网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

谙海横流

执行体全量识别与精细管控

从零信任技术演进
看网络安全创新的规律特点

安天 | 安天研究院

零信任与网络安全创新演进

- 网络安全的发展和创新演进十分复杂，涉及多种能力升级换代方式、多类主体以及多种复杂关系。零信任技术自诞生之日起就备受关注，其创新性安全防护理念成为网络安全技术发展的主流方向。零信任的演进和发展为分析网络安全的创新规律提供了很好的研究样板。

什么是零信任？发展历程？

零信任的产生原因和创新特点是什么？

零信任的演进历程对我们有什么启示？

由安天研究院徐菲、肖新光等主笔的
《从零信任技术演进看网络安全创新的规律特点》

目 录

01 零信任的发展和演进过程

探索与初步实践阶段

理念探索阶段

学术、产业界研究和初步实践阶段

2004 年以“寻求网络**去边界化**趋势下的全新安全架构及解决方案”为目的而成立的耶利哥论坛最早体现零信任理念。

2010 年，咨询机构 Forrester 首席分析师 John Kindervag 首次提出“零信任”这一术语，认为**零信任本质是以身份为基石的动态访问控制**，即以身份为基础，通过动态访问控制技术，以细粒度的应用、接口、数据为核心保护对象，遵循最小权限原则，构筑端到端的安全边界。

2011-2017 年，**Google BeyondCorp** 实践落地，发表系列论文，验证了零信任安全在大型网络场景下的可行性。

2013年，国际云安全联盟在零信任理念的基础上提出了**软件定义边界SDP**，并发布了SDP标准规范1.0，进一步推动零信任从概念走向落地。

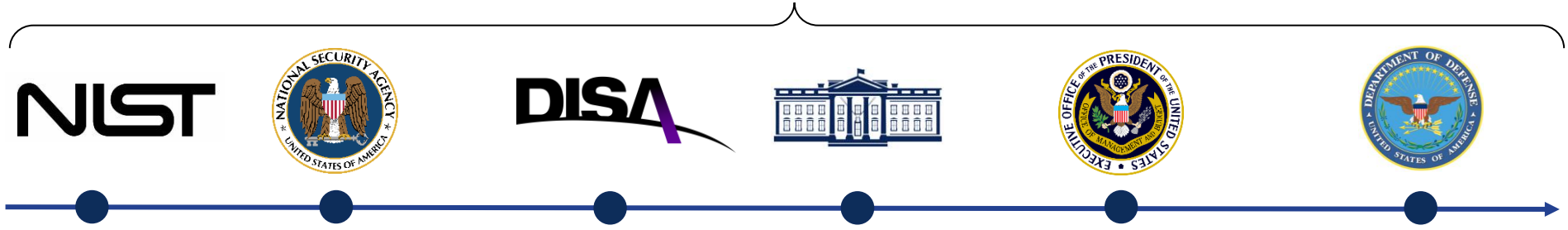
2017年，Gartner提出持续自适应风险与信任评估CARTA的概念，零信任是实现CARTA的基本步骤。随后，分析师 Riley 将CARTA的概念改编成了**零信任网络访问（ZTNA），**ZTNA包括持续自适应风险和信任评估，在不影响可用性的情况下提供最大的安全性。

2018 年起，Forrester 发布年度**零信任扩展生态系统 ZTX** 研究报告，探索零信任架构在企业中的应用，系统性对零信任厂商的能力进行评估。

2019年，Gartner 的市场报告中，采用了**零信任网络访问（ZTNA）**作为主题。

美国政府整体将零信任作为国家战略推动阶段

美国政府整体将零信任作为国家战略推动阶段



2019-2020 年，美国国家标准与技术研究院（NIST）在5个月内连续发布两版《零信任架构》标准草案，零信任正向标准化进展。

2021年2月，美国国家安全局（NSA）发布指南《拥抱零信任安全模型》，强烈建议国家安全系统（NSS）内的所有关键网络、国防部（DoD）的关键网络、国防工业基础（DIB）关键网络和系统考虑零信任安全模型。

2021年5月，美国防信息系统局（DISA）在其官网公开发布《国防部零信任参考架构》，旨在为国防部增强网络安全并在数字战场上保持信息优势。

2021年6月，美国总统拜登发布行政命令，要求政府的计算机系统实行零信任。

2021年9月，美国管理和预算办公室（OMB）发布了《联邦政府零信任战略》草案，2022年1月《联邦政府零信任战略》正式版发布。该战略没有描述或规定一个成熟的零信任实现，但给出了零信任战略的五大支柱和三大基石，并给出了五大支柱目标的分解行动。

2022年11月22日，美国防部正式发布《零信任战略》，计划在2027财年之前实施战略和相关路线图中概述的独特的零信任能力和活动。战略概述了四个高层次的综合战略目标，并围绕7个支柱设定了45项需具备的网络安全能力。

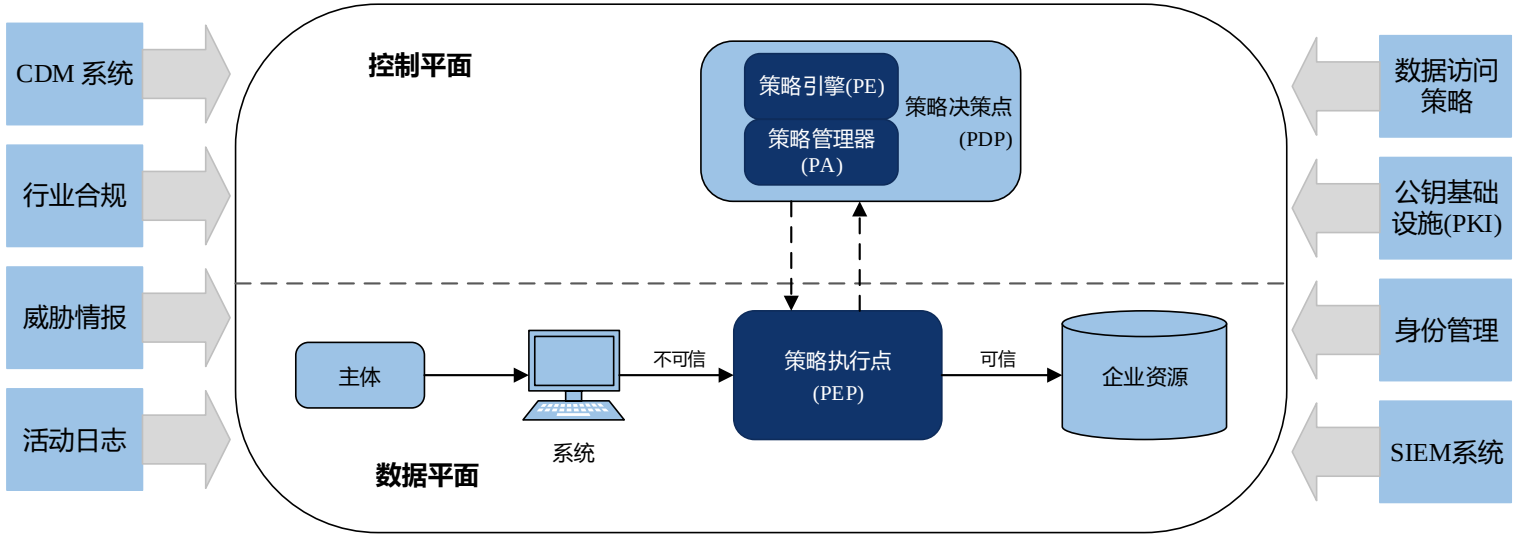
NIST《零信任架构》标准

美国国家标准与技术研究院（NIST）

2019-2020年，NIST在5个月内连续发布两版《零信任架构》标准草案，对零信任安全原则、架构模型、应用场景做了详细的描述。零信任架构（ZTA）是一种企业网络安全规划、部署和运营信息技术架构所依据的一系列原则，通过全局视角来衡量给定任务或业务流程中所有的潜在风险，以及考虑如何减轻这些风险。

零信任原则：

- 所有数据源和计算服务都被视为资源；
- 所有网络通信都应安全保障，与网络位置无关；
- 基于每个会话授予对单个企业资源的访问权限；
- 对资源的访问由动态策略决定；
- 企业监控和检测所有自有资产和相关资产的完整性和安全态势；
- 所有的资源认证和授权都是动态的，并在允许访问之前严格执行；
- 企业尽可能收集有关资产、网络基础设施和通信的当前状态信息，并利用这些信息改善其安全状况。

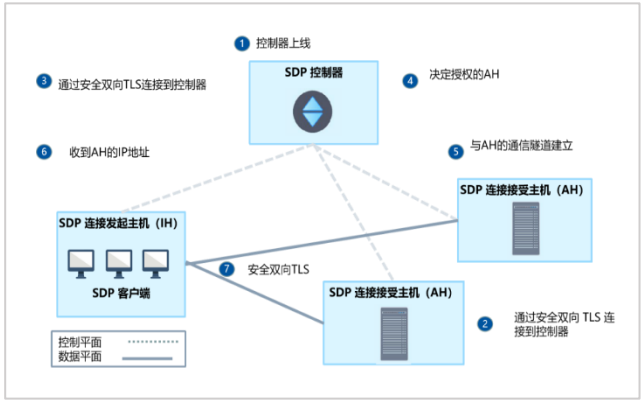


NIST 零信任架构

NIST《零信任架构》标准

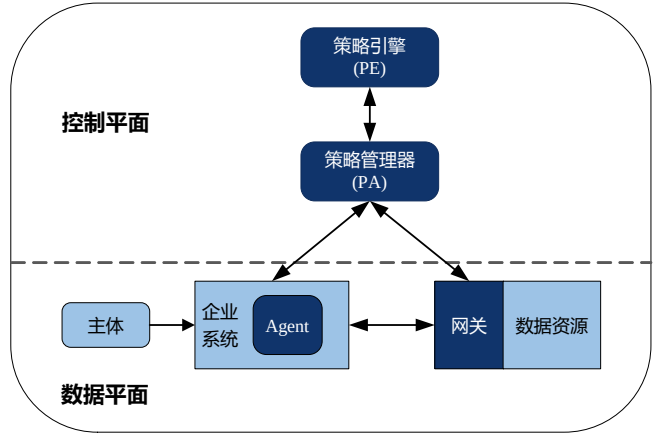
根据 NIST《零信任架构》中的定义：零信任提供了一系列概念和思想，假定网络环境已经被攻陷，在执行信息系统和服务中的每次访问请求时，降低其决策准确度的不确定性。

在NIST标准中明确提到零信任的**三种核心技术包括：软件定义边界（ SDP ），身份与访问管理（ IAM ）和微隔离（MSG）**。这三个技术实际上是对过去的VPN技术，4A技术和防火墙技术在新的应用场景中的发展和应用升级。



国际云安全联盟（CSA）SDP技术架构

身份与访问管理



NIST基于MSG技术实现的零信任架构

美国管理和预算办公室《联邦政府零信任战略》

以OMB为代表的美国联邦政府

2022年1月，美国管理和预算办公室（OMB）发布了《联邦政府零信任战略》正式版。该战略从身份、设备、网络、应用、数据等五个方面提出了具体行动计划和要求。从网络方面的战略愿景与行动计划来看，身份认证、访问控制和流量传输加密是这些行动的重点，而所提出的目标动作要求没有超出现有网络安全技术能力供给频谱。

愿景

各联邦机构对其网络环境中的所有 DNS 请求和 HTTP 流量进行加密，并开始执行实施计划，将其边界分解为孤立的环境。

- 只要技术条件允许，联邦政府机构都必须使用**加密DNS**解析DNS查询。网络安全和基础设施安全局的保护DNS计划支持加密DNS请求；
- 联邦政府机构都必须对其网络环境中的所有Web网站和API调用流量强制实施**HTTPS加密**。必须与网络安全和基础设施安全局合作，将其.gov域名“预加载”到浏览器中实现浏览器只能通过HTTPS访问联邦政府网站；
- 网络安全和基础设施安全局将与联邦风险和授权管理计划项目管理办公室合作，评估联邦政府范围内可行的**电子邮件加密**解决方案，并向管理和预算办公室提出建议；
- 联邦机构必须与网络安全和基础设施安全局协商，制定一个零信任架构计划，说明如何实施**网络环境的隔离**，并将其作为零信任实施计划的一部分提交给管理和预算办公室。

网络方面战略愿景与行动计划

美国国防部《零信任战略》

美国国防部（DoD）

2022年11月22日，美国防部正式发布《零信任战略》，计划在2027财年之前实施战略和相关路线图中概述的独特的零信任能力和活动。该战略概述了四个高层次的综合战略目标，这些目标定义了为实现其零信任愿景将采取的行动，并围绕7个支柱设定了45项需具备的网络安全能力。不难看到，这45项大都是现有的网络安全技术能力。

美国防部零信任战略能力要求

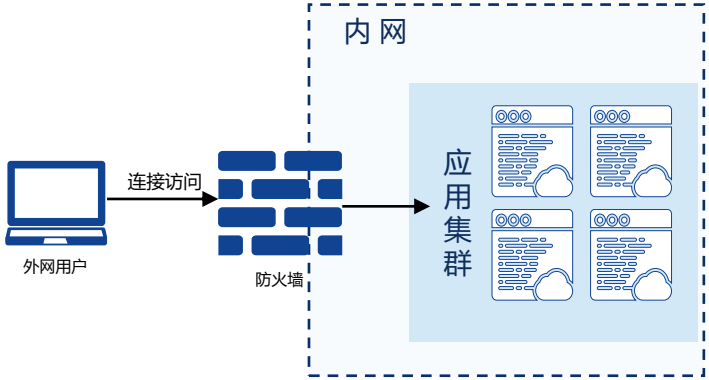
小结

- 零信任的发展，是从一个相对模糊而理想化的安全目标和设想，到提出具体支撑技术和实施方案，进而演化为整体安全解决方案，包括实施体系架构、策略和持续的安全流程的过程。

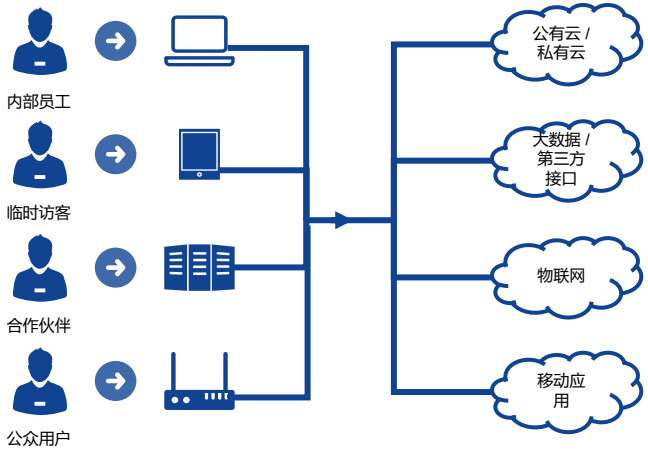
- **实现零信任需要端到端的体系化安全能力支撑，零信任的部署需要复杂的产品体系的相互联动配合。**零信任的实施是对传统的安全技术、产品提出了更高的要求，而不是一种颠覆性的安全技术替代了传统的技术。

02 零信任产生的原因和创新价值

传统网络边界的消失对安全提出了新挑战



传统安全防护体系



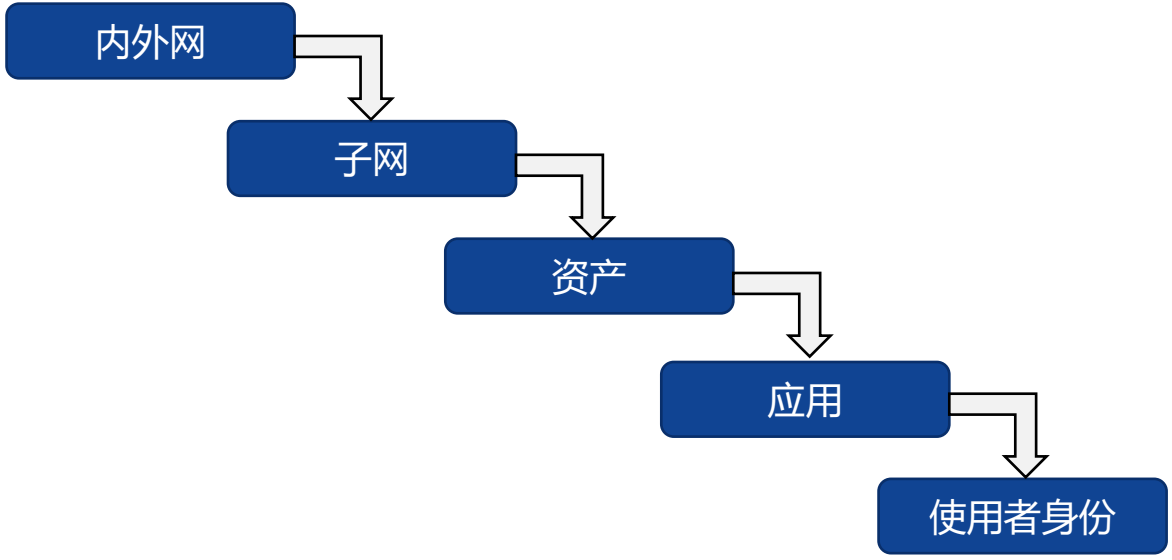
数字化时代，传统安全边界“消失”

网络边界模糊　**外部攻击频繁**　**内部威胁加剧**　**访问需求复杂**

数字化时代网络空间面临的安全挑战

零信任是在传统IT边界消亡时对安全边界的重塑

人员和资产位置是在体系之外，逻辑权限却在体系之内，使得整个安全边界无法基于统一的安全网关来约束，必须跟随着资产的弹性范围动态延展。因此，**安全边界并非消失，而是需要最小化**。安全边界的概念也不再是一个绝对的网络通讯边界的概念，而是转变成为**行为边界**的概念。



安全边界细粒度管控

零信任的核心诉求和本质是细粒度到每一个执行体、操作、身份都有自己的安全边界。

零信任是对原有安全能力体系的重新整合

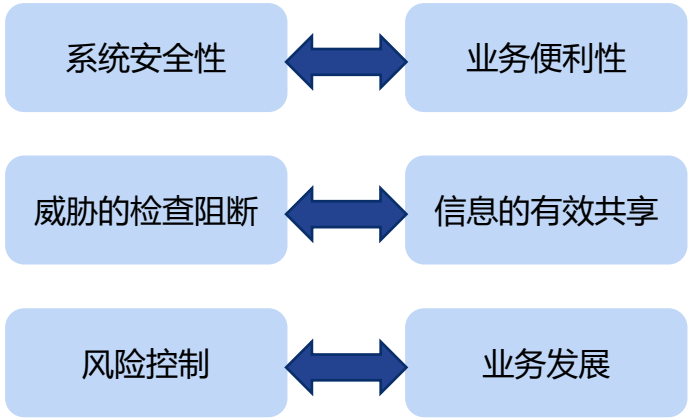
零信任本质上是一种细粒度、动态的可信方法，以安全的基础和层次，如资产与系统、应用与执行体、网络与拓扑、身份与认证、数据与业务进行安全整合。基于对漏洞和攻击的关注，按照识别、塑造、防护、检测、响应形成安全能力集合，不断地夯实**基础能力**。

安天ISPDR防御技术框架

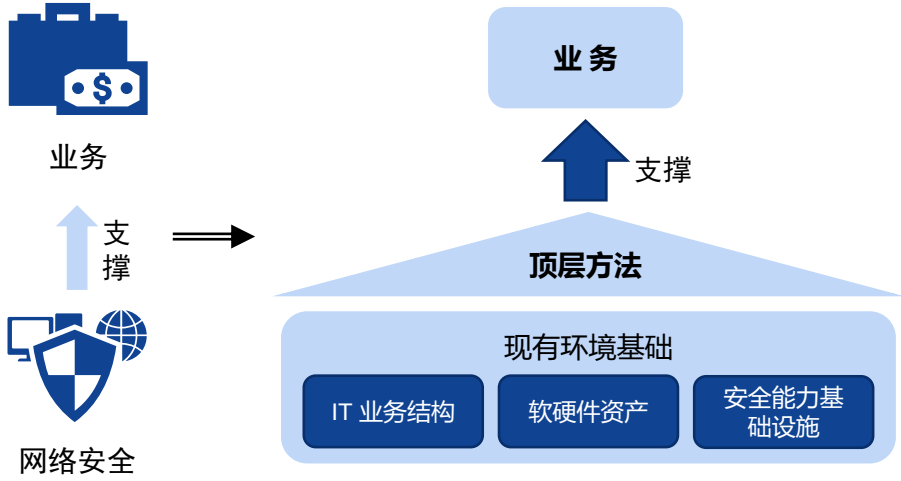
零信任对传统的安全能力体系提出了更高的要求，是对原有安全能力体系的重新整合。

零信任创新特点：以支撑业务为第一性原则

零信任理念承认安全和业务间矛盾性，但更加**强调目标的统一性**，以更有效地**保障业务的连续性、效率、共享为前提，来构建安全**。零信任改变了原有的安全能力演进以安全为第一性诉求，兼顾业务系统的稳定性和持续性的局面，通过安全与业务的深层次融合，充分保障信息的访问共享连接、消除信息孤岛和达成更高效的运行。



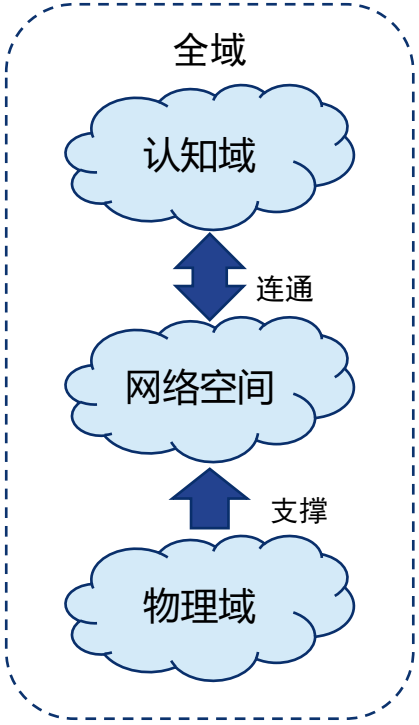
安全和业务的矛盾性



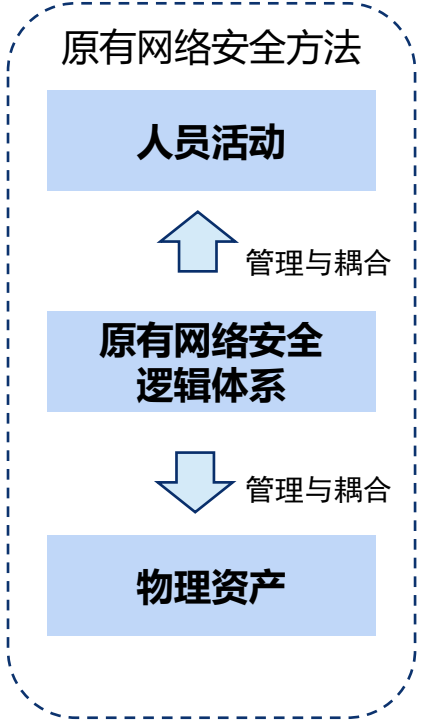
零信任理念充分兼顾业务和安全一致性

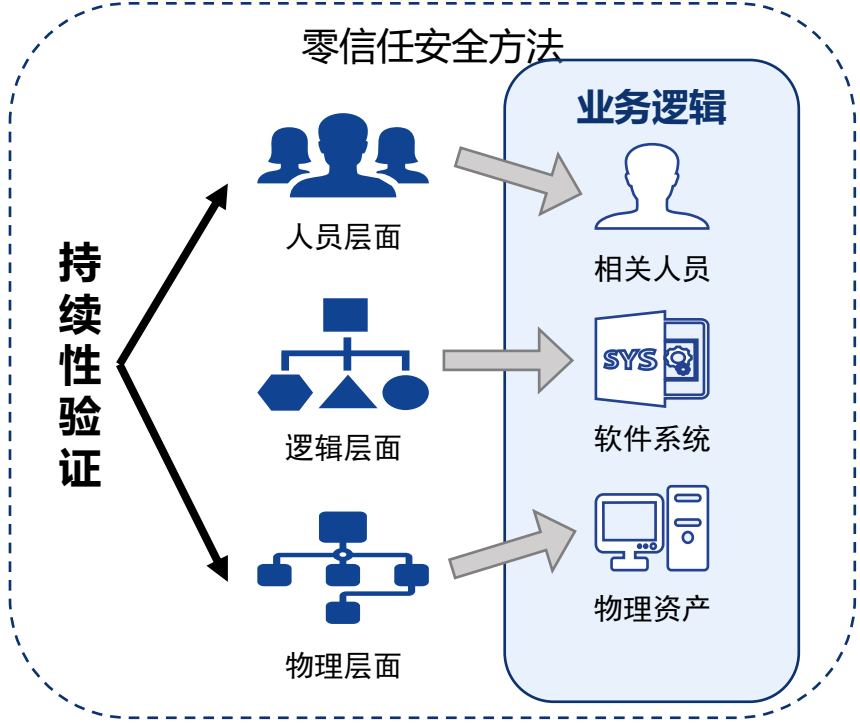
零信任创新特点：保障范围更加全域化

零信任把持续性验证方法系统地覆盖物理资产和相关人员，深层次的嵌入到了由物理资产所支撑、由软件系统所承载、基于人机共同形成的业务逻辑。



网络空间与物理域、认知域的关系

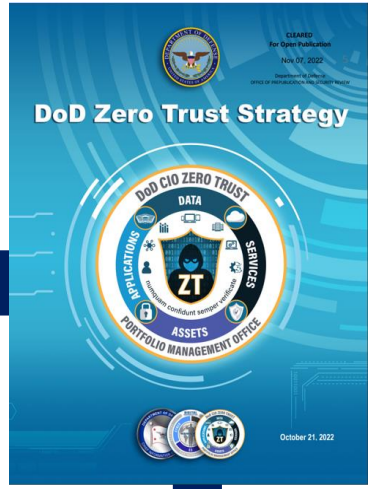




相比于原有的网络安全方法，零信任保障范围更加全域化

零信任创新特点：能力和文化的融合

零信任是构建于“网络的发展趋势是更加开放、共享”这一认知基础上的。过去几年重大的网络安全与信息化的复合型创新，例如安全左移、SecDevOps等，都不止是技术与能力层面的组织和融合方法，而带有鲜明的技术、能力、流程与文化融合的特点。**零信任本质上所要达成的不止是一种能力升级，同时也是理念和心智的升级，是文化的升级。**



文化，不仅仅是科技

DoD如何保护和保障美国国防部信息设备，不能仅靠技术解决；它需要改变思维方式和文化，从国防部的领导到任务操作员，跨越所有的国防部信息设备用户。

对安全需要重新思考

实施零信任需要重新思考如何利用现有基础设施，以更简单、更高效的方式通过设计实现安全性，同时提高作战人员性能，提高互操作性，并实现畅通无阻的行动和恢复能力。”

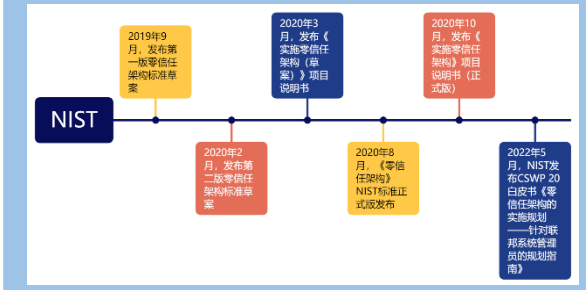
信息革命本质上不能够以一种身体行走在21世纪，而头脑停留在20世纪的方式来推动。

03

从美国官方机构参与推动零信任的过程分析政府在网络安全战略创新的作用

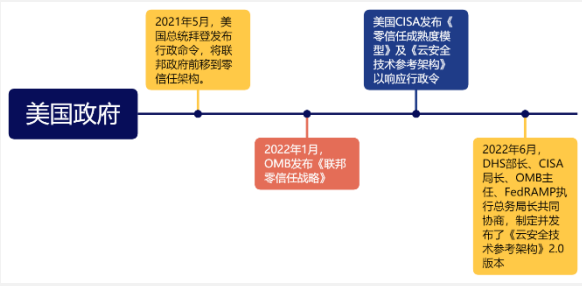
NIST、OMB和DOD等机构参与推动零信任的过程

美国国家标准与技术研究院 (NIST)



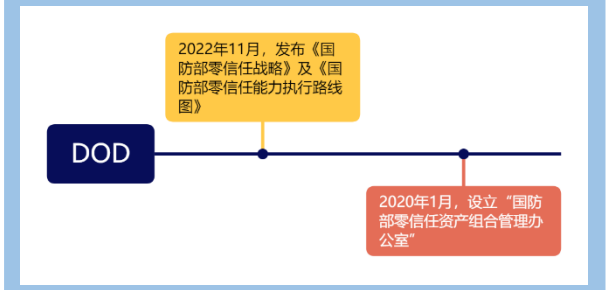
- 《零信任架构》中提出，**零信任模式**并不是单一的网络架构或技术产品，**而是一套理念、战略、架构**。
- 《实施零信任架构》**瞄准零信任架构的落地实践**，旨在使用商用产品，在通用企业IT基础设施中实施零信任架构。
- CSWP 20白皮书**解读了零信任基本原则**，比较了RMF框架与零信任实施过程。给出了**管理员在每个RMF环节中要重点关注和完成的事项**。

美国管理和预算办公室 (OMB)



- 行政命令启动政府范围内全面努力，实现基于云的基础设施安全优势，并降低相关风险。
- 《联邦零信任战略》，目标是**加速政府机构尽快向零信任成熟度的安全基线迈进**。
- 《云安全技术参考架构》2.0版本，明确了**通过云安全态势管理从而促进零信任架构**来实现行政命令目标。提出云迁移需要文化改变、确定优先顺序和设计新的方法，这些都必须得到所有机构支持才能取得成功。
- 这些文件也组成了联邦各级机构的零信任安全架构路线。

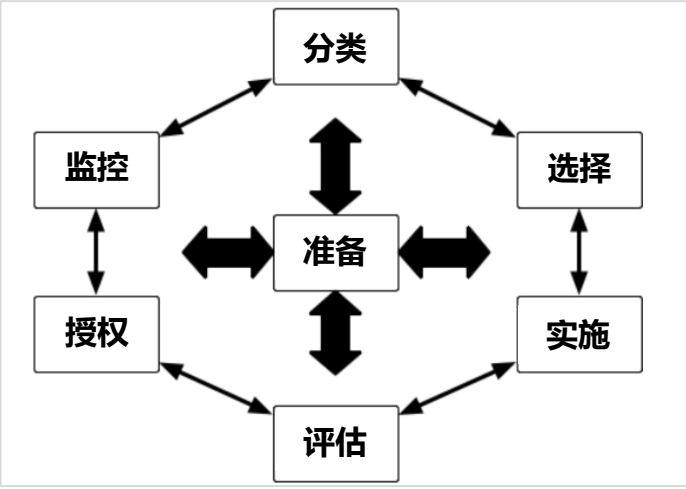
美国国防部 (DoD)



- 计划**在2027财年前在DoD范围全面实施零信任网络安全框架**。
- 《零信任战略》**为DoD推进零信任理念落地提供必要的指导**，涵盖了差距分析、需求开发、实施和决策制定等内容，并阐述了如何通过采购和部署/开展必要的零信任能力和活动，使网络安全水平得到有价值的改善。
- 设立办公室协调零信任战略所述的各项工作和**加快零信任理念落地，实现DoD在零信任方面的总体目标**。

NIST《实施零信任架构》瞄准零信任架构落地实践

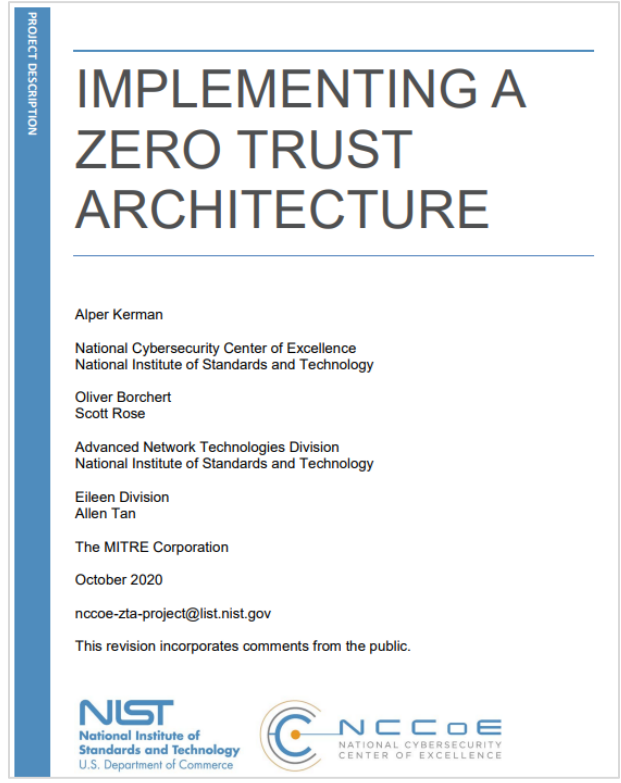
2020年3月NIST的国家网络安全卓越中心（NCCoE）发布《实施零信任架构（草案）》项目说明书，10月发布《实施零信任架构》项目说明书（正式版），瞄准零信任架构的落地实践，旨在使用商用产品，建立与NIST《零信任架构》标准中的概念和原则相一致的零信任架构的实现示例。



NIST 风险管理框架（RMF）步骤

NIST零信任迁移过程

- 组织和制度准备（**准备**步骤）
- 系统分类（**分类**步骤）
- 控制选择（**选择**步骤）
- 控制实施（**实施**步骤）
- 控制评估（**评估**步骤）
- 系统授权（**授权**步骤）
- 控制监控（**监控**步骤）


PROJECT DESCRIPTION

IMPLEMENTING A ZERO TRUST ARCHITECTURE

Alper Kerman

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Oliver Borchert
Scott Rose

Advanced Network Technologies Division
National Institute of Standards and Technology

Eileen Division
Allen Tan

The MITRE Corporation

October 2020

nccoe-zta-project@list.nist.gov

This revision incorporates comments from the public.

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

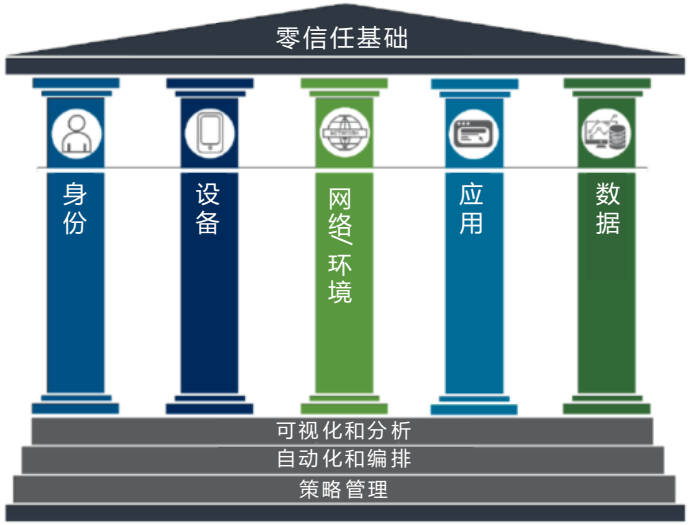
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NCCoE《实施零信任架构》

2022年5月，NIST发布CSWP 20 白皮书《零信任架构的实施规划——针对联邦系统管理员的规划指南》，解读了NIST《零信任架构》的零信任基本原则，给出了联邦信息系统在实施零信任迁移改造时，管理员在每个RMF环节中要重点关注和完成的事项。

美国OMB基于政府引导视角提出目标导向和行动计划

美国《联邦零信任战略》提出了零信任安全五大目标和行动计划，明确具体落实要求，旨在加快将美政府机构的企业安全架构迁移到零信任架构。该战略就推动实施零信任架构明确了重点任务的落实期限，要求对零信任落实更深入的机构与那些仍在起步阶段的机构合作，共同致力于彻底改革机构的安全架构和运作，通过构建运营模型来部署并维持零信任能力。



美国《联邦零信任战略》五大支柱

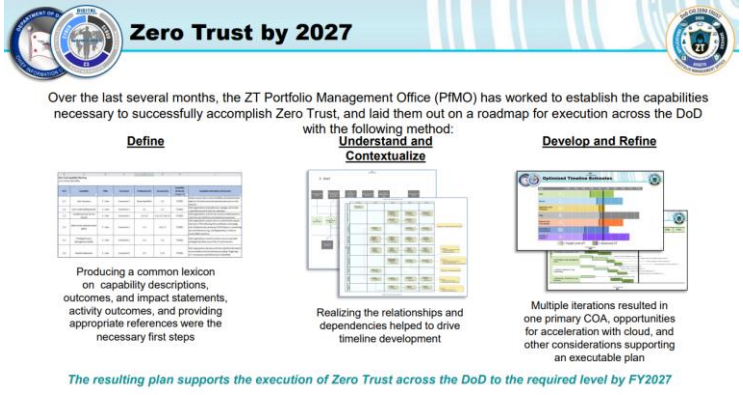
为加快落实联邦零信任战略的支柱领域目标要求，备忘录专门列出了各机构需纳入各自实施计划并在规定期限内优先完成的重点任务。

美国《联邦零信任战略》重点任务规划

类目	任务	期限
常规	各机构必须向OMB和CISA提交22- 24财年的实施计划供OMB批准，并提交23- 24财年的预算估计	自本备忘录发布之日起60天内
身份	各机构必须为机构用户采用能够集成到应用程序和通用平台中的集中身份管理系统	纳入机构实施计划
	各机构必须要求其用户使用防网络钓鱼的方法访问机构托管的账户	纳入机构实施计划
	支持MFA的面向公众的机构系统必须为用户提供使用防钓鱼认证的选项	自本备忘录发布之日起一年内
	各机构必须从所有系统中删除要求特殊字符和定期密码轮换的密码策略	自本备忘录发布之日起一年内
	机构授权系统应将至少一个设备级信号与认证用户的身份信息结合起来	纳入机构实施计划
设备	各机构必须建立持续、可靠和完整的资产清单，包括利用CDM项目	纳入机构实施计划
	各机构必须确保其EDR工具符合CISA的技术要求，并在整个机构内部署和运行	见备忘录M-22-01
	各机构必须与CISA合作，找出差距，协调部署，并与CISA建立信息共享能力	见备忘录M-22-01
网络	在技术支持的任何地方，各机构都必须使用加密DNS解决DNS查询	纳入机构实施计划
	各机构必须对所有HTTP流量强制执行经认证的HTTPS，包括不跨公共互联网的流量	纳入机构实施计划
	各机构必须与CISA的DotGov计划合作，将机构拥有的.gov域名在网络浏览器中“预加载”为仅HTTPS	纳入机构实施计划
	各机构必须与CISA协商，制定零信任架构计划，描述如何隔离其应用程序和环境，并将其纳入本备忘录要求的全面实施和投资计划	纳入机构实施计划
应用程序和工作负载	机构系统授权过程必须采用自动分析工具和手动专家分析	纳入机构实施计划
	各机构必须欢迎其互联网接入系统的外部漏洞报告	2022年9月，与OMB M-20-32和BOD 20-01一致
	各机构必须选择至少一个需要认证且目前无法通过互联网访问的FISMA中级系统，并允许在互联网上全功能安全操作	自本备忘录发布之日起一年内
	各机构必须开始向CISA和GSA提供其互联网信息系统使用的任何非.gov主机名	自本备忘录发布之日起60天内
	各机构在部署服务时，尤其是在基于云的基础设施中，要尽量使用不可变的工作负载	纳入机构实施计划
数据	各机构必须为其敏感电子文档制定一套初始分类，旨在自动监控并限制这些文档的共享方式	自本备忘录发布之日起120天内

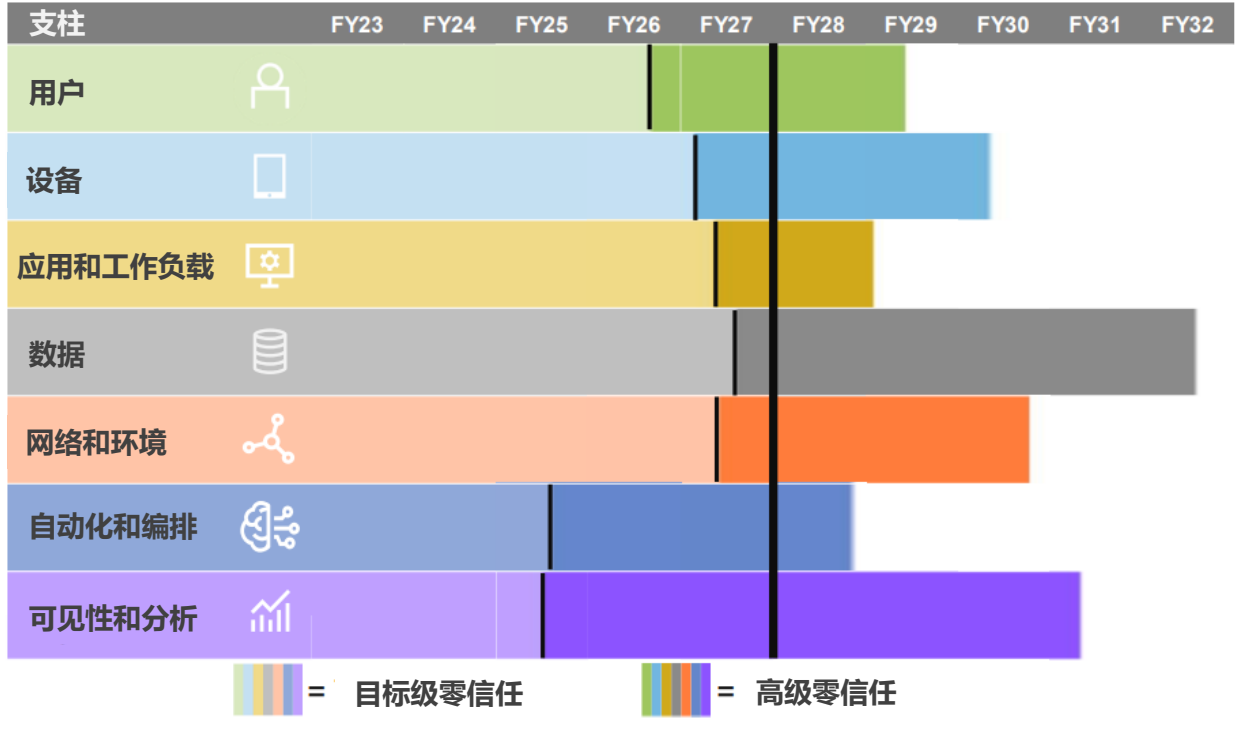
美国防部基于体系规划视角提出完整的框架和路径方法

美国防部的《零信任战略》给出了零信任的执行纲要、战略背景、愿景、战略目标目的以及执行方法，从体系规划的视角提出了框架方法，战略围绕7个支柱设定了45项网络安全能力。执行路线图概述了影响顺序和并行开发的依赖关系和相互依赖关系，并提供了按财年实现成果的计划表。



零信任工作基线

- 通过Brownfield开发模式方法利用现有基础设施和环境；
- 全面实现零信任现代化：5年以上的实施计划（从2023财年开始）；
- 建立所需的能力和活动，以达到目标级和高级零信任；
- 对完成零信任的工具或方法暂不设限。



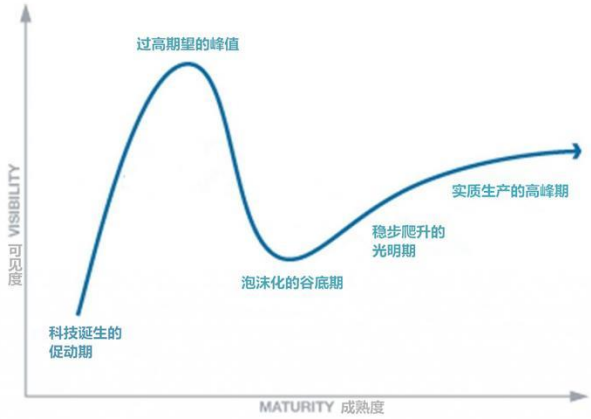
预计到2027年，所有国防部机构都将达到目标级零信任。

美国官方机构在推动零信任发展中的角色对比分析

各方积极探索零信任与现有技术的结合方法，并在美国大型IT企业落地实施，形成了若干最佳实践。在关乎国家安全的领域，美国采用自顶向下的推进模式，对国家层面的战略到具体架构设计、技术规范和迁移步骤等，均**采用政府主导顶层规划，创造系统、刚性、深度的安全需求，拉动防御能力体系的建设和产业发展**。

推动零信任发展的不同主体的不同视角

名称	角色定位	作用分析	主要贡献	推进视角
NIST	NIST制定网络安全标准、指南、最佳实践和其他资源，以满足美国行业、联邦机构和更广泛公众的需求。	OMB要求所有联邦机构实施 NIST 的网络安全标准和针对非国家安全系统的指南。	NIST作为标准化组织，在一种新的安全概念和范式的形成过程中，给出更为明确清晰的定义和实施方法，并解决概念的内涵、范畴和边界等问题。因此NIST方案是窄带的在微隔离、SDP、身份认证的强化要求上展开的。	推出的是局部标准，是技术实现机理。
OMB	协助总统编制和审核国家预算；监督对预算的管理；加强政府的行政管理。	其财务能力使其对国防部和政府的国防政策具有相当大的影响力。	以OMB代表的联邦政府作为行政指导部门，同时也是用户部门，给出了相对清晰的目标和行动导向。	给出了相对清晰的目标导向和具体行动计划。
DoD	负责协调和监督与美国国家安全和美国武装部队直接相关的所有政府职能。	由于其规模、结构、全球影响力以及所处理数据的性质，DOD对美国政府的策略具有重大影响。	DOD是通过用户规划，建构一个全局的体系战略。	推出的是全局战略，包括了从顶层规划到具体实施的全生命周期。

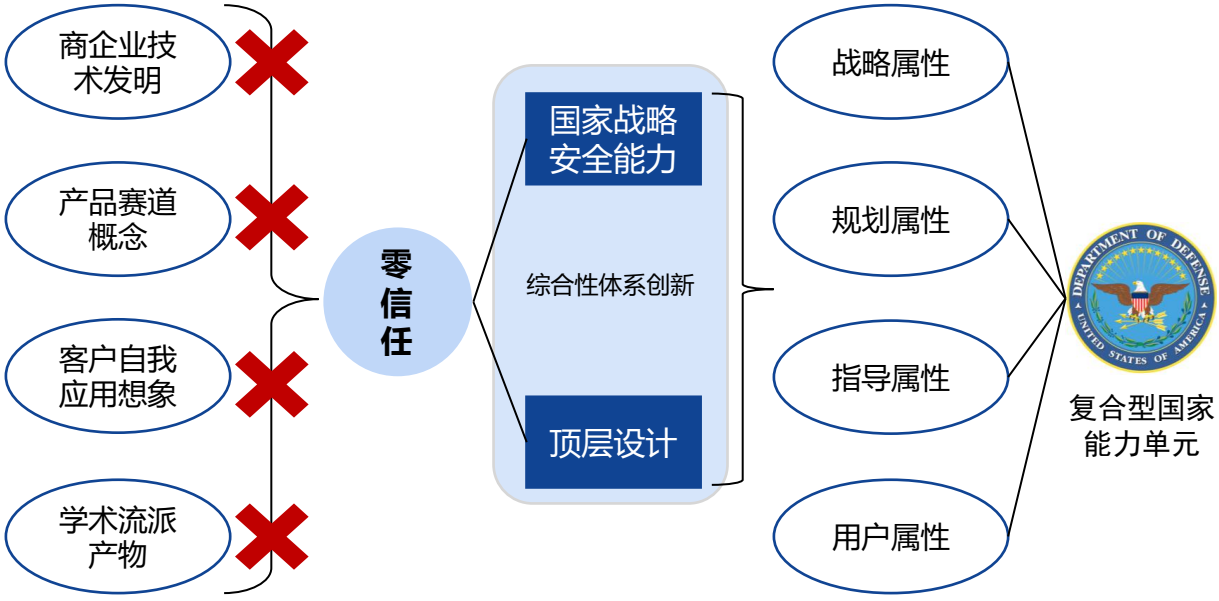


Gartner技术成熟度曲线

04 从零信任的演进分析网络安全创新规律的特点

网络安全和信息化的创新基础规律

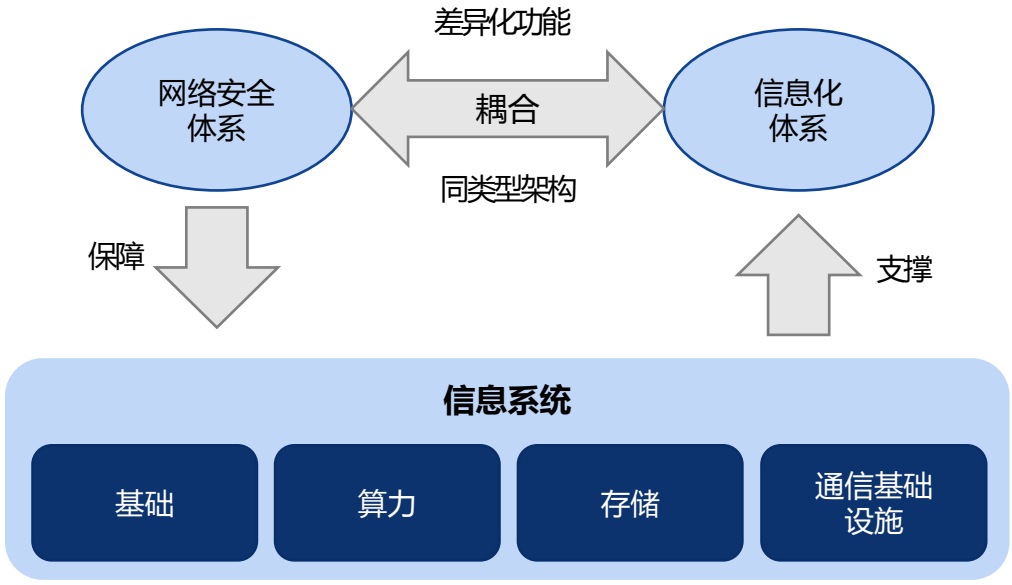
研究零信任创新发展过程，有利于我们超越单纯的理论与技术层面、企业个体层面，而是建构在整个产业乃至整个国家层面来认知网络安全规律，以服务于我国政府更好的构建网络安全创新顶层机制。



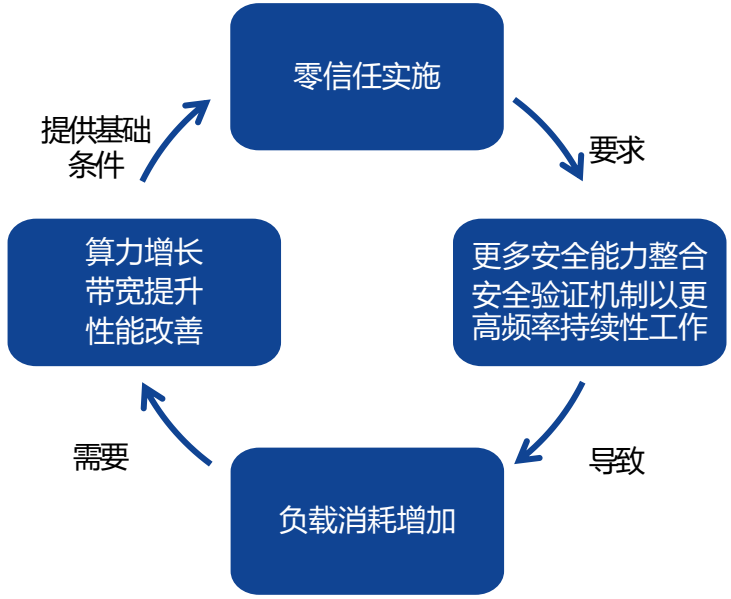
零信任在美国发展演进到今天所取得的进展，不是单一主体主导的，而是多主体协同推动的共同结果

网络安全和信息化的创新基础规律，是若干组辩证统一的属性特点的平衡

从与信息化关系的视角看，网络安全创新是以伴生性为主，自生性为辅的创新



网络安全的价值取决于所保障的目标资产对象



安全工作需要依赖基础计算环境、能力和条件

安全本身不是第一性目标，网络安全的第一性目标是保障信息系统的运行，保障机密性、完整性和可用性。因此，在绝大部分场景情况下，**脱离信息环境场景的网络安全创新都成为一种“看上去很美”的空中楼阁。**

从创新形态上看，网络安全创新是以开放性为主，封闭性为辅的创新

	网络安全创新以开放性为主导，是由于信息系统先天具有开放式信息交换的特点	网络安全创新也有封闭性的需要，网络安全的对抗优势是建立在对攻击者的低可见性上
网络安全创新体系	● 信息化本身有高度开放协同的基础文化，有开源的体系作为基础，有开放式的标准作为遵循和参照。通常来看，在网络安全体系中，越是有联通和兼容性需求的越需要开放，如接口、通讯标准、密码算法等。 ● 网络安全对抗本质上就是一种开放式对抗。	● 在面向强威胁对抗的场景中，往往需要对遏制威胁的基础作用原理、检测规则、检测方法、识别方式、判定逻辑等进行保密，来增加对攻击方的低可见性。威胁检测方法过于公开，会降低攻击者剖析研究绕过安全机制的成本。 ● 由于网络安全的商业组织通常都具有比较强的逆向研究能力，因此可以比较完整的还原出竞争产品的基础实现逻辑并予以借鉴。也就使得网络安全成为相对封闭的领域。
零信任创新演进过程	零信任是作为一个尝试引导潮流的共同理念提出的，其理念、思路和技术标准规范等始终处于开放迭代状态。	零信任能力集合中的很多能力域，如威胁检测规则、威胁检测模型等依然还是封闭式创新方式演进。

在进行创新时要基于网络安全是开放的不是封闭的总体基调，统合好开放和封闭之间的关系。

从演化模式来看，网络安全创新是以叠加性为主，颠覆性为辅的创新

新技术要依托于既有基础技术和实现能力来产生

- 网络安全在大的理念框架演进中具备迭代与颠覆的特点，但是在具体能力组织方面更多的表现为对既有能力的叠加重组。
- 信息化和网络安全主要由代码编程实现，在基础的系统平台和体系结构发生重大变化的情况下，网络安全的基础能力大多数表现为商业产品的持续功能演进和升级过程。

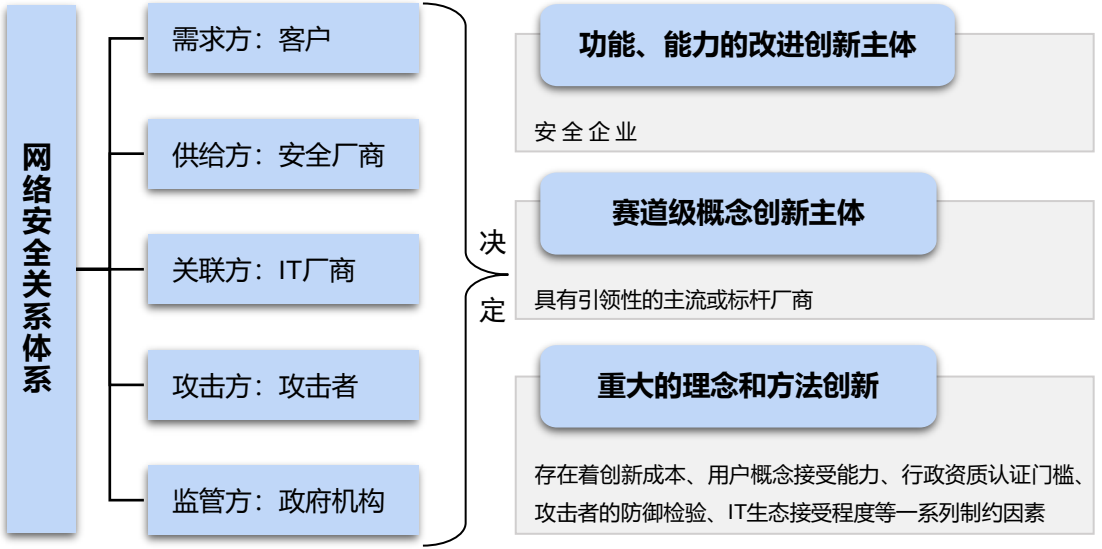
将零信任看成某个产品赛道，或是一种彻底的技术创新和颠覆，都是错误的

- DoD的零信任战略与NIST零信任标准已经超出了零信任原有的定义范畴。这是美方在关键技术发展过程中，抽取出了带有示范性维度的理念框架，以实现对能力整体演进的统领。
- 零信任在其标准内涵、产品边界、整体架构和能力集合上是不断发展、逐渐扩大的。

没有基础能力的积累是无法完成一个理念从创新到到落地实施施、产生价值的过程的。

从参与创新的主体关系看，网络安全创新是协同式为主，独立式为辅的创新

网络安全不是简单的供需关系，而是一种多边主体关系。这种复杂的多边关系，一方面为各环节主体发挥创新的能动性提供了丰富的空间和资源，但也决定了要推动重大的战略体系演进，必然需要**带有顶层设计的协同创新**来推动。



网络安全创新是多主体多层次协同创新

协同性创新

零信任是在理念和学术探索的基础上进行顶层设计，符合信息化的大规模供应生产和协同的特点，为我们提供了一个战略协同创新的范式。**安全技术本身的突破无法解决所有问题，网络安全需要对用户场景和需求的理解，对威胁方威胁意图、威胁目标和手段的掌握，需要监管方的标准、体系、理念等的共同推进。**

总结

- 网络安全创新要遵循其客观规律，避免“伪创新”和“为了创新而创新”。
- 我国网络安全创新的推动要积极吸取发达国家的理念和实践成果，既不一味照搬照抄，也不因为他们产生于西方国家就嗤之以鼻。美方在零信任领域的实践为我们提供了很好的思路和示范样本。
- 在借鉴国外已有经验的同时，也要注意到网络安全创新的推动也需要立足我国信息化发展的不平衡不充分的实际情况。零信任的落地需要大量已有技术的支撑，对已有的网络安全体系提出了更好的要求。我国的网络安全发展，即需要创新，也需要补课。
- 面对当前普遍存在的资产碎片化、信息孤岛化、系统难以充分连接和云化的情况，安天提出了一种以执行体治理为抓手，更加兼容现状的零信任路径。

感谢大家的关注

安天冬训营 wtc.antiy.cn