零信任关键技术与产业发展研究

Key Technologies and Industrial Development of Zero Trust

张云畅/ZHANG Yunchang，柴瑶琳/CHAI Yaolin，
穆琋博/MU Yubo

（中国信息通信研究院，中国 北京100083）
(China Academy of information and Communications Technology, Beijing 100083, China)

DOI：10.12142/ZTETJ.202306010
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20231212.1442.004.html
网络出版日期：2023-12-13
收稿日期：2023-10-16

摘要：零信任架构作为一种网络安全的新理念、新架构、新技术，基于“持续验证，永不信任”的核心思想，通过融合软件定义边界、身份识别与访问管理、微隔离三大技术，将重塑现有网络安全架构和网络安全设施，并深刻改变关键基础设施的部署与应用模式，带来网络安全领域的一场新变革。从零信任演进与技术发展情况入手，分析零信任当前产业发展现状，通过对比全球零信任战略部署、技术革新、产业规划研提中国发展建议。同时剖析中国零信任发展中的问题，研提中国在零信任顶层设计、技术革新发展、产业生态闭环的针对性建议。

关键词：零信任；零信任架构；网络安全战略

Abstract: As a new concept, new architecture, and new technology of network security, zero trust architecture is based on the idea of "continuous verification, never trust". By integrating software-defined borders, identity and access management, and micro-isolation technologies, zero trust architecture will reshape the existing network security architecture and network security facilities, and furthermore, profoundly change the deployment and application method of key infrastructure, leading to a new revolution in the field of network security. The current status of the zero trust industry from the perspective of zero trust evolution and its technological development is analyzed, and the suggestions on further development are provided by comparing global zero trust strategic deployment, technological innovation, and industrial planning. At the same time, the problems in the development of zero trust in China are discussed. Finally, originating from the micro level, targeted suggestions on the top-level design of zero trust, technological innovation and development, and closed-loop industrial ecology are proposed.

Keywords: zero trust; zero trust architecture; cyber security strategy

引用格式：张云畅, 柴瑶琳, 穆琋博. 零信任关键技术与产业发展研究 [J]. 中兴通讯技术, 2023, 29(6): 60-65. DOI: 10.12142/ZTETJ.202306010
Citation：ZHANG Y C, CHAI Y L, MU Y B. Key technologies and industrial development of zero trust [J]. ZTE technology journal, 2023, 29(6): 60-65. DOI: 10.12142/ZTETJ.202306010

网络安全是产业数字化升级中的关键保障。近10年来层出不穷的网络安全问题不仅阻碍了各行业发展，更是减缓了产业革新的速度，迫使全球经济发展受到制约。零信任作为破解当前困境的强有力手段，在其理念形成的初期便受到了业界的广泛关注。各国高度重视零信任领域的战略布局和创新研究，抢抓国际新技术主导权。中国也在不断推进零信任领域的技术创新应用。如何借助零信任重塑网络安全架构，已成为中国网络安全领域的研究热点。

本文将围绕总体研究、核心技术、产业发展3个方面，梳理零信任的发展态势，深入解析当前中国零信任产业发展存在的问题及其演进趋势，并提出发展建议。

1 零信任整体发展态势

1.1 国际零信任战略部署加快

零信任成为美国重塑政府整体网络安全架构的重要手段。2021年5月12日，美国发布总统行政命令[1]“（强制）要求联邦机构制定零信任安全架构的实施计划”。2021年9月7日，美国公布《推动美国政府朝向零信任网络安全演进的基本准则》[2]，明确指出各级政府部署零信任安全架构的时间表和发展目标。2021年11月，美国正式推出以零信任实施方案为核心的Thunderdome[3]（雷霆穹顶）项目，这标志着全球首个零信任国家级战略部署计划正式启动。2022年，美国白宫管理与预算办公室（OMB）发布备忘录（编

号为M-22-09）[4]，要求所有行政部门于2024年实现零信任全面部署。此外，美国2023财年年度预算[5]显示，总额8 133亿美元的年度预算中将有112亿美元用于网络战建设，其中包括“实施”部门的零信任架构。2024财年网络安全预算备忘录[6]再次将零信任在联邦民事行政部门机构的实施升为第一优先级。

新加坡[7]、加拿大[8]等在美国一系列零信任战略规划文件出台后快速做出响应。2021年4月12日，加拿大公布的《网络与安全战略》[8]详细介绍了零信任的概念及架构，并指出其对未来网络服务和安全的支撑性作用。新加坡于2021年10月5日宣布发布《网络安全战略2021》[7]以强调零信任应用的必要性，同时明确将积极在全国范围推行零信任落地实践。此外，欧盟于2022年3月22日公布《为联盟的机构、机关、办公室和机构制定高水平的网络安全措施》[9]，指出要明确朝向零信任架构迈进的具体步骤。根据多家第三方机构发布的数据，日本、澳大利亚、印度及一些中东国家均已在本土企业开展零信任模型的部署应用，并持续关注该领域的发展。

1.2 全球SASE技术标准体系不断完善

零信任技术发展趋近成熟，国际化组织标准建设进程不断加快。2020年8月，美国国家标准与技术研究院（NIST）加紧推动零信任架构研究，经过多轮修订发布了SP 800-207《零信任架构》[10]。2021年9月，网络安全基础设施安全局（CISA）发布《零信任成熟度模型》征求意见稿[11]，这标志着一种针对军政商三方零信任架构成熟度的评测方案正式形成。

全球各国/地区针对零信任领域的标准制定速度不断加快。作为一个权威的国际产业组织，云安全联盟（CSA）率先针对零信任三大技术之一的软件定义边界，进行了标准化研究，并在2014年发布《SDP标准规范V1.0》[12]，接着在2022年发布《软件定义边界（SDP）标准规范V2.0》[13]。与此同时，中国也在产业各方的推动下于2022年形成《零信任能力成熟度模型》，以指导中国零信任网络安全架构的落地。

1.3 零信任产业全面高速发展

全球零信任产业生态已初步形成，供需双方均在积极推进规模化部署进程。以谷歌、微软、思科为代表的美国网络安全领军企业对零信任市场进行了全面布局，与美国政府联动引领产业活力化发展。以电信、金融、能源为首的各垂直行业也在积极采用零信任网络安全架构，从试点试验到大面积落地部署应用，逐步从需方立场支撑零信任产业的发展。

Gartner[14]在2020年曾预测，2022年在面向生态合作伙伴开放的新型数字业务应用程序中，80%的业务将通过零信任网络访问（ZTNA）进行访问。据IDC预测，到2024年，安全远程访问解决方案将以260亿美元价值占据全球网络安全市场12.5%的份额[15]，其中零信任相关产品和解决方案将占据重要地位。2022年6月，Markets and Markets[16]在到2027年的全球预测报告中表示：全球零信任证券市场规模预计从2022年的274亿美元增长到2027年的607亿美元。

2 零信任网络安全架构及关键技术

2.1 零信任网络安全架构

零信任是一种新型网络安全理念，秉承着“持续验证，永不信任”的原则，拒绝隐式授予信任，持续进行安全评估，其体系架构是一种端到端的企业资源和数据安全方法，包括身份（人类和非人类的实体）、凭证、访问管理、操作、端点、宿主环境和基础设施，旨在通过利用网络分段、防止横向移动、提供第7层威胁预防和简化精细用户访问控制来保护现代数字环境。因此，零信任总体功能架构围绕技术和管理两个维度，涵盖八大关键能力，即身份安全、基础设施、网络安全、数据安全、应用/负载安全、网络可持续安全检测、评估和网络安全可视化以及综合安全管理，如图1所示。

身份安全：身份（人员、设备、应用、进程）是资源访问的入口，是零信任的基础。

网络安全：建立可信、可靠的网络链路是数据访问的重要环节。

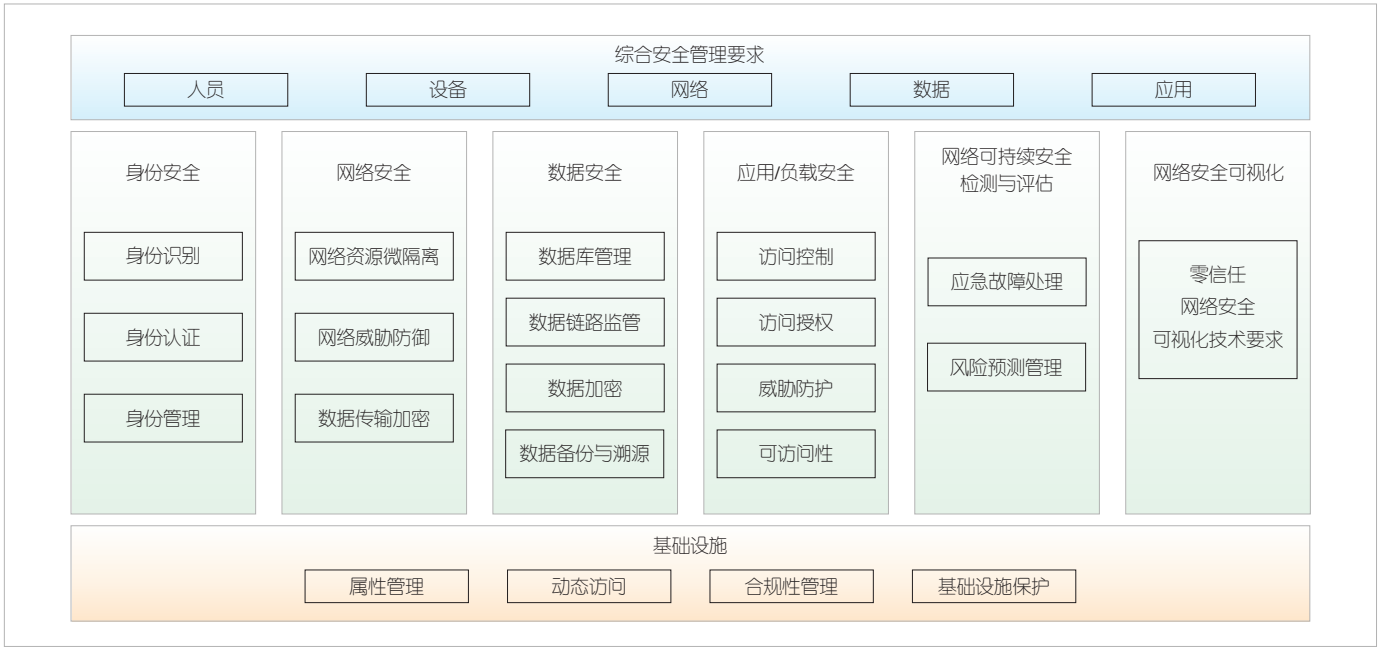
数据安全：数据是安全的核心，应被分类、标记和加密，并基于这些属性有条件地访问。

应用/负载安全：应用程序和应用程序编程接口（API）提供了数据访问接口，同时负载安全保障了资源交互的稳定性。

基础设施：建立安全的基础设施（本地服务器、云端虚拟机、容器、微服务）是减少风险的有效措施。

网络可持续安全检测与评估：网络可持续安全检测与评估是零信任架构实施的保障，其着眼于应急事件处理和风险管理两个维度，形成流程化处理模式。

网络安全可视化：网络安全可视化是零信任架构的坚实基础，其借助终端、应用、行为和事件这四大主体实现。



▲图1 零信任总体功能架构图

安全管理：安全管理是网络安全架构部署实践的保障。

2.2 零信任关键技术

零信任的关键技术包括软件定义边界、身份识别与访问管理、微隔离。

1）软件定义边界

作为零信任理念的实践方案，软件定义边界实现了对基于网络的攻击行为的阻断，分离了控制平台与数据平台，最小化攻击面；通过预验证、预授权，拒绝未经验证授权业务的端口访问；隐藏关键资产的同时对应用访问实现可视化，实现实时监督；可集成安全架构，大幅提升产品的兼容性；可代替部分传统网络安全的人力资源，节约成本。

2）身份识别与访问管理

作为零信任模型的应用基础，身份识别与访问管理是企业应用零信任的第一步，同时也是零信任项目取得信任的关键一步。身份识别与访问管理涵盖了用户身份、规则、身份验证管理软件以及访问管理策略和协议，实现了持续的动态认证与动态授权，融合了多因子身份认证、单点登录和用户行为分析，提供了静态密码以外的针对用户凭据的安全保护，对相关但独立的多个系统实施一种访问机制，可检查用户行为并自动应用算法和分析，以监测潜在的安全威胁。

3）微隔离

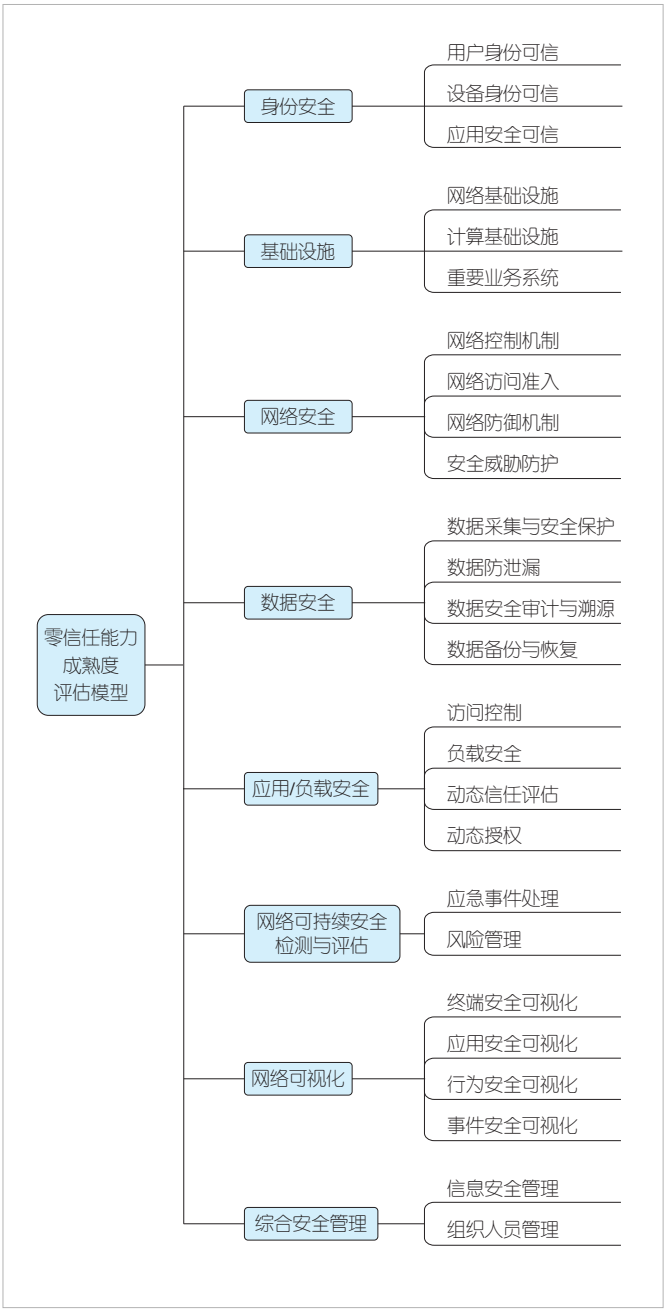
作为零信任概念的技术实践，微隔离实现了数据中心内工作负载间流量可视化与访问控制，在保留传统防火墙的安全边界防御的同时，限制工作负载流量间通信。攻击面的可视化加强了应用程序活动的管理细粒度。无须基于硬件的防火墙，微隔离可将安全性集成到虚拟化工作负载中，其安全策略与虚拟网络（虚拟机、操作系统或者其他安全目标）同步，实现纯软件方式的安全模型部署，改善监管合规态势，同时隔离信息技术（IT）基础设施，在混合云模式下支持跨平台的数据流量识别及统一管理。

4）零信任能力成熟度评估模型

本文中，我们参考《零信任能力成熟度模型》标准，遵循零信任的定义和原则，依据零信任总体功能架构，提出零信任能力成熟度评估模型，将零信任总体架构细分为8个技术模块与26个能力域，形成零信任关键能力图谱，如图2所示。

为使零信任能力成熟度判定标准详细且规范化，本文将零信任能力成熟度划分为无零信任阶段、传统阶段、初级阶段、优化阶段和持续安全阶段五大成熟度等级，旨在以全局或专业领域视角从零信任核心功能子组件、技术交互方式等方面展示零信任安全能力成熟度，助力零信任技术优化升级，如表1所示。

以身份安全技术模块为例，我们对该模块下四大能力域涵盖的能力要点进行量化打分。用户身份可信域的计算公式为：用户身份可信子领域4级能力符合度=（达到4级的安全能力数量+达到更高等级的安全能力数量）/用户身份可信



▲图2 零信任关键能力图谱

▼表1 零信任能力成熟度五大阶段

零信任能力成熟度阶段	阶段描述
无零信任阶段	不具备零信任安全技术能力的原始阶段
传统阶段	具备基本网络安全技术能力、概念级的零信任系统能力
初级阶段	具备基础零信任安全技术能力、部分零信任功能模块的安全技术能力
优化阶段	具备系统级别的零信任安全技术能力，支持主动防御能力
持续安全阶段	具备标准级别、可持续提升的零信任安全技术能力

子领域内安全措施总数 ×100%。能力符合度达到80%即可判定用户身份可信域达到“优化阶段”。

零信任能力成熟度评估模型是《零信任能力成熟度模型》标准落地的重要抓手，更是零信任技术规范化发展的基石。对各厂商零信任产品进行成熟度测试，有助于各企业查漏补缺，不断完善零信任产品的功能，提升零信任安全服务的质量，推动零信任产业规范化、规模化发展。

3 中国零信任发展面临三大挑战

1）战略统筹布局未开展，规划前瞻性不足

中国已将网络安全建设视为国家长远发展的核心，明确“网络安全牵一发而动全身，深刻影响政治、经济、文化、社会、军事等领域安全”[17]。“十四五”期间出台《网络安全产业高质量发展三年行动计划（2021–2023年）》[8]等文件，逐步推进零信任相关研究与试点实验项目落地。但是，与美政府持续加大零信任技术投资力度相比，中国仍缺乏整体发展路线图与具体配套支持资金，政府机构、行业企业、社会组织等未形成落地应用的引导措施，缺乏自主技术引领的解决方案和应用实例支撑，零信任战略布局相对滞后。

2）技术体系建设待完善，自主创新力不足

当前，中国零信任技术研究紧紧跟随国际发展趋势。2020年8月全国信息技术标准化技术委员会决定对《信息安全技术零信任参考体系架构》标准进行立项。2021年6月中国通信学会组织开展《零信任能力成熟度》标准的研制工作，并于2022年7月完成文稿的发布。虽然已有部分标准成功落地，但是中国零信任网络安全架构尚未形成自主技术体系，创新力仍然较低，仅仅对美国已发布的部分标准进行对标立项，标准化建设还不足，整体架构仍停留在概念、原型阶段，形成的产品细节、规格等方面也存在着诸多差异，难以适配垂直行业多样化应用部署，整体技术发展缓慢且成熟度低，并且尚未开展垂直行业的零信任架构升级和应用部署。

3）产业生态闭环未形成，供需协同性不足

近两年，中国网络安全龙头企业已推出部分零信任产品及方案，在医疗、电信等行业快速实践落地。但中国零信任产业发展尚处于初期阶段，缺乏全面实施零信任架构的标杆企业。2021年，第三方咨询机构Forrester[19]从推出时间、成熟度和客户情况3个方面筛选出34家国际零信任方案供应商代表，中国仅有3家厂商入选。2022年，第三方咨询机构Gartner发布的《零信任网络访问市场指南》[20]共调研了42家全球零信任代表性供应商，中国仍是仅3家上榜。此外，

中国缺少产业服务平台支撑，零信任需求侧与供给侧的发展步调不一，市场流通产品方案存在覆盖面不广、适配性不高、服务性不足等基础问题。

4 零信任产业发展建议

1）全面统筹规划，强化零信任整体战略布局

强化政策引导，完善中国零信任体系构建。依托财政资金、国家专项等，全面跟进和研判美国在参考架构、关键技术、融合应用等方面的最新进展，加大零信任架构关键技术的科研投入。抓住行业数字化升级转型机遇，推动网络安全架构向零信任架构迁移，鼓励组织研究并出台零信任创新应用试点示范、专项项目等支持政策，并在财政投资的网络安全项目中同步配套零信任架构和关键网络安全基础设施建设措施，明确零信任高质量发展路线图。广泛征集零信任应用实践案例，并对独具行业代表性和可推广性的优秀案例进行宣传，鼓励零信任产品供应商借鉴学习，不断优化产品升级，促进各行业需求方与供应商的长期稳定合作。鼓励传统信息安全提供商、新型云安全提供商与行业用户深度融合，打造一批有影响力的零信任行业应用标杆。在党政、金融、能源、交通等领域开展零信任安全试点示范，提升零信任网络安全架构在实际应用中的市场影响力。

2）重视培育创新，发展零信任自主创新技术

深化核心自主研究，打造中国零信任创新引擎。加快构建基于软件定义边界、身份安全、微隔离三大技术路线的零信任标准体系，推进跨云跨网智能安全管控、基于数字身份的细颗粒度访问控制、可持续数据安全监测和评估等产品升级。同步构建零信任安全测评体系，深入剖析零信任技术能力与功能需求，助力零信任应用部署，依托“零信任能力成熟度”的评估模型，分级分类分步骤差异化部署零信任。推进电信运营商、互联网企业、行业用户、安全企业、科研机构、高等院校等建立零信任联合创新中心、联合实验室等，打造创新试验床，促进研究成果应用转化，保障零信任产品创新能力持续供给，同时定期开展零信任技术专题研讨，助力零信任技术创新以及产品研发。

3）增强产业协同，构建零信任健康产业生态

积极推动供需联动，释放中国零信任集群效应。针对中国大型网络安全供应商提供政策优化保障，打造可以带动跨领域、跨行业能力整合的龙头企业，带动中小型企业蓬勃发展。依托算网融合产业及标准推进委员会等第三方产业平台，提供交流论坛、项目推介、实践比赛、案例评优等多举措多层次供需对接服务，切实强化零信任产业合作。聚焦零信任产业链上下游，绘制零信任产业图谱，适配党政、金融、能源、交通等领域建立多维度零信任能力评估体系，从核心技术功能、应用解决方案、关键能力成熟度等多维度，引导以优秀产品服务能力为导向的零信任市场良性发展。

参考文献

[1] The White House. Improving the nation´s cybersecurity [EB/OL]. (2021-05-12)[2023-10-25]. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

[2] The White House. Draft federal strategy for moving the U.S. government towards a zero trust architecture [EB/OL]. (2021-09-07) [2023-10-25]. https://www. whitehouse. gov/omb/briefing-room/2021/09/07/office-of-management-and-budget-releases-draft-federal-strategy-for-moving-the-u-s-government-towards-a-zero-trust-architecture

[3] Defense Information Systems Agency. Thunderdome realizing zero trust [EB/OL]. [2023-10-25]. https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b. ssl. cf1. rackcdn. com/external/fact-sheetthunderdometemplatefinal.pdf

[4] The White House. Moving the U. S. government toward zero trust cybersecurity principles [EB/OL]. (2022-01-26)[2023-10-25]. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[5] U. S. Department of Defense. The department of defense releases the president´s fiscal year 2023 defense budget [EB/OL]. (2022-03-28)[2023-10-25]. https://www.defense.gov/News/Releases/Release/Article/2980014/the-department-of-defense-releases-the-presidents-fiscal-year-2023-defense-budg

[6] The White House. Administration cybersecurity priorities for the FY 2024 budget [EB/OL]. (2022-07-22)[2023-10-25]. https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-16.pdf

[7] CSA. The Singapore cybersecurity strategy 2021 [EB/OL]. (2021-10-05)[2023-10-25]. https://www. csa. gov. sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021

[8] Government of Canada. Network and security strategy [EB/OL]. (2021-04-12) [2023-10-25]. https://www. canada. ca/en/shared-services/corporate/publications/network-security-strategy.html

[9] European Commission. Laying down measures for a high common level of cybersecurity at the institutions, bodies [EB/OL]. (2022-03-22)[2023-10-25]. https://eur-lex. europa. eu/legal-content/EN/TXT/? uri=CELEX:52022PC0122

[10] National Institute of Standards and Technology. Zero trust architecture [EB/OL]. [2023-10-25]. https://nvlpubs. nist. gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[11] Cybersecurity and Infrastructure Security Agency. Zero trust maturity model draft [EB/OL]. [2023-10-25]. https://www. cisa. gov/zero-trust-maturity-model

[12] Cloud Security Alliance. SDP specification v1.0 [EB/OL]. (2014-04-30) [2023-10-25]. https://downloads. cloudsecurityalliance. org/initiatives/sdp/SDP_Specification_1.0. pdf? _ga=2.228130653.1951536048.1669190328-1229248686.1669036181

[13] Cloud Security Alliance. Software-defined perimeter (SDP) specification v2.0 [EB/OL]. (2022-03-10) [2023-10-25]. https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2

[14] Gartner. Market guide for zero trust network access [EB/OL]. (2019-04-29)[2023-10-25]. https://www.gartner.com/en/documents/3912802

[15] 白杨. 零信任安全的2022: 产业迎来爆发期, “去虚向实”将成行业共识 [EB/OL]. (2021-04-19) [2023-10-25]. https://finance. sina. com. cn/chanjing/cyxw/2022-03-03/doc-imcwipih6443414.shtml

[16] Market Research. Zero trust security market by solution type, deployment mode, authentication type, organization size, vertical and region - global forecast to 2027 [EB/OL]. (2019-04-29) [2023-10-25]. https://www.marketresearch. com/MarketsandMarkets-v3719/Zero-Trust-Security-Solution-Type-31844180

[17] 中共中央党史和文献研究院. 习近平关于网络强国论述摘编 [M]. 北京: 中央文献出版社, 2021

[18] 中华人民共和国工业和信息化部. 网络安全产业高质量发展三年行动计划（2021—2023年）[R]. 2021
[19] Forrester. New tech: zero trust network access, Q2 2021 [EB/OL]. (2021-04-19)[2023-10-25]. https://www.forrester.com/report/new-tech-zero-trust-network-access-q2-2021/RES161768?objectid=RES161768
[20] Gartner. Market guide for zero trust network access [EB/OL]. (2023-09-25)[2023-10-25]. https://www.gartner.com/en/documents/4773531

作　者　简　介

张云畅，中国信息通信研究院技术与标准研究所技术专家；主要从事零信任、算网安全等方面的研究工作；起草并参与多个零信任白皮书撰写、标准研制工作，目前拥有专著1部，起草行业白皮书1个，参与研制行标/团标5项。

柴瑶琳，中国信息通信研究院技术与标准研究所高级项目主管；主要从事SD-WAN、零信任、算网安全等相关技术研究工作；起草并参与20多项行业/团体标准的制订，发表论文10余篇，授权/申请技术专利6项，拥有软著7项，组织发布行业白皮书3个。

穆珒博，中国信息通信研究院技术与标准研究所互联网中心副主任，高级工程师；主要从事算网融合、未来网络、云计算等方面的研究工作；牵头多个技术体系的标准研制，发表论文10余篇，拥有软著12项。