行业应用场景

1. 零信任迎接银行业金融服务创新中的安全挑战

传统银行历经多年积累和发展，都已建立自己的核心系统。随着互联网金融的兴起，引领了线下业务线上化和移动化趋势，运用大数据、云计算等新兴信息技术，为社会各阶层和群体提供信息、资金、产品等全方位金融服务。相比传统银行 IT 环境，云计算环境中面临了更多来自开放环境带来的安全挑战：

1）分支机构接入需求增多：商业银行集团化发展，纷纷成立理财、消费金融子公司等，子公司依据业务发展分布于多地，分支机构需要购置高额专线或 VPN 组网连入集团数据中心，用以实现多地分支安全接入的需求。

2）对外开放接口增多：随着银行开放共享、跨界经营，业务变得繁杂，对外开放很多接口，供外部合作伙伴接入银行内网资源，然而接口的增多致使难以完全进行安全审计。

3）远程办公需求增多：后疫情时代居家办公和移动办公模式逐渐被接受，访问者多使用动态 IP，无法实施网络层面访问控制。

4）不具备精细化访问控制能力：商业银行内部根据业务划分了核心区、外联区、互联网接入区和数据应用区等，区域之间通过网络层防火墙隔离，而区域内部的东西向流量无法实现精细化控制。

零信任引导安全架构从以网络为中心转向以身份为中心，进行细粒度的自适应访问控制，解决方案能够有效缓解上述问题：

1）信任最小化：所有设备、用户和网络流量都应该被认证、授权和加密。在账号安全方面，对首次认证、新的环境登陆、密码错误等情况要求动态验证码输入；对弱密码进行识别，并进行账号安全增强。在认证安全方面，通过识别异地登陆、凌晨登陆等进行登录环境检查；仅允许从限定浏览器及对应版本或限定 IP 范围接入访问。

2）访问权限管控：零信任平台不直接对外开放 Web 服务，实现业务隐藏，所有后台管理业务通过零信任平台统一对外发布，零信任

平台成为用户获取服务的统一可信入口。通过零信任平台可信认证和业务系统认证，实现访问权限管控。

2. 零信任适应互联网业快速发展与迭代需求

互联网为国内云计算、大数据、物联网等新一代信息技术发展提供了基础，互联网企业是数字化转型的最大推手之一，企业业务蓬勃发展和迭代，规模迅速扩张，体现在：一是企业员工和设备数量多，设备类型多样化（PC、智能手机、平板电脑等）；二是业务类型丰富，涵盖社交、游戏、云服务、大数据服务、互联网金融、视频等方方面面；三是职场分部及合作伙伴组成复杂，包括分布在全国甚至全球的办事处，特殊外包职场，收购子公司，投资公司，协作供应商等。

这种现状面临如下的安全需求：

1）远程办公和运维的诉求增多，终端管理困难：与供应商系统对接、协作研发运维，企业内各职场分部间的互访和人员流动等，都催生越来越多的远程办公和运维诉求。

2）职员年轻化对接入体验的要求提高：除企业设备外，员工期望使用自有设备更加便捷的访问企业资源，涉及智能手机、平板电脑等各种终端。同时，互联网企业大多将研发网络与办公网络隔离，员工使用两台电脑接入网络十分不便，维护成本高。

3）面临海量互联网安全威胁：互联网行业业务对外开放端口多，面对来自外部黑客的海量威胁，如专门针对游戏公司的黑客组织长期

的渗透行为，利用云服务商云服务资源的挖矿、网络攻击等行为。

零信任方案能够有效缓解上述问题:

1）强化终端安全合规接入：零信任方案通过对接入终端安装 Agent 等组件，实现安全日志采集、安全管控、合规检查、系统加固、数据防止泄漏等能力，让企业管理员具备对远程办公、远程运维的终端进行安全管理的能力。

2）接入方式升级，员工访问体验改善：一是零信任方案改善登录体验，支持用户单点登录 OA、运维等内部系统；二是比传统 VPN 有更好的访问速度和稳定性体验，提高外网访问体验，提供链路加密与全球接入点部署加速，满足弱网络（如小运营商，丢包率高）、跨境（跨洋线路，延迟大）接入网络延迟等问题，解决频繁断线重连，提升远程办公体验。

3）零信任与 SOC 联动，威胁发现与阻断效率提升：零信任方案与安全运营中心（SOC）联动，借助 SOC 海量安全数据分析能力实现对风险访问行为的阻断，通过自动化响应、安全编排等方式，提升风险事件处置效率。

3. 零信任缓解通信业管理模式痛点

电信运营商在全国部署了大量的营业厅，其中有直营模式也有加盟模式，由于营业厅地理位置分散、人员结构复杂等因素，运营商通常把部分业务系统直接部署在公网上提供访问，例如运营商将营业厅

常用的10多个业务系统(包括:2G/3G/4G移动客户端体验管理平台、综合外呼平台、渠道销售实况监控、BSS3.0等)开放在公网上供员工或合作伙伴进行访问。这种管理模式，给安全运维部门增加了很多管理上的困扰，特别是增加安全的风险。

这种方式面临如下的安全挑战:

1）业务暴露面增加：暴露在公网上的业务服务器、VPN 设备经常受到来自全球的网络攻击以及各类网络爬虫的侵扰。

2）运维复杂：访问业务支撑系统的人员结构比较复杂，包括员工、装维人员、渠道代理商、外呼人员、施工监理单位等“四方”人员。上述人员操作水平及安全意识参差不齐，容易形成有意或无意的破坏或越权访问。

3）传统 VPN 安全性不足，稳定性欠佳：VPN 产品只负责构建一条安全访问的隧道，但是缺乏对访问者设备及系统安全性的关注，易被网络攻击者利用通道去访问或破坏内网资源。同时 VPN 容易受到多方因素的影响，访问速度无法保持稳定性，从而影响业务办理

零信任方案能够有效缓解上述问题:

1）网络隐身、减少暴露面：

零信任网关能够将运营商业务系统从互联网上彻底“隐身”。只提供给营业厅等授权第三方认证用户访问。来自网络上的未授权访问、网络攻击、爬虫都将被直接拒绝。

2） 最小化授权访问，杜绝越权访问

零信任方案中的身份管理系统能够对业务人员进行细粒度的访问控制，具体到哪些人员可以访问哪些业务系统，只有拥有相对应业务系统授权的用户才能够访问相对应的业务系统，其余无授权的业务系统，无法进行访问。从而有效控制内部员工的越权访问、蓄意或无意的破坏行为。

3）提升效率，降低运维成本：

零信任中的网络连接机制不再采用传统 VPN 长连接的模式，因此不会掉线，访问的稳定性体验更好，能够提高员工的办公体验和效率。

4. 零信任推动物流业数字化赋能安全发展

物流业是经济贸易和国计民生的生命线，尤其在当前新冠疫情防控和复工复产中发挥了重要作用，保障医疗民生物资运输和全球产业链供应链稳定。近年来，政府连续发布多个物流行业及其相关上下游的政策，在“建设交通强国”“畅通国内大循环、国际双循环”等发展战略中都提出了加强物流信息化、数字化、智能化建设，并在“十四五”规划中提到了构建现代物流的目标。

随着物流业数字化赋能，从为用户提供物流服务，延伸至价值链前端的产、供、销、配等环节，以数据为牵引，利用大数据等技术，实现智能仓储管理、配送服务等业务升级。物流业业务网点离散且数量庞大，员工体量大、权限复杂，为行业网络安全建设带来了诸多挑

战：

1） **瘦终端防护能力有限：**瘦终端是基于行业应用定制的专用终端，相比较于普通终端设备，硬件配置较低，因此难以适配高复杂度的安全算法，导致业务系统更容易被不法分子攻击。

2） **身份/权限管理困难：**物流业职场员工、快递员等员工数量众多，分布在全国办公地点和快递收发点，且快递员在配送过程中处于外网环境，访问内部业务系统需求频繁，如何根据职责权限进行有效的访问控制，实现内外网无差别访问内部业务系统十分困难。

3） **安全产品/理念相互割裂：**物流业往往针对多元的业务线和安全需求，配备了多种多样的安全产品，这些安全产品之间相互割裂严重，安全理念和信息也无法通用共享，缺乏一套完整的安全管理方案，给系统带来严重漏洞。

零信任方案能够有效缓解上述问题：

1） **有效的终端设备安全防护：**零信任按照业务需求，对终端的安全保护诉求进行安全等级的划分，分配不同的安全策略。同时，将终端安全感知代理、威胁检测等组件部署在安全访问通道内，实现对终端的环境信息采集、威胁检测等功能。

2） **统一的身份和权限管理：**零信任针对员工身份、活动、环境等因素，进行动态的身份认证，针对员工需求进行分析，提供单次访问所需的最小权限，限制了资源的可见性，保障业务系统安全。同时还可以指定可信白名单，在确保系统安全可信的前提下提供更多的便

捷性，实现对访问用户的身份和权限的安全管理。

3） **安全产品共享与协同：**零信任通过统一的安全管理中心，对各安全产品进行统一管理，包括下发安全策略，汇总安全数据等；同时，各安全产品间通过接口等方式，实现信息共享和联动，协同处置安全事件，增强了系统防范漏洞的能力，保障了系统安全。

5. 零信任助力能源业应对数字化转型安全风险

近年来，我国能源行业积极拥抱数字经济蓝海，纷纷把数字化转型作为降本增效的重要手段和开拓新业务的重要途径，能源数字化转型在行业内外取得了广泛共识，探索发展新模式和新业态，加强了内外部、上下游数据贯通和共享。然而，在其应用云大物移智链技术完成数字化转型的过程中，安全风险也日益突出：

物联网终端设备网络异构：物联网设备数量/种类众多，且在计算能力、计算资源、网络拓扑差异性很大，致使网络异构问题严重，每类业务或终端部署独立的安全接入方式会导致接入系统数量太多，给企业管理造成困难，安全网络覆盖面的扩张也给企业网络的安全建设带来了严峻的挑战。在终端接入安全方面，考虑物联网终端可能是存在多代设备并存的现象，很多遗留设备未考虑安全防护或安全防护不到位的情况。

身份和授权管理复杂：相比较于其他传统行业，能源行业的身份管理面临着更加复杂的接入场景和访问模式，访问者可能是设备、人

或者其他服务和应用程序，所以身份标识可能是终端 ID、应用 ID、用户 ID、用户组 ID、应用或服务类型 ID 以及服务实例 ID 等; 同时，能源行业业务层面与技术层面都具有高度的开放性，业务系统的设计无法预见所有的场景并进行安全设计，计算技术迭代发展也需要安全防护措施不断更新。

缺少统一处理模型实现原生安全：原生安全是当前能源业应用开发的重要发展方向，通过多种技术把安全措施内嵌到业务流程中，前置安全管理，大大提高业务安全防护能力，降低安全事件发生后业务流程安全漏洞改造成本。然而，能源企业往往缺乏统一的处理模型，大大加剧了安全应用开发和安全防护的复杂度。

零信任方案能够有效缓解上述问题:

物联网安全代理实现终端接入安全：零信任通过采用物联网安全代理的模式，隔离物联网终端到后台系统的访问，终端监测和安全加强可以在物联网代理中实现。物联网代理以软件模块的形式部署在边缘侧，可依据安全需求动态升级。

统一身份和动态授权管理：零信任方案能够对人员、资产、服务和应用程序统一管理，全面掌握企业资源，同时可以简化访问控制的处理机制。此外，采用动态授权机制，打破原来以业务系统为基础的安全防护，构建更细粒度的管控机制，对每次请求进行授权，实现身份和权限的安全统一管理。

安全与业务解耦，降低业务安全防护设计要求：零信任解决方案

将所有的交互访问规范成请求响应模型，采用独立于应用程序的安全策略库和访问控制引擎处理，充分利用 ACL 和授权管理模式，通过细化服务的注册接口，提升访问控制的粒度，并结合安全作为服务设施，规范身份管理、密码管理、加解密设施和监测审计等服务设施，最终实现安全防护和应用程序的解耦，降低业务系统在安全防护方面的设计要求。

6. 零信任为地产业探寻第二增长曲线安全护航

在过往的发展中，地产行业步入存量时代，开发环节行业集中度快速提升，整体利润水平下降，企业需要从开发销售业务向资产运营和服务转型。地产业希望借助数字化转型的契机，通过数字化进行赋能，来助力行业探寻新的业务方向和可能的第二增长曲线。而在其转型升级和实现降本增效的过程中，面临诸多安全风险:

1)人员安全意识与终端安全水平参差不齐：相比较与企业的 IT 环境中设备统一管理、专人维护的情况，地产业的行业特性致使其终端数量众多分散在各处，并且由终端用户自行维护，用户的使用习惯、安全意识参差不齐，往往让终端成为安全风险集中爆发的场所，所谓牵一发而动全身，进而直接影响企业现有网络环境的安全。

2)数据泄漏防范困难：终端分散在各处，终端设备往往需要通过 VPN 等方式来频繁访问企业内网的数据，由于 VPN 自身安全系数低以及缺乏良好的管理手段，致使数据安全隐患日益增加，近年来由于数

据泄密导致的安全事件比例日益上升，这种事件的出现对于企业形象以及企业核心竞争力的影响往往是毁灭性的，如何有效的解决数据防泄漏的问题日益困扰着企业的管理层。

零信任方案能够有效缓解上述问题:

1）多数据源信任评估，提升人员安全意识和终端安全水平：零信任策略引擎通过对多源数据分析，实现对每一次访问行为的信任评估，包括终端安全情况、用户行为信息等，终端、用户行为等若存在安全风险，信任评估结果将无法满足零信任控制引擎要求，不被授予访问资源的权限，倒逼人员提升安全意识，保证访问终端的安全性。

2）持续动态认证和权限评估，及时发现数据泄露事件：零信任方案对用户的访问行为进行持续监测，动态身份认证和权限判定，在发现可疑的数据泄露事件时，及时阻断当前的访问行为，将数据泄露事件控制在最小范围。

四、零信任安全趋势

（一）零信任与原生安全理念融合，助力企业构建全因子信任安全架构

基于零信任理念，结合原生安全的思想，全因子信任安全架构期望建设一个所有要素都处于安全可信状态的 IT 架构，对架构的形态进行进一步丰富，强调架构中各组件分布式部署能力、组件灵活扩展能力、组件联动协同处置安全事件能力。**全因子信任指**构成 IT 架构

的所有因子处在可信任状态或具备恢复至可信任状态的能力；所有因子包括静态因子和动态因子，静态因子指数据、网络、应用系统、服务器、终端设备等物理和虚拟资源，动态因子指 IT 架构运营中的所有活动，如静态因子间的访问、操作等，动态因子作用于静态因子使其发生变化。**全因子信任安全架构**由多个逻辑组件构成，各逻辑组件间通过安全信息共享、安全事件协同处置保障 IT 系统全生命周期安全。

全因子信任安全尽可能保证所有因子处在可信任状态，但因子的安全性动态变化，仍存在不安全的可能。对于静态因子，在发现其可能存在安全问题时应及时采取措施，使其恢复至可信任状态；对于动态因子，仅在其处于可信任状态时才允许进行，禁止不可信任的动态因子的进行，以避免其对可信任静态因子产生影响，直到动态因子通过采取措施恢复至可信任状态。

基于零信任的基本原则，全因子信任基本原则补充了原生安全的能力：

安全产品原生化。实现全因子信任所依赖的安全产品原生化发展。第一，**部署应用更加便捷高效**，以组件形式虚拟化、容器化部署，或以 SaaS 形式交付，统一配置和管理，能够按需使用，安全防护能力弹性扩展，底层资源利用率高；第二，**与 IT 架构深度融合**，避免传统安全架构与 IT 架构割裂的问题，能够获取和整合 IT 架构的各类数据信息，深入挖掘潜在安全风险，同时适应 IT 架构特性，解决 IT 架

构面临的特有安全问题；第三，**开放协同**，对外通过接口等方式，实现安全产品间的信息共享和联动，协同处置安全事件，对因子进行更有力的控制。

全因子信任安全架构如图 7 所示，架构由因子和多个逻辑组件构成，在实际应用中，每个逻辑组件可以由一个或多个实体组件组成，同时，不同逻辑组件也可能由一个实体组件实现。

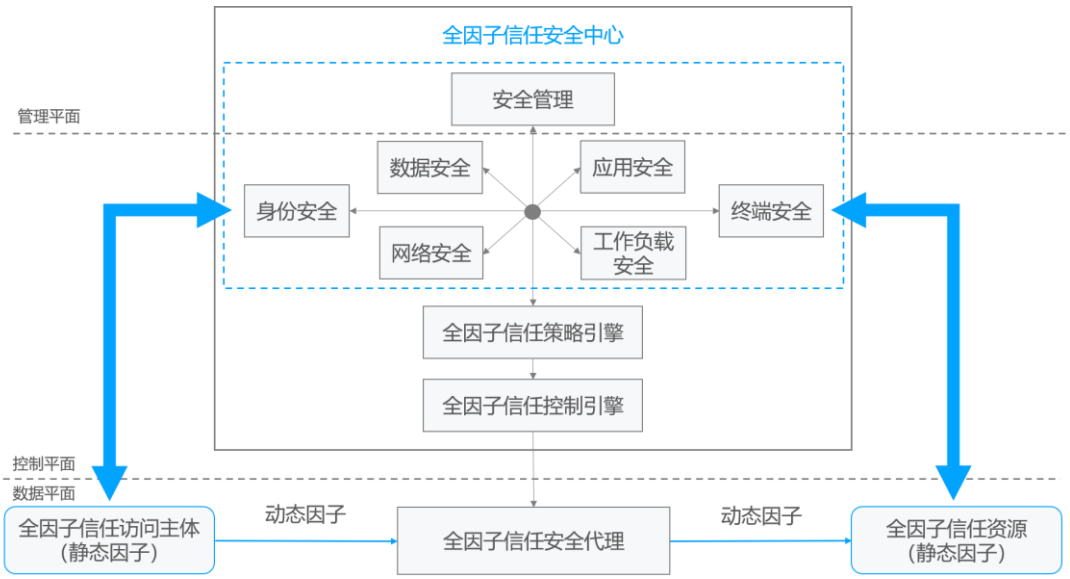

图 7 全因子信任安全架构

在全因子信任安全架构中，静态因子分为全因子信任资源和全因子信任访问主体两种角色，后者对前者进行访问、操作等活动，既实施某一动态因子。一个静态因子既可以成为全因子信任访问主体，也可以作为全因子信任资源：

全因子信任资源：被实施动态因子的一方，为企业内部资源，包括物理设备、云服务等基础设施资源，软件与系统，接口，数据等。

全因子信任访问主体：实施动态因子的一方，主要包括，**一是具**

备发起动态因子能力的企业内部资源（基础设施资源，软件与系统，接口，电脑、打印机等终端设备），无论其是否处于企业内部网络中；**二是非企业内部资源**，如员工手机、平板电脑等自有终端设备，第三方应用系统等。无论访问主体为何种资源，其发起的动态因子都需经过动态验证和授权。

全因子信任安全架构逻辑组件主要分为四部分，各逻辑组件受管理平面统一纳管，通过控制平面进行交互通信，而全因子信任访问主体和资源间通过数据平面进行通信：

全因子信任策略引擎：该组件负责权限的评估和决策。

全因子信任控制引擎：该组件作为策略控制点。

全因子信任安全代理：该组件作为策略执行点，建立其访问主体和被访问资源之间的安全通道。

全因子信任安全中心：对 IT 架构进行安全防护，**一是确保静态因子处于安全状态**，在发现安全风险时及时采取防护措施，**二是与全因子信任策略引擎协同**，将收集和分析后的安全信息传递给策略引擎，为其进行信任评估和决策提供依据，同时也可以收集策略引擎获取的全因子信任访问主体信息，为安全事件分析提供更多数据支撑。安全中心又可分为多个子组件，包括：**网络安全子组件、数据安全子组件、应用安全子组件、身份安全子组件、工作负载安全子组件、终端安全子组件、安全管理子组件**。

零信任理念仍处于渐进式发展阶段，在每个发展阶段融入时下新

的理念，基于零信任理念和原生安全的全因子信任安全架构，最终能实现全部组件的互联互通，协同处理安全事件，做到全部因子处于可信状态的安全体系。

（二）广域网络与零信任结合，实现企业网络边缘安全接入

SASE 将零信任与 SD-WAN 融合，是未来企业实现网络边缘安全接入的主要选择。 SASE 将网络即服务和安全即服务的概念聚合，并以分布式云服务的方式向企业提供，无需企业对现有物理网络进行大规模改造，就可以以最便捷方式落地零信任。**企业利用 SASE 实现信任接入能解决总部/分支机构协同办公、远程办公无感接入，以及 SD-WAN 安全场景。**

SASE 为企业提供端到端安全。传统网络架构是基于数据中心的技术堆栈，主要面向实体数据中心时代用户和设备的访问。随着企业纷纷拥抱云服务、边缘计算和混合云等新兴技术，云端采用传统网络安全架构面临诸多问题：云计算分布式部署模式打破网络边界、云边界的安全设备不具备更细粒度的防护能力、依靠单一终端进行安全服务的方式难以完成云上安全防护、分支机构需要通过数据中心才能安全连接到企业云上资源。SASE 作为云服务可以解决上述问题。**一是 SASE 具备全球网络连接能力。**SASE 集成 SD-WAN，SD-WAN 提供了遍布全球的网络连入基础设施，通过扩展 SD-WAN，在网络边缘提供

安全能力，令企业分支变薄。**二是 SASE 使用云原生架构不依赖任何硬件设备。**SASE 使用云原生架构，在 PoP 点处基于云上资源构建整合云原生安全功能的、支持多租户运营的云服务，同时利用云的弹性、自适应性、自恢复能力、自维护能力等，提供了技术层面与商业模式共具灵活敏捷的厚云端。**三是 SASE 具备分布式的安全能力。**随着企业分支遍布于各地，且数据中心不再是整个网络的中心，SASE 支持将检查引擎带到用户附近的 PoP 点，更加符合边缘环境实际情况，兼容所有边缘，并向全部边缘交付尽可能好的体验。