CAICT 中国信通院

奇安信
新一代网络安全领军者

网络安全先进技术与应用发展系列报告

零信任技术（Zero Trust）

（2020 年）

中国信息通信研究院安全研究所
奇安信科技集团股份有限公司

2020 年 8 月

版权声明

前　言

随着全球数字化转型的逐渐深入，在“云大物移智工”等新技术发展支撑下，零信任从原型概念加速演进，成为新一代信息技术安全架构。在过去的 2019 年，国内零信任从概念走向落地，零信任安全架构以其兼容移动互联网、物联网、5G 等新兴应用场景，支持远程办公、多云环境、多分支机构、跨企业协同等复杂网络架构，受到各界青睐，从产品研制、解决方案到应用试点示范，到逐步探索完善适应不同场景的零信任应用实践。进入 2020 年以来，在“新基建”和疫情的双重刺激下，零信任作为一种可支撑未来发展的最佳业务安全防护方式，成为我国网络安全界的焦点。

本报告聚焦零信任发展，从技术、产业、应用和实践四个维度进行剖析：技术部分包含零信任安全架构定义和关键技术的最新研究成果；产业部分介绍了国内外产业发展、标准化等方面的最新进展；应用部分汇集远程办公、大数据中心、云计算、物联网和 5G 应用等核心应用场景的零信任解决方案建议；实践部分聚焦零信任规划与部署，介绍零信任实施经验。最后以零信任建议和展望总结全文，希望通过本书帮助更多的人理解和实践零信任，加快推进零信任创新发展，为以新基建为代表的数字化转型保驾护航。

目 录

一、零信任技术和产业发展现状.....1
（一）零信任核心原则.....2
（二）零信任安全架构及组件.....4
（三）零信任关键技术.....7
（四）国外产业发展及应用规划.....10
（五）国内零信任概念走向落地.....12
二、零信任应用场景.....14
（一）远程办公.....14
（二）大数据中心.....18
（三）云计算平台.....22
（四）物联网.....26
（五）5G 应用.....30
三、零信任实施建议.....34
（一）使用范围.....34
（二）实施规划.....38
（三）技术实现.....40
四、零信任思考和展望.....46

图 目 录

图 1 零信任概念演进历程图.....2
图 2 零信任架构总体框架图.....4
图 3 基于零信任架构的远程办公安全参考架构.....18
图 4 数据中心内部访问流程示意图.....21
图 5 数据中心安全接入区案例示意图.....22
图 6 基于零信任架构的云计算平台安全参考架构.....26
图 7 基于设备指纹的物联边缘网关零信任方案示意图.....30
图 8 零信任实施技术路线示意图.....41

表 目 录

表 1 零信任解决方案市场供应商分析.....11
表 2 5G 架构下的主要对象.....31
表 3 5G 架构下的风险来源.....31
表 4 5G 架构下的攻击情况.....31
表 5 5G 典型攻击行为案例.....32

一、零信任技术和产业发展现状

近年来，中央地方高度重视新型基础设施建设（简称“新基建”），国家高层会议密集提及新基建，各省积极推动新基建项目集中开工。作为新基建三大领域之一的信息基础设施，成为数字经济的关键乃至整个经济社会的神经中枢，其安全性、敏捷性、稳定性等将对新基建安全发展产生至关重要的影响。因此，在主动拥抱新基建的同时，首先应当系统性地评估网络安全的准备工作是否到位。随着新一代信息技术的快速演进，新技术态势下的网络安全威胁和风险不断涌现、扩散，移动互联网、物联网、工业互联网、车联网等新型应用场景致使物理网络安全边界逐步瓦解，用户、设备、业务、平台等多样化趋势不可阻挡，新场景叠加的安全风险不容忽视。为了应对逐渐复杂的网络环境，一种新的网络安全技术架构—零信任逐步走入公众视野，其创新性的安全思维契合数字基建新技术特点，着力提升信息化系统和网络的整体安全性，受到了广泛关注，并被寄予厚望。

零信任雏形最早源于 2004 年成立的 Jericho Forum[1]，其成立目的是寻求网络无边界化趋势下的全新安全架构及解决方案。2010 年，Forrester[2]的分析师约翰·金德维格正式提出了“零信任”（Zero Trust）一词[3]。随着业界对零信任理论和实践的不断完善，零信任从原型概念向主流网络安全技术架构逐步演进，从最初网络层微分段的范畴开

[1] Jericho Forum：耶利哥论坛，成立于 2004 年，公益论坛

[2] Forrester：弗雷斯特研究公司，成立于 1983 年，技术和市场调研公司

[3] S. Rose et al., Zero Trust Architecture, National Institute of Standards and Technology (NIST) Draft (2nd) Special Publication 800-207, Gaithersburg, Md., February 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207- draft2.pdf.

始，逐步演变成为覆盖云环境、大数据中心、微服务等众多场景的新一代安全架构。

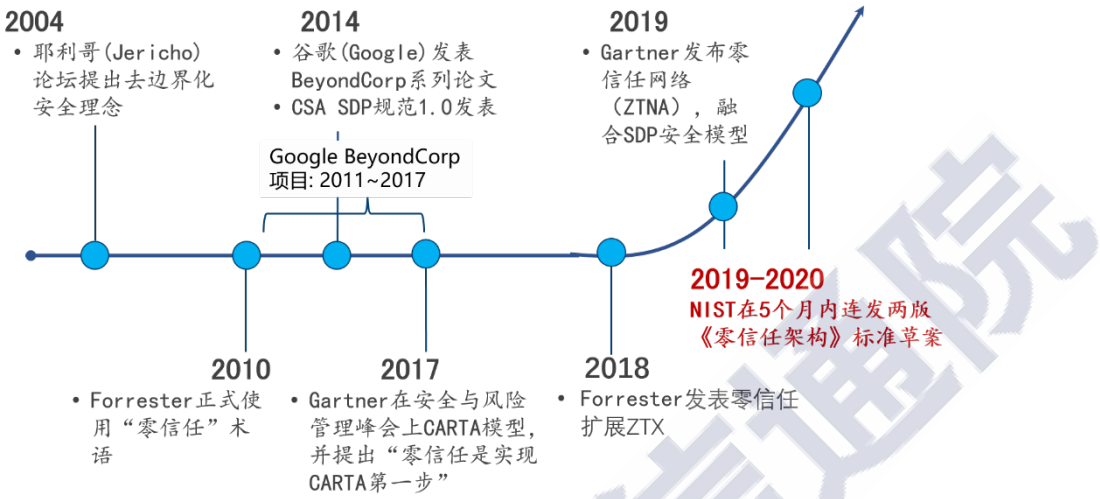

图 1 零信任概念演进历程图

（一）零信任核心原则

《零信任网络：在不可信网络中构建安全系统》一书中，作者使用如下五句话对零信任安全进行了抽象概括：

- 网络无时无刻不处于危险的环境中。
- 网络中自始至终存在外部或内部威胁。
- 网络位置不足以决定网络的可信程度。
- 所有的设备、用户和网络流量都应当经过认证和授权。
- 安全策略必须是动态的，并基于尽可能多的数据源计算而来[4]。

简而言之，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**

[4]【美】埃文·吉尔曼（Evan Gilman）、道格·巴特（Doug Barth），零信任网络：在不可信网络中构建安全系统，人民邮电出版社，北京，2019 年 7 月

资源的人、事、物进行验证。

基于对零信任安全框架的理解，可将零信任架构的原则归纳如下：

（1）**将身份作为访问控制的基础**：零信任的信任关系来自于对所有参与对象的身份验证。所有参与对象共同构成端到端信任关系的基础，这些参与对象包括基础网络、设备、用户、应用等。零信任架构为所有对象赋予数字身份，基于身份而非网络位置来构建访问控制体系。

（2）**最小权限原则：**零信任架构强调资源的使用按需分配，仅授予执行任务所需的最小特权，同时限制了资源的可见性。通过使用端口隐藏等技术手段，默认情况下资源对未经认证的访问主体不可见。授权决策时将人员、设备、应用等实体身份进行组合，形成访问主体。针对主体的组合信息和访问需求，以及信任评估和权限策略计算情况，确定是否授予访问权限。

（3）**实时计算访问控制策略**：授权决策依据主体的身份信息、权限信息、环境信息、当前主体信任等级等，通过将这些信息进行实时计算，形成访问控制策略。在资源访问过程中，一旦授权决策依据发生了变化，将重新进行计算分析，必要时即时变更授权决策。

（4）**资源受控安全访问：**零信任架构对所有业务场景、所有资源的每一个访问请求进行强制身份识别和授权判定，确认访问请求的权限、信任等级符合安全策略要求后才予以放行，实施会话级别的细粒度访问控制。零信任默认网络互联环境是不安全的，要求所有的访问连接都必须加密。

（5）**基于多源数据进行信任等级持续评估**：主体信任等级是零信任授权决策的判定依据之一，主体信任等级根据实时多源数据，如身份、权限、访问日志等信息计算得出，参与计算的数据种类越多，数据的可靠性越高，信任等级的评估就越准确。人工智能技术的迅猛发展为信任评估赋能，通过专家系统、模型训练、机器学习等人工智能技术，紧扣应用场景，提升信任评估策略计算效率，实现零信任架构在安全性、可靠性、可用性、安全成本等方面的综合平衡。

（二）零信任安全架构及组件

参考美国国家标准与技术研究院 NIST 特别出版物 SP800-207《零信任架构》定义的零信任体系架构，结合零信任的实践探索，本报告将零信任架构的总体框架归纳如下：

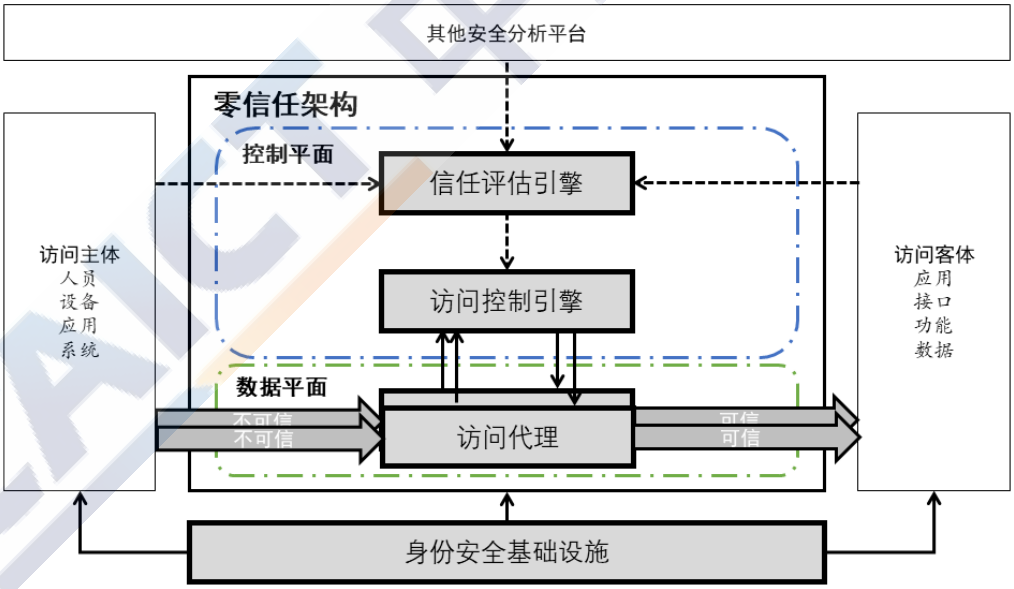

图 2 零信任架构总体框架图

零信任秉承“从不信任并始终验证”的安全原则，对访问主体和访问客体之间的数据访问和认证验证进行处理，并将访问行为实施平

面分解为用于网络通信控制的控制平面和用于应用程序通信的数据平面。访问主体通过控制平面发起的访问请求，由信任评估引擎、访问控制引擎实施身份认证和授权，一旦访问请求获得允许后，系统动态配置数据平面，访问代理接受来自访问主体的流量数据，建立一次性的安全访问连接。信任评估引擎将持续进行信任评估，把评估数据提供给访问控制引擎进行零信任策略决策运算，判断访问控制策略是否需要改变，如有需要及时通过访问代理中断连接，快速实施对资源的保护。

1.核心组件

（1）信任评估引擎

零信任架构中实现持续信任评估能力的核心组件之一，与访问控制引擎联动，持续为其提供主体信任等级评估、资源安全等级评估以及环境评估等评估数据，作为访问控制策略判定依据。

（2）访问控制引擎

持续接收来自信任评估引擎的评估数据，以会话为基本单元，秉承最小权限原则，对所有的访问请求进行基于上下文属性、信任等级和安全策略的动态权限判定，最终决定是否为访问请求授予资源的访问权限。

（3）访问代理

零信任架构的数据平面组件，是动态访问控制能力的策略执行点。

访问代理拦截访问请求后，通过访问控制引擎对访问主体进行身份认证，对访问主体的权限进行动态判定。访问代理将为认证通过、并且具有访问权限的访问请求，建立安全访问通道，允许主体访问被保护资源。当访问控制引擎判定访问连接需要进行策略变更时，访问代理实施变更，中止或撤销会话。

2. 身份安全基础设施

身份安全基础设施是实现零信任架构的关键支撑组件，甚至可以说，零信任架构借助现代身份管理平台实现对人/设备/系统的全面、动态、智能的访问控制。身份管理和权限管理为访问控制提供所需的基础数据来源，其中身份管理实现各种实体的身份化及身份生命周期管理，权限管理实现对授权策略的细粒度管理和跟踪分析。典型的身份安全基础设施包括：PKI[5]系统、身份管理系统、数据访问策略等。

身份基础设施可以是企业的 4A[6]、IAM[7]、AD[8]、LDAP[9]、PKI 等基础设施，也可以是企业的人力资源等业务系统。随着企业规模的发展，企业人员、设备、权限都会越来越庞大，零信任架构的身份基础设施需要能满足现代 IT[10]环境下复杂、高效的管理要求。作为零信任架构的支撑组件，还需要支持数字证书，提供生物特征、电子凭证等多模式身份鉴别，并结合身份管理，对主体和客体进行有效性验证。

[5] PKI：Public Key Infrastructure，公钥基础设施
[6] 4A：认证 Authentication、授权 Authorization、账号 Account、审计 Audit，统称为统一安全管理平台解决方案
[7] IAM：Identity and Access Management，身份与访问管理
[8] AD：Active Directory，活动目录
[9] LDAP：Lightweight Directory Access Protocol，轻型目录访问协议
[10] IT：Internet Technology，信息技术，用于管理和处理信息所采用的各种技术的总称

3. 其他安全分析平台

企业现有的安全平台建设成果，为零信任提供资产状态、规范性要求、运行环境安全风险、威胁情报等数据。综合大量的日志信息能够支撑零信任实现持续的动态评估。其中，典型的其他安全分析平台包括: 终端防护与响应系统、安全态势感知分析系统、行业合规系统、威胁情报源、安全信息和事件管理系统等。

（三）零信任关键技术

1. 现代身份与访问管理技术

现代身份与访问管理技术通过围绕身份、权限、环境、活动等关键数据进行管理与治理的方式，确保正确的身份、在正确的访问环境下、基于正当的理由访问正确的资源。现代身份与访问管理技术主要包括身份鉴别、授权、管理、分析和审计等，是支撑企业业务和数据安全的重要基础设施。

随着数字化转型的进一步深化，用户访问关系更加复杂，新型服务和设备的需求与日俱增。比如用户从企业雇员、外包员工，发展到合作伙伴、顾客等；设备涵盖手机、平板电脑、可穿戴设备等各种物联网设备；此外，同一个用户可能使用多台设备，这些都增加了用户和设备管理的难度。同时，大量企业、机构办公地点遍布全国，甚至全世界，地理位置分散导致身份和访问管理系统需要遵守不同地区关于数据隐私保护、数据留存等方面的法律要求。

业务系统自身的技术架构和环境也在发生变化，例如，越来越多

的 IT 基础设施和业务应用云服务化，可扩展的混合 IT 环境已成为主流的系统运行环境。传统静态、封闭的身份和访问管理机制已经不能满足现代信息系统对身份与访问管理的要求，即：确保正确的人或“物”，出于正确的原因，能够在正确的时间、正确的地点，从正确的设备中获取到正确的资源（应用、数据等）。

采用现代身份与访问管理技术构建的智能身份管理平台，具有敏捷和灵活的特点，适配各种新技术应用场景。零信任具备高级分析能力，能够应对外部攻击、内部威胁、身份欺诈等各种安全威胁，并通过采用动态的策略，实现持续自我完善，不断调整以满足新的业务、技术和安全性要求。

2.软件定义边界技术

SDP[11]技术旨在通过软件的方式，在“移动+云”的时代背景下，为企业构建起虚拟边界，利用基于身份的访问控制以及完备的权限认证机制，为企业应用和服务提供隐身保护，使网络黑客因看不到目标而无法对企业的资源发动攻击，有效保护企业的数据安全。

SDP 具有五大特点：

（1）网络隐身：SDP 应用服务器没有对外暴露的 DNS[12]、IP[13]地址或端口，必须通过授权的 SDP 客户端使用专有的协议才能进行连接，攻击者无法获取攻击目标。

（2）预验证：用户和终端在连接服务器前必须提前进行验证，

[11] SDP：Software Defined Perimeter，软件定义边界
[12] DNS：Domain Name System，域名系统（服务）协议
[13] IP：Internet Protocol，网络之间互连的协议

确保用户和设备的合法性。

（3）预授权：根据用户不同的职能以及工作需求，依据最小权限原则，SDP 在设备接入前对该用户授予完成工作任务所需的应用和最小访问行为权限。

（4）应用级的访问准入：用户只有应用层的访问权限，理论上无法获取服务器的配置、网络拓扑等其他信息，无法进行网络级访问。

（5）扩展性：除采用特殊协议对接 SDP 服务器以外，其他访问依然基于标准的网络协议，可以方便的与其它安全系统集成。

3. 微隔离技术

微隔离（Micro-segmentation）（又称软件定义隔离、微分段）最早由 Gartner[14]在其软件定义的数据中心相关技术体系中提出。对数据中心而言，主要有南北向流量和东西向流量：南北向流量是指通过网关进出数据中心的流量；东西向流量是指数据中心内部服务器彼此相互访问的内部流量。传统防护模式通常采用防火墙作为南北向流量的安全防护手段，一旦攻击者突破防护边界，缺少有效的安全控制手段用来阻止东西向流量之间的随意访问。随着东西向流量占比越来越大，微隔离技术应运而生，其作为一种网络安全技术，重点用于阻止攻击者在进入企业数据中心网络内部后的东西向移动访问。

从广义上讲，微隔离就是一种更细粒度的网络隔离技术，使用策略驱动的防火墙技术（通常是基于软件的）或者网络加密技术来隔离

[14] Gartenr，高德纳咨询公司，成立于 1979 年，信息技术研究和分析公司

数据中心、公共云 IaaS[15]和容器，在逻辑上将数据中心划分为不同的安全段，每个段包含混合场景中的不同工作负载、应用和进程，可以为每个段定义安全控制和所提供的服务。此外，数据中心往往包括海量的节点，频繁变化带来的工作量不可预估，传统的人工配置模式已无法满足管理的需求，自动适应业务变化的策略计算引擎是微隔离成功的关键。

（四）国外产业发展及应用规划

近年来，零信任在国际上的应用已经越来越广泛，零信任产业已初具规模。Google[16]、Microsoft[17]等业界巨头率先在企业内部实践零信任并推出完整解决方案；Duo[18]、OKTA[19]、Centrify[20]、Ping Identity[21]为代表的身份安全厂商当仁不让，推出“以身份为中心”的零信任方案；Cisco[22]、Akamai[23]、Symantec[24]、VMware[25]、F5[26]等公司推出了偏重于网络实施方式的零信任方案；同时，零信任也催生了一批非常成功的创业公司，包括 Vidder[27]、Cryptzone[28]、Zscaler[29]、Illumio[30]等。根据 Forrester 2020 年二季度对于零信任产业的统计数据，按照零信

[15] IaaS：Infrastructure as a Service，基础设施即服务
[16] Google：谷歌公司，成立于 1998 年，跨国科技企业
[17] Microsoft：微软公司，成立于 1975 年，跨国科技企业
[18] Duo：美国网络安全公司，成立于 2010 年
[19] OKTA：美国网络安全公司，成立于 2009 年
[20] Centrify：美国网络安全公司，成立于 2004 年
[21] Ping Identity：美国网络安全公司，成立于 2002 年
[22] Cisco：思科，成立于 1984 年，网络解决方案供应商
[23] Akamai：阿卡迈，成立于 1998 年，互联网服务供应商
[24] Symantec：赛门铁克，成立于 1982 年，网络安全公司
[25] VMware：威睿，成立于 1998 年，云基础架构和移动商务解决方案供应商
[26] F5：应用交付网络和业务解决方案供应商，成立于 1996 年
[27] Vidder：初创企业，网络安全公司
[28] Cryptzone：美国网络安全公司，成立于 2008 年
[29] Zscaler：美国网络安全公司，成立于 2008 年
[30] Illumio：美国网络安全公司，成立于 2013 年

任解决方案收入，将该市场的供应商分为三类，见下表所示。其中，零信任营收超过 1.9 亿美元的厂商已有 10 余家，零信任已经进入规范化、规模化产业发展阶段。

表 1 零信任解决方案市场供应商分析

公司规模	公司列表（字母排序）	营收标准
大型	Akamai、Cisco、Fortinet、Google、Illumio、Microsoft、Okta、Palo Alto Networks、Proofpoint、Unisys	收入超过 1.9 亿美元
中型	AlgoSec、Armis、Centrify、Check Point Software Technologies、FireMon、Forcepoint、Forescout、Gigamon、GitLab、Ionic Security、MobileIron、Tufin、Venafi	收入在 0.35 亿—1.9 亿美元
小型	A10 Networks、AppGate、Awingu Axis Security、BlackBerry、ClearedIn、ColorTokens、Edgewise、Guardicore、HyperQube、IDENProtect、Infocyte、ShieldX Networks、ThreatLocker、Zentera Systems	收入少于 3500 万美元

数据来源：Forrester[31]

随着技术的成熟和产业基础的逐步完善，2019 年以来，美国军方、联邦政府和标准化组织纷纷发表各自的白皮书、评估报告和标准草案，阐述各自对零信任的认识和规划。Forrester 在《2019 年度预测：转型走向务实》中明确指出零信任将在美国某些特定的领域成为标准的、阶段性的网络安全架构。美国军队、政府将其作为优先选用的网络安全战略和指导原则，并对其它行业产生深刻的影响。

DIB[32]作为美国国防部下属专注于技术与创新的机构于 2019 年 7 月发布了 DIB 零信任架构白皮书《零信任安全之路》，指导国防部网

[31] 数据来源：Forrester，Now Tech: Zero Trust Solution Providers, Q2 2020

[32] DIB：Defense Innovation Board，美国国防创新委员会

络实施零信任架构。紧接着在 2019 年 10 月发布报告《零信任架构（ZTA）建议》，建议国防部将零信任列为最高优先事项实施。这两个重量级文件的发布，反映出美国国防部对零信任的重要定位：零信任架构是美国国防部网络安全架构的必然演进方向。

作为联邦政府顾问智囊的美国技术委员会-工业咨询委员会，于 2019 年 4 月发布了《零信任网络安全当前趋势》白皮书。通过开展市场研究，评估了零信任技术成熟度和准备度、适合性、可扩展性和基于实际实现的可承受性，最终，对美国政府机构采用零信任提出评估建议。

（五）国内零信任概念走向落地

2019 年 9 月，工信部公开发布的《关于促进网络安全产业发展的指导意见（征求意见稿）》中，将“零信任安全”列入需要“着力突破的网络安全关键技术”。

国内安全厂商，一直以来都关注着零信任在国际上的发展并结合国内实际场景进行落地实践。奇安信、腾讯、阿里、华为、深信服、启明等安全和互联网厂商都利用各自在安全领域的技术优势，推出了零信任整体解决方案，并积极寻找机会，开展全面应用实践；竹云、九州云腾等身份管理厂商积极推动身份管理技术在零信任架构上的应用；云深互联、蔷薇灵动、山石科技等厂商则积极推动 SDP、微隔离等零信任技术方案的应用实践。2019 年以来，我国相关部委、部分央企、大型集团企业开始将零信任架构作为新建 IT 基础设施安全架

构；银行、能源、通信等众多领域和行业针对新型业务场景，开展采用零信任架构的关键技术研究和试点示范。

同时，我国也在积极推进零信任的标准化进程。2019 年 7 月，在中国通信标准化协会 CCSA TC8 WG3[33]第 60 次工作会议上，腾讯牵头提交的《零信任安全技术-参考框架》行业标准正式通过评审，成为国内首个立项的零信任安全技术行业标准。

2020 年 5 月，在全国信息安全标准化技术委员会 2020 年第一次线上工作组“会议周”上，奇安信牵头提出的《信息安全技术 零信任参考体系架构》，在 WG4[34]（认证与鉴别组）工作组成功立项，这是零信任标准层面的首个国家标准，对接身份鉴别、认证、风险评估、可信计算环境等相关信息安全标准，确定零信任架构组成、功能及内外部组件间关系，对于应对数字化转型与信息技术革新下的新型网络环境的安全威胁，推进零信任在云计算、大数据、物联网、5G[35]等领域的横向应用，具有重大意义。

[33] CCSA TC8 WG3：China Communications Standards Association，中国通信标准化协会网络与信息安全技术工作委员会安全管理工作组

[34] WG4：全国信息安全标准化技术委员会 认证与鉴别组

[35] 5G：The 5th Generation Mobile Communication Technology，第五代移动通信技术

二、零信任应用场景

面向不同的应用环境、业务场景，零信任架构有多种灵活的实现方式和部署模式。面向远程办公、云计算平台、大数据中心、物联网、5G 应用等典型场景，按照访问主体和资源之间的关系，数据平面的访问代理重点考虑采用便于和被保护资源相结合的部署模式，如“设备代理+网关”模式、“资源门户”模式、“设备应用沙箱”模式等，搭建安全的访问通道，对访问请求进行分流。控制平面的访问控制引擎负责指挥，按照“先认证后连接”原则，建立、维持有效连接，实施对资源的安全访问控制。在此过程中，持续开展安全监控评估，对应用场景中出现的安全威胁及时响应，消减风险。

（一）远程办公

远程办公已经逐步成为一种常态化的工作模式，这也是移动办公延展后的必然结果。从国内 2 月份以来的情况看，全民在抗击疫情和复工复产两手抓的形势下，开始了规模庞大的居家远程办公，据第三方调查数据显示，2020 年春节期间，中国有超过 3 亿人远程办公[36]，以前在办公室开展的工作全部搬回了员工的家中，不再局限于日常工作协同沟通、视频会议等，包括远程办公平台、远程开发、远程运维、远程客服、远程教学等等都已成为现实，远程办公已经成为走出固定地点（如办公室、写字楼），随时随地的办公形态。事实上，在欧美国家远程办公早就已经成为一种常态化的办公模式。在我国，远程办公

[36] 全球抗疫云办公云教育陡然升温 - 环球网 [EB/OL].(2020-03-21)[2020-03-23]. https://finance.huanqiu.com/article/3xVW4gmkvN7

也将逐步作为未来工作模式之一，而不仅仅是特殊时期的一种办公形式。

1. 应用场景分析

在现在企业的信息化建设环境中，远程办公必须涵盖的应用场景越来越复杂：

（1）接入人员和设备的多样性增加

员工、外包人员、合作伙伴等各类人员，使用家用 PC[37]、个人移动终端、企业管理设备等，从任何时间、任何地点远程访问业务。各种接入人员的身份和权限管理混乱，弱密码屡禁不止；接入设备的安全性参差不齐，接入程序漏洞无法避免等，带来极大的风险。

（2）企业资源暴露程度大幅度增加

企业资源可能位于企业内网服务器，也可能被企业托管在公有云上的数据中心；企业服务通常需要在不同的服务器之间交互，包括部署在内网、公有云、私有云中的服务器。一个典型的场景，公有云上的网站服务器与内网应用程序服务器通信后，应用程序服务器检索获得内网数据，返回给网站服务器。资源信息基础设施与应用服务之间的关系越复杂，引入的系统风险越高。

（3）数据泄露和滥用风险大幅增加

在远程办公过程中，企业的业务数据会在不同的人员、设备、系

[37] PC：Personal Computer，个人计算机

统之间频繁流动，原本只能存放于企业数据中心的数据也不得不面临在员工个人终端留存的问题。同时，数据移动增加了数据“意外”泄露的风险，安全措施相对较弱的智能手机频繁访问企业数据也将对企业数据的机密性造成威胁。

2. 先进性和创新性

近年来外部攻击的规模、手段、目标等都在演化，有组织的、武器化的、以数据及业务为攻击目标的高级持续攻击屡见不鲜。利用远程办公找到漏洞，突破企业边界后进行横向移动访问，成为最常见和最有效的攻击手段之一。

常见远程接入的方式主要有两种，一种是通过端口映射将业务系统直接在公网上开放；另一种是使用 VPN[38]打通远程网络通道。各组织都在对自己的安全边界进行“加固”，尽量使用 VPN 远程接入而非直接开放业务端口，增强威胁检测的能力等等。然而，这些手段基本上可以视作是传统的边界安全方案上的单点增强，难以系统性缓解远程移动办公带来的安全威胁。攻击者可以轻易利用弱密码破解或撞库，通过 VPN 进入内网，甚至可以利用 VPN 漏洞、业务系统漏洞直接进行渗透，突破企业边界，最终窃取有价值的数据资产。

零信任安全架构针对远程办公应用场景，不再采用持续强化边界的思维，不区分内外网，针对核心业务和数据资产，梳理访问这些资产的各种访问路径和场景，在人员、设备和业务之间构建一张虚拟的、

[38] VPN：Virtual Private Network，虚拟专用网络

基于身份的逻辑边界，针对各种场景构建一体化的零信任动态访问控制体系。主要包括以下创新点和先进性：

（1）构建更安全的远程办公网络

通过实施“从不信任并始终验证”，不同类型用户只能按照预先确定的信任级别，访问预先申请的企业资源，未预先申请的企业资源将无法被访问，阻止企业内部“漫游”情况。

（2）增强对企业应用和数据的保护

在实施“按需受控访问”的基础上，有效整合资源保护相关的数据加密、网络分段、数据防泄露等技术，保护应用资源、数据在网络中的传输和存储，并优先保护高价值资源。

（3）大面积减少攻击暴露面

用户通过访问认证之前，资源对用户隐身；即便在用户通过访问认证和授权，成功进入网络以后，零信任架构也将阻止用户漫游到未经授权的区域。零信任思维从根本上降低了外部（互联网可发现）和内部（内部威胁）攻击面。

（4）减少违规行为的影响

零信任架构中，用户只能按需获得有限访问权限，有助于限制违规操作、业务中断、安全漏洞等的危害范围和危害后果，降低了补救成本。

（5）缩减安全管理成本和潜在建设成本

零信任架构终结了安全防护手段各自为政的现状，在零信任架构实施时，可以通过与现有工具的集成，大幅度降低零信任潜在建设成本；零信任的“无边界信任”思想减少了 VPN 的使用，简化了运营模式，缩减了安全管理成本。

3. 典型案例

零信任架构基于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，并根据信任的程度对权限进行动态调整，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。针对远程移动办公场景，基于零信任架构的安全参考架构如下图:

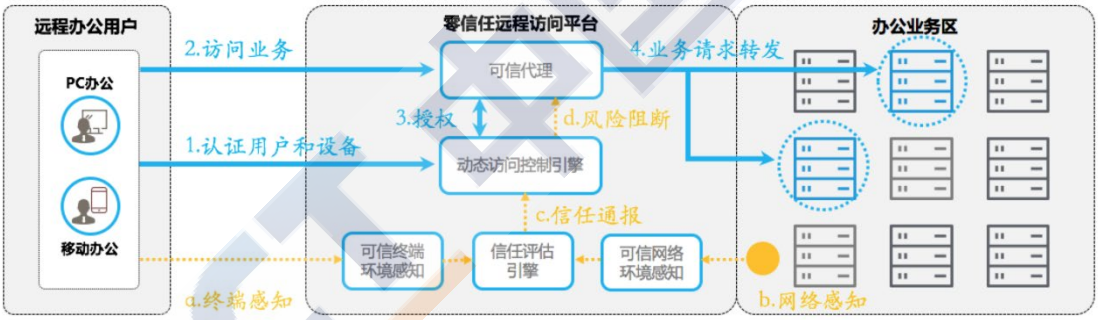

图 3 基于零信任架构的远程办公安全参考架构

（二）大数据中心

数字经济时代，数据是推动经济社会发展的必要生产要素，作为数据集中承载的数据中心，其重要性日益凸显。面对新基建的历史机遇，随着 5G 网络、人工智能、工业互联网等产业的成熟，移动互联网、物联网、工业互联网、车联网等新型应用场景的持续推广带来数据指数级增长，海量数据进入数据中心进行集中存储和处理，对以数

据中心为代表的计算基础设施提出了更高的要求。特别在新冠肺炎疫情防控中，各大城市的科技防疫、远程办公、远程教育和电商消费都离不开大数据中心的支撑，未来，随着社会对于数据处理能力的需求急剧增长，经济社会与人们日常生活将越来越依赖于大数据中心安全、稳定的运行。

1.应用场景分析

大数据中心业务上要求数据集中与共享，一方面实现了多部门、多平台、多业务的数据融合；另一方面在数据中心内部打破了业务之间、部门之间的网络边界，实现互通互访。

大数据中心在实现数据的集中存储与融合的同时，也将集中更多的风险，从而使其更容易成为攻击的目标。大数据中心面临以下安全挑战：

（1）针对高价值数据边界的猛烈攻击

攻击者大量利用弱口令、口令爆破等惯用伎俩，在登录过程中突破企业边界、在传输过程中截获或伪造登录凭证。大型组织甚至国家发起的 APT[39]高级攻击，还可以绕过或攻破数据中心的访问权限边界，在数据中心内部进行横向访问。

（2）内部员工对数据的恶意窃取

在非授权访问、员工无意犯错等情况下，“合法用户”非法访问特定的业务和数据资源后，造成数据中心内部数据泄漏，甚至可能发

[39] APT：Advanced Persistent Threat，高级持续性威胁

生内部员工“获取”管理员权限，导致更大范围、更高级别的数据中心灾难性事故。

2. 先进性和创新性

目前大数据中心访问中东西向（内部）流量大幅度增加，而传统的安全产品基本都是在南北向业务模型的基础上进行研发设计的，在大数据中心内部部署使用时，出现诸如部署困难、运算开销太高，策略管理不灵活等问题。零信任架构通过微隔离技术，实现环境隔离、域间隔离、端到端隔离，根据环境变化自动调整策略，具有以下先进性和创新性：

（1）精细化隔离的网络安全策略

零信任通过关闭网络中的无用服务，消减网络结构(例如，不再采用 VLAN[40]、子网、区域或 IP 地址等管理方式)，改进策略创建过程，在不同等级的网络区域边界设置访问控制规则，建立扁平化的网络管理，真正实现精细化部署。

（2）以身份为基石的逻辑边界

零信任将用户、设备和应用程序组合作为访问主体，对访问主体进行身份鉴别和安全监测，并将其作为访问控制信任基础，保证身份可信、设备可信。同时，将访问主体到大数据中心内部资源的连接进行隔离，建立细粒度访问权限控制，防止访问主体越权访问。

[40] VLAN：Virtual Local Area Network，虚拟局域网

（3）安全策略自适应调整

基于业务之间的访问逻辑，快速发现内部不合规访问流量，为安全策略的调整提供决策依据。当数据中心发生变化时，通过策略分析引擎的计算，快速自动配置安全策略，加速安全工作流程，减少人为错误风险。

3. 典型案例

（1）内部隔离

数据中心应用资源和数据资源采用设备应用沙箱隔离模式部署，通过分配虚拟机隔离或者使用内部防火墙设置隔离区域，对外服务接口采用特殊应用或者 API[41]服务实现对接。

数据中心内部隔离服务访问流程如下图所示：

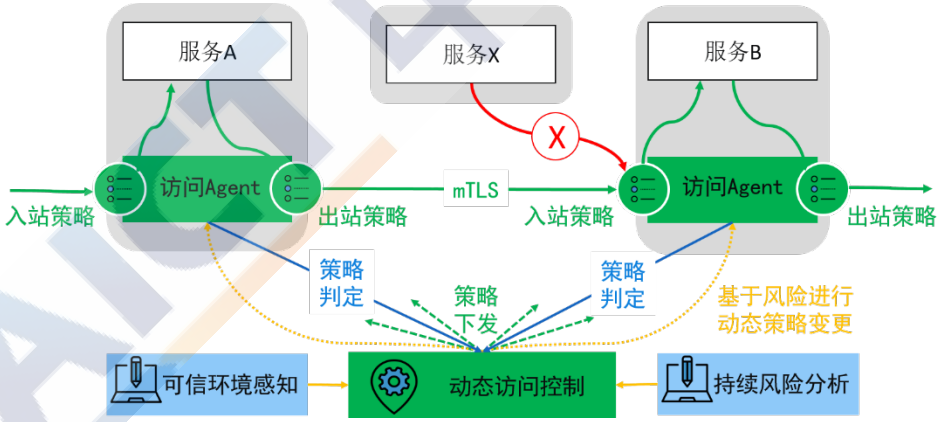

图 4 数据中心内部访问流程示意图

（2）设置安全接入区

数据中心外部设置安全接入区，所有用户接入、终端接入、API 调用都通过安全接入区访问数据中心，实现内部、外部用户和应用对

[41] API：Application Programming Interface，应用程序接口

于数据中心 API 服务的安全接入，并且可根据访问主体实现细粒度的访问授权。在访问过程中，可基于用户环境的风险状态动态调整授权，以持续保障数据访问的安全性。

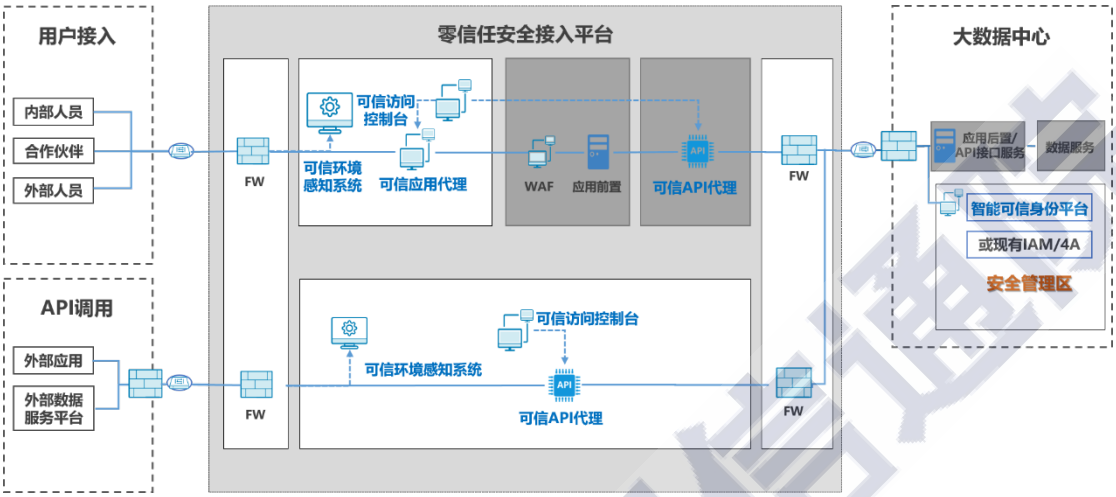

图 5 数据中心安全接入区案例示意图

（三）云计算平台

云计算以按需自助服务、泛在接入、资源池化、快速伸缩性与服务可计量为特征，同时，云计算作为基础支撑平台，参与角色复杂，包括云服务商、云服务客户、云审计者、云代理者和云基础网络运营者等。在过去十年，随着云计算技术的快速发展，云的形态也在不断演进。云计算快速发展带来“云边协同”、“云网融合”等云计算硬件和网络体系的结构重组，以容器、微服务、DevOps[42]为代表的云原生技术成为主流支撑技术。云平台特定技术引入的管理短板和技术瓶颈，使云平台面临极大安全威胁，成为发生网络攻击的重灾区。

1. 应用场景分析

[42] DevOps：Development & Operations，过程、方法与系统的统称

云计算技术的快速发展带来了云平台的大量部署、应用和数据的大量迁移，在庞大复杂的云环境下，如何保证云系统资源安全，保证云服务提供商为云消费者提供安全诚信的服务，同时阻止非法用户对云资源的访问，成为云安全亟需解决的问题。云平台面临以下安全问题的挑战:

（1）云管理服务的安全性要求

未严格满足云管理服务的安全性要求会导致系统性风险。为保障云服务的安全性和可用性，通常云服务提供商会提供一组软件用户界面或 API，供客户用来管理云服务，实际使用过程中由于客户能力不足、意识不强等各种原因，这些安全功能往往形同虚设。此外，客户可能直接将应用程序转移到云中，云应用程序和影子程序共存情况下也会开放新的访问通道。

（2）共享技术漏洞带来的威胁

支持云服务基础设施的基本组件隔离程度不足，多租户架构或多客户应用的情况下，不同企业的系统彼此相邻，并且可以访问共享内存和资源，从而为攻击者创建了新的暴露面。

（3）云平台开源代码自身风险

云计算技术借助开源技术取得巨大发展的同时，也面临极大威胁。开源代码自身的开放性，也给了不法分子机会，例如针对容器基础设施的攻击在加速，不断有容器漏洞被利用的情况出现。

2. 先进性和创新性

云计算逐渐进入到重新定义服务模式的发展路径，专为云计算模型开发的云原生技术，涵盖一系列云计算技术体系和管理方法，可帮助用户快速将应用构建和部署到与硬件解耦的平台上。企业部署在云上的应用具备更高的敏捷性、弹性和云间的可移植性，广泛支持包括Kubernetes[43]、OpenShift[44]、Docker EE[45]、OpenStack[46]和裸金属服务等平台。随着越来越多的公有云上服务组件被使用，SaaS[47]安全也变得越来越重要，其中，用户最关注服务的身份认证、访问控制以及数据保护。在云计算中实施零信任访问控制，采用适配云计算平台、工作负载的技术，确保只有经过动态授权的工作负载才能运行、交互或进行数据访问。具有以下的先进性和创新性:

（1）实施细粒度的访问控制

零信任采用适用于虚拟机、容器、微服务等云平台组件的微分段策略，将网络策略和身份策略相结合，只允许数据在许可的系统和连接之间流动，并在不断变换的云环境进行更新时保持细粒度的访问控制。其中微分段策略不受虚拟、动态资产的物理位置限制。

（2）面向微服务的隔离机制

零信任基于微服务管理平台所提供的连接、安全、控制和观测模

[43] Kubernetes：一个开源的，用于管理云平台中多个主机上的容器化的应用
[44] OpenShift：红帽公司面向开源开发人员开放的平台即服务
[45] Docker EE：Docker enterprise edition，Docker 企业版本，Docker 是一个开源的应用容器引擎
[46] OpenStack：一个开源的云计算管理平台项目，是一系列软件开源项目的组合
[47] SaaS：Software-as-a-Service，软件即服务

块，实现应用程序或服务隔离，帮助开发人员聚焦核心的业务逻辑，实施流量监控、负载匹配、访问控制和审计。

（3）“先认证后连接”的微服务

通过基于身份的验证和授权，对微服务间的访问进行鉴权，取得授权后在全链路采用双向 mTLS[48]进行加密，在集群中实现安全的服务间通信，通过自适应的访问控制来执行最小化的访问控制策略。

3. 典型案例

网络安全形势日渐严峻的同时，企业内部使用的微服务、容器编排和云计算资源池等技术架构导致云计算环境也越来越复杂。在此背景下，企业可通过梳理云平台内部资源，建立微隔离机制（参照“大数据中心”应用场景），实现零信任安全架构。在通过分析内部人员访问路径、外部人员访问通道、外部应用调用、外部数据服务平台对接通道等确定其暴露面后，可部署相应访问代理，在可信访问控制台的控制下，基于微服务管理平台等建立动态的虚拟身份边界，并通过计算环境感知等安全信息分析平台数据，建立最小权限动态访问控制体系。

[48] mTLS：Mutual Transport Layer Security，双向安全传输层协议

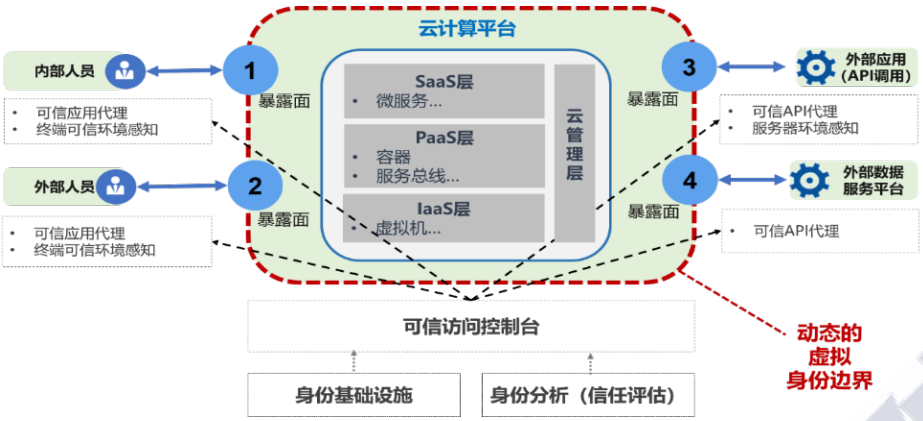

图 6 基于零信任架构的云计算平台安全参考架构

（四）物联网

万物互联时代，5G、大数据、人工智能等新技术为物联网带来了创新活力，催生了智能家居、智慧车联、个人智能穿戴等新兴应用领域，衍生出繁荣多样的物联网业务，同时，物联网可以提供先前设备缺少的数据存储、网络连接以及计算功能，赋予设备新的效率和技术能力。在物联网越来越普及的同时，网络安全问题也甚嚣尘上。

1. 应用场景分析

物联网呈现出与传统网络不同的特性，其中海量多样化的物联网设备入网方式和自身弱点都带来无法忽视的系统风险。连接物联网的终端普遍存在自我保护能力弱，极易遭受攻击者恶意破坏的特点，在物联网发展如火如荼的同时，网络安全问题也逐步暴露出来。研究显示，利用木马、僵尸等手段针对物联网发动攻击的技术已经非常成熟，数以万亿感染的物联网终端，将会给智能家居、智能制造、智慧城市、工业互联网等物联网应用场景带来极大的风险。物联网面临以下安全问题的挑战：

（1）泛终端自身的安全短板

研究报告显示，攻击者越来越多地利用智能家居传感器、智能手机、路由器上的各种漏洞将其作为新的攻击媒介，物联网终端已经成为事实上的攻击“跳板”，将安全威胁带入全网。根据银行业的最新安全警报，出现通过生物识别终端，发动对金融机构供应链攻击的案例，泛终端自身漏洞导致的安全风险防不胜防。

（2）多样化终端接入管理困难

随着物联网的广泛使用，物联网设备快速兴起，传统的哑终端、非智能终端也开始向智能终端靠拢。数量众多、类型多样、不同接入方式的泛终端，既需要传统的网络准入控制、企业资源管理等产品对办公终端进行接入管理，也需要统一终端管理等产品对移动端和服务器进行接入资产管理。同时，对于物联终端，尤其是在传统 PC 终端、移动端混合接入的场景下，还面临接入认证和管理的难题。

（3）物联终端攻击易于成功

物联网终端采用多样化接入技术，包括 2G[49]/3G[50]/4G[51]/5G、WiFi[52]、蓝牙、Zigbee[53]、LoRa[54]、NB-IoT[55]等，在云网融合背景下，5G 物联网装置绕过了中央路由器直接接入 5G 网络云端。由于物联

[49] 2G：The Second Generation Mobile Communication Technology，第二代移动通信技术
[50] 3G：The Third Generation Mobile Communication Technology，第三代移动通信技术，与第一代移动通信技术（1G）与第二代数字手机通信技术（2G）相比，3G 主要是将无线通信和国际互联网等通信技术全面结合，形成一种全新的移动通信系统
[51] 4G：The 4th Generation Mobile Communication Technology，第四代移动通信技术，将 WLAN 技术和 3G 通信技术进行了很好的结合
[52] WiFi：无线上网，将电子终端以无线方式互相连接
[53] ZigBee：一种低速短距离传输的无线网上协议
[54] LoRa：Semtech 公司创建的低功耗局域网无线标准
[55] NB-IoT：Narrow Band Internet of Things，窄带物联网

网终端具有数量巨大、安全防护能力较弱等特性，在安全管控措施不到位的情况下，高级攻击者利用设备的脆弱性，从内部攻击服务平台，将更容易获得成功。

2. 解决思路

随着边缘计算技术的不断完善，边缘计算在本地执行计算和分析的思想也越来越被接受，云边协同成为新的基础架构，极大地满足物联网大部分场景在敏捷连接、实时业务、数据优化、安全与隐私等方面的计算需求。在物联网实施零信任架构，可借助边缘计算技术，解决终端的身份认证和访问控制，允许身份可信、经过动态授权的物联设备入网，并动态监测，及时发现并处置假冒、伪造的非法连接。

（1）部署边缘物联接入管理设备

在物联设备接入侧部署边缘物联接入管理设备，接管物联设备的身份管理、权限分配、接入控制等接入管理功能，物联接入管理设备和数据中心联动，在网络边缘处协同使用计算、连接、存储能力，及时处理物联设备相关请求，控制安全风险范围。

（2）建立物联设备标识管理机制

面对物联终端主要存在的终端设备仿冒、用户身份仿冒问题，根据物联终端各自不同的特性，可以采用不同的身份标识实施身份鉴别。高可信设备采用可信芯片+可信 OS[56]，直接标识身份；嵌入式设备采

[56] OS：Operating System，操作系统

用设备标签，如移动设备识别码（IMEI[57]）、应用开发商标识符（IDFA[58]）、唯一设备标识码（UDID[59]）等，以及设备外贴 RFID[60]电子标签、密码模组等，都可以帮助建立设备身份标识；对于智能程度较低的物联设备，也可以采用设备数字指纹的方式来构建设备标识，解决设备入网身份管理问题。

（3）建立物联设备安全基线库

采用灵活的方式，对物联设备建立安全基线。在物联设备标识管理基础上，综合获取物联设备信息，包括操作系统类别、操作系统版本、涉及敏感数据的 App 特征、业务访问记录、行为特征等，运用人工智能深度学习等技术手段，建立安全基线库，帮助快速精准判断设备运行环境是否正常，及时发现被“攻陷”设备。

3. 典型案例

零信任身份指纹的解决方案，借助边缘物联代理，已进入关键技术突破和实验验证阶段。其核心指导思想是对物联设备建立身份指纹，由主体属性（包括：MAC[61]地址、操作系统、端口、协议、服务、厂商）、环境属性（包括：上线时间、IP、接入位置、业务流量大小）和客体属性（包括：所属部门、管理人员、授权时间、授权级别）构成，通过持续主动扫描、被动监听检测、安全接入控制区等方式，对物联终端进行持续信任评估、访问控制，解决物联终端的身份仿冒和恶意

[57] IMEI：International Mobile Equipment Identity，国际移动设备识别码
[58] IDFA：Identifier for Advertisers，苹果公司独有的广告标识符
[59] UDID：Unique Device Identifier，唯一设备识别符
[60] RFID：Radio Frequency Identification，射频识别
[61] MAC 地址：Media Access Control Address，在网络中唯一标识一个网卡

访问。

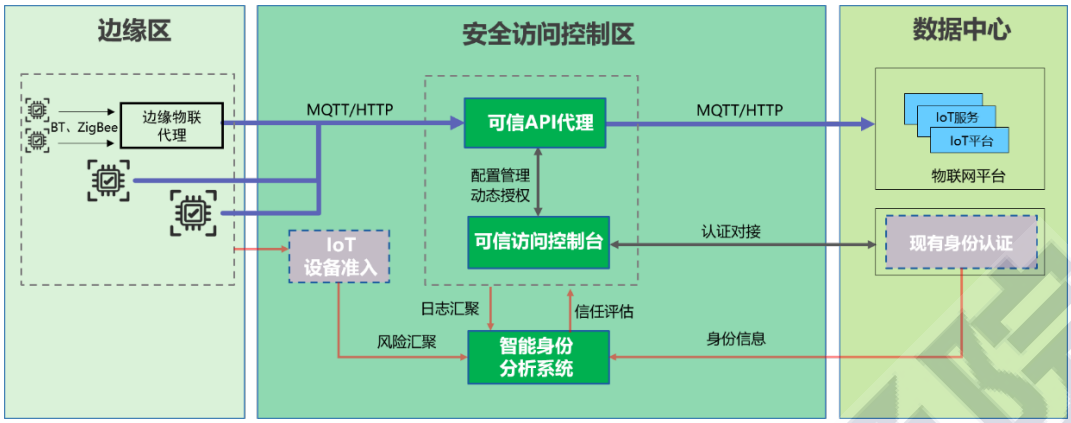

图 7 基于设备指纹的物联边缘网关零信任方案示意图

（五）5G 应用

在 Gartner 行业报告《市场报告：通信服务提供商应对 5G 安全挑战的策略》[62]中，把纵深防御、持续性和自适应以及零信任安全列为 5G 安全战略的三大支柱。可以预见，零信任作为解决 5G 安全的战略思维，未来将开展实践探索。

1. 5G 应用安全风险分析

5G 将多样化的应用统一到了一个网络中，并且凭借网络切片和边缘计算技术实现网络的划分和对应用的支撑，但是安全需求仍然呈现多样化的特点。5G 网络从云、管、边、端多维度引进了安全风险，同时，2G/3G/4G 的一些应用风险在 5G 中仍然存在。基于 5G 应用架构，对 5G 应用进行安全风险分析和梳理。

（1）按照网络侧和用户端梳理 5G 架构下的主要对象，如下表所示：

[62] Gartenr，Market Report：Strategies Communications Service Providers Can Use To Address Key 5G Security Challenges

表 2 5G 架构下的主要对象

网络侧	用户端
无线接入网 核心网络 多址边缘计算（移动边缘网关） 物理基础设施 虚拟化设备 ……	用户设备 用户/设备标识 用户会话 应用程序数据—存储中、网络上、内存中 API 接口 ……

（2）按照内部和外部梳理 5G 架构面对的风险来源，如下表所示：

表 3 5G 架构下的风险来源

内部	外部
超级管理员 内部特权用户 用户-有意违规 用户-意外失误 ……	国家背景的攻击者 网络罪犯 职业骇客 竞争对手 前授权用户 ……

（3）对 5G 架构下的攻击情况进行梳理，如下表所示：

表 4 5G 架构下的攻击情况

和 4G 情况相同	5G 新增情况
假冒接入的网络节点 IMSI[63]捕捉 会话劫持 网络间信令欺诈 滥用合法拦截 滥用远程访问 ……	流氓云服务提供商滥用 SDN 中的内存残留泄露 绕过网络虚拟化攻击 边缘网关伪造 边缘网关越权 （边缘）API 非受控开发 核心网络中的横向访问 ……

典型的攻击案例列表如下：

[63] IMSI：International Mobile Subscriber Identity，国际移动用户识别码

表 5 5G 典型攻击行为案例

攻击者	攻击方式	攻击性质	操作
网络罪犯	伪造接入网络节点	机密性、完整性	伪装成合法的流氓基站，允许中间人攻击（MitM[64]）。
边缘网关的内部越权管理员	数据过滤	机密性	有权访问 MEC[65]节点的恶意管理员可以复制敏感数据并将其发送到其他地方。
职业黑客	边缘计算开放 API 的滥用	机密性、可用性	黑客利用云平台对边缘计算开放 API 服务的漏洞，包括用于身份验证的联盟服务等。
核心网络层的越权管理员	恶意网络功能注册	机密性	由内部人员或供应商/服务提供商设置并注册未经授权的网络功能（NFC[66]）或嵌入特洛伊木马的功能。

通过系列梳理，可以看到，在 5G 网络的复杂条件下，尽管对象千差万别，但是对 5G 应用的安全威胁还是集中在对数据的机密性、完整性、可用性、防抵赖性攻击以及对于应用资源和服务的身份授权等方向，由于 5G 应用表现形式的不同，所采用的资源保护方式也有所不同。

2. 基于零信任的 5G 应用风险消减思路

5G 应用面临的安全挑战主要源于开放的 5G 架构下，攻击面大大增加；同时，5G 网络作为新型基础设施，重要性不言而喻。但是 5G 应用安全建设一直滞后于 5G 业务建设，给 5G 整体安全带来极大的隐患。梳理影响 5G 应用安全的关键技术要素如下:

- 获取 5G 网络中用户的唯一永久身份标志（SUPI[67]）加密后

[64] MitM：Man-in-the-MiddleAttack，中间人攻击。作为“间接”入侵攻击，通过技术手段将受入侵者控制的计算机虚拟放置具有网络连接关系的两台计算机之间，这台受控计算机被称为“中间人”

[65] MEC：Mobile Edge Computing，移动边缘计算。一种基于 5G 架构将移动接入网与互联网业务深度融合的技术

[66] NFC：Near Field Communication，近场通信。使用 NFC 技术的设备（如手机）可在彼此靠近的情况下进行数据交换

[67] SUPI：SUbscription Permanent Identifier，是 5G 网络中用户的唯一永久身份标志

的隐藏标识符（SUCI）

- 更新后的身份验证和密钥协议（AKA）
- 增强完整性的无线接入网数据
- 增强密码算法
- 增强网间连接安全性
- 增强家庭网络安全控制
- 基于用户设备数据的虚假基站检测

结合 5G 应用架构和零信任体系架构方法，可以很有针对性地采取 5G 风险消减的办法:

（1）建立 5G 统一的身份管理机制

5G 网络与应用是一个庞大的生态，涉及设备商、运营商、平台商、安全商、用户单位及个人等诸多安全主体。3GPP[68]标准框架提出了如 SUCI[69]、AKA[70]等安全标识与认证机制，基于 5G 网络中用户的 SUPI 加密后的 SUCI、AKA 在云端或核心网数据中心建设身份安全管理平台，实现统一的多角色/可扩展的身份管理、强身份验证和端点保护、认证管理，以及设备和（虚拟）网络的认证和合规性。

（2）实现细粒度用户访问控制

5G 网络层和应用层的分割和隔离易于实现。软件定义是 5G 网络核心技术，通过软件定义，实现安全的企业虚拟组网，使得企业可

[68] 3GPP：3rd Generation Partnership Project，《第三代合作伙伴计划》，多个电信标准化组织共同在 1998 年 12 月签署。最初的工作范围是为第三代移动通信系统制定全球适用的技术规范和技术报告，现调整为对无线和网络标准长期演进的系统研究和标准制定。目前成员单位包括欧洲的 ETSI、美国的 ATIS、日本的 TTC、ARIB、韩国的 TTA、印度的 TSDSI 以及我国的 CCSA

[69] SUCI：SUbscription Concealed Identifier，是 SUPI 通过公钥加密后的密文，放置在核心网

[70] AKA：Authentication and Key Agreement，第三代移动通讯网络的认证与密钥协商协议

以在 5G 基础设施上灵活方便地建设和改进自己的分支组网架构，实现动态网络安全域的划分和隔离防护。在 5G 边缘云上部署的安全能力，需建设动态调度、弹性扩展的虚拟接入网络，在边缘侧构建感知、分析、执行的闭环，实现细粒度安全管控。

（3）访问控制策略自动化配置

5G 安全需求的多样化和定制化要求能够快速建立和修改安全能力，并分布式部署安全部件；组件在基础架构内自适应调整配置，与信息系统聚合提升协同能力；在统一身份管理机制上，实现安全策略自动化配置和动态访问控制，最终实现智能主动防御。

三、零信任实施建议

（一）使用范围

1. 是否需要零信任

目前，企业与组织等的信息化系统正在面临来自多方面严峻的安全挑战。业务系统面临着多种类型的终端设备接入，包括手机、台式机、平板电脑及各类终端；组织的网络环境愈发多样，包括 3G、4G、5G 等移动网络、固定网络接入、虚拟化网络等；访问业务系统协同工作的人员类型激增，包括办公场所固定办公员工、移动办公员工、外协组织及安保企业等短期员工、供应商及运维服务商等合作组织员工、实习员工、离职员工等；外部威胁防护安全需求大幅增加，包括利用僵木蠕发动的各类攻击行为、伪造和假冒身份攻击、社会学攻击等；内部风险演化的安全困局日益严重，包括恶意用户横向窃取、普

通用户违规操作、被劫持用户恶意操作等；需要满足的法律法规、标准规范的合规性要求愈发严格。

严峻的安全态势和数字化转型浪潮下的新安全需求促使身份与访问控制成为信息系统架构安全的第一道关口，零信任安全正是拥抱了这种技术趋势，让企业在无法基于传统的物理边界构筑安全基础设施时，有了新的安全选择。

通常，企业与组织等零信任的未来使用者在决定是否将零信任安全架构列入信息化建设规划时，至少需要考虑以下几点：

- 采用零信任架构，是否可以在一定时间范围内解决已存在的安全现实问题和发现未知的安全威胁？
- 采用零信任架构，是否可以在未来一定时间范围为信息化系统的发展持续提供安全保障？
- 采用零信任架构，是否可以顺畅对接现有安全投资，在此基础上还需要多大的持续安全投入？
- 采用零信任架构，是否可以满足上级机构和国家对于信息化系统的安全检查要求？

零信任架构的核心就是重构访问控制，采用更灵活的技术手段对动态变化的人、终端、系统建立新的逻辑边界。通过对人、终端和系统进行识别、访问控制、跟踪实现全面的身份化，这样身份就成为了网络安全新的边界。基于身份建立的零信任架构具有动态化、开放化的特点，其能对接信息化系统原有的身份基础设施、各种安全分析平台，持续发挥原有安全投资效益，同时通过动态化的系统维护，实现

对未来信息化系统的持续保障；零信任架构的动态化和开放性还体现在以自适应的方式对未知安全威胁的发现和快速响应，在一定程度上减少用户的持续投入。零信任架构同时具备细粒度的访问控制、动态的安全策略，可以很好地满足各种安全标准规范的要求，实现系统合规。

零信任安全架构将为现在和未来的信息化系统建设提供更好的安全、隐私、性能和可用性。通过审视零信任架构可以解决的问题，以及零信任架构的兼容性、成长性等，信息化系统的管理者们可以对是否引入零信任架构形成初步判断。

2.正确的零信任思维

在确定零信任架构方案之前，还需要树立正确的零信任思维。

“零信任”并不意味着“零访问”。它的意思是“安全访问”所需的资源（网络、数据、系统、应用程序、业务等），并基于应用情况的评估，通过分配“恰如其分”的用户权限来限制资源访问风险。与传统安全思维对比，不再追求越强越好的认证手段、粒度越细越好的访问控制、越明确越好的身份管理策略。一刀切的安全手段会极大的影响信息系统的易用性和可用性。在正确的零信任思维下，没有绝对的安全，也就没有绝对的信任。

对认证手段的评估：在认证手段上，零信任安全并不要求必须在各种场景下都一视同仁的采用强认证的手段，而是同时支持可选的多种认证手段，并且将认证手段的强弱作为一个信任度量因子，认证手

段的强弱直接影响主体的信任度，影响后续的访问控制判定。比如，终端具备 TPM[71]、使用了人脸识别可以得到一个较高的信任评分，反之，用户如果只使用了用户名口令进行登录，那只能得到一个较低的信任评分，信任评分太低将禁止访问某些安全等级高的业务。

动态访问控制: 零信任安全架构下的访问控制基于持续度量的思想，是一种微观判定逻辑。对主体的信任度、客体的安全等级和环境的风险进行持续评估并动态判定是否允许当前访问请求。

渐进式身份管理: 访问控制需要身份治理和授权策略的管理作为基础支撑。现代企业内部存在着内部员工、客户、合作机构、外包人员等不同的身份，零信任架构并不寄希望于以一套大一统的管理逻辑和流程囊括万千，而是对不同的身份进行分类分析和梳理，制定不同的身份生命周期管理流程。例如：对内部员工，通过和企业的目录服务器、HR[72]服务系统等现有身份源系统进行数据同步，统一建立员工数字身份；而对于客户，因为其具备未知性和动态性，则按照统一标准，逐步纳入管理范围。

零信任架构以安全与易用平衡的持续认证改进固化的一次性强认证手段，以基于风险和信任度量的动态授权逻辑替代简单的二值判定逻辑，以开放智能的身份治理优化封闭僵化的身份管理。通过有效的信任和风险评估，支撑持续进化的访问控制，在实践中发现规律，从而得到相对稳定的安全态势。

[71] TPM：Trusted Platform Module，可信平台模块，一种植于计算机内部为计算机提供可信根的芯片
[72] HR：Human Resource，人力资源管理，又称人事管理

（二）实施规划

零信任安全架构不是单一的网络体系结构，而是一整套网络基础设施设计和运行的指导原则，可以用来提升网络安全整体能力。零信任实施的规划过程，就是谋求逐步实现零信任原则、流程更改以及保护其数据资产和业务功能的解决方案。

1.零信任实施关键“时刻”

零信任安全是一种架构理念，因此，企业何时、如何实施零信任安全并无放之四海而皆准的金科玉律。但是，结合信息化系统建设经验和零信任战略实施情况，企业引入零信任安全的最佳时机是和企业数字化转型进程保持相同的步伐。将零信任安全作为企业数字化转型战略的一部分，在企业进行云迁移战略或建设大数据平台的时候同步规划实施，必然会事半功倍。

现在许多企业的网络基础设施中已经有了零信任安全的元素，但是，过渡到零信任安全的历程不可避免地伴随着大规模的技术替代。对于尚无基础设施转型计划的企业来说，实施部分零信任安全实践也未尝不可，企业遵循零信任安全基本理念，结合现状，以零信任/遗留模式混合运行，同时继续致力于正在进行的 IT 现代化革新和改进组织业务流程，逐步规划实施零信任，当企业完成数字化转型之时，零信任安全也就水到渠成了。

2.零信任实施关键“人物”

零信任的建设和运营需要企业各干系方积极参与，直接涉及到安

全部门、业务开发部门、IT 技术服务部门和 IT 运营部门等，牵头者通常是安全部门或者信息化部门。需要特别注意的是，很多情况下企业安全部门话语权并不高，安全项目往往受到业务部门的阻碍甚至反对，而零信任实施的最佳时机是与业务同步规划、同步建设，因此，零信任项目的发起者需要从零信任的业务价值出发，说服业务部门和企业的高层决策者。如果企业数字化转型的关键决策者将基于零信任的新一代安全架构上升到战略层面，指派具有足够权限的负责人，如 CIO[73]/CSO[74]或 CISO[75]级别的负责人进行整体推进，零信任实施会事半功倍。

在零信任推进过程中，建议成立专门的组织（或虚拟组织），在负责人的领导下进行零信任迁移工作的整体推进。吸纳关键领域负责人，包括安全、身份、网络、访问控制、客户端和服务器平台软件、关键业务应用程序，以及任何第三方合作伙伴或 IT 外包等各类技术的管理负责人，实现多部门之间的配合和支持，减少对业务部门的冲击。

零信任项目的实施最终将影响到企业大部分的员工，因此，得到普通员工的支持也是项目成功的关键。有效的沟通、尽可能少的影响员工工作，将有助于取得相关人员的理解和支持。

3. 零信任实施优先级

[73] CIO：Chief Information Officer，首席信息官或信息主管，属于公司的最高决策层，主要负责制定公司的信息政策、标准、程序的方法，并对全公司的信息资源进行管理和控制

[74] CSO：Chief Solution Officer，首席问题官，企业里负责挖掘问题、协调缓解问题和解决问题的高级管理人员

[75] CISO：Chief information security officer，首席信息安全官，隶属于 CIO，对企业信息安全进行评估

基于安全持续演进的零信任思维，零信任实施前需要基于业务需求、安全运营现状、技术发展趋势等，进行持续演进的技术规划。考虑未来移动设备和应用程序激增、云服务采用、社交媒体使用和第三方依赖性等扩展性问题，在规划之初需确定零信任安全架构与企业资源对接的优先级。

企业的资源和数据对接零信任架构，可以从两个维度进行安全规划梳理和评估：一是能力成熟度，二是业务范围。企业需要评估当前具备的安全能力，并基于风险、安全预算、合规要求等信息，确定安全能力建设的优先级。

- 能力优先型：针对少量的业务构建从低到高的能力，通过局部业务场景验证零信任的完整能力，然后逐步迁移更多的业务，扩大业务范围；
- 范围优先型：先在一个适中的能力维度上，迁移尽量多的业务，然后再逐步对能力进行提升。

零信任架构最终需要覆盖企业的所有资源，在规划阶段，按照需求迫切度、能力完善程度进行组合，确定迁移至零信任的业务优先级。一般来说，建议将新建业务和核心业务作为第一优先级考虑。对于大多数企业，在零信任/遗留模式混合运行状态下，企业向零信任方法的迁移，也可以采取一次迁移一个业务流程的方式。在规划中，企业需要确保公共元素（例如身份凭证管理、设备管理、事件日志等）足够灵活，从而支持零信任在遗留混合安全架构中运行。

（三）技术实现

综合考虑组织目标、组织架构、网络和应用现状等因素，参考零信任实施技术路线（如下图所示），可制定差异化的、场景式的解决方案，并推动其落地实施。

图 8 零信任实施技术路线示意图

零信任工程实践，通常可按照实施准备、部署连通、调测运行等三个阶段展开:

1. 零信任实施准备

在实施准备阶段，按照零信任规划明确的任务目标，确定保护目标、识别业务暴露面等，准备阶段可以通过人工登记，或者零信任系统工具辅助实施。

（1）识别系统资产，明确资产清单

基于对接零信任架构的业务系统目标范围，识别企业的资源和数据资产，了解何人、何物、何时、何地、为什么以及如何使用企业的资源和数据资产。参考零信任实施规划，充分考虑目前实现方案的现实情况和未来规划，确定保护目标，建立零信任实施清单。零信任实

施清单将覆盖以下多个方向的内容：零信任架构需要对接的基础数据如人员、帐户、设备清单；零信任架构需要改造的应用系统和需要保护的数据资产清单；零信任架构部署的网络环境，等等。

（2）梳理访问全路径，确定业务暴露面

分析零信任体系中所有内部和外部流量；分析工作流的流动方式以及主体对象访问客体对象的方式；利用现有应用访问和业务流程资料，定位并映射所有相关网络和系统对象；结合资源保护方案的现实情况和未来规划，围绕保护对象的保护模型，确定业务暴露面。

（3）制定零信任组件配置、实施方案

针对业务暴露面，设计零信任网络架构，限制并严格执行保护目标的保护模型，验证所有资源身份，制定强制执行访问控制和检查策略方案，构筑资源保护面。建议主要围绕以下四个方向进行方案设计：围绕核心资产构建保护面；通过物理或虚拟安全控制实施保护；定义可实施的跨区域、用户和设备的访问策略；定义最小化访问控制权限，严格执行细粒度授权原则，等等。

需要特别强调的是，梳理访问权限将建立访问权限基线，同时需确保梳理过程不影响现有业务的正常访问。

（4）梳理实施方案，确定建设步骤

对实施的工作量、难易程度和工作进度等进行充分评估，确定建设步骤。优先建设零信任基础架构，进行最小化部署，然后按照能力

叠加原则，逐步建设。

2.零信任部署连通

在部署阶段，按照实施准备阶段制定的实施方案，分别进行部署连通，并且与外部的身份安全基础设施和其他安全分析平台进行对接。

（1）零信任网络改造和组件部署

按照控制平面和数据平面分离的原则，基于零信任实施准备阶段梳理的资源保护对象清单，调整网络拓扑，划分零信任网络分区，确定各个区域的访问策略。

构建数据平面访问通道，建立用户访问资源、应用访问资源、资源互访的数据通道；构建资源保护最小化隔离区域，支持对资源进行最小权限访问；部署策略执行和策略决策组件。

（2）连接身份安全基础设施，支持用户身份管理

身份基础设施可以依托企业的 4A、IAM、AD、LDAP、PKI 等基础设施，也可以是来自企业的业务系统。作为零信任架构的支撑组件，身份基础设施还有可能需要连接支持数字证书，提供生物特征、电子凭证等多模式身份鉴别。随着企业规模的发展，企业人员、设备、权限都非常庞大，应满足复杂 IT 环境下高效管理要求。该部分有可能依托零信任架构新建或者重建，通过部署统一身份认证平台，进行帐号的统一管理与单点登录，并实现权限管理与多因素认证等安全能力。

（3）对接信任评估安全数据，支持持续信任评估

零信任的持续动态评估应充分利用现有安全平台建设成果。通过其他安全分析平台，包括安全事件管理系统、威胁情报系统、预警监测系统、终端防护系统等，为零信任提供资产状态、规范性要求、运行环境安全风险、威胁情报等数据，从而帮助零信任开展持续动态评估。

（4）建立动态访问控制机制

零信任架构连通控制平面和数据平面，基于数据平面的访问会话，对所有访问请求建立访问控制策略。基于安全策略和基础信任等级，建立访问控制基础权限；根据安全上下文，最小化访问控制原则，持续开展信任评估，动态调整访问权限；严格执行动态访问控制策略，对无访问权限的访问请求进行阻断。

3. 零信任调测运行

完成零信任组件部署以及与环境联调以后，进行零信任架构调测运行。在基础功能稳定一段时间以后，扩大应用和安全组件对接范围，逐步实现零信任各项功能。

（1）持续监控评估

持续监控已部署零信任架构体系是否有漏洞或其他恶意活动的迹象，对零信任业务保护面和记录在案的安全策略进行监控，监控现在和未来的安全策略管理和更新，评估零信任安全架构运行状况。建议采用以下方式进行规划：

- 统一管理和更新安全策略运行状况;
- 基于评估工具，进行用户行为分析，发现风险和威胁，调整和完善访问控制策略;
- 建立网络分析、安全可视化和安全用户行为分析等，统计各类资产访问情况和安全风险。

（2）自动化安全编排

安全编排自动化工具，可通过制定自动化策略，了解可用的自动化选项；评估并记录策略执行过程；按照策略进行自动化编排等一系列步骤。鉴于实现这一过程将面临很强的场景化和剧本化要求，技术实现方向还存在一些瓶颈，随着条件的成熟可以逐步实现。

四、零信任思考和展望

零信任作为新型网络安全理念，将资源保护作为核心，融合身份认证、权限控制、实时评估等多种技术，实现细粒度、精准化、自适应的访问控制，有效防范远程接入、大数据中心、云计算平台、物联网、5G 等场景下的内外部安全威胁，引起了产业内外高度关注。然而，零信任理念仍然在技术实现、大众认知、应用推广等方面存在诸多挑战。例如，尚无标准评判零信任解决方案的成熟度；将采购部署零信任产品等同于实现零信任架构；与企业现有网络安全框架兼容并存的问题等。因此要实现零信任架构，仍需要从各方面付出诸多的努力。

国家层面，加强政策技术指引。为更好推动零信任等新技术理念的研究和应用，结合国家新型基础设施建设安全保障需求，建议国家层面和政府层面出台相关政策，引导加大新基建安全保障的资金投入，促进技术手段升级，鼓励开展以零信任为代表的安全技术理念创新、架构创新和应用部署。加快编制适应我国网络建设现状和行业应用实际的零信任安全标准，集合相关企业、科研机构、高校、行业用户等多方角色参与标准规范编制，指导零信任安全架构建设部署。建立零信任产品和解决方案的评估机制，编制网络架构、技术方案、产品能力、部署成效等指标体系，开展技术检测和效果评估，提升零信任安全部署能力。

技术层面，着力解决技术瓶颈。零信任架构理念新、应用场景多、技术要求高，且与网络的基础架构、资源配置、安全管理等密切相关，

应用部署具有一定复杂性。国内安全企业已积极开展零信任布局，但产品和解决方案尚处于起步阶段。需要加大对零信任技术研发，重点研究突破零信任身份管理、信任评估、数据加密等关键技术。同时，还应加快探索面向 5G、物联网等应用场景解决方案并逐步走向成熟。

产业层面，深入开展协作实践。产学研用各方需加强协同合作，推动零信任架构与传统安全架构间的优化、利用、衔接、过渡，推进各平台、各厂家相关安全产品和解决方案的适配。对于 5G 网络、大数据平台等典型场景开展零信任架构应用试点，总结最佳实践，加强产业输出，为后续推广部署奠定基础。

企业层面，有序推动升级部署。长期来看，企业将逐步实现安全体系架构从网络中心化走向身份中心化，达成以身份为中心的访问控制，但这一过程应该是漫长而艰巨的。首先企业需要开展系统全面地资产梳理、业务安全分析，深入研究零信任在企业部署实施的必要性和适应性、部署场景和方案可行性、与现有安全保障框架的兼容性，在保障网络和业务安全稳定运行前提下，分阶段、循序渐进推动系统迁移，完善网络安全保障体系，建立自适应的安全防御能力。

2020 年恰逢“十三五”收官，“十四五”将至，5G、数据中心、物联网、工业互联网、人工智能等新型基础设施的建设大潮火热开启，硬核的新基建要求有相配套的网络安全基础设施以及网络安全保障体系，零信任等新兴网络安全技术面临广阔前景，期待其成为网络安全保障体系升级的中流砥柱。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62305321

传真：010-62300264

网址：www.caict.ac.cn