CSA GCR cloud security GREATER CHINA REGION alliance ®

NIST特别出版物800-207（正式版）

零信任架构
Zero Trust Architecture

NIST

National Institute of Standards and Technology
U.S. Department of Commerce

美国国家标准与技术研究院
美国商务部

云安全联盟大中华区翻译

2020年9月

中文翻译版说明

本文档由云安全联盟大中华区（CSA GCR）SDP 工作组专家对 NIST（美国国家标准与技术研究院）的《零信任架构》白皮书进行翻译审校。

翻译审校工作专家：

组长：陈本峰（云深互联）

组员：陈智雨（国网信通公司）、邓辉（吉大正元）、靳明星（易安联）、王永霞（腾讯云）、魏小强（360）、闫龙川（国网信通公司）、于继万（华为）、余晓光（华为）、余强（中宇万通）、袁初成（缔安科技）、郑大义（万物安全）、崔泷跃、高巍、何国锋、刘洪森、王贵宗、姚凯、于乐、周杰

CSA 大中华区研究助理：高健凯

正式版：陈本峰（云深互联）、高巍、高健凯

贡献单位：缔安科技、国网信通公司、华为、吉大正元、360、腾讯云、万物安全、易安联、云深互联、中宇万通

特别感谢

奇安信、云深互联、字节云智为本次翻译提供草稿版翻译文档。

在此感谢以上参与翻译审校工作的专家们以及工作人员。如译文有不妥当之处，敬请联系 CSA GCR 秘书处给予雅正！联系邮箱：info@c-csa.cn 。

授 权

本文档由 NIST 根据美国 2014 年《联邦信息安全现代化法案》（FISMA）（美国《法典》第 44 卷，第 3551 节，第 113-283 条）规定的法定职责开发。NIST 负责制定信息安全标准和指南，包括联邦信息系统的最低要求，但未经对此类系统行使政策权力的相关联邦官员的明确审批，此类标准和指南不应用于国家安全系统。该准则符合管理和预算办公室第 A-130 号通知的要求。

本文档中的任何内容都不应被视为与商务部长根据法定授权而对联邦机构强制和具有约束力的标准和准则相抵触。也不应将这些准则解释为改变或取代商务部长、监事会主任或任何其他联邦官员的现有权力。本文档可由非政府组织自愿使用，在美国不受版权限制。使用请注明出处，NIST 将对此表示感谢。

国家标准与技术研究院特别出版物 800-207

国家标准与技术研究院特别出版物 800-207， 总 59 页（2020 年 8 月）

分类编号: NSPUE2

本文档可从以下地址免费获取：

https://doi.org/10.6028/NIST.SP.800-207

本出版物中可能会涉及某些商业实体、设备或材料，以便充分描述实验程序或概念。这并非暗示被NIST推荐或认可，也不意味着这些实体、材料或设备一定是最佳选择。

本出版物可能会涉及NIST根据其法定职责正在编写的其他出版物。本出版物中的信息，包括概念和方法，可能会在这些配套出版物完成之前就被联邦机构使用。因此，在每份出版物完成之前，现行的要求、准则和程序（如果存

在）仍然有效。出于规划和过渡的目的，联邦机构不妨密切关注NIST这些新出版物的发展。

欢迎各组织在公众意见征集阶段审阅所有出版物草案，并向NIST提供反馈。请访问以下地址获得NIST其他网络安全出版物信息：https://csrc.nist.gov/publications。

关于本出版物的意见可提交至：

国家标准与技术研究院

地址：先进网络技术处信息技术实验室

盖瑟斯堡市 Bureau Drive 路 100 号（邮递站 8920），马里兰州 20899-8920

电子邮件: zerotrust-arch@nist.gov

所有反馈意见均根据《信息自由法》（FOIA）予以发布

计算机系统技术报告

美国国家标准与技术研究院（NIST）的信息技术实验室（ITL）通过引领国家测量和标准基础，促进美国经济和公共福利。信息技术实验室通过开发测试、测试方法、参考数据、概念证明实施和技术分析，以推进信息技术的发展和生产使用。信息技术实验室的责任包括制定管理、行政、技术和物理标准和指南，以在联邦信息系统中为与国家安全相关的信息以外的其他信息提供具有成本效益的安全和隐私。特别出版物 800 号系列报告，介绍了信息技术实验室在信息系统安全方面的研究、指南和外联工作，以及与工业界、政府和学术组织的合作活动。

摘要

零信任（Zero Trust，缩写 ZT）是一组不断演进的网络安全范式，它将网络防御的重心从静态的、基于网络的边界转移到了用户、设备和资源上。零信任架构（ZTA）使用零信任原则来规划企业基础设施和工作流。零信任取消了传统基于用户的物理或网络位置（即，相对公网的局域网）而授予用户帐户或者设备权限的隐式信任。认证和授权（用户和设备）是与企业资源建立会话之前执行的独立步骤。零信任顺应了企业网络发展的趋势：位于远程的用户和基于云的资产，这些资产都不位于企业拥有的网络边界内。零信任的重心在于保护资源，而不是网段，因为网络位置不再被视为资源安全与否的主要依据。本文档包含零信任架构（ZTA）的抽象定义，并给出了零信任可以改进企业总体信息技术安全状况的通用部署模型和使用案例。

关键词

架构；网络空间安全；企业；网络安全；零信任

致谢

本文档是多个联邦机构合作的成果，由联邦首席信息官委员会监督。架构组负责本文档的开发，同时一些专家的贡献有目共睹。其中包括联邦首席信息官委员会 ZTA 项目的项目经理 Greg Holden、NIST/国家网络安全卓越中心 ZTA 项目的项目经理 Alper Kerman,以及 Douglas Montgomery。

读者

本文档旨在为企业安全架构师介绍零信任理念。它旨在帮助理解民用非保密系统的零信任，并为移植和部署零信任安全概念到企业环境提供路线图。网络安全经理、网络管理员和管理者也可以从本文档中了解零信任概念及其架构。由于企业会具有需要保护的独特业务用例和数据资产，因此本文档并非 ZTA 的单一部署计划。对组织业务和数据的充分理解会有利于零信任的有效建立。

商标信息

专利公开声明

声明：信息技术实验室（ITL）已要求其专利要求的持有人向 ITL 公开这些专利要求，因为要遵守本文档的指导或要求，可能需要使用这些专利。然而，专利持有人没有义务响应 ITL 的专利要求，ITL 也没有进行专利检索以确定哪些专利（如有）可能适用于本文档。

在 ITL 呼吁确定其使用可能需要符合本文档指南或要求的专利权利要求后，已收到一项或多项此类权利要求的通知。

通过本文档，ITL 对任何专利权利要求或与之相关的任何权利的有效性或范围不采取任何立场。然而，已知的专利持有人已经向 NIST 提供了一封保证信，信中说明：(1)它(他们)没有持有且目前也不打算持有任何基本专利权利要求的一般免责声明；或(2)它(他们)将在明显的非歧视性基础上与其他方就合理的条款和条件进行免版税或含版税的许可进行谈判。

详情可从 zerotrust-arch@nist.gov 获取。

但这不代表或暗示使用本文档时避免专利侵权问题所需的唯一授权许可。

序 言

零信任代表着业界正在演进的网络安全最佳实践，它的思路是把防御从依靠网络边界的马其顿防线向个体保护目标收缩。把防护重心从网段转移到资源本身后，当今企业面临的安全挑战得以缓解，比如远程访问与云资源使用这些离开了企业网络边界的应用场景。

美国国家标准与技术研究院 NIST 认识到向零信任架构的转型是漫长的旅程而不是简单的置换企业现有基础设施，预计大部分企业将以混合模式（即零信任模式与传统模式）运作很长时间。零信任模式并不是一个单一的网络架构或技术产品，它是一套理念、战略、架构，NIST 在本书提出的零信任架构属于参考架构，对零信任的解决方案如 ZT-IAM，SDP，MSG 的部署与整合起到指导作用。

很高兴 CSA 大中华区的专家们参与了 NIST 这项标准工作的起草、评审、翻译，大中华区研究院贾良玉等参与了英文原著的设计与评审，大中华区 SDP 工作组陈本峰等对本文做了深入解读并翻译成为中文，这是 CSA 与 NIST 长期合作的又一项重要成果，感谢 NIST 本工作组进行原创的专家们和 CSA 大中华区进行翻译的专家们。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

1 介绍

企业的典型 IT 基础设施变得越来越复杂。一家企业可能运营多个内部网络，拥有本地基础设施的分支机构，远程办公接入和/或移动办公的个人，以及云上的服务。这种复杂性已经超越了传统基于边界防御的网络安全策略，因为没有单一的、可以清晰辨别的企业边界。此外，基于边界防御的网络安全控制已显示出明显的不足，一旦攻击者突破了边界，进一步的横向攻击将不受阻碍。

这种复杂性导致了新的网络安全理念及模型的出现，即“零信任（ZT）”。典型的零信任，主要关注于数据保护，但可以(且应该)被扩展到包括所有的企业资产（设备、基础设施组件、应用程序、虚拟化和云组件）以及主体（最终用户、应用程序和其他请求资源信息的非人类实体）。在本文中将使用 "主体"泛指请求资源信息的角色，除非有些段落中特指人类用户，则会以"用户"指代。零信任安全模型假设网络上已经存在攻击者，并且企业自有的网络基础设施（内网）与其他网络（比如公网）没有任何不同，不再默认内网是可信的。在这种新模式中，企业必须连续进行分析和评估其内部资产和业务功能可能面临的风险，然后采取措施减轻这些风险。在零信任状态下，这些保护通常涉及对资源（例如数据、计算资源和应用程序）的最小化授权访问，仅提供给那些被识别为需要访问的用户和资产，并且对于每个访问请求持续进行身份和权限的验证。

零信任架构（ZTA）基于零信任理念的企业网络安全战略，目的是防止数据泄露并限制内部横向移动攻击。本文讨论 ZTA 的逻辑组件、常见的部署方案以及面临的威胁。它还为希望将网络基础设施迁移到零信任设计的组织提供了总体

路线图，并讨论可能对零信任战略造成影响的相关联邦政策。

零信任不是单一网络体系结构，而是网络基础设施中的一组指导原则以及系统设计和运营方法，可用于改善任何类型或敏感度等级的安全状况[FIPS199]。过渡到 ZTA 是一段过程，与一个组织如何评估其任务中的风险相关，无法简单地通过技术替代来完成。也就是说，许多组织已经在他们今天的企业基础设施中拥有部分零信任元素。组织应寻求逐步达成零信任的原则，完成流程更改和技术解决方案，以保护其数据资产和应用的业务功能。大多数企业的基础设施将以零信任/传统边界安全的混合运行的模式，同时持续进行 IT 现代化改造和业务流程改善。

为了使零信任有效落地，组织机构需要实施全面的信息安全和弹性的控制措施。在兼顾现有的网络安全策略和指南、访问管理、持续监控和一些最佳实践的同时，ZTA 策略可以通过风险管控策略来防范常见威胁，并改善组织的安全状况。

1.1 与联邦机构有关的零信任历史

零信任的概念早在“零信任”一词出现以前就一直存在于网络安全领域之中。国防信息系统局（DISA）和国防部（DoD）最早发布了他们的更安全的企业战略研究工作，称为“黑核”[BCORE] 。黑核提倡从基于边界防御的安全模型转变为基于用户操作行为的安全模型。1994 年的耶利哥论坛（Jericho Forum）也提出了去边界化的网络安全概念，指出大型网络中单一静态防御的局限性以及应该去除基于网络位置的隐式信任 [JERICHO]。这种去边界化的思想后来演进成为约翰·金德瓦格（John Kindervag）在 Forrester 报告中提出的更大的零信

任概念。零信任便成为一个专用词汇，用来描述从基于网络位置的隐式信任安全模型转移到基于用户行为的持续信任评估安全模型。私营企业和高等学校教育也都拥抱了这一安全模型的演进，从基于边界的安全转换到了基于零信任理念的安全。

自十多年前，美国联邦机构已经开始积极地迁移到基于零信任理念的网络安全。联邦机构一直在建设相关的能力和政策，从《联邦信息安全管理法》(FISMA)开始，然后是风险管理框架（RMF）、联邦身份、凭证和访问管理（FICAM）、可信互联网连接（TIC）、持续诊断和缓解（CDM）计划。所有这些计划都旨在限制被授权方的对于数据和资源访问。这些计划最初启动时，因受限于信息系统的技术能力，安全策略大部分是静态的，只能在强制在企业比较大的“瓶颈”点上执行以获得最佳效果。但随着技术的成熟，对于每个访问请求进行持续的、动态的、和细粒度的分析和评估成为可能，这种“按需授权”的安全策略可以有效缓解由于被盗账号、黑客网络监听等各种威胁造成数据泄露事故。

1.2 本文结构

本文的结构如下：

- **第 2 节**定义了零信任（ZT）和零信任架构（ZTA），并列出了为企业建立零信任架构的一些假设。本节还包括了零信任设计原则的列表。
- **第 3 节**描述 ZTA 的逻辑组件或构成模块。以不同的方式组合 ZTA 组件以获得不同的实现方式并提供相同的逻辑功能是有可能的。
- **第 4 节**列出了 ZTA 一些可能的应用场景。这些 ZTA 应用场景让企业环境更

安全，更难被入侵，包括远程员工、云服务和访客网络等。

- **第 5 节**讨论 ZTA 环境下企业会面临的威胁。其中许多威胁是与传统的架构网络下的威胁相似，但可能需要不同的防御技术。
- **第 6 节**讨论 ZTA 原则如何适用和/或补充联邦机构现有的合规要求。
- **第 7 节**介绍企业机构（例如联邦政府）过渡到零信任架构的着手点。这里面包括部署以零信任理念为纲领的应用程序和企业基础设施所需的常见步骤。

2 零信任基本概念

零信任是一种以资源保护为核心的网络安全范式，其前提是信任从来不应该被隐式授予，而是必须进行持续地评估。零信任体系架构是一种针对企业资源和数据安全的端到端方案，其中包括身份（人和非人的实体）、凭证、访问管理、操作、终端、主机环境和互联基础设施。初始的重点应该是将资源访问限制在有实际访问需求的主体并仅授予执行任务所需的最小权限（如读取、修改、删除）。传统上，组织机构（和一般的企业网络）专注于边界防御，合法认证用户被授予广泛的资源访问权限。因此，网络内未经授权的横向攻击一直是联邦政府面临的最大挑战之一。

可信 Internet 连接（TIC）和边界防火墙提供了强大的互联网网关。这有助于阻止来自互联网的攻击者，但它们在检测和阻止来自网络内部的攻击方面用处不大，并且也无法保护边界外的用户（例如，远程工作者、基于云的服务）。

关于的零信任（ZT）和零信任架构（ZTA）通俗的定义如下：

零信任（Zero Trust，ZT）提供了一系列概念和思想，在假定网络环境已经被攻陷的前提下，当执行信息系统和服务中的每次访问请求时，降低其决策准确度的不确定性。零信任架构（ZTA）则是一种企业网络安全的规划，它基于零信任理念，围绕其组件关系、工作流规划与访问策略构建而成。因此，零信任企业是作为零信任架构规划的产物，是针对企业的网络基础设施（物理和虚拟的）及运营策略的改造。

一个企业决定采用零信任作为它的网络安全基准原则，就需时刻将零信任架

构作为一个基本原则进行规划。然后以此计划部署一个零信任环境供企业使用。

此定义聚焦的问题关键包括：消除对数据和服务的非授权访问，以及使访问控制的执行尽可能精细化。也就是说，授权过和经批准的主体（用户、应用、和设备的组合）可以访问数据，同时排除其他所有主体（例如，攻击者）。进一步讲，可以用"资源"一词代替"数据"，从而变为 ZT 和 ZTA 对资源进行访问（例如打印机、计算资源、IoT 执行器等），而不仅仅是数据访问。

为了达到降低不确定性的目的（因为它们不能完全消除），重点是通过身份验证、合法授权和缩小隐含信任区域，同时最小化认证机制中的时间延迟来实现。访问规则被限制为最小权限，并尽可能细颗粒度。

在图 1 的抽象模型中，当主体需要访问企业资源时，其需要通过策略决策点（PDP）和相应的策略执行点（PEP）授予访问权限。

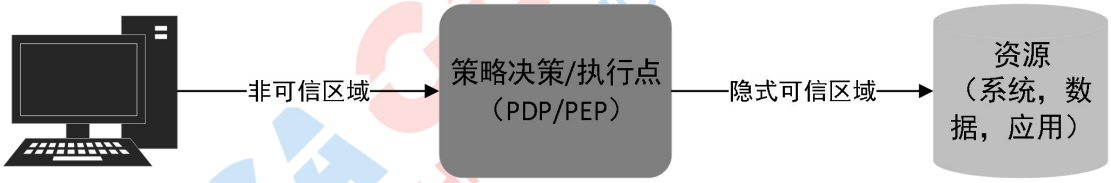

图 1：零信任访问

零信任访问系统必须确保用户可信且请求合法。PDP/PEP 会做出合适的判断以允许主体访问资源。这意味着零信任适用于两个基本领域：身份验证和授权。对于某个单一的请求，用户的身份的信任等级是什么级别？考虑到对用户身份的信任等级，是否允许访问资源？用于请求的设备是否具有正确的安全状态？是否有其他因素需要考虑，这些因素可能改变信任等级（如时间、主体位置、主体安全状态）？总体而言，企业需要为资源访问制定和维护基于风险的动态策略，并

建立一个系统来确保这些策略得到正确和一致的执行。这意味着企业不应依赖于隐含的可信性。所谓隐含可信性是指：如果用户满足基本身份验证级别（如，登录到某个资产），则假定所有资源请求都同样合法。

“隐含信任区”表示一个区域，其中所有实体都至少被信任到最后一个 PDP/PEP 网关的级别。例如，可以参考机场的乘客安检模型。所有乘客通过机场安检点（PDP/PEP）进入登机口。乘客可以在候机区内闲逛，所有通过检查的乘客都被认为是可信的。在这个模型中，隐含信任区域是登机区。

PDP/PEP 采用一系列的控制策略，使得所有通过检查点之后的通信流量都具有一个共同信任级别。PDP/PEP 不能对访问流量使用超出其位置的策略。为了使 PDP/PEP 尽可能明确，隐含信任区必须尽可能小。

零信任架构提供了一套原则和概念，使得 PDP/PEP 更接近资源。其思想是显式地验证和授权企业的所有用户、设备、应用程序和工作流。

2.1 零信任原则

关于零信任的许多定义和讨论都强调去除以广域边界防御（如企业防火墙等）为因素的概念。然而，大多数的概念仍然以某种方式定义自己与边界的关系（例如微隔离或微边界，请参阅章节 3.1），并把边界作为零信任架构的一部分。以下是根据应引入而非排除的方式来定义 ZT 和 ZTA 的基本原则。这些原则是理想的目标，同时必须承认并非所有的原则都可以在给定的战略中以其最纯粹的形式充分实施。

零信任架构的设计和部署遵循以下基本原则：

1．所有数据源和计算服务均被视为资源。网络可以由几种不同类别的设备组成。网络可能还拥有小微型设备，这些设备将数据发送到聚合器/存储、软件即服务（SaaS），还有将指令发送到执行器的系统等。此外，如果允许个人自带的设备访问企业拥有的资源，则企业也可以决定将其归类为资源。

2．无论网络位置如何，所有通信都必须是安全的。网络位置并不意味着隐式信任。来自位于企业自有网络基础设施上的系统的访问请求（例如，在传统概念中内网）必须与来自任何其他非企业自有网络的访问请求和通信采用相同的安全要求。换言之，不应对位于企业自有网络基础设施上的设备自动授予任何的信任。所有通信应以最安全的方式进行，保证机密性和完整性，并提供源身份认证。

3．对企业资源的访问授权是基于每个连接的。在授予访问权限之前，需要对请求者的信任进行评估。这意味着此特定事务只能在“以前某个时间”发生，并且在启动会话或使用资源执行事务之前不应该直接发生。但是，对某一个资源访问的身份认证和授权不会自动授予到其他不同的资源访问。

4．对资源的访问权限由动态策略（包括客户身份、应用和请求资产的可观测状态）决定，也可能包括其他行为属性。一个组织通过定义其所拥有的资源、其成员是谁（或对来自联盟的用户进行身份认证的能力）、这些成员需要哪些资源访问权等方式来保护资源。对于零信任模型，用户身份包括使用的用户账户和由企业分配给该帐户或组件以认证自动化任务获取的任何相关属性。请求发送者的资产状态包括设备特征，例如：已安装的软件版本、网络位置、请求时间和日期、以前观测到的行为、已安装的凭证等。行为属性包括自动化的用户分析、设备分析、度量到的与已观测到的使用模式的偏差。策略是一系列基于组织机构分

配给用户、数据资产或应用的属性的访问规则集。这些属性基于业务流程的需要和可接受的风险水平。资源访问和操作权限策略可以根据资源/数据的敏感性而变化。最小特权原则应该被应用于限制可视性和可访问性。

5．企业应该监控并且测量其所有自有或关联的资产的完整性和安全态势。没有设备是天生可信的。当企业评估一个资源请求时，也应该同时评估资产的安全态势。实施 ZTA 战略的企业应建立一个 CDM 或类似的系统来监控设备和应用的状态，并根据需要应用补丁/修复程序。那些被攻陷、具有已知漏洞和/或不受企业管理的设备（包括拒绝与企业资源的所有连接设备），与那些企业所拥有的或与企业关联的被认为处于最安全状态的设备相比，应该被区别对待。这种要求也应该适用于允许访问某些资源但不允许访问其他资源的关联设备（例如，个人自带的设备）。因此，需要一个强大的监控和报告系统来提供关于企业资源当前状态的可操作数据。

6．所有资源的身份认证和授权是动态的，并且在资源访问被允许之前严格强制实施。这是一个不断的访问请求、扫描和评估威胁、自适应、在通信中进行持续信任评估的循环过程。实施 ZTA 策略的企业具有身份、凭证和访问管理系统（ICAM）以及资产管理系统。这其中包括使用多因子身份验证（MFA）访问某些（或所有）企业资源。整个用户交互过程应该持续地监视，根据策略（如基于时间的、新的资源请求、检测到异常用户活动）的定义和执行，可能进行重新的身份认证和重新授权，以努力实现安全性、高可用性、易用性和成本效率之间的平衡。

7．企业应该尽可能收集关于资产、网络基础设施和通信的当前状态信息，

并将其应用于改善网络安全态势。一个企业需要收集关于网络流量和访问请求的数据，并将这些数据用于提高安全策略的创建和改进。这些数据还可以作为某个主体的访问请求的上下文信息（请参阅第 3.3.1 节）。

上述原则试图尽可能的无技术倾向性 (technology-agnostic)。例如，“用户身份 ID”可以包括多种方式：例如用户名/口令、证书、一次性密码等等。这些原则适用于在一个组织机构内或与一个或多个合作伙伴组织，但不适用于面向公众或消费者的业务流程。因为组织不能将内部政策强加给外部参与者（例如，客户或普通互联网用户），但可以对与组织有特殊关系的非企业用户（如注册客户、员工家属等）实施一些基于 ZT 的策略。

2.2 零信任视角的网络

对于在网络规划和部署中使用 ZTA 的任何组织，都有一些关于网络连接性的基本假设。其中一些假设适用于企业自有的网络基础设施，另一些适用于非企业拥有的网络基础设施上（例如，公共 WiFi 或公共云提供商）。这些假设被用来指导 ZTA 的形成。在实施 ZTA 的企业中，网络开发应该遵循上述的 ZTA 原则和以下的假设。

1. **整个企业专网不被视为隐式信任区。**资产应该始终假设企业网络上存在攻击者，通信应该来以最安全的方式进行（见上文的原则 2）。这需要对所有连接进行身份验证，对所有通信流量进行加密操作。
2. **网络上的设备可能不归企业所有或不可配置。**访客和/或外包服务可能需要用非企业自有的设备进行网络访问才能履行其职责。此外，员工自

带设备（BYOD）策略，允许企业用户使用非企业自有的设备访问企业资源。

3. **没有资源是天生可信的。**在连接到企业拥有的资源之前，每个资产都必须通过 PEP 评估其安全态势（与针对资产和主体的上述原则 6 类似）。该评估应该持续进行直到会话结束。与来自非企业自有设备的相同请求相比，企业自有设备可能具有启用身份验证的构件并提供高于同一请求的信任等级。仅使用用户凭证并不足以对企业资源进行设备认证。
4. **并非所有的企业资源都在企业拥有的基础设施上。**资源包括远程用户和云服务。企业拥有或管理的资产可能需要利用本地（即非企业）网络进行基本的连接和网络服务（如 DNS 解析）。
5. **远程企业主体不能信任本地网络连接。**远程主体应该假设本地（即非企业所有）网络是恶意的。资产应该假设所有的流量都被监控中并可能被修改。所有连接请求都应经过身份认证和授权，所有通信都应尽可能以最安全的方式完成（即提供机密性、完整性保护和源身份认证）。（参见上面的 ZTA 原则）。
6. **在企业和非企业基础设施之间移动的资产和工作流应具有一致的安全策略和态势。**在移入或移出企业拥有的基础设施时，资产和工作负载应保持其安全态势。这包括从企业网络移动到非企业网络的设备（即远程用户）。这也包括从企业内部数据中心迁移到非企业云实例的工作负载。

3 零信任体系架构的逻辑组件

在企业中，构成 ZTA 部署的逻辑组件很多。这些组件可以作为本地服务或通过基于云的服务来运行。图 2 中的概念框架模型显示了组件及其相互作用的基本关系。注意，这是显示逻辑组件及其相互作用的理想模型。从图 1 中，**策略判定点（PDP）**被分解为两个逻辑组件：**策略引擎（PE）**和**策略管理器（PA）**（定义如下）。ZTA 逻辑组件使用单独的控制平面进行通信，而应用数据则在数据平面上进行通信（见 3.4 节）。

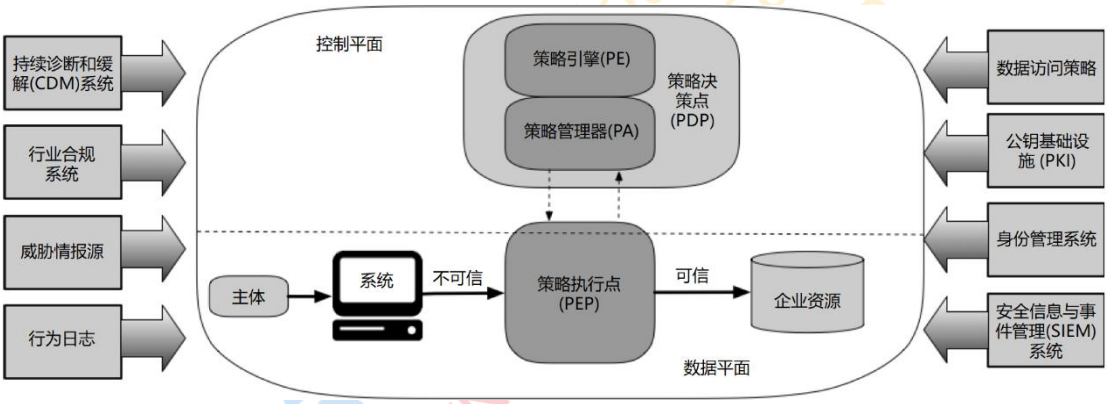

图 2：核心零信任逻辑组件

以上组件的具体描述：

- **策略引擎（Policy Engine, PE）**：该组件负责最终决定是否授予指定访问主体对资源（访问客体）的访问权限。策略引擎使用企业安全策略以及来自外部信息源（例如 IP 黑名单、威胁情报服务）的输入作为“信任算法”（TA）的输入，以决定授予或拒绝对该资源的访问（请参阅章节 3.3 了解详情）。策略引擎（PE）与策略管理器（PA）组件配对使用。策略引擎做出并记录决策，策略管理器执行决策（批准或拒绝）。

- **策略管理器（Policy Administrator, PA）**：该组件负责建立和(或)切断主体与资源之间的通信路径(通过给 PEP 的命令)。它将生成客户端用于访问企业资源的任何身份验证令牌或凭证。它与策略引擎 PE 紧密相关，并依赖于其决定最终允许或拒绝会话。如果会话被授权且请求已被认证，则 PA 配置 PEP 以允许会话启动。如果会话被拒绝（或之前的批准被拒绝），PA 向 PEP 发出信号以切断连接。一些实现可能会将 PE 和 PA 视为单独的服务；这里，它们被划分为两个逻辑组件。PA 在创建连接时与策略执行点（PEP）通信。这种通信是通过控制平面完成的。
- **策略执行点（Policy Enforcement Point, PEP）**：此系统负责启用、监视并最终终止访问主体和企业资源之间的连接。PEP 与 PA 通信，以转发请求和/或从 PA 接收策略更新。这是 ZTA 中的单个逻辑组件，但也可能分为两个不同的组件：客户端（例如，用户笔记本电脑上的 Agent 代理程序）和资源端（例如，在资源之前部署的访问控制网关）或充当通信路径防护的单个门户组件。在 PEP 组件的后面就是放置企业资源的隐含信任区域（请参阅第 2 节）。

除了企业中实现 ZTA 策略的核心组件之外，还有几个数据源提供输入和策略规则，以供策略引擎在做出访问决策时使用。这些数据源包括本地的和外部(即非企业控制或创建的)，其中包括：

- **持续诊断和缓解（CDM）系统**（Continuous diagnostics and mitigation system）：该系统收集关于企业资产当前状态的信息，并更新配置和软件组件。企业 CDM 系统向策略引擎提供关于发出访问请

求的系统的信息，例如它是否正在运行适当的打过补丁的操作系统和应用程序、企业批准的软件组件的完整性或是否存在未经批准的组件、以及该资产是否存在任何已知的漏洞。CDM 系统还负责对活跃在企业基础设施上的非企业设备进行识别并可能执行子集策略。

- **行业合规系统**（Industry compliance system）：该系统确保企业遵守其可能隶属的任何监管制度（如 FISMA、医疗或金融行业信息安全要求 HIPAA、PCI-DSS 等）。这包括企业为确保合规性而制定的所有策略规则。
- **威胁情报源**（Threat intelligence feeds）：该系统提供外部来源的信息，帮助策略引擎做出访问决策。这些可以是从多个外部源获取数据并提供关于新发现的攻击或漏洞的信息的多个服务。这还包括新发现的软件缺陷、新识别的恶意软件以及报告的对其他资产的攻击（策略引擎 PE 将会拒绝来自该企业设备的访问）。
- **网络与系统行为日志**（Network and system activity logs）：该企业系统聚合资产日志、网络流量、资源授权行为和其他事件，这些事件提供对企业信息系统安全态势实时（或者非实时）的反馈。
- **数据访问策略**（Data access policies）：这是一组由企业围绕着企业资源而创建的关于数据访问的属性、规则和策略。这组策略规则可以编码(通过管理界面)，也可以由策略引擎 PE 动态生成。这些策略是授予对资源的访问权限的起点，因为它们为企业中的参与者和应用程序提供了基本的访问特权。这些角色和访问规则应基于用户角色和组织的任务需

求。

- **企业公钥基础设施（PKI）**：该系统负责生成和记录企业向资源、主体、服务和应用程序签发的证书。这还包括全球 CA 生态系统和联邦 PKI，它们可能与企业 PKI 集成，也可能未集成。此系统还可以是非基于 X.509 数字证书构建的 PKI 体系。
- **身份管理系统**（ID management system）：该系统负责创建、存储和管理企业用户账户和身份记录（例如：轻量级目录访问协议 LDAP 服务器）。该系统包含必要的用户信息（如姓名、电子邮件地址、证书等）和其他企业特征，如角色、访问属性或分配的系统。该系统通常利用其他系统（如上面的 PKI）来处理与用户账户相关联的工件。该系统可能是更大的联合社区的一部分，可能包括非企业员工或链接到非企业资产的协作。
- **安全信息和事件管理（SIEM）系统**：该系统收集以安全为核心、可用于后续分析的信息。这些数据可被用于优化策略并预警可能对企业系统进行的主动攻击。

3.1 零信任架构的常见方案

企业可以通过多种方式为工作流引入零信任架构 ZTA。这些方案因使用的组件和组织策略规则的主要来源而有所差异。每种方案都实现了零信任的所有原则（请参阅第 2.1 节），但可以使用一个或两个（或一个组件）作为策略的主要驱动元素。一个完整的 ZT 解决方案将包括所有三种方案的要素。这些方案包括增

强的身份治理、逻辑微隔离、和基于网络的隔离。

不同的场景使用不同的方案。为企业开发零信任架构 ZTA 的组织可能会发现，其所选择的用例和已有策略会导向某一种方案。这并不是意味着其他方案不起作用，而是意味着其他方案可能更难实施，可能需要更多针对企业当前开展的业务流程的基础改变。

3.1.1 基于增强身份治理的 ZTA

基于增强身份治理的 ZTA 使用参与者身份作为策略创建的关键组件。如果不是请求访问企业资源的主体，则无需创建访问策略。对于这种方案，企业资源访问策略基于身份和分配的属性。资源访问的主要诉求是基于给定主体身份的访问授权。其他因素，如使用的设备、资产状态和环境因素，可以改变其最终信任评分计算（和最终访问授权），或者以某种方式调整结果（例如，基于网络位置仅授予对给定数据源的部分访问权限）。保护资源的 PEP 组件必须有能力可以把请求转发到策略引擎服务，在访问授权之前进行主体身份认证和请求核准。

基于增强身份治理的企业 ZTA 方案通常使用开放网络模型，或允许外部访问者访问的企业网络，或允许网络上的常见非企业设备（如下面第 4.3 节中的用例）。网络访问初始被授予在具有访问权限的资产上，仅限于具有适当访问权限的身份。授予基本的网络连接有一个缺点，因为恶意行为者仍然可以尝试网络侦查和/或利用网络对内部或第三方发起拒绝服务攻击。企业仍然需要在这种行为影响工作流程之前对其进行监控和响应。

身份驱动的方法与资源门户网站模型（见 3.2.3 节）配合得很好，因为设备

身份和状态为访问决策提供了辅助支持数据。其他模型也可以使用，具体取决于现有的策略。身份驱动的方法对于使用基于云的应用/服务的企业也很有效，因为这些应用/服务可能不允许使用企业所有或运营的 ZT 安全组件（如许多 SaaS 产品）。企业可以使用请求者的身份在这些平台上建立和执行策略。

3.1.2 基于微隔离的 ZTA

企业可以将单个或一组资源放在由网关安全组件保护的私有网段上来实施 ZTA。在这种方案中，企业将智能交换机(或路由器)、下一代防火墙(NGFWs)等基础设施设备或特殊用途的网关设备作为保护每个资源（或一小组相关资源）的 PEP。或者（或额外），企业可以选择使用软件代理（见第 3.2.1 节）或端点资产上的防火墙来实现基于主机的微隔离，这些网关设备动态授权访问来自客户端资产的各个请求。根据模式的不同，网关可以是唯一的 PEP（Policy Enforcement Point）组件，也可以是由网关和客户端代理组成的多部分 PEP 的一部分。（请参阅第 3.2.1 节）

由于保护设备充当 PEP，而该设备的管理充当 PE / PA 组件，因此该方法适用于各种用例和部署模型。此方法要求身份管理程序(IGP)完全发挥作用，但依赖网关组件充当 PEP，从而保护资源免受未经授权的访问和/或发现。

该方案关键必要的一环是对 PEP 组件进行管理，并应能够根据需要做出反应和重新配置，以应对威胁或工作流的变化。可以通过使用一般的网关设备甚至无状态防火墙来实现微隔离企业的某些功能是可行的，但是管理成本和快速适应变化的难度使这成为非常糟糕的选择。

3.1.3 基于网络基础设施和软件定义边界 SDP 的 ZTA

最后一种方案是使用网络基础设施来实现 ZTA。零信任的实现可以通过使用顶层网络来实现（即第 7 层，但也可以将其部署在更低的 ISO 网络协议栈）。这种方案有时称为软件定义边界（SDP）方法，并且经常包含 SDN [SDNBOOK]和基于意图的联网（IBN）[IBNVN]的概念。在这种方案中，PA 充当网络控制器，根据 PE 做出的决定来建立和重新配置网络。客户端继续请求通过 PEP（由 PA 组件管理）进行访问。

当在应用网络层（即第 7 层）实施该方案时，最常见的部署模型是代理/网关(见 3.2.1 节)。在此实现中，代理和资源网关（充当单个 PEP，由 PA 配置）建立用于客户端和资源之间通信的安全通道。这种模型可能还有其他的变体，也适用于云虚拟网络、非 IP 网络等。

3.2 抽象架构的常见部署方案

以上所有组件都是逻辑组件。他们未必都是单一系统。单个系统可以履行多个逻辑组件的职责，同样，一个逻辑组件可以由多个硬件或软件元素组成以执行其任务。例如，企业管理的 PKI 可能由负责发行的设备证书的一个组件，与另一个用于向最终用户颁发证书的组件共同构成，但两者都使用由同一个企业根证书颁发机构颁发的中间证书。在目前市面上一些的零信任产品中，PE 和 PA 组件合并在同一个服务中。

以下各节会描述架构的各个所需组件的不同部署方式。根据企业网络的设置方式不同，多种 ZTA 部署模型可能会适用于一个企业中的不同业务流程。

3.2.1 基于设备代理/网关的部署

在此部署模型中，PEP 分为两个组件，一个驻留在资源上，另一个直接位于资源前面。例如，每个企业分配的资产上都有个已安装的设备 Agent 代理程序用于创建和管理连接，并且每个资源都有一个组件（即网关）放置在最前面，以便资源仅与网关通信，该组件本质上充当资源的代理。代理是一个软件组件，它将部分（或全部）流量引导到相应的 PEP，以便对请求进行评估。网关负责连接到策略管理器（PA），并对由 PA 配置所允许的通信放行（请参见图 3）。

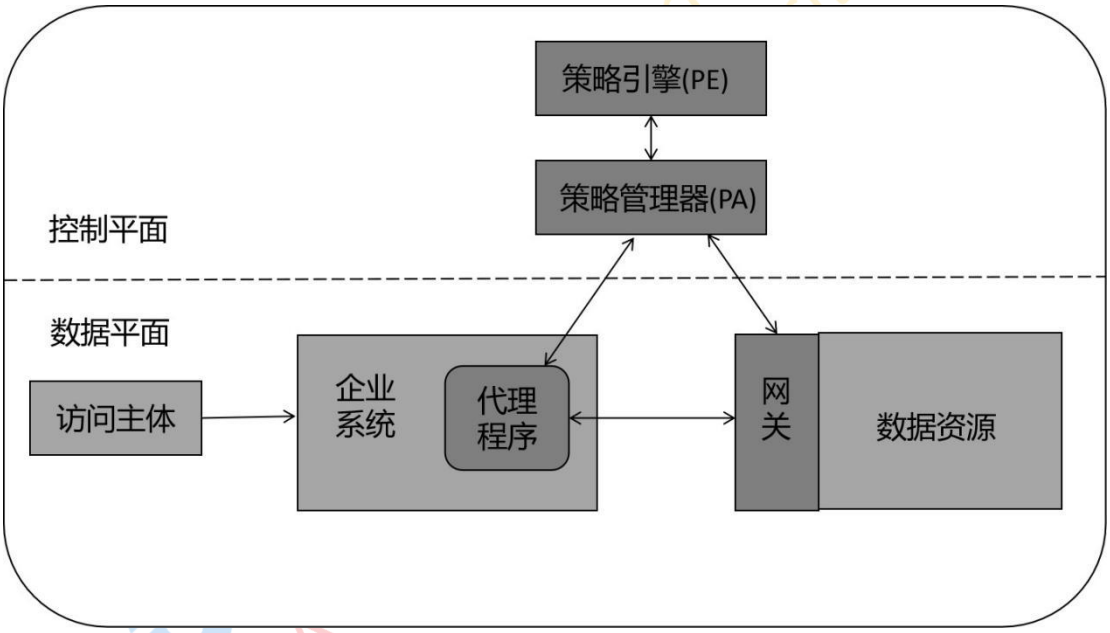

图 3：设备代理/网关模型

举一个典型场景为例，一个用户希望通过企业分配的笔记本电脑连接到一个特定企业资源(例如，人力资源应用程序/数据库)。该访问请求由本地代理 Agent 接收，然后将请求发送给策略管理器（PA）。策略管理器（PA）和策略引擎（PE）可以是企业本地部署产品或云托管服务。策略管理器 PA 将请求转发到策略引擎 PE 进行评估。如果请求被授权，则 PA 配置设备代理与相关设备之间的通信通

道通过控制平面的资源网关。这可能包括网际协议（IP）策略管理器 PA 将请求转发到策略引擎 PE 进行评估。如果请求被授权，则策略管理员 PA 通过控制平面在配置设备上 Agent 代理程序与对应的资源网关 Gateway 之间配置一个连接通道。这可能包括 IP 地址，端口信息，会话密钥或类似的安全元件。然后，设备代理程序和网关连接，加密的应用程序数据流开始工作。当工作流完成或由于安全事件（例如，会话超时、无法重新认证）而由策略管理器 PA 触发时，设备代理与资源网关之间的连接将终止。

此模型最适合于在中拥有强大的设备管理程序的企业。或者是分散的资源都可以与网关通信。对于大量利用云服务的企业来说，这是云安全联盟（CSA）软件定义边界（SDP）[CSA-SDP]的客户端-服务器实现。这个模型也适用于不想制定严格 BYOD 政策的企业。所有对于资源的访问只能通过设备代理 Agent，这个 Agent 可以安装在企业的设备资产上。

3.2.2 基于飞地的部署

此部署模型是上述设备代理/网关模型的变体。在这个模型中，网关组件可能不驻留在资产上或在某个资源的前面，而是驻留在资源飞地（例如，本地数据中心）的边界上（如图 4 所示）。通常，这些资源仅用于实现单个业务功能，或者它们可能无法与网关直接通讯（例如，一些陈旧数据库系统可能没有 API 接口可以与网关通信 [API]）。这个部署该模型也可以应用于基于云上微服务的业务流程（例如，用户通知、数据库查询、工资支出）。在这个模型中，整个私有云位于网关后面。

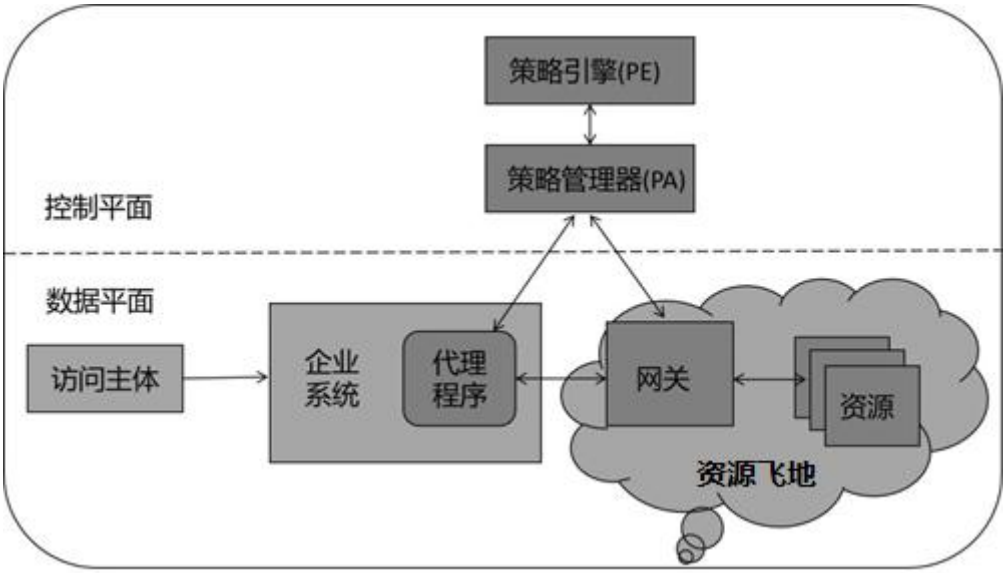

图 4：飞地网关模型

该模型可以和设备代理/网关模型进行混合部署。在这个模型中，企业设备资产上安装一个代理程序 Agent，用于连接飞地的网关，但是创建这些连接的过程和上面提到的设备代理/网关模型的使用的过程是一样的。

该模型可以应用于企业比较陈旧的应用程序或者在无法独立部署网关的本地数据中心。企业需要一个比较强大的设备和配置管理系统来安装和配置所有终端上的代理程序（Agent）。这个模型的缺点是网关只能保护一组资源而并非每个独立的资源，这将导致访问主体可能会看到一些他们不该看到的资源。

3.2.3 基于资源门户的部署

在此部署模型中，PEP 是充当用户请求网关的唯一组件。网关门户既可以用于单个资源，也可以用于实现单个业务功能的一组资源所处的飞地。例如，通过网关门户连接到运行老旧应用程序的私有云或数据中心（如图 5 所示）。

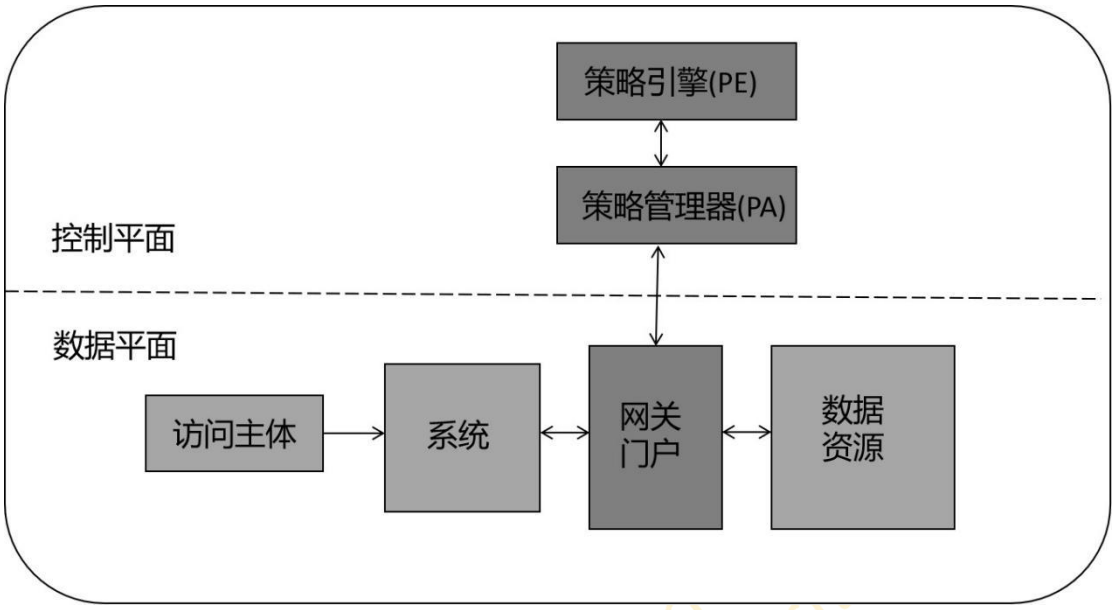

图 5：资源门户模型

该模型相对于其他模型的主要优势是，无需在所有客户端设备上安装软件组件。这种模型对于 BYOD 政策和跨组织协作而言非常灵活。企业管理员无需确保每个设备在使用前都安装有适当的设备 Agent 代理程序。但是，来自访问请求的设备的信息也会非常有限。此模型只能在资产和设备它们连接到 PEP 门户时进行一次性的扫描和分析，但无法持续地进行恶意软件和正确配置的监控。

此模型的主要区别在于，无需本地代理程序处理请求，因此企业可能无法对于对资产有完整可见性或任意控制权，因为只能当他们连接到门户时才能看到/扫描。企业可能可以采用浏览器隔离的方式来缓解这个问题。在这些会话之间，资产可能是企业看不见的。该模型还允许攻击者发现并尝试访问门户或尝试对门户进行拒绝服务（DoS）攻击。门户系统应配置完善，可提供抵御 DoS 攻击或网络中断的可用性。

3.2.4 设备应用沙箱

代理/网关部署模型的另一个变体是将应用程序或进程在资产设备上的隔离区运行。这些隔离专区可以是虚拟机，容器或其他实现方式，但目标是相同的：保护在设备上运行的应用程序，或者来自可能受到威胁的主机的应用程序实例，或者其他应用程序。

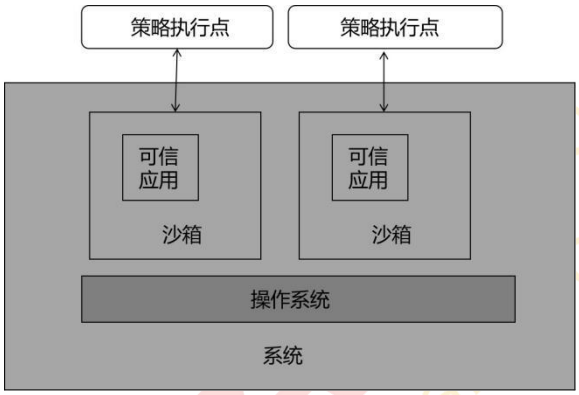

图 6：应用程序沙箱

在图 6 中，用户在设备上的沙箱中运行已批准和审查过的应用程序。该应用程序可以与 PEP 通信以请求访问资源，但 PEP 将拒绝来自该设备资产上的其他应用程序。这个模型中，PEP 可以是企业本地服务或云服务。

此模型的主要优点是，单个的应用程序和该设备上的其他应用程序隔离。即使无法扫描设备资产上的漏洞，这些独立运行在沙盒的程序也能免受主机上潜在的恶意软件感染。但这种模型有一个缺点，就是企业必须为所有设备资产维护这些沙盒中应用程序，但又可能无法看到这些资产。企业还需要确保每个沙盒应用程序都是安全的，这需要比简单地监控设备花费更多的成本。

3.3 信任算法

对于已经部署零信任架构 ZTA 的企业，策略引擎 PE 可以看作是大脑，而 PE 的信任算法（TA）则是其主要的思维过程。TA 是策略引擎 PE 用来最终授予或拒绝对资源的访问的进程。策略引擎 PE 接受来自多个源的数据输入（见第 3 节）：用户信息、用户属性和角色、用户历史行为模式、威胁情报源和其他元数据源的策略数据库。流程可以分为几大类别，如图 7 所示。

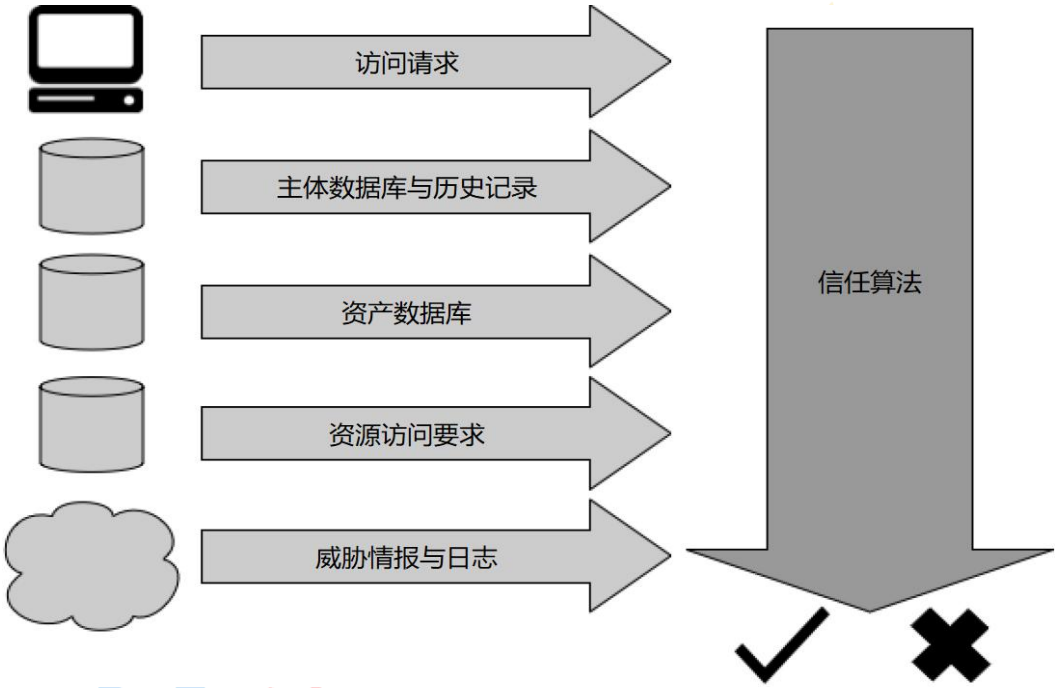

图 7：信任算法输入

在上图中，根据提供给信任算法的内容将输入分为以下几类：

- **访问请求（Access request）：**这是来自访问主体的实际请求。所请求的资源是主要有用信息，但有关请求者的信息也会被使用。这些信息包括操作系统版本、使用的软件(例如，请求的应用程序是否出现在批准的应用程序列表中？)和补丁级别。根据这些因素和设备资产安全状况，来判断限制或拒绝

访问资产。

- **主体数据库(Subject database)**:这是“谁”在请求访问资源 [SP800-63-3]。这是企业或合作伙伴的一组用户（人员和进程）以及所分配的一组用户属性/权限。这些用户和属性构成了资源访问策略的基础[SP800-162][NITIR 7]。用户身份认证包括逻辑身份（例如，帐户 ID）和 PEP 执行的认证检查结果的混合。在推导信任度时可以考虑的身份属性包括时间和地理位置。授予多个用户的权限集合可以被视为一个角色，但将权限分配给一个用户应独立处理，而不能简单认为属于某个特定角色而授权。此集合应编码并存储在 ID 管理系统和策略数据库中。在一些（TA）实践方案中，这也需要包括过去观测到的用户行为的数据（请参阅第 3.3.1 节）。
- **资产数据库 (和可观测状态)（Asset database and observable status)**:这是一个包含每个企业拥有资产已知状态（包括物理和虚拟）的数据库。这与发出请求的资产的观测状态进行比较，包括操作系统版本、使用的应用程序、位置（网络位置和地理位置）和补丁级别。根据与数据库中的资产状态对比，对资源的访问可能会被限制或拒绝。
- **资源访问要求（Resource requirements）**：这组策略补充了用户 ID 和属性数据库[SP800-63-3]，并定义了访问资源的最低要求。要求可以包括认证器保证级别，例如 MFA 网络位置（例如，拒绝来自海外 IP 地址的访问）、数据敏感度（有时称为“数据毒性”）和资产配置请求。这些要求应由数据保管人（即负责数据的人员）和负责利用数据的业务流程的人员（即任务负责人）共同制定。

- **威胁情报（Threat intelligence）：**这是一个或多个有关一般威胁和活动恶意软件的信息源。这也可以包括从设备上看到的可能是可疑的通信的具体信息（如查询可能的恶意软件命令和控制节点）。这些可以是外部服务，也可以是内部扫描和发现，可以包括攻击特征和缓解措施。这是唯一最有可能由服务方提供而不是企业控制的组件。

每个数据源的都有重要性的权重值，权重值可以通过专有算法计算得出，也可以由企业配置。这些权重值可用于反映数据源对企业的重要性。

最终决定结果将传递给策略管理器 PA 执行。策略管理器 PA 的工作是配置必要的 PEP，以开启授权的通信。根据零信任架构 ZTA 的部署方式，这可能涉及向网关、代理或资源门户发送身份验证结果和连接配置信息。策略管理器 PA 还可以保持或暂停通信会话，以便根据策略要求重新验证和重新验证连接。策略管理器 PA 还负责根据策略发出终止连接的命令（例如，在超时后、工作流完成时、或由于安全告警）。

3.3.1 信任算法的常见实现方法

有多种信任算法 TA 的实现方法。不同的实施者可能希望根据因素的感知重要性对上述因素进行不同的权衡。有两个主要特性可用于区分信任算法 TA。第一是以上这些因素如何被评估，无论是作为二元决策或是作为整个“得分”或信任级别的加权部分。第二是对比来自同一主体、应用或设备的请求的差异性来评估请求。

- **基于条件与基于分值：**基于条件的信任算法 TA 假设在授予对资源的访问或

允许操作（例如读/写）之前必须满足一组合格属性。这些条件由企业为每个资源独立配置的。只有在满足所有条件时，才授予对资源的访问权或对资源应用操作。基于分值的信任算法 TA 基于每个数据源的值和企业配置的权重计算信任等级。如果得分大于资源的配置阈值，则授予访问权限或执行操作。否则，请求被拒绝，或访问权限降低（例如，授予读取权限，但不授予对文件的写入权限）。

- **独立（Singular）与基于上下文（Contextual）：**一个独立的信任算法 TA 将每个请求独立处理，在进行信任评估时并不考虑用户/应用程序的历史。这种评估方式的优点是速度快，但存在的风险是如果攻击者停留在用户允许的角色范围内则有可能无法检测到攻击。基于上下文的信任算法 TA 在评估访问请求时考虑用户或网络代理的最近历史记录。这意味着 PE 必须维护所有用户和应用程序的某些状态信息，当攻击者使用被盗的凭据以一种被 PE 感知到的不同平常的模式访问信息时，攻击能被检测到。对于用户行为的分析可用于建模出可被系统接受的用户使用方式，与此行为的偏差可能会触发额外的身份验证或者资源请求拒绝。

这两个因素并不总是相互依赖的。可以有一个信任算法 TA 为每个用户和/或设备分配一个信任等级，并且独立地考虑每个访问请求（即，独立的信任算法）。然而，基于分数的情境信任算法 TA 效果最好，因为分数为请求用户账户提供了当前的信任等级。

理想情况下，ZTA 信任算法应该是上下文相关的，但对于企业可用的基础结构组件来说，未必始终可行。当攻击者利用被破解账户或内部攻击，他们通常保

持接近一组“正常”的访问请求，基于上下文的信任算法 TA 可以更好的减少此类威胁。在定义和实现信任算法时，必须平衡安全性、可用性和成本效益。在用户执行任务时，在和历史模型或行为范式不一致时，不断地提示用户重新验证可能会导致用户体验问题。例如，如果一个机构的人力资源部门的员工通常在一个典型的工作日访问 20 到 30 个员工记录，如果访问请求在一天中突然超过 100 个记录，基于上下文的信任算法 TA 可能会发送警报。如果有人在正常工作时间后提出访问请求，基于上下文的信任算法 TA 也可能发送警报，因为这有可能是攻击者使用受损的 HR 帐户来提取记录。以上这些例子说明基于上下文的信任算法 TA 可以检测到攻击，而独立信任算法 TA 可能无法检测到新行为。另外一个例子，一个通常在正常工作时间访问金融系统的会计现在正试图在半夜从一个无法识别的位置访问该系统，基于上下文的信任算法 TA 可能触发警报，并要求用户满足更严格的信任等级或 NIST 特别出版物 800-63A[SP800-63A]中概述的其他标准。

为每种资源制定一套标准或权重/阈值需要计划和测试。在最初实施 ZTA 期间，企业管理员可能会遇到问题，例如由于配置错误而拒绝了应批准的访问请求。这需要一个部署的初始“调整”阶段，对标准或计分权重进行调整，以确保在执行政策的同时仍允许企业业务正常运作。调整阶段持续多长时间取决于企业定义的进程指标和在业务流程中对错误拒绝/批准的容忍率。

3.4 网络/环境组件

在零信任环境中，用于控制和配置网络的通信流，与用于执行组织的实际工

作的应用程序通信流之间，应该存在隔离（可能是逻辑的或物理的）。这通常被分解为用于网络控制通信的控制平面和用于应用程序通信流的数据平面[Gilman]。

控制平面被各种基础设施组件(企业所有和服务提供商提供)用于维护系统；判断、授予或拒绝对资源的访问；以及执行任何必要的操作以建立资源之间的连接。数据平面用于应用程序之间的实际通信。在通过控制平面建立连接之前，可能无法使用该通信通道。例如，PA 和 PEP 可以使用控制平面在用户和企业资源之间建立连接。然后，应用程序工作负载才能使用已建立的数据平面连接。

3.4.1 支持 ZTA 的网络需求

1．**企业系统应具有基本的网络连接性。**本地网络 LAN(无论是否由企业控制)提供基本的路由和基础设施（如 DNS 等）。远程企业的设备资产不一定能使用所有基础设施服务。

2．**企业必须能够区分哪些资产是由企业拥有或管理的，以及设备当前的安全态势。**这是由企业颁发的凭证决定的，而不是使用不能被认证的信息（例如，可以被伪造的网络 MAC 地址）。

3．**企业能够捕获所有网络流量。**企业能够记录在数据平面上看到的数据包，但可能无法对所有数据包执行应用层检查（即，ISO 第 7 层）。企业能够过滤出关于连接的元数据（例如，目的地、时间、设备标识等），在评估访问请求时动态更新策略并通知 PE。

4．**企业资源不应该在未经 PEP 的情况下就可达。**企业资源不接受来自

Internet 的任意入栈连接。资源仅在客户端经过身份验证后，接受自定义配置的连接。这些连接是由 PEP 建立的。如果不访问 PEP，资源甚至不可能被发现。这可防止攻击者通过扫描 PEPs 后面的资源并对其发起 DoS 攻击来识别目标。请注意，并非所有资源都应以这种方式隐藏；某些网络基础结构组件（如 DNS 服务器）必须可访问。

5．**数据平面和控制平面在逻辑上是分开的。**PE、PA 和 PEP 都是在逻辑上独立、企业系统和资源无法直接访问的网络上进行通信。数据平面用于应用数据通信。PE、PA 和 PEP 使用控制平面来通信和管理系统之间的连接。PEP 必须能够发送和接收来自数据平面和控制平面的信息。

6．**企业设备资产可以到达 PEP 组件。**企业用户必须能够访问 PEP 组件以访问资源。可以采用的方式有企业系统上启用连接的 Web 门户，网络设备或软件代理。

7．**作为业务流的一部分，PEP 是唯一可以访问 PA 的组件。**在企业网络上运行的每个 PEP 都有一个与 PA 的连接，以便从客户端建立连接。所有企业业务流程流量都通过一个或多个 PEP。

8．**远程企业设备资产应能够直接访问任何企业资源，无需回连到企业基础网络设施。**例如，不应要求远程用户使用回连到企业网络的安全隧道（即 VPN）来访问由企业提供的服务，这些服务可以是由公共云提供商托管的服务（例如电子邮件）。

9．**用于支持 ZTA 访问决策过程的基础设施应具有可扩展性，以考虑处理负载的变化。**ZTA 中使用的 PE、PA 和 PEP 成为任何业务流程中的关键组成部分。

延迟或无法访问到 PEP（或 PEP 无法访问到 PA/PE）对执行工作流的能力产生负面影响。实现 ZTA 的企业需要为预期的工作负载提供组件，或者能够在需要时快速扩展基础设施以处理增加的使用量。

10．**企业设备资产由于某些可观测因素而可能无法访问某些 PEP。**例如，可能有一项策略规定，如果请求的移动设备资产可能位于企业之外时无法访问到某些资源。这些因素可能基于位置（地理位置或网络位置）、设备类型或其它标准等。

4 部署场景/用例

任何企业环境都可基于零信任原则来设计规划。大多数组织机构在企业基础设施中已经有一些零信任的要素，或者正在实施信息安全和弹性政策及最佳实践来实现零信任。一些部署场景和用例可以更容易实施零信任体系架构。例如，零信任架构 ZTA 更易于在地理上分散和/或员工流动性高的组织机构中扎根。总的来说，任何组织都可以从零信任架构中受益。

下面提及的用例没有明确要求 ZTA，因为企业可能同时拥有边界基础设施和 ZTA 基础设施。如第 7.2 节所述，一个企业在某一时期可能同时运行 ZTA 组件和基于边界的网络基础设施。

4.1 具有分支机构的企业

最常见的情况是一个企业有一个总部和一个或多个地理上分散的分支机构，并企业拥有的物理网络（内网）无法把他们连接一起（请参见图 8）。远程地点的员工可能不具备完整的企业本地网络，但为了执行工作任务仍然需要访问企业资源。企业可能有一个多协议标签交换机（MPLS）链接到企业总部网络，但可能没有足够的带宽来满足所有的流量，或者可能不希望基于云的应用/服务的流量穿越企业总部网络。同样，员工可能是远程办公或在外部地区使用企业所有或个人拥有的设备。在这种情况下，企业可能希望授予员工日历、电子邮件等某些资源的访问权限，但拒绝其访问或限制操作更敏感的资源（例如，人力资源数据库）。

在这种使用场景下，PE / PA 通常作为云服务托管（提供了卓越的可用性，并且不需要远程员工依靠企业基础设施访问云资源），终端设备资产安装了 Agent 代理程序 (请参阅第 3.2.1 节) 或直接访问资源门户 (请参阅第 3.2.3 节)。将 PE / PA 托管在企业本地网络可能不是最有效的方法，因为远程办公室和工作人员必须将所有流量发送回企业网络才能访问由云服务托管的应用程序。

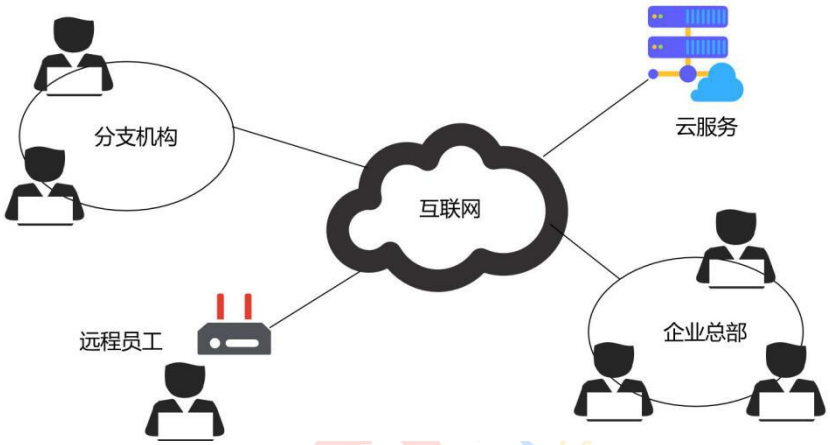

图 8：具有远程员工的企业

4.2 多云企业/云到云企业

一种越来越普遍的部署 ZTA 用例是企业使用了多个云供应商(请参见图 9)。在这种情况下，企业拥有本地网络，但同时使用两个或多个云服务提供商托管应用程序和数据。有时，应用程序托管在与数据源分离的云服务上。考虑性能和便于管理，云提供商 A 中托管的应用程序应该能够直接连接到托管在云提供商 B 中的数据源，而不应强制应用程序通过企业网络连接。

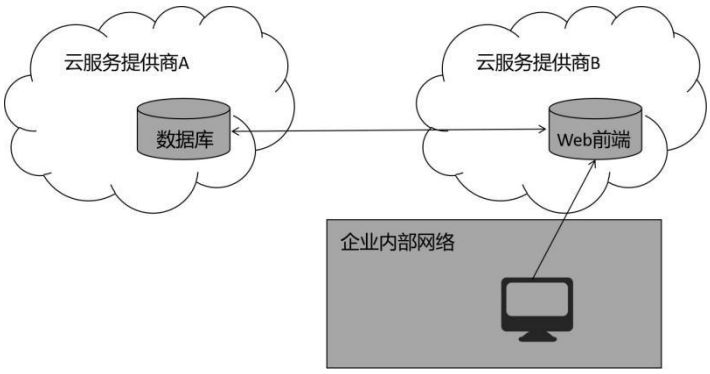

图 9：多云场景

该用例是 CSA SDP 规范[CSA-SDP]的服务器-服务器实现。随着企业转向更多的云托管应用程序和服务，显然传统依靠企业边界提供安全的方式成为一种负担。如第 2.2 节所述，零信任原则认为企业自有和运营的网络基础设施与任何其他服务提供商拥有和运营的基础设施之间应该没有任何区别。多云所用的零信任方案是把 PEP 放在每个应用程序和数据源的访问点。PE 和 PA 可以是位于云中或甚至是托管在第三方提供商的云服务。然后，客户端（通过门户或本地安装的 Agent 代理程序）直接访问 PEP。这样，即便资源托管在企业外部，企业仍然可以管理资源的访问。一个挑战是，不同的云提供商有独特的方式来实现类似的功能。企业架构师需要了解如何在他们所利用的每个云提供商中实现企业 ZTA。

4.3 具有外包服务和/或访客的企业

另一个常见的场景是企业的现场访客和/或外包服务人员需要对企业资源进行有限访问（请参见图 10）。例如，企业有自己的内部应用程序、数据库和资产，其中包括外包给供应商偶尔需要在现场提供维修的服务（例如，由外部供应商拥有和管理的智能供暖和照明系统，即 HVAC）。这些访客和服务提供商需要

网络连接以执行任务。实施零信任原则有助于企业在允许这些设备和来访的技术人员访问互联网的同时隐藏企业资源。

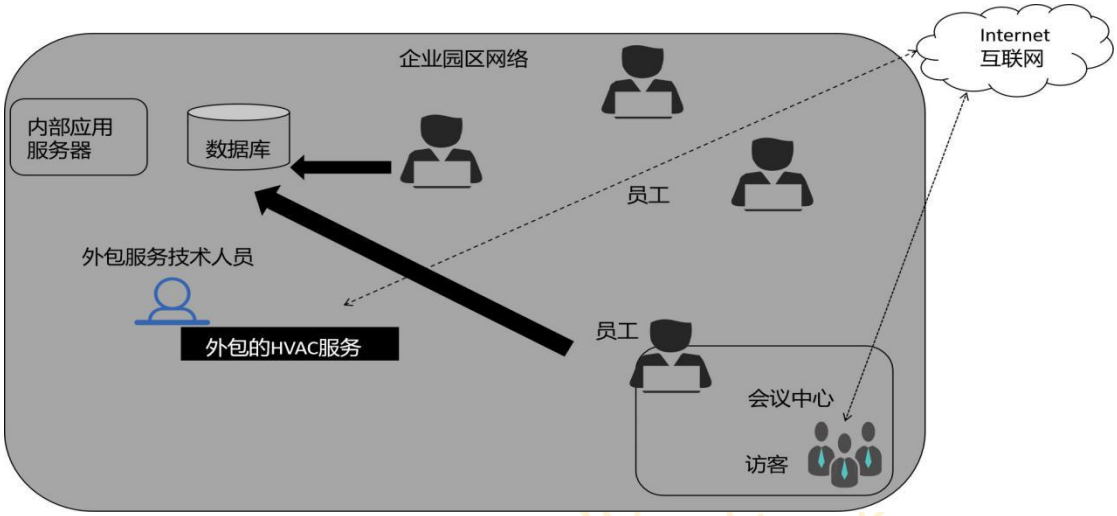

图 10：允许非员工访问权限的企业

在本用例中，组织机构还有一个供访客和员工交互的会议中心。同样，使用零信任 ZTA 的 SDP 软件定义边界方案，员工和普通用户的设备是区别开来的，并且可以访问适当的企业资源。企业园区中的访客可以访问互联网，但无法访问企业内部资源。访客甚至可能无法通过网络扫描发现企业服务（即防止主动网络侦察/东西向移动攻击）。

在这种用例下，PE 和 PA 可以是托管的云服务或部署在局域网中（假设很少甚至不使用云托管服务）。企业设备资产可能已安装 Agent 代理程序（请参见第 3.2.1 节）或通过门户网站访问资源（请参见第 3.2.3 节)。PA 确保所有非企业设备资产（那些没有安装 Agent 代理程序或无法连接到门户的资产）不能访问本地资源，但可以访问互联网。

4.4 跨企业协作

第四个用例是跨企业协作。例如，一个项目涉及企业 A 和企业 B 的员工（参见图 11）。两家企业可能是独立的联邦机构（G2G），甚至是联邦机构和私人企业（G2B）。企业 A 运维项目所使用的数据库，但必须允许企业 B 中的某些成员访问数据库中的数据。企业 A 可以为企业 B 中的员工设置可以访问所需数据的特定账号并拒绝这些账号访问所有其他资源，但这么做很快变得难以管理。如果两个组织机构都使用联盟 ID 管理系统将可以更快地建立这些关系，前提是两个组织的 PEP 都可以在联盟 ID 社区中对请求主体进行身份认证。

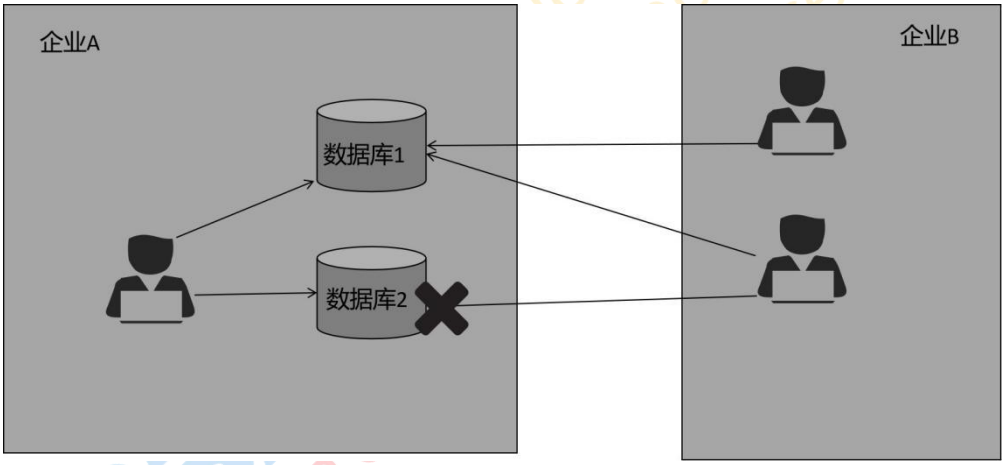

图 11：跨企业协作

这种情况可能类似用例 1（第 4.1 节），两家企业的员工都可能不在他们组织的网络基础设施上，他们需要访问的资源可能在一个企业环境中也可能托管在云中。这意味着无需通过复杂的防火墙规则或企业范围的访问控制列表（ACL）允许某些属于企业 B 的 IP 地址访问企业 A 的资源。如何进行访问取决于使用的技术。与用例 1 类似，托管为云服务的 PE 和 PA 可以向所有各方提供可访问性，无需建立 VPN 或采用类似的方案。企业 B 的员工可能会要求在其资产上安装软

件代 Agent 理程序，或通过 Web 网关访问必要的数据资源(请参见第 3.2.3 节)。

4.5 具有面向公共或面向用户服务的企业

许多企业的一个常见特征是面向公众的服务，该服务可能包括也可能不包括用户注册（即，用户必须创建或已颁发一组登录凭证）。这些服务可以服务于一般公众、一组具有现有业务关系的客户、或一组特殊的非企业用户，如员工家属。在所有情况下，很可能请求的设备资产不是企业所有，因此企业可以实施的内部网络安全策略是受局限的。

通常来说，对于不需要登录凭证即可访问的面向公众的通用资源（例如，公共网页），ZTA 的原则并不直接适用。企业不能严格控制请求设备资产的状态和公共资源不需要凭证才能访问。

企业可以为注册的公共用户 (即，那些已有业务关系的客户) 和特殊用户 (例如，员工家属）制定政策。如果用户需要创建或被颁发凭证，企业可以制定有关密码长度，生命周期和其他详细信息的政策，并可能提供 MFA（多因子认证）作为选项或要求。然而，企业对于此类用户可以实施的策略可能会受到限制。关于请求的信息可能有助于确定公共服务的状态，以及发现伪装成合法用户的潜在攻击。例如，一个需注册的用户门户是由已注册客户使用常用 Web 浏览器之一进行访问。突然来自未知浏览器类型或已知过时版本的访问请求增加，表示其正在遭受某种自动攻击，企业可以采取措施限制来自这些已识别的客户端请求。企业还应了解任何关于可以收集和记录有关请求用户和设备资产的信息的法规或法规。

5 与零信任架构相关的威胁

任何一家企业都不可能完全消除网络安全风险。若与现有网络安全相关政策和指南、身份和访问管理、持续监控和一般网络可用相结合，恰当实施并维护的零信任架构 ZTA 可以减少总体风险暴露，并抵御常见威胁。但是，即使实施了 零信任架构 ZTA ，某些威胁仍具有独特的能力。

5.1 ZTA 决策过程的破坏

在 ZTA 中，策略引擎 PE 和策略管理器 PA 是整个企业的关键组件。除非获得批准以及由 PE 和 PA 配置，否则企业资源之间不会发生任何通信。这意味着这些组件必须被正确地配置和维护。任何具有 PE 规则配置权限的企业管理员可能会执行未经批准的改动或配置错误，从而干扰企业的运营。同样，被攻陷的 PA 可能会批准一个理论上不应该许可的资源访问（例如，被攻陷的个人设备）。为缓解相关风险， PE 和 PA 组件必须被正确配置及监控，并且必须记录任何配置修改，同时进行审计。

5.2 拒绝服务或网络中断

在 ZTA 中，PA 是资源访问的关键组件。企业资源未经 PA 许可或者配置操作则无法互相连接。如果攻击者破坏或阻断对 PEP 或 PA 的访问（即 DoS 攻击或路由劫持），可能会给企业运营造成不利影响。企业可以通过制定强制驻留在云中的策略来缓解这种威胁，或根据网络弹性技术规范地在几个位置进行复

制[SP 800-160]。

这会减轻风险，但并不能消除风险。僵尸网络（如：Mirai）生产大量的 DoS 攻击，主要攻击关键的互联网服务提供商 ISP，并中断数百万互联网用户的服务。攻击者还可能拦截和阻止一部分或企业中的所有用户帐户（例如，分支机构，甚至单个远程员工）的流量。在这种情况下，只有一部分企业用户受到影响。这也可以在传统 VPN 访问的场景中也会出现，并非零信任架构 ZTA 独有。

托管提供商也可能意外地导致基于云的 PE 或 PA 离线。云服务过去曾经历过中断，无论是 IaaS 还是 SaaS。一个操作错误可能会阻止整个企业运行，如果 PE 或者 PA 组件无法从网络中访问。

还有一种风险，即 PA 无法访问企业资源，因此，即使访问权限授予用户，PA 也无法配置网络上的通信通道。这可能是由于 DDoS 攻击或仅仅是由于意外的大量使用。这类似于任何其他网络中断事故，部分或全部企业用户由于某种原因无法访问特定的资源。

5.3 凭证被盗/内部威胁

正确地实施零信任、信息安全和弹性策略以及最佳实践可以减少攻击者通过窃取的凭证或内部攻击而获得大规模访问权限的风险。零信任理念，即不基于网络位置的隐式信任，意味着攻击者需要入侵现有帐户或设备以在企业网络中立足。正确实施的 ZTA 应防止受攻击的帐户或设备资产访问超出其正常值的资源权限或访问模式。这意味着，具有攻击者感兴趣的资源的访问权限策略的帐户，将是攻击者的主要目标。

攻击者可能使用网络钓鱼、社会工程或多种攻击组合来盗取有价值的账户的登录凭证。根据攻击者的动机，"有价值"可能意味着不同的东西。例如，企业管理员帐户可能很有价值，但攻击者从财务收益角度可能考虑具有财务或支付资源的账户。在网络访问上实施 MFA 可降低来自被盗帐户的风险。但是，与传统企业一样，具有有效登录凭证（或恶意内部人员）可能仍然能够访问该帐户授予访问权限的资源。例如，攻击者或内部恶意员工所具备的账号可以访问人力资源系统，仍可通过被盗的账号和设备资产访问员工数据库。ZTA 可以降低风险，并防止任何帐户或资产被盗后横向移动攻击整个网络。如果泄露的凭证未授权访问特定资源，它们将继续被拒绝访问该资源。此外，基于上下文信任算法 TA（请参阅第 3.3.1 节）更有可能检测攻击并对此做出快速响应，相比在传统的基于边界的防御而言。基于上下文的信任算法 TA 可以检测异常行为的访问模式，并拒绝被入侵的帐户或内部威胁访问敏感资源。

5.4 网络可见性

如第 3.4.1 节所述，所有流量都经过网络检查和记录，并分析识别针对企业的潜在攻击并作出反应。然而，正如所提到的那样，一些企业网络上的（可能大多数）流量可能与传统层 3 层网络分析工具不透明。此流量可能来自非企业拥有的设备资产（例如，外包服务人员使用企业网络访问互联网）或一些拒绝网络流量监控应用程序。企业无法执行 DPI 或检查加密的流量，并且必须使用其他方法来评估网络上可能的攻击者。

这并不意味着企业无法分析它所在网络。企业可以收集有关加密流量的元数

据（如源地址和目的地址等），并用它来检测活跃攻击者或可能在网络上通信的恶意软件。机器学习技术[Anderson] 可用于分析无法解密和检查的流量。采用这种类型的机器学习将允许企业将流量归类为有效或可能的恶意流量且需要修复。

5.5 系统和网络信息的存储

企业网络流量分析的相关威胁可能是分析组件本身。如果网络流量和元数据被存储，用于构建上下文策略、取证或以后分析，该数据将成为攻击者的目标。就像网络结构图、配置文件等各类网络架构文档一样，这些资源应受到保护。如果攻击者可以成功访问到存储的流量信息，他们也许能够获得深入了解网络架构，并找到用于进一步侦察和攻击的资产。

零信任企业中攻击者的另一个侦察信息来源是用于编辑访问策略的管理工具。与存储的流量一样，此组件包含资源访问策略，并可向攻击者提供有关哪些最有价值的被攻击的帐户（例如，有权访问所需数据资源的人）。

对于所有有价值的企业数据，应建立适当的保护，以防止未经授权的访问和访问尝试。由于这些资源对安全至关重要，它们应具有最严格的访问策略，只能通过指定或专用访问管理员帐户。

5.6 依赖专有数据格式或解决方案

ZTA 依靠几个不同的数据源来做出访问决策，包括关于请求用户、使用的设备资产、企业和外部智能，以及威胁分析等信息。通常，用于存储和处理此信

息的资产没有通用的关于如何交互和交换信息的开放式标准。这可能导致企业所在的实际场景中由于互操作性问题被个别供应商商锁定。如果某个供应商有安全性问题或突然中断，企业可能无法迁移到新的产商，除非付出高昂的成本（例如，更换多个资产），或经历一个长期过渡计划（例如，将策略规则从一个专有格式转换到另一个专有格式）。与 DoS 攻击一样，此风险并非 ZTA 独有，但由于 ZTA 严重依赖于对信息的动态访问（包括企业和服务提供商），中断可能会影响企业的核心业务正常进行。为了降低相关风险，企业应该对服务提供商进行综合评估，除了考虑性能、稳定性等比较典型的因素外，还要考虑供应商安全控制、企业切换成本、供应链风险管理等因素。

5.7 在 ZTA 管理中使用非人类实体 （NPE）

人工智能和其他软件代理 Agent 正在被用来管理企业网络上的安全性问题。这些组件需要与 ZTA 的管理组件（例如，PE 和 PA）交互，甚至有时代替人工管理员。这些组件如何在实施 ZTA 的企业中进行身份验证是一个仍未解决的问题。通常假定大多数自动化技术系统在调用 API 资源都将以某些方式进行身份验证。

在使用自动化技术进行配置和策略实施时，最大的风险是可能出现误报（将无害操作误认为攻击）和漏报（将攻击误认为是正常操作）。 这种风险可以通过定期重新调整分析来纠正错误的决策并将其改善，从而减少这种情况的出现。

相关的风险是攻击者能够诱使或强迫 NPE 执行某些攻击者无权执行的任务。与人类用户相比，软件代理 Agent 可能以较低的认证标准（例如，API 密钥与

MFA）去执行管理或安全相关的任务。如果攻击者能够与代理交互，理论上他们可以诱使代理允许攻击者获得更大的访问权限或代表攻击者执行某些任务。同时，攻击者还有可能获得软件代理凭证的访问权限，并在执行任务时冒充该代理。

6 零信任架构及与现有联邦政府引导的相互作用

联邦政府的一些围绕着 ZTA 的规划、部署和运营的政策和指南已经发布。这些策略不会阻碍企业向更高阶的零信任架构转移，但会促进机构对于零信任策略的开发应用。 结合现有的网络安全政策和指南、ICAM、持续监视和一般网络安全，零信任架构 ZTA 能够加强组织的安全态势，并防御常见威胁。

6.1 ZTA 和 NIST 风险管理框架（RMF）

零信任架构 ZTA 部署过程会涉及围绕指定任务或业务流程的制定风险相关的访问策略（请参阅第 7.3.3 节）。为了保证安全，可以默认拒绝所有对资源的网络访问，并且仅允许通过已连接的终端进行访问。但是在大多数情况下，这种不成比例的过度限制会阻碍工作的完成。当联邦机构执行其工作任务时，风险需要在一个可接受的水平，且执行任务的相关风险必须被确定、评估和规避。为此，NIST 制定了风险管理框架（RMF）。

ZTA 计划和实施可能会更改企业定义的授权边界。 这是由于增加了新的组件（例如，PE、PA 和 PEP），并减少了对网络边界防御的依赖。RMF 中描述的整个过程在零信任架构 ZTA 中不会改变。

6.2 ZT 和 NIST 隐私框架

保护用户隐私和私人信息（例如，个人身份信息）的隐私是组织机构的首要

任务之一。隐私和数据保护已包含在合规项目中，例如 FISMA 和《健康保险可移植性和责任法案》（HIPAA）。 作为回应，NIST 制定了供组织使用的隐私框架[NISTPRIV]。该文档提供了一个框架来描述隐私风险和缓解策略，以及企业对于用户隐私和私人信息存储及处理的识别、衡量和规避风险。这包括企业用于支持 ZTA 操作的个人信息及访问请求评估中使用的任何生物统计属性。

零信任架构 ZTA 的部分核心要求是企业应检查和记录其环境中流量（或加密流量中的元数据），其中一些流量可能包含私人信息或具有相关的隐私风险。组织机构将需要确定与拦截、扫描和记录网络流量有关的任何可能的风险[NISTIR 8062]。这可能包括诸如通知用户、获得同意（通过登录页面、横幅或类似方式）以及指导企业用户等操作。NIST 隐私框架有助于建立一个正式流程，以识别和规避企业开发零信任架构面临的任何与隐私有关的风险。

6.3 ZTA 和联邦身份、凭证和访问管理体系结构（FICAM）

用户配置是零信任架构 ZTA 的关键组成部分。如果 PE 没有足够的信息来标识关联的用户和资源，则 PE 无法确定尝试的连接是否被授权连接到资源。在转向零信任度更高的部署之前，需要有强有力的用户配置和身份验证策略。企业需要一套清晰的用户属性和策略能够被 PE 用来评估访问请求。

管理和预算办公室（OMB）发布了 M-19-17，内容涉及改善联邦政府的身份管理。 该政策的目标是发展“……一个将身份作为实现国家使命、信任度和安全的推动力的共同愿景” [M-19-17]。 该备忘录呼吁所有联邦机构组建一个 ICAM 办公室，以期管理关于身份的发放的有关工作。这些管理策略中大部分应

使用 NIST SP 800-63-3 “数字身份准则” [SP800-63]中的建议。由于 ZTA 高度依赖精确的身份管理，因此 ZTA 的任何工作都需要整合该机构的 ICAM 政策。

6.4 ZTA 和可信 Internet 连接（TIC）3.0

可信互联网连接（TIC）是一项联邦网络安全计划，由管理和预算办公室（OMB），国土安全部网络安全和基础设施安全局（DHS CISA）以及总务管理局共同管理，以建立整个联邦政府网络安全基准线。从历史上看，TIC 是基于边界的网络安全策略，要求各机构整合和监控其外部网络连接。TIC 1.0 和 TIC 2.0 中固有的假设是边界以内是受信任的，而零信任架构 ZTA 则假定网络位置不能推断出信任（即，机构的内部网络也认为是不可信的）。 TIC 2.0 提供了一系列基于网络的安全功能（例如，内容过滤、监控、身份验证）部署在机构边界的 TIC 接入点上，其中许多功能都与 ZTA 保持一致。

TIC 3.0 已经被更新以适应云服务和移动设备[M-19-26]。在 TIC 3.0 中，人们认识到 "信任 "的定义可能会因具体的计算环境而有所不同，而且各机构在定义信任区时有不同的风险容忍度。此外，TIC 3.0 还更新了《TIC 安全能力手册》，定义了两类安全能力。(1)通用安全能力，适用于企业级；(2)PEP 安全能力，是网络级能力，适用于多个策略执行点(PEP)，如 TIC 用例所定义。PEP 安全能力可应用于沿给定数据流的任何适当的 PEP，而不是机构周边的单个 PEP。这些 TIC 3.0 安全能力中有许多直接支持 ZTA（例如，加密流量、强认证、微隔离、网络和系统清单等）。TIC 3.0 定义了具体的用例，这些用例描述了在特定应用、服务和环境中实现信任区和安全能力。

TIC 3.0 专注于基于网络的安全保护，而 ZTA 是一种更具包容性的体系结构，可解决应用程序、用户和数据的保护问题。随着 TIC 3.0 用例的演进，将来很可能开发 ZTA TIC 用例来定义将在 ZTA 实施点部署的网络保护。

6.5 ZTA 和 EINSTEIN（NCPS-国家网络安全保护系统）

NCPS（也称为 EINSTEIN）是一个提供入侵检测、高级分析、信息共享和入侵防御功能的集成系统，可保护联邦政府免受网络威胁。NCPS 的目标与零信任的总体目标一致，旨在管理网络风险和改善网络保护，并赋予合作伙伴确保网络空间安全的能力。EINSTEIN 传感器使 CISA 的国家网络安全和通信集成中心能够捍卫联邦网络，并应对联邦机构发生的重大事件。

NCPS 传感器的位置基于联邦政府的边界网络防御，而零信任体系结构使保护更接近数据和资源。NCPS 计划正在不断发展，以确保通过利用云端流量的安全信息来维护态势感知，帮助为 ZTA 系统扩展态势感知遥测奠定基础。NCPS 的入侵预防功能也需要演进，以便能够为当前 NCPS 地点以及 ZTA 系统的政策执行提供信息。随着整个联邦政府采用 ZTA，NCPS 的实施将需要不断发展，或者需要部署新的功能来实现 NCPS 的目标。事件响应者可以利用联邦机构已实施零信任架构的身份验证、流量检查以及流量日志中的信息。零信任架构中产生的信息可以更好地为事件影响量化提供信息；机器学习工具可以使用零信任架构数据来改进检测；零信任架构中的额外日志可以被保存下来，供事件响应者事后分析。

6.6 ZTA 和 DHS 连续诊断和缓解（CDM）计划

DHS CDM 计划是一项旨在改善联邦机构信息技术（IT）的工作。 对于这种情况至关重要的是机构在资产、配置等方面的自身洞察力。为了保护系统，各机构需要建立过程发现和了解其基础结构中的基本组件和参与者：

- **连接了什么？** 组织机构中使用哪些设备，应用程序和服务？ 这包括发现漏洞和威胁时监测并改善这些资产的安全状态。
- **谁在使用网络？** 哪些用户是组织机构的一部分，或者是外部用户但是允许访问企业资源？ 这其中包括 NPEs（非人类实体）正在执行的自动的操作。
- **网络上正在发生什么？**企业需要深入了解系统间的流量模式和交互消息。
- **数据如何受到保护？** 企业需要制定一套信息在存储、传输和使用中信息保护的保护策略。

拥有一个强大的 CDM 实施计划是 ZTA 成功的关键。例如，要迁移到 ZTA，企业必须具有发现和记录物理和虚拟资产以创建可用清单的系统。国土安全部 CDM 计划已启动了数项工作，以建立联邦机构内部转移到 ZTA 所需的功能。例如，DHS 硬件资产管理（HWAM）[HWAM]计划旨在帮助机构识别其网络基础设施上的设备以便部署安全配置。这类似于制定 ZTA 路线图的第一步，机构必须对网络中的活动资产（或那些远程访问资源的资产）具有可见性，以便对网络活动进行分类、配置和监控。

6.7 ZTA，智能云和联邦数据策略

智能云策略、更新后的数据中心优化计划[M-19-19]政策以及联邦数据策略

都会对规划 ZTA 机构的某些要求造成影响。这些策略要求机构盘点和评估它们是如何收集、存储和访问本地及云上数据的。这项工作非常重要，它可以确定哪些业务流程和资源可以从 ZTA 实施中受益。如果数据和服务主要基于云，或者员工主要使用远程办公的形式办公，这种情况下由于用户和资源位于企业网络边界之外，那么零信任架构 ZTA 就是一个很好的架构方案（请参阅第 7.3.3 节），它可以使你在可用性、可扩展性和安全性方面会获得最大收益。联邦数据战略的另一个考虑因素是如何使某机构的数据被其他机构或公众访问。这与跨企业协作零信任架构 ZTA 案例相对应（请参见第 4.4 节）。在制定策略时，这些应用 ZTA 的联邦机构可能需要考虑协作或发布要求。

7 迁移到零信任架构

实施零信任架构 ZTA 是一个过程，而不是全面替换基础设施或流程。企业应寻求逐步实施零信任的原则、流程变革和技术解决方案，以保护其最高价值的数据资产。大多数企业将在一段不确定的时间内继续以“零信任+边界防御”的混合模式运营，同时继续投资于持续的 IT 现代化举措。制定一个 IT 现代化计划，包括转向基于 ZT 原则的架构，可以帮助企业形成小规模工作流迁移的路线图。企业如何迁移到某一战略，取决于其当前的网络安全态势和运营情况。企业应达到能力基准，再部署以零信任为中心的重要环境[ACT-IAC]。这个基准包括为企业确定资产、用户和业务流程，并对其进行分类。企业需要有这些信息，然后才能制定一个候选业务流程和该流程所涉及的用户/资产清单。

7.1 纯零信任架构

在从零新建模式中，可以从头开始建立一个零信任架构。假设企业知道它想在运营中使用的应用和工作流程，就可以为这些工作流程建立一个基于零信任原则的架构。一旦确定了工作流程，企业就可以缩小所需的组件范围，并开始绘制各个组件的交互方式。从这一点上看，这就是构建基础设施和配置组件的工程和组织工作。这可能包括根据企业目前的设置和运营方式，进行额外的组织变革。

在实际情况中，这种模式对于联邦机构或任何拥有现有网络的组织机构来说，基本不是一个可行的选择。然而，有时可能会要求一个组织机构履行一项全新的职责，这项职责需要建立自己的基础设施。在这种情况下，也许可以在一定程度

上引入零信任概念。例如，一个机构可能被赋予一个新的职责，需要建立一个新的应用程序和数据库。该机构可以围绕零信任原则来设计新的基础设施，例如，在授予访问权限之前，对用户的信任度进行评估，并在新资源的周围设置微边界。成功的程度取决于这个新的基础设施对现有资源（如身份管理系统）的依赖程度。

7.2 零信任架构和基于边界的传统架构并存

任何一个具备规模的企业不太可能在一个技术更迭周期内迁移到零信任。零信任架构工作流程在传统企业中可能会有一段不确定的共存期。企业向零信任架构方式的迁移可能会在一个个业务流程中进行。企业需要确保共同的元素（如身份管理、设备管理、事件日志）足够灵活，以便在零信任架构和基于边界防御的混合安全架构中运行。企业架构师可能也希望在零信任架构方案选型时选择那些能够与现有组件对接的解决方案。将现有的工作流迁移到 ZTA 中，很可能需要（至少）进行部分重新设计。如果企业尚未对工作流采用安全系统工程[SP800-160v1]做法，则可借此机会采用这种做法。

7.3 在基于传统架构的网络中引入零信任架构的步骤

迁移到零信任架构需要组织对其资产（物理和虚拟）、用户（包括用户权限）和业务流程有详细的了解。在评估资源请求时，PE 会访问这些信息。不完整的信息往往会导致业务流程失败，即 PE 因信息不足而拒绝请求。如果企业内部存在未知的 "影子 IT "部署，那么这个问题就显得尤为突出。

在将零信任架构引入企业之前，应该对资产、用户、数据流和工作流进行调

查。这是零信任架构部署之前必须达到的基础状态。如果对当前的运营状态不了解，企业就无法确定需要建立哪些新的流程或系统。这些调查可以同时进行，但两者都与企业业务流程的检查联系在一起。这些步骤与 RMF[SP800-37] 相关联，因为采用零信任架构都是降低机构业务职能风险的过程。图 12 显示了实施零信任架构的路径。

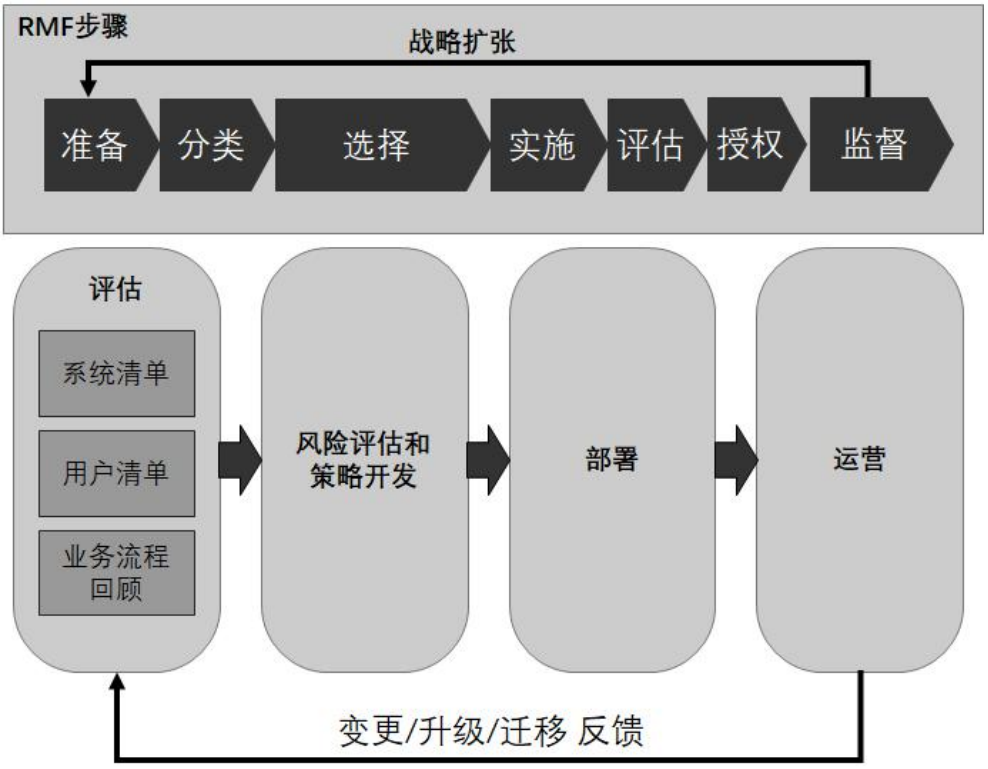

图 12：零信任架构部署周期

在初始清单建立后，有一个定期的维护和更新周期。这种更新可能会改变业务流程，也可能不会产生任何影响，但应该对业务流程进行评估。例如，数字证书提供商的变更可能看起来没有明显的影响，但可能涉及到证书根库管理、证书透明日志监控以及其他一开始并不明显的因素。

7.3.1 确定企业中的参与方

对于一个零信任企业来说，PE 必须对企业主体有一定的了解。主体可以包括人和可能的非人类实体(NPE)，如与资源交互的服务账户等。

拥有特殊权限的用户，如开发人员或系统管理员，在被分配属性或角色时，需要进行额外的审查。在传统的安全架构中，这些账户可能拥有访问所有企业资源的一系列权限。零信任架构应该允许开发人员和管理员有足够的灵活性来满足他们的业务需求，同时使用日志和审计操作来识别访问行为模式。零信任架构部署可能要求管理员满足 NIST SP 800-63A 第 5 节[SP800-63A]中概述的更严格信任级别或标准。

7.3.2 识别企业自有资产

如 2.1 节所述，零信任架构的关键要求之一是识别和管理设备的能力。零信任架构还要求有能力识别和监控可能在企业自有网络基础设施上或访问企业资源的非企业自有设备。管理企业资产的能力是零信任架构成功部署的关键。这包括硬件组件（如笔记本电脑、电话、IoT 设备）和数字制品（如用户账户、应用程序、数字证书）。有可能无法对所有企业自有资产进行完整的普查，因此企业应该考虑进行能力建设，以便对企业自有基础设施上新出现的资产进行快速识别、分类和评估。

这不仅仅是简单地对企业资产进行编目和维护数据库，还包括配置管理和监控。观察资产当前状态的能力是评估访问请求过程的一部分（见 2.1 节）。这意味着企业必须能够配置、调查和更新企业资产，例如虚拟资产和容器等企业资产。

这还包括其物理位置（作为尽量预估）和网络位置。在做出资源访问决策时，这些信息应该为策略引擎 PE 提供参考。

非企业拥有的资产和企业拥有的 "影子 IT "也应尽可能地编入目录。这可以包括企业能看到的任何信息（例如，MAC 地址、网络位置），并通过管理员数据录入的方式加以补充。这些信息不仅用于访问决策（因为合作者和 BYOD 资产可能需要访问策略执行点），还可以用于企业的监控和取证记录。影子 IT 带来了一个特殊的问题，因为这些资源是企业所拥有的，但不像其他资源那样被管理。某些零信任架构方法（主要是基于网络的）甚至可能会导致影子 IT 组件无法使用，因为它们可能不为人所知，也不包括在网络访问策略中。

许多联邦机构已经开始识别企业资产。已建立持续诊断和缓解(CDM)计划能力的机构，如硬件资产管理[HWAM]和软件资产管理(SWAM)[SWAM]等，在制定零信任架构时有丰富的数据可供借鉴。各机构还可能有一份涉及高价值资产（HVA）[M-19-03]的零信任架构候选流程清单，这些资产已被确定为机构任务的关键。这项工作需要在企业或机构范围内进行，然后才能用零信任架构（重新）设计任何业务流程。这些方案的设计必须具有可扩展性和适应性，以适应企业的变化，不仅在向零信任架构迁移时，而且在核算成为企业的一部分的新资产、服务和业务流程时，也必须如此。

7.3.3 确定关键流程并评估其运行风险

一个机构应进行的第三项清查是对业务流程、数据流及其在机构任务中的关系进行识别和排序。业务流程应说明在何种情况下批准和拒绝资源访问请求。企

业可能希望从低风险的业务流程开始向零信任架构过渡，因为业务中断可能不会对整个组织产生负面影响。一旦获得足够的经验，更关键的业务流程就可以成为候选对象。

利用基于云的资源或由远程员工使用的业务流程通常是零信任架构的良好候选对象，并可能会看到可用性和安全性的改善。企业用户应该可以直接访问云服务，而不是将企业边界扩展到云上或者通过 VPN 将用户接入企业内网。企业的 PEP 确保在授予客户端访问资源的权限之前，企业安全策略是被执行的。规划人员还应考虑在为特定业务流程实施 ZTA 时，在性能、用户体验和可能增加的工作流脆弱性方面的潜在折衷。

7.3.4 如何选择零信任架构实施对象

确定候选应用程序或业务工作流的过程取决于几个因素：该流程对组织的重要性、受影响的用户群体以及工作流所使用资源的当前状态。可以使用 NIST 风险管理框架[SP800-37]对资产或工作流的价值进行评估。

在确定资产或工作流后，确定所有使用或受工作流影响的上游资源（如身份管理系统、数据库、微服务）、下游资源（如日志、安全监控）和实体（如用户、服务账户）。这可能会影响作为第一次迁移到零信任架构的待选对象选择。相比对企业的整个用户群至关重要的应用程序（如电子邮件），一个确定性高、范围小的企业用户群体所使用的应用程序（如采购系统）可能是首选。

然后，企业管理员需要为候选业务流程中使用的资源确定一组阈值（如果使用基于阈值的信任算法）或信任等级权重（如果使用基于评分的信任算法）（请

参阅第 3.3.1 节）。管理员可能需要在调优阶段对这些阈值或权重进行调整。这些调整应该确保策略有效但不妨碍资源的访问。

7.3.5 确定候选解决方案

一旦制定了一个候选业务流程清单，企业架构师就可以编制一个候选解决方案清单。有些部署模式（请参阅第 3.1 节）更适合特定的工作流程和当前的企业生态系统。同样，有些厂商的解决方案也比其他厂商的解决方案更适合某些用例。通常考虑以下因素：

- **该解决方案是否要求在终端资产上安装组件？**这可能会不利于使用非企业自有资产访问的业务流程，如 BYOD 或跨机构协作等。
- **在业务流程资源完全存在于企业本地的情况下，该解决方案是否可以工作？**有些解决方案假设所请求的资源部署在云端（所谓的南北流量），而不是在企业边界内（东西流量）。候选业务流程中资源的位置将影响候选解决方案以及流程的零信任架构。
- **该解决方案是否提供交互记录以进行分析的方法？**零信任的一个关键组成部分是收集和使用与流程流相关的数据，在做出访问决策时，这些数据会反馈到 PE 中。
- 该解决方案是否为不同的应用、服务和协议提供广泛的支持？一些解决方案可能支持广泛的协议（Web、SSH 等）和传输（IPv4 和 IPv6），而其他解决方案可能只支持有限的重点，如 Web 或电子邮件。
- 该解决方案是否需要改变用户行为？一些解决方案可能需要额外的步骤来

执行给定的工作流。这可能会改变企业用户执行工作流的方式。

一种解决方案是将现有的业务流程建模为试点方案，而不仅仅是替代方案。这种试点计划可以是通用的，以适用于多个业务流程，也可以是特定于一个用例。在将用户过渡到零信任架构部署并脱离传统的流程基础设施之前，可以将试点方案作为零信任架构的 "试验场"。

7.3.6 初期部署和监控

一旦选定了候选工作流程和零信任架构组件，就可以开始启动部署。企业管理员必须通过使用选定的组件来实现所制定的策略，但一开始可能希望以观察和监控的方式进行操作。在第一次迭代时，很少有企业策略集是完整的：重要的用户账户（例如管理员账户）可能会被拒绝访问他们需要的资源，或者他们所分配的全部访问权限并不是必须的。

新的零信任业务工作流可以在一段时间内以“报告模式”运行，以确保策略是有效和可行的。这也使企业能够了解基线资产和资源访问请求、行为和通信模式。报告模式意味着应该对大多数请求授予访问权限，并将连接的日志和跟踪的痕迹与最初制定的策略进行比较。基本的策略，如拒绝多因子认证失败的请求或从已知的、黑名单的 IP 地址出现的请求，应该强制执行并记录下来，但在初始部署后，访问策略应该更加宽松，以便从零信任工作流的实际交互中收集数据。一旦建立了工作流的基线活动模式，就可以更容易地识别异常行为。如果无法做到更加宽松的操作，企业网络运营者应密切关注日志，并随时根据运营经验修改访问策略。

7.3.7 扩大零信任架构的范围

当获得足够的信心，工作流策略集细化后，企业进入稳定运行阶段。仍然需要对网络和资产进行监控，并对流量进行记录（请参阅第 2.2.1 节），但响应和策略修改的节奏较慢，因为应该不会很严重。所涉及的资源和流程的用户和利益相关者也应该提供反馈，以改善运营。在这个阶段，企业管理员可以开始规划下一阶段的零信任部署。和之前的部署一样，需要确定一个候选工作流程和解决方案集，并制定初步的策略。

但是，如果工作流程发生变化，则需要重新评估运行的零信任架构。系统的重大变化，如新设备、软件（尤其是零信任逻辑组件）的重大更新，以及组织结构的变化，都可能导致工作流程或策略的变化。实际上，整个流程应该在假设部分工作已经完成的前提下重新考虑。例如，新设备已经购买了，但没有创建新的用户账户，因此只需要更新设备清单。

参考资料

[ACT-IAC]	美国技术和工业咨询委员会（2019）零信任网络安全现状趋势。https://www.actiac.org/zero-trust-cybersecurity-current-trends
[Anderson]	Anderson B, McGrew D (2017) 使用机器学习对恶意软件的加密流量进行识别分类: 噪声标记与非静态计量。计算机械协会(ACM)知识发现和数据挖掘特别关注组(SIGKDD)第23届国际会议论文集(ACM，哈利法克斯，新斯科舍省，加拿大), 1723页-1732页，https://doi.org/10.1145/3097983.3098163
[BCORE]	国防部首席信息官（2007）。国防部全球信息网格架构愿景版本 1.0 2007年6月。http://www.acqnotes.com/Attachments/DoD%20GIG%20Architectural%20Vision,%20June%2007.pdf
[CSA-SDP]	云安全联盟(2015)SDP规范1.0。2015年4月 https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/
[FIPS199]	国家标准与技术研究院（2004）联邦信息和信息系统安全分类标准。(美国商务部，华盛顿特区)，联邦信息处理标准出版物 (FIPS)

	199。https://doi.org/10.6028/NIST.FIPS.199
[Gilman]	Gilman E, Barth D(2017)零信任网络：在不可信网络中构建安全系统(O’ Reilly媒体有限公司，塞巴托波尔，加利福尼亚)，第一版。
[HWAM]	国土安全局(2015)硬件资产管理(HWAM)功能说明。https://www.us-cert.gov/sites/default/files/cdm_files/HWAM_CapabilityDescription.pdf
[IBNVN]	R. Cohen, K. Barabash, B. Rochwerger, L. Schour, D. Crisan, R. Birke, C. Minkenberg, M. Gusat, R. Recio 和V. Jain. 一种基于意图的网络虚拟化方法。2013 IFIP/IEEE综合网络管理国际研讨会。(IM 2013) 42页-50页 https://ieeexplore.ieee.org/xpl/conhome/6560458/proceeding
[JERICHO]	Jericho论坛(2017)原则条款 版本1.2 https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf
[M-19-03]	管理和预算办公室（2018）通过加强高价值资产计划加强联邦机构的网络安全。（白宫，华盛顿特区），OMB备忘录M-19-03，2018年12月10日。

	https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
[M-19-17]	管理和预算办公室（2019）通过改进身份、凭据和访问管理实现任务交付。（白宫，华盛顿特区），OMB备忘录M-19-17，2019年5月21日 https://www.whitehouse.gov/wpcontent/uploads/2019/05/M-19-17.pdf
[M-19-19]	管理和预算办公室 （2019） 数据中心优化计划 （DCOI） 更新。（白宫，华盛顿特区），OMB备忘录M-19-19，2019年6月25日。 https://datacenters.cio.gov/assets/files/m_19_19.pdf
[M-19-26]	管理和预算办公室 （2019） 更新可信互联网连接 （TIC） 计划。（白宫，华盛顿特区），OMB备忘录M-19-26，2019年9月12日 https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf
[NISTIR 7987]	Ferraiolo DF, Gavrila S, Jansen W (2015) 政策机器：功能、架构和规范。（美国国家标准与技术研究院，马里兰州盖瑟斯堡），NIST机构间报告或内部报告（IR） 7987，修订版1

	https://doi.org/10.6028/NIST.IR.7987r1
[NISTIR 8062]	Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) 联邦系统的隐私工程和风险管理简介。（美国国家标准与技术研究院，马里兰州盖瑟斯堡），NIST机构间报告或内部报告（IR） 8062。 https://doi.org/10.6028/NIST.IR.8062
[NISTPRIV]	国家标准与技术研究院（2020）隐私框架：通过企业风险管理改善隐私的工具。版本 1.0 2020 年 1 月 16 日。 https://www.nist.gov/privacy-framework/privacy-framework
[SDNBOOK]	T. Nadeau and K. Gray (2013) SDN：软件定义的网络：网络可编程技术的权威回顾。（O’Reilly）第一版
[SP800-37]	联合工作组（2018）信息系统和组织风险管理框架：安全和隐私的系统生命周期方法。（美国国家标准与技术研究院，盖瑟斯堡，马里兰州），NIST特别出版物（SP） 800-37，修订版2 https://doi.org/10.6028/NIST.SP.800-37r2
[SP800-63]	Grassi PA, Garcia ME, Fenton JL (2017) 数字身份指南。（美国马里兰州盖瑟斯堡国家标准与技术研究院），NIST 特别出版物 （SP） 800-63-3，包括截至 2017 年 12 月 1 日的更新 https://doi.org/10.6028/NIST.SP.800-63-3

[SP800-63A]	Grassi PA, Fenton JL, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) 数字身份指南：注册和身份证明。（美国马里兰州盖瑟斯堡国家标准与技术研究院），NIST 特别出版物（SP）800-63A，包括截至2017年12月1日的更新。https://doi.org/10.6028/NIST.SP.80063A
[SP800-160v1]	Ross R，McEvilley M，Oren JC（2016）系统安全工程。可信安全系统工程中多学科方法的考虑因素。（美国国家标准与技术研究院，马里兰州盖瑟斯堡），NIST Special Publication（SP）800-160，Vol. (National Institute of Standards and Technology，Gaithersburg，MD)，NIST Special Publication (SP) 800-160，Vol.1，包括截至2018年3月21日的更新。https://doi.org/10.6028/NIST.SP.800-160v1。
[SP800-160v2]	Ross R, Pillitteri V, Graubart R, Bodeau D, and McQuaid R (2019) 开发网络弹性系统：系统安全工程方法。（美国马里兰州盖瑟斯堡国家标准与技术研究院），最终公开草案 NIST 特别出版物 （SP） 800-160，第 2 卷。https://csrc.nist.gov/publications/detail/sp/800-160/vol2/draft
[SP800-16	Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller

2]	R, Scarfone KA (2014) 基于属性的访问控制 （ABAC） 定义和注意事项指南。(美国马里兰州盖瑟斯堡国家标准与技术研究院)，NIST 特别出版物 （SP）800-162，包括截至2019 年2月25日的更新 https://doi.org/10.6028/NIST.SP.800-162
[SWAM]	国土安全局(2015) 软件资产管理（SWAM）功能说明。https://www.uscert.gov/sites/default/files/cdm_files/SWAM_CapabilityDescription.pdf

附录 A 缩略语

API	应用程序编程接口
BYOD	自带设备
CDM	持续诊断和缓解
DHS	国土安全局
DoS	拒绝服务
G2B	政府对企业（私营企业）
G2G	政府对政府
NIST	国家标准与技术研究院
NPE	非人类实体
PA	策略管理器
PDP	策略决策点
PE	策略引擎
PEP	策略执行点

PKI	公钥基础设施
RMF	NIST风险管理框架
SDN	软件定义网络
SDP	软件定义边界
SIEM	安全信息和事件监控
TIC	可信的互联网连接
VPN	虚拟专用网络
ZT	零信任
ZTA	零信任架构

附录 B 识别 ZTA 当前技术水平的差距

对于零信任组件和解决方案的当前成熟度，在本文档的背景研究期间进行了调查。这个调查给出结论：ZTA 生态系统还没有成熟到足以大范围应用的程度。虽然可以使用 ZTA 策略去规划和部署一个企业环境，但是没有一个解决方案提供所有的必需组件。能够在企业所有工作流场景下使用的组件还很少。

以下是 ZTA 生态系统和需要进一步调查的领域中识别出的差距的总结。其中某些领域已经有一些基础，但是 ZTA 准则将如何改变这些领域还不清楚，因为在这些不同的以 ZTA 为重心的企业场景中，我们目前的经验还不够。

B.1 技术调查

多个供应商受邀展示了他们关于零信任的产品和观点。本次调查的目标是找出那些阻碍机构现在迁移到 ZTA 基础设施或维护现有 ZTA 部署的遗漏部分。这些差距可分类为即时部署（即时或短期）、影响运维或运营的系统性差距（短期或中期）、知识缺失（未来研究领域）。表 B-1 总结了这些内容：

表 B-1：关于部署的认知盲区汇总

分类	问题示例	认知盲区
立即部署	● 如何编制采购要求 ● ZTA 规划如何与 TIC、FISMA 等其他需求整合。	● 缺乏 ZTA 的通用框架和词汇； ● 认识到 ZTA 与现行政策的冲突；

系统性	● 如何防止供应商锁定； ● 不同的 ZTA 环境如何相互作用；	● 过于依赖供应商 API；
需要进一步研究的领域	● 面对 ZTA，威胁将如何演变？ ● 面对 ZTA，业务流程如何变化？	● 已经采用 ZTA 的企业中，成功的入侵是什么样的？ ● 记录采用 ZTA 的企业中的最终用户体验；

B.2 阻碍立即转移至 ZTA 的鸿沟

这些都是目前阻碍 ZTA 战略采用的问题。这些问题被归类为“立即的”问题，考虑未来维护或迁移的问题没有没有被划分在这个类别。一个前瞻性思考的企业也许会把运维问题分类也作为阻碍 ZTA 初始部署的考量问题，但是这些问题在这个分析中会作为独立的分类。

B.2.1）缺乏 ZTA 设计、规划和采购的通用术语

零信任在企业基础设施的设计和部署方面仍旧是一个发展阶段中的概念。业界还没有一套术语或概念来描述零信任架构 ZTA 的组件和运行。这使得组织（如联邦机构）很难为设计 ZTA 基础设施和采购组件制定一致的要求和政策。

本文档的 2.1 和 3.1 小结试图努力为描述 ZTA 的术语和概念建立一个中性的基础。开发抽象的 ZTA 组件和部署模型作为思考 ZTA 的基础术语和方法。目

标是为开发企业需求和执行市场调研时提供一个思考 ZTA 的共同的视图、模型和讨论方法。以上的章节在联邦机构获取更多 ZTA 经验时可能会被证明是不完整的，但是目前可以作为公共概念框架的基础。

B.2.2）关于 ZTA 与现有联邦网络安全政策冲突的认知

有一种误解认为零信任架构 ZTA 是一个带有解决方案集合的单一框架，且与现有的网络安全概念并不兼容。而实际上，零信任应该被视为当前网络安全战略的演变，因为许多概念和想法已经存在发展了很长时间。鼓励联邦机构在网络安全方面通过现有的指南采用更加零信任的方法。如果一个机构拥有成熟的身份管理系统和强大的 CDM 能力，那么它已经在通往 ZTA 战略的路上。这一差距其实是源于对 ZTA 的误解以及它是如何从以前的网络安全范式演变而来的。

B.3 影响 ZTA 的系统性差距

这些差距影响了零信任架构 ZTA 战略的初始实现和部署，以及持续运营/成熟度。这些差距表明机构对 ZTA 的接受或者 ZTA 组件产业界的碎片化。系统的差距是开放标准（由标准开发组织（SDO）或行业联盟制定）可以发挥助力的领域。

B.3.3）组件间接口的标准化

在技术调查中表明没有一个厂商能独立提供一套完整的零信任解决方案。更进一步讲:采取单一厂商解决方案完成零信任架构是不可能的，而且这样还会导

致供应商锁定。这就导致组件内部的互操作性问题，不仅发生在采购的时候，而且会随着时间推移一直存在。

在更广泛的企业应用领域中，组件的范围非常广泛，许多产品专注于 ZTE 内部的单个市场定位，并依赖于其他产品来向另一个组件提供数据或某些服务（例如，为资源访问而集成多因素认证（MFA））。供应商常常依赖合作伙伴提供的专有 API，而不是标准化的、独立于供应商的 API 来实现这种集成。这种方法的问题在于，这些 API 是专有的，由单个供应商控制。一旦供应商改变 API 的行为，将导致集成商需要更新他们的产品来响应。这就要求供应商社区之间建立密切的合作关系，以确保及早通知 API 内的修改，这可能会影响产品之间的兼容性。这给供应商和消费者增加了额外的负担：供应商需要花费资源对其产品进行改变，当一个供应商对其专有 API 进行变更时，消费者需要把变更应用到多个产品。另外供应商需要为每个合作伙伴组件实现和维护一个封装器以提供最大的兼容性和互操作性.例如，需要 MFA 产品供应商被要求为不同的云服务商或者身份管理系统创建不同的封装器，以便这些系统能在不同种类的客户组合场景下仍旧可用。

在客户侧，这在制定产品采购需求时产生了额外的问题。购买者没有标准可以用来识别产品之间的兼容性。因此，很难为迁移 ZTA 架构创建一个多年的路径图，因为无法确定一套最低限度的组件兼容性要求。

B.3.4）解决过度依赖专有 API 的新兴标准

没有一个开发 ZTA 架构的完整解决方案，在构建零信任企业架构方面，也

没有一个完整的工具服务集可用。因为想用一个单独的协议或框架来赋能企业迁移到 ZTA 架构几乎是不可能的。目前有很多的模型和解决方案谋求获得 ZTA 方面的主导权。

这表明有机会开发一套开放的、标准化的协议（或框架），以帮助组织迁移到 ZTA 战略。标准开发组织（SDO）如 Internet 工程任务组（IETF）已经指定了在交换威胁信息时可能有用的协议。云安全联盟（CSA）已经为软件定义边界（SDP）开发了一个框架，该框架在 ZTA 中也很有用。大家的努力的方向应该是探讨 ZTA 相关框架的当前状态以及确认我们应该在那些方面创建和增强标准。

B.4 ZTA 的认知差距与未来研究方向

此节列出的差距，并不妨碍组织为其企业采用 ZTA 战略。这些是关于运行 ZTA 环境的知识的灰色区域。绝大多数是因为缺乏 ZTA 成熟部署的时间和经验。它们是未来研究人员的工作领域。

B.4.5）攻击者对 ZTA 的反击

对一个企业来说，一个正确实施的零信任架构 ZTA 相对于传统的基于网络边界的安全而言，将提升其网络安全。ZTA 的宗旨是减少对攻击者的资源暴露，并在主机系统被攻陷时，最小化（或防止）攻击在企业内部的横向扩展。

然而，坚定的攻击者不会坐以待毙，而是会改变面对 ZTA 的行为。一个开放的话题是攻击将如何演变。一种可能性是旨在窃取凭证的攻击可能会扩展为以 MFA(多因素认证)为目标（例如网络钓鱼、社会工程）。另一种可能性是，在混

合型 ZTA 或边界防御为主的企业中，攻击者将重点关注尚未应用 ZTA 原则的业务流程（即执行传统的基于网络边界的安全策略的那些）。 最有效的方式是将目标指向最容易摘到的果子，试图在 ZTA 业务流程中获得一些立足点。

随着 ZTA 的更加成熟，实现了更多的部署，并获得了经验，ZTA 相对于基于网络边界安全的旧方法的优势将会变得显而易见。此外，还需要制定 ZTA 相对于较老网络安全策略的“成功”指标。

B.4.6）ZTA 环境中的用户体验

对于最终用户在使用 ZTA 战略的企业中表现得如何，还没有进行严格的审查。主要是因为缺乏可供分析的大型 ZTA 落地案例。已有研究表明，用户面对 MFA 和其他安全运营(被视为 ZTA 企业战略的一部分)的反应是什么样。这项工作可以成为在企业中使用 ZTA 工作流时预测最终用户体验和行为的基础。

一些研究可以预测 ZTA 如何影响最终用户体验的，这些研究是在企业 MFA 落地应用和安全疲劳方面工作中完成。安全疲劳是指最终用户面对如此多的安全策略和挑战，开始以负面方式影响其生产力的现象。其他研究表明 MFA 改变用户行为，但是整个改变是混合的，一些用户很容易接受 MFA，如果这个过程是流畅的，并且涉及到他们习惯于使用或拥有的设备（例如，智能手机上的应用程序）。然而，有些用户讨厌用个人设备处理业务，或者觉得他们被持续监控，以防止可能违反 IT 政策

B.4.7）ZTA 对企业和网络中断的适应能力

对 ZTA 供应商生态系统的调查，表明企业部署 ZTA 战略需要考虑到广泛的 IT 基础设施。就像之前提到的，目前没有一个供应商能提供完整的零信任解决方案。造成的结果就是，企业需要购买若干种不同的服务和产品，这会导致组件间的依赖网。如果一个关键组件被破坏或不可达，可能会出现一连串的故障，影响一个或多个业务流程

大多数被调查的产品和服务，都依赖于云的存在以提供健壮性，但众所周知即使是云服务也会在在遭遇攻击或简单错误时变得不可用。当这种情况发生时，用于做出访问决策的关键组件，可能无法访问或无法与其他组件通信。例如，位于云中的 PE 和 PA 组件，可能在分布式拒绝服务（DDoS）攻击期间可访问，但可能无法访问所有位于资源中的 PEP。需要研究如何发现 ZTA 部署模型的可能的单点依赖瓶颈以及 ZTA 组件不可达或可访问性有限时对网络运行的影响。

在采用 ZTA 战略时，企业的运行连续性（COOP）计划可能需要修订。ZTA 战略使许多 COOP 因素变得更容易，因为远程工作者可能与他们在本地拥有相同的资源访问权限。然而，如果用户没有得到适当培训而缺乏经验，像 MFA 这样的策略也可能产生负面影响。用户可能会在突发情况下忘记（或无法访问）令牌或无法访问企业设备，这将影响企业业务流程的速度和效率。

B.5 ZTA 参考资料

[1] Cam-Winget N (ed.), Appala S, Pope S, Saint-Andre P (2019) Using Extensible Messaging and Presence Protocol (XMPP) for Security Information Exchange. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8600. https://doi.org/10.17487/RFC8600

[2] Software Defined Perimeter Working Group "SDP Specification 1.0" Cloud Security Alliance. April 2014.

[3] Stanton B, Theofanos MF, Spickard Prettyman S, Furman S (2016) Security Fatigue. IT Professional 18(5):26-32. https://doi.org/10.1109/MITP.2016.84

[4] Strouble D, Shechtman GM, Alsop AS (2009) Productivity and Usability Effects of Using a Two-Factor Security System. SAIS 2009 Proceedings (AIS, Charleston, SC), p 37. Available at http://aisel.aisnet.org/sais2009/37

[5] Weidman J, Grossklags J (2017) I Like It but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017) (ACM, Orlando, FL), pp 212-224. https://doi.org/10.1145/3134600.3

零信任架构实施

Implementing a Zero Trust Architecture

HUYHY8

Alper Kerman

Oliver Borchert

Scott Rose

国家网际安全卓越中心（NCCoE）

国家标准与技术研究院（NIST）

Eileen Division Allen Tan

麻省理工学院(MIT)

草案

2020 年 3 月

zta-nccoe@nist.gov

国家网络安全卓越中心(NCCoE)是国家标准与技术研究院(NIST)的一部分，并且是一个协作中心，行业组织、政府机构和学术机构在此合作，共同应对企业最紧迫的网络空间(Cybersecurity)安全挑战。通过这种协作，NCCoE 开发了模块化的、易于适应的网络安全解决方案，通过举例展示了如何利用商业化可获得的技术来实施标准和最佳实践。要了解更多关于 NCCoE 的信息，请访问 https://www.nccoe.nist.gov 。要了解 NIST 的更多信息，请访问 https://www.nist.gov。

本文描述了一个与许多行业领域相关的问题。NCCoE 网络安全专家将通过与包括网络安全解决方案供应商在内的利益共同体合作来应对这一挑战。由此产生的参考设计将细化该方案，该方案可以被多个领域集成。

摘要

云计算、移动设备使用和物联网的激增已经消除了传统的网络边界。企业安全方案必须不断发展，提供用户从任何位置和设备安全地访问公司资源的方式，保护与业务合作伙伴的交互，并保护客户端-服务器以及服务器间通信。

零信任网络空间安全方法消除了用户和网络的信任假定。它侧重于以安全的方式访问资源，而不管网络位置、用户和设备如何，实施严格的访问控制，并持续检查、监视和记录网络流量。这需要数据字段级保护、强大的身份验证架构和至关重要的微隔离，以便围绕组织的数字资源创建细粒度信任区域。零信任方案在整个开放的连接访问期间实时评估访问请求和网络流量行为，并根据策略持续一致地校正对组织资源的访问。面向零信任设计提供了系统之间几乎所有交互和访问决策的架构，使企业能够安全地适应各种业务案例的复杂性。

本 NCCoE 项目将展示一个基于标准实现的零信任架构。本项目说明的发布将首先开始于进一步确定项目需求和范围，以及该方案在实验室环境搭建所需要的软硬件组件。在实验室研究中，NCCoE 将构建一个模块化的端到端零信任架构范例，以解决一系列对齐 NIST 网络安全框架提出的网络安全挑战。本项目将提供一个免费可用的 NIST 网络安全实践指南。

关键词

网络空间安全(cybersecurity)；企业(enterprise)；网络安全(network security)；零信任(zero trust)；零信任架构(zero trust architecture)

免责声明

本文档中可能会涉及某些商业实体、设备、产品或材料，以便充分描述实验性的流程或概念。此类标识并不意味着 NIST 或 NCCoE 的推荐或认可，也不意味着暗示这些实体、设备、产品或材料一定最适合此目的。

NCCoE 文档反馈

鼓励各组织在公开反馈期间审阅所有文档草案并提供反馈意见。NIST 国家网际安全卓越中心的所有文档均可在 https://www.nccoe.nist.gov/ 上获取。

有关本发布的意见可以提交给 zta-nccoe@nist.gov

公开反馈收集截止：2020 年 4 月 14 日

1 执行摘要

1.1 目的

传统的网络安全侧重于边界防御 - 一旦进入网络边界内部，用户通常可以广泛访问许多企业资源。这意味着恶意行为者可以来自网络内部或外部。此外，云计算和远程员工的增加使组织数字资源的保护工作更加复杂，因为存在比以往更多的出入口和数据访问点。

组织不得不重新思考传统的网络安全边界。零信任体架构（ZTA）通过重点保护资源而不是网络边界来应对这一趋势，网络位置不再被视为资源安全态势的主要组成部分。

零信任是一套网络空间安全原则，用于创建策略，侧重于将网络防御从粗粒度的、静态网络边界转移到更细粒度的关注用户、系统以及个人或小组资源。ZTA 使用零信任原则来规划和保护企业基础设施和工作流。根据该设计原则，ZTA 环境不再包含对系统和用户隐含的信任，该信任与物理或网络位置（例如：局域网或互联网）无关。因此在用户和设备通过可靠的身份验证和授权进行彻底地验证之前，ZTA 不会授予其对资源的访问权限。

本文定义了国家网际安全卓越中心（NCCoE）的项目，以帮助组织为零信任进行设计。该项目将提供 ZTA 的示例实现，该 ZTA 实现是根据国家标准与技术研究院（NIST）特别文档（SP）800-207、零信任架构中记录的概念和原则设计部署的[1]。更具体地来说，此项目的主要目标是展示一个建议的

网络拓扑，该拓扑囊括了广泛分布于本地和云端的不同企业资源(例如：数据源，计算服务和物联网设备)并具备以下零信任架构 ZTA 的方案特征：

- 所有网络流量都会加密，与网络拓扑中的位置无关。
- 访问每项企业资源都是按单个连接来授权，且已授权连接不会被自动授权允许访问其它企业资源。
- 根据环境中获取的以下信息动态确定对企业资源的访问：
    - 组织策略，这主要用于：
        - 用户
        - 网络位置
        - 企业设备特征
        - 访问请求的日期时间
        - 企业资源特征
    - 可观测到的状态：
        - 访问请求的设备标识
        - 访问请求的企业资产
    - 以前观测到的与用户/设备标识和访问请求相关的行为
        - 识别并持续重新评估和监控企业资产、设备和资源，以将它们保持在最安全的状态。

- 通过多因子认证对用户与设备的交互尽可能地进行持续监控及重新认证和授权。
- 当前网络和通信状态的信息会被记录下来并用于后续更好的策略调整以提高企业的总体安全态势。

该项目的第二个目标是识别并尽可能减少由于采用上述特性的 ZTA 战略解决方案而对用户体验造成的负面影响。 一个成功的 ZTA 解决方案应该尽可能减少给用户带来不便。

这个项目将出版一个公共可获取的 NIST 网际安全实践指南，需要有每一步的详细实施指南，用来指导网际安全参考设计实施以实现项目目标。

1.2 范围

目前对零信任的理解集中在企业层面。通用企业信息技术（IT）基础设施将用户（包括员工、承包商和访客）、设备以及本地托管、云或两者的整合相结合。也可能有分支机构、远程工作人员和自带设备使用，这使得访问策略的构成和执行复杂化。

本项目将主要侧重于企业资源访问。更具体地说，重点将是企业员工、承包商和访客在从公司（或企业总部）网络、分支机构或互联网连接时访问企业资源的行为。接入请求可以发起在企业拥有的基础设施上或者公共/非企业拥有基础设施部分进行。 这就要求所有访问请求在授予访问权限之前都是安全的、授权的和验证的，无论请求是从哪里发起，无论资源在什么地点。

1.3 假设/挑战

许多组织都希望建立零信任，但也存在挑战。实施 ZTA 目前面临的挑战包括：

1.支持 ZTA 的产品成熟度

2.组织切换到 ZTA 的能力/意愿，因为：

a) 技术的大量投资，包括遗留资产的处理

b) 缺乏制定过渡计划、试点或概念证明的能力或资源

3.安全问题，如：

a) 零信任控制平面的折中性

b) 识别攻击的能力

4.ZTA 产品/解决方案与传统技术的互用性，例如：

a) 标准接口与专有接口

b) 能够与企业和云服务交互

5.用户体验：到目前为止，还没有关于 ZTA 可能影响最终用户体验和行为的详细研究。ZTA 的目标应该是增强安全性，并提供基本无缝的用户体验。

本指南旨在通过为示范项目选择的解决方案和合作者来解决这些问题。

1.4 背景

历史上，基于边界的网络安全模型一直是信息安全的主要模型。它假设用户在企业网络边界内的用户是“受信任的”，而外部的任何人都是“不受信任的”。几十年来，这种观点一直是确定用户/设备可以访问哪些资源的准则。

近年来的几起备受瞩目的网络攻击，包括 2015 年人事管理办公室（Office of personal Management breah）数据泄露事件，都颠覆了这种基于边界安全模型。此外，由于云计算的增长、移动办公和现代劳动力的变化等因素，网络边界变得不那么重要。正是在这种背景下，联邦首席信息官（CIO）委员会在 2018 年与 NIST NCCoE 接洽，帮助联邦机构围绕 ZTA 的定义达成共识，以及 ZTA 的好处和局限性。这个跨机构合作促成了《零信任架构》的发布（NIST SP 800—207）。

本 NCCoE 项目建立在与联邦机构和联邦 CIO 委员会合作的基础上，同时，我们试图使用商用产品构建并记录一个符合 NIST SP 800-207 中的概念和原则的 ZTA 示例。

2 场景

参与该项目的行业组织的回复造将影响所描述的场景的具体内容和数量。

2.1 场景一：员工访问企业资源

员工希望从任何工作地点可以方便安全地访问公司资源。此场景将展示一种特定的用户体验，其中员工尝试使用企业管理的设备访问企业服务，如企业内部网、考勤系统和其他人力资源系统。该资源的相关访问请求将由本项目中实现的 ZTA 解决方案动态和实时提供。员工将能够执行以下操作：

- 从企业内部网连接访问企业内部资源。
- 直接从企业内部网连接访问云中的企业资源。
- 从分支机构访问企业内部资源。
- 从分支办公室访问云中的企业资源。
- 从公共互联网访问企业内部资源。
- 从公共互联网访问云中的企业资源。

2.2 场景二：员工访问互联网资源

员工试图通过互联网完成某些任务。此方案将展示一种特定的用户体验，其中员工尝试使用企业管理的设备在 Internet 上访问基于 Web 的服务。尽管基于 Web 的服务不是由企业拥有和管理的，但该项目中实现的零信任架构 ZTA 解决方案仍将动态和实时地提供对该资源的相关访问请求。该解决方案将允许员工访问任何位置，也就是说，员工可以使用企业管理设备在企业内部网、分支机构或

公共互联网内连接时访问互联网。

如果公司政策允许员工使用企业管理的设备访问公共互联网中非企业管理的资源和服务，ZTA 解决方案将允许企业确定访问的范围。

上述段落中的访问限制示例可以包括：

- 不允许访问社交媒体网站。
- 允许访问互联网搜索引擎，当员工在分公司或远程（如咖啡厅或机场）工作时，不需要公司网络实时提供与此资源相关的访问请求。
- 员工可以直接访问公共互联网上的关键业务服务（如电子邮件、GitHub），但必须使用企业用户凭证对这些服务进行授权。

2.3 场景三：外包人员访问公司和互联网资源

外包人员试图访问企业的某些资源和 Internet。该场景展示一个特定的用户体验，即一个被企业雇佣的临时外包人员为了完成计划中的任务需要访问特定的企业职员和公共互联网。企业资源可以是本地或云中的，外包人员将能够在本地或从公共互联网访问企业资源。外包人员试图访问的资源的相关网络访问请求将由本项目中实施的零信任架构 ZTA 解决方案实时并且动态地提供。

2.4 场景四：企业内部的服务器间通信

企业服务通常由不同的服务器相互通信来实现。例如，Web 服务器与应用服务器通信。应用服务器与数据库服务器通信将数据检索传回 Web 服务器。此场景演示企业内服务器间交互的示例，其中包括本地、云或本地与云混合模式的服务器之间的服务器。本项目中实施的零信任架构 ZTA 解决方案将动态和实时

地提供相互交互的指定服务器之间的关联网络通信。

2.5 场景五：跨企业合作

两个企业可以在协作时需要一些共享的资源。在这种情况下，本项目中实现的零信任架构 ZTA 解决方案将使一个企业的用户能够安全地访问另一个企业的特定资源，反之亦然。例如，企业 A 用户将能够访问企业 B 特定的应用程序，而企业 B 用户将能够访问企业 A 特定的数据库。

2.6 场景六：基于信任等级的企业资源访问

企业通过监控系统、SIEM 系统和其他一些安全系统为策略引擎提供数据形成更加细粒度的信任等级，进而实现更严格的基于信任等级的企业资源访问。在此场景中，零信任架构 ZTA 解决方案将监控系统和 SIEM 系统等与策略引擎集成起来，生成更精确的信任等级计算。

备注：上述场景在本项目中通过不同的步骤来创建和演示

3 顶层架构

图 1 展示了一个达成目标能力的零信任架构的逻辑组件图。

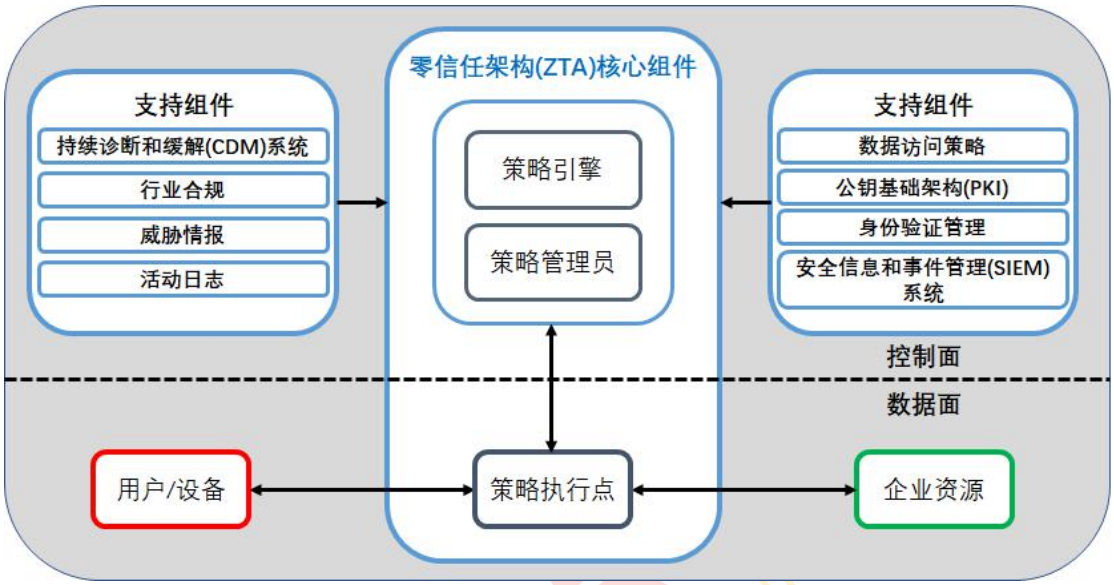

图 1：ZTA 架构概要

3.1 组件列表

下文中组件的定义来自《零信任架构》（NIST SP 800-207）白皮书。

核心组件：

- 策略引擎 PE：为特定用户/设备的资源访问提供决策，通过策略引擎完成授权决策和信任等级计算。
- 策略管理 PA：负责在用户/设备和资源之间建立和维护连接。
- 策略执行点 PEP：负责开启/监控/中止用户/设备和资源之间的连接。

支撑组件：

- CDM 系统收集关于企业资产现状的信息，并对配置设置和软件应用更新。
- 行业合规性系统包括企业制定的所有政策规则，以确保符合其可能所属的任何监管制度（例如，医疗或金融行业信息安全要求）。
- 威胁情报馈送将从内部和/或外部来源收集到的关于新发现的攻击或漏洞的信息输送到策略引擎，以帮助做出访问决策。
- 网络和访问日志系统负责记录在网络上看到的流量元数据以及对企业资源的访问请求。
- 数据访问策略是关于访问企业资源的属性、规则和策略。 这组规则可以在策略引擎中编码或动态生成。
- PKI 系统负责生成和记录企业向资源、设备和应用颁发的密钥和/或证书。
- 身份管理系统负责创建，存储，管理企业用户账号和身份记录。
- SIEM 系统收集以安全为中心的信息，供以后分析。 这些信息被用来完善策略，并对企业资源可能受到的攻击发出警告。

设备和网络基础设施组件：

- 设备包括笔记本电脑、平板电脑和其他连接到企业的移动或物联网设备。
- 网络基础设施组件包括中型或大型企业通常在其环境中部署的网络资源。

注：图 1 未描述网络基础设施。 假设 ZTA 核心和支持组件和设备通过

网络基础设施连接。

3.2 所需要求

本项目旨在开发满足以下要求的参考设计和实施方案：

- 代表基于标准的解决方案结构，是一种有效和安全实施 ZTA 的方法。
- 无需使用第三方工具（例如虚拟专用网络 VPN、受信任的互联网连接 TIC）即可直接在内部和云端访问 Internet 和企业资源。
- 展示与云和企业内部资源的集成度。
- 显示与标准目录协议和身份管理服务的集成（例如，轻量级目录访问协议 [LDAP]、活动目录、OpenLDAP、安全声明标记语言）。
- 通过标准应用程序编程接口 API，展示了与遗留的和当前 SIEM 工具的集成。
- 显示所需的企业用户设备安全要求，包括：
  - 保护静态数据安全
  - 防止因设备漏洞而导致对存储在设备上或该设备可访问的数据进行未经授权访问，以及设备的滥用。
  - 减轻因设备上恶意软件的执行，而导致存储在设备上或设备可访问的数据的未经授权访问，以及设备的滥用。
  - 减少因设备意外、故意或恶意删除或篡改设备上存储的数据而导致数据丢失的风险。

- 保持对设备内和针对设备的可疑或恶意活动的感知和反应，以阻断或检测到设备受到入侵，并尽快进行补救。

4 相关标准和准则

适用于本项目的参考资料、标准和指南如下。

- NIST 网络安全框架 v.1.1，改善关键基础设施网络安全框架
  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NIST SP 800-30 修订本 1，进行风险评估指南
  https://doi.org/10.6028/NIST.SP.800-30r1
- NIST SP 800-37 修订本 2，信息系统和组织风险管理框架：安全和隐私的系统生命周期方法
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- NIST SP 800-53 修订本 4，联邦信息系统和组织的安全和隐私控制
  https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-327 30/documents/sp800-53-rev4-ipd.pdf
- NIST SP 800-57 第 1 部分 修订版 4，密钥管理建议：第 1 部分：概要
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
- NIST SP 800-61 修订版 2，计算机安全事件处理指南
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.

800-61r2.pdf

- NIST SP 800-63 修订版 3，数字身份指南

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

- NIST SP 800-92，计算机安全日志管理指南

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

- NIST SP 800-122，个人身份信息机密性保护指南（PII）

  https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf

- NIST SP 800-160 第 2 卷，开发网际弹性系统：系统安全工程方法

  https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final

- NIST SP 800-162，基于属性的访问控制 （ABAC） 定义和注意事项指南

  https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

- NIST SP 800-175B，联邦政府使用加密标准指南：加密机制

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175b.pdf

- NIST SP 800-171 修订版 2，保护非联邦信息系统和组织中受控的非分类信息

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

- NIST SP 800-205，访问控制系统的属性注意事项

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf

- NIST SP 800-207（第二稿），零信任架构

  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

- NIST SP 1800-3，基于属性的访问控制

  https://www.nccoe.nist.gov/sites/default/files/library/sp1800/abac-nist-sp1800-3-draft-v2.pdf

- 云安全联盟、软件定义边界工作组、SDP 规范 1.0

  https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf

- ISO/IEC 27001，信息技术-安全技术-信息安全管理系统

- 美国技术产业顾问理事会，零信任网络安全当前趋势

  https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

- 联邦信息处理标准 140-3，加密模块的安全要求

  https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

5 安全控制图

本表列出了 NCCoE 将适用于此次网络安全挑战的商业产品的特征，这些特征与《改善关键基础设施网络安全框架》中描述的适用标准和最佳实践以及 NIST 的其他活动相吻合。这项工作旨在展示标准和最佳做法在现实世界中的适用性，但并不意味着具有这些特征的产品将满足行业的监管审批或认证要求。

表 1：安全控制图

网际安全框架(Cybersecurity Framework) v1.1			适用组件
功能	**分类**	**子分类**	
识别 (ID)	资产管理 (ID.AM)	ID.AM-1：组织内的物理设备和系统被清点。	SIEM 用户/设备 数据资源
		ID.AM-2：组织内的软件平台和应用程序已清点。	SIEM
		ID.AM-5：资源（例如硬件、设备、数据、时间、人员和软件）根据其分类、关键度和业务价值确定优先级。	SIEM PE
	风险评估 (ID.RA)	ID.RA-1：识别和记录资产漏洞	SIEM 威胁情报
		ID.RA-3：识别和记录内部和外部威胁	SIEM 威胁情报

网际安全框架(Cybersecurity Framework) v1.1			适用组件
功能	**分类**	**子分类**	
防护 (PR)	身份管理 验证和访问 控制 (PR.AC)	PR.AC-1：针对授权设备、用户和流程颁发、管理、验证、吊销和审核标识和凭证。	身份管理系统 PE
		PR.AC-3：远程访问被管理	PE PA PEP
		PR.AC-4：访问权限和授权得到管理，纳入了最小权限和职责分离的原则。	PE PA PEP
		PR.AC-5：网络完整性受到保护（例如，网络隔离、网络分段）	PEP
		PR.AC-6：标识被证明并绑定到凭证，并在交互中验证。	身份管理系统 PKI PE
		PR.AC-7：用户、设备和其他资产经过身份验证（例如，单因素、多因素）与交易风险（例如，个人的安全和隐私风险以及其他组织风险）相称。	身份管理系统 PKI PE PA
	数据安全 (PR.DS)	PR.DS-2：传输中的数据受到保护	PE PA

网际安全框架(Cybersecurity Framework) v1.1			适用组件
功能	**分类**	**子分类**	
			PEP
		PR.DS-5：实现数据防泄漏	PE PA PEP
		PR.DS-6：完整性检查机制用于验证软件、固件和信息完整性。	SIEM PE
		PR.DS-8：完整性检查机制用于验证硬件完整性。	SIEM PE
	信息保护流程和程序(PR.IP)	PR.IP-1：创建和维护信息技术/工业控制系统的基线配置，纳入安全原则（例如，最小功能的概念）。	SIEM
		PR.IP-3：配置更改控制进程已就位。	SIEM
	防护技术(PR.PT)	PR.PT-3：通过配置系统来仅提供基本功能，从而纳入了最小功能的原则。	PE PA PEP
		PR.PT-4：通信和控制网络受到保护。	PE PA PEP
		PR.PT-4：通信和控制网络受到保护。	SIEM 威胁情报

网际安全框架(Cybersecurity Framework) v1.1			适用组件
功能	**分类**	**子分类**	
			PE PA PEP
检测	异常和事件 (DT.AE)	DE.AE-2：分析检测到的事件以了解攻击目标和方法。	SIEM 威胁情报 PE PA
		DE.AE-3：事件数据从多个源和传感器收集并关联。	SIEM 威胁情报 PE PA
		DE.AE-5：建立事故警报阈值。	SIEM 威胁情报 PE PA
	安全持续监控 (DE.CM)	DE.CM-1：网络受到监控，以检测潜在的网络安全事件。	SIEM 威胁情报
		DE.CM-2：监视物理环境以检测潜在的网络安全事件。	SIEM

网际安全框架(Cybersecurity Framework) v1.1			适用组件
功能	**分类**	**子分类**	
		DE.CM-4：检测到恶意代码。	SIEM 威胁情报
		DE.CM-5：检测到未经授权的移动代码	SIEM 威胁情报
		DE.CM-6：监控外部服务提供商活动以检测潜在的网络安全事件。	
		DE.CM-7：对未经授权的人员、连接、设备和软件进行监视。	SIEM 威胁情报
		DE.CM-8：执行漏洞扫描。	SIEM 威胁情报
	检测流程 (DE.DP)	DE.DP-5：检测流程不断改进。	SIEM 威胁情报
响应	缓解 (RS.MI)	RS.MI-1：事故被控制。	SIEM 威胁情报 PEP
		RS.MI-2：事故得到缓解。	SIEM 威胁情报 PEP

6 附录 A 参考文献

[1] S. Rose 等人，零信托架构，国家标准与技术研究院（NIST）草案（第 2 版）特别出版物 800-207，盖瑟斯堡，马里兰州，2020 年 2 月。

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf