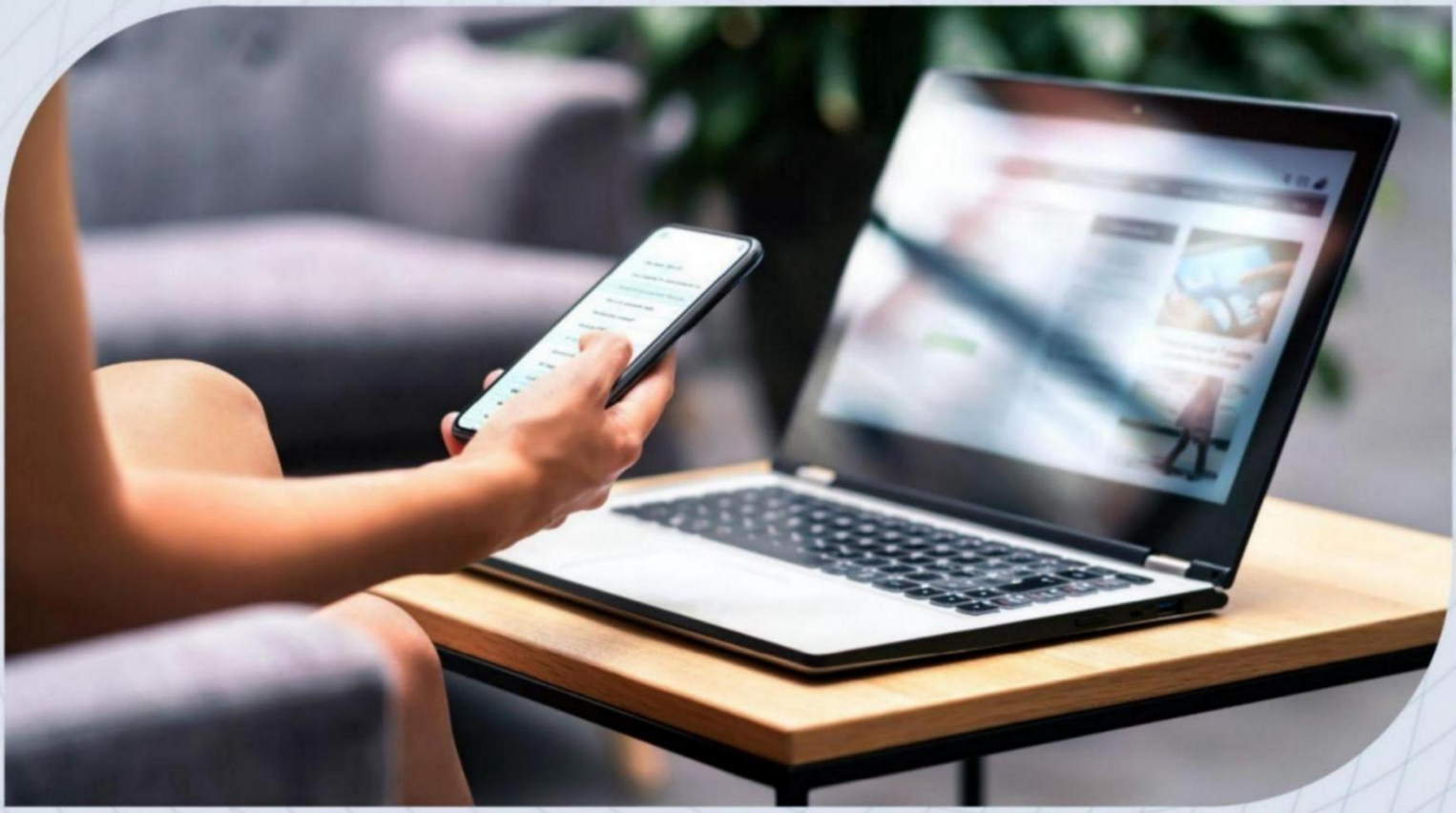
面向IAM的零信任原则与指南



Release Candidate

CSA GCR GREATER CHINA REGION cloud security alliance®

CSA cloud security alliance®

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

报告中文版支持单位

上海派拉软件股份有限公司成立于2008年，是国内最早从事身份安全研发的原厂商，致力于为企业和机构提供以“数字身份”为核心的数字化能力底座与安全基石，覆盖身份安全、应用安全、数据安全，在上海、北京、广州、武汉、成都、长春、深圳、济南、厦门、合肥、杭州、西安等地设有研发中心和服务机构，拥有600+行业专家和资深团队，服务能力遍布全国。派拉软件已成功为全球范围内的金融、制造、医疗、教育、零售、政府、地产、科研院所等多行业2000余家企业和机构提供极致体验的“全域数字身份统一安全管控”专业服务，覆盖五百强客户300余家。

派拉软件是CSA会员单位，支持该报告内容的翻译，但不影响 CSA 研究内容的开发权和编辑权。

主要贡献专家：

茆正华 徐安哲 王育恒 王磊

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

英文版本编写专家

主要作者：

Hani Raouda	Jonathan Flack	Kevin Dillaway
Paul Simmonds	Rohini Sulatycki	Shruti Kulkarni
Clement Betacorne	Irshad Javid	John Yeoh
Paul Simmonds		

审校者：

Anna Pasupathy

CSA全球员工：

Erik Johnson	Ryan Gifford	Stephen Lumpe

目录

摘要

身份及身份相关的属性，以及其他零信任（ZT）标识（零信任中关于身份的其他属性）是零信任架构的关键原则之一。零信任方法旨在通过基于风险的访问控制来减少网络攻击和数据泄露的几率。也就是说，在授予对资源（数据、系统）的访问权限之前，必须进行身份验证和授权。

为了满足这一要求，重要的是要通过零信任的视角来审视现存和新的身份、访问管理和云解决方案。

零信任是一个技术无关的指导性框架，将访问控制措施更加靠近受保护资产（保护面）。从身份、访问管理的角度来看，它提供了基于风险的决策授权能力，而不是仅基于单一访问控制方法的二元信任来进行授权访问。

目标受众

主要：零信任（ZT）实施和架构的技术经理

次要：CISO / ISO / 信息安全、IAM 供应商

零信任的背景和推动因素

多年来，有各种论文谈论信任作为人类和社会现象，其中一些使用了“零信任”这个术语。2001 年，开源安全测试方法手册（OSSTMM）开始解决信息技术中的信任问题，并在其第三版（2007 年）中将“信任”标记为漏洞，并专门撰写了一整章来讨论这个主题。

Sun Microsystems 在 1990 年代引入了“Chewy Center”①（智能糖果或 M＆M 糖果模型②）的概念。在 2005-2007 年期间，Jericho Forum(visioning paper and Jericho Forum® Commandments)和 OpenGroup 为零信任做了一些基础工作，讨论了

传统网络边界安全模型的失败以及去边界化的必要性，这是 Open Group 零信任安全准则的灵感来源。

零信任网络（ZTN）概念是在 21 世纪初由美国国防部（DoD）提出的，当时正在定义全球信息网（GIG）网络运营黑核网络路由技术和路由寻址架构，这是 DoD 的网络中心服务战略的一部分。随着时间的推移演变为 ZTN 架构（ZTNA）和软件定义的边界（SDP）框架，并被 DoD、CSA 和 NIST 所采纳和进一步推广。

在经过两年的研究，Forrester Research 的 John Kindervag 于 2010 年正式将这些概念整合成我们现在所知道的零信任实践领域 。John 的工作独特之处在于他正式确定了成功实施这些架构所需的组件，并提供了一种可理解的实施零信任的方法，包括利用 Kipling 方法开发有效的零信任策略，以及启用扩展授权控制，例如基于上下文的访问控制。

2019 年左右，美国国防部（DoD）在与国家安全局（NSA）进行情报磋商后开始拥抱零信任，美国国防部认为当时的安全方法不再有效，且需要调整其安全战略，以更好地抵御日益复杂的网络攻击。

2020 年 8 月，NIST 发布了 SP 800-207 零信任架构。2021 年 5 月，美国总统拜登签署行政命令（EO）14028，特别提到了零信任安全实践，要求联邦机构加强网络安全，为政府采用零信任提供了第一个重要的法规。虽然全球都对零信任的兴趣在最近几年不断增加，由于受到美国政府法规的影响，美国目前在零信任应用和相关指导方面处于领先地位。

无论是来自 NIST、DoD、CISA 还是像 CSA、Forrester Research 或英国 NCSC 这样的组织的专家贡献，其中相关的指导原则都基于相同的基本原则（最初在 John Kindervag 的基础研究中描述），其中许多是已经确立为信息安全概念（例如“最小特权”，“拒绝所有，例外允许”）。

关于零信任的一个关键要点是它不是预设架构或单一产品。零信任是一种策略和一系列指导原则，用于指导架构和采购决策。这使组织能够根据其特定的业务需求、资产、风险和优先事项从内部向外设计。

零信任实施方法论

美国国家安全电信咨询委员会（NSTAC）将零信任实施描述为一个 5 个步骤的过程。这五个步骤包括：

- 定义保护范围
- 映射事务处理流
- 构建零信任架构
- 制定零信任策略
- 监控和维护网络

图 1 零信任实施步骤

https://blogs.nvidia.com/blog/2022/06/07/what-is-zero-trust/

要进行零信任架构的战略规划和实施，定义组织的保护范围是重要的一环。

范围

本文的范围包括以不受技术限制的方式，透过零信任的视角来审视身份和访问管理，因此不会详细说明任何工程解决方案。

本文阐述了在“授予访问权限之前进行身份验证和授权”的过程中，使用身份属性和其他标识的必要性。

本文泛指“实体”，既包括个人也包括非个人。从身份和访问控制管理的角度来看，这两种实体都具有身份属性和标识，这些属性和标识提供了更高级别的上下文风险感知。

引言

认证是一个实体（如人、动物、物体、设备、网络、应用程序、数据库、进程、服务等）向另一个实体证明自己是其所声称的身份的过程。NIST 将认证定义为“验证用户、进程或设备的身份，通常作为允许访问信息系统资源的前置条件”。

为了使认证能够抵御诸如网络钓鱼的常见认证攻击，认证过程引入了额外的安全屏障，增加了攻击者成功突破认证的难度。例如，多因素认证（MFA）通过引入额外的安全认证方式来增强认证，使黑客难以成功破坏启用了 MFA 的认证流程。

授权通常发生在成功认证之后，它使经过认证的实体能够基于最佳实践（如基于角色的访问和最小权限原则）访问资源。NIST 将授权定义为授予系统实体访问系统资源的权利或许可。

就像多因素认证增强了认证一样，零信任通过在控制授权的属性中增加上下文风险感知来增强授权。本文的其余部分将描述零信任如何实现安全性，以及通过可扩展的授权方式实施零信任所需的步骤。

身份识别的实体和属性

身份是构建零信任安全架构的一个至关重要的因素，因为它提供了属性和标识用于验证和授予资源访问权限。

在零信任模型中，一个请求不会基于位置、网络或资产所有权来而被默认是可信的，而是使用多因素来进行明确地验证。比如发出请求的实体、行为、生物特征、加密签名验证、位置、设备健康状况、操作系统健康状况等。每个因素（理想情况下）都应具有已知的评判标准。

在评估身份属性和标识之后，根据上下文感知和风险评估作出是否允许访问的决策。这意味着可以根据请求的风险和验证的需要进行调整，验证很少是一次性事件，而是一个持续的过程。理想情况下，所有访问都应遵循最小权限原则。

通过运用零信任原则，组织可以减少攻击面，降低遭受入侵的风险，同时提升员工的生产力和灵活性。

零信任策略的一个关键原则是能够识别请求和访问的上下文，从而做出更好的基于风险的访问决策。系统不再仅依赖静态凭证或角色，而是基于动态属性评估每个请求的上下文，例如：

- 用户及其所属的群组（谁 Who）
- 位置（在哪 Where）
- 设备（什么 What）
- 时间（何时 When）
- 应用程序类型（如何 How）
- 用户和资源的行为和风险水平

基于上下文，系统可以强制执行基于风险的细粒度访问控制策略，并应用自适应授权机制，以确保只有正确的实体在正确的时间、正确的条件下访问正确的资源。这减少了攻击面，降低了身份和凭证被盗窃的风险，并且可以提升用户的整体体验。

在任何零信任架构中的挑战在于，正确管理组织中真正具有权威性的实体和属性的数据。同样重要的是，确保组织及其拥有管理权限的系统（如云系统）能够从其权威身份来源中获取具有已知可信度的受信任身份属性和标识。

身份验证与确认

当一个组织的零信任解决方案中使用具有权威性的身份属性和标识时，那么用于管理和维护这些属性和标识的流程的可靠性变得至关重要。如果没有使用经过验证的可靠流程，那么该组织可能无法获得需要使用或依赖这些身份属性和标识的第三方权威信任。

一个良好的信任水平，首先有良好的验证和确认过程。NIST SP 800-63A 定义了包含 3 个阶段的身份验证和注册的流程，通常是一个五步或六步的过程：

- 解析收集到的一些属性和标识
- 验证或确认，对收集到的身份属性和标识进行审核，以确定其是真实的、准确的、实时的和未过期的
- 验证，对收集到的身份属性和标识与将要生成的数字身份（实体）进行比较
- 数字身份生成，将数字身份创建到权威身份源（主要是身份提供者）
- 凭证生成，将数字身份与一个或多个认证器关联起来
- 数字身份注销，将数字身份从权威身份源中移除

下面是一个权威源的示例（来自 NIST SP 800-63A）：

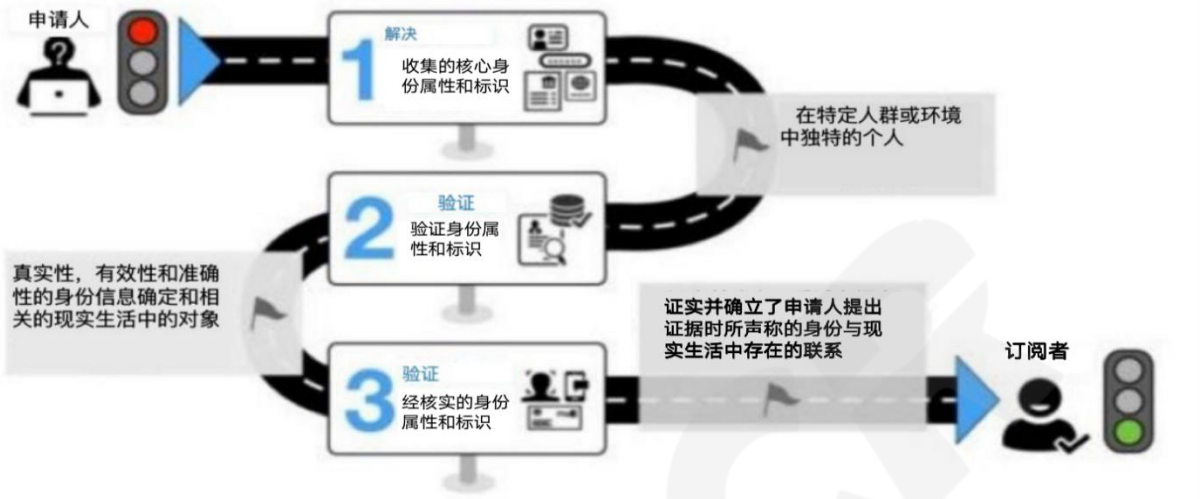


图 2 权威源实列

在这个方案实施过程中，将基于环境中数据源、资产、应用程序和服务（DAAS）组件进行风险控制。这意味着要求每个 DAAS 组件应该提供相应的验证和确认流程。

表 1 零信任身份和凭证管理

#	功能	说明	阶段步骤
1	身份认证	验证身份凭证的真实性	● 验证可以是手动的、自动的，或两者的结合 ● 定义可接受的身份证明类型（例如，驾驶执照、护照、X509 数字证书、令牌等） ● 定义验证身份真实性所需的流程、基础设施和工具

2	身份配置	将经过验证的身份信息提供给权威身份源（AD、IdP）	●除了用户名和密码（MFA、SSO、无密码等）之外，定义用于验证用户身份的身份属性。 ●定义对这些选定属性的限制策略（密码长度、MFA 技术、无密码等） ●定义一项尽职调查流程，以确保提供的身份不是内部或外部黑名单的一部分（例如，PKI 吊销列表）。
3	凭证配置	将用户纳入通用访问解决方案中	●定义解决方案将如何与规则引擎集成，以便进行授权标识的交换 ●安全地将 AD/IdP 与解决方案集成 ● *更多信息详见“参考”部分
4	身份取消配置		●由管理员或代码触发 ●由来自 AD/IdP 身份属性变更的事件触发

决策因子

根据 NIST SP 800-207 所示，最基本的决策因子如下图所示。请注意，这些决策因子不需要全部来自同一实体（例如，供应商、提供者、技术栈等）。然而，每个信息源的真实性应该是（在密码学上）可验证的，它产生的决策因子必须是可靠的、可扩展的和防篡改的，并且在风险决策过程中拥有可信任程度以供决策

使用。根据风险等级，可能需要更多的决策因子来提供更高级别的上下文认知判断，例如动态用户行为（例如击键模式）或特殊需求（如深度数据包检查）。请注意，下面的图表是一个信任算法。信任算法是策略执行点授予或拒绝访问的过程。信任算法的输出取决于从资源（如访问请求、资产数据库等）接收到的决策因子和输入，如下图所示：

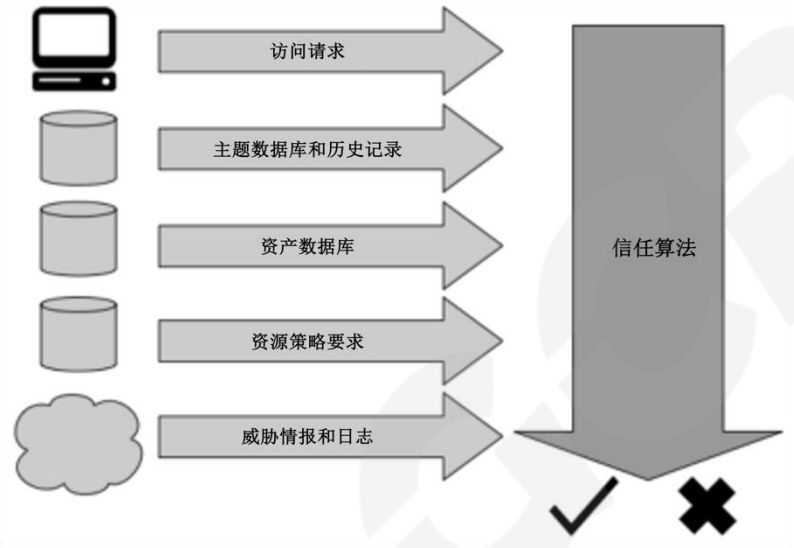


图 3 NIST SP 800-207.

https: / nvlpubs. nist. gov/ nistpubs/ SpecialPublications/ NIST. SP. 8 0 0 - 2 0 7 . pdf

主体向资源发出的访问请求应包括：

- 所请求的资源
- 请求者的信息，包括但不限于：
  - ○操作系统版本
  - ○使用的软件
  - ○补丁级别
  - ○访问持续时间（即时访问）

主体数据库和历史记录显示了“谁”正在请求对资源的访问。这是主体属性和分配权限的集合，例如：

- 用户属性（例如，帐户 ID）
- PEP（策略执行点）执行的身份验证检查结果

- 角色和权限

资产数据库包含了每个企业所管理的资产的已知状态。与发出请求的资产的实际状态进行比较，可能包括：

- 操作系统版本
- 存在的软件
- 资产完整性
- 位置（网络位置和地理位置）
- 补丁级别

根据与资产数据库的状态比较，可能会限制或拒绝对资产的访问。

资源访问策略定义了访问资源的最低要求。这组策略与用户 ID 和属性数据库相结合。资源访问策略的要求可能包括身份验证保障级别，例如：

- 网络位置（例如，拒绝来自海外 IP 地址的访问）
- TLS 1.2 及以上
- 数据敏感性
- 资产配置请求

资源访问策略的要求应由数据保管者（即负责数据的人）、数据所有者以及利用数据的业务流程的责任人（即业务负责人）共同制定。

威胁情报和日志提供来自各种来源的常规威胁和恶意软件活动的相关信息来源。这可能包括在设备上看到的可疑指标，如可能的恶意软件对执行和控制节点的查询，以及与执行和控制节点的通信。

- 威胁情报源可以是外部服务或内部扫描
- 发现可能包括攻击签名和缓解措施

这个组件很可能由第三方服务而非企业的控制。

决策规则：五个 W，有时称为五个 W 和一个 How，即 5W1H，或六个 W 或者 Kipling 方法，可以用于通过规则引擎在授权过程中获得至少 6 个维度的上下文信息。

NIST SP 800-207 描述了，用于提供基于上下文的授权方案中的核心零信任组件包括（规则引擎 → 策略引擎，策略管理，策略执行点，信任算法）。

每个受保护面（例如，要使用零信任保护的单个 DAAS 组件）将分别具有上行和下行的流量。该流量可能前往公共网络、员工，或者前往另一个受保护面，比如数据库、服务器或 API。

每个进出受保护面的出站和入站数据包必须根据规则引擎进行验证，根据这些决策因子（谁、什么、何时、何地、为什么、如何）正确组合的策略。规则引擎可以接收与用户行为、设备状况、深度数据包检查结果、DLP 结果等相关的决策因子。

零信任授权流程中的规则引擎将利用其算法，在 OSI 模型的所有层次上实现上下文感知的访问控制。

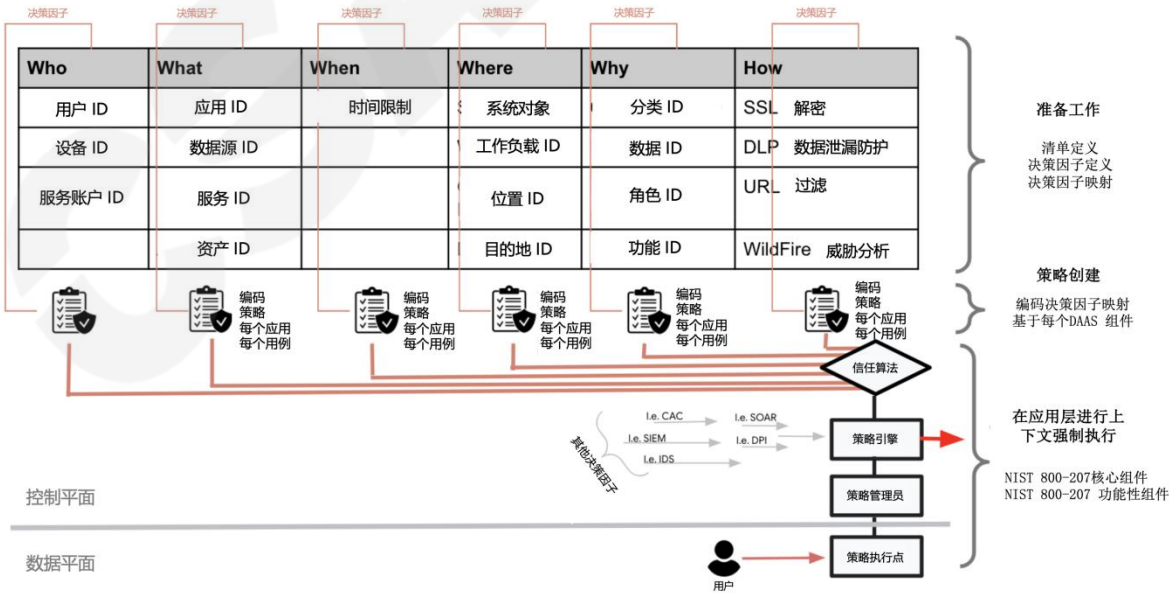


图 4 零信任上下文感知访问控制 .

记录每个受保护面、每个用例中的这些决策因子及其相应的策略代码的目标是为了让安全工程师能够便捷地为特定的受保护面，设计、实施、测试和版本管理零信任的上下文感知的访问控制。

上述图片旨在清晰的展示如何将决策因子定义便捷地转化为策略代码。这些策略代码随后可以容易地被现有的规则引擎所使用。

基于策略的授权

在零信任（ZT）中，我们寻求基于风险的访问控制，这包含了传统的基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）的概念，但远不止于这些概念，这些概念通常依赖于组织管理的单一可信权威身份源。

无论如何，在设计零信任架构时，从零信任的角度审视现有的和新的身份和访问管理解决方案至关重要。

策略提供了授权的第一个接触点。策略基于请求者和资源之间的交互流程。在零信任解决方案上实施时，应该创建精细的策略。例如，实体 A 被允许在标准时间的上午 9:00 到下午 5:00 之间，从一个已定义的设备访问资源 B。

策略在零信任环境中定义了明确的授权方式，并通过与 DAAS 业务系统相关的决策因子进行访问控制和策略决策，这些策略接收多个来源中的决策因子，其中一个来源可能是身份提供商（IdP）。

处理失败的策略决策

当不满足授予访问的条件时，可以采取以下典型解决方案（这只是列出的部分参考方案）：

- 实体可能会被阻止

● 实体被通知访问已被拒绝

● 实体可以被放置在队列中

● 实体可以被暂停一段时间

● 可以要求进行升级身份验证

● 可以向策略管理员发送通知，以核实是否需要策略优化

● 可以将相关数据发送到安全信息与事件管理（SIEM）系统进行进一步分析，然后用于优化策略或预警可能的攻击

● 实体可以被送入蜜罐（honeypot）中

通过实施这些额外的工作流程，组织可以有效地处理失败的策略决策，保持符合零信任原则的安全环境，并根据实际情况和不断演变的威胁内容调整对应的安全措施。

业务价值

注：本节不涵盖零信任的通用业务价值。有关更多详细信息，请参阅《传达零信任的商业价值》。与零信任相关的身份业务价值如下所示：

在零信任环境中，基于身份来控制对数据或系统（资源授权）的访问可以提供以下几个业务优势：

● 提高安全性：通过基于身份控制对资源的访问，组织可以减少未经授权访问敏感数据和资源的风险，避免最小化横向移动，从而减少系统被攻击和数据泄露的潜在风险。

● 提高合规性：相关法规和标准，如 HIPAA 和 GDPR，要求组织实施强大的访问控制以保护敏感资源。通过使用一系列精细的授权规则，组织可以明确地证明满足这些合规要求。

● 减少摩擦：通过实施基于身份的授权控制，实体可以获得更平滑和安全的访问体验，无需反复输入凭据或浏览多个控制层（网关）。

● 提高敏捷性：通过将业务访问需求和身份访问控制进行对应匹配，组织可以更快速、更轻松地适应业务环境的变化，比如新员工加入组织或部署新应用程序。如果实施准确，可允许来自组织外部的实体（简单直接地）访问允许的系统和数据，无需创建“虚拟”用户或实施特殊的网关或其他访问控制层。

● 提高生产力：通过将业务访问需求和身份访问控制进行对应匹配，用户应自动获得所需的访问权限，以便能够高效工作（仅限于此）。而无需获得 IT 部门的访问资源许可。

● 降低成本：通过减少未经授权的访问尝试次数，组织可以减少安全事件、数据泄露和勒索软件攻击事件的潜在和实际的相关成本。

总结

在过去，访问计算机系统的前提是基于隐式的信任；用户只要提供正确的密码就认为身份可信，因为他们在默认可信的网络环境中（通常是组织的内部网络）使用计算机而受到信任。现阶段大部分的组织都是按照这种原则来判断环境是否可信，因为在最开始的网络环境中，内网默认就是可信的，外网默认是不可信的，因此外网的访问权限往往是最小的。

但是随着近二十年的发展，越来越多的组织开始使用云计算和云服务，传统的边界被完全打破，业务系统部署于不受组织控制也不属于其控制范围的位置，并且这种趋势还在蔓延。

因此，传统的有强大防御能力的边界安全模型已经变得难以配置、实施、生效和维护。

零信任模型秉持“永不信任、持续验证”的理念，对访问的数据和业务系统进行安全风险评估验证。并且这种验证不仅仅针对访问者本身，也包括基于身份的设备标识、组织标识、代码标识和代理标识。

在零信任架构中，认证方式从主体可信转变为自适应身份验证和授权模型。业务系统和数据的访问权限基于访问主体提供的一系列身份属性进行授权。这些身份属性和访问请求相关的情报（标识）进行组合校验，当访问主体的信任评估结果达到（或超过）预设置的访问请求阈值时，才允许该访问主体对系统和数据的访问请求。

此外，零信任架构下的访问请求是基于访问应用、访问途经、访问设备及访问请求的频率而持续动态评估的。因此无需考虑组织的 IT 资源和环境位于什么位置，通过零信任架构的持续动态评估即可增强访问的安全性。

当访问者完成了一次访问请求，将针对已完成的访问请求进行建模，同时将一次可信的访问请求日志进行记录，便于为后续出现潜在风险请求时的积极应对。同时也可将访问请求进行分段分析。

在本文中，我们结合零信任对身份和访问管理进行了细致说明，并希望这对您在未来组织建设零信任的过程中提供一定帮助。

参考文献

决策因子-为组织管理员提供访问上下文决策因子所需的输入，以满足细粒度的基于属性的访问控制，并验证对 DAAS 系统所有授权的访问控制；回答“什么”、“在哪里”和“什么时候”、“如何”和“为什么”以及“谁”的问题。

许多基础信息及资源会变成有效的上下文访问信息，身份提供商（IdP）可以提供明确的身份确认信息，同时根据组织已有的用户身份管理策略（多因素、统一认证等），回答“访问主体”的问题。同时通过访问请求可以明确知道访问的是什么资源，以及资源所处的环境。

通过上述信息，我们可以很容易地构建一个安全可控的用户身份和访问管理机制。

美国国家安全电信咨询委员会（NSTAC）-节选自 NSTAC 报告：3.3.3 章节

安全防护的定义：NSTAC 将安全防护的表层含义定义为零信任架构防护区域。每次访问请求只针对单个业务数据、应用程序、资产及服务（数据即服务），同样的，零信任架构防护有多个安全防护的场景。

参考链接：

https: / media. defense. gov/ 2023/ Mar/ 14/ 2003178390/ -1/ -1/ 0/ CSI_ ZERO%20 TRUST%20 USER%20 PILLAR. PDF

https:/docs.google.com/document/d/1yMH8vcT0ROwtXG4n8uYPibNLspjAul3Opiut0xnyuKg/edit?usp= sharing

以下是一个发放身份凭证并提供凭证与身份认证集成的解决方案的示例：

- 发放任意数量的公钥对，给配对的身份提供数字签名
- 将每个身份的公钥作为属性之一发送到AD/IdP的源
- 发放身份对称密钥，供身份用于加密
- 在授信平台存储模块中存储私钥和对称密钥
- 发放X.509证书或私钥证书
- 通过组织机构的CA签署证书
- 将身份及其相应的公钥存储在不可变分类账本上（可以是私人分类账，也可以是托管分类账）
- 创建机制，以使其他认证能够安全地获取给定身份的公钥和证书

基础参考文献

NSTAC报告

NIST SP 800-63：是美国国家标准技术研究院（NIST）发布的一系列数字身份验证准则的修订版，该文档强调了专门针对数字身份进行风险评估的重要性，考虑了身份注册、身份验证、认证和权限等方面。

NIST SP 800-63:以用户身份为核心实现零信任成熟度（NSA刚刚发布了《零信任贯穿用户业务访问生命周期：CSI_ZERO TRUST USER PILLAR.PDF》（美国国防部））

以用户身份为核心推进零信任战略：该报告将用户身份分为5个模块（身份管理、凭证管理、访问管理、联邦和治理），并为3个模块（身份管理、凭证管理和访问管理）定义了从初级到高级零信任战略的成熟度级别

Kipling方法：[介绍：https://en.wikipedia.org/wiki/Five_Ws]

https://www.paloaltonetworks.com/blog/2019/05/network-layers-not-created-equal/

https://federalnewsnetwork.com/wp-content/uploads/2020/01/simplify-zero-trust-implementation-with-a-five-step-methodology.pdf

https://cloudsecurityalliance.org/cloud-security-glossary/

①Sun Microsystems曾在1990年代提出了“Chewy Center”这个概念。该概念是指将计算机系统的核心功能从中央处理器(CPU)中分离出来，形成一个类似于软件的“软核心”，从而使系统更加灵活和可扩展。这种方法可以提高系统的可靠性和性能，并使其更容易适应不同的应用场景。

②“the smartie or M&M model”是一种经济学模型，用于解释市场中的产品差异化现象。该模型基于一个假设，即消费者对不同产品的偏好不同，因此愿意为某些产品支付更高的价格。在这个模型中，市场上的产品可以被分为两种类型：一种是“智能糖果”(Smarties)，另一种是“M&M糖果”(M&Ms)。Smarties是指高端产品，价格较高，而M&Ms则是指低端产品，价格较低。在这个模型中，生产商可以选择生产Smarties或者M&Ms，取决于他们对市场需求的预测和成本效益分析。同时，消费者也可以根据自己的偏好选择购买Smarties或者M&Ms。

这个模型可以用来解释为什么市场上存在大量不同的产品，以及为什么一些产品价格比其他产品高。它也可以用来分析市场竞争和定价策略等问题。

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