CSA GCR cloud security alliance
GREATER CHINA REGION ®

Toward a Zero Trust Architecture

实战零信任架构

面向复杂且混合的数字世界的权威安全指南

序 言

伴随着云计算、移动互联、物联网等新兴技术的发展、移动办公等需求的增加，互联网渗透到经济社会的方方面面，网络安全问题也愈演愈烈，网络安全事件带来的危害越来越大。传统的“纵深防御+边界防护”这类基于边界的安全防护体系因为边界的模糊而渐渐失效，难以适应企业的快速增长及业务的快速变化。

聚焦资源保护，不允许隐式信任的零信任理念在过去几年里获得了众多政府及企业的认可。为了便于企业合理评估自身零信任安全建设实施进度并为企业后续相关安全能力建设发展提供指引及决策依据，本文引入了CISA发布的基于身份、设备、网络、应用程序工作负载和数据五大模块构建的零信任成熟度模型ZTCMM及零信任路线图，供组织机构评估自身建设情况并针对评估结果制定企业后续零信任安全能力建设发展规划。

伴随着云原生、DevSecOps在企业内的成功落地，本文在SDP、IAM和微隔离（网络分段）的基础上额外讨论了和容器高度契合的服务网格、边缘计算和策略即代码技术与零信任架构融合的可行性。并从技术、文化、策略及监管措施多个领域分析解决方案影响，帮助行业利益相关方识别挑战和机遇。

本白皮书再次体现了CSA在零信任领域为业界做出的贡献，这也是我们的领军专家Juanita的最后遗著，感谢大中华区参与本次翻译和支持的工作者们的无私奉献。

李雨航 Yale Li
CSA 大中华区主席兼研究院院长

致 谢

本文档《实战零信任架构》(Toward a Zero Trust Architecture)由CSA的DC分会专家编写，CSA大中华区工作组专家翻译并审校。

中文版翻译专家组（排名不分先后）：

组　长：陈本峰

翻译组：余晓光　林艺芳　滕　伟　王　彪　苏泰泉

　　卞乐彬　江　澎　姜政伟　李芊晔

审校组：余晓光　于继万　林艺芳　滕　伟　王 彪　吴 满

　　郭鹏程　苏泰泉　卞乐彬　姜政伟　李芊晔　姚 凯

研究协调员：陈 龙

感谢以下单位对本文档的支持与贡献：

云深互联（北京）科技有限公司、北京天融信网络安全技术有限公司、北森云计算有限公司、广东美云智数科技有限公司、华为技术有限公司、上海缔安科技股份有限公司

英文版原创作者:

Juanita Koilpillai　Jyoti Wadhwa　Dr.Allen Harper　Salil Parikh、

Paul Deakin　Vivian Tero　Greg Bateman　Aubrey Merchant-Dest

Jay Kelley　Phyllis Thomas　Uma Rajagopal　Rebecca Choynowski

英文版原创贡献者:

Jason Keplinger　Tom Stilwell　Lauren Bogoshian　Bob Klannukarn

Joe Klein　Daniele Catteddu　Nirenj George　Jagan Kolli　Andres Ruz

特别感谢:

本文档由云安全联盟 (CSA) 的 DC分会创建。 CSA 的 DC 分会由一直处于云安全前沿的志愿者组成。 请访问我们的网站 https://www.cloudsecurityalliance-dc.org/ 了解更多信息。

在此感谢以上专家。

如译文有不妥当之处，敬请读者联系CSA GCR秘书处给与雅正！联系邮箱：research@c-csa.cn； 云安全联盟CSA公众号

摘 要

企业利益相关者必须考虑与日俱增的实时系统复杂度所带来的挑战、新网络安全策略带来的需求，以及在复杂和混合世界中安全地运行系统所需的强大文化支持。零信任等新兴技术解决方案和方法对于满足美国总统拜登的第14028号行政令《改善国家网络安全》中的要求至关重要。本文探讨了新兴的、丰富的、多元化的解决方案格局的影响以及组织机构最终交付零信任架构(ZTA)的能力所面临的挑战。对行业如何改善关键利益相关者群体之间的协作以加速企业领导者和安全从业者在其环境中采用零信任提出了建议。

云安全联盟出品-华盛顿特区分会(CSA-DC)研究委员会

研究委员会主席：Mari Spina

悼 词

本文献给Juanita Koilpillai，她突然意外的离开，意味着网络安全界和她CSA-DC分会朋友们的巨大损失。Juanita即是这篇论文的主要作者和贡献者，也是撰写这篇文章的CSA-DC分会工作组的贡献者。Juanita对网络安全的所做的贡献将继续代表她不断加强世界各地组织的网络安全态势。她的技术领导力和开发的软件定义边界(SDP)技术形成了零信任架构(ZTA)的早期基础。

Juanita是一盏真正的明灯，在网络安全社区中闪耀着光芒。我们怀着极大的悲伤向一位真正伟大的领袖和工程师告别。

Anil Karmel

CSA-DC分会主席

目录

1 背景

由于全球COVID疫情大流行，组织机构不得不迅速适应全球远程办公的方式。随着远程办公的不断扩张和云计算技术的采用，安全边界的定义也随之扩展，因此需要采用零信任（ZT）策略保护未来的工作。加上企业向更敏捷和更易规模化的多云、混合架构的不断转变，这些变化导致我们比以往任何时候都需要改善信息系统的安全性和风险管理。于是，IT组织现在有强大的驱动力将重点放在定义和采用适合其环境的独特的零信任架构（ZTA）上。最近颁布的（美国）总统行政命令要求改善国家网络安全[1]和实施联邦零信任战略[2]，进一步促进了 ZTA零信任架构的采用。

随着基于边界和纵深防御方法让位于这种新的安全范式，企业正在寻求降低安全风险，尤其是当他们开始采用现代微服务、微隔离和软件定义架构提高远程生产力的时候更是如此。尽管得到IT供应商的广泛支持，ZTA的现实状态仍然是一个雄心勃勃的未来目标，因为组织机构才刚刚开始为其ZTA方案制定基线，而行业正在寻求洞察力，通过持续合作形成最佳实践或标准。

本文适合网络安全从业人员、工程师、架构师、商业领袖和IT业务相关者。虽然本文内容广泛且有价值，但主要代表美国政府的观点。因此，本文假定您已经熟悉NIST的SP800-207文档。

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[2] https://zerotrust.cyber.gov/ federal-zero-trust-strategy/

1.1 为什么选择零信任?

信息安全的零信任模型于2003年在Jericho项目上提出，当时人们已经认识到传统边界网络面临的安全挑战，随后在2009年(2014年公开可用)的谷歌Beyond Corp项目中实施了零信任模型，然后由Forrester Research在2010年予以定义。零信任模型“消除了可信网络的概念”并教导“在零信任(ZT)中，因为所有网络流量都是不可信的，所以安全专业人员必须验证和保护所有资源、限制并严格执行访问控制、检查和记录所有网络流量。”[3] 2019年，NIST撰写了零信任架构特别出版物[4](SP 800-207），该文章将零信任理念融入零信任架构（ZTA）的抽象定义，并提出了ZTA开发和实施的指导原则，如图 1 所示。

行业的变化推动了ZT零信任安全的新格局，包括急速上涨的安全成本、以及5G 、云计算、物联网 (IoT) 和面向微服务的架构的广泛使用。这些因素重新定义了所有权边界和应用模式，导致了固定物理边界或软件定义的网络边界的消失。

[3] https://media.paloaltonetworks.com/documents/ Forrester-No-More-Chewy-Centers.pdf

[4] https://csrc.nist.gov/publications/detail/sp/800-207/final

图1.零信任原则，NIST SP 800-207

随着组织机构不断将其全部或部分网络迁移到云，政府机构和商业企业的业务负责人必须以新的方式保护其私有、公共或专有云实例。尽管需求迫在眉睫，但安全格局的这种变化的实施需要时间和决心。组织机构将需要通过新技术栈、技能集和流程提高他们在云中保护系统的能力。这对开发新的安全治理和策略提出了挑战，要求基于持续验证、微分段、软件定义网络以及持续监控和持续可见性。为了实施和执行这些现代化策略，行业从业者需要设计和运营传统和现代访问控制和网络技术的复杂组合，并随着时间的推移进行适合自己环境的定制。常见的部署方法（如始终在线的VPN连接和将所有流量路由到企业网关），从成本和用户体验的角度看，变得低效或不再可行。

此外，许多网络安全方法都采用基于特征的概念，即安全工具寻找已知的不良行为“特征”，但根据定义，零日威胁并没有已知特征。零信任解决了这个问题，因为零信任架构不依赖基于特征或异常的技术帮助降低风险。在零信任中，实际的数据和功能无论何时何实例化，安全控制都将无处不在，并且正朝着更接

近实际数据和功能的方向发展。然而，鉴于各组织机构的现代化速度和水平存在差异，关于如何保护这些现代化架构的行业指南的进展和成熟度已经落后，充其量也太不协调，无法最好地保护系统及其数据。

鉴于架构和市场的复杂性，零信任解决方案和路线图的成熟度才刚刚开始。例如，安全从业人员面临着在实时、多云环境中识别用户和自动化检测新网络威胁的挑战。鉴于当今复杂混合的环境，本文提出了零信任体系架构能力成熟度模型（ZTA-CMM）的基本要素，并使之与零信任路线图关联。持续与政府和产业的交流合作将有助于制定ZTA-CMM最佳实践，并评估如何将零信任原则应用于当前架构以及相应的零信任路线图，以缩小差距、提高风险管理和网络弹性。

1.2 评估当前的零信任成熟度

组织机构必须了解其零信任架构的当前成熟度水平，调研整个组织机构范围，进行彻底和有效的分析。该分析应涉及到目前与零信任所有模块相关的人员、流程和技术。虽然CISA联邦零信任战略[5]文件主要服务于联邦机构，但也可作为一个指南文件帮助理解对成功实施零信任架构至关重要的流程和技术。美国国家标准与技术研究院（NIST）和行业领导者[6]（如ACT-IAC[7]和Forrester[8]）正在定义概念模型和框架并不断改进；然而，应当指出，目前这些框架还没有结合在一起。CISA发布了零信任成熟度模型ZT CMM[9]，由以下模块组成：身份、设备、网络、应用程序工作负载和数据。这五大模块共同组成了一个整体方案，指导了一个组织机构如何将资源用于开发零信任架构。

[5] 美国管理和预算办公室.联邦零信任战略.网络安全和基础设施安全局.2021年9月29日检索自 https://zerotrust.cyber.gov/ federal-zero-trust-strategy/

[6] 微软.零信任模型-现代安全架构.2021年9月29日检索自 https://www.microsoft.com/en-us/security/business/zero-trust

[7] 美国技术工业咨询委员会.（2019年4月18日）.零信任网络安全当前趋势.https://www.actiac.org/system/files/ACT-IAC%20Zero%20 Trust%20Project%20Report%2004182019.pdf

[8] Forrester.2020年零信任安全手册.2021年9月29日检索自 https://www.forrester.com/playbook/The+Zero+Trust+Security+Playbook+For+2020/-/E-PLA300

[9] 网络安全和基础设施安全局.网络安全司.（2021年6月）.零信任成熟度模型-决策前草案，版本1.0。网络安全和基础设施安全局。 https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20 Maturity%20Model_Draft.pdf

零信任架构模块（DHS CISA CMM）

身份	在复杂的混合与移动环境中，所有参与者的身份都存储在联合活动目录中，并基于公钥基础设施（PKI）体系。此外，组织机构可以使用单独的身份管理解决方案，该解决方案可能与联合活动目录服务完全集成，也可以不集成。
设备	组织机构的终端包括但不限于：传统服务器、台式机、笔记本电脑、VDI实例、客户端、移动设备、物联网（IoT）设备。
网络	网络包括传统、无线、移动（5G、Zigbee等）、云、以及软件定义网络（例如在超融合基础设施（HCI）中，在网络和应用层建立了微分段）。
应用程序 工作负载	组织机构的应用程序工作负载或其支撑平台可能来自第三方和/或自主开发，包括应用程序以及用于支持应用程序的平台、容器和服务器。
数据	数据可能是由组织机构收集的业务数据，用于业务开展，但也可能包括为了业务可见性所建立的数据。

图2.零信任支柱，DHS CISA ZT-CMM

零信任架构成熟度模型ZTA-CMM提供了每个模块成熟度级别的洞察（如图2所示）。深入了解每个领域有助于组织机构负责人了解环境中采用零信任架构方面的独特优势和差距。目前，组织机构并没有赋予一个普适的零信任成熟度模型执行零信任架构评估，这是行业指南中的一个空白，因此整个行业需要增强关于零信任成熟度ZTA-CMM的排名和评级合作。在此过渡期，个别组织可能会先执行初步评估，这些初步评估的结果将成为该组织的基线评估。

1.3 制定零信任路线图

随着组织机构对其零信任架构成熟度级别的当前状态有更多的了解，可以确定其所在级别并将新的解决方案纳入其架构，缩小差距并提高成熟度。例如，DHS CISA ZT CMM（DHS CISA）使用三个级别：传统、高级和最优，如图3所示

DHS CISA 零信任成熟度模型

图3. CISA ZT-CMM, (DHS CISA)

为了达到理想的零信任架构成熟度，组织需要评估自己当前的成熟度，并根据评估结果确认要优先建设的领域、需要的资源以及在一段时间内达到目标所需的预算。

相较于在安全和IT现代化建设处于起步阶段的组织，ZTA成熟度在已经实现了较好零信任的环境下更具相关性。为了满足ZTA路线图的要求，负责人需要更好地理解不断发展的前沿技术，这些技术为达到目标成熟度提供了先进的方式。

首先，完成对组织零信任成熟度五大模块能力的评估。对于每个模块可以制定几个问题，以便负责人全面评估每个重点领域的成熟度水平。这些问题按照难

度和范围递增，从而使零信任在该模块中更为成熟。完成调查问卷后，组织机构可以利用量化结果作为组织当前零信任架构ZTA成熟度的评估基线。组织架构的的当前成熟度水平和组织预期的成熟度水平目标可以按照量化规则图展现，量化规则图类似CMMC[10]建议的蜘蛛图表示方法，如图4所示。

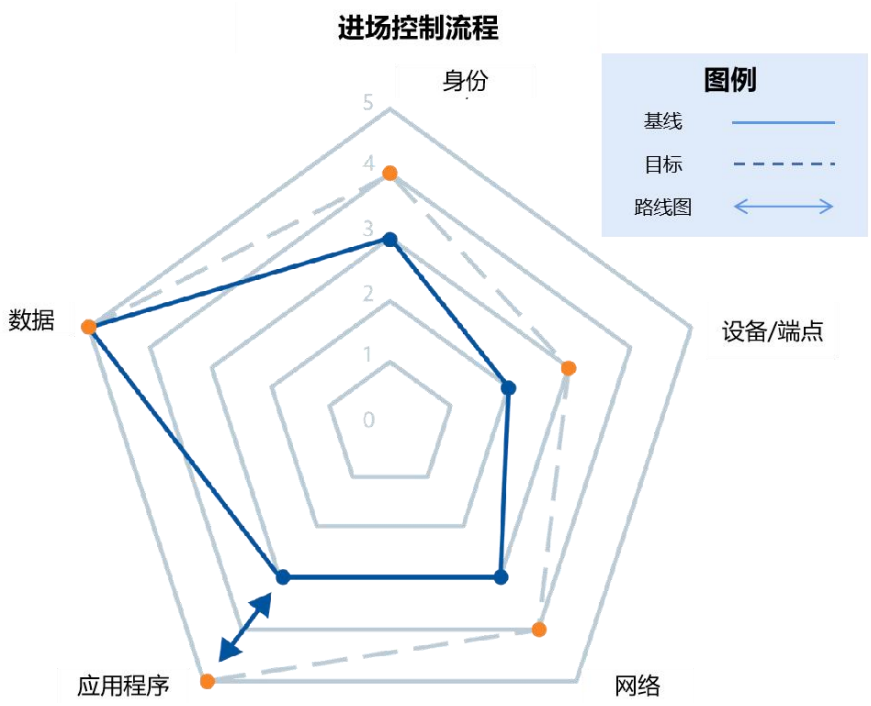

图4. 零信任成熟度蜘蛛图(概念)

由此产生的基线和目标点的差异是差距评估。差距评估包括每个模块的具体领域，零信任ZT路线图将在一到三年内系统化地逐步从当前状态提升到目标状态。

[10] https://cmmcinfo.org/cmmc-info-tools/dod-nist-sp-800-171-basic-self- assessment-scoring-template/

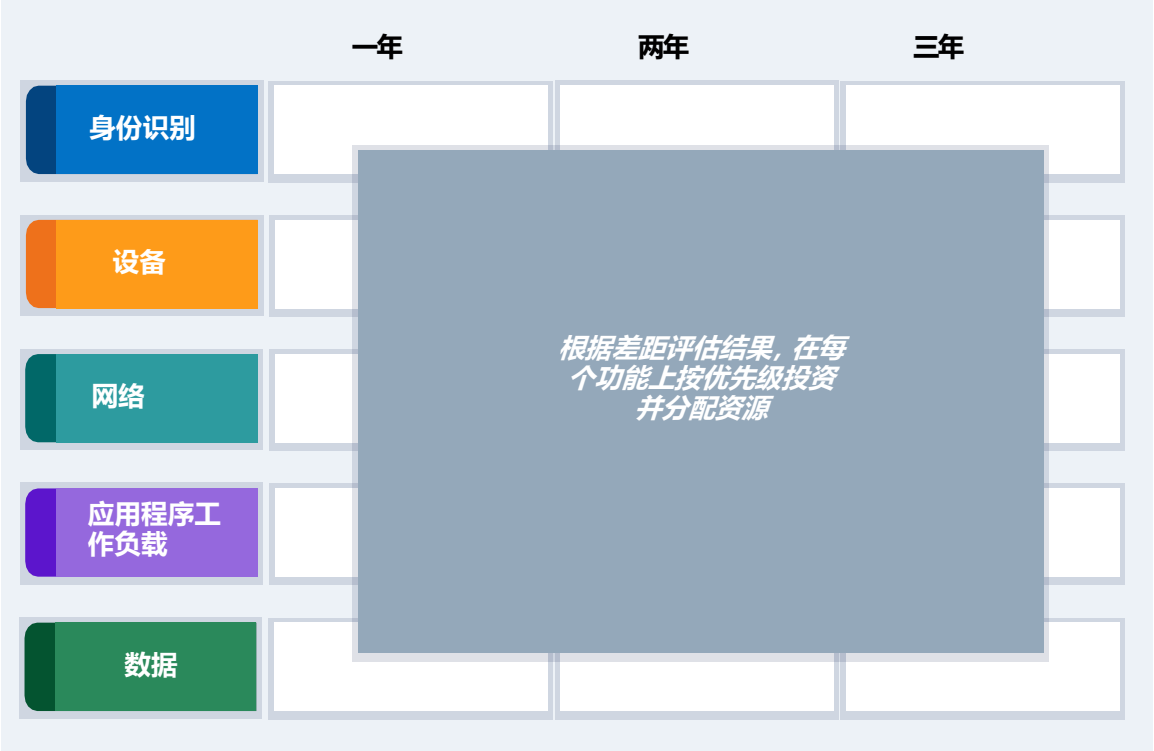

图5. ZT 优先投资线路图(概念)

这种方法产生了一个零信任ZT的投资优先级路线图，如图5所示。投资优先级路线图应结合应用行业最佳实践和框架，如NIST特别出版物(SP) 800系列，CSA云控制矩阵(Cloud Controls Matrix ，CCM)，或政府安全技术实施指南(Government Security Technical Implementation Guides, STIG)。这些最佳实践和框架适用于每个模块，有助于指导组织机构了解其当前状态中缺乏的详细流程和技术需求，以便在一到三年内达到预期的成熟度水平。这种方法只是一个示例，每个组织机构都可以根据自身情况量身定做。未来的工作组和组织可能会制定一套标准的规范性问题和图形描述采用ZTA零信任架构的整体能力成熟度水平。

2 采用零信任的考量因素

除了考量零信任成熟评估和路线图因素外，技术、组织文化、策略和监管要

求这四个因素是建设零信任架构（ZTA）的重要考量因素。这些内外部因素影响一个组织机构在当前复杂和混合的环境中理解、设计及实施零信任架构的能力，帮助负责人确定哪些变量是当前零信任架构成熟度水平的关键障碍或加速因素，哪些变量最有助于推进其零信任架构之旅。

采用零信任架构的关键步骤之一是形成人员、流程技术、关键资产及安全控制措施清单。这是成功采用该架构的关键。NIST建议从单个流程入手不断推进架构部署。

组织机构应以 “速赢”为目标，并理解采用零信任架构是一项长期的、战略级的举措。因此，零信任需要管理层的支持，并在三到五年内持续考虑所有相关因素。能力成熟度模型可以引导组织机构了解现有及传统的能力，同时提出适当的问题并寻求答案。例如，问题可以包含：

1. 组织使用的传统技术是什么？

2. 它们使用什么类型的数据和服务？

3. 具体实施了哪些云服务？

4. 是否已经实施了云访问安全代理的解决方案？

5. 如何管理身份以及实施了哪些工具？

6. 组织机构处于云应用的哪个阶段？

然而，问题应当结合组织机构的特定业务和使命量身定制。每个问题应当解决与技术状态、组织文化、运营策略、运营所处的监管环境及组织所面临的云安全架构相关的组织业务愿景。对联邦机构而言，这部分内容在CISA的云安全技术参考架构中有详细说明[11]。

[11] 网络安全和基础设施安全局。（注）。云安全技术参考架构。2021年9月29日，https://zerotrust.cyber.gov/cloud-security- technical-reference-architecture/

2.1 技术

对技术的考虑至关重要。传统技术解决方案以向边界添加层为核心，但这种基于边界的方法无法遏制对IT系统种类和数量都在不断攀升的攻击。应用程序交付的计算单元已从集中式的大型服务器过渡到众多虚拟化服务器和服务，再到分布在不同云资源中的高度细粒度的容器。功能的原子化给零信任的应用带来了可移植性的挑战；然而，随着数字转型计划驱动云采用率的不断提高，零信任代表了预防和抵御网络攻击的下一代趋势和先进网络空间方案。组织机构在关键能力方面的技能水平，如身份和凭证访问管理（ICAM）、软件定义网络（SDN）、微分段环境、身份感知代理（IAP）以及持续监控系统的能力，将推动向零信任架构的演进。了解组织架构中的技术环境以及市场生态系统中的可用选项将有助于选择适合其环境的正确解决方案。

2.2 组织文化

组织文化是所有利益相关方考虑的另一个重要因素。事实证明，COVID-19疫情是推动组织机构启用“居家办公模式”和安全团队向零信任战略迈进的一个催化剂。要采用零信任，组织机构必须愿意通过企业重构实现改变，并培养“永不信任”的思维。与传统环境相比，拥抱了可扩展云和混合模式的主动式组织更具优势，能够更轻松地采用“零信任思维”。了解组织文化和变革管理能力至关重要。

2.3 策略

除了文化，组织机构更新其策略的能力也至关重要。现代IT组织是一个复杂的私有部署和云托管架构交错的混合体，使组织机构的网络安全控制策略面临巨大挑战。策略变更的影响将渗透到组织的所有基础架构、应用程序和数据。对于每个组织机构来说，识别和制定基于零信任的新安全策略的能力将是一个重要因素，也是每个组织独有的。鉴于零信任架构的成熟度水平，组织可能面临识别、创建和规范这些策略的挑战。

2.4 监管环境

采用零信任的最后一个关键影响因素源于监管环境。美国政府有两个推动网络安全合规的主要框架：风险管理框架（RMF）[12]和网络安全框架（CSF），都由NIST管理。这两个框架为安全评估、实施、授权和监控提供指导。2013年2月12日发布的《改善关键基础设施网络安全的总统第13636号行政令》[13]建立了一个减少网络安全对关键基础设施风险的基于现有标准、指南和实践的框架。

本指南是对2014年《网络安全增强法案》[14]的加强。尽管这些合规框架灵活，但并未专门或更好地促进零信任架构的实施。[15]2021年5月12日颁布的第14028号行政令（“改善国家网络安全”）要求组织机构应负责管理网络安全风险，并呼吁行政部门支持关键基础设施所有者和运营者及其供应链改善网络安全水平。这些努力值得肯定，并为更多策略创造了动力。比如国防部参照零信任架构理念搭建的零信任架构体系，需要引入零信任成熟度评估(ZTA-CMM)和带有时间表计划的零信任路线图，以实现安全层面的实质性提升。这些监管举措有助于激发必要的变革，以挫败新的网络攻击，增强网络弹性。新法规的出台，将鼓励行业服务提供商和相关利益方（如软硬件供应商、系统集成商、服务提供商、信息技术组织及更多将创新引入解决方案的机构）的参与。

---

12 安全小组（2019年10月8日）。NIST 800–53修订版。5：这是什么，为什么应该关心。安全小组，https://www.securicon.com/nist-800-53-rev-5-what-it-is-and-why-you-should-care/

13 第13636号行政令，78 FR 11737（2013年2月12日）。https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

14 NIST（2021年7月14日）。网络安全框架|开始。NIST。https://www.nist.gov/cyberframework/getting-started

15 第14208号行政令，86 FR 26633（2021年5月12日）。https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

3 零信任解决方案的全景图

为了提高组织机构的零信任成熟度，有必要审查和确定适用的技术和解决方案。例如，云计算的传统基础设施已经发展，其中包含现代组件，如容器和服务网格，需要与零信任核心组件集成（“策略引擎”[PE]、相关的“策略管理器”[PA]和各种“策略执行点”[PEP]）.[16]管理零信任架构的这些新战略一定会出现，而下文中提及的技术领域和相关示例仅代表了向零信任架构演进过程中涉及的现代化安全环境解决方案的一小部分。本文探讨的代表性技术方法和其影响包括了软件定义架构组件、服务网格功能、边缘计算趋势和策略即代码可能性。

3.1 软件定义边界

举一个显而易见的例子，软件定义边界（SDP）和零信任原则同时演变，对安全行业全景图中蕴含的挑战、实现和变化作出可同样的响应。此外，鉴于SDP组件解决了零信任原则中的许多问题，因此这两个概念是完美融合的。如今，SDP已被业界视为实现零信任原则的软件定义架构的一个明确部分，NIST零信任架构白皮书将SDP作为零信任架构具体落地实现的方法之一[17]。

Gartner Research将SDP描述为一种提供“对企业应用程序安全访问”的技术，强调设备认证和用户授权是一种“固有功能”，以及“建立多个加密隧道到不同目的地的能力”[18] 。SDP仅在通过请求系统和应用程序基础设施之间的实时加密连接进行设备认证和身份验证后，才提供对应用程序基础设施的访问。2019年，Gartner继续通过其零信任网络访问（ZTNA）模型支持SDP，[19]该模型围绕一个应用程序或一组应用程序创建基于身份和上下文的逻辑访问边界。这种情况下，应用程序隐藏起来无法发现，并且通过受信任的代理限制对一组命名实体的访问。这会将应用程序资产从公共可见性中移除并减少攻击面。

---

16 .Rose, S., Borchert, O., Mitchell, S., & Connelly, S.（2020年8月11日）。SP 800–207，零信任架构。NIST。https://csrc.nist.gov/publications/detail/sp/800-207/final

17 Rose, S., Borchert, O., Mitchell, S., & Connelly, S.（2020年8月11日）。SP 800–207，零信任架构。NIST。https://csrc.nist.gov/publications/detail/sp/800-207/final

18 Gartner Research（2018年11月9日）。事实还是虚构：软件定义的外围设备真的是下一代VPN吗？https://www.gartner.com/document/3892882

19 Riley, S., MacDonald, N., & Orans, L（2019年4月29日）。零信任网络接入市场指南。盖特纳。https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

[20]云安全联盟（CSA）在其 2020 年报告《软件定义边界》（SDP）和《零信任》[21] 中也支持这一演变，将 SDP 视为“网络层零信任”。

3.2 网络分段

尽管软件定义边界（SDP）提供了一种实现零信任架构的方法，但必须同时进行如下工作：采取分段（在零信任文献中常称为微隔离）的方法，用默认拒绝模型减小攻击面并防止横向移动特征造成的数据泄露问题。网络分段功能允许访问之前强制执行身份验证和授权，而SDP正是该功能的一种进阶——在网络分段的基础上对共享网络链接使用密钥加密。另一种基于主机的分段方法则不需要使用密钥：通过控制主机防火墙建立认证信道，以在大规模异构计算系统平台（私有部署、公共和私有云、容器）上实施动态策略和分段控制，同时允许策略随工作负载变化。

为了保证安全性，使用网络分段时需要创建多个安全分区，这些安全分区根据服务类型及其通信关系、用户身份、每个分区的数据敏感程度定义[22]。传统的网络安全分区模式受到资源开销、防火墙规则管理的复杂性和集成风险的限制，从而导致可选用的安全分区数量受限且粒度较大，这与“减小攻击面/最小权限”的零信任准则相悖。此外，一些先进的组织机构采用了最新应用架构，其工作负载可能运行在虚拟机、容器、无状态服务器上，导致传统方法可能很难在应用了容器、无服务器和托管云服务等新兴技术的环境下有效分段。

软件定义网络（SDN）将管理流量的网络控制平台与转发平台分离，可以通过API编辑网络控制，允许更多的动态流量调整和微分段链路的分段控制。通过SDN实现的分段使人们可以创建更细粒度的安全分区。

---

[20] Riley, S., MacDonald, N., & Orans, L（2019年4月29日）。零信任网络接入市场指南。盖特纳。https://www.gartner.com/en/documents/3912802/market-guide-for-zero-trust-network-access

[21] 云安全联盟SPD和零信任工作组。（2020年5月27日）。软件定义周界（SDP）和零信任。云安全联盟。https://cloudsecurityalliance.org/artifacts/ software-defined-perimeter-and-zero-trust/

[22] Riley, S., MacDonald, N., & Orans, L. (2019, April 29). Market Guide for Zero Trust Network Access. Gartner.

一套完整的分段解决方案需要提供关于工作负载、设备/端点和用户识别信息的全面和统一的可视化集成。理想情况下，它还可以在预防性和响应性的安全事件场景中自动、协调地分段。随着零信任技术的成熟，合并元数据标签治理的功能将帮助实现分段的自动化与协调化。示例如下：

- 根据IP地址、工作负载、用户和设备连接状态等的变化，动态执行准入列表。
- 与DevSecOps CI/CD环节集成，在新的工作负载和容器加入时进行新的分段。
- 将报警和分析信息添加到动态策略管理中。
- 集成威胁检测、监控和漏洞扫描功能，自动重新计算适用的准入列表，并协调流程等级的分段。

并非所有的分段方法都是相同的，因而组织机构必须酌情选择最适合其云基础设施的结构和部署模型。

云服务提供商（CSP）为许多IT组织提供安全、可扩展性、敏捷的计算以及存储业务，其地位至关重要，因此在零信任框架中普遍采用SDP和SDN的情况尤其值得关注。如今，云服务提供商使用SDN作为设计、搭建、运营全球范围IPv4和IPv6网络的零信任方法。这也反过来促使云服务商提升其安全性和本地服务的可用性，以便更好地支持庞大的客户与合作伙伴群体的零信任环境。每个组织需要考虑如何将本地资源和第三方服务提供商的作用发挥到最大程度，从而依照路线图稳步推进零信任架构的研发和部署工作。

3.3 服务网格

零信任框架的另一项重要技术考量是基于容器实现的服务网格——一种实现配置和管理集中化的架构技术。在现代云计算环境中，容器已经成为首选的应用架构。因为现有的容器已经能以很高的效率部署，所以很有可能在IT架构中大量增加端点数量。如果不使用服务网格技术，将很难实现在跨容器环境广泛部署安全策略的目标。

现在大多数新的容器环境都由Kubernetes，RedHat OpenShift，Docker Swarm，Nomad以及AWS的云容器服务等容器平台提供[23]。容器平台通常不支持容器

[23] ClickIT. (2021, August 5). The most popular Kubernetes alternatives and Competitors. https://www.clickittech.com/devops/kubernetes-alternatives

内通信安全，而服务网格已经发展为支持容器环境下安全地管理、部署和实时业务流的一种解决方案。边车容器（Sidecar Container）或边车进程（Sidecar Process）是实现服务网格的主要方法。边车容器或进程常部署为策略执行点(PEP)，为基于容器的工作负载提供前端安全性保证。Kubernetes集群中的策略执行点应具有高性能和安全代理的特点，用以承担策略执行和安全保护（如web应用防火墙）工作。集中化的配置管理服务可以作为网络安全规则的策略决策点（PDP），通常与访问控制和事件监测模块关联。这种Kubernetes内部架构应该与控制界面和企业的ICAM服务良好地集成，同时支持传统与新兴的认证标准。

将零信任扩展到容器化的微服务端点的一个创新实践是实现一个ISTIO之类的服务网格。ISTIO是一种开源的服务网格搭建方案，提供一种为已部署的服务快捷建立服务网格的方法，对基于Kubernetes的容器化应用产品是透明的[24]。正如美国国防部一号平台（Department of Defense Platform One）所证实的那样，它非常适合支持今天的DevSecOps环节[25]。ISTIO解决方案可以为容器环境提供与NIST零信任架构SP 800-207标准草案一致的零信任架构解决方案。

3.4 边缘计算

基于Kubernetes的新式应用程序架构日渐普及的同时，企业持续将IT基础设施分散部署到多个云服务提供商，对多个部署位置的零信任架构ZTA进行管理的需求将会涌现（如在本地、多云、甚至在最接近用户的网络边缘）。“边缘”(Edge)计算是另一个不断发展的考虑要点，在未来几年，它对于机器人、自动驾驶汽车、增强现实（AR）等互联行业将变得越来越至关重要。由高度分布式应用程序组成的世界将需要现代堆栈中的所有组件。然而，对用户来说，安全且透明的边缘计算将引入加强安全性的需求，例如在分布式应用程序及其应用程序源（云端或本地）的“网格（Mesh）”上建立零信任架构ZTA的能力。这种分布式应用程序的概念可能认为是“边缘 2.0”(Edge 2.0)[26]，考虑到对处理本地遥测和/或双向数据交换请求的传统云基础设施的扩展日趋复杂，它将需要更成熟的ZTA设计。

---

[24] Istio. (n.d.). Istio. Retrieved September 29, 2021, from https://istio.io/

[25] Chaillan, N. (n.d.). How did the Department of Defense move to Kubernetes and Istio? NIST Computer Security Resource Center. Retrieved September 29, 2021, from https://csrc.nist.gov/CSRC/media/Presentations/dod-enterprise-devsecops-initiative/images-media/DoD%20Enterprise%20DevSecOps%20Initiative%20%20v2.5.pdf

[26] Lin, G. (2021, February 8). Edge 2.0 Manifesto: Redefining Edge Computing. F5. https://www.f5.com/company/blog/edge-2-0-manifesto-redefining-edge-computing

3.5 策略即代码

本文最后的技术考虑要点是策略即代码（Policy as Code）的重要性。策略即代码的目标是跨越不同的技术实现统一的策略执行（不局限于云原生）。这一目标通过CI/CD环节以及基于单声明策略的ABAC和RBAC中对合规性和配置自动实施。这使得它非常适合正在尝试零信任架构ZTA成熟化的混合和云环境。

策略即代码实现了一个声明性机制，以执行服务的合规验证和访问规则，通过对部署前检查/测试（企业和/或监管架构）进行标准化评估实现所需的状态运行时控制。这是零信任架构ZTA中包含的一种赋能的技术方法。因为策略是以代码的形式实现的，使用和源代码控制相同的方法，即创建文档化的审计轨迹，因此可根据应用程序和服务接口的严格要求，对定义操作性访问和服务依赖关系的规则进行标记或映射，实现了在云原生环节中编写策略实例化的框架。

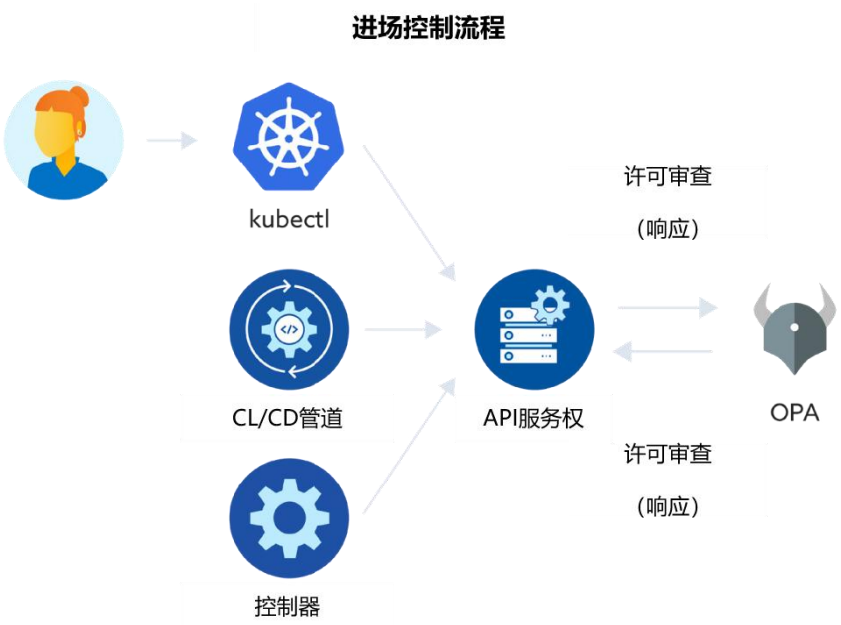

图6. OPA许可控制，CNCF

开放策略代理（OPA）是一个于2018年启动的项目，并于2021年2月通过云原生计算基金会（CNCF）[27]完成，帮助定义和实践策略即代码。如图6所示，OPA实际上是一个准入控制器，也是一个PEP，通过声明性规则引擎和自动化在集成和部署环节中实施特定的需求和检查。OPA可以作为库或守护进程实现，与Kubernetes、API AuthZ和Linux PAM环境集成。在处理每个API请求时，需要执

[27] Cloud Native Computing Foundation. (2021, February 4). Cloud Native Computing Foundation Announces Open Policy Agent Graduation. https://www.cncf.io/announcements/2021/02/04/cloud-native-computing-foundation-announces-open-policy-agent-graduation/

行该策略的应用程序或服务向OPA请求以获得PEP决策。[28]因此，它通过强制访问和配置策略一致性增强ZTA，如图7所示。[29]

图7. OPA支持的ZTA，OpenPolicyAgent.org

3.6 身份感知代理

策略即代码的一个例子是身份感知代理（IAP）。身份和上下文感知是零信任架构ZTA中访问控制的基石；身份、上下文和访问意图结合，也是IAP的基础。IAP要求使用可信的身份根认证用户及其设备，以及用户可以授权访问的内容，这就是身份感知访问。IAP使用代理层提供经认证和授权的对特定资源的安全访问，因此，IAP允许企业使用零信任改造传统网络，在应用程序之前放置一个智能代理执行企业安全策略。

IAP关注于应用层的身份和访问，依赖于访问控制，而不是防火墙规则。配置的策略反映了用户和访问意图，而不是端口和IP地址。此外，IAP基于最小特权访问原则建立了一个中央授权层，并基于每个单独的请求执行访问控制，为零信任提供了实践治理模型。使用IAP，任何访问请求都可被终止、检查或重新检查、修改和授权。

[28] Open Policy Agent. (n.d.). OPA Ecosystem. https://www.openpolicyagent.org/docs/latest/ecosystem/
[29] Open Policy Agent. (n.d.-b). Open Policy Agent. Retrieved September 29, 2021, from

4 对行业的影响

本节将从技术、文化、策略和监管举措等关键性影响方面简要分析解决方案格局的相关影响。尽管这些影响并非详尽无遗，但可以帮助行业利益相关者识别突出的挑战和机遇，需要在每个行业协作领域被持续关注。

4.1 技术

鉴于不断涌现的丰富多样的技术解决方案和功能，选择一个强大健壮的零信任架构ZTA是复杂、丰富并且可憧憬的。 随着IT组织将这些演进的解决方案融合为其零信任架构ZTA的一部分，安全格局将从根本上反映出一种不同的、改进的网络安全方法，因此有可能弯曲成本曲线。这意味着，我们现在有一种潜在的方法，通过更全面的、持续的验证大幅度提高攻击者的成本，从而降低防御者成本。实施零信任架构ZTA 有初始成本，但随着时间的推移，其他技术考虑到其重复性，必要性将降低，甚至完全消除。随着零信任ZT标准的成熟，任何有关经济或商业影响的讨论都需要由行业成员辩论。如此复杂的环境还需要政府就NIST风险管理框架 (RMF) 如何帮助开发和实施提供持续的ZTA指导，如NIST出版的《零信任架构规划：管理员入门指南》[30] 中所示，仍然需要其他行业指南帮助IT和安全专家了解如何评估、评估和统一现有的各种各样的零信任方法。

例如，对于SDP和SDN，为每个组织环境制定对应的SDP正确因素的挑战仍然很突出。例如，SDP的执行边界是在数据、应用程序、平台还是主机级别？在现实中可能会选择混合的解决方案。这种差距将需要更多的行业和政府合作，为组织领导者提供指导，帮助他们为其环境选择合适的因素。无论如何，确保 SDP 越来越成熟对于一个组织机构的零信任架构ZTA来说至关重要。

关于服务网格，未来的服务交付架构将变得更加分散和原子化。虽然 Kubernetes 和服务网格架构通常与正在实施的组件（如容器和sidecar代理）无关，但鉴于当今混合环境中软件和硬件的多样性，将零信任架构ZTA正确应用于容器化应用程序环境，需要对最佳实践进行一定程度的行业标准化。

---

[30] Rose, S. (2021, August 4). Planning for a Zero Trust Architecture: A Starting Guide for Administrators. NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf

一座桥梁用于连接传统硬件或虚拟机基础架构（私有或云端部署）与本地容器环境上的运行组件将是必要的。 行业面临的挑战将是如何允许零信任ZTA的核心组件驻留在本地相对较小运行态（如磁盘和RAM要求）的容器环境中。 作为来自CISA和第三方云集成商的可信互联网连接策略(TIC)演进的一部分，这种开发模式可能值得考虑和指导。

4.2 组织文化

如本文开始所述，行业对于变革的主观倾向性对零信任原则落地来说至关重要。要改变业务和安全文化，需要更深入地了解各种角色。零信任ZT起初对管理员或开发人员来说可能看起来很吓人，会被认为进一步限制了他们的访问权限和执行工作的能力。组织机构将需要支持和培养他们的人才和资源，了解采用零信任ZT原则和技术的好处，以及评估其环境和实施既定路线图的行动。再一次，这将需要行政支持、明确的变更管理流程以及资本和资源投资来设计、评估和实施零信任架构ZTA，活动可能超出当前预算周期。

4.3 策略

在互操作性领域和动态云环境中的管理问题方面策略挑战将继续存在。可见性、上下文和控制对现代组织机构来说将对治理格局形成严峻挑战。值得庆幸的是，今天的零信任ZT原则、框架和架构可以帮助组织机构在这一挑战中的获得进展。首先，随着采用新的角色、流程和技术实现零信任架构ZTA，可能需要修改或制定全组织范围的策略。因为云支持跨组织的多租户，所以产生了新的策略挑战。简言之，有些策略无法在全球范围内实施。此外，随着访问策略和最佳实践的发展，策略逻辑将需要在它们保护的应用程序外部管理，但仍支持集中管理，这是实现管理经济性所必需的。在多租户/多系统所有者环境中，这个概念很复杂，在这种环境中，应用程序开发的演变因DevSecOps环境缓慢发展，烟囱心态占据了主导地位。作为 DevSecOps 流程的一部分，行业将受益于改进的、更自动化和更高效的策略管理解决方案的发展。

策略即代码越来越重要，行业也有很强的驱动力在整个软件供应链中开发和

整合零信任架构ZTA实施方法。DevSecOps和CI/CD环节是应用程序和基础设施的新供应链，并且越来越多地利用容器技术。在软件供应链的CI/CD方法内部和整个过程中，ZTA的实施不容忽视。 现代应用程序有时部分由第三方供应商和开源组件组成，这些组件通常称作“依赖项”。 因此，采用方组织可能对其供应商的供应链知之甚少，并且组织受到越来越多的不同法规的影响，增加了审核新范式（如ZTA）的成本。这可能会减慢采用速度。

即使在边缘计算中，网络安全策略也是通过核心操作系统、网络和云服务实施的。 在强制执行访问、授权和记账(AAA)方面需要有明确的责任。CDN和CSP等提供商严格执行 AAA记账是法规可审计和可验证的方式要求的。 这是“共享责任”的核心，应作为边缘计算环境中ZTA的问责模型继续存在，业界认可这一观点为最佳实践。

4.4 监管环境

目前尚不清楚政府当局是否可以监管安全，但政府政策可以培养对安全的关注并指导投资决策。最近的14028号总统行政令“改善国家的网络安全”[31] 就是为了做到这一点。但是，必须制定政府政策促进和指导网络安全解决方案实施的整体观点的发展。如果不考虑可用的访问、网络和数据安全功能，就不能再将应用程序安全性内置到应用程序中。互操作性和可集成性必须是促进采用零信任ZT原则的策略的标志。从长远来看，仅仅关注解决用户交互，但不解决机器对机器通信的数据流将是不够的。供应链中促进技术烟囱策略只能导致在防御上产生漏洞。

5 建议

本文简要介绍了采用零信任的多样性、复杂性和初期阶段，通过对零信任成熟度、路线图方法，以及对不断发展的零信任场景、及技术、文化、策略和监管因素等的影响的广泛探索。尽管已经提及了多个主题，零信任在安全方面的演变仍是业内正在被经常讨论的话题。为支持全行业采用零信任架构ZTA的下一步行

[31] 国家网络安全卓越中心（n.d）,零信任架构, 美国国家标准与技术研究院 NCCoE, 发布于 2021年9月28日，源自https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

动，本文提出以下建议：

如本文所述，应采用CISA ZTA能力成熟度模型(ZTA-CMM)评估方法。 应使用该方法执行成熟度评估，其评估结果应告知利益相关者如何制定一个具体的、基于优先级的ZTA路线图，以在三到五年的时间内达到目标成熟度水平。 这反过来将有助于提供所需要的资源分配、技术评估或投资等信息，并作为零信任（ZT）路线图和相关企业规划周期的一部分加以考虑。 根据目标成熟度和路线图要求，组织领导者应该在路线图要求中采用“以点到面”的扩展方法。即便在10年后，零信任（ZT）技术、技能和流程的创新仍处于起步阶段。

行业和政府应继续合作，为组织机构提供持续指导，以评估最适合其路线图要求的零信任（ZT）解决方案。 正如本文刚才讨论的内容，政府和行业组织才刚刚开始探索一个复杂且不断发展的环境，以确定能够最好地实现其ZT成熟度目标的解决方案。 然而，随着其中许多解决方案的不断演变发展，评估过程将变得复杂。

因此，**领先的组织机构应继续通过行业论坛分享他们在解决方案评估方面取得的进展**。这将有助于制定在类似环境中适合的ZTA最佳实践。此外，政府和行业的持续合作将有助于加快ZTA的采用并推动行业走向标准化。最近，美国国家网络安全卓越中心（NCCOE）发起了一个实验室项目，帮助评估考量零信任（ZT）的技术选型样本。最近，在本文中引用的政府参考文件（用于指导零信任实施中的RMF要求）是政府如何响应行业诉求的另一个例子。另一个建议采取的行业举措是成立一个国家级CSA零信任工作组，帮助捕捉和整合行业利益相关者的声音，这个丰富的生态环境中将包含组件制造商（硬件/软件）、系统集成商、服务提供商以及更多的相关者。

最后，建议**供应商生态系统重新评估其满足零信任架构ZTA需求范围的能力，包括：从策略自动化到互操作性、控制和上下文的实际技术推动能力。**越能快速识别和分享在零信任领域独特作用的更具透明的解决方案，IT组织就越能更快地吸引早期采用者，不断完善其能力，以实现更安全的国家和全球基础设施。解决方案提供商应积极主动，寻求客户-合作伙伴关系，促进一个全面、轻松的评估周期，支持新的效率，并帮助确定能够在当今时代以低成本为用户提供服务的解决方案。