ICS 35.040
L80

T

中关村可信计算产业联盟团体标准

T/ZTCIA XXX—202X

面向信息系统的可信纵深防御参考架构

Reference Architecture for Trusted Depth Defense to Information Systems

（征求意见稿）

（本稿完成日期：2026 年 3 月 13 日）

202X - XX - XX 发布　　202X - XX - XX 实施

中关村可信计算产业联盟　发布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中关村可信计算产业联盟提出并归口。

本文件起草单位：。

本文件主要起草人：。

引 言

随着国家数字化转型发展战略的深入推进，各行业领域，尤其是具备互联网业务的企业，正加速向数字化、智能化转型。企业信息系统和服务呈现线上化、数字化、智能化趋势，数字化资产在线密集度持续增加，网络边界趋于模糊，安全挑战日益严峻。

本文件旨在将可信纵深防御的先进理念与实践经验，为具备互联网业务的企业提供参考框架。通过构建覆盖硬件、固件、系统软件、应用软件的全栈可信防御体系，针对企业信息系统的安全防御专项设计解决方案，为企业信息系统提供事前主动防御、多层纵深覆盖的安全保障方案。

本文件按照《网络安全法》《数据安全法》《个人信息保护法》《关于规范人工智能发展的指导意见》等相关法律法规和政策要求，结合云计算、大数据、人工智能等新技术特点，为企业建设适应新时代网络安全形势的防御体系提供指导。

面向信息系统的可信纵深防御参考架构

1 范围

本文件给出了应用可信技术构建信息系统纵深防御架构的基本原则、体系架构、技术能力和实施路径等。

本文件适用于面向互联网/公共网络提供服务的企业应用，为其可信技术建设及信息系统纵深防御体系架构的构建与评估提供参考。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信 trust

基于可信计算技术，通过度量、验证、证明等手段，确保计算环境、数据和行为符合预期的一种安全属性。

3.2

纵深防御 defence in depth

通过复合性防护，利用各种技术特点，形成多层次、多技术功能互补的多重防线，以满足防护的均衡性、抗损性要求，避免一处防御措施失效后，全线被突破的局面。

3.3

可信纵深防御 defence in depth based on trust

以可信根为支撑，以密码学方法为主要手段，通过度量、检测、证明等手段，构建贯穿硬件、固件、系统软件、应用软件和网络行为的完整信任链，为信息系统运行提供安全可信的底座。最终实现事前高效规避高级威胁与未知威胁的目标，并在安全性与业务连续性之间取得平衡。

3.4

可信计算平台 trust computing platform

构建在计算系统中，用于实现可信计算功能的支撑系统。

3.5

可信根 root of trust

可信根是可信计算平台的信任源点，由TPCM、TCM和TSB组成。TPCM是可信平台控制模块，负责发起可信验证、获取可信验证数据、执行可信验证中运算（非密码相关）、存储相关策略信息、执行可信控

制等。TCM是可信密码模块，为可信验证操作提供密码服务支撑。可信根是用于支撑可信计算平台信任链建立和传递的可对外提供完整性度量、安全存储、密码运算等服务的功能模块。

[来源：T/ZTCIA 001-2023，3.3]

3.6

信任链 chain of trust

在计算节点启动和运行过程中，使用完整性度量方法在部件之间所建立的信任传递关系。

[来源：GB/T29829-2013.定义3.1.13]

3.7

可信策略 trusted strategy

定义应用系统可信行为的规则集合。

3.8

可信计算产品 Trusted computing products

具备可信计算功能的各类计算机设备，包括但不限于通用PC机、通用服务器、笔记本电脑、移动终端设备、网络安全设备、网络通信设备、工控设备、物联网设备等。

[来源：T/ZTCIA 001-2023，3.1]

4 基本原则

4.1 安全可信原则

通过度量、检测、证明以及管控等手段确保资源加载、业务交互等是符合预期且无风险的。同时，构建贯穿硬件、固件、系统软件、应用软件、网络和终端的完整信任链，并构建可信策略，为信息系统的运行提供安全可信的底座。

4.2 多层覆盖原则

根据面临的威胁状况、业务特性、IT架构、建设成本、管控效率等因素来综合评估所需建设防御层数，在降低风险事件发生的概率，有效应对威胁和企业合规要求、安全成本投入、管控效率上取得平衡。

4.3 自身安全保障原则

在可信防御能力设计时，包括但不限于：

a）充分利用硬件可信芯片的可信存储和密码技术，通过构建完备的可信信任链等方式来保障可信防御能力的安全性；

b）应采用密码技术（如数字证书、数字签名等）保护可信策略及管控内容的机密性与完整性，并保障传输安全；

c）充分利用数字证书等密码技术保障数字资产在传输过程中的安全性；

d）根据风险行为的响应信息或拦截日志确保防御能力和策略的持续有效。

4.4 稳定性保障原则

在企业可信防御体系的建设中，稳定性保障原则应包括但不限于：

a） 可信防御能力及策略配置的稳定性需重点建设与保障，以降低可信防御能力或策略配置不当导致业务服务水平下降的风险；

b）可信防御能力及策略自身的稳定性应重点建设和保障，以有效发挥可信防御能力和策略的价值。

5 体系架构

可信纵深防御体系架构建设内容包括基础设施可信、应用可信、网络可信、移动端及终端可信、构建信任链以及可信策略，体系架构见图1。针对开放的应用系统服务，在访问链路上，通过在移动端及终端层、网络层、应用层及基础设施层建立不同层面的可信策略控制点，并配置符合可信防御强度要求的安全防御策略。

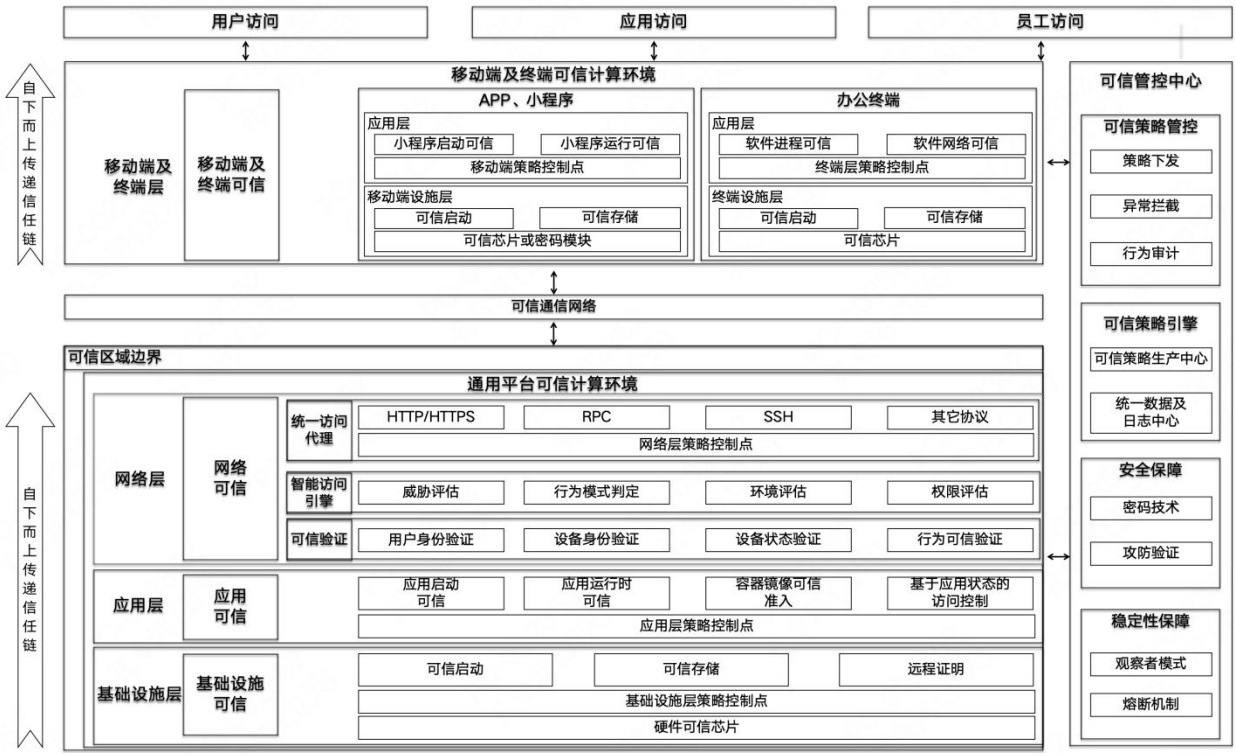


图1 可信纵深防御体系架构

可信纵深防御体系架构包括：

a）基础设施可信指服务器、存储等基础设施可信，不包括数据中心、机房和网络和终端。其建设内容和具备的技术能力见 6.1，其实施路径和要点见 7.2.1，附录 A 提供了可信纵深防御体系场景案例，附录 B.1 提供了基于云原生场景的基础设施可信构建案例作为参考示例；

b）应用可信。其建设内容见 6.2，其实施路径和要点见 7.2.2，附录 B.2 提供了代码及配置可信、代码运行时环境可信等应用可信构建案例作为参考示例；

c）网络可信。其建设内容见 6.3，其实施路径和要点见 7.2.3，附录 B.3 提供了网络入向交互可信（含身份、权限和行为等）、网络出向交互可信等网络可信构建案例作为参考示例；

d）移动端及终端可信指用户、员工和应用接入的各类终端，包括 PC、移动终端或者其他端侧设备。其建设内容见 6.4，其实施路径和要点见 7.2.4，附录 B.4 提供了移动端可信、终端可信等端安全可信构建案例作为参考示例；

e）针对信任链构建，其建设内容见 6.5，其实施路径和要点见 7.2.5，附录 B.5 提供了信任链构建的案例作为参考示例；

f）针对可信策略构建，其建设内容见 6.6，其实施路径和要点见 7.2.6，附录 B.6 提供了可信策略

能力、模型设计的案例作为参考示例。

6 技术能力

6.1 基础设施可信

基础设施可信对物理机节点的启动和运行进行可信管控，使物理机是可信的。基于硬件可信根构建基础设施的信任链，确保基础设施从启动到运行的全过程可信。功能包括但不限于：

a）基于可信根对硬件、固件、引导程序及内核等组件逐级度量，确保启动可信；

b）基于可信根对所有系统服务、应用程序及依赖库等二进制文件实施可信验证，包括加载时的静态度量与运行时的动态度量，确保执行代码来源及运行可信；

6.2 应用可信

应用可信负责对容器、应用调用的进程、类、方法、函数、文件和网络行为建立白名单的可信管控策略，确保容器和应用仅能按照预期内的方式启动或运行。功能包括但不限于：

a）代码及配置可信；

b）代码运行时环境可信；

c）应用运行时可信。

6.3 网络可信

网络可信入向负责对访问主体的身份、权限、环境、行为等构建可信策略控制点，确保网络身份、权限、环境、网络行为等是可信的；网络出向通过构建可信策略控制点确保交互的域名、IP和内容等是可信的。功能包括但不限于：

a）网络入向交互可信，对来访者身份、权限、环境和行为等进行可信验证和管控；

b）网络出向交互可信，对出向交互的应用、容器或主机访问的域名、IP 或内容等进行可信验证和管控。

c）基于可信根对网络连接的两端设备进行双向可信验证，可信验证要素应包括设备身份、启动信任链状态和运行状态。其中启动信任链状态和运行状态通过可信报告来进行体现，并能够依据可信策略进行网络控制并记录日志。

6.4 移动端及终端可信

负责对移动端、终端进行管控、监测与防护，确保终端的设备、进程、网络行为等是可信的。功能包括但不限于：

a）移动端安全可信；

b）终端安全可信。

6.5 构建信任链

信任链负责将信任机制由硬件可信根逐层传递至基础设施层、应用层、网络层，实现包含每层可信策略控制点自身在内的全链路的安全可信。

通过定义安全防护能力指标体系，针对企业可信纵深防御体系覆盖率、有效率等指标进行动态量化测绘，实时展示安全防护能力状态，及时修复失效点。

6.6 可信策略

可信策略将企业的业务特性和形态进行有机结合，在风险应对与管控效率上取得平衡，确保可信策略可以有效应对面临的高级和未知威胁，同时可以兼顾企业发展效率要求。要点包括但不限于：

a）可信策略能力设计；

b）可信策略模型设计：要点包括但不限于：

——可收敛性；

——可管理性；

——稳定性；

——安全性。

7 实施路径

7.1 建设基线

基于可信纵深防御体系的建设思路和设计原则，应将企业安全防御体系建设中的可信场景、行为基线和行为内容在不同层面上做拆分，包括但不限于：

a）基础设施可信；

b）应用可信；

c）网络可信；

d）移动端及终端可信。

同时基于单个防御平面设计不同的防御能力，结合各个场景的安全可信要求建设可信防御能力和可信策略。具体的场景定义参见附录A。

7.2 能力建设

基于硬件芯片作为可信根从底层到顶层构建信任链，可根据实际情况分期建设，选择是否将可信防御能力建设与信任链构建分期或并行完成。具体实施时，建议优先对具备可信管控基础的安全能力进行升级，使其转变为可信级防御能力。在此过程中，应当前瞻性地设计和预留构建信任链所需的功能模块，从而降低后续系统改造的复杂性和工作量。随着可信防御能力的逐步部署，系统的安全防护能力将相应增强，整体防护水平也随之提升。最终，通过信任链构建方案，将所有可信防御能力串联整合，形成一个完整的可信纵深防御体系。

7.2.1 基础设施可信

基础设施可信在能力建设上，包括但不限于：

a）基于可信根，充分利用硬件可信芯片的可信存储和密码技术构建完备的信任链，实现物理机在启动时的硬件、BIOS、内核等进行可信管控，确保均是符合预期的、可信的；

b）针对物理机节点中的二进制文件建立可信验证和管控机制，确保物理机上启动和运行的二进制文件也均是符合预期的；

c）在策略配置上应支持策略的观察者模式、策略的拦截模式、支持阻断内核的加载、应用启动及白名单基线更新等功能。

7.2.2 应用可信

7.2.2.1 代码及配置可信

代码及配置可信，可根据相关文件的生命周期建立可信准入管控机制，整个管控机制贯穿于代码、相关配置文件（如源代码、镜像文件等）的整个生命周期，以保证交付全链路的一致性、完整性和安全性。

在容器镜像可信管控策略的配置上应支持的策略内容包括但不限于：

a）可支持细粒度的策略配置，例如可针对代码或镜像名称添加拦截策略；

b）可针对扫描发现的漏洞添加拦截策略，且基础规则的升级应定期从内外部漏洞数据库采集漏洞信息，编写为扫描插件，并定期更新扫描插件；

c）可保证运行态的镜像不被篡改，针对容器镜像从开发态到运行态在持续集成的流转过程中通过签名、权限控制等措施管控；

d）需落实最小必要权限原则，针对版本库、制品库、镜像仓库等重要的应用开发过程产出物，严格执行相关安全配置及最小必要权限分配原则；

e）三方引入软件需保障其安全性。对第三方软件（含组件），如开源软件、商用软件等，需从可信源引入，在软件引入前需经过安全扫描、安全评估等，验证软件不包含高危漏洞及恶意代码，从源头确保引入第三方软件的安全性和合规性。软件引入后应根据安全威胁情报和漏洞扫描结果，及时修复软件安全漏洞。

7.2.2.2 代码运行时环境可信

代码运行时环境可信是基于容器、主机当中建设的安全管控模块或组件，对容器和主机当中启动时和运行态的进程等建立可信级的管控能力。

a）在可信管控策略的配置上，宜支持如下场景的可信策略：

——进程启动可信：支持对进程启动行为，执行的命令、参数、用户、执行二进制文件哈希值等维度的可信管控；

——文件可信：支持对系统访问文件及文件内容的可信管控，保证系统读取的文件及文件的内容均是符合预期的；

——网络可信：支持对系统监听端口及网络请求的可信管控；

——基础配置可信：支持对操作系统、数据库、中间件、云基础设施组件等基础配置的可信管控，避免重要基础性安全配置被篡改，确保配置符合安全基准。

b）由于对容器、主机当中的进程、指令进行精细化管理时，策略配置稳定性风险较高，宜额外关注如下几点功能：

——可支持细粒度策略配置，例如支持按照应用维度进行配置；

——告警日志需支持截断，避免告警大量输出对系统造成性能影响；

——策略配置下发需支持灰度发布、过程监控与回滚机制；

——熔断机制的差异化配置，开发环境应禁止触发熔断机制，生产环境则应支持熔断功能。

7.2.2.3 应用运行时可信

应用运行时可信，在应用层基于应用运行时防护能力建立的可信策略控制点，可以对应用运行时依赖的网络行为、文件操作行为、高危反序列化函数的加载等行为建立可信级的白名单管控规则和策略，确保只有预期内的行为是可以执行成功的。

实施应用运行时可信防护能力的关键技术点包括但不限于：

a）注入安全检查逻辑；

b）动态下发应用策略；

c）上报事件限流；

d）进程熔断机制；

e）拦截策略熔断；

f）建立行为基线。

应用运行时可信防御能力涉及对于应用运行流程和逻辑的精细化管控，因此在发布至生产环境前宜从安全、架构、稳定性等多方视角进行全面的评估。结合企业务技术栈、业务特性和基础架构等，针对应用运行时可信防御能力进行能力部署、策略开启，保障能力及策略开启期间的稳定性风险和安全风险是可控的，防止造成业务影响。

7.2.3 网络可信

7.2.3.1 网络入向交互可信

在网络入向网关处除了常规的 4 层网络防火墙及 7 层 WEB 应用防火墙等能力外，还可基于网关建立对于访问者身份、权限、环境和行为的可信管控能力。

网络入向交互可信方案的关键点应在网络交互合适的位置构建网络层的可信策略控制点，同时在可信策略的控制点对访问者的身份、权限、环境和行为进行有效地识别和判断，确保是符合预期的、可信的。可通过搭建统一的访问代理网关，实现全流量的接管；针对接管的流量建立访问者身份、权限、环境和行为的管控能力；基于业务特征分析出可信的行为特征，最终建立可信级的管控策略。关键步骤包括但不限于：

a）开启安全管控模块；

b）配置基础语义策略；

c）配置可信管控策略。

7.2.3.2 网络出向交互可信

网络出向交互可信防御能力建设，可建立网络出口流量网关，并实现对全量出口流量的安全接管，并对于应用主机外联的系统服务进行服务地址、接口、参数、行为等信息的可信管控，确保外联的行为是安全可信的、合法合规的。对此，分别在网络出口流量网关的方案设计上和应用外联流量的可信管控上给出指导。

a）在网络出口流量网关的方案设计上，包括但不限于如下关键技术点：

——流量劫持；

——TLS 证书植入。

b）网络出向交互可信防御能力在应用外联流量的管控上，关键步骤包含但不限于如下步骤：

——出口流量网关的接入；

——出向外联域名服务的精细化管控。

7.2.4 移动端及终端可信

7.2.4.1 移动端可信

作为独立可信计算节点，应保障设备可信及应用层的可信。设备层需使用符合可信要求的移动设备；应用层实施以 IOS 端为例，基于移动端的安全切面实现应用层服务的可信管控，关键技术及特性包括但不限于如下几点：

a）移动端动态切面技术原理；

b）灵活的安全配置。

7.2.4.2 终端可信

作为独立可信计算节点，终端可信管控能力的落地，需使用符合可信要求的终端设备，并基于终端携带的可信芯片对设备的启动、系统运行进行校验，确保终端设备及系统的可信；进一步通过 EDR 等管控组件或模块，对终端设备运行的软件、运行的进程及网络行为进行可信管控，确保终端运行态的资源加载和网络行为均是可信的，是符合预期的。

a）以有效规避内外部的攻击和违规行为，其中关键技术点包括但不限于如下几个部分：

——终端设备可信；

——终端进程可信；

——终端网络行为可信。

b）终端可信管控能力的落地，关键实施流程包括但不限于如下内容：

——终端设备可信；

——终端进程可信；

——终端网络行为可信。

7.2.5 构建信任链

整个系统的信任链构建及验证流程如下：

a）首先，设备加电，硬件可信芯片最先启动，对 BIOS 进行可信验证和管控，可信芯片直接访问存储芯片获取 BIOS 数据，依据策略对 BIOS 进行可信验证，BIOS 验证通过后，CPU 可启动；

b）然后，依据可信固件的逻辑和可信策略基线对 OS Loader 进行可信度验证，验证通过后，可加载启动 OS Loader；

c）接下来，对操作系统进行可信验证，验证通过后，可加载启动操作系统；

d）下一步，对应用程序进行可信验证，验证通过后，可加载执行应用程序，系统启动完成，由此进入一个可信的启动环境；

e）最后，针对内嵌至应用程序的安全组件或者模块，在功能设计上需设计实现组件或者模块的守护程序来对内嵌至应用的组件或模块进行可信验证，验证通过后，可加载执行应用模块或组件。

7.2.6 可信策略

7.2.6.1 可信策略能力设计

可信策略能力设计包括但不限于如下内容：

a）可对企业业务现状进行具体分析，明确业务可接受的预期行为并确定策略管控粒度，进一步细化为实施的管控逻辑。具体的案例参见附录 B；

b）可建立大数据分析平台，具备海量数据存储能力的同时，提供便捷可靠的数据分析能力，以提供数据支撑支持制定策略、作为策略上线前的离线测试元数据等重要功能。

7.2.6.2 可信策略模型设计

可信策略应具备的特性包括但不限于：

a）可收敛性；

b）可管理性；

c）稳定性；

d）安全性。

7.2.6.3 可信策略生成和上线

企业业务应用完成可信防御能力及策略的集成后，为保证业务安全水位和稳定性能力逐步上升，可信策略生成和上线宜遵循如下原则：

a）准确采集并统计现有业务行为的全量数据，包括不同环境（预发、灰度和生产等） 、不同时期（当前数据、历史数据等）及不同场景（日常阶段、促销阶段等典型场景）数据，以保障可信策略的生成能够覆盖所有的业务行为；

b）在可信策略的变更过程中能够控制可信策略上线导致的稳定性风险。

在可信策略制定的过程中，可将人工分析的经验沉淀为自动化分析策略，再与可信策略管控中心对接，实现自动化的策略推荐与配置机制。

7.3 技术保障

7.3.1 安全性保障

7.3.1.1 可信防御能力安全设计保障

可信防御能力在设计和落地过程当中应充分利用密码技术，保障设计和落地的可信防御能力在能力及策略运行期间数据存储、传输的安全性。确保数据在传输过程中不被篡改或泄露。

7.3.1.2 可信防御能力及策略安全保障

针对建设和引入的可信防御能力在上线前需经过严格的安全评估流程，至少包含如下内容：

a) 需进行严格的 SDL 评估流程，通过黑盒、白盒、灰盒等技术措施保障可信防御能力无已知漏洞；

b) 需纳入至红蓝演练重点检验目标，从攻击者视角对可信纵深防御体系各层可信防御能力进行实战化检验评估，解决已知漏洞和短板，确保每个可信防御能力在安全性和健壮性上具备较高水位。

通过如上措施，最终保障可信纵深防御体系整体防御能力和状态是符合预期的。在实战化攻防检验方案上包括如下方面：

a）可信防御能力和策略已知绕过手法的评估；

b）可信防御能力和策略未知绕过手法的挖掘；

c）可信防御能力自身安全性评估；

d）前沿安全对抗技术跟踪研究。

7.3.1.3 极端状态下的可信防御效果保障

可信策略的安全攻防应对已建立的可信防御策略体系在极端苛刻条件下进行单点可信策略、可信策略纵深效果、熔断机制等测试，以验证其可信防御的效果。全面降低可信防护体系在极端情况下失效的概率。场景上需覆盖容器、应用、物理机、芯片等软硬件不可用的情况，以及业务流量、安全产品阈值极限场景的验证。

针对已建设的可信纵深防御体系，通过红蓝演练的方式，从真实黑客攻击视角演练验证企业可信纵深防御体系整体防御的有效性，避免可信防御能力存在威胁漏过或可绕过的情况，确保企业面临的全量威胁场景均部署了有效的可信防御措施。

7.3.2 稳定性保障

可信防御能力及策略的落地应满足企业应用稳定性的要求，核心目标包括两点：保障业务应用稳定可用；保障可信防御能力及策略对业务应用性能的影响处于可控范围内。关键保障手段包含如下方式：

a）充分测试验证；
b）变更风险左移；
c）变更可观测及可应急保障；
——可监控：保证各项稳定性指标可以实时监控及告警，基础指标推荐包括 CPU、内存、负载、IO、网络性能等；业务指标，接口请求成功率、接口请求耗时、业务错误量；策略指标，可信策略匹配数，通过数，拦截数；
——可灰度：可信策略覆盖应有合理的灰度策略；
——可回滚：可信策略在变更过程之后可以随时回滚；
——可应急：建立可快速应急的一键应急能力；
——自动化监控：通过建设自动化的监控能力，做到更细粒度的监控及响应机制；
——精准告警：针对预期内的告警及拦截事件，筛选出应重点关注的告警信息。
d）合理设计灰度策略；评估变更风险等级：
——按照风险等级从低到高逐步变更；
——变更分批次精细化操作；
——不同批次状态的变更间隔足够长。
e）熔断能力设计；
f）舆情监控。

7.4 实战检验

7.4.1 概述

针对企业已建设的可信纵深防御体系，应通过实战的方式检验防御体系的效果，挖掘可纵深防御体系的短板，引导后续防御体系的建设方向。实战检验架构见图2。

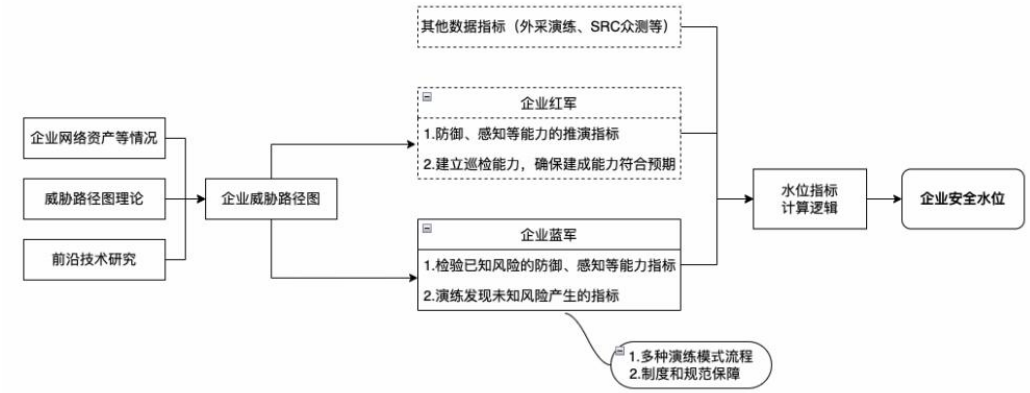


图2 实战检验架构图

实战检验体系以威胁路径图为理论依据，企业红军基于威胁路径图理论打标获得推演的安全能力建设指标，企业网络安全攻防演练基于威胁路径图通过实战攻防演练覆盖全部攻击路径，以发现未知安全风险，通过自动化有效性检验来验证已建成安全能力的有效性，整个过程使用实战检验管理系统进行管理，配合实战检验管理制度和规范等形成完整的实战检验体系。通过企业蓝军、企业红军、外部攻击者（外采演练、SRC众测等）等多方数据的校正计算，最终得到一个时间段内企业真实的安全能力水平指标数据。

7.4.2 威胁路径图建设

威胁路径图中包含攻防实体数据、攻防场景数据、攻击技术数据、攻击技术链数据、攻击用例数据以及攻防关联数据。

图3所示的威胁路径图样例从全局视角展示了威胁路径图模型的数据结构，图中圆圈代表攻防实体，代表企业的IT资产。圆圈之间的连线代表攻防场景，代表攻击发生的位置信息。攻防场景上关联了场景内从攻防实体对攻防实体进行攻击所有可能的攻击技术链。如图1中黑色加粗部分代表一条完整攻击路径，包含黑客从攻击起点实体“S”到攻击目标实体“E”经过的路径及使用的攻击技术链。

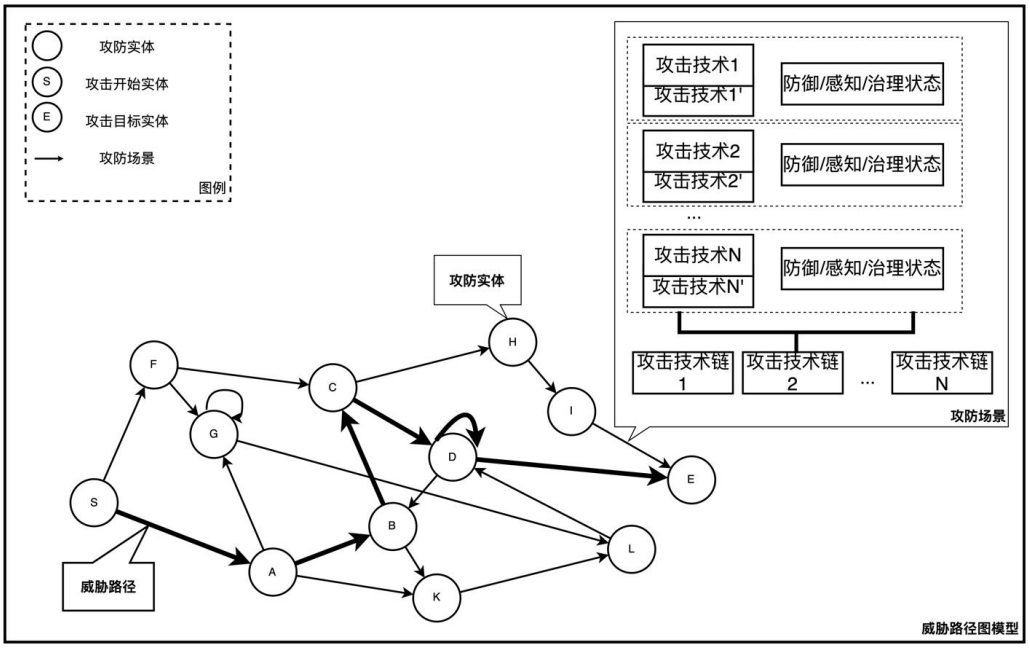


图3 威胁路径图

在威胁路径图中，可将攻击者的攻击路径抽象成图3中“S->A->B->C->D->E”的一条折线，图中的字母代表资产节点，其中“S”代表攻击起点，“E”代表攻击目标。节点之间的连线代表攻击场景，攻击场景内会包含可能的攻击方法列表。

通过上述得到的威胁路径图内只包含了基础的资产和攻击场景信息，还应结合实际的攻击场景、方法、工具等信息对威胁路径图添加更多的属性。可增加资产属性和优先级属性。

威胁路径图中的攻击场景内细化了该场景内可以使用的所有攻击方法。同时攻击方法细分为攻击技术，不同的攻击技术可以进行同等的替换。每种攻击方法都会涉及到很多攻击技术，如信息投递方式、信息投递内容、攻击载荷加载方式等。每种攻击技术都有相应的替换方案如信息投递方式可以是微信投递、QQ投递等，投递内容可以是钓鱼链接、钓鱼附件等；攻击载荷加载方式可能是聊天软件漏洞、用户点击运行、浏览器漏洞等，这样可以大幅提高攻击的灵活性和覆盖的全面性。

建设威胁路径图，步骤如下：

a）梳理资产节点和威胁场景，资产宜具备网络属性、开发技能栈、业务类型、历史漏洞等信息；

b）梳理攻击场景，攻击场景由资产节点之间的网络连线组成；

c）根据各个场景攻击发生的概率、攻击的成本、被攻击后造成的损失综合评估攻击场景的优先级信息。

7.4.3 红蓝演练机制建设

7.4.3.1 检验机制

红蓝演练是检验企业可信纵深防御体系有效性的重要机制，检验机制可包括常规演练、定向测试演练、预设场景演练和全链路演练等不同形式：

a）日常测试工作；

b）安全产品测试；

c）预设场景演练；

d）全链路演练；

e）数据质量和时效性检验。

7.4.3.2 路线建设

红蓝演练建设路线如下：

a）针对已建设的威胁路径图，额外补充企业可信防御能力的数据信息（例如安全能力列表以及覆盖情况、安全策略列表以及覆盖情况等等）；

b）基于威胁路径图的数据定期进行人工对抗演练（包含日常测试工作、安全产品测试、预设场景演练、全链路演练），并在每次演练过后记录演练的结果和效果数据，并填充到平台，形成实战检验平台系统；

c）基于人工对抗演练中沉淀出经验，形成常态化演练。

通过建设红蓝演练机制，结合基于专家经验的人工检验以及高效常态化的自动化检验，不断为安全建设提供升级、整改的指导意见，促进防御能力不断升级完善。

附 录 A
（资料性）
场景示例

A.1 概述

企业可信纵深防御体系场景列示了各个分层、子分类场景的可信定义及防护场景。

A.2 典型场景

企业可信纵深防御体系场景列示于表A.1。

表 A.1 企业可信纵深防御体系场景示例

分层	子分类	可信定义	防护场景
基础设施可信	硬件可信	针对硬件加载时的硬件类型、版本、固件内容、配置等进行可信验证，确保系统运行前依赖的硬件是符合预期的	目的是抵御硬件供应链风险：若硬件在生产和采购过程中被替换或植入后门，应在启动时检测并阻止硬件使用
	OS 启动时可信	针对 OS 引导、启动的每个环节进行可信验证和管控，确保 OS 启动的过程是符合预期的	目的是抵御来自攻击者入侵后植入的可驻留的 OS 级别的后门和 Rootkit 的风险。 以及攻击者控制了 OS 供应链，并植入后门的风险
	OS 运行时可信	针对 OS 运行状态持续进行可信验证和管控，确保运行中 OS 是不被篡改的	目的是抵御 OS 级别的 Rootkit
	虚拟机可信	针对虚拟机 Hypervisor 持续进行可信验证和管控，确保虚拟化机制状态是符合预期的；同时也应验证和管控通过虚拟机启动的 OS，确保是符合预期的，实现虚拟化场景的安全可信	目的是抵御在虚拟化场景中，攻击者通过在虚拟机 Hypervisor 层或者虚拟机 OS 中植入恶意代码的攻击行为
应用可信	容器可信	针对容器 Driver 持续进行可信验证和管控，确保容器底层机制的运行状态是符合预期的；同时进一步验证，确保容器镜像符合预期，禁止加载不安全的镜像	目的是抵御在容器化场景中，容器镜像存在软件供应链的攻击威胁
	应用启动可信	针对主机、容器中启动的应用程序进行可信验证和管控，确保启动的应用代码和配置是符合预期的	目的是抵御攻击者入侵到主机、容器后，尝试执行自己的木马程序以进一步攻击或者留后门的攻击行为
	运行时可信	针对主机、容器当中运行的应用进程持续进行可信验证和管控，以判断程序运行空间的代码是否被篡改、程序行为是否符合预期	目的是抵御攻击者入侵到主机、容器中的某个应用，在应用进程代码执行空间中插入自己的恶意代码的行为

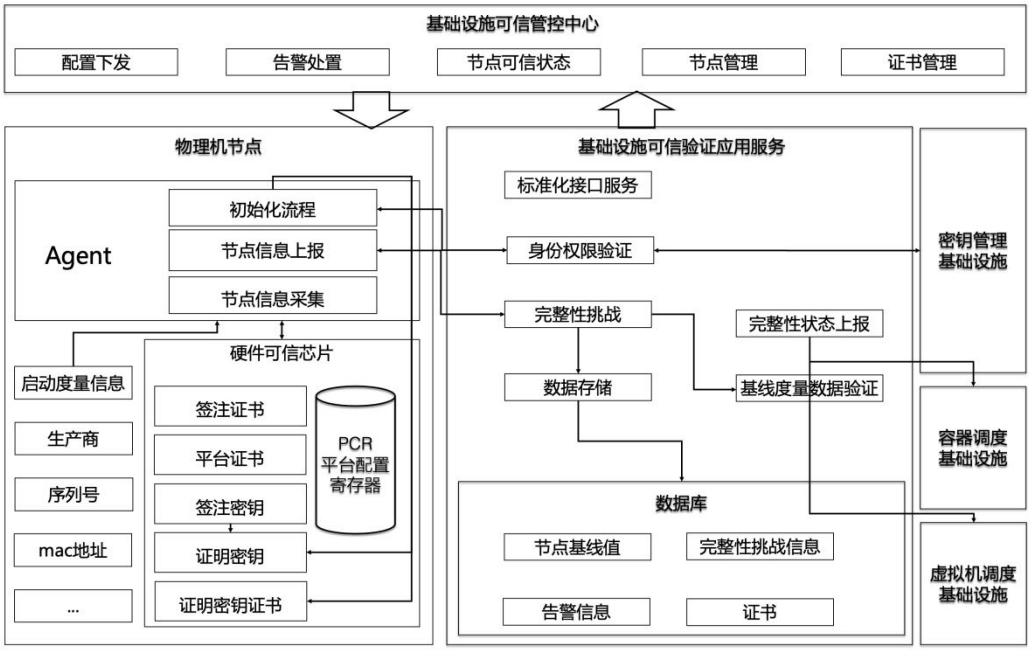
表 A.1 企业可信纵深防御体系场景示例（续）

分层	子分类	可信定义	防护场景
网络可信	网络入向访问者身份可信	访问者定义为业务场景当中请求的发起方，此处包括人员、终端、应用、WEB、RPC、DB 服务等。针对网络服务的访问者进行授权，并持续的对授予的身份可信验证和管控，以判断访问者身份是否符合预期的	目的是抵御攻击者通过 0Day 漏洞或 APT 攻击获得一定权限，进一步攻击办公网、生产网内开放的服务，利用其中的漏洞入侵窃取数据
	网络入向访问者状态可信	针对访问者所处的运行环境和运行状态持续进行可信验证和管控，以确保发起访问者的运行环境、运行状态和身份是可信的，而非攻击者伪造的	目的是抵御攻击者利用已经入侵的应用服务器或利用其身份发起攻击来扩大攻击面的风险
	网络出向交互可信	针对容器、服务器及网络设备的外联访问行为进行可信验证和管控，以确保外联的域名、IP 及传输的内容是可信的	目的是抵御攻击者利用域名、IP 回连攻击者服务器，外发数据等攻击行为
	网络信息传输可信	针对访问者信息传输的链路进行加密，建立安全的信息传输通道，以确保发起访问者的身份及传输的信息是可信的，没有被攻击者篡改的	目的是抵御攻击者利用已经入侵的应用服务器劫持传输链路当中的敏感信息来获取敏感数据或敏感配置
移动端及终端可信	终端设备可信	针对终端硬件、系统及 OS 运行状态进行可信验证和管控，确保终端设备是可信的、不被篡改的	目的是抵御硬件供应链风险、OS 级别的 Rootkit 等风险
	终端进程可信	针对访问者使用的终端使用的应用和进程行为建立白名单的管控策略，以确保发起者的终端运行时的应用进程是可信的，非攻击者的恶意应用程序	目的是抵御攻击者利用已经入侵的终端运行恶意的病毒、木马软件
	终端网络可信	针对访问者使用的终端的网络行为建立白名单的管控策略，以确保发起者的终端网络行为是可信的，非攻击者的恶意后门和恶意数据、文件的外发行为	目的是抵御攻击者利用已经入侵的终端建立持久化的后门或者进行敏感数据和文件的外发
	移动端小程序加载可信	针对访问者使用的小程序应用加载前进行签名验证，只有满足验签通过的小程序才会被 APP 加载。同时会验证小程序启动参数，对不满足预期的启动参数，不允许小程序加载	目的是抵御攻击者利用恶意小程序或利用小程序漏洞获取非法权限进而导致用户敏感信息泄露
	移动端小程序运行时可信	针对访问者使用的小程序运行过程中运行模式，调用的 Jsapi，运行的插件、使用的标签等进行运行时白名单校验，对于不满足预期的内容不允许小程序使用	目的是抵御攻击者利用小程序运行时依赖的组件、接口漏洞获取非法权限进而导致用户敏感信息泄露

附 录 B
（资料性）
实践案例

B.1 基础设施可信能力构建案例

一个可供参考的架构图如图B.1所示:



图B.1 基础设施可信防御能力架构示例图

基础设施可信防御能力架构主要包含如下功能模块：

a）内核模块签名；

b）证书白名单管理；

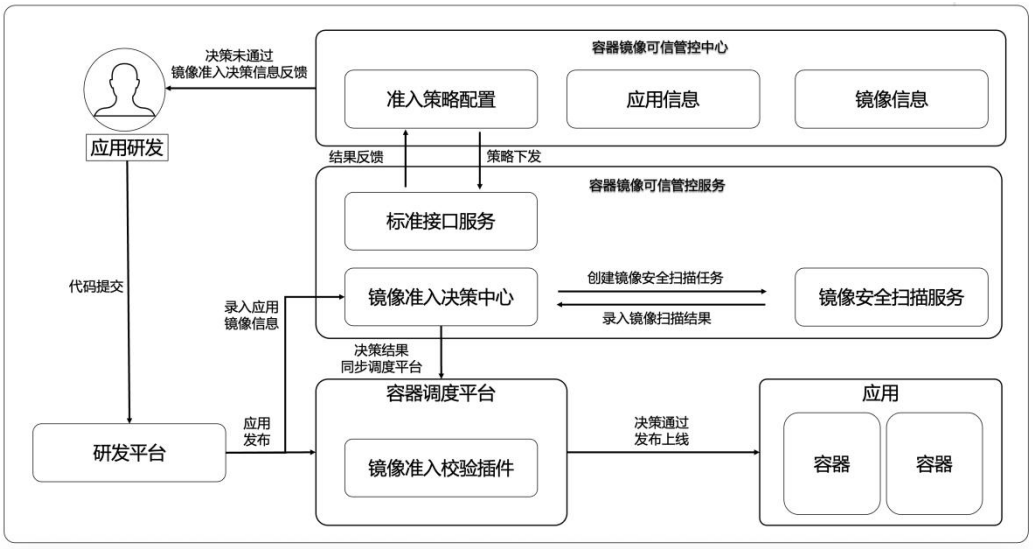
c）运行时可信验证；

d）灵活的策略配置。

B.2 应用可信构建案例

B.2.1 代码及配置可信

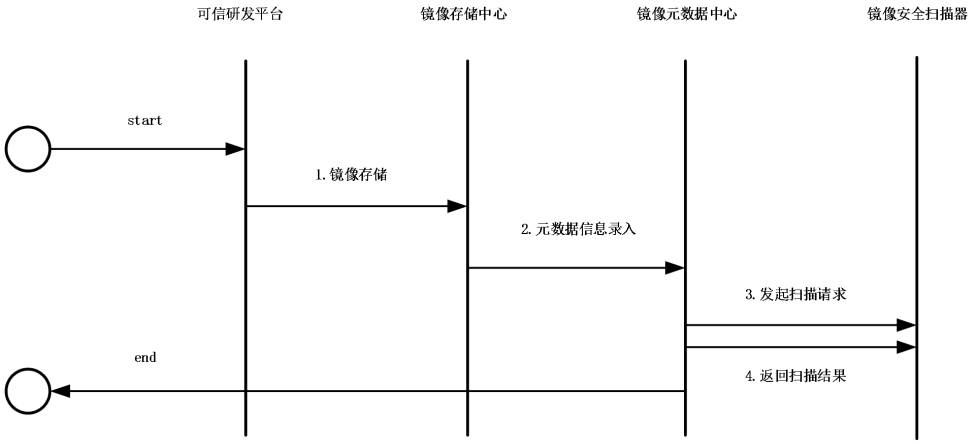
一个可供参考的实践案例如图B.2所示，在云原生的架构模式下完成代码及配置可信，可建设容器镜像安全检测及容器镜像可信准入两大能力：



图B.2 容器镜像可信架构示例图

B.2.2 容器镜像安全检测

容器镜像安全检测路径，如图B.3所示。



图B.3 容器镜像安全检测

容器镜像安全风险检测主要包含如下步骤：

a）可信研发平台完成镜像构建及签名后将镜像上传到镜像存储中心；

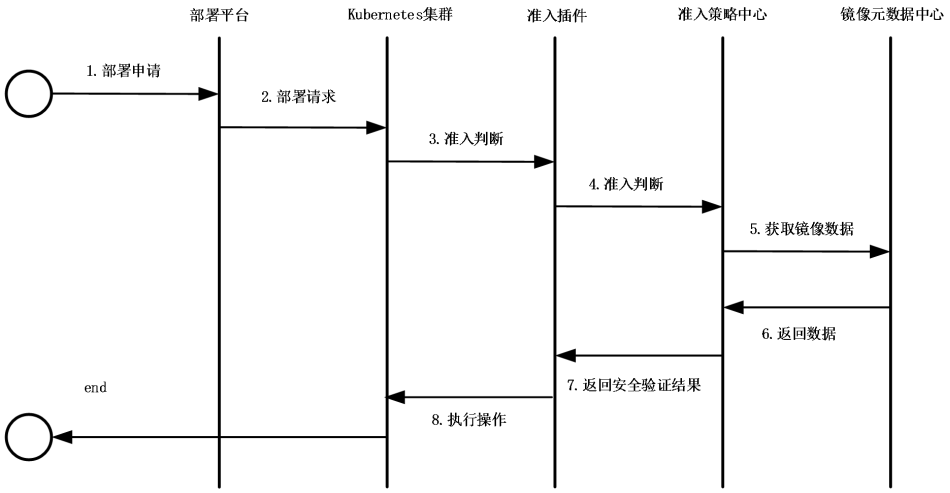
b）可信研发平台将镜像名称、存储位置、签名信息录入元数据中心；

c）镜像元数据中心在新增记录后，请求镜像安全扫描器进行镜像扫描；

d）镜像安全扫描器将扫描结果返回镜像元数据中心进行结果录入。

B.2.3 容器镜像可信准入步骤

容器镜像可信准入路径：



图B.4 容器镜像可信准入

容器镜像可信准入主要包含如下步骤，如图 B.4 所示：

a）企业研发人员提交应用部署申请；

b）部署平台将需要部署的镜像提交至容器调度集群，并下发镜像部署请求；

c）容器调度平台加载镜像准入插件，判断当前镜像准入策略；

d）准入插件获取准入策略判断当前镜像是否符合准入要求；

e）准入策略中心根据镜像唯一标识获取镜像签名和镜像扫描数据；

f）准入策略中心进行可信验证，判断当前应用镜像是否可以部署上线；

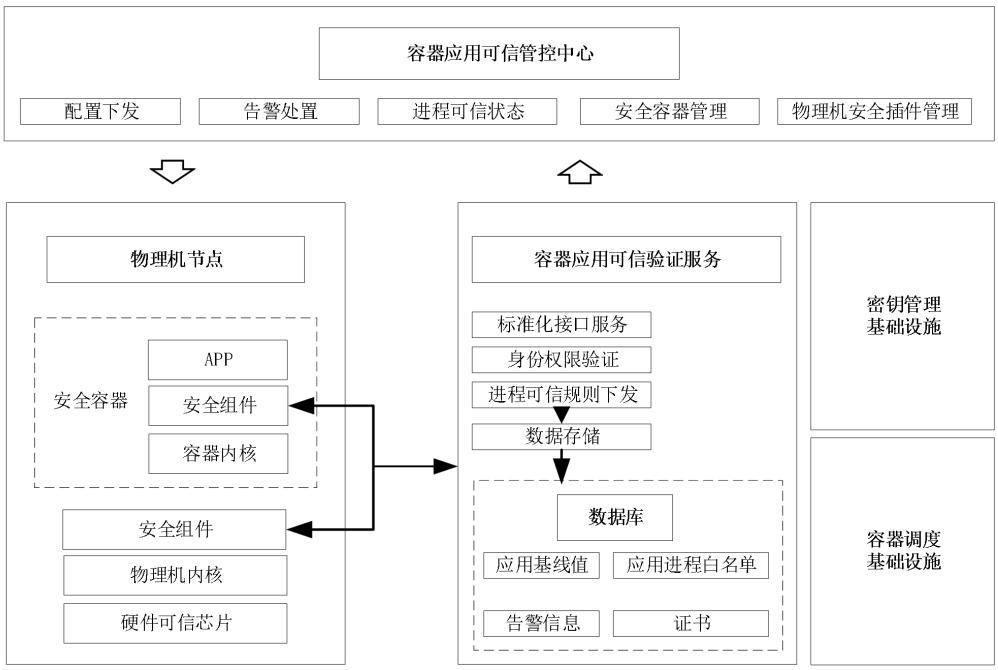
g）准入策略中心将安全验证结果返回给镜像准入插件；

h）容器调度平台根据准入插件评估的结果执行后续操作，决策通过则获取应用镜像进行部署，否则返回报错。

容器镜像可信防御能力的构建主要依赖控制面如可信研发平台、可信镜像存储中心、可信镜像元数据平台、镜像安全扫描器、镜像准入策略中心、容器调度集群等组件。容器镜像准入插件在 Kubernetes 集群中继承。同时，收集全量镜像数据支持风险分析和策略配置。

B.2.4 代码运行时环境可信

一个可供参考的代码运行环境可信的实践如图B.5所示，在云原生的架构模式下建立可信级管控能力，具备对容器和主机当中启动时和运行态的进程等进行可信级的管控：

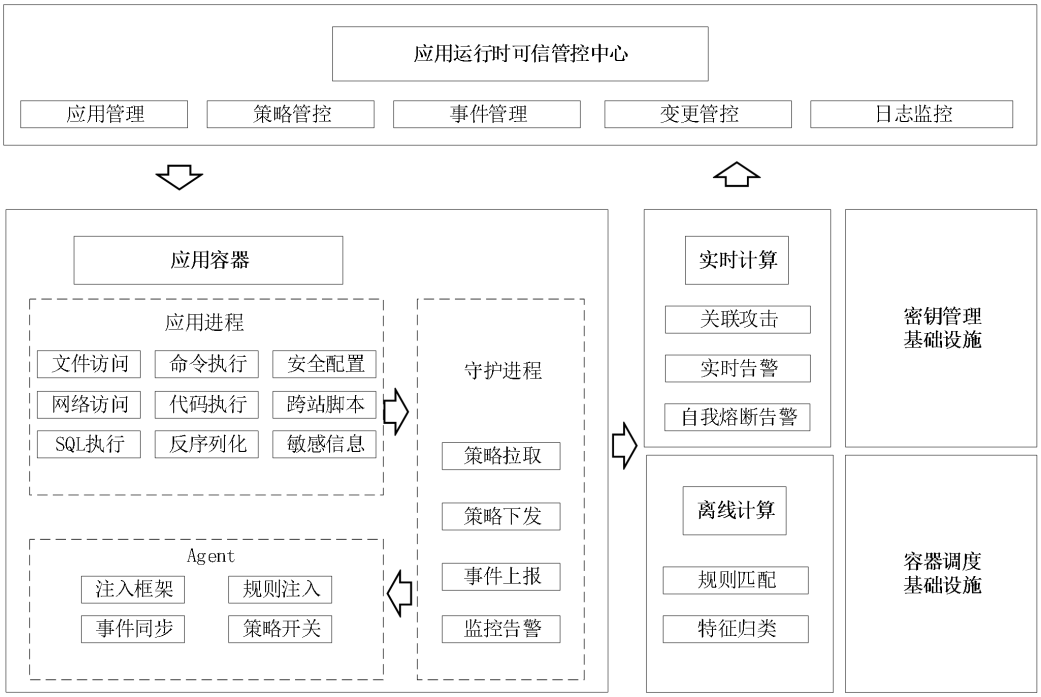


图B.5容器应用可信架构示例图

基于安全加固和管控要求，可以针对使用的容器、主机定制开发容器管控模块或插件，实现对容器主机中 syscall 行为的风险识别、判断、拦截、追溯和审计，如可以基于开源gVisor，在容器当中设计并落地可信防御的内核模块，实现对于容器的可信管控。针对物理机的方案可以通过内核集成方案来实现，将物理机内核管控模块和主机入侵检测系统结合来实现，通过主机入侵检测系统在物理机内核指令执行前配置拦截模块，确保启动和运行的进程及行为都是经过了安全模块度量的、可信的。

B.2.5 应用运行时可信

一个应用运行时可信的实践案例如图B.6。对企业在线应用系统建立运行时的网络访问、文件访问、系统命令执行及应用代码执行等行为建立可信级的管控规则，对于异常的攻击和未知的网络访问、文件访问、系统命令执行、应用代码执行等行为默认进行拦截，最终实现应用运行时可以防御0Day漏洞攻击的效果。

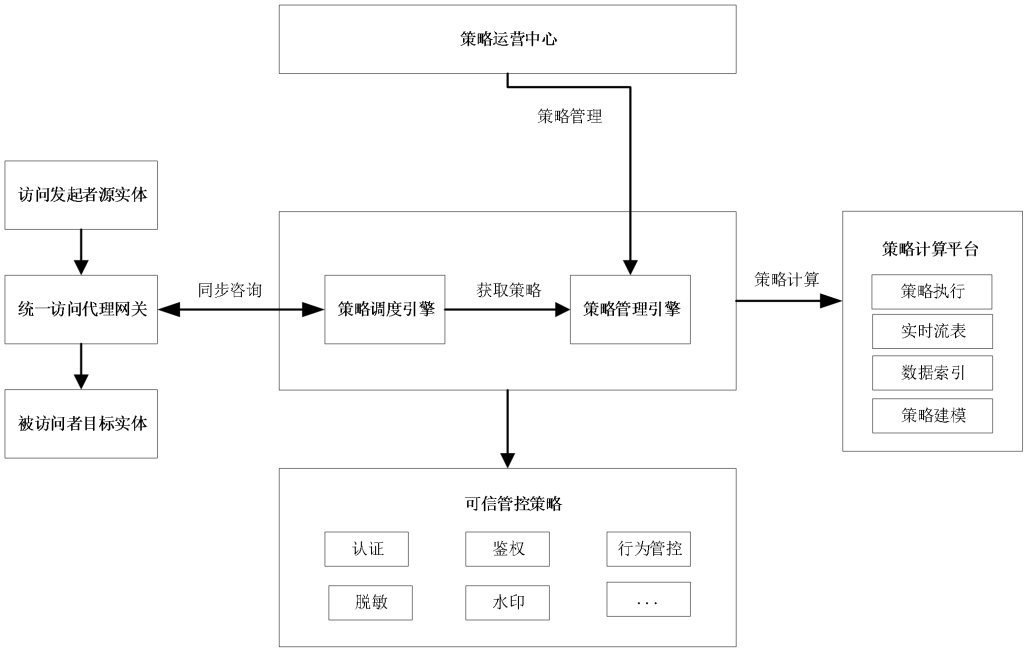


图B.6 应用运行时可信架构示例图

B.3 网络可信构建案例

B.3.1 网络入向交互可信

一个可供参考的网络入向交互可信管控的实践架构，覆盖身份、权限、行为等可信管控，如图B.7。



图B.7 统一访问代理网管可信架构示例图

以人员及终端身份可信及运行时和管理时的行为可信为例进行说明。

a）人员及终端身份可信：基于终端安全管控组件实现对于设备的可信管控。企业分发的办公终端应默认安装终端安全管控组件，当员工使用该办公终端访问办公系统时，统一访问代理层的可信网关会采集终端设备相关信息，通过校验设备信息与使用的账号信息，确保使用的终端是可信的。如果校验发现来源的设备是可信的则放行访问请求。如发现来源的设备是非可信的，则直接拦截或应完成多因子认证后并校验通过后才允许本次的访问行为。多因子认证应优先选择具有可变更属性的认证技术，如二次密码、动态令牌等，确保应用系统访问者的身份是可信的。

b）运行时和管理时行为可信：统一访问代理网关承载了开放应用服务的全量实时请求，是实现网络行为可信防御能力建设的关键点。因此，在统一访问代理网关处应按照不同的业务类型进行拆分，并针对性地建立多业务场景的可信管控策略，如针对于开放至互联网的服务，应根据来自互联网的访问请求严格地校验来源的 IP、用户的身份和权限都是符合预期的，以有效规避越权类的安全风险；针对开放至办公网的数据、资金类后台，严格地校验来源的终端、员工身份、员工权限和员工的行为是符合预期的，才能允许后台功能的操作，以有效地规避员工违规操作等风险事件的发生；针对于生产网内部应用接口之间的调用，应对于来访的应用、主机、接口和服务进行校验，确保是符合预期的应用服务之间的调用，以有效地规避生产网内部接口的滥用风险。通过如上所述方案，最终实现全链路的网络身份行为可信。

B.3.2 网络出向交互可信

一个可供参考的网络出向交互可信的实践架构如图B.8。对于网络出方向的流量进行可信度量，确保应用主机的外联行为均是可信的。此处以云原生及容器化技术为例进行举例说明，基于微隔离及应用身份技术下对应用主机发起网络行为进行管控，通过服务方的身份、权限、API路径、API参数、API内容进行可信度量，确保对外发起的网络请求是安全的、可信的、合法合规的。

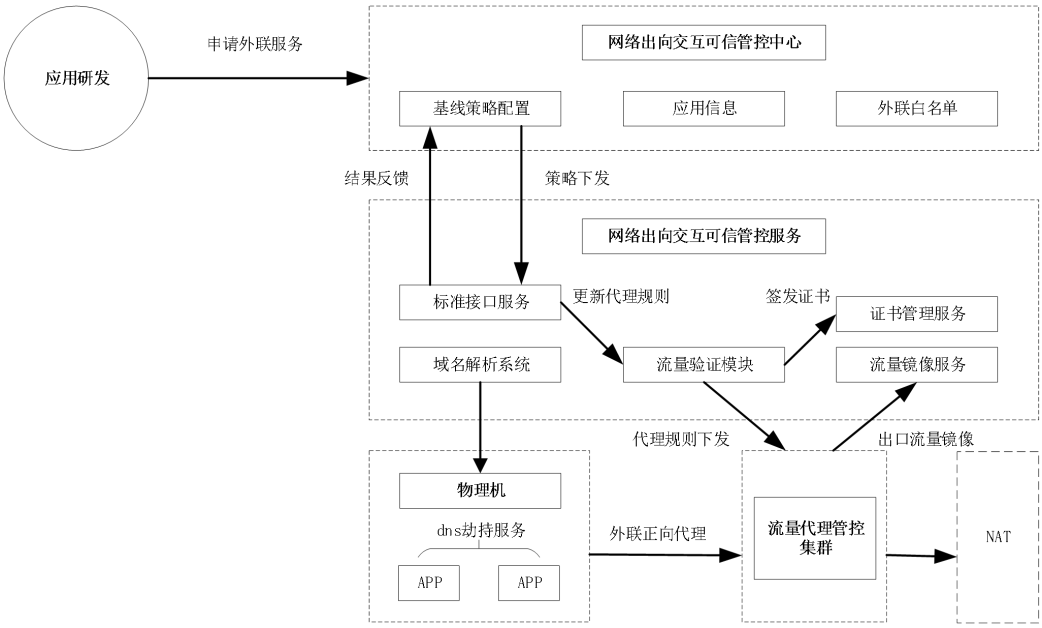


图 B.8 网络出向交互可信架构示例图

B.4 移动端及终端可信构建案例

B.4.1 移动端可信

以IOS移动端的可信管控为例，一份可参考的管控能力架构如图B.9。以IOS安全切面作为切入点，保障策略的控制点不侵入APP的构建流程，仅需集成即可，可以根据下发的配置动态注册/注销切点，最终实现对于线上APP服务的快速管控、防护和止血。

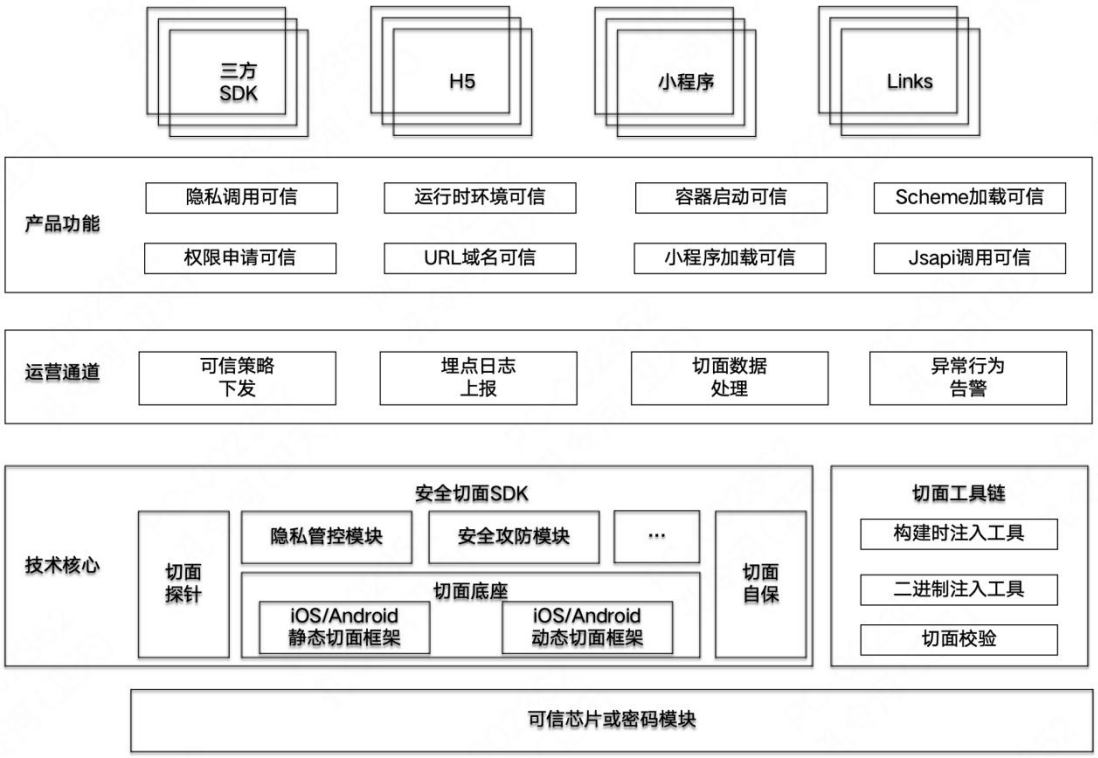
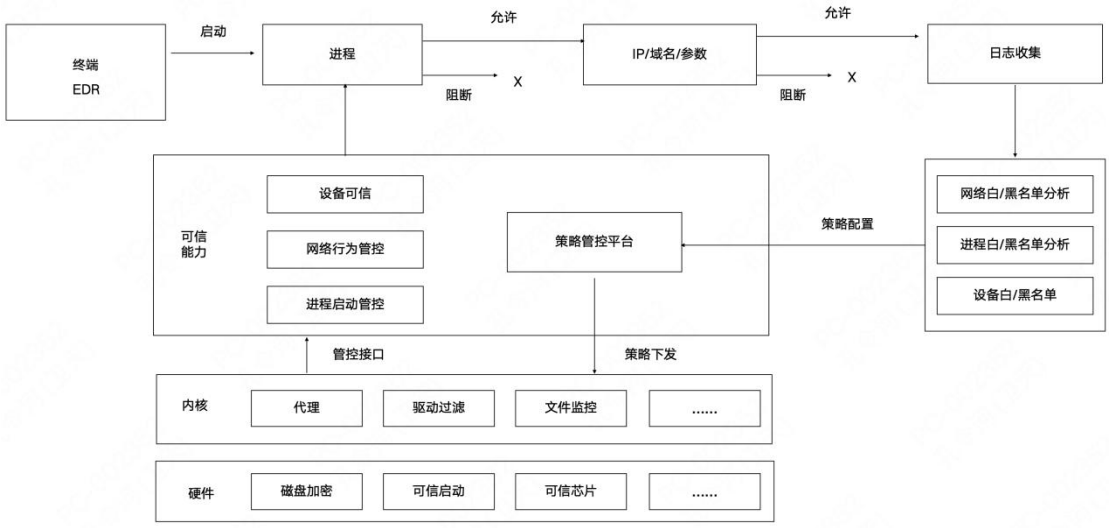


图 B.9 移动端安全可信架构示例图

B.4.2 终端可信

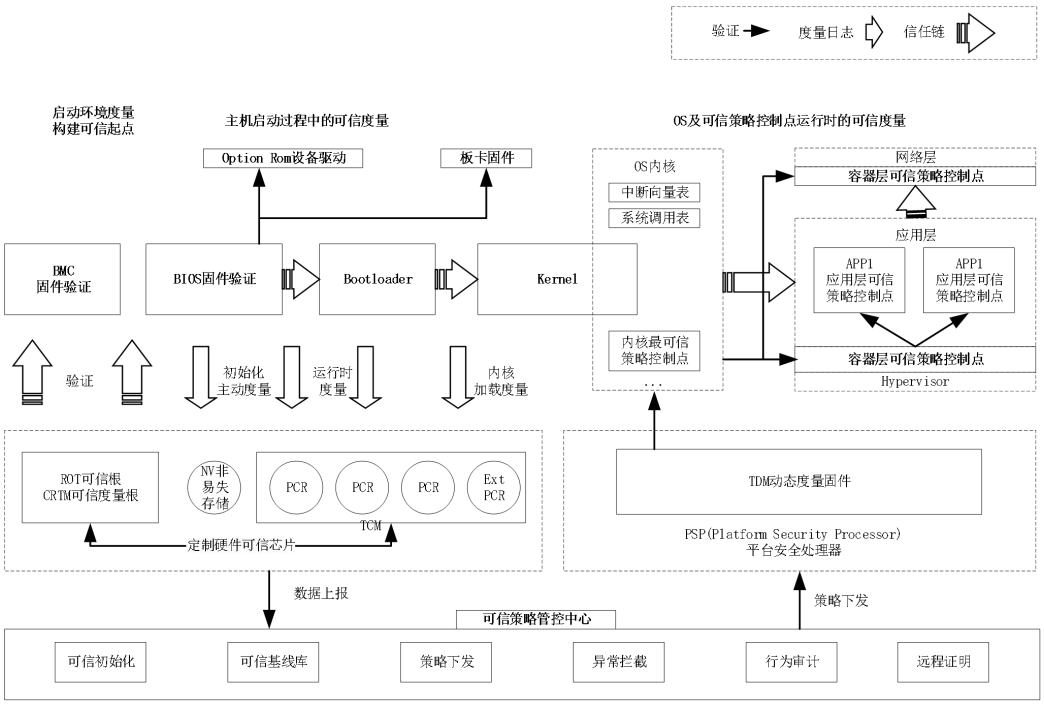
一个可供参考终端安全可信实践的架构如图B.10。办公终端是员工与办公应用的边界，是数据泄露、钓鱼攻击、水坑攻击的重灾区。因此应基于终端管控组件实现设备可信、软件可信、进程可信和网络可信的能力，以有效应对外部复杂的攻击行为以及内部员工的违规行为，规避内外部导致的数据泄露风险。



图B.10 终端安全可信架构示例图

B.5 构建信任链案例

一个可供参考的基于硬件可信芯片的信任链构建案例如图B.11。基于硬件可信芯片提供的可信存储和密码技术能力逐步建立并完善信任链，并将信任机制由硬件可信芯片逐层传递至基础设施层、应用层、网络层，实现全链路的安全可信。



图B.11 基于硬件可信芯片的信任链构建示例图

B.6 可信策略案例

B.6.1 可信策略能力设计

B.6.1.1 网络安全缺陷

HTTP作为主流的七层协议使用广泛，因此网络层可信策略以HTTP协议为例进行重点说明。网络安全的风险主要来源于入参（身份、权限等）、出参（响应时间、响应内容等），面临的威胁主要包括如下方面：

a）身份认证及身份标识缺陷；
b）垂直权限控制缺陷；
c）水平权限控制缺陷；
d）入参不可控缺陷；
e）其他类型攻击等。

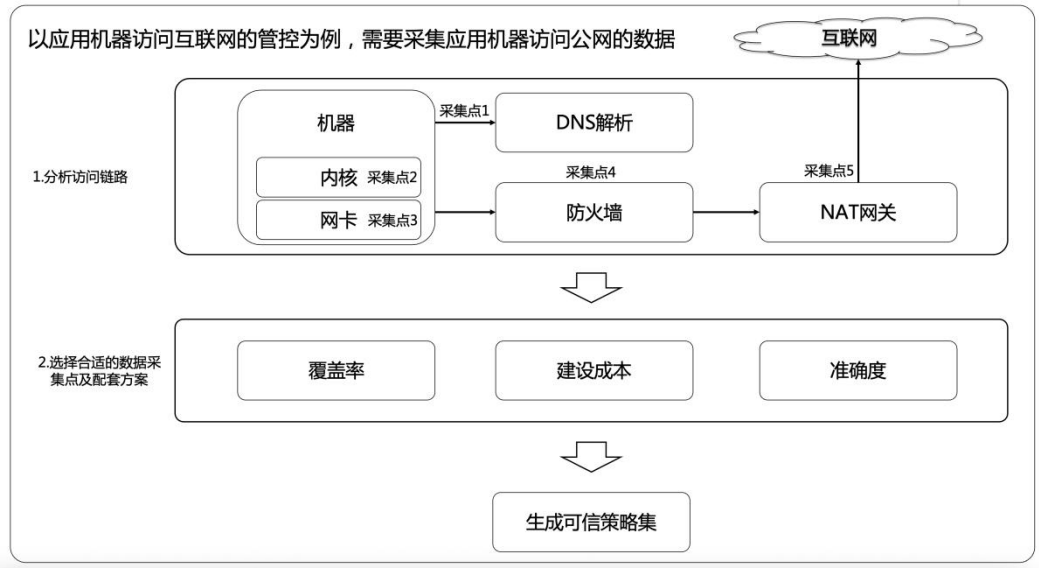
B.6.1.2 策略管控

针对以上安全缺陷风险，结合企业业务现状分析出业务可接受的预期行为并确定策略管控粒度，细化为如下策略内容：

a）服务有效识别；
b）服务注册可信；
c）人员身份认证可信；
d）人员身份会话可信；
e）应用身份认证可信；
f）授权可信；权限控制需遵从最小化及合规化等安全原则：
——默认设置不可信，线上服务默认无权限调用，需通过权限申请并完成审批方可执行，预期外权限先打印错误日志，后进行拦截；
——动态分级授权，通过对环境、上下文、行为序列等多种因素综合判断行为的可信度，实时计算行为可信分，针对不同行为做不同安全等级的实时授权；
——权限及时回收，当无业务权限使用需求时，应及时回收权限；
——合理划分权限，在角色划分上应平衡体验问题及权限问题，高风险场景由安全、合规及隐私部门判断权限分配的合理性；
——不同业务场景的权限申请需设置不同的流程，比较典型由外部机构发起的权限申请应邀请企业合规团队参与评估。
g）语义内容可信。

B.6.2 可信策略模型设计

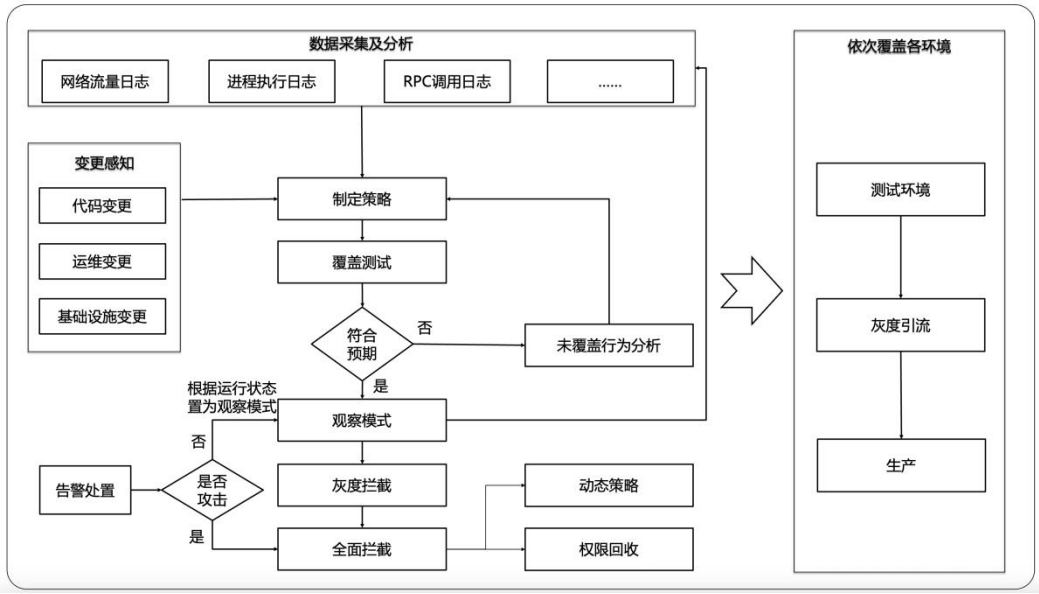
对于可信策略的制定，一个可供参考的网络可信策略生成实践案例如图B.12。



图B.12 网络可信策略生成实践参考案例

预期目标是应用主机访问公网的行为均是可管控的，因此需要收集应用主机访问公网的全量数据。如应用主机访问公网，首先经过DNS解析，然后应用主机构造网络请求，网络请求经过主机内核及网卡进行路由，经过交换机、防火墙、NAT网关等设备，最后路由至公网。根据应用主机的请求链路共需建立5个采集点，分别是DNS系统、机器内核、机器网卡、防火墙以及NAT网关，结合管控目标决定需要采集的数据类型和量级，如需管控到IP粒度，则不需采集DNS数据，如需管控到域名粒度，则需采集DNS数据，综合以上因素确定最优数据采集方案。

对于可信策略的上线，一个可供参考的可信策略生成稳定性保障实践案例如图B.13。



图B.13 可信策略生成稳定性保障实践案例

为建立完善的可信策略变更配套的稳定性保障机制，对于已生成的可信策略，应对策略进行覆盖率测试，确保策略覆盖行为内容的范围是符合预期的；对于首次上线的可信策略，应先以观察模式运行，观察模式是指当可信策略执行点判断为不通过时，不实际拦截行为，

只记录日志，因为日志分析是辅助措施，为了防止行为遗漏，应以实际的执行情况再做一次验证，对于观察模式运行稳定的策略，才能逐步切换到拦截模式。

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范
[4] GB/T 30276—2022 信息安全技术 网络安全漏洞管理规范
[5] GB/T 30847.1-2014 系统与软件工程 可信计算平台可信性度量 第1部分:概述与词汇
[6] GB/T 30847.2-2014 系统与软件工程 可信计算平台可信性度量 第2部分:信任链
[7] GB/T 35279—2017 信息安全技术 云计算安全参考架构
[8] GB/T 36639-2018 信息安全技术 可信计算规范 服务器可信支撑平台
[9] 国家金融与发展实验室《中国数字银行发展报告》