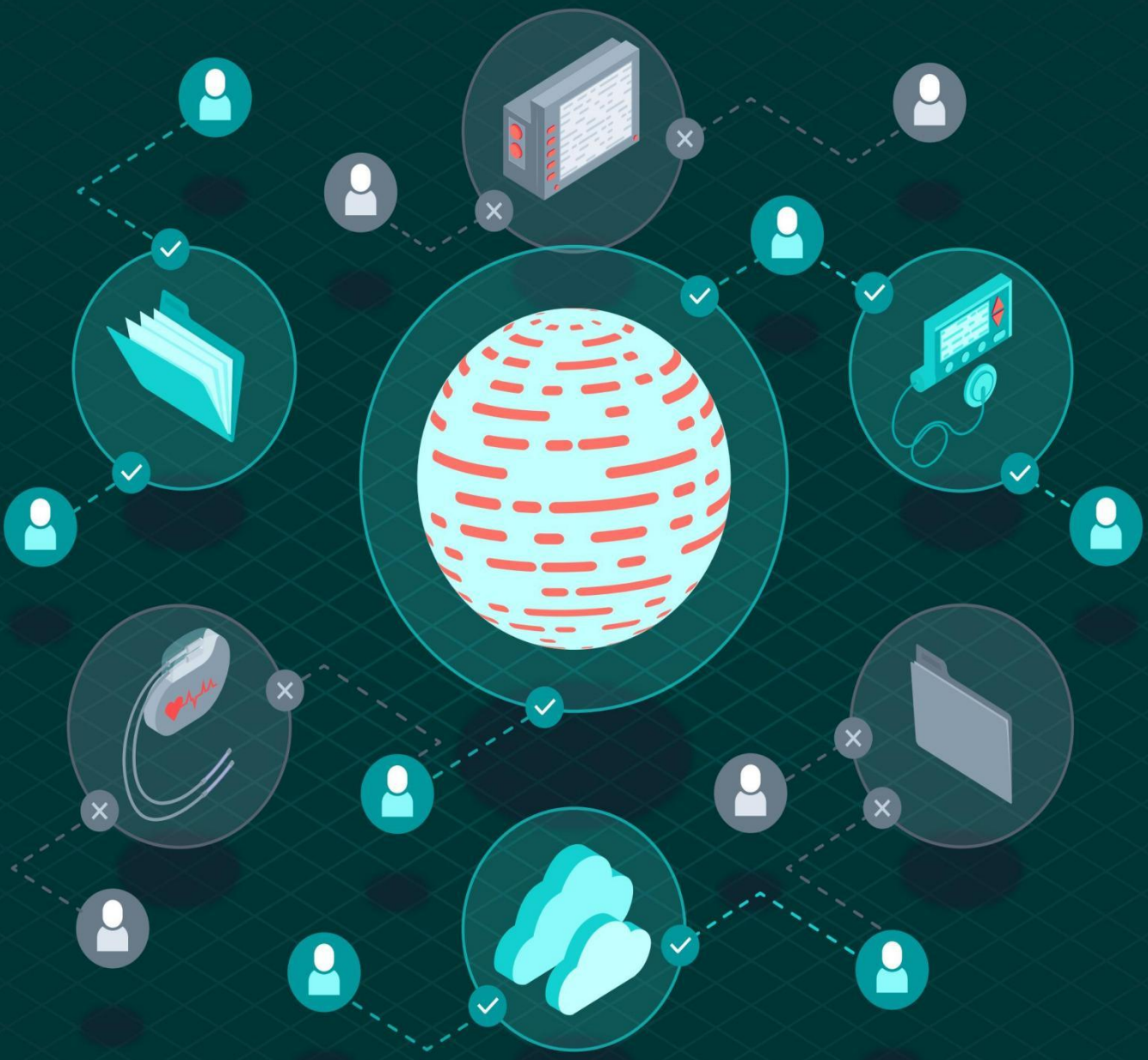
基于零信任架构的医疗设备安全



CSA GCR cloud security GREATER CHINA REGION alliance®

CSA a cloud security alliance®

卫生信息管理(HIM)工作组的常设和正式地点是:

https://cloudsecurityalliance.org/research/working-groups/health-information-management/

联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息

加入我们

CSA大中华区官网
（https://c-csa.cn）

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

《基于零信任架构的医疗设备安全（Medical Devices In A Zero Trust Architecture ）》由CSA工作组专家编写，CSA大中华区零信任工作组组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组 长：

陈本峰　　严强

翻译组：

江楠　　欧建军　　汪海　　王贵宗　　谢琴

审校组：

董雁超　　杨涛

研究协调员：

夏营

感谢以下单位的支持与贡献：

北京启明星辰信息安全技术有限公司　　北京赛虎网络空间安全技术发展有限公司

北京天融信网络安全技术有限公司　　苏州云至深技术有限公司

腾讯云计算（北京）有限责任公司　　湖州市中心医院

英文版本编写专家

主要作者：

Dr. James Angle

贡献者：

Michael Roza　　Wayne Anderson

审校者：

Ashish Vashishtha　　Jennifer Minella (jj)　　David Nance　　Shamik Kacker

CSA员工：

Alex Kaluza

健康信息管理(HIM)工作组旨在直接影响健康信息服务提供商如何向其客户提供安全的云解决方案(服务、传输、应用程序和存储)，并在医疗保健和相关行业的各个方面培养云意识。

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秘书处给予雅正! 联系邮箱research@c-csa.cn；国际云安全联盟CSA公众号。

目录

序言

医疗保健行业正面临着越来越多针对健康信息、医疗设备和关键系统的网络攻击浪潮。随着医疗设备之间的连接日益增多，漏洞继续增多，攻击面在不断扩大。传统的网络安全已经不再足够应付，因为边界防御可以被突破。

为了应对这些风险，医疗机构需要重新思考其安全方案。本文讨论了零信任架构如何增强医疗设备的安全性。零信任消除了对用户、设备和网络流量的隐式信任。相反,它根据细粒度的策略验证和授权每一个访问的尝试。

实施零信任需要解决身份、设备、网络、应用和数据等安全支柱。需要强大的设备发现、监控、微隔离和加密技术。细粒度的访问控制、多因素认证和持续验证为设备和数据流创建了分层保护。

通过全面可视性、最低权限访问和持续监控，零信任最大限度地减少了医疗设备的风险。它假设网络已被入侵，并专注于入侵后的损失遏制。尽管将零信任应用于医疗机器设备存在挑战,但本文概述了医疗机构可以遵循的策略。

采用零信任方法代表了一个范式的转变。随着攻击的增加和复杂化，零信任为医疗服务提供商提供了一条根据消除隐式信任而重塑安全态势的途径。本文旨在成为零信任架构在医疗设备上成功实施的指南。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

概述

确保某个网络的安全首先要了解与之相连的一切事物，包括用户、设备、应用程序、系统，以及访问主体试图访问的数据。 当设备作为访问主体时，整个访问过程的安全性又是怎样的呢？一般来说，安全必须关注最有可能发生威胁之处。 今天的医疗设备经常连接到云端，而威胁和漏洞、技术问题、软件风险和人为因素等各类问题给医疗服务交付组织 (HDO) 带来了攻击面扩大、风险提升的困扰[1]。医疗设备对 HDO 构成了重大安全风险，可能会危及他们的运营和患者数据。 因此，安全架构师被迫重新审视身份的概念。 从本质上讲，每个连接的医疗设备都应有一个身份，并纳入到零信任框架内。[2]

介绍

随着网络攻击的显著增加，医疗健康行业需要确保系统和设备的网络及数据安全。HDO 通常有成百上千个医疗设备连接到医疗网络中，且每个医疗设备本身的软/硬件环境和应用程序存在多个安全漏洞。[3] 其中小到嵌入式设备，大到基于服务器的系统，都无一幸免。 随着 HDO 致力于保护这些设备做出的一系列探索得出结论：一种切实可行的方法就是实施零信任架构 (ZTA)。

从安全的角度来看，医疗保健行业面临极高的风险，每天发生的勒索软件攻击和数据泄露事件的数量就证明了这一点。 受保护健康信息 (PHI) 的系统、医疗设备，甚至保存救生药物和治疗的冰箱都连接到 HDOs 网络， 如果网络发生事故，可能会对整个系统及其患者造成严重破坏。 [4]

传统的网络安全会使用边界隔离的方法，即 HDO 构建强大的外部安全边界并信任边

---

[1] Angle, J., 2020. Managing the Risk for Medical Devices Connected to the Cloud, Cloud Security Alliance, Retrieved from https://cloudsecurityalliance.org/artifacts/managing-the-risk-for-medical-devices-connected-to-the-cloud/
[2] Kumar, S., 2021. Embracing Zero Trust for IoT and OT: A Fundamental Mind Shift, Retrieved from https://www.forescout.com/blog/embracing-zero-trust-for-iot-and-ot-a-fundamental-mind-shift/
[3] Lerman, L., 2021. Zero Trust Approach Can Defend Against IoMT Device Attacks for Healthcare Organizations, Retrieved from https://www.toolbox.com/tech/iot/guest-article/zero-trust-approach-can-defend-against-iomt-device-attacks-forhealthcare-organizations/
[4] McKeon, J., 2021. Exploring Zero Trust Security in Healthcare, How It Protects Health Data, Retrieved from https://healthitsecurity.com/features/exploring-zero-trust-security-in-healthcare-how-it-protects-health-data

界内的网络流量。 这种方法基于一定程度的信任假设，这会使 HDO 更易受到来自内部的网络攻击。 零信任网络是当今的医疗健康企业保持韧性的必备基础。 零信任网络不是建墙，而是建立在五个基本断言之上：

- 网络总被假定是充满攻击者的
- 网络上始终存在内外部威胁
- 网络隔离后也不足以决定该网络可信任
- 每个设备、用户和网络流都需经过身份验证和授权
- 安全策略必须是动态的，并基于尽可能多的数据源来计算[5]

网络上的所有连接和操作都被视为恶意和不可靠的，而边界防护存在默式信任。 换句话说，对所有网络组件应给予“零信任”。 本文将研究 HDO 如何基于零信任成熟度模型对医疗设备实施零信任方案。

零信任成熟度的五个支柱分别是：

- 身份
- 设备
- 网络
- 应用
- 数据

“零信任成熟度模型代表了五个不同支柱的实施梯度，随着时间的推移可以在优化方面不断推进和提升。 如图 1 所示，这些支柱包括身份、设备、网络、应用程序工作负载和数据。 每个支柱都包括关于可见性分析、自动化编排以及治理有关的一般细节。 这种成熟度模型是支持向零信任过渡的通用途径之一。”[6]

[5] Gilman, E. & Barth, D., 2017. Zero Trust Networks: Building Secure Systems in Trusted Networks, O’Reilly Media Inc.
[6] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

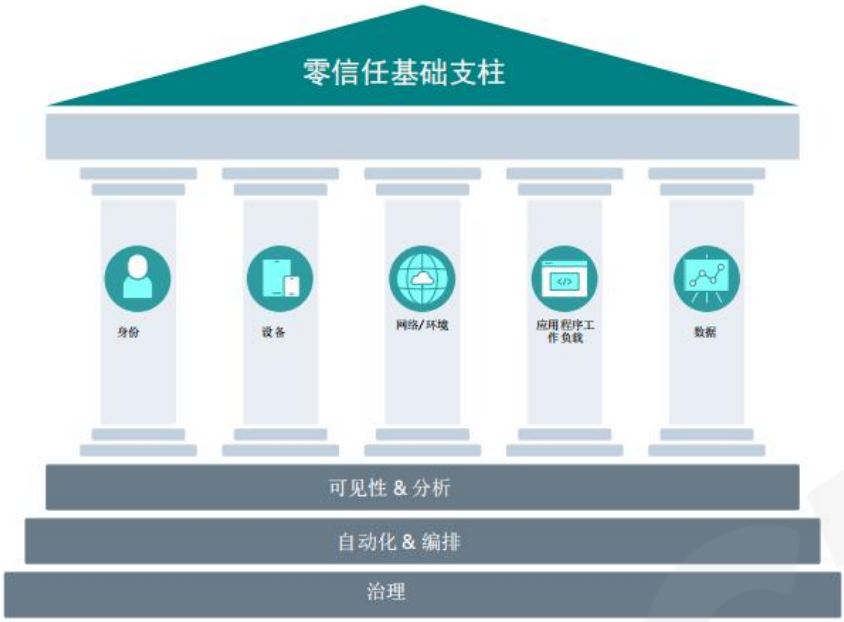


图 1：零信任的基础

以下描述可用于确定每个阶段的不同零信任技术支柱的成熟度，并提供完整一致的成熟度模型：

- **基础：**手动配置和属性分配，静态安全策略、对外部系统具有粗略依赖性的支柱级解决方案，按需配置、最小必要功能、专有且不灵活的策略实施支柱，手动事件响应和缓解部署。
- **进阶：**一些跨支柱协调、集中可见性、集中身份控制、基于跨支柱输入和输出的策略实施，对预定义响应的一些事件响应，对外部系统的依赖关系的细节变动，以及基于风险评估的一些最小特权更改。
- **最佳：**资产和资源的属性完全自动分配，基于自动/观察到的触发器的动态策略配置，具有资产自发现能力以实现阈值内动态的最小权限访问，与跨支柱互操作性的开放标准保持一致，具有可见的历史记录功能以实现可审计的集中式信息汇集。

每个支柱还包括有关该支柱的可见性分析、自动化编排以及治理的有关的通用细节。[7]

[7] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

以下是身份支柱的示例：

功能	基础	进阶	最佳
可见性分析能力	机构根据基本和静态属性来区分用户活动可见性	机构汇总用户活动的可见性，并结合基本属性进行分析和报告，以进行手动优化	机构集中化的用户可见性，基于高保真度属性和用户实体行为分析（UEBA）
自动化编排能力	机构手动管理和编排（复制）身份和凭证	机构使用基本的自动化编排来联合身份，并在身份存储中进行授权管理	机构完全编排身份生命周期，实现动态用户配置文件、动态身份、群组成员资格，并实施实时和足够的访问控制。
治理能力	机构在初始配置后，使用静态技术执行凭证策略（例如，复杂性、重用性、长度、截断、多因素身份验证等），手动审计身份和权限	机构基于策略实施自动化权限调整。不存在共享账户。	机构完全自动化技术层面上的策略执行。机构会更新策略，以映射新的编排选项。

表 1 示例:CISA 成熟度模型身份支柱

通过五个支柱来检验医疗设备安全，将为医疗机构（HDO）提供明确的医疗设备安全状况。[8]

零信任

随着云计算、移动设备和医疗物联网（IoMT）设备的广泛应用，强大的边界防御和定义的网络边界的理念已经消失。此外，如今的工作人员更加分散，远程工作者需要随时随地、在任何设备上进行访问。医疗机构需要为所有资源提供安全访问，无论用户的位置在哪里。

零信任（Zero Trust）原则消除了对设备、主体和网络的信任假设。零信任专注于无论网络位置、主体或资产如何，实施基于风险的访问控制，确保安全访问。它提供了一系列的概念，旨在通过实施严格的访问控制和特权管理，最大程度地减少执行过程中的不确定

[8] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

性[9]。它基于网络已被入侵的假设，所有的访问授权是由信息系统和服务的需要最终决策的。[10]用户只能看到和访问允许他们执行指定任务的基础架构组件。

零信任要求设备健康检查、数据级别的保护、强大的身份架构以及策略级的微隔离，以在医疗机构的数字资源周围创建细粒度的信任区域。零信任实时评估访问请求和通信行为。访问权限不断根据 HDO 的资源进行重新调整。以下图表是美国国家标准与技术研究院（NIST）[11]提供的零信任架构示意图。组织需要实施全面的信息安全和弹性实践，以使零信任有效。在平衡现有的网络安全政策和指南、身份和访问管理、持续监控以及最佳实践的基础上，零信任架构可以防范常见的威胁，提升组织的安全性。

使用风险管理方法的姿态。这可以在介绍或开发过程中提出。[12]

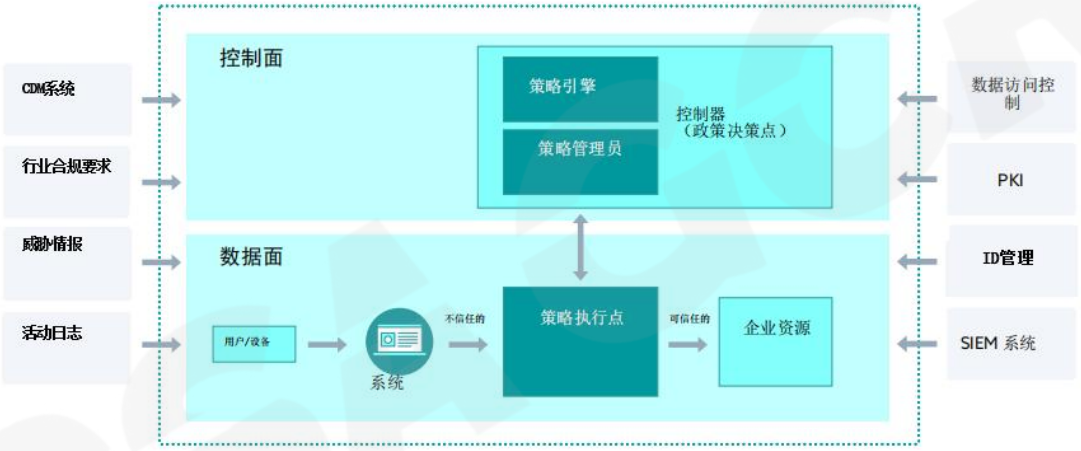


图2:核心零信任逻辑组件

医疗设备管理项目

在讨论为医疗设备实施零信任之前，需要注意的是，由于大多数医疗机构拥有大量设备，尝试手动管理将非常耗时。医疗机构需要工具来管理网络的微细分、执行策略、识别

[9] Rose, S., 2022. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. National Institute of
Standards and Technology, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf
[10] Kumar, S., 2021. Embracing Zero Trust for IoT and OT: A Fundamental Mind Shift, Retrieved from https://www.forescout.
com/blog/embracing-zero-trust-for-iot-and-ot-a-fundamental-mind-shift/
[11] Rose, S., 2022. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. National Institute of
Standards and Technology, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf
[12] https://doi.org/10.6028/NIST.SP.800-207

漏洞，并提供终端检测和响应。

此外，他们还需要一个能够查看所有设备的管理系统。管理系统应提供所有设备及其位置的完整清单。清单应包括对设备进行设备身份识别，以提供足够具体和详细的清单，以便对资源请求进行近实时的有效授权决策。市面上有许多专门用于医疗设备管理系统，这些系统还可以识别与医疗设备相关的漏洞和风险。无论 HDO 选择哪种产品，该产品都应提供医疗设备生态系统的完整图景。

身份

成熟度模型的第一个支柱是身份（Identity）。身份成熟度模型的功能包括身份验证、身份信息存储和身份风险评估。身份是零信任架构的核心组成部分。成熟度模型从简单口令验证转向使用多种因素进行验证，并在所有交互过程中持续验证。身份指的是唯一描述用户或实体的属性或属性集合。

HDO 应确保正确用户和设备在正确的时间能够访问正确的资源[13]。在零信任的环境下，对接入到网络中的设备进行验证，是设备获得信任的一种重要手段。而 IoMT 设备的问题是，它们可能无法像其他网络设备一样进行身份验证。HDO 可能无法利用控制平面验证 IoMT 设备身份，而且 IoMT 设备无法安装可信模块（TPM）。其他一些方法可以为 IoMT 设备提供一定程度的信任。[14]这些方法将在后面“网络”章节部分进行讨论。

在将零信任策略应用于医疗设备之前，HDO 必须知道存在哪些设备及它们的功能，用途和位置。因为 HDO 通常使用的设备数量众多。所以这可能特别具有挑战性。而且，在许多情况下，HDO 可能只知道设备 IP 地址是属于那个子网的。[15]

HDO 需要一种可靠的方法来发现、分类和清点管辖范围内的所有医疗设备。收录的设备信息，应尽可能囊括设备的品牌、功能、位置、应用程序/端口和行为等信息。入网医疗设备是否安全依赖于对其的身份认证。只有经过身份认证入网的医疗设备，才会被视

---

[13] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[14] Gilman, E. & Barth, D., 2017. Zero Trust Networks: Building Secure Systems in Untrusted Networks, O’Reilly Media Inc., Sebastopol CA.

[15] Order White Paper,2022. 5 Steps to Zero Trust for Unmanaged and IoT Devices, retrieved from https://resources.ordr.net/whitepapers/5-steps-to-zero-trust-for-unmanaged-and-iot-devices

为可信的，能够按预期执行操作的。

大多数医疗设备通信都是机器对机器的。小型手持设备通常使用扩展坞连接到工作站，然后再通过网络连接到服务器，如病人监控设备连接到工作站/服务器。对这些设备身份而言，用于管理设备用户的标准化身份标识是不存在的，如某些机器不携带加密令牌来标识身份，并且总是会“记住”任何被告知要记住的内容（例如，通过注入或硬编码密码。这是一种反常规实践的行为）。因此，在 HDO 环境下，身份认证和授权必须基于机器固有的方式，使用安全存储和注入的凭据，联用/或单用证书等机制作为整个过程的一部分。

医疗设备属性应被当做设备安全运行环境信任状态的上下文信息，且设备的安全运行环境信任状态是动态的。医疗设备属性结合设备强标识、运行环境、当前运行条件等信息将被持续地用于判定安全操作环境的安全性。使用医疗设备管理系统可以使 HDO 收集有关每个医疗器械的所有相关信息。这些信息可以用于确定应将哪些策略应用于哪个设备中。此外，医疗设备管理系统可以在零信任环境中充当网络的策略决策点 （PDP），如下图所示。

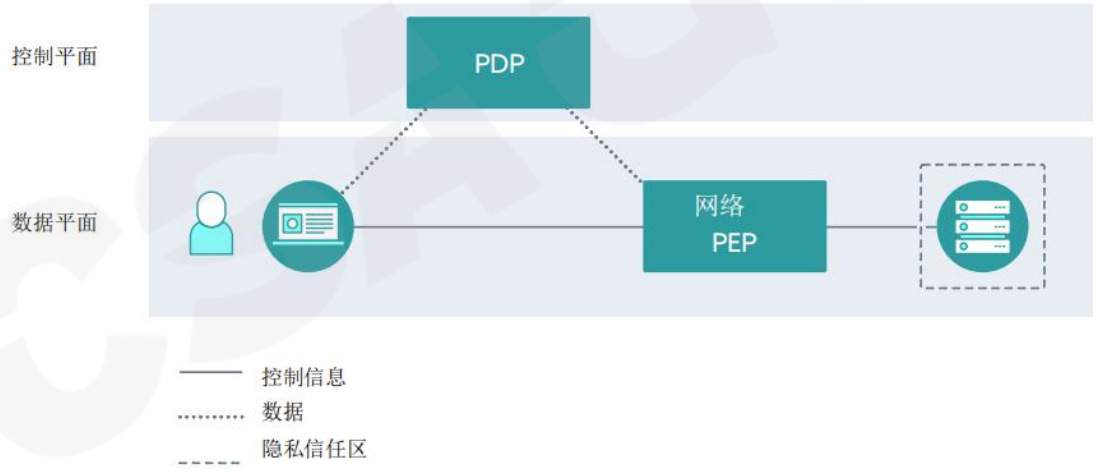


图3: 零信任网络数据流

设备

第二个支柱是设备。设备是可以连接到网络的任何硬件资产，包括 IoMT 设备以及相关管理终端和人机交互终端。设备成熟度模型包括合规监视、数据访问和资产管理三个部分。HDOs 必须确保只有满足安全合规要求的设备才能访问到服务和数据。设备成熟度模

型会将执行策略推向边缘侧的终端设备，以增强向用户直接提供服务和数据的能力，而无需通过传统的人工操作设备进行路由。[16]

虽然联网的医疗设备提高了 HDOs 优质医疗服务的能力，但它们也带来了安全问题，使病人和 HDOs 面临网络安全和信息泄露的风险。以下是联网医疗设备安全管理的一些挑战：

- 缺乏对医疗设备的清晰认知，对其暴露风险没有明确的了解
- 看不见的漏洞产生指数级风险
- 威胁的变化速度超过了 HDO 阻止它们的能力
- 传统安全架构阻碍了合规性的进行
- 未经授权的个人可以物理访问 IoMT 医疗物联网 设备。他们可以篡改设备或从设备中窃取敏感信息。
- IoMT 设备通常无法针对漏洞进行更新或修补。
- IoMT 设备可能无法引入现代化的身份验证方法。

HDO 可以通过对医疗设备行完整和准确的清点梳理和风险评估来应对这些挑战。

- 完整和准确的设备发现和风险评估
- 建议和强制实施最小授权策略
- 持续监控和威胁预防[17]

借助零信任框架，HDO 可以最大限度地降低联网的医疗设备安全风险。以下建议可帮助 HDO 使用零信任措施实现设备安全：

- 编排的可见性：全局可见性实现需要一份全面分析、风险分值动态记录的有关所有托管和非托管的医疗设备清单。全局可见性是指每个设备的安全状况、网络状态、位置和利用率都被详实的记录，并能被查阅。（值得注意的是，检测未经授权的资产行为，不仅需对授权行为有详细的了解，而且要对每类

[16] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[17] Palo Alto Networks, 2022. The Right Approach to Zero Trust for Medical IoT Devices, Retrieved from https://www.paloaltonetworks.com/resources/whitepapers/right-approach-zero-trust-medical-iot

设备的操作要求和工作流程有所分析和了解。）在这基础上，进行相关更改时，正确的数据将会被即刻提供给正确的系统和工作负载。在这种情境下，医疗设备管理系统执行编排操作，仅依赖被动地从网络流量中捕获的设备数据是不够的，还要主动获取保存在其他网络系统中的数据。例如，终端检测和响应系统或者其它上下文处理和响应相关系统的数据。

- 扩展检测和响应（XDR）： XDR 扩展了端点检测和响应能力（提供实时多域检测和编排响应的能力），提高了整个 HDO 环境下威胁的可见性，加速了安全操作，并降低风险。XDR 通常是一个位于云端的集成多种安全产品和数据的工具，能够提供整体的、优越的安全能力。XDR 安全为预防、检测、调查和响应提出了一个高效、主动的解决方案，提供了可见化、安全分析、关联事件警报和自动响应等能力，提高了 HDO 数据安全和打击威胁的水平。
- 动态隔离：为了遏制对网段的破坏，必须快速地创建适当的安全策略，并允许在部署之前进行验证。创建不太复杂的、合理的安全策略一直是医疗保健领域的一项挑战。经过多年发展，医疗设备管理系统现在可以自动生成策略基线。并且，由于这程序知道每个设备的操作要求（例如，内部/外部连接要求、预期的工作流程等）。因此它能够高效自动化地完成这项工作。通过与微隔离的有机结合，管理员可以：
    - 了解设备的标识和关系
    - 模拟安全策略产生的影响
    - 测试底层策略规则的影响并根据需要进行修改
    - 在不中断临床操作的情况下进行研究隔离效果[18]

网络

第三个支柱是网络。网络是指开放的通信媒介，包括内部网络、无线和互联网。网络成熟度模型包括隔离、威胁防护和加密三块内容。HDO 需要根据应用程序工作流的需求

[18] Crowdstrike, 2022. Healthcare IoT Security Operations Maturity: A Rationalized Approach to a New Normal, Retrieved from, https://www.crowdstrike.com/resources/reports/healthcare-iot-security-operations-maturity/

来调整网络隔离和保护，而不是传统网络隔离中固有的隐式信任。[19]

医疗设备的联网是造成安全风险的原因。虽然安全源于设备，但 HDOs 必须设法解决网络拓扑问题。当企业局域网中的设备需要连接其他设备时，它们需要一个标准来识别彼此。这个标准就是 IEEE 802.1X20[20]。通过使用 802.1X 协议能够增强医疗设备的安全性。IEEE 802.1X 是 IEEE 802.1X 工作组定义的一个标准，该标准定义了在有线和无线网络中采用身份验证实现基于端口的访问控制。RADIUS 服务根据用户的凭据或证书进行身份鉴别。

要理解图 4 所示的 802.1X，需要理解三个术语：

- 请求方: 发起认证请求的用户或客户端
- 认证服务器(AS): 实际执行认证的服务器，通常是一个 RADIUS 服务器
- 认证方:请求方与认证服务器之间的设备，如无线接入点

802.1X 的一个好处在于认证方无需大量内存或计算处理能力，这使 802.1X 非常适合无线接入点。[21]

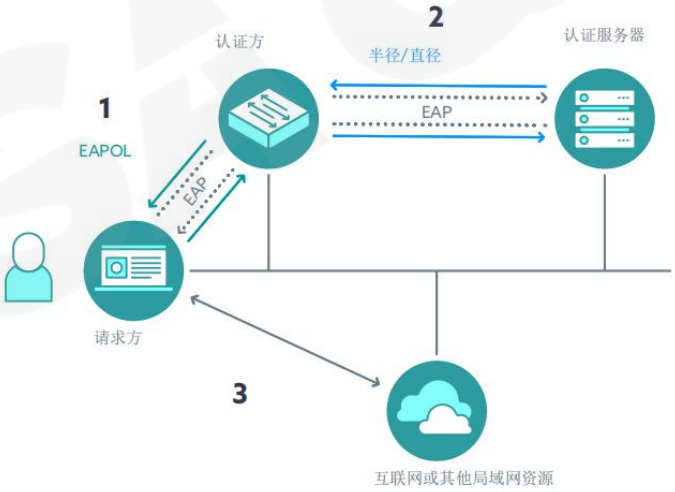


图 4: CCNA 研究指南中基本的 EAP 认证

[19] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[20] Study CCNA.com, 2022. Cisco CCNA Study Notes, Retrieved from https://study-ccna.com/802-1x-authentication/

[21] Fruhlinger, J. and Snyder, J., 2021. 802.1X: What you need to know about this LAN-authentication standard, Network World. Retrieved from https://www.networkworld.com/article/2216499/wireless-what-is-802-1x.html

基本的 EAP 认证方式包括：

- **轻量级 EAP (LEAP):** 认证流程为由客户端提供认证凭据给认证服务器，例如用户名与口令。
- **基于 EAP 的安全隧道(EAP-FAST):** 该方式通过在请求方和认证服务器之间传递一个受保护的访问凭据。
- **受保护的 EAP (PEAP):** 使用内部和外部身份认证。然而，在外部认证中，认证服务器提供一个数字认证给请求方来验证自己的身份。
- **传输层安全 EAP(EAP-TLS):** 认证服务器和请求方通过交换证书相互认证身份。EAP-TLS 只有在无线客户端能够收到和使用数字证书时才是切实有效的。许多医疗类的无线设备，其底层操作系统无法对接 CA 或使用证书。[22]

需要注意的是，并不是所有的医疗设备都可以使用 802.1X 中提供的安全认证方式。在接入边缘侧，最好、最安全的解决方案是利用网络情报。通过 MAC 认证旁路(MAB)，认证服务器可以使用客户端设备的 MAC 地址对其进行认证，而不是通过这里概述的 EAPOL 认证过程。MAB 使用 MAC 地址来确定网络访问级别。MAB 在网络边缘为不支持 IEEE 802.1X 的 IoMT 设备提供可见性和基于身份的访问控制。支持 MAB 的端口可以根据尝试连接的设备的 MAC 地址动态启用或禁用。下面展示了使用 IEEE 802.1X 之前和之后的网络接入情况。

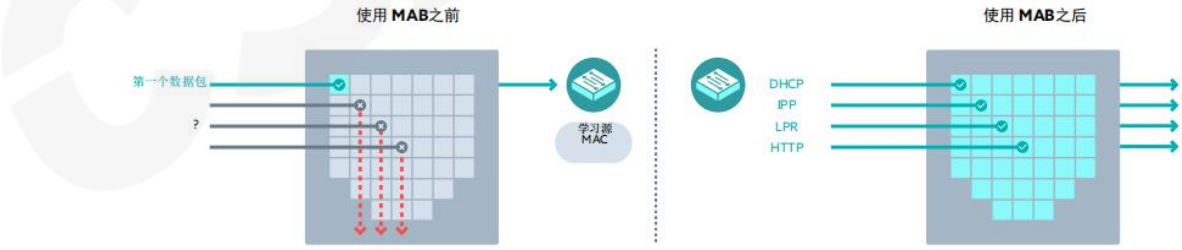


图 5 MAB 前后对比，检索自 Cisco

在 MAB 认证之前，设备的身份是未知的，流量被阻断。交换机检查单个报文，并学习和认证源 MAC 地址。MAB 认证成功后，设备的身份变为已知，来自该设备的流量就被

[22] Study CCNA.com, 2022. Cisco CCNA Study Notes, Retrieved from https://study-ccna.com/802-1x-authentication/

允许通过。[23]

MAB 不能检查除 MAC 地址外的其它身份标识项，这使它不能成为一个安全的身份认证选项，因为 MAC 地址很容易仿冒。使用医疗设备管理系统和微隔离才是安全的。医疗设备管理系统知道设备处于哪个网段，能够识别特定设备的传输通信，更难以仿冒设备。

在 CSA 云安全联盟的 “医疗设备入云的风险管理”白皮书中，强调了医疗设备分段和隔离的重要性。[24]在零信任的环境中，我们需要更进一步实现微隔离。虽然微隔离听起来像是对隔离的一种微小的增量改进，但实际上它代表着整体关注点的重大改变。传统的网络隔离关注的是网络性能和管理。然而，微隔离解决的是安全性和业务敏捷性相关的问题。微隔离是动态变化的 IT 环境中减少风险和自适应安全的强有力方法。微隔离通过将 IT 环境划分为可控的隔离域来解决阻止横向移动的挑战，允许基于应用概念的安全规则，当应用程序和基础设施发生变化时自动重新配置，从而使安全具有动态性。[25]

微隔离创建跨云和数据中心环境的安全域，使工作负载彼此隔离来分别的保证它们的安全。防火墙策略基于零信任安全方法隔离工作负载之间的东西向流量，以减少攻击面，并防止威胁的横向移动以阻止入侵。医疗设备管理系统可以将策略推到策略执行点执行动态策略配置。

所有医疗设备流量都应使用医疗设备管理系统和安全监控与响应软件进行监控。例如：EDR、MDR、NDR 和 XDR。如果发现异常，HDO 可以执行限制横向移动和防止恶意软件和非法活动传播的策略。此外，所有的网络流量都应该被加密。

应用

第四个支柱是应用，包括在本地和云端执行的应用程序。应用程序成熟度模型的功能包括访问授权、威胁防护、可访问性和应用程序安全。HDOs 需要将安全防护与应用工作

---

[23] Cisco, 2011. MAC Authentication Bypass Deployment Guide, Retrieved from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/MAB/MAB_Dep_Guide.html

[24] Angle, J., 2020. Managing the Risk for Medical Devices Connected to the Cloud, Cloud Security Alliance, Retrieved from https://cloudsecurityalliance.org/artifacts/managing-the-risk-for-medical-devices-connected-to-the-cloud/

[25] Friedman, J., 2017. The Definitive Guide to Micro-Segmentation, Illumio. Retrieved from https://www.illumio.com/lp/definitive-guide-to-micro-segmentation

流紧密结合起来，以确保具有提供足够的安全所需的可见性和理解力。[26]

确保医疗设备应用程序的安全性是防止设备被攻击的关键。零信任安全模型可以做到这一点，但零信任不是一个产品，而是一种可以转化为安全的网络和应用架构的方法和准则。本质上，它是一个解决方案生态系统的融合，能够确保默认情况下没有任何内部或外部的用户或设备是被信任的，在获得应用程序访问权限之前需要进行验证。为保护医疗设备应用，需要进行以下操作。[27]

- 访问前进行身份认证：这涉及到构建零信任环境，以便内部和外部用户在授权之前不能进行访问，从而减少设备和应用被破坏的机会。
- 最小权限访问模型：设备连接应基于最小权限的策略。为此，HDO 必须确定用户试图完成什么、正在访问的服务类型以及所需的通信协议。一旦确定，就可以验证是否应该根据当前情况允许访问。即使授予了访问权限，也应该使用规定的通讯方式访问。[28]
- 微隔离：微隔离允许企业简单地将物理网络划分为逻辑网络分段，然后进行保护，通过仅允许已授予访问权限的人员查看数据来降低风险。微隔离旨在使攻击面尽可能小，同时防止未经授权的横向移动。传入应用进程请求的来源应纳入授予的访问权限级别和类型的计算中。[29]
- 持续验证/监控：在向特定用户在特定设备上及特定位置上提供应用进程访问权限后，需要持续监控，以便在风险级别发生变化时可以终止连接以最大程度地降低风险。医疗设备管理进程和 XDR 支持从网络级别进行监控，这是检测和响应异常的关键。

此外，无论是内部还是外部访问的动态和静态数据加密对于应用进程安全性都至关重

---

[26] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf
[27] F5, 2022. Zero Trust in an Application-Centric World, Retrieved from https://www.f5.com/services/resources/use-cases/zero-trust-in-an-application-centric-world
[28] Bomba, M., 2021. Basic Zero Trust Principles for Application Security, Retrieved from https://kemptechnologies.com/blog/zero-trust-application-security
[29] Cigniti, 2022. Implement Zero Trust to secure your applications, Retrieved from https://www.cigniti.com/blog/zero-trustsecure-applications/

要。[30]

数据

第五个支柱是数据。数据应该在设备、应用进程和网络上受到保护。数据成熟度模型功能是资产管理、访问决策和加密。 HDO 应该采用以数据为中心的安全方法。 HDO 需要识别、分类和清点所有数据资产。[31]

医疗设备产生大量的面向各种用途的电子保护健康信息(ePHI)，这些信息数据用于诊断、监测和治疗患者，有助于提供安全有效的医疗保健。此外，这些数据还可用于人口健康和预防分析的大数据分析。这些数据在传输和静止时都必须得到保护。在零信任环境中，必须标识敏感数据、映射所有数据流和标识所有存储。

零信任框架下的数据使用是基于颗粒化的访问控制。零信任数据管理侧重于基于零信任原则的基础、以数据为中心的网络空间安全方案。无论数据位于何处，数据都受到保护，对单个 HDO 资源的访问基于单个会话，动态策略通过对所有数据源的访问控制来保护企业业务。通过不断地对数据进行核算，并建立与位置、特权、应用程序需求和行为相匹配的信任区域和访问控制，可以实现所有数据的管理可见性。

在零信任架构中使用异常检测和机器学习的预测分析记录所有访问尝试，并分析这些异常行为或可疑活动的尝试。由于系统可以识别任何异常，自动拒绝访问请求并发出警报，因此 HDO 可以主动防御攻击。[32]

在零信任环境中，数据使用需要考虑多个阶段。数据可以是静态、动态或使用中的数据。这些阶段中的每一个都对数据管理和安全性提出了挑战。

数据保护从控制访问开始。访问控制应确定谁可以查看数据、更改数据以及删除数据，并且必须确定和强制实施。但在此之前，静态数据应该被加密。此外，传输中的所有数据都必须加密。

---

[30] Bomba, M., 2021. Basic Zero Trust Principles for Application Security Retrieved from https://kemptechnologies.com/blog/zero-trust-application-security

[31] Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved from https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

[32] Ross, J., 2022. The Zero Trust Approach to Data Management, Retrieved from https://thenewstack.io/the-zero-trustapproach-to-data-management/

HDO 应采用数据丢失防护（DLP）解决方案。DLP 解决方案围绕以下元素提供控制：

- 设备控制：在设备级别定义如何使用数据的方法
- 内容感知控制：根据数据内容实施和调整控制
- 强制加密：确保静态数据已加密
- 数据发现：提供查找敏感数据的方法

在零信任中，数据是需要保护的资源。这意味着所有数据访问都必须通过 PDP 和 PEP，以确保执行以身份为中心的架构的安全。[33]

结论

医疗设备的安全防护使零信任安全更具挑战性；但是，如果可以正确实施必然会增强 HDO 的设备安全性。如果使用医疗设备管理系统来识别和追踪所有设备，HDO 可以将该程序用作 PDP。PDP 可以帮助控制访问，并确保使用正确的策略。微隔离允许 HDO 完全控制数据流，并可以防止可疑活动的横向移动。端点保护和 XDR 增强了早期检测和响应；使用 DLP 可以减少数据丢失的机会。

这些安全工具以及 HDO 当前的安全工具，将提供一个安全的零信任环境。在此环境中，所有设备都被识别，并且所有访问都受到限制和控制。所有数据都经过加密，并且位置都是已知的。访问控制、隔离和持续监视的组合提供了一个良好环境，可在其中识别漏洞，并在可以修复设备漏洞之前采取缓解控制措施。虽然 HDO 无法消除风险，但零信任目前提供了最好的安全性。

[33] [1] Garbis, J. & Chapman J. W., 2021. Zero Trust Security: An Enterprise Guide, Apress Media, California.

参考资料

Angle, J., 2020. Managing the Risk for Medical Devices Connected to the Cloud, Cloud Security Alliance, Retrieved from https://cloudsecurityalliance.org/artifacts/managing-the-risk-for-medical- devices-connected-to-the-cloud/

Bomba, M., 2021. Basic Zero Trust Principles for Application Security, Retrieved from https://kemptechnologies.com/blog/zero-trust-application-security

Cigniti, 2022. Implement Zero Trust to secure your applications, Retrieved from https://www.cigniti.com/blog/zero-trust-secure-applications/

Cisco, 2011. MAC Authentication Bypass Deployment Guide, Retrieved from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/MAB/MAB_Dep_Guide.html

Crowdstrike, 2022. Healthcare IoT Security Operations Maturity: A Rationalized Approach to a New Normal, Retrieved from, https://www.crowdstrike.com/resources/reports/healthcare-iot-security- operations-maturity/

Cybersecurity & Infrastructure Security Agency, 2021. Zero Trust Maturity Model, retrieved fromhttps://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

F5, 2022. Zero Trust in an Application-Centric World, Retrieved from https://www.f5.com/services/resources/use-cases/zero-trust-in-an-application-centric-world

Friedman, J., 2017. The Definitive Guide to Micro-Segmentation, Illumio. Retrieved from https://www.illumio.com/lp/definitive-guide-to-micro-segmentation

Fruhlinger, J. and Snyder, J., 2021. 802.1X: What you need to know about this LAN-authentication standard, Network World. Retrieved from https://www.networkworld.com/article/2216499/wireless- what-is-802-1x.html

Garbis, J. & Chapman J. W., 2021. Zero Trust Security: An Enterprise Guide, Apress Media, California.

dio.org/10.1007/978-1-4842-6702-8

Gilman, E. & Barth, D., 2017. Zero Trust Networks: Building Secure Systems in Trusted Networks, O'Reilly Media Inc. Sebastopol, CA.

Kumar, S., 2021. Embracing Zero Trust for IoT and OT: A Fundamental Mind Shift, Retrieved from

https://www.forescout.com/blog/embracing-zero-trust-for-iot-and-ot-a-fundamental-mind-shift/

Lerman, L., 2021. Zero Trust Approach Can Defend Against IoMT Device Attacks for Healthcare

Organizations, Retrieved from https://www.toolbox.com/tech/iot/guest-article/zero-trust-approach- can-defend-against-iomt-device-attacks-for-healthcare-organizations/

McKeon, J., 2021. Exploring Zero Trust Security in Healthcare, How It Protects Health Data, Retrieved from https://healthitsecurity.com/features/exploring-zero-trust-security-in-healthcare-how-it- protects-health-data

Order White Paper,2022. 5 Steps to Zero Trust for Unmanaged and IoT Devices, retrieved from

https://resources.ordr.net/whitepapers/5-steps-to-zero-trust-for-unmanaged-and-iot-devices

Palo Alto Networks, 2022. The Right Approach to Zero Trust for Medical IoT Devices, Retrieved from

https://www.paloaltonetworks.com/resources/whitepapers/right-approach-zero-trust-medical-iot

Rose, S., 2022. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. National Institute of Standards and Technology, Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf

Ross, J., 2022. The Zero Trust Approach to Data Management, Retrieved from https://thenewstack. io/the-zero-trust-approach-to-data-management/

Study CCNA.com, 2022. Cisco CCNA Study Notes, Retrieved from https://study-ccna.com/802-1x-authentication/

CSA GCR cloud security alliance
GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905