

Zero Trust Maturity Model

零信任成熟度模型

April 2023

Version 2.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

April 2023

Version 2.0

网络安全和基础设施安全局网络安全处

免责声明：本文件标记为 TLP:CLEAR。披露不受限制。当信息带有极小或无可预见的滥用风险时，来源可根据适用的公开发布规则和程序使用 TLP:CLEAR。在遵守标准版权规则的前提下，TLP:CLEAR 信息可不受限制地分发。有关交通灯协议的更多信息，请参见 http://www.cisa.gov/tlp/.

本译本由机器翻译生成，供快速理解条文与内部培训使用；
涉及合规判断或法律适用时，请咨询专业顾问，并以官方英文文本为准。
翻译您自己的文件，请选择桐鸾译馆 · https://www.ivyivy.com.cn

扫码关注服务号

Revision History

The version number will be updated as the document is modified. This document will be updated as needed to reflect modern security practices and technologies. Table 1 presents the document revision history.

Table 1: Revision History

Version	Date	Revision Description	Sections/Pages Affected
1.0	August 2021	Initial Release	All
2.0	March 2022	Response to RFC Feedback	All

修订历史

版本号将随文件修改而更新。本文件将根据需要更新，以反映现代安全实践和技术。表 1 列出了文件修订历史。

表 *1*：修订历史

版本	日期	修订说明受影响章节/页面
1.0	2021年8月首次发布	全部
2.0	2022年3月对RFC反馈的回应	全部

Zero Trust Maturity Model

Table of Contents

1. Introduction 4
2. Current Environment 4
3. What Is Zero Trust? 5
4. Challenges in Zero Trust Adoption 6
5. Zero Trust Maturity Model 6
5.1 Identity 13
5.2 Devices 16
5.3 Networks 20
5.4 Applications and Workloads 23
5.5 Data 26
5.6 Cross-Cutting Capabilities 29
6. References 31
7. CISA Resources 31

List of Figures

Figure 1: Zero Trust Maturity Model Pillars 7
Figure 2: Zero Trust Maturity Journey 8
Figure 3: Zero Trust Maturity Evolution 9
Figure 4: High-Level Zero Trust Maturity Model Overview 10

List of Tables

Table 1: Revision History ii
Table 2: Identity Pillar 13
Table 3: Devices Pillar 17
Table 4: Networks Pillar 20
Table 5: Applications and Workloads 23
Table 6: Data 26
Table 7: Cross-Cutting Capabilities 29

零信任成熟度模型

目录

1. 引言 4
2. 当前环境 4
3. 什么是零信任? 5
4. 零信任采用中的挑战 6
5. 零信任成熟度模型 6
5.1 身份 13
5.2 设备 16
5.3 网络 20
5.4 应用与工作负载 23
5.5 数据 26
5.6 横向能力 29
6. 参考文献 31
7. CISA 资源 31

图目录

图1：零信任成熟度模型支柱 7
图2：零信任成熟度之旅 8
图3：零信任成熟度演进 9
图4：零信任成熟度模型高层概览 10

表格列表

表1：修订历史 ..... ii 表 2：身份支柱 13
表3：设备支柱 17
表4：网络支柱 20
表 5：应用与工作负载 23
表 6：数据 26
表 7：横向能力 29

1. Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) leads the nation's effort to understand, manage, and reduce cybersecurity risk, including by supporting Federal Civilian Executive Branch agencies in evolving and operationalizing cybersecurity programs and capabilities. CISA's Zero Trust Maturity Model (ZTMM) provides an approach to achieve continued modernization efforts related to zero trust within a rapidly evolving environment and technology landscape. This ZTMM is one of many paths that an organization can take in designing and implementing their transition plan to zero trust architectures in accordance with Executive Order (EO) 14028 "Improving the Nation's Cybersecurity" § (3)(b)(ii),[1] which requires that agencies develop a plan to implement a Zero Trust Architecture (ZTA). While the ZTMM is specifically tailored for federal agencies as required by EO 14028, all organizations should review and consider adoption of the approaches outlined in this document.

2. Current Environment

Recent cyber incidents[2,3] have highlighted the broad challenges of ensuring effective cybersecurity across the federal government, as with many large enterprises, and demonstrate that "business as usual" approaches are no longer sufficient to defend the nation from cyber threats. In leading the national effort to understand, manage, and reduce cyber risks, CISA must meet new challenges to safeguard the federal civilian executive branch using a clear, actionable, and risk-informed approach. Adequate cyber defense against emerging threats requires increased speed and agility to outpace adversaries by substantially increasing costs to threat actors and improving durability and resiliency to quickly recover to full operational capability.

CISA's cybersecurity mission is to defend and secure cyberspace by leading national efforts to drive and enable effective national cyber defense, enhance resilience of national critical functions, and advance a robust technology ecosystem. CISA plays a critical role in maintaining cyber situational awareness across FCEB agencies; securing the .gov domain; and aiding federal civilian agencies, critical infrastructure owners and operators, as well as industry partners in managing major cyber incidents. While CISA maintains capabilities to defend against and mitigate known or suspected cyber threats, an evolving threat landscape and the adoption of new and emerging technologies pose challenges.

EO 14028 marked a renewed commitment to and prioritization of federal cybersecurity modernization. Among other policy mandates, EO 14028 embraced zero trust as the desired security model for the federal government and called for FCEB agencies to develop plans to implement ZTAs. A typical plan will assess an agency's current cybersecurity state and plan for a fully implemented ZTA. As the lead agency on federal cybersecurity and risk reduction, CISA's ZTMM assists agencies in development of their zero trust strategies and continued evolution of their implementation plans and presents ways in which various CISA services can support zero trust solutions across agencies.

[1] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 17, 2021). https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[2] DHS CISA. *Emergency Directive 21-01- Mitigate SolarWinds Orion Code Compromise*. https://www.cisa.gov/emergency-directive-21-01.

[3] DHS CISA. *Emergency Directive 21-02 - Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*. https://www.cisa.gov/emergency-directive-21-02.

1. 引言

网络安全和基础设施安全局(CISA)引领全国理解、管理和降低网络安全风险的工作，包括支持联邦文职行政部门机构发展和运营网络安全项目与能力。CISA的零信任成熟度模型(ZTMM)提供了一种方法，以便在快速演变的环境和技术格局中实现与零信任相关的持续现代化工作。该ZTMM是组织根据第14028号行政命令(EO)"改善国家网络安全"(3)(b)(ii)、[1]设计和实施其向零信任架构过渡计划时可采用的众多路径之一，该行政命令要求各机构制定实施零信任架构(ZTA)的计划。虽然ZTMM按EO 14028的要求专门为联邦机构量身定制，但所有组织都应审查并考虑采用本文件中概述的方法。

2. 当前环境

近期的网络事件[2,3]凸显了在联邦政府(如同许多大型企业一样)确保有效网络安全所面临的广泛挑战，并表明"一切照旧"的方法已不足以保护国家免受网络威胁。在引领全国理解、管理和降低网络风险的努力中，CISA必须通过清晰、可操作且基于风险的方法应对新挑战，以保护联邦文职行政部门。针对新兴威胁的充分网络防御需要提高速度和敏捷性，通过大幅增加威胁行为者的成本来超越对手，并提高持久性和韧性以快速恢复至全面运行能力。

CISA的网络安全使命是通过引领全国努力来推动和赋能有效的国家网络防御、增强国家关键功能的韧性并推进强大的技术生态系统，从而保卫和保护网络空间。CISA在维持FCEB机构网络态势感知、保护.gov域名以及协助联邦文职机构、关键基础设施所有者和运营者以及行业合作伙伴管理重大网络事件方面发挥着关键作用。虽然CISA具备防御和缓解已知或可疑网络威胁的能力，但不断演变的威胁格局以及新兴技术的采用带来了挑战。

EO 14028标志着对联邦网络安全现代化的 renewed 承诺和优先重视。除其他政策要求外，EO 14028将零信任作为联邦政府期望的安全模型，并呼吁FCEB机构制定实施ZTA的计划。典型计划将评估机构当前的网络安全状态并规划全面实施的ZTA。作为联邦网络安全和风险降低的牵头机构，CISA的ZTMM协助各机构制定其零信任战略并持续演进其实施计划，并展示各种CISA服务可如何支持各机构的零信任解决方案。

[1]第 14028 号行政命令，86 Fed.Reg.26633(2021 年 5 月 17 日)。https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf。

[2] DHS CISA。紧急指令 *21-01--*缓解 *SolarWinds Orion* 代码泄露事件。https://www.cisa.gov/emergency-directive-21-01.

[3] 急指令 *21-02--*缓解 *Microsoft Exchange* 本地部署产品漏洞。https://www.cisa.gov/emergency-directive-21-02.

OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,"[4] detailed specific actions for federal agencies to adopt in alignment with the pillars outlined in the ZTMM. This memorandum sets forth a Federal ZTA strategy, requiring agencies to meet cybersecurity objectives by the end of Fiscal Year (FY) 2024 to reinforce FCEB defense. CISA revised the ZTMM to further align with M-22-09's direction for agencies. FCEB agencies should review this memo in parallel with developing and implementing their zero trust strategies.

3. What Is Zero Trust?

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 provides the following zero trust and ZTA operative definition:

> **Zero trust** provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. **ZTA** is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.[5]

SP 800-207 emphasizes that the goal of ZT is to "prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible." Similarly, the National Security Telecommunications Advisory Committee (NSTAC) describes Zero Trust as "a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified."[6] Zero trust presents a shift from a location-centric model to an identity, context, and data-centric approach with fine-grained security controls between users, systems, applications, data, and assets that change over time; for these reasons, adopting a ZTA is a non-trivial effort. This shift provides the visibility needed to support the development, implementation, enforcement, and evolution of security policies. Fundamentally, zero trust may require a change in an organization's cybersecurity philosophy and culture.

> The path to zero trust is an incremental process that may take years to implement.

Initially, the implementation of required capabilities and services will often lead to additional costs; however, in the long-term, zero trust will enable a more prudent allocation of security investments toward

[4] OMB Memo M-22-09. *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*. January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[5] NIST SP 800-207: Zero Trust Architecture. 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[6] The President's National Security Telecommunications Advisory Committee. Report to the President on Zero Trust and Identity Management. February 2022. https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf.

OMB 备忘录 M-22-09,"推动美国政府迈向零信任网络安全

原则，"[4]详细说明了联邦机构应与 ZTMM 中概述的支柱保持一致而采取的具体行动。该备忘录提出了联邦 ZTA 战略，要求各机构在 2024 财年(FY)结束前实现网络安全目标，以加强 FCEB 防御。CISA 修订了 ZTMM，以进一步与 M-22-09 对各机构的指导方向保持一致。FCEB 机构应在制定和实施其零信任战略的同时审阅本备忘录。

3. 什么是零信任?

美国国家标准与技术研究院(NIST)特别出版物(SP)800-207 提供了以下零信任和 ZTA 的实用定义：

> 零信任提供了一组概念和理念，旨在面对被视为已遭入侵的网络时，最大限度地减少在信息系统和服务中执行准确、最小权限的逐请求访问决策时的不确定性。
>
> **ZTA**是企业的网络安全计划，采用零信任概念，涵盖组件关系、工作流规划和访问策略。因此，零信任企业是作为 ZTA 计划产物而为企业部署的网络基础设施(物理和虚拟)及运营策略。[5]

SP 800-207强调，ZT的目标是"防止未经授权访问数据和服务，同时使访问控制执行尽可能细粒度化。"同样，国家安全电信咨询委员会(NSTAC)将零信任描述为"一种网络安全战略，其前提是任何用户或资产都不应被隐式信任。它假设 breach 已经发生或将发生，因此不应通过在企业边界进行的一次验证就授予用户访问敏感信息的权限。相反，每个用户、设备、应用和事务都必须持续验证。"[6]零信任呈现了从以位置为中心的模型向以身份、上下文和数据为中心的方法的转变，在用户、系统、应用、数据和资产之间实施随时间变化的细粒度安全控制；基于这些原因，采用ZTA是一项艰巨的工作。这种转变为支持安全策略的开发、实施、执行和演进提供了所需的可见性。从根本上说，零信任可能需要改变组织的网络安全理念和文化。

> 通往零信任的路径是一个渐进过程，可能需要数年才能实施。

最初，实施所需能力和服务往往会带来额外成本；然而，从长远来看，零信任将使安全投资能够更审慎地分配到

[4] 零信任网络安全原则。2022 年 1 月 26 日。https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[5] 。https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[6]总统国家安全电信咨询委员会。《关于零信任与身份管理的致总统报告》。2022年2月。https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Zero%20信任与可信身份管理.pdf.

the most critical data and services, rather than “one size fits all” security investments across the entire enterprise.

4. Challenges in Zero Trust Adoption

The Federal Government, as with most large enterprises, faces several challenges in implementing ZTA. Legacy systems often rely on “implicit trust,” in which access and authorization are infrequently assessed based on fixed attributes; this conflicts with the core principle of adaptive evaluation of trust within a ZTA. Existing infrastructures built on implicit trust will require investment to change systems to better align with zero trust principles. Furthermore, as the technology landscape continues to evolve, new solutions and continued discussions on how to best achieve zero trust objectives are paramount.

Zero trust adoption requires engagement and cooperation from senior leadership, IT staff, data and system owners, and users across the Federal Government to effectively achieve design objectives and improve cybersecurity posture. Modernization of the Federal Government’s cybersecurity will require agencies to transition stove-piped and siloed IT services and staff to coordinated and collaborative components of a zero trust strategy, with agency-wide buy in for a common architecture and governance policies. This includes current and future plans to adopt cloud technologies.[7]

Federal agencies are beginning their journeys to zero trust from different starting points. Some agencies may be further along or better positioned to make these advancements than others; however, regardless of starting point, successful zero trust adoption can produce numerous benefits such as improved productivity, enhanced end-user experiences, reduced IT costs, flexible access, and bolstered security.

5. Zero Trust Maturity Model

The ZTMM represents a gradient of implementation across five distinct pillars, in which minor advancements can be made over time toward optimization. The pillars, depicted in Figure 1, include **Identity**, **Devices**, **Networks**, **Applications and Workloads**, and **Data**. Each pillar includes general details regarding the following cross-cutting capabilities: *Visibility and Analytics*, *Automation and Orchestration*, and *Governance*.

[7] Agencies should review CISA’s, United States Digital Services’, and FedRAMP’s jointly authored Cloud Security Technical Reference Architecture for additional guidance on recommend approaches to cloud migration and data protection. Cloud Security Technical Reference Architecture v.2 (cisa.gov).

最关键的数据和服务，而不是在整个企业范围内进行“一刀切”的安全投资。

4. 零信任采用中的挑战

联邦政府与大多数大型企业一样，在实施 ZTA 时面临若干挑战。遗留系统往往依赖“隐式信任”，即访问和授权很少基于固定属性进行评估；这与 ZTA 内自适应评估信任的核心原则相冲突。建立在隐式信任之上的现有基础设施将需要投资来改变系统，以更好地符合零信任原则。此外，随着技术格局的不断演变，新的解决方案以及关于如何最好地实现零信任目标的持续讨论至关重要。

零信任的采用需要联邦政府上下高级领导层、IT 人员、数据和系统所有者以及用户的参与和合作，以有效实现设计目标并改善网络安全态势。联邦政府网络安全的现代化将要求各机构将各自为政、孤岛式的 IT 服务和人员转变为零信任战略中协调协作的组成部分，并在机构范围内对共同架构和治理政策达成共识。这包括当前和未来采用云技术的计划。[7]

联邦机构从不同的起点开始其零信任之旅。一些机构可能比其他机构进展更远或更有条件实现这些进步；然而，无论起点如何，成功采用零信任都能带来诸多益处，例如提高生产力、增强最终用户体验、降低 IT 成本、灵活访问和加强安全性。

5. 零信任成熟度模型

ZTMM 代表了跨越五个不同支柱的实施梯度，其中可以随着时间的推移取得小幅进展以走向优化。如图 1 所示，这些支柱包括**身份**、**设备**、**网络**、**应用与工作负载**和**数据**。每个支柱都包含有关以下横向能力的一般细节：可见性与分析、自动化与编排和治理。

[7]各机构应审阅 CISA、美国数字服务局和 FedRAMP 联合编写的《云安全技术参考架构》，以获取有关云迁移和数据保护推荐方法的更多指导。云安全技术参考架构 v.2(cisa.gov)。

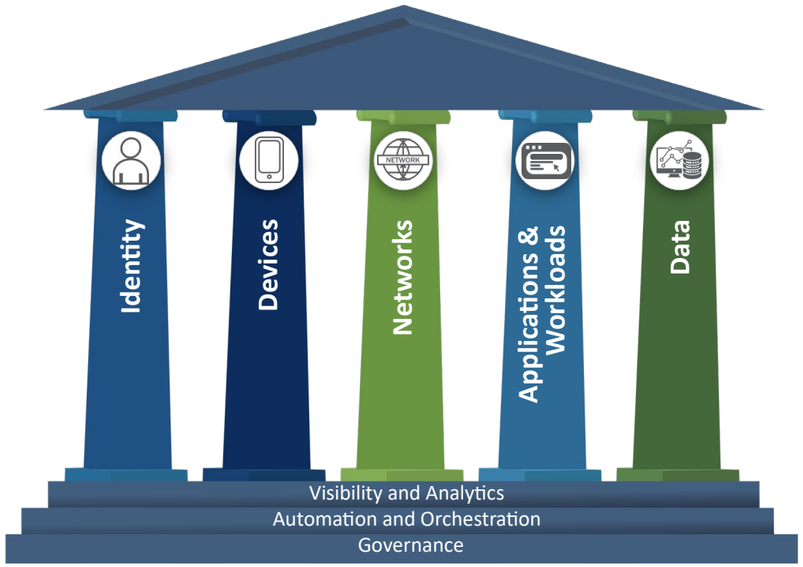


Figure 1: Zero Trust Maturity Model Pillars[8]

CISA's ZTMM is one of many paths to support the transition to zero trust.

Various ZTA publications informed the development of this maturity model (see Section 6 for additional details). This model reflects the seven tenets of zero trust as outlined in NIST SP 800-207:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

As agencies transition towards optimal zero trust implementations, associated solutions increasingly rely upon automated processes and systems that more fully integrate across pillars and more dynamically enforce policy decisions. Each pillar can progress at its own pace and may progress more quickly than others until cross-pillar coordination is required. However, this coordination can only be achieved with capabilities and dependencies compatible with one another and the enterprise-wide environment. This

[8] This illustration was inspired by Figure 1 of the American Council for Technology (ACT) and Industry Advisory Council (IAC) "Zero Trust Cybersecurity Current Trends," (2019). https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf.

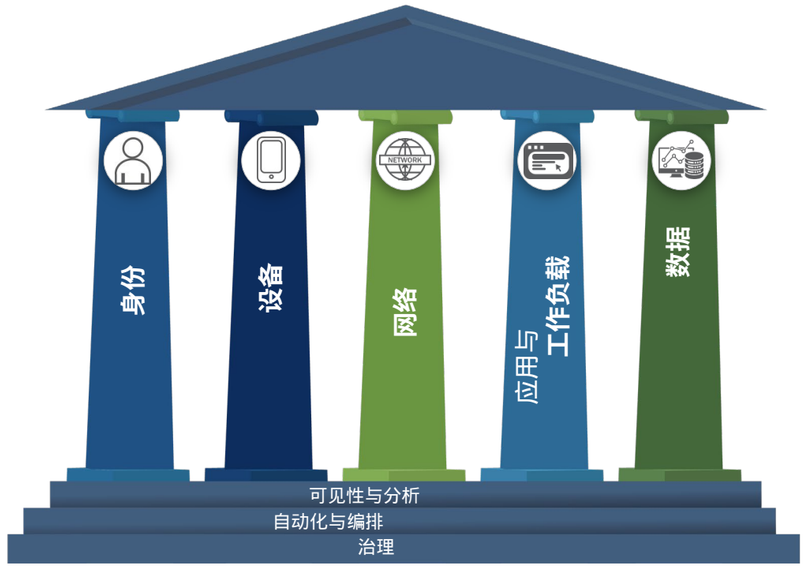


图1:零信任成熟度模型支柱[8]

CISA 的 ZTMM 是支持向零信任过渡的众多路径之一。

各种 ZTA 出版物为本成熟度模型的制定提供了参考(详见第 6 节)。本模型体现了 NIST SP 800-207 中概述的零信任七项原则：

1. 所有数据源和计算服务均视为资源。
2. 所有通信无论网络位置如何均受到保护。
3. 对单个企业资源的访问是按会话授予的。
4. 对资源的访问由动态策略决定。
5. 企业对所有自有及相关资产的完整性和安全态势进行监测和度量。
6. 所有资源的身份验证和授权都是动态的，并在允许访问前严格执行。
7. 企业尽可能收集有关资产、网络基础设施和通信当前状态的信息，并利用这些信息改进其安全态势。

随着各机构向最优零信任实施过渡，相关解决方案日益依赖自动化流程和系统，这些流程和系统更全面地跨支柱集成，并更动态地执行策略决策。每个支柱可以按自己的节奏推进，并且在需要跨支柱协调之前可能比其他支柱进展得更快。然而，这种协调只有在能力和依赖关系彼此兼容并与企业范围环境兼容的情况下才能实现。这

[8]本图受美国技术委员会(ACT)与行业咨询委员会(IAC)《零信任网络安全当前趋势》(2019年)图1启发。https://www.actiac.org/system/files/ACT-

allows for and defines a gradual evolution to zero trust, distributing costs over time rather than entirely upfront.

In alignment with NIST's steps for transitioning to zero trust, agencies should assess their current enterprise systems, resources, infrastructure, personnel, and processes before investing in zero trust capabilities (including for the pillars and functions outlined in this model).[9] This assessment can assist agencies in identifying existing capabilities to support further zero trust maturity and gaps for prioritization. Agencies can also plan for opportunities to coordinate capabilities across the pillars to enable granular, least privilege access controls and mitigate additional risks. [10]

The three stages of the ZTM journey that advance from a Traditional starting point to Initial, Advanced, and Optimal will facilitate federal ZTA implementation. Each subsequent stage requires *greater* levels of protection, detail, and complexity for adoption.

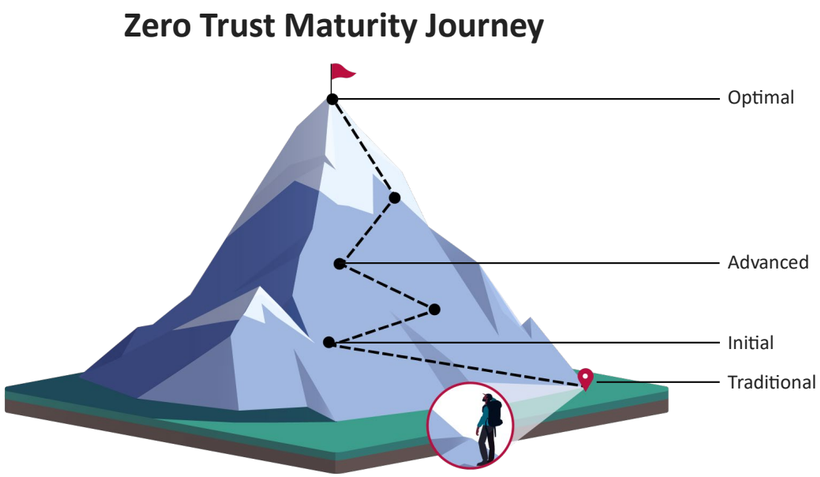


Figure 2: Zero Trust Maturity Journey

As seen in Figure 2, agencies should expect that required levels of effort and realized benefits will significantly increase as zero trust maturity progresses across and within pillars. As agencies chart their ZTA journey, they should explore opportunities to advance pillar maturity to align to specific mission needs and support further growth across other pillars. Figure 3 highlights the intended agency evolution over time from a traditional enterprise to a future state that features more dynamic updates, automated processes, integrated capabilities, and other characteristics of the Optimal stages (as described in the maturity model). These stages are dynamic and grow exponentially; planned progress from one maturity stage to another may shift in scope and impact over time.

[9] NIST White Paper. Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators. https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final.

[10] See AC-6 in NIST SP 800-53 Revision 5. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

允许并定义向零信任的渐进式演进，将成本分摊到各个时间段，而非全部前期投入。

为与 NIST 向零信任过渡的步骤保持一致，各机构应在投资零信任能力(包括本模型中概述的支柱和功能)之前评估其当前的企业系统、资源、基础设施、人员和流程。[9]该评估可以帮助各机构识别支持进一步零信任成熟度的现有能力以及需要优先处理的差距。各机构还可以规划跨支柱协调能力的机会，以实现细粒度、最小权限的访问控制并缓解额外风险。[10]

ZTM 旅程的三个阶段从传统起点推进至初始、进阶和最优，将促进联邦 ZTA 的实施。每个后续阶段在采用时都需要更高级别的保护、细节和复杂性。

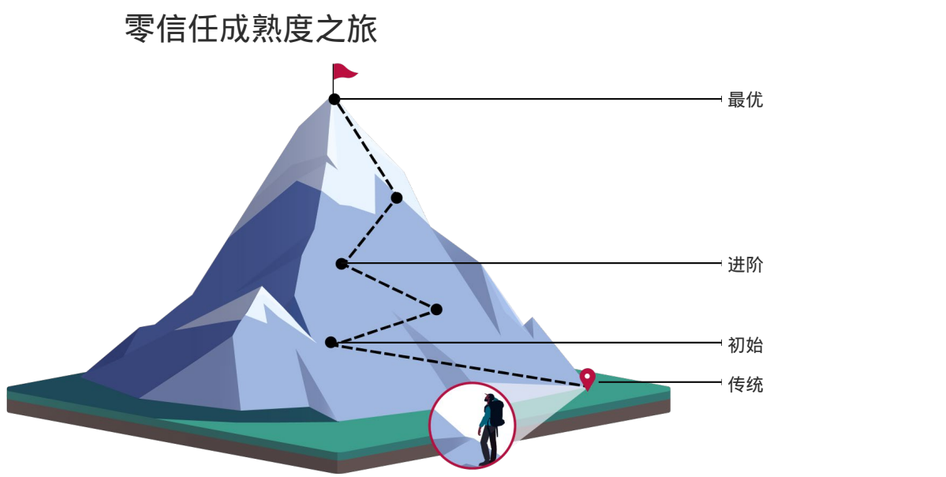


图2:零信任成熟度之旅

如图2所示，各机构应预期，随着零信任成熟度在各支柱内部及跨支柱推进，所需投入水平和实现收益将显著增加。当各机构规划其ZTA旅程时，应探索提升支柱成熟度的机会，以对齐具体任务需求并支持其他支柱的进一步增长。图3强调了机构随时间从传统企业向未来状态的预期演进，该未来状态具有更动态的更新、自动化流程、集成能力以及最优阶段的其他特征(如成熟度模型中所述)。这些阶段是动态的并呈指数级增长；从一个成熟度阶段到另一个阶段的计划进展可能会随时间在范围和影响上发生变化。

[9] NIST白皮书。《为零信任架构做规划：联邦管理员规划指南》。https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-fo

[10]参见 NIST SP 800-53 第 5 修订版中的 AC-6。https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

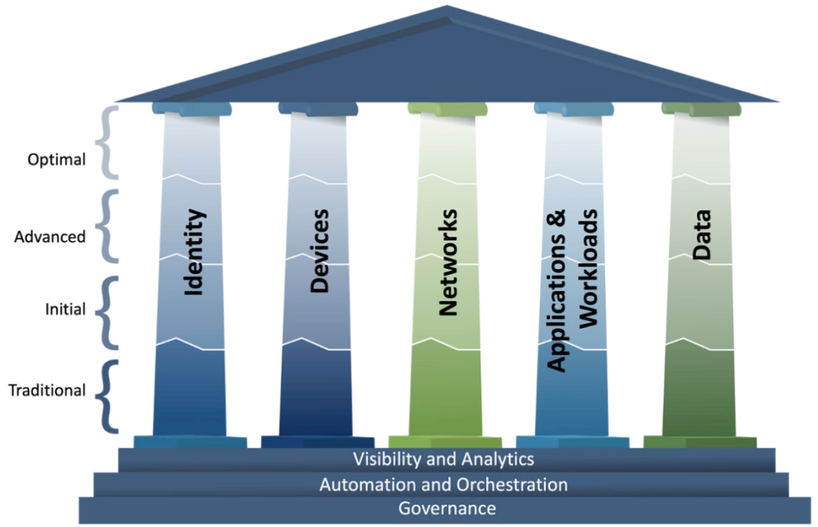


Figure 3: Zero Trust Maturity Evolution

Agencies should use the following guiding criteria of each stage to identify maturity for each zero trust technology pillar and provide consistency across the maturity model:

- **Traditional**—manually configured lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging); static security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry.
- **Initial**—starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems.
- **Advanced**—wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources).
- **Optimal**—fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers; dynamic least privilege access (just-enough and within thresholds) for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; and centralized visibility with comprehensive situational awareness.

Figure 4 provides a high-level overview of the ZTMM, including key aspects of the pillar-specific functions for each pillar and across each maturity stage.

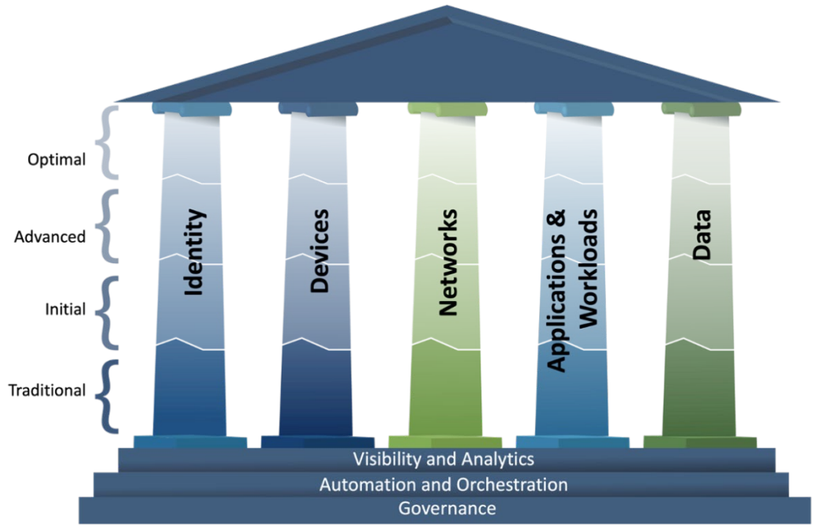


图3:零信任成熟度演进

机构应使用以下各阶段的指导标准来确定每个零信任技术支柱的成熟度，并在整个成熟度模型中保持一致：

- **传统** - 手动配置生命周期(即从建立到退役)和属性分配(安全与日志记录)；静态安全策略和解决方案，一次只处理一个支柱，对外部系统存在离散依赖；仅在配置时建立最小权限；策略执行支柱彼此孤立；手动响应和缓解部署；依赖关系、日志和遥测数据的关联有限。
- **初始** - 开始自动化属性分配和生命周期配置、策略决策与执行，以及集成外部系统的初始跨支柱解决方案；配置后对最小权限进行一些响应性更改；以及内部系统的聚合可见性。
- **进阶** - 在适用的情况下，通过跨支柱协调实现生命周期以及配置和策略分配的自动化控制；集中式可见性和身份控制；策略执行跨支柱集成；对预定义缓解措施作出响应；基于风险和态势评估更改最小权限；并逐步建立企业范围的意识(包括外部托管的资源)。
- **最优** - 完全自动化、即时(just-in-time)的生命周期以及向资产和资源分配属性，这些资产和资源基于自动化/观测到的触发器进行自我报告并采用动态策略；在企业范围内为资产及其各自依赖关系提供动态最小权限访问(恰好足够且在阈值内)；通过持续监测实现跨支柱互操作性；以及具有全面态势感知的集中式可见性。

图 4 提供了 ZTMM 的高层概览，包括每个支柱在各成熟度阶段中支柱特定功能的关键方面。

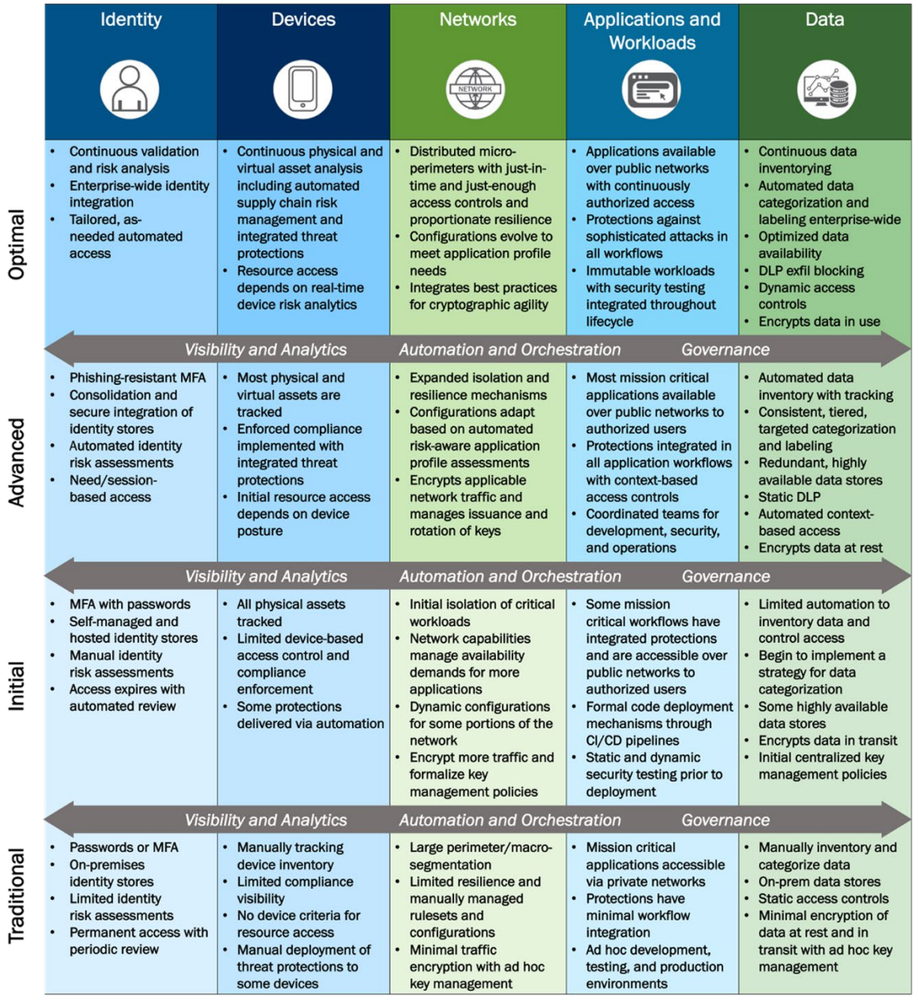


Figure 4: High-Level Zero Trust Maturity Model Overview

These maturity stages and the details associated with each pillar allow agencies to assess, plan, and maintain the investments needed to progress toward a ZTA. Subsections 0–5.5 provide high-level information to support agencies in transitioning to zero trust across the five different pillars: **Identity**, **Devices**, **Networks**, **Applications and Workloads**, and **Data**. Each pillar also includes general details regarding *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* capabilities to support integration with that pillar and across the model.

These three cross-cutting capabilities highlight activities to support interoperability of functions across pillars based on the following descriptions:

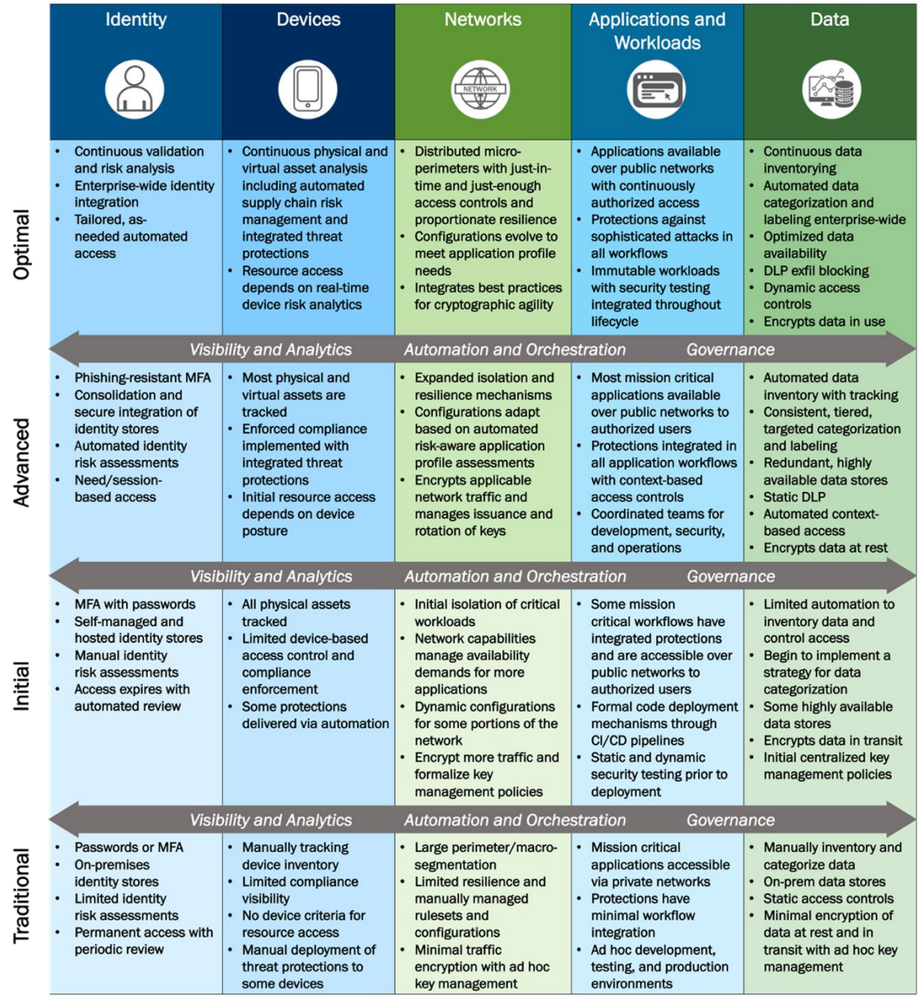


图4:高层级零信任成熟度模型概览

这些成熟度阶段以及与每个支柱相关的细节使机构能够评估、规划并维持向 ZTA 推进所需的投资。第 0-5.5 小节提供了高层级信息，以支持机构在五个不同支柱上过渡到零信任：**身份**、**设备**、**网络**、**应用与工作负载**和**数据**。每个支柱还包含有关可见性与分析、自动化与编排和治理能力的一般细节，以支持与该支柱以及跨模型的集成。

这三项横向能力突出了基于以下描述支持跨支柱功能互操作性的活动：

- **Visibility and Analytics:** Visibility refers to the observable artifacts that result from the characteristics of and events within enterprise-wide environments.[11] The focus on cyber-related data analysis can help inform policy decisions, facilitate response activities, and build a risk profile to develop proactive security measures before an incident occurs.[12]
- **Automation and Orchestration:** Zero trust makes full use of automated tools and workflows that support security response functions across products and services while maintaining oversight, security, and interaction of the development process for such functions, products, and services.
- **Governance:** Governance refers to the definition and associated enforcement of agency cybersecurity policies, procedures, and processes, within and across pillars, to manage an agency's enterprise and mitigate security risks in support of zero trust principles and fulfillment of federal requirements.[13]

While the ZTMM covers many aspects of cybersecurity critical to federal enterprises, it does not address other aspects of cybersecurity such as activities related to incident response, specifics for logging, monitoring, alerting, forensic analysis, risk acceptance, recovery.[14] Other aspects of and best practices for enterprise cybersecurity posture management are not explicitly included within the maturity model functions. Although the maturity model is not intended to be exclusionary, it does not address challenges specific to operational technologies,[15] certain classes of internet of things (IoT) devices,[16] or broadly incorporating emerging technologies such as deception platforms, authenticated web application firewalls, behavior analytics, etc. Methodologies such as recommendations to best incorporate machine learning and artificial intelligence capabilities within zero trust solutions are not included in this model. Mature Agencies should take steps to monitor and assess the performance and integrity of their security capabilities, underlying infrastructure, and policies to detect unauthorized access and changes as they mature each pillar. Agencies should be careful to not create new opportunities for exploitation or weaken security protocols. Research and development are required to effectively assure software and hardware systems integrity at scale across federal enterprises.[17,18,19]

[11] See CISA's extensible Visibility Reference Framework (eVRF) Guidebook: https://www.cisa.gov/blog/2022/04/19/scuba-it-means-better-visibility-standards-and-security-practices-government-cloud.

[12] Agencies should review OMB Memo M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021) for further guidance on logging requirements as they make decisions and investments for visibility needs. https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

[13] Based on the Governance function of the Identify category of the NIST Cyber Security Framework Version 1.1: https://www.nist.gov/cyberframework/framework.

[14] Backups are included within the Data Pillar; however, for detailed guidance on data integrity and recovery, Agencies should consult NIST SP 1800-11: https://csrc.nist.gov/News/2020/sp-1800-11-data-integrity-ransomware-recovery.

[15] NIST. Guide to Operational Technology Security: NIST Requests Comments on Draft SP 800-82r3. April 2022. https://csrc.nist.gov/News/2022/guide-to-operational-technology-ot-security.

[16] NIST. Cybersecurity for IoT Program. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

[17] NIST NCCOE: Supply Chain Assurance. https://www.nccoe.nist.gov/supply-chain-assurance.

[18] NIST NCCOE: Software Supply Chain and DevOps Security Practices. https://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.

[19] Agencies should review the information and resources available for Software Bill of Materials (SBOM) and Vulnerability Exploitability eXchange (VEX) as community advancements continue at: https://www.cisa.gov/sbom.

可见性与分析：可见性是指由此产生的可观察工件
企业范围环境的特征和事件所产生的可观测产物。[11]对网络相关数据分析的关注有助于为策略决策提供信息、促进响应活动，并构建风险画像，以便在事件发生前制定主动安全措施。[12]

自动化与编排：零信任充分利用自动化工具和工作流，这些工具和工作流
支持跨产品和服务的安全响应功能，同时对此类功能、产品和服务的开发过程保持监督、安全性和交互。

治理：治理是指在支柱内部和跨支柱之间定义并相关执行机构网络安全
政策、程序和流程，以管理机构的 enterprise 并降低安全风险，支持零信任原则和满足联邦要求。[13]

尽管 ZTMM 涵盖了联邦企业至关重要的许多网络安全方面，但它并未涉及网络安全的其他方面，例如与事件响应相关的活动、日志记录、监控、告警、取证分析、风险接受、恢复的具体细节。[14]企业网络安全态势管理的其他方面和最佳实践并未明确纳入成熟度模型的功能之中。尽管该成熟度模型并非意在排他，但它并未涉及运营技术特有的挑战，[15]某些类别的物联网(IoT)设备，[16]或广泛纳入新兴技术，如欺骗平台、经过身份验证的 Web 应用防火墙、行为分析等。诸如关于如何在零信任解决方案中最佳地纳入机器学习和人工智能能力的建议等方法论并未包含在本模型中。成熟的机构应采取措施，监控和评估其安全能力、底层基础设施和策略的性能与完整性，以便在成熟每个支柱的过程中检测未经授权的访问和变更。机构应谨慎避免创造新的利用机会或削弱安全协议。需要开展研究与开发，以有效保障联邦企业范围内软件和硬件系统的大规模完整性。[17,18,19]

[11]参见CISA的可扩展可见性参考框架(eVRF)指南：https://www.cisa.gov/blog/2022/04/19/scuba-it-means-better-Visibility-standards-and-security-practices-政府云。

[12]各机构在就可见性需求做出决策和投资时，应查阅 OMB 备忘录 M-21-31《提升联邦政府与网络安全事件相关的调查与修复能力》(2021 年 8 月 27 日)，以获取有关日志记录要求的进一步指导。https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-与网络安全事件相关的能力.pdf.

[13]基于 NIST 网络安全框架 1.1 版识别类别的治理功能： https://www.nist.gov/cyberframework/framework.

[14]备份包含在数据支柱中；然而，关于数据完整性和恢复的详细指导，各机构应参考 NIST SP 1800-11:https://csrc.nist.gov/News/2020/sp-1800-11-data-integrity-ransomware-recovery.

[15] 0-82r3 草案征求意见。2022 年 4 月。https://csrc.nist.gov/News/2022/guide-to-Operational-Technology-ot-security.

[16] NIST。物联网网络安全项目。https://www.nist.gov/itl/applied-Cybersecurity/nist-Cybersecurity-iot-program.

[17] NIST NCCOE：供应链保障。https://www.nccoe.nist.gov/supply-chain-assurance.

[18] ttps://www.nccoe.nist.gov/projects/software-supply-chain-and-devops-security-practices.

[19]随着社区不断推进，联邦机构应查阅软件物料清单(SBOM)和漏洞可利用性交换(VEX)可用的信息与资源，详见：https://www.cisa.gov/sbom.

When planning ZTA implementation, agencies should make decisions based on factors which include risk, mission, federal requirements, and operating constraints. While this model is generally aligned to a federal enterprise's single administrative domain or accreditation boundary, agencies should also assess how their interactions with and reliance upon external partners, stakeholders, and service providers factor into their ZTA.[20] This maturity model should not be viewed as a strict set of requirements but as a general guide to help agencies successfully implement their ZTA and adopt an overall improved cybersecurity posture.

[20] These considerations span pillars and functions such as trusting credentials, assessing supply chains, differences in data categorization, policy exceptions, variations in risk thresholds, and more.

在规划 ZTA 实施时，各机构应基于包括风险、任务、联邦要求和运营约束在内的因素做出决策。虽然本模型总体上与联邦企业的单一管理域或认证边界保持一致，但各机构还应评估其与外部合作伙伴、利益相关者和服务提供商的互动及依赖关系如何纳入其 ZTA。[20]本成熟度模型不应被视为一套严格的要求，而应作为一份通用指南，帮助各机构成功实施其 ZTA 并实现整体安全态势的改进。

[20]这些考量跨越多个支柱和功能，例如信任凭证、评估供应链、数据分类差异、策略例外、风险阈值差异等。

5.1 Identity

An identity refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities.

Agencies should ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access. Agencies should integrate identity, credential, and access management solutions where possible throughout their enterprise to enforce strong authentication, grant tailored context-based authorization, and assess identity risk for agency users and entities. Agencies should integrate their identity stores and management systems, where appropriate, to enhance awareness of enterprise identities and their associated responsibilities and authorities.

Table 2 lists identity functions pertaining to zero trust and considerations for Visibility and Analytics, Automation and Orchestration, and Governance within the context of identity.

Table 2: Identity Pillar

Function	Traditional	Initial	Advanced	Optimal
Authentication	Agency authenticates identity using either passwords or multi-factor authentication[21] (MFA) with static access for entity identity.	Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password-	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.

[21] CISA resources for MFA available at: https://www.cisa.gov/mfa.

5.1 身份

身份是指唯一描述联邦机构用户或实体(包括非人员实体)的一个属性或一组属性。

机构应确保并强制执行用户和实体在正确的时间为正确的目的访问正确的资源，而不授予过多的访问权限。机构应尽可能在其整个企业中集成身份、凭证和访问管理解决方案，以强制执行强身份验证、授予定制的基于上下文的授权，并评估机构用户和实体的身份风险。机构应酌情集成其身份存储和管理系统，以增强对企业身份及其相关职责和权限的了解。

表 2 列出了与零信任相关的身份功能，以及在身份背景下对可见性与分析、自动化与编排和治理的考量。

表2:身份支柱

功能	传统	初始	进阶	最优
身份验证	机构对身份进行认证 使用密码或 多因素认证[21] (MFA) 静态访问用于 实体身份。	机构进行认证 使用MFA对身份进行认证，其 可能将密码作为 一个因素，并要求 多个实体的验证 属性(例如，区域设置或活动)。	机构开始 使用以下方式认证所有身份 抗网络钓鱼MFA以及 属性，包括初始 密码的实施	机构持续 通过以下方式验证身份 抗网络钓鱼MFA，而非 仅在访问最初 授予时。

[21] CISA 提供的 MFA 资源见：https://www.cisa.gov/mfa.

Function	Traditional	Initial	Advanced	Optimal
			less MFA via FIDO2[22] or PIV[23].	
Identity Stores	Agency only uses self-managed, on-premises (i.e., planned, deployed, and maintained by agency) identity stores.	Agency has a combination of self-managed identity stores and hosted identity store(s) (e.g., cloud or other agency) with minimal integration between the store(s) (e.g., Single Sign-on.).	Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.	Agency securely integrates their identity stores across all partners and environments as appropriate.
Risk Assessments	Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).	Agency determines identity risk using manual methods and static rules to support visibility.	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.
Access Management (New Function)	Agency authorizes permanent access with periodic review for both privileged and unprivileged accounts.	Agency authorizes access, including for privileged access requests, that expires with automated review.	Agency authorizes need-based and session-based access, including for privileged access request, that is tailored to actions and resources.	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.

[22] FIDO2 is a set of protocols developed in collaboration by the Fast IDentity Online (FIDO) Alliance and World Wide Web Consortium (W3C). FIDO2 is designed to enable easy, secure, and passwordless authentication. This approach leverages W3C's WebAuthn protocol and the FIDO Alliance's Client to Authenticator Protocol (CTAP) protocol.

FIDO Alliance. *FIDO Alliance - Open Authentication Standards More Secure than Passwords*. https://fidoalliance.org/.

World Wide Web Consortium. *Web Authentication: An API for accessing Public Key Credentials*. https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.

FIDO Alliance. Client to Authenticator Protocol. Proposed Standard, June 2021. https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-errata-20220621.html.

[23] Personal Identity Verification. A PIV credential is a U.S. federal government-wide credential used to access federally controlled facilities and information systems at the appropriate security level. https://playbooks.idmanagement.gov/piv/.

功能	传统	初始	进阶	最优
			通过 FIDO2 [22]或 PIV [23].	
身份存储	机构仅使用自身 托管的、本地部署的（即， 已规划、已部署和 由机构维护） 身份存储。	机构采用组合 自管理身份 存储和托管身份 存储（例如，云或其他 机构）以最小 之间的集成 存储（例如，单点登录）。	机构开始安全地 整合并集成 一些自管理和 托管身份存储。	机构安全地集成 其身份存储在所有 合作伙伴和环境作为 适当。
风险评估	机构进行有限的 对身份进行判定 风险（即，可能性 身份被泄露）。	机构确定身份 使用手动方法进行风险 和静态规则以支持 可见性。	机构确定身份 通过一些自动化进行风险 分析和动态规则以 为访问决策提供信息并 响应活动。	机构确定身份 基于以下内容实时进行风险 持续分析和 动态规则以提供 持续保护。
访问管理(新增) **Function)**	机构授权永久 访问并定期审查 针对特权和 非特权账户。	机构授权访问， 包括针对特权 访问请求，该请求会过期 并自动审查。	机构授权按需 基于和基于会话的 访问，包括针对 特权访问请求，该请求 针对行动和 资源。	机构使用自动化来 授权即时和 恰到好处的访问，量身定制 针对单个操作和 个别资源需求。

[22] FIDO2 是由快速身份在线(FIDO)联盟和万维网联盟(W3C)合作开发的一套协议。FIDO2 旨在实现简便、安全且无密码的身份验证。该方法利用 W3C 的 WebAuthn 协议和 FIDO 联盟的客户端到认证器协议(CTAP)。

FIDO 联盟。*FIDO* 联盟--比密码更安全的开放认证标准。https://FIDO Alliance.org/.

万维网联盟。*Web* 认证：用于访问公钥凭据的 *API*。https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.FIDO 联盟。客户端到认证器协议。拟议标准，2021 年 6 月。https://FIDO Alliance

authenticator-protocol-v2.1-ps-errata-20220621.html.

[23]个人身份验证。PIV 凭证是美国联邦政府范围内用于在适当安全级别访问联邦控制设施和信息系统的凭证。https://playbooks.idmanagement.gov/piv/.

Function	Traditional	Initial	Advanced	Optimal
Visibility and Analytics Capability	Agency collects user and entity activity logs, especially for privileged credentials, and performs some routine manual analysis.	Agency collects user and entity activity logs and performs routine manual analysis and some automated analysis, with limited correlation between log types.	Agency performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.	Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.
Automation and Orchestration Capability	Agency manually orchestrates (onboards, offboards, and disables) self-managed identities (users and entities), with little integration, and performs regular review.	Agency manually orchestrates privileged and external identities and automates orchestration of non-privileged users and of self-managed entities.	Agency manually orchestrates privileged user identities and automates orchestration of all identities with integration across all environments.	Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.
Governance Capability	Agency implements identity policies (authentication, credentials, access, lifecycle, etc.) with enforcement via static technical mechanisms and manual review.	Agency defines and begins implementing identity policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements identity policies for enterprise-wide enforcement with automation and updates policies periodically.	Agency implements and fully automates enterprise-wide identity policies for all users and entities across all systems with continuous enforcement and dynamic updates.

功能	传统	初始	进阶	最优
可见性与分析能力	机构收集用户和实体活动日志，尤其是针对特权凭证，以及执行一些常规手动分析。	机构收集用户和实体活动日志和执行常规手动分析和一些自动化分析，并之间有限的相关性日志类型。	机构执行自动化跨部分用户和实体活动日志类型和增强收集以解决可见性方面的差距。	机构维护全面可见性和态势感知跨企业通过执行自动化分析优于用户活动日志类型，包括基于行为的分析。
自动化与编排能力	机构手动编排（入职、离职和禁用）自管理身份（用户和实体），集成很少，并且执行定期审查。	机构手动编排特权用户和外部身份和自动化编排非特权用户和自我管理的实体。	机构手动编排特权用户身份并自动化所有身份的编排与所有方面的集成环境。	机构自动化所有身份的编排全面集成跨所有环境基于行为、注册以及部署需求。
治理能力	机构实施身份策略（认证、凭证、访问、生命周期、等），并通过以下方式执行静态技术机制以及手动审查。	机构定义并开始实施身份企业范围的策略以最少资源执行自动化和手动更新。	机构实施身份企业范围的策略通过自动化执行并更新策略定期。	机构实施并为所有完全自动化企业范围的身份策略跨所有方面的用户和实体具有持续性的系统执行和动态更新。

5.2 Devices

A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, IoT devices, networking equipment, and more.

Devices may be agency-owned or bring-your-own-device (BYOD) property of employees, partners, or visitors. Agencies should secure all agency devices, manage the risks of authorized devices that are not agency-controlled, and prevent unauthorized devices from accessing resources. Device management includes maintaining a dynamic inventory of all assets including their hardware, software, firmware, etc., along with their configurations and associated vulnerabilities as they become known.

Many devices present specific ZTA challenges and must be evaluated on a case-by-case basis as part of a risk-based process. For example, networking equipment, printers, and others may offer limited options for authentication, visibility, and security. Agencies employing BYOD policies will likely have fewer options to maintain visibility and control of such devices. The technological landscape for devices continues to change and as agencies incorporate additional devices into their enterprise, they will need to continue to manage the evolving risks associated with these devices.[24] In some cases, agencies may be unable to adopt the guidance for certain subsets of their devices. Agencies will also face challenges in ensuring trusted devices and their services have not reached end-of-life and are still covered by their life-time-support, as legacy devices often have a higher number of unmitigated vulnerabilities, available misconfigurations, and unknown risks. However, despite these challenges, agencies should still be able to make considerable progress toward a ZTA.

On-premises computing asset management involves documenting and managing physical assets (devices). As agencies move to cloud environments, this creates new considerations and opportunities for managing and tracking agency cloud and virtual assets. Cloud assets include compute resources (e.g., virtual machines, servers, or containers), storage resources (e.g., block storage or file storage), platform assets (e.g., databases, web servers, message buses/queues), and network resources (e.g., virtual networks, VPNs, gateways, DNS services, etc.) and virtual resources associated with other managed cloud services (e.g., artificial intelligence models).

Table 3 lists functions for devices pertaining to zero trust, as well as considerations for *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* within the context of devices.

[24] Agencies should consult OMB Memo M-22-01 *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*. October 8, 2021. https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.

5.2 设备

设备是指任何可连接到网络的资产(包括其硬件、软件、固件等)，包括服务器、台式机和笔记本电脑、打印机、移动电话、IoT 设备、网络设备等。

设备可以是联邦机构所有，也可以是员工、合作伙伴或访客自带设备(BYOD)财产。联邦机构应保护所有机构设备，管理非机构控制的授权设备的风险，并防止未授权设备访问资源。设备管理包括维护所有资产的动态清单，包括其硬件、软件、固件等，以及其配置和已知的相关漏洞。

许多设备带来了特定的 ZTA 挑战，必须作为基于风险流程的一部分逐案评估。例如，网络设备、打印机和其他设备可能在身份验证、可见性和安全性方面提供的选项有限。采用 BYOD 政策的机构在保持对此类设备的可见性和控制方面可能选项较少。设备的技术格局不断变化，随着机构将更多设备纳入其企业，它们将需要继续管理这些设备相关的不断演变的风险。[24]在某些情况下，机构可能无法对其某些设备子集采用该指南。机构在确保可信设备及其服务尚未达到生命周期终止且仍在其终身支持覆盖范围内方面也将面临挑战，因为遗留设备通常有更多未缓解的漏洞、可用的错误配置和未知风险。然而，尽管存在这些挑战，机构仍应能够在实现 ZTA 方面取得相当大的进展。

本地计算资产管理涉及记录和管理物理资产(设备)。随着机构迁移到云环境，这为管理和跟踪机构云和虚拟资产创造了新的考量和机会。云资产包括计算资源(例如，虚拟机、服务器或容器)、存储资源(例如，块存储或文件存储)、平台资产(例如，数据库、Web 服务器、消息总线/队列)和网络资源(例如，虚拟网络、VPN、网关、DNS 服务等)以及与其它托管云服务相关的虚拟资源(例如，人工智能模型)。

表 3 列出了与零信任相关的设备功能，以及在设备背景下对可见性与分析、自动化与编排和治理的考虑因素。

[24]各机构应查阅 OMB 备忘录 M-22-01 通过端点检测与响应提升联邦政府系统上网络安全漏洞和事件的检测能力。2021 年 10 月 8 日。https://www.whitehouse.gov/

Table 3: Devices Pillar

Function	Traditional	Initial	Advanced	Optimal
Policy Enforcement & Compliance Monitoring (New Function)	Agency has limited, if any, visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Agency receives self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.	Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.
Asset & Supply Chain Risk Management (New Function)	Agency does not track physical or virtual assets in an enterprise-wide or cross-vendor manner and manages its own supply chain acquisition of devices and services in ad hoc fashion with a limited view of enterprise risks.	Agency tracks all physical and some virtual assets and manages supply chain risks by establishing policies and control baselines according to federal recommendations using a robust framework, (e.g., NIST SCRM.)[25]	Agency begins to develop a comprehensive enterprise view of physical and virtual assets via automated processes that can function across multiple vendors to verify acquisitions, track development cycles, and provide third-party assessments.	Agency has a comprehensive, at- or near-real-time view of all assets across vendors and service providers, automates its supply chain risk management as applicable, builds operations that tolerate supply chain failures, and incorporates best practices.
Resource Access (Formerly Data Access)	Agency does not require visibility into devices or virtual assets used to access resources.	Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.	Agency's initial resource access considers verified device or virtual asset insights.	Agency's resource access considers real-time risk analytics within devices and virtual assets.

[25]NIST. NIST Updates Cybersecurity Guidance for Supply Chain Risk Management. May 5, 2022. https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management.

表3:设备支柱

功能	传统	初始	进阶	最优
策略执行与合规监控(新功能)	机构拥有有限的能力（如果有的话）可见性（即，能够检查设备行为）对设备合规性的少数执行方法策略或管理软件、配置或漏洞。	机构接收自我报告的设备特征（例如，密钥、令牌、用户等，在设备）但具有有限的执行机制。机构有一个初步的、基本流程以批准软件使用并推送更新与配置设备变更。	机构已验证的洞察（即，管理员可以检查和验证数据在设备上）在初始访问时到设备并执行大多数设备的合规性和虚拟资产。机构使用自动化方法管理设备和虚拟资产，批准软件，并识别漏洞并安装补丁。	机构持续验证洞察并执行整个生命周期内的合规性设备的生命周期和虚拟资产。机构整合设备、软件、配置和漏洞管理在整个机构范围内环境，包括针对虚拟资产。
资产与供应链风险管理(新增 Function)	机构不跟踪物理或虚拟资产在以企业范围或跨供应商的方式，并管理其自身的供应链设备和以临时方式提供服务对.....的有限可见性企业风险。	机构跟踪所有物理和部分虚拟资产和通过以下方式管理供应链风险制定政策和根据以下内容控制基线使用联邦建议一个稳健的框架，（例如，NIST SCRM。）[25]	机构开始制定全面的企业级物理和虚拟资产的视图通过自动化方式获取资产能够运作的流程跨多个供应商以验证采购，跟踪开发周期，以及提供第三方评估。	机构拥有全面的、实时或近实时所有资产的实时视图跨供应商和服务提供商，自动化其供应链风险视情况适用的管理，构建的运营能够容忍供应链故障，并纳入最佳实践。
资源访问(原数据访问)	机构不要求对设备或用于访问的虚拟资产资源。	机构要求部分设备或虚拟资产进行报告特征，然后使用此信息以批准资源访问。	机构的初始资源访问考虑经过验证的设备或虚拟资产洞察。	机构的资源访问考虑实时风险设备内及.....的分析虚拟资产。

[25] NIST。NIST 更新供应链风险管理的网络安全指南。2022 年 5 月 5 日。https://www.nist.gov/news-events/news/2022/05/nist-updates-网络安全指导--供应链风险管理。

Function	Traditional	Initial	Advanced	Optimal
Device Threat Protection (New Function)	Agency manually deploys threat protection capabilities to some devices.	Agency has some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration.	Agency begins to consolidate threat protection capabilities to centralized solutions for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring.	Agency has a centralized threat protection security solution(s) deployed with advanced capabilities for all devices and virtual assets and a unified approach for device threat protection, policy enforcement, and compliance monitoring.
Visibility and Analytics Capability	Agency uses a physically labeled inventory and limited software monitoring to review devices on a regular basis with some manual analysis.	Agency uses digital identifiers (e.g., interface addresses, digital tags) alongside a manual inventory and endpoint monitoring of devices when available. Some agency devices and virtual assets are under automated analysis (e.g., software-based scanning) for anomaly detection based on risk.	Agency automates both inventory collection (including endpoint monitoring on all standard user devices, e.g., desktops and laptops, mobile phones, tablets, and their virtual assets) and anomaly detection to detect unauthorized devices.	Agency automates status collection of all network-connected devices and virtual assets while correlating with identities, conducting endpoint monitoring, and performing anomaly detection to inform resource access. Agency tracks patterns of provisioning and/or de-provisioning of virtual assets for anomalies.
Automation and Orchestration Capability	Agency manually provisions, configures, and/or registers devices within the enterprise.	Agency begins to use tools and scripts to automate the process of provisioning, configuration, registration, and/or deprovisioning for devices and virtual assets.	Agency has implemented monitoring and enforcement mechanisms to identify and manually disconnect or isolate non-compliant (vulnerable, unverified certificate; unregistered mac address) devices and virtual assets.	Agency has fully automated processes for provisioning, registering, monitoring, isolating, remediating, and deprovisioning devices and virtual assets.

功能	传统	初始	进阶	最优
设备威胁防护 (新功能)	机构手动部署 威胁防护能力 到部分设备。	机构拥有一些自动化 用于部署和 更新威胁防护 设备和设备的 capabilities 虚拟资产，且仅有有限的 策略执行和 合规监控 集成。	机构开始 整合威胁防护 能力至集中式 面向设备和 虚拟资产并集成 这些能力中的大部分 具备策略执行和 合规监控。	机构拥有一个集中式 威胁防护安全 部署的解决方案，具备 面向所有的高级能力 设备和虚拟资产 以及统一的方法，用于 设备威胁防护、 策略执行和 合规监控。
可见性与分析 能力	机构使用物理 带标签的清单和 有限的软件监控 定期审查设备 定期进行一些 手动分析。	机构使用数字标识符 （例如，接口地址、 数字标签）以及 手动资产清单和端点 在以下情况下对设备进行监控 可用。一些机构 设备和虚拟资产 在自动化分析下（例如， 基于软件的扫描）用于 基于以下内容的异常检测 风险。	机构同时自动化 资产清单收集 （包括端点 对所有标准进行监控 用户设备，例如台式机 和笔记本电脑、移动电话、 平板电脑及其虚拟 资产）和异常 检测以检测 未经授权的设备。	机构自动化状态 所有联网设备的集合以及 虚拟资产同时 与身份相关联， 进行端点 监控，并执行 异常检测以告知 资源访问。机构 跟踪以下模式 为虚拟资产的供应和/或取消 供应以应对异常情况。
自动化与 编排能力	机构手动 配置、设置、 和/或注册设备 在企业内部。	机构开始使用工具并 用于自动化该流程的脚本 配置、设置、 注册和/或 设备和 虚拟资产。	机构已实施 监控与执行 用于识别和 手动断开或 隔离不合规 （存在漏洞、未经验证 证书；未注册的 MAC 地址) 设备和虚拟资产。	机构已完全自动化 用于配置、设置的流程 注册、监控、 隔离、修复和 取消配置设备和 虚拟资产。

Function	Traditional	Initial	Advanced	Optimal
Governance Capability	Agency sets some policies for the lifecycle[26] of their traditional and peripheral computing devices and relies on manual processes to maintain (e.g., update, patch, sanitize) these devices.	Agency sets and enforces policies for the procurement of new devices, the lifecycle of non-traditional computing devices and virtual assets, and for regularly conducting monitoring and scanning of devices.	Agency sets enterprise-wide policies for the lifecycle of devices and virtual assets, including their enumeration and accountability, with some automated enforcement mechanisms.	Agency automates policies for the lifecycle of all network-connected devices and virtual assets across the enterprise.

[26] Lifecycle includes procuring, configuring, tracking, monitoring, updating, using, sanitizing, deprovisioning, and recovering devices.

功能	传统	初始	进阶	最优
治理能力	机构制定部分策略 对于其生命周期[26] 传统及外围 计算设备以及 依赖人工流程 维护（例如，更新、 修补、清理）这些 设备。	机构制定并执行 采购策略 新设备、生命周期 非传统计算 设备和虚拟资产，以及 定期开展 监控和扫描 设备。	机构制定企业级 生命周期策略 设备和虚拟资产、 包括其枚举 和问责制，并具有 一些自动化 执行机制。	机构自动化策略 所有 网络连接设备 以及虚拟资产，跨越 企业。

[26]生命周期包括设备的采购、配置、跟踪、监控、更新、使用、净化、取消配置和恢复。

5.3 Networks

A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages.

ZTAs enable a shift away from traditional perimeter-focused approaches to security and permit agencies to manage internal and external traffic flows, isolate hosts, enforce encryption, segment activity, and enhance enterprise-wide network visibility. ZTAs permit security controls to be implemented closer to the applications, data, and other resources and augment traditional network-based protections and improve defense-in-depth. Each application can be treated uniquely by the network for its demands on access, priority, reachability, connections to dependency services, and connection pathways. These network application demands can be captured as an application profile, and repeated profiles can then be treated as a traffic class.

Table 4 lists network functions pertaining to zero trust and the considerations for *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* within the context of networks.

Table 4: Networks Pillar

Function	Traditional	Initial	Advanced	Optimal
Network Segmentation	Agency defines their network architecture using large perimeter/macro-segmentation with minimal restrictions on reachability within network segments. Agency may also rely on multi-service interconnections (e.g., bulk traffic VPN tunnels).	Agency begins to deploy network architecture with the isolation of critical workloads, constraining connectivity to least function principles, and a transition toward service-specific interconnections.	Agency expands deployment of endpoint and application profile isolation mechanisms to more of their network architecture with ingress/egress micro-perimeters and service-specific interconnections.	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.
Network Traffic Management (New Function)	Agency manually implements static network rules and configurations to manage traffic at service provisioning, with limited monitoring capabilities (e.g.,	Agency establishes application profiles with distinct traffic management features and begins to map all applications to these profiles. Agency expands	Agency implements dynamic network rules and configurations for resource optimization that are periodically adapted based upon automated risk-aware	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications

5.3 网络

网络是指一种开放通信媒介，包括机构内部网络、无线网络和互联网等典型渠道，以及蜂窝和应用层渠道等其他用于传输的潜在渠道

messages.

ZTA 支持从传统的以边界为中心的安全方法转变，使机构能够管理内部和外部流量、隔离主机、实施加密、分段活动并增强企业范围的网络可见性。ZTA 允许将安全控制实施在更靠近应用、数据和其他资源的位置，并增强传统的基于网络的防护并改进纵深防御。每个应用都可以因其对访问、优先级、可达性、与依赖服务的连接以及连接路径的需求而被网络独特地对待。这些网络应用需求可以捕获为应用配置文件，重复的配置文件随后可以被视为一个流量类别。

表4列出了与零信任相关的网络功能，以及在可见性与分析、自动化与编排和治理在网络语境中。

表4:网络支柱

功能	传统	初始	进阶	最优
网络分段	机构定义其网络架构使用大范围边界/宏观分段，且最小化对可达性的限制在网络段内。机构也可能依赖多服务互连（例如，批量流量 VPN 隧道）。	机构开始部署网络架构与关键隔离工作负载，限制到最小功能的连接原则，以及一个过渡朝向特定服务的互连。	机构扩展部署终端和应用配置文件隔离机制到其网络的更多部分架构，具有入口/出口微边界及服务特定互连。	机构网络架构由完全分布式入口/出口微边界及广泛基于微隔离的围绕应用配置文件具有动态即时以及恰好足够的连接用于特定服务的互连。
网络流量管理(新增 Function)	机构手动实施静态网络规则和配置以在服务层面管理流量配置，且有限的监控能力（例如，	机构建立应用配置文件，具有不同的流量管理功能并开始映射所有应用到这些配置文件。机构扩展	机构实施动态网络规则和资源配置优化，这些定期调整，基于基于自动化风险感知	机构实施动态网络规则和配置，其持续演进以满足应用配置文件需求以及重新确定应用优先级

Function	Traditional	Initial	Advanced	Optimal
	application performance monitoring or anomaly detection) and manual audits and reviews of profile changes for mission critical applications.	application of static rules to all applications and performs periodic manual audits of application profile assessments.	and risk-responsive application profile assessments and monitoring.	based on mission criticality, risk, etc.
Traffic Encryption (Formerly Encryption)	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications[27], to formalize key management policies, and to secure server/service encryption keys.	Agency ensures encryption for all applicable internal and external traffic protocols,[28] manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.[29]	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise-wide, and incorporates best practices for cryptographic agility as widely as possible.
Network Resilience (New Function)	Agency configures network capabilities on a case-by-case basis to only match individual application availability demands with limited resilience mechanisms for workloads not deemed mission critical.	Agency begins to configure network capabilities to manage availability demands for additional applications and expand resilience mechanisms for workloads not deemed mission critical.	Agency has configured network capabilities to dynamically manage the availability demands and resilience mechanisms for the majority of their applications.	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.
Visibility and Analytics Capability	Agency incorporates limited boundary-focused network monitoring capabilities with	Agency employs network monitoring capabilities based on known indicators of	Agency deploys anomaly-based network detection capabilities to develop	Agency maintains visibility into communication across all agency networks and

[27] For example, when both HTTP and HTTPS options are available, policies and settings prefer HTTPS.

[28] There are a variety of resources agencies should review in regard to encrypting and decrypting network traffic (or not) for inspection and visibility needs as part of their zero trust adoption: OMB M-15-13, M-19-26, M-22-09, DHS Binding Operational Directive 18-01, NIST SP 800-207, among others. See also: https://www.cisa.gov/uscert/ncas/alerts/TA17-075A.

[29] DHS. Cryptographic Agility Infographic. May 12, 2022. https://www.dhs.gov/publication/cryptographic-agility-infographic.

功能	传统	初始	进阶	最优
	应用性能 监控或异常 检测）和人工审计 以及对关键任务配置文件变更的审查 应用。	将静态规则应用于 所有应用并执行 定期人工审计 应用配置文件 评估。	以及风险响应式 应用配置文件 评估和监控。	基于任务关键性， 风险等。
流量加密（原加密）	机构加密最少的 流量并依赖人工 或临时流程来 管理和保护 加密密钥。	机构开始加密所有 流量到内部 应用，以优先 为流量提供加密 外部应用[27]，至 正式化密钥管理 策略，并保护 服务器/服务加密 密钥。	机构确保加密 适用于所有适用的内部和 外部流量协议，[28] 管理签发和 密钥轮换和 证书，并开始 纳入最佳实践以 密码敏捷性。[29]	机构继续加密 酌情处理流量， 强制执行最小权限 安全密钥的原则 企业范围的管理，并纳入最佳 密码学实践 尽可能广泛地实现敏捷性。
网络韧性（新功能）	机构配置网络 根据具体情况逐案确定能力，仅进行匹配 单个应用 具备以下条件的可用性需求 有限的韧性 针对未被认定为关键任务的机制。	机构开始配置 网络能力以 管理可用性需求 用于其他应用 并扩展韧性 工作负载的机制 不被视为关键任务。	机构已配置 网络能力以 动态管理 可用性需求以及 韧性机制，用于 其大部分 应用。	机构整合整体 交付和意识在 适应变化在 所有系统的可用性需求 工作负载并提供 相称的韧性。
可见性与分析能力	机构采用有限的 以边界为中心的网络 监控能力，具备	机构采用网络 监控能力，基于 基于已知的以下指标	机构部署基于异常的网络检测 能力以开发	机构保持可见性 融入跨以下范围的通信 所有机构网络以及

[27]例如，当 HTTP 和 HTTPS 选项均可用时，策略和设置优先选择 HTTPS。

[28]作为零信任采用工作的一部分，机构应审查多种资源，以决定是否对网络流量进行加密和解密以供检查和可见性需求：OMB M-15-13、M-19-26、M-22-09、DHS 约束性操作指令 18-01、NIST SP 800-207 等。另见：https://www.cisa.gov/uscert/ncas/alerts/TA17-075A.

[29] DHS。密码敏捷性信息图。2022 年 5 月 12 日。https://www.dhs.gov/publication/Cryptographic-agility-Infographic.

Function	Traditional	Initial	Advanced	Optimal
	minimal analysis to start developing centralized situational awareness.	compromise (including network enumeration) to develop situational awareness in each environment and begins to correlate telemetry across traffic types and environments for analysis and threat hunting activities.	situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities.	environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources.
Automation and Orchestration Capability	Agency uses manual processes to manage the configuration and resource lifecycle for agency networks and environments with periodic integration of policy requirements and situational awareness.	Agency begins using automated methods to manage the configuration and resource lifecycle for some agency networks or environments and ensures that all resources have a defined lifetime based on policies and telemetry.	Agency uses automated change management methods (e.g., CI/CD) to manage the configuration and resource lifecycle for all agency networks and environments, responding to and enforcing policies and protections against perceived risks.	Agency networks and environments are defined using infrastructure-as-code managed by automated change management methods, including automated initiation and expiration to align with changing needs.
Governance Capability	Agency implements static network policies (access, protocols, segmentation, alerts, and remediation) with an approach focused on perimeter protections.	Agency defines and begins to implement policies tailored to individual network segments and resources while also inheriting corporate-wide rules as appropriate.	Agency incorporates automation in implementing tailored policies and facilitates the transition from perimeter-focused protections.	Agency implements enterprise-wide network policies that enable tailored, local controls; dynamic updates; and secure external connections based on application and user workflows.

功能	传统	初始	进阶	最优
	以最少的分析开始 开发集中式 态势感知。	入侵（包括 网络枚举）以 发展态势 每个环境中的意识 环境并开始 跨以下范围关联遥测数据 流量类型和 用于分析的环境 以及威胁狩猎活动。	态势感知跨 所有环境，开始 关联来自以下来源的遥测数据 多个来源进行分析， 并纳入自动化 流程以实现稳健的威胁 狩猎活动。	环境，同时实现 企业范围的态势 意识与进阶 监控能力， 自动化遥测数据 跨所有范围的关联 检测来源。
自动化与 编排能力	机构使用手动 流程来管理 配置和资源 机构生命周期 网络与环境 并定期集成 策略要求与 态势感知。	机构开始使用 自动化方法以 管理配置 以及资源生命周期 某些机构网络或 环境并确保 所有资源都具有 基于以下定义的生存期 策略与遥测数据。	机构使用自动化 变更管理 方法（例如，CI/CD）以 管理配置 以及所有资源生命周期 机构网络与 环境，响应 并执行策略与 针对感知到的威胁的防护 风险。	机构网络和 环境被定义 使用基础设施即代码 由自动化管理 变更管理 方法，包括 自动化启动与 到期以符合 不断变化的需求。
治理能力	机构实施静态 网络策略（访问、 协议、分段、 警报和修复）与 一种专注于 边界保护。	机构定义并开始 以实施策略 针对个体量身定制 网络分段和 资源的方法，同时也 继承企业范围的 的适当规则。	机构纳入 在实施中采用自动化 量身定制的策略和 促进从 以边界为中心 保护。	机构实施 企业级网络 能够实现量身定制的策略， 本地控制；动态 更新；以及安全的外部 基于 应用和用户 工作流。

5.4 Applications and Workloads

Applications and workloads include agency systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments.

Agencies should manage and secure their deployed applications and should ensure secure application delivery. Granular access controls and integrated threat protections can offer enhanced situational awareness and mitigate application-specific threats. Per OMB M-22-09, agencies should begin to explore opportunities to make their applications available over public networks to authorized users. Best practices for DevSecOps and CI/CD processes, including the use of immutable workloads, should also be adopted to the extent possible.[30,31] Agencies should explore options to shift their operations away from a focus on accreditation boundaries and updating ATOs to supporting applications as if they are externally facing and provide commensurate security.

Table 5 lists application workload functions pertaining to zero trust, as well as the considerations for *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* within the context of applications and workloads.

Table 5: Applications and Workloads

Function	Traditional	Initial	Advanced	Optimal
Application Access (Formerly Access Authorization)	Agency authorizes access to applications primarily based on local authorization and static attributes.	Agency begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance, and/or other attributes) per request with expiration.	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.	Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.
Application Threat Protections (Formerly Threat Protections)	Agency threat protections have minimal integration with application workflows, applying general purpose	Agency integrates threat protections into mission critical application workflows, applying	Agency integrates threat protections into all application workflows, protecting against some	Agency integrates advanced threat protections into all application workflows, offering real-time visibility

[30] NIST Projects: DevSecOps. https://csrc.nist.gov/Projects/devsecops#plans.

[31] NIST SP 800-204C: Implementation of DevSecOps for a Microservices-based Application with Service Mesh. March 8, 2022. https://csrc.nist.gov/publications/detail/sp/800-204c/final.

5.4 应用与工作负载

应用与工作负载包括在本地、移动设备上执行的机构系统、计算机程序和服务设备，以及在云环境中。

机构应管理和保护其已部署的应用，并应确保安全的应用交付。精细的访问控制和集成的威胁防护可以提供增强的态势感知并缓解特定于应用的威胁。根据 OMB M-22-09，机构应开始探索机会，使其应用可通过公共网络供授权用户使用。还应尽可能采用 DevSecOps 和 CI/CD 流程的最佳实践，包括使用不可变工作负载。[30,31]机构应探索选项，将其运营重点从认证边界和更新 ATO 转向将应用视为

面向外部并提供相应的安全。

表5列出了与零信任相关的应用工作负载功能，以及在应用与工作负载背景下对可见性与分析、自动化与编排和治理的考虑因素。

表5:应用与工作负载

功能	传统	初始	进阶	最优
应用访问 (原“访问”） Authorization)	机构授权访问 应用主要基于 基于本地授权和 静态属性。	机构开始实施 授权访问 应用的能力 结合上下文 信息（例如，身份、 设备合规性，和/或 其他属性)按请求设置并带过期时间。	机构自动化 应用访问决策 具有扩展的上下文 信息和强制执行的 过期条件， 遵循最小权限 原则。	机构持续 授权应用 访问，纳入实时风险分析并 行为等因素或 使用模式。
应用威胁 保护措施 (原威胁 Protections)	机构威胁防护 具有最小集成 与应用工作流， 应用通用	机构将威胁 防护融入任务 关键应用 工作流，应用	机构将威胁 防护融入所有 应用工作流， 防护部分	机构将进阶 威胁防护融入所有 应用工作流， 提供实时可见性

[30] NIST Projects: DevSecOps. https://csrc.nist.gov/Projects/devsecops#plans.

[31] NIST SP 800-204C：为基于微服务且带服务网格的应用实施 DevSecOps。2022 年 3 月 8 日。 https://csrc.nist.gov/publications/detail/sp/800-204c/final.

Function	Traditional	Initial	Advanced	Optimal
	protections for known threats.	protections against known threats and some application-specific threats.	application-specific and targeted threats.	and content-aware protections against sophisticated attacks tailored to applications.
Accessible Applications (Formerly Accessibility)	Agency makes some mission critical applications[32] available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission critical applications available over open public networks to authorized users with need via brokered connections.	Agency makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.
Secure Application Development and Deployment Workflow (New Function)	Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms.	Agency provides infrastructure for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls in support of least privilege principles.	Agency uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment.	Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.
Application Security Testing (Formerly Application Security)	Agency performs application security testing prior to deployment, primarily via manual testing methods.	Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.	Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.	Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.

[32] This does not include National Security Systems. See National Security Memorandum (NSM)-8 "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems." https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

功能	传统	初始	进阶	最优
	针对已知的防护 威胁。	针对已知的防护 威胁及部分应用 特定威胁。	特定于应用的和 针对性威胁。	以及内容感知 针对以下内容的防护 量身定制的复杂攻击 到应用程序。
可访问的应用 (原无障碍)	机构将部分任务 关键应用[32] 仅可通过私有 网络和受保护的 公共网络连接 （例如 VPN）并加以监控。	机构将其部分 适用的任务关键型 应用程序可通过 开放公共网络向 有需求的授权用户 通过代理连接。	机构将其大部分 适用的任务关键型 应用程序可通过 开放公共网络 与授权对象的连接 按需为用户提供。	机构将所有适用的 应用程序可通过 开放公共网络向 授权用户和设备， 在适当情况下，作为 按需提供。
安全应用 开发与 部署工作流 (新功能)	机构设有临时 开发、测试和 生产环境 使用非健壮代码 部署机制。	机构提供 基础设施，用于 开发、测试和 生产环境 （包括自动化）与 正式的代码部署 通过CI/CD的机制 流水线及必要的访问权限 控制措施以支持最小 权限原则。	机构使用独特且 协调团队，用于 开发、安全和 运营，同时移除 开发者访问权限 生产环境用于 代码部署。	机构利用不可变 在可行的情况下为工作负载， 仅允许对以下内容进行更改 通过以下方式生效 重新部署，并移除 管理员访问权限 部署环境在 转而采用自动化流程 用于代码部署。
应用安全 测试(原为 应用安全)	机构执行应用程序 安全测试在 部署，主要通过 手动测试方法。	机构开始使用静态 和动态（即， 应用程序正在执行） 要执行的测试方法 安全测试，包括 手动专家分析，事先 到应用部署。	机构集成 应用程序安全测试 进入应用程序 开发和 部署过程， 包括使用定期 动态测试方法。	机构集成 应用程序安全测试 贯穿整个软件 开发生命周期贯穿 企业以常规 自动化测试 已部署的应用程序。

[32]这不包括国家安全系统。见国家安全备忘录(NSM)- 8"改善国家安全的网络安全，国防部与情报界系统。" https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-改善国家安全、国防部和情报界系统的网络安全/。

Function	Traditional	Initial	Advanced	Optimal
Visibility and Analytics Capability	Agency performs some performance and security monitoring of mission critical applications with limited aggregation and analytics.	Agency begins to automate application profile (e.g., state, health, and performance) and security monitoring for improved log collection, aggregation, and analytics.	Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.	Agency performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility.
Automation and Orchestration Capability	Agency manually establishes static application hosting location and access at provisioning with limited maintenance and review.	Agency periodically modifies application configurations (including location and access) to meet relevant security and performance goals.	Agency automates application configurations to respond to operational and environmental changes.	Agency automates application configurations to continuously optimize for security and performance.
Governance Capability	Agency relies primarily on manual enforcement policies for application access, development, deployment, software asset management, security testing and evaluation (ST&E) at technology insertion, patching, and tracking software dependencies.	Agency begins to automate policy enforcement for application development (including access to development infrastructure), deployment, software asset management, ST&E at technology insertion, patching, and tracking software dependencies based upon mission needs (for example, with Software Bill of Materials).	Agency implements tiered, tailored policies enterprise-wide for applications and all aspects of the application development and deployment lifecycles and leverages automation, where possible, to support enforcement.	Agency fully automates policies governing applications development and deployment, including incorporating dynamic updates for applications through the CI/CD pipeline.

功能	传统	初始	进阶	最优
可见性与分析能力	机构执行一些性能和安全任务监控关键应用以有限聚合和分析。	机构开始自动化应用配置文件（例如，状态、健康状况和性能）和安全监控以改进日志收集、聚合和分析。	机构自动化配置文件和安全监控用于大多数应用以启发式方法以识别特定于应用的和企业范围的趋势和随时间推移改进流程以解决可见性方面的缺口。	机构执行持续和动态监控跨所有应用以维护企业级全面的可见性。
自动化与编排能力	机构手动建立静态应用托管位置和访问权限在配置，且有限的维护与审查。	机构定期修改应用配置（包括位置和访问权限）以满足相关的安全性和性能目标。	机构自动化应用配置以响应运营和环境变化。	机构自动化应用配置以持续优化以实现安全性和性能。
治理能力	机构主要依赖手动执行策略应用访问的策略，开发、部署、软件资产管理、安全测试和评估（ST&E）在技术插入、修补和跟踪软件依赖关系。	机构开始自动化策略执行以实现应用开发（包括访问开发基础设施）、部署、软件资产管理、ST&E 在技术插入、修补和跟踪基于任务需求的软件依赖关系（例如，使用软件物料清单）。	机构实施分层的、为企业量身定制的策略广泛适用于应用及所有应用程序的各个方面开发和部署生命周期和利用自动化，在尽可能，以支持执行。	机构完全自动化管理应用开发和部署，包括纳入动态应用程序更新通过 CI/CD 管道。

5.5 Data

Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.

Agency data should be protected on devices, in applications, and on networks in accordance with federal requirements. Agencies should inventory, categorize, and label data;[33] protect data at rest and in transit; and deploy mechanisms to detect and stop data exfiltration. Agencies should carefully craft and review data governance policies to ensure all data lifecycle security aspects are appropriately enforced across the enterprise.

Table 6 lists data functions pertaining to zero trust, as well as the considerations for *Visibility and Analytics, Automation and Orchestration, and Governance* within the data context.

Table 6: Data

Function	Traditional	Initial	Advanced	Optimal
Data Inventory Management	Agency manually identifies and inventories some agency data (e.g., mission critical data).	Agency begins to automate data inventory processes for both on-premises and in cloud environments, covering most agency data, and begins to incorporate protections against data loss.	Agency automates data inventory and tracking enterprise-wide, covering all applicable agency data, with data loss prevention strategies based upon static attributes and/or labels.	Agency continuously inventories all applicable agency data and employs robust data loss prevention strategies that dynamically block suspected data exfiltration.
Data Categorization (New Function)	Agency employs limited and ad hoc data categorization capabilities.	Agency begins to implement a data categorization strategy with defined labels and manual enforcement mechanisms.	Agency automates some data categorization and labeling processes in a consistent, tiered, targeted manner with simple, structured formats and regular review.	Agency automates data categorization and labeling enterprise-wide with robust techniques; granular, structured formats; and mechanisms to address all data types.

[33] NIST NCCOE: Data Classification. https://www.nccoe.nist.gov/data-classification.

5.5 数据

Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, 应用、数据库、基础设施和备份(包括本地和虚拟环境)中的所有结构化和非结构化文件与片段，以及相关的 metadata.

机构数据应按照联邦要求，在设备、应用和网络上受到保护。机构应清点、分类和标记数据；[33]保护静态和传输中的数据；并部署检测和阻止数据外泄的机制。机构应精心制定和审查数据治理政策，以确保所有数据生命周期安全方面在企业范围内得到适当执行。表6列出了与零信任相关的数据功能，以及在数据语境下对可见性与分析、自动化与编排、治理的考虑因素。

表6:数据

功能	传统	初始	进阶	最优
数据清单管理	机构手动识别并清点一些机构数据（例如，关键任务数据）。	机构开始自动化数据清点流程用于本地和云环境，覆盖大部分机构数据，并开始纳入数据丢失防护措施。	机构自动化数据清点和跟踪全企业范围，涵盖所有适用的机构数据，并具备数据丢失防护基于静态的策略属性和/或标签。	机构持续清点所有适用的机构数据并采用强大的数据丢失防护动态的策略阻止可疑数据数据外泄。
数据分类(新增) **Function)**	机构采用有限且临时数据分类能力。	机构开始实施数据分类策略具有定义的标签和手动执行机制。	机构自动化部分数据分类和标记以一致的流程分层、有针对性的方式并简单、结构化格式和定期审查。	机构自动化数据分类和标记企业范围内具有强大的技术；细粒度、结构化格式；以及用于处理所有数据类型的机制。

[33] NIST NCCOE：数据分类。https://www.nccoe.nist.gov/data-Classification.

Function	Traditional	Initial	Advanced	Optimal
Data Availability (New Function)	Agency primarily makes data available from on-premises data stores with some off-site backups.	Agency makes some data available from redundant, highly available data stores (e.g., cloud) and maintains off-site backups for on-premises data.	Agency primarily makes data available from redundant, highly available data stores and ensures access to historical data.	Agency uses dynamic methods to optimize data availability, including historical data, according to user and entity need.
Data Access	Agency governs user and entity access (e.g., permissions to read, write, copy, grant others access, etc.) to data through static access controls.	Agency begins to deploy automated data access controls that incorporate elements of least privilege across the enterprise.	Agency automates data access controls that consider various attributes such as identity, device risk, application, data category, etc., and are time limited where applicable.	Agency automates dynamic just-in-time and just-enough data access controls enterprise-wide with continuous review of permissions.
Data Encryption	Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys.[34]	Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility, and protects encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis).	Agency encrypts data in use where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.[35]
Visibility and Analytics Capability	Agency has limited visibility into data including location, access, and usage, with analysis consisting primarily of manual processes.	Agency obtains visibility based on data inventory management, categorization, encryption, and access attempts, with some	Agency maintains data visibility in a more comprehensive, enterprise-wide manner with automated analysis and correlation and	Agency has visibility across the full data lifecycle with robust analytics, including predictive analytics, that support comprehensive views of agency data and

[34] This should include efforts to consolidate key stores and reduce reliance on one-off or siloed key stores.

[35] See NIST for relevant standards and updates such as: (1) https://www.nist.gov/itl/fips-general-information, (2) https://www.nist.gov/cryptography, and (3) https://csrc.nist.gov/publications/detail/nistir/8413/final

功能	传统	初始	进阶	最优
数据可用性(新增 Function)	机构主要生成数据 可从本地获取 具有一定异地 备份。	机构生成部分数据 可从冗余、 高可用数据存储 （例如，云）并维护 本地数据的异地备份 场所数据。	机构主要生成数据 可从冗余、 高可用数据存储 并确保访问 历史数据。	机构使用动态 优化数据的方法 可用性，包括 历史数据，根据 用户和实体的需求。
数据访问	机构管理用户和 实体访问（例如， 读取、写入、 复制、授予他人访问权限、 等）通过静态方式访问数据 访问控制。	机构开始部署 自动化数据访问 包含以下内容的控制 最小权限的要素 在整个企业范围内。	机构自动化数据 访问控制，考虑 各种属性，例如 身份、设备风险、 应用、数据类别、 等，并且有时间限制 在适用的情况下。	机构自动化动态 即时和恰好足够的 数据访问控制 企业范围内，具有 持续审查 权限。
数据加密	机构加密最少的 机构对静态数据和 传输中，并依赖手动 或临时流程来 管理和保护 加密密钥。	机构对所有数据进行加密 传输中的数据进行加密，并在可行的情 静态数据（例如，任务 关键数据和存储的数据 在外部环境中） 并开始正式化密钥 管理策略和 安全的加密密钥。[34]	机构对所有数据进行加密 静态和传输中的数据在整个 企业最大限度地 尽可能开始 纳入加密 敏捷性，并保护 加密密钥（即，机密 不是硬编码的，并且是 定期轮换)。	机构对使用中的数据进行加密 在适当的情况下，执行 最小权限原则，适用于 安全的密钥管理 全企业范围，并应用 使用最新的加密 标准和加密 敏捷性达到.....的程度 possible.[35]
可见性与分析能力	机构可见性有限 深入数据，包括位置、 访问和使用情况，并具备 分析主要由.....组成 人工流程的。	机构获得可见性 基于数据清单 管理、分类、 加密和访问 尝试，并具备一些	机构维护数据 以更.....的方式实现可见性 全面的、企业级的 以广泛的方式，并具备自动化 分析和关联以及	机构在以下范围内具有可见性 覆盖完整数据生命周期，并具备 强大的分析能力，包括 预测性分析，其 支持全面的 机构数据的视图以及

[34]这应包括整合密钥存储并减少对一次性或孤立密钥存储的依赖的努力。

[35]相关标准和更新参见 NIST，例如：(1) https://www.nist.gov/itl/fips-general-information,(2) https://www.gov/cryptography,以及 (3) https://csrc.nist.gov/publications/detail/nistir/8413/final

Function	Traditional	Initial	Advanced	Optimal
		automated analysis and correlation.	begins to employ predictive analytics.	continuous security posture assessment.
Automation and Orchestration Capability	Agency implements data lifecycle and security policies (e.g., access, usage, storage, encryption, configurations, protections, backups, categorization, sanitization) through manual, and potentially ad hoc, processes.	Agency uses some automated processes to implement data lifecycle and security policies.	Agency implements data lifecycle and security policies primarily through automated methods for most agency data in a consistent, tiered, targeted manner across the enterprise.	Agency automates, to the maximum extent possible, data lifecycles and security policies for all agency data across the enterprise.
Governance Capability	Agency relies on ad hoc data governance policies (e.g., for protection, categorization, access, inventorying, storage, recovery, removal, etc.) with manual implementation.	Agency defines high-level data governance policies and relies primarily on manual, segmented implementation.	Agency begins integration of data lifecycle policy enforcement across the enterprise, enabling more unified definitions for data governance policies.	Agency data lifecycle policies are unified to the maximum extent possible and dynamically enforced across the enterprise.

功能	传统	初始	进阶	最优
		自动化分析和 关联。	开始采用预测性 分析。	持续安全态势 评估。
自动化与 编排能力	机构实施数据 生命周期与安全 策略（例如，访问、使用、 存储、加密、 配置、保护、 备份、分类、 净化）通过手动、 且可能为临时性的， 流程。	机构使用一些 自动化流程以 实施数据生命周期与 安全策略。	机构实施数据 生命周期与安全 策略主要通过 针对大多数情况的自动化方法 机构数据以一致、 分层、有针对性的方式 在整个企业范围内。	机构实现自动化，达到 尽可能最大程度， 数据生命周期与安全 适用于所有机构数据的策略 在整个企业范围内。
治理能力	机构依赖临时性数据 治理策略（例如，针对 保护、分类、 访问、清点、存储、 恢复、移除等）与 手动实施。	机构定义高层级 数据治理策略与 主要依赖手动、 分段实施。	机构开始整合 数据生命周期策略 在整个范围内执行 企业，从而实现更多 数据的统一定义 治理策略。	机构数据生命周期 策略统一至 尽可能最大程度 并动态执行 在整个企业范围内。

5.6 Cross-Cutting Capabilities

The cross-cutting capabilities *Visibility and Analytics*, *Automation and Orchestration*, and *Governance* provide opportunities to integrate advancements across each of the five pillars. As agencies mature these capabilities with respect to a given pillar, they can also mature each capability independent of the pillars. *Visibility and Analytics* supports comprehensive visibility that informs policy decisions and facilitates response activities. *Automation and Orchestration* capabilities leverage these insights to support robust and streamlined operations to handle security incidents and respond to events as they arise. *Governance* enables agencies to manage and monitor their regulatory, legal, environmental, federal, and operational requirements in support of risk-based decision making. Governance capabilities also ensure the right people, process, and technology are in place to support mission, risk, and compliance objectives.

Table 7 provides a high-level maturity evolution for each of these cross-cutting capabilities.

Table 7: Cross-Cutting Capabilities

Function	Traditional	Initial	Advanced	Optimal
Visibility and Analytics	Agency manually collects limited logs across their enterprise with low fidelity and minimal analysis.	Agency begins to automate the collection and analysis of logs and events for mission critical functions and regularly assesses processes for gaps in visibility.	Agency expands the automated collection of logs and events enterprise-wide (including virtual environments) for centralized analysis that correlates across multiple sources.	Agency maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events.
Automation and Orchestration	Agency relies on static and manual processes to orchestrate operations and response activities with limited automation.	Agency begins automating orchestration and response activities in support of critical mission functions.	Agency automates orchestration and response activities enterprise-wide, leveraging contextual information from multiple sources to inform decisions.	Agency orchestration and response activities dynamically respond to enterprise-wide changing requirements and environmental changes.
Governance	Agency implements policies in an ad hoc manner across the enterprise, with policies enforced via manual processes or static technical mechanisms.	Agency defines and begins implementing policies for enterprise-wide enforcement with minimal automation and manual updates.	Agency implements tiered, tailored policies enterprise-wide and leverages automation where possible to support enforcement. Access policy decisions incorporate	Agency implements and fully automates enterprise-wide policies that enable tailored local controls with continuous enforcement and dynamic updates.

5.6 横向能力

横向能力可见性与分析、自动化与编排和治理提供了在五大支柱中分别整合进展的机会。随着机构在特定支柱方面使这些能力趋于成熟，它们也可以独立于支柱使每项能力趋于成熟。可见性与分析支持全面的可见性，为政策决策提供信息并促进响应活动。自动化与编排能力利用这些洞察来支持稳健且精简的运营，以处理安全事件并在事件出现时作出响应。治理使机构能够管理和监控其监管、法律、环境、联邦和运营要求，以支持基于风险的决策。治理能力还确保适当的人员、流程和技术到位，以支持任务、风险和合规目标。

表 7 提供了这些横向能力各自的高层成熟度演进。

表7:横向能力

功能	传统	初始	进阶	最优
可见性与分析	机构在其企业范围内手动收集有限的日志，保真度低且分析极少。	机构开始针对关键任务功能自动化收集和分析日志与事件，并定期评估流程中的差距 可见性。	机构扩大企业范围(包括虚拟环境)内日志和事件的自动化收集，以进行跨 多个来源。	机构通过集中式动态监控以及对日志和事件的高级分析，维持企业级的全面可见性。
自动化与编排	机构依赖静态和手动流程来 以有限的自动化编排操作和响应活动。	机构开始自动化编排与响应活动，以支持关键任务功能。	机构在企业范围内自动化编排和响应活动，利用来自多个来源的上下文信息为决策提供依据。	机构的编排与响应活动能够动态响应企业级不断变化的需求和环境变化。
治理	机构以临时方式在整个企业实施策略，策略通过手动流程或静态技术 机制。	机构制定并开始实施企业级强制执行策略，自动化程度最低且需手动更新。	机构在整个企业实施分层、量身定制的策略，并在可能的情况下利用自动化来支持执行。访问 政策决策纳入	机构实施并全面自动化企业级策略，实现定制化本地控制，并具备持续强制执行和动态 更新。

Function	Traditional	Initial	Advanced	Optimal
			contextual information from multiple sources.	

功能	传统	初始	进阶	最优
			来自多个来源的上下文信息。	

6. References

CISA consulted the following Federal Government ZTA publications while developing and revising this guidance.

Office of Management and Budget M-22-09
This memorandum sets forth a Federal zero trust architecture strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defense against increasingly sophisticated and persistent threat campaigns. The strategy includes components that place significant emphasis on strong enterprise identity and access controls (including MFA), require encrypting all network traffic as soon as practicable, support building a foundation to automate security access rules, and treat every application as internet accessible.

National Institute of Standards and Technology Special Publication 800-207
NIST's SP 800-207 describes zero trust for enterprise security architects to aid understanding of zero trust for civilian unclassified systems and provides a road map to migrate and deploy zero trust security concepts to an enterprise environment. SP 800-207 is the product of a collaboration between multiple federal agencies and is overseen by the Federal Chief Information Officer (CIO) Council. NIST is developing and releasing additional ZTA implementation guidance.[36]

Department of Defense Zero Trust Reference Architecture
The Department of Defense (DoD)'s Zero Trust Reference Architecture describes data-centric enterprise standards and capabilities that can be used to successfully advance the DoD Information Network (DoDIN) into an interoperable zero trust end state. [37]

National Security Agency Embracing Zero Trust Security Model
The NSA's Embracing Zero Trust Security Model explains the benefits and implementation challenges of a zero trust security model. [38] It discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to the zero trust model to achieve the desired results. The document's recommendations will assist cybersecurity leaders, enterprise network owners, and administrators considering embracing this modern cybersecurity model.

7. CISA Resources

CISA programs provide cybersecurity support and guidance across the zero trust pillar areas, including the integration of the pillars into a ZTA. The following documents are useful resources for agencies migrating to zero trust. CISA will continue to review and refine these resources as agencies develop ZTAs and will add additional resources to the collection over time.

Continuous Diagnostics and Mitigation
CDM guidance can be found on the CDM homepage.

High Value Assets

[36] NIST. "Implementing a Zero Trust Architecture Project". https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture.

[37] DoD. "Zero Trust Reference Architecture". Version 2.0. July 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

[38] NSA. "Embracing a Zero Trust Security Model". Version 1.0. February 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

6. 参考文献

CISA 在制定和修订本指南时咨询了以下联邦政府 ZTA 出版物。

管理和预算办公室 M-22-09
本备忘录提出了一项联邦零信任架构战略，要求各机构在2024财年(FY)结束前达到特定的网络安全标准和目标，以加强政府对日益复杂和持续威胁活动的防御。该战略包含的组成部分高度重视强大的企业身份与访问控制(包括MFA)，要求尽早在可行情况下加密所有网络流量，支持构建自动化安全访问规则的基础，并将每个应用视为可通过互联网访问。

美国国家标准与技术研究院特别出版物 800-207
NIST的SP 800-207描述了面向企业安全架构师的零信任，以帮助理解民用非机密系统的零信任，并提供了将零信任安全概念迁移和部署到企业环境的路线图。SP 800-207是多个联邦机构合作的成果，由联邦首席信息官(CIO)委员会监督。NIST正在制定和发布更多的ZTA实施指南。[36]

国防部零信任参考架构
国防部(DoD)的零信任参考架构描述了以数据为中心的企业标准和能力，可用于成功推动国防部信息网络(DoDIN)进入可互操作的零信任最终状态。[37]

国家安全局采用零信任安全模型
NSA 的《拥抱零信任安全模型》阐述了零信任安全模型的优势与实施挑战。[38]该文件讨论了制定详细策略、投入必要资源、逐步成熟实施以及完全致力于零信任模型以实现预期成果的重要性。该文件的建议将帮助正在考虑采用这一现代网络安全模型的安全负责人、企业网络所有者和管理员。

7. CISA 资源

CISA 项目在零信任支柱领域提供网络安全支持和指导，包括将各支柱集成到 ZTA 中。以下文件是机构迁移到零信任的有用资源。随着机构开发 ZTA,CISA 将继续审查和完善这些资源，并随时间向集合中添加更多资源。

持续诊断与缓解
可在CDM 主页上找到 CDM 指南。

高价值资产

[36] NIST。"实施零信任架构项目"。https://www.nccoe.nist.gov/projects/Implementing-zero-信任架构.

[37] https://dodcio.defense.gov/Portals/0/Documents/Library/(U) ZT_RA_v2.0(U) _Sep22.pdf.

[38] NSA。"拥抱零信任安全模型"。版本 1.0。2021 年 2 月。https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

HVA guidance can be found on the HVA PMO | CISA homepage.

- High Value Asset Control Overlay, Version 2.0, January 2021
- High Value Asset Control Overlay FAQ, Version 1.0, January 2018
- Securing High Value Assets, July 2018
- CISA Insights: Securing High Value Assets, September 2019
- Binding Operational Directive 18-02—Securing High Value Assets, May 2018

National Cybersecurity Protection System

NCPS guidance can be found on the NCPS Guidance Repository page.

- National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture Volume 1: General Guidance, Version 1.4, May 2021
- National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture Volume 2: Reporting Pattern Catalog DRAFT, Version 1.1, May 2021

Cybersecurity Shared Service Offering (formerly Quality Service Management Office)

- Quality Services Management Office Fact Sheet
- Centralized Mission Support Capabilities for the Federal Government (M-19-16), April 2019

Trusted Internet Connections

TIC guidance can be found on the TIC Guidance Repository page.

- Trusted Internet Connections 3.0 Program Guidebook, Version 1.1, July 2021
- Trusted Internet Connections 3.0 Reference Architecture, Version 1.1, July 2021
- Trusted Internet Connections 3.0 Security Capabilities Catalog, Version 2.0, October 2021
- Trusted Internet Connections 3.0 Traditional TIC Use Case, Version 1.0, April 2021
- Trusted Internet Connections 3.0 Branch Office Use Case, Version 1.0, April 2021
- Trusted Internet Connections 3.0 Remote User Use Case, Version 1.0, October 2021
- Trusted Internet Connections 3.0 Cloud Use Case, DRAFT, June 2022

Other CISA Resources

- Cloud Security Technical Reference Architecture
- Applying Zero Trust Principles to Enterprise Mobility
- Secure Cloud Business Applications (SCuBA) Technical Reference Architecture (TRA) (Draft)
- Extensible Visibility Reference Framework (eVRF) Guidebook (Draft)
- Multifactor Authentication
- Applying Zero Trust Principles to Enterprise Mobility
- Cyber Resilience Review Assessments
- govCAR Factsheet
- Cybersummit 2021 Session Day 2: Zero Trust

可在HVA PMO | CISA 主页上找到 HVA 指南。

- 高价值资产控制叠加层，版本 2.0,2021 年 1 月
- 高价值资产控制覆盖常见问题解答，版本 1.0,2018 年 1 月
- 保护高价值资产，2018年7月
  洞察：保护高价值资产， 年 月
- 约束性操作指令 18-02--保护高价值资产，2018年5月

国家网络安全保护系统

可在NCPS 指南库页面找到 NCPS 指南。

- 国家网络安全保护系统(NCPS)云接口参考架构第1卷：通用指南，版本1.4,2021年5月
- 国家网络安全保护系统(NCPS)云接口参考架构第2卷：报告模式目录草案，版本1.1,2021年5月

网络安全共享服务产品(原质量服务管理办公室)

- 质量服务管理办公室情况说明书
- 联邦政府集中式任务支持能力(M-19-16),2019年4月

可信互联网连接

TIC 指南可在TIC 指南存储库页面上找到。

- 可信互联网连接 3.0 计划指南，版本 1.1,2021 年 7 月
- 可信互联网连接3.0参考架构，版本1.1,2021年7月
- 可信互联网连接3.0安全能力目录，版本2.0,2021年10月
- 可信互联网连接3.0传统TIC用例，版本1.0,2021年4月
- 可信互联网连接3.0分支机构用例，版本1.0,2021年4月
- 可信互联网连接3.0远程用户用例，版本1.0,2021年10月
- 可信互联网连接 3.0 云用例，草案，2022 年 6 月

其他 CISA 资源

- 云安全技术参考架构
- 将零信任原则应用于企业移动性
- 安全云业务应用(SCuBA)技术参考架构(TRA)(草案)
- 可扩展可见性参考框架(eVRF)指南(草案)
- 多因素认证
- 将零信任原则应用于企业移动性
- 网络韧性审查评估
- govCAR 情况说明书
- 网络安全峰会 2021 会议第二天：零信任

How this file was made

This is a complete Chinese translation of the CISA Zero Trust Maturity Model, Version 2.0. Tables, captions, headers, footers and numbering all keep their original positions. Nothing has been cut.

If you have documents of your own

- Contracts, tenders, standards, patents, reports: original layout kept, CNY 0.15/page
- PDF to Word: free up to 100 pages, CNY 0.10/page beyond that
- Scanned or image-only PDFs: OCR to Word, free
- No sign-up, no login: upload and download

Open the address below and try it with your own file:

https://www.ivyivy.com.cn/cisa-zero-trust-maturity-model-zh

On-premise deployment available (subject to model and compliance review)

Machine translation, provided for reading reference only. For professional judgement and compliance citation, please refer to the original English source.

This page is a translator's note; it is not part of the original document.

这份文件是怎么做出来的

本译本是《零信任成熟度模型 2.0》的中文全译本，共 32 页。表格、图注、页眉页脚、编号层级都按原文位置一一还原，未做任何删节。

你手上如果也有英文文件要处理

- 合同、标书、标准、专利、报告：翻译后保留原版式，0.15 元/页
- PDF 转 Word：100 页内免费，超出 0.1 元/页
- 扫描件、图片版 PDF：先 OCR 再转 Word，免费
- 不用注册、不用登录，传上去直接下载

打开下面这个地址，把你自己的文件传上去试试：

https://www.ivyivy.com.cn/cisa-zero-trust-maturity-model-zh

支持私有化部署（需按贵方模型与合规要求评估）

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。