蚂蚁集团
ANT GROUP

ITSTEC

安全平行切面白皮书

蚂蚁科技集团股份有限公司
信息产业信息安全测评中心

2021 年 12 月

顾问委员会主任

李京春　中国网络安全审查技术与认证中心首席专家

顾问委员会副主任

严寒冰　中国互联网协会网络与信息安全工作委员会秘书长

陈世翔　中国网络安全审查技术与认证中心网络安全审查二部主任

陈　鑫　国家市场监督管理总局信息中心网络安全处处长

任　奎　浙江大学网络空间安全学院院长、计算机科学与技术学院副院长

顾问专家

严　妍　中国网络安全审查技术与认证中心产品认证部副主任

李秋香　公安部第一研究所信息安全等级保护测评中心副主任

高　强　国家计算机网络应急技术处理协调中心网络安全三处副处长

于　盟　国家工业信息安全发展研究中心检查评估所副所长

梁振凯　新加坡国立大学计算学院副教授

杨　珉　复旦大学计算机科学技术学院副院长、教授

苏璞睿　中国科学院软件研究所可信计算与信息保障实验室常务副主任、研究员、博导

武成岗　中国科学院计算技术研究所研究员级高级工程师、博导

韩心慧　北京大学王选计算机研究所高级工程师

张　超　清华大学网络科学与网络空间研究院副教授

编制组

蚂蚁科技集团股份有限公司：韦　韬、李婷婷、刘晓舟、顾为群、郑　旻、李　强、孙少磊、靳宇星、边立忠、余　瞰、龙　啸、崔帅华、张恒茂、方　超、贾依真

信息产业信息安全测评中心：霍珊珊、刘　健、金　达、刘润一、张　岩

中国科学院信息工程研究所：梁瑞刚、刘玉岭

鸣谢

杨　宁（鸟哥）、林　鑫、林子敏、李　铮、陈　恺、马传雷、秦承刚、谈鉴锋、徐子腾、赵　勇、董晓康、王少宇、鲍姝睿、华　巍、陈松年、许蓓蓓

前　言

随着云计算、大数据、工业互联网、人工智能等新兴技术的快速更新，中国数字经济蓬勃发展，在国民经济各行业得到广泛应用。数字经济的外延不断拓展，由狭义的数字产业化转向广义的产业数字化，由传统的基础电信、软件服务、互联网等信息产业延伸至工业、农业、服务业等其他非信息行业，成为国民经济重要组成部分。随着数字经济的不断发展，资产价值愈加重要，面临的网络安全、数据安全、隐私保护等威胁和挑战与日剧增，病毒攻击、数据泄露等网络和数据安全事件频发，严重影响国家安全、社会秩序、公众利益。

2021 年国家相继颁布和实施了《数据安全法》、《关键信息基础设施保护条例》和《个人信息保护法》，与之前的《网络安全法》、《密码法》等法律法规，逐步建立了我国较为全面的网络安全保护和数据安全保护的法律体系，对网络安全、数据安全、个人信息保护提出了明确要求。《网络数据安全管理条例（征求意见稿）》、《数据出境安全评估办法（征求意见稿）》等部门规则制度进一步细化了相关要求，表明已经进入一个数据安全有法可依、有法必依的新发展阶段。

数据只有流动才有价值，如何平衡数据开发利用和数据安全保护，实现业务发展和安全齐头并进，是必须解决的重大课题。当前企业架构和业务逻辑呈爆炸性复杂态势，为数字化建设的安全提出了更高的挑战。针对当前数字化建设的安全需求，零信任安全网络架构、内生安全框架和内置式主动防御体系等新型安全体系和理念相继产生，原生安全理念已经成为业界共识。但当前原生安全强耦合式内嵌安全的实现方式，带来了绑腿走路的困境：安全团队与业务团队强耦合，存在投入人员成本高、应急响应时效不足、协调难度大等困难。原生安全的“最后一公里”如何落地，如何实现安全和业务逻辑平行发展，又相互协同，实现低侵入式的安全建设，成为原生安全体系发展的痛点和难点。

针对复杂性数字化业务的安全需求，本白皮书在分析数字化对安全新要求、安全体系面临的挑战和困境的基础上，提出了新一代安全体系—安全平行切面，并介绍了安全平行切面在应急攻防、安全治理与布防、数据安全治理等场景的实践案例。安全平行切面通过嵌入在端—管—云内部的各层次切点，使得安全管控与业务逻辑解耦，并通过标准化的接口为安全业务提供内视和干预能力，以既融合又解耦的方式实现安全防护，为“原生安全”落地提供了解决路径。

目　录

1. 概　述

1.1 国家数字化发展战略对安全的新要求

随着云计算、大数据、物联网、工业互联网、区块链、人工智能等新兴技术的快速发展，中国数字经济蓬勃发展，数字经济成为经济发展中创新最活跃、增长最快、影响最广泛的领域。我国数字经济在产业规模、科技水平、平台影响力、独角兽企业数量等方面居于世界前列，经济增长引擎作用持续增强。根据 2021 年 4 月 25 日第四届数字中国建设峰会上发布的《数字中国建设发展报告（2020 年）》，我国数字经济总量跃居世界第二，成为驱动经济高质量发展的核心关键力量。

数字技术是典型的通用技术，可以在国民经济各行业广泛应用。随着数字基础设施不断完善，云计算、物联网、人工智能等新一代数字技术不断成熟，数字技术加速与国民经济各行业深度融合，产业赋能作用进一步增强，数据成为重要生产要素，深刻影响和改变企业的组织结构、生产方式、商业模式等，加快各行业质量变革、效率变革、动力变革进程。《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》明确提出“加快数字化发展，建设数字中国”，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。未来，我国数字经济的规模和范围将得到极大扩展，成为经济发展的新动能。

中国数字经济蓬勃发展的同时，网络安全、数据安全、隐私保护等威胁和挑战日益严峻，从信息产业领域逐渐扩大到各行各业，包括电信、电力、金融、医疗等，影响国家安全、社会秩序、公众利益。网络安全和信息化是事关国家安全

和国家发展、事关广大人民群众工作生活的重大战略问题。习近平总书记强调：“没有网络安全就没有国家安全，没有信息化就没有现代化。”习近平总书记还深刻阐述了网络安全和信息化发展的辩证关系，指出“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。”

国家高度重视网络安全和数据安全的顶层设计，相继颁布的《网络安全法》、《密码法》、《数据安全法》、《关键信息基础设施保护条例》和《个人信息保护法》等法律法规，逐步建立了较为全面的网络安全保护和数据安全保护的法律体系，重点加强金融、能源、电力、通信、交通等领域关键信息基础设施安全保护，建立网络安全审查制度，强化重要数据、敏感数据和个人信息的保护要求。

在大力发展数字经济，加速数字化转型的同时，必须面对网络安全和数据安全威胁日益严峻的态势，着力解决网络安全和数据安全领域的突出问题，符合国家相关法律要求合规经营，这些新兴挑战也推动行业研究新一代安全体系，实现安全和业务高效协同发展。

本章在 1.2 节简要回顾近年来出现的新兴网络安全体系，在 1.3 节阐述当前安全体系面临的挑战和困境，并在 1.4 节介绍安全平行切面体系。

1.2 国内外相关安全体系

1.2.1 零信任安全网络架构

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，通过主要包括身份鉴别、授权、管理、分析和审计等，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和所提供的服务。

传统的网络安全方法侧重于边界保护，将攻击者拒之门外，同时假定边界内的所有人和所有事物均已获得访问权限。因此一旦攻击者突破边界保护，在内部将被认为是合法访问者，从而可对内部系统造成严重威胁。零信任架构显著优于传统的“城堡和护城河”式网络安全方法。基于这种显著优点和多年的发展，目前，国内外企业已有不少零信任方案落地。典型的如 Google 已上市的零信任平台 BeyondCorp Enterprise、IBM Security 零信任蓝图、阿里云远程办公零信任解决方案和奇安信“支撑零信任安全架构的人工智能信任决策系统”项目。

同时，零信任架构在落地应用中也面临如下挑战：（1）员工思维转变难：当前企业默认其内部环境是可信的，通过防火墙即可实现外在风险的隔离；零信任架构的部署类似于企业基础设施转型，首要任务是转换安全管理的方式，而让员工具备该新理念的思维方式需要漫长的过程；（2）部署复杂性高：零信任架构的部署意味着企业收回安全战场控制权，在各部门应用网络分隔和下一代防火墙，控制网络接入的身份、对象、地点和时间，从内而外地施行控制。从之前单一的边界保护转移到允许对每个应用程序和设备进行身份验证和授权访问的零信任架构绝非易事；（3）代价大，迁移漫长：企业从零开始的部署相对容易，而对于已经包含复杂 IT 环境和大量遗留系统的企业来说，零信任迁移则是一项漫长的任务。

1.2.2　内生安全框架

2019 年，奇安信集团提出了内生安全理念，即需要依靠聚合，从信息化系统内不断生长出自适应、自主和自成长的安全能力。内生安全框架包含三个重点——“理清楚”、“建起来”、“跑得赢”，目的是通过“新管理”，让网络安全体系具有动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控的能力。

内生安全框架以系统工程的方法论结合“内生安全”理念，改变了以往“局

部整改”和产品堆叠为主的安全规划及建设模式，按照系统工程的思想，将安全能力组件化，由规划方法、工具集、模型、架构和项目纲要构成，能够让安全产品和服务相互联系、相互作用，在整体上具备单个产品和服务所没有的功能，从而保障复杂系统的安全。

内生安全有三个关键点：内生安全的关键是管理，管理的关键是框架，框架的关键是组件化。奇安信把各种安全能力组件化，分别以系统、服务、软硬件资源等不同形态，合理部署到信息化系统的不同区域、节点、层级中。各种安全能力组件之间，通过网络和数据进行整体协同，使安全能力全面覆盖信息化所有范围，实现对各个层次的管理。

内生安全模式由数据驱动，通过与安全体系中的能力平台和服务平台有效对接，实现对安全技术、安全运行等各方面要素的有效管理，从而发现和规避黑客利用安全体系里的漏洞发起的攻击，克服人的不可靠性、弥补人的能力不足。

与零信任安全网络架构类似，内生安全的落地也是一套复杂的系统工程，实施的关键是如何部署一套完整的内生安全框架。然而，由于现有信息化系统多为新老结合的模式，往往需要若干年的时间才可以完成老系统的替换任务。因此，如何在现有安全体系的基础上，采用渐进式的方式将安全框架组件化，使其既能适应新系统、又能部署到老系统，进而将安全组件与信息系统进行体系化聚合是当前内生安全落地面临的主要挑战。

1.2.3 内置式主动防御体系

2020 年，中国科学院信息工程研究所在国际上首次提出了内置式主动防御理念，突破了安全优先体系结构等关键核心技术，推动网络空间防御由“被动”转为“主动”。

内置式主动防御强调从分析漏洞利用机理和攻击路径入手，找出信息系统漏洞背后攻击者所利用的信息技术安全脆弱性，从安全需求出发，重新设计、改造现有的信息技术，在芯片层面设计中加入主动安全处理器模块 ASP（Active Security Processor），实现单向物理隔离，使其具备有效抑制、发现、调控、消除自身安全脆弱性造成的安全威胁的能力，变“信息技术 + 安全”为“安全的信息技术”。

内置式主动防御安全结构的主要设计理念如下：（1）在体系结构设计阶段，

安全性需要在系统和芯片级别共同考虑，即需要全面平衡性能、安全性和成本；（2）物理隔离安全性高于逻辑隔离，从物理上对非安全单元进行隔离能够最小化攻击面；（3）ASP 具有最高的访问权限，主要优势在于其能够高效地访问所有 CPU 资源，并收集多维信息来监视恶意行为，同时 CPU 不能以任何方式访问 ASP 的私有资源；其次，ASP 能够主动管理 CPU 或 ASP 中使用的安全机制，而不是由 CPU 调度。

与传统修复漏洞思路不同，由于有效控制了信息技术的安全脆弱性，内置式主动防御不试图消灭漏洞，而是努力使漏洞无法被成功利用。同时，区别于边界防御和纵深防御的“防盗门模式”、零信任的“保险箱模式”，内置式主动防御建立以攻击路径为中心的“藏宝洞模式”。

1.3 安全体系面临的挑战和困境

随着数字经济蓬勃发展，网络安全和数据安全进入新发展阶段，信息系统的安全体系面临着合规、风险、技术三大方面的挑战。

1.3.1 合规挑战

（1）遵守法律法规是数据处理者的法定责任和义务

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《国家安全法》、《网络安全法》、《密码法》、《数据安全法》、《个人信息保护法》、《民法典》“五法一典”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”。数据处理者必须按照要求，接受和通过国家相关部门和机构的审查和测评，不然存在违法运营的风险。

（2）个人信息保护的新挑战

数字经济能够产生高附加值的重要原因之一是数据资源的共享。由于个人信息蕴含了巨大的商业价值，如个性化广告推荐、千人千面营销、个性化推送等个性化商业行为都需要详细的个人隐私数据。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严重违反个人信息保护法。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共享，是个人信息处理者面临的巨大挑战。

（3）数据跨境流动成为重点监管对象

数据跨境流动的价值与风险越来越凸显，数据跨境流动风险与隐忧主要集中于数据的传输、存储和使用三个环节，由于所在国政策和法律的差异甚至冲突，存在数据滥用、敏感信息泄露的风险，甚至影响国家安全。《数据出境安全评估办法（征求意见稿）》中规定，“处理个人信息达到一百万人的个人信息处理者向境外提供个人信息”，“应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估”。这些都对数据处理者提出了更高、更严格的要求，传统的数据治理手段已经不能满足，需要从技术层面进行创新。

1.3.2 安全风险挑战

（1）数字基础设施面临日益增强的攻击威胁

数据交易中心、移动智能终端承载大量重要业务数据和用户个人信息，但数据资产没有进行全生命周期跟踪，存在安全漏洞。近年来针对 IDC 的攻击日趋增加，侵犯数据安全的恶意应用、木马等日益增多，对用户隐私和资产安全构成极大隐患。

（2）数据全生命周期安全防护挑战巨大

在传统企业架构下，各类数据在一张大网内，数据的流入和流出通过固定的采集 / 输出渠道，呈现安全边界固定、数字资产量少、业务复杂度低的特点，依靠网关侧的流量采集再加上人工手动梳理基本可完成数据治理。但是在云计算模式下，数据的产生、流通和应用变得空前密集。数据像血液一样流转在业务的每个环节中，数据链路触及范围更广，动态性更强，在数据收集、存储、使用、加工、传输、销毁等全生命周期都存在着攻击和数据泄露的危险。特别是在数字经济时代，数据附带的价值日益凸显，成为了攻击者重要攻击目标，风险形式日益严重。

1.3.3 技术挑战

（1）复杂性爆炸对网络和数据安全防护挑战空前

集成电路工艺、计算机体系结构、云计算等技术的快速发展，大大提升了系统的计算能力和存储规模，而且使得业务实时弹性扩缩，但是带来了系统边界模糊、引入更多未知漏洞、大量用户数据隔离困难，给安全防护工作带来了巨大挑战。在数据资产海量化、使用方式多样化、共享与流动刚需化、数字业务复杂化

的情况下，要满足数据有效使用的同时保证数据使用的安全性与合法，将会大幅提升网络和数据安全防护的复杂度，亟需采用新技术来应对挑战。

（2）业务和安全深入耦合的原生安全面临两难困境

传统的边界安全或者外挂式安全已经很难满足复杂性爆炸场景下的安全保障工作的需要。原生安全以内建安全、主动防御、整体防御为主要特点，已经成为业界应对挑战的共识。但是大型数字化业务在实践原生安全时，容易落入一个两难困境：原生安全推动业务和安全深入耦合，导致业务和安全经常性冲突。比如，在安全治理时，安全团队设计的关键安全增强组件，可能因为业务需求变更回滚，导致安全增强组件前功尽弃。业务和安全深度耦合在漏洞应急修复的时候更加力不从心，表现在：安全团队需要小时级的应急响应，而业务团队由于功能、性能和稳定性测试要求无法满足小时级的应急要求。安全与业务深度耦合导致的“绑脚走路”困境显然不是安全未来的出路。

1.4 新一代安全体系——安全平行切面

针对当前数字化建设的安全需求，零信任安全网络架构、内生安全框架和内置式主动防御体系等新型安全体系和理念相继产生。但安全体系建设往往由安全团队独立完成，虽然安全体系的覆盖范围是贯穿整个企业架构的（例如我们熟知的纵深防御体系），但与企业架构及企业经营业务流程完全独立，因此安全体系建设往往滞后于企业架构的演进速度，往往每一次新型技术给企业架构带来的演进都可能对已有安全架构带来巨大的影响。为了满足早期业务快速发展的诉求，安全架构一直以外挂式的防护模型保障业务发展，但随着网络安全、数据安全、个人隐私保护等监管要求的加强，由于安全体系仍处于企业架构范围之外，安全治理需求开始对企业已有的技术、应用、数据和业务架构带来强大冲击。

当前企业架构和业务逻辑呈爆炸性复杂态势，特别是大型数字化业务，系统、网络、应用、供应链都在高速发展和快速变化，云上业务和安全边界实时弹性扩缩，进一步加剧了安全问题。以前在小规模场景下简单的安全问题，在快速变化的复杂性爆炸场景下都变成巨大的挑战。比如最基础的数字资产盘点，在复杂性爆炸场景下，准确、全面、及时地刻画网络、设备、系统、应用、模块、数据等资产，对于整个业界都是一个巨大挑战。

单个安全能力的提升无法应对巨大挑战，在业务系统架构中应默认集成安全体系而非单个安全能力，使安全体系提供的安全服务原生化，与业务系统紧密结合产生正向业务价值。未来业务系统与安全体系共同演进是发展趋势。安全服务原生化，与业务系统建设完毕之后再提升安全能力相比，可以大大节省建设成本并提升安全有效性。

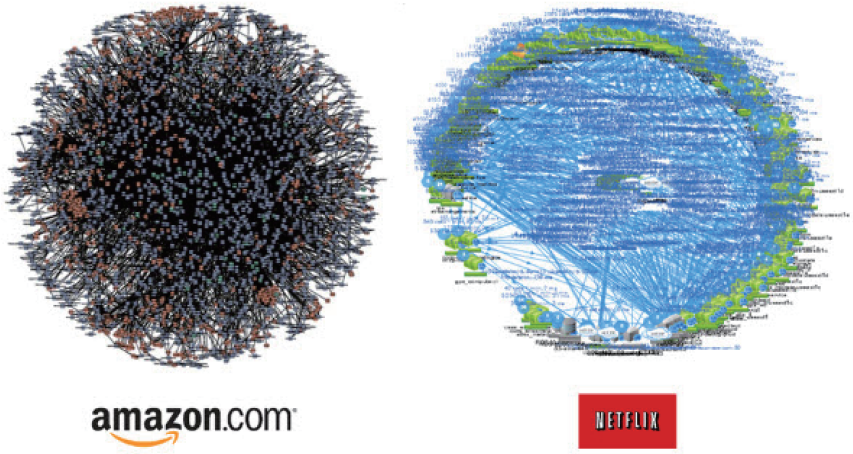

图 1 复杂性爆炸业务场景 [1]

相对于传统外挂式安全，原生安全以内建安全、主动防御、整体防御为主要特点。但当前原生安全普遍采用强耦合式内嵌方式实现，虽然提升了安全防御能力，但是带来了绑腿走路的困境：安全团队与 IT 团队同步规划、同步建设的安全增强组件，因为基础设施的缺陷或强业务需求而回滚，导致安全建设前功尽弃。原生安全的“最后一公里”如何落地，如何与企业架构和业务逻辑平行发展又相互协同、实现低侵入式的安全建设，这些都是原生安全体系发展的痛点和难点。

在数字化业务复杂性爆炸，强耦合式的原生安全可行性低的困境之下，原生安全的未来应该走向何方？企业需求是业务和安全能够融合在一起但又相互解耦，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。原生安全需要一个正交融合的平行空间，以既融合又解耦的方式进

1 图片来源：https://www.divante.com/blog/10-companies-that-implemented-the-microservice-architecture-and-paved-the-way-for-others

行安全防护，非常好地满足了企业建立“原生安全”能力的需求。

在 1997 年施乐帕洛阿尔托研究中心的 Gregor 等学者在著名的 ECOOP 编程语言会议上提出面向切面编程 (Aspect-oriented Programming，AOP)。研究发现，面向对象编程（OOP）不能解决所有的问题，特别是涉及到大量类 (Class) 的横切（Cross-cut）系统性功能很难用面向对象编程（OOP）解决。而面向切面编程（AOP）通过预编译、运行时动态代理、注入等方式能够在不修改原码情况下给程序的正常业务逻辑中动态添加或修改功能，能很好解决上述问题。面向切面编程（AOP）在 AspectJ 和 Spring 等项目中得到应用。

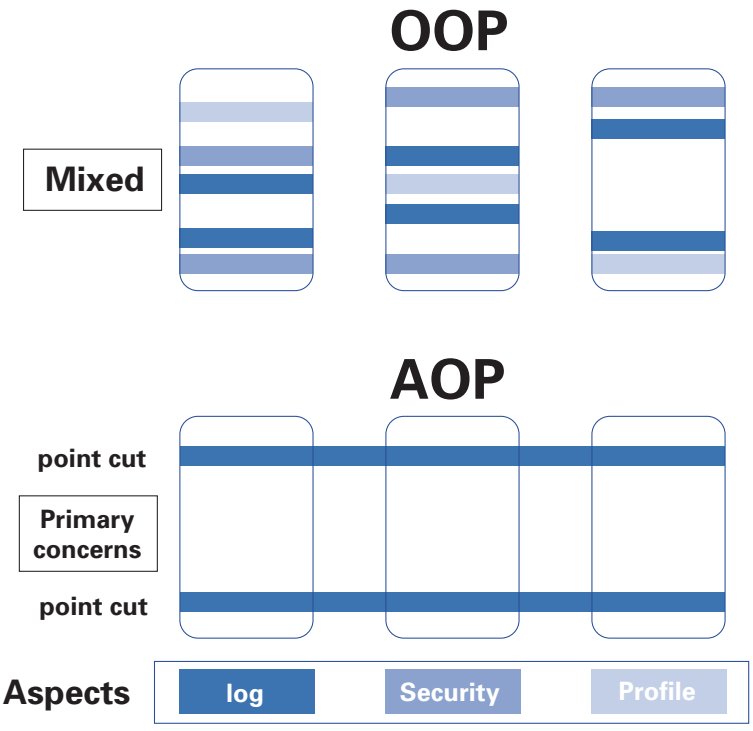

图 2　面向切面编程（AOP）思想

将编程语言环境下的面向切面编程(AOP)思想推广应用到安全体系建设中，构建与业务正交融合的安全平行空间，在不修改业务正常逻辑的情况下，实现更高维度的安全防护，称之为安全平行切面。安全平行切面的定义：通过嵌入在端—管—云内部的各层次切点，使得安全管控与业务逻辑解耦，并通过标准化的接口为安全业务提供内视和干预能力的安全基础设施。安全平行切面是一种创新的安全体系思想，是实现“原生安全”的一条可行路径。

安全平行切面能够更好地应对复杂性爆炸带来的安全挑战，具备三大显著优点，包括：

（1）感知覆盖能力强

感知覆盖是安全领域“看得见”的基础能力，做不到感知覆盖就很难保障系统安全和数据安全。由于系统复杂性和碎片化导致想要做到感知覆盖挑战艰巨：在微观层面，应用内部行为的内视和细颗粒度数据的流转追溯难；在宏观层面，网络和数据安全态势感知更加不易。安全平行切面技术将安全基础设施融入应用和系统内部，且可以根据安全需求来调整感知目标，能极大的提升感知覆盖能力。

（2）快速应急攻防响应

在安全应急时往往需要快速发现和阻断攻击链，并且实现低漏报、零误报。但是让业务团队快速修补漏洞并不现实，由于业务系统的复杂性，导致补丁修复需要大量的测试，修复时间比较漫长。正交融合的安全平行切面能够在业务漏洞修复之前，快速阻断攻击链，达到快速应急响应的目的，保障业务系统安全连续性运行。

（3）高效的安全治理与灵活安全布防

在复杂性爆炸的场景下，在安全治理上的投入经常远大于做安全攻防的投入，甚至超过 80% 的安全成本是安全治理投入，导致治理的效率往往比较低。正交融合的安全平行切面可以支撑对业务的高效安全治理。再进一步，安全需要灵活部署安全阵地。攻防是人与人的对抗，核心是知己知彼。如果所有的防御体系都一样，那么有经验的攻击者总能找到机会来绕过这样僵化的防御体系。安全平行切面与业务解耦和独立演化，可以灵活部署安全防护，能提供差异化的安全防御体系，可以有效应对攻击者的挑战。

安全平行切面将业务部署维度与安全部署维度正交融合——两者既能融合为一体，又能独立解耦，各自平行发展，而不是绑在一起演进。安全平行切面这种正交融合难以用现实的物理场景来类比，它更像是科幻场景中的五维平行时空。安全运营者可以通过这样的平行空间跨维度追踪和阻止恶意网络攻击，或者通过这样的高维空间视角把低维空间展开并做应急的干预或者是深入的审计。通过这样的能力，安全平行切面实现了业务和安全的解耦和共同进化，可以高效保障业务的安全和发展，而不是与业务相互制约。安全平行切面为原生安全落地提供了一种切实可行的方案。

2. 构建安全平行切面防御体系

2.1 安全平行切面架构与实现

2.1.1 总体架构

安全平行切面通过在移动 APP、云端应用、操作系统等应用与基础设施中嵌入各层次切点，形成端—管—云的立体安全防护体系，并使安全管控与业务逻

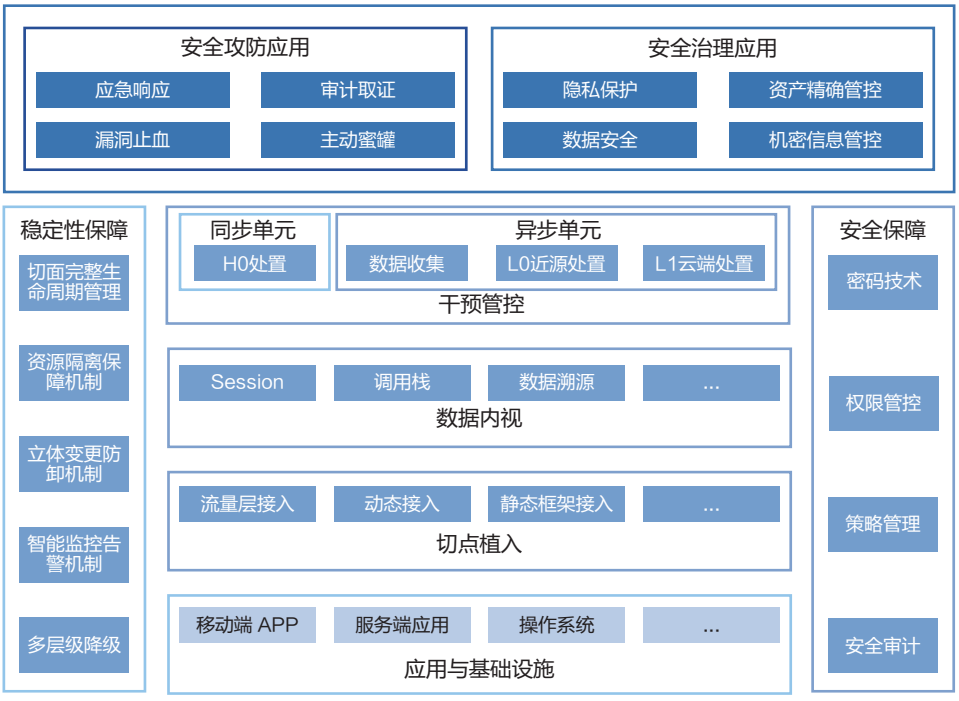

图 3　安全平行切面总体架构

辑解耦，通过标准化的接口为安全业务提供内视和干预能力，从而达到网络安全和数据安全的微观和宏观感知覆盖，实现应急响应、漏洞止血、数据安全、隐私保护等安全攻防和安全治理。安全平行切面由切点植入、数据内视、干预管控、稳定性保障、安全保障等模块组成，其架构如下图所示。

核心技术点包括切点植入、数据内视和干预管控，下面分别介绍一下：

（1）切点植入

切点植入是选取业务关键逻辑处理点，并将安全逻辑嵌入其中的机制。切点植入支持多种方式，如流量层（网关 /Service Mesh）接入、动态（AOP/Hook）接入和静态框架接入。通过在技术栈的各个层次，如操作系统内核、应用程序、移动 APP 中植入大量切点，来支撑安全功能实现。不同层的切点集合决定了安全切面的内视和管控能力触达范围。

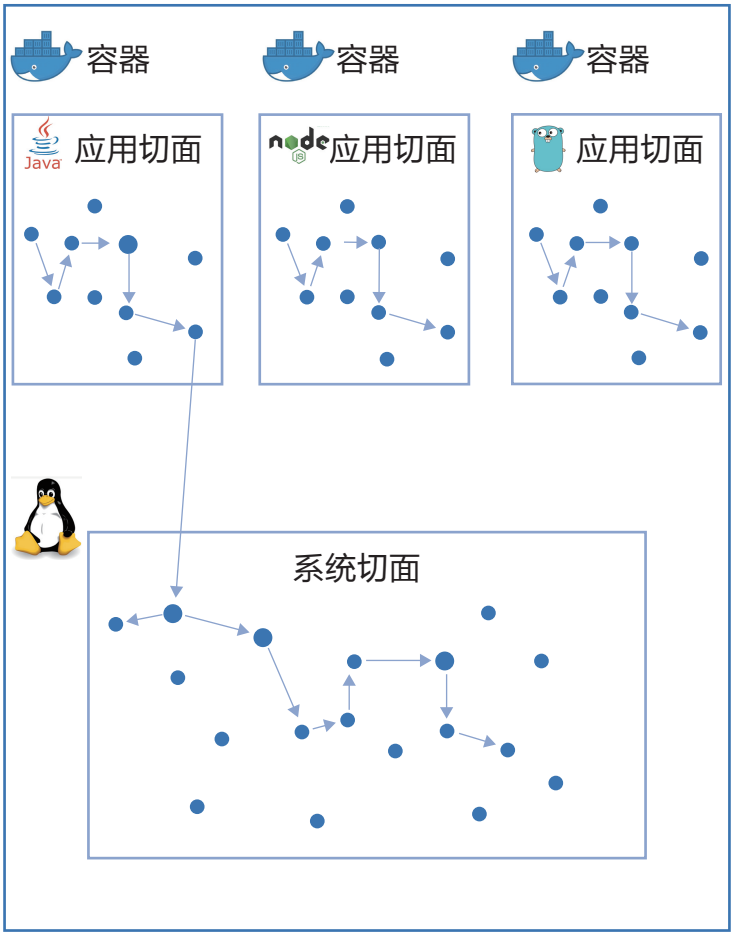

图 4　切点植入

（2）数据内视

这是与外挂式安全的最大区别。由于安全平行切面深入应用逻辑内部，具有强大的数据内视能力，不需要经过序列化与反序列化等转换过程即可直接访问应用内部数据，包括 Session 应用上下文、Session 安全独立的状态空间、RPC 调用的出入参、调用栈信息等，使攻防和治理效果得到质的提升。

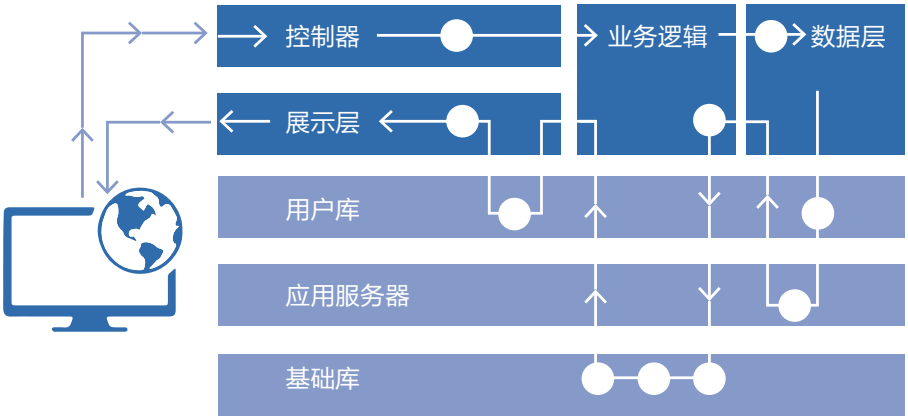

图 5　深入业务逻辑的数据内视能力

（3）干预管控

干预管控通过同步单元和异步单元实施，其中同步单元进行高速轻量级处理（H0），实现快速的安全阻断工作；异步单元负责数据收集和比较复杂的操作，支持本地的 L0 近源处置、云端的 L1 离线处置等。干预管控需要有严格的能力约束，需要分级分类限定能力和资源，防止安全能力被滥用。

2.1.2　建设要则

安全平行切面防御体系支持从应用和基础设施构建不同层级的安全切面，实现各层级的安全管控，也支持多层级安全切面相互联动形成整体防御体系。下面从分层实现、联合防御、安全稳定保障等方面给出安全平行切面防御体系的建设要点指引。

（一）分层建设

安全平行切面是一个跨应用和基础设施的管控体系，切点可以内嵌到移动 APP、流量网关、服务端应用、操作系统等不同层次的业务逻辑位置，实现全面、高效、精确的监测，阻断复杂攻击。根据自身技术和业务特点采用不同技术手段实现切点植入，如下表所示。我们在实践中发现各层切面有各自的优势，底层的

切面（如操作系统）并不能替代上层的切面（如应用），反之亦然。

表 1　不同层次安全平行切面

	移动应用 APP	流量网关	服务端应用	操作系统内核
切点植入方式	编译前的代码注入或运行时动态代理	采用服务网格的 sidecar 的流量接管机制实现植入	采用语言或应用框架内置机制，如 Java 的 instrument	利用系统内核提供的运行时机制实现植入，如在 LSM 层植入切点
优势	抵御第三方 SDK 引入的隐私合规和安全风险；满足日益严格的移动 APP 监管要求	屏蔽编程语言差异，对服务流量行为进行细粒度安全控制，包括支持服务间认证和加密	深入业务逻辑，感知应用上下文，抵御隐私合规风险	性能影响低，通用性好；主要用于对内核漏洞、系统组件漏洞修复

（二）多层联动

不同层级的安全平行切面可以有机配合，形成对复杂业务系统的整体防御体系。安全平行切面的整体防御体系由切面基础设施、各层级安全切面、切面服务组成，支撑资产精确管控、保护线上“带伤”业务、数据流动风险闭环、恶意攻击精确拦截等应用，如下图所示。其中切面基础设施包括可信信道、热部署、安全保障、稳定性保障等基础模块组成。安全切面由业务系统不同层级的切面组成，如移动端安全切面、网关切面、服务端应用安全切面、系统安全切面、Mesh 切面等组成。切面服务包括内视感知、异常检测、攻击阻断、跨应用追溯、沙箱隔离等。

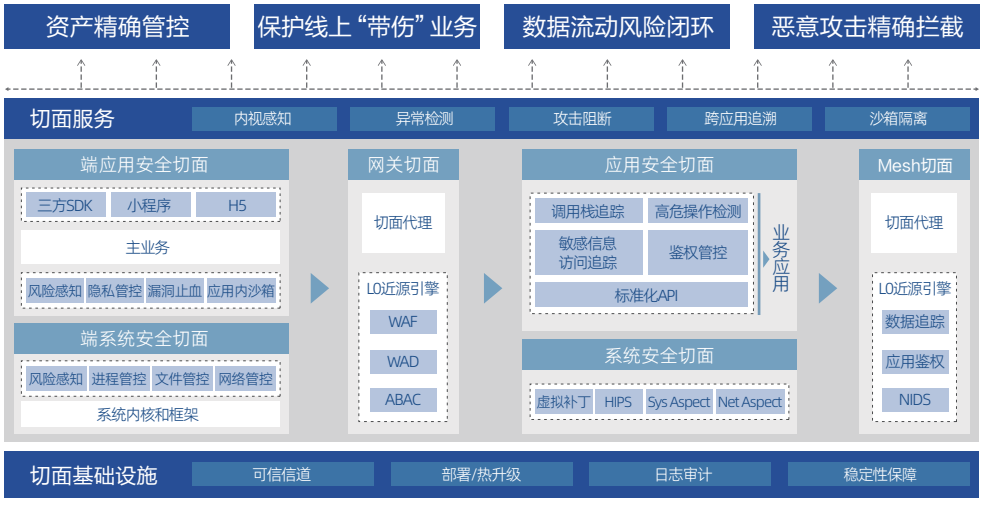

图 6　多层级安全平行切面的防御体系

基于安全平行切面的整体防御体系在数据流转的各业务层级建立安全切面。通过各层级安全切面的有机配合，实现数据流转的全流程追溯，对复杂攻击进行多层次检测、阻断，并通过不同安全切面之间的协同管控联动、威胁检测数据融合等机制，实现复杂业务系统的纵深防御，充分发挥了整体防御的优势。

在攻防对抗实践中，通过切面拦截攻击后仍需对漏洞进行后续修复升级，让切面上的安全拦截工作保持在简洁可控的状态，避免滥用导致产生额外的复杂性问题。切面和 DevSecOps 安全代码升级等中长期治理工作相互配合，达到更好的安全治理、防护、对抗的效果。

（三）稳定保障

安全平行切面融入应用和基础设施，其自身的稳定性至关重要，从以下几个方面来实现稳定保障：（1）做好切面使用资源的限制与隔离，避免过度使用控制资源，避免切点隐蔽死锁问题，避免设计过度复杂的安全逻辑等；（2）安全切面组件要进行能力分级管理，安全能力不能够不加限制对所有安全组件开放，防止切面能力被滥用；（3）要具备完善的变更防御机制、智能监控告警和多层级降级保障机制，建立运营保障规范，安全策略和变更过程要符合可灰度、可监控、可回滚的稳定性要求。

（四）自身安全保障

作为一个横跨应用和基础设施的超级管控平面，安全平行切面自身安全保障极其重要，从以下几个方面来保障：（1）切面组件和安全策略都要有签名验证，防止被篡改和滥用；（2）组件的安装升级和安全策略下发等特权操作要接入强身份认证和权限管控，必须落实到人，降低被攻击者冒用风险；（3）切面内部信息传输存储要采取强加密管控，防止敏感数据的泄漏；（4）切面管控平面要与外界隔离，减小攻击面；（5）切面管控要防止被攻击者绕过。

（五）碎片化适配

随着长时间演进，大型复杂环境的应用系统、操作系统、云等基础设施，少则有十几个，多则有成百上千个软件版本组合，呈现碎片化特征。安全平行切面需要充分考虑碎片化场景需求，适配不同版本基础设施环境，为上层业务提供相对统一的安全环境和安全机制，拉平基础设施环境的差异，而不是为特定环境定制化实现某个性能指标的极致优化。这样才可以更好地适用于不同应用场景，为

业务系统和安全系统的快速迭代提供高效保障。

下面介绍各层次切面的参考实现方案。

2.1.3 移动应用端 APP 安全平行切面

移动应用特别是平台型 APP，存在大量第三方 SDK、小程序等第三方代码。由于缺少运行时监测和管控的技术，无法对线上的实际调用行为进行观测，存在盗取用户敏感数据、推送恶意广告等风险，严重影响 APP 的合规性。移动应用 APP 端的安全平行切面技术可以提供移动应用 APP 的数据内视、行为刻画和业务干预能力，实现针对运行时的威胁发现和恶意收集用户隐私行为的监测和防护。其关键技术点如下：

（1）关键技术

1）代码植入技术

研发切面工具链，可以根据不同的隐私数据获取行为，确定隐私调用相关函数的切点列表，并且可以根据切点列表生成对应的切点逻辑处理代码，并在 APP 预编译期间对 APP 的二进制文件进行自动化的静态符号替换 / 注入或在 APP 运行时加载动态代理，从而可以做到整个切面的过程可以无感接入到业务的研发流程中。

2）端上隐私信息获取监测技术

被切面处理过的目标函数在运行时会进入切面代理函数。切面代理函数会先判断切面开关是否打开，如果没有打开则直接调用之前的逻辑并返回。如果打开了开关，则会拉取对应的切点配置，切面代理函数会通过调用栈、参数和上下文等信息获取到该切点函数调用链路的详情，针对不同的业务场景做出对应的分析判断并上报信息。

3）隐私风险行为检测

根据切面监控到的调用链路数据，可以分析和刻画出业务的实际行为特征并筛选出异常的行为。

4）端上隐私行为管控能力

在检测到异常行为并确认风险后，可通过切面对函数调用进行拦截管控，从而对有风险的隐私泄露或漏洞攻击链路进行管控。

（2）架构

移动应用 APP 端的安全平行切面主要由工具链、客户端 SDK 和云端管控平台组成。下图是移动应用 APP 端的安全平行切面的架构图。移动应用 APP 端的安全平行切面所提供的数据内视和业务干预能力，可以实现不同的安全业务，比如隐私管控、RASP（应用运行时自我防护）和 IAST（交互式安全测试）等。

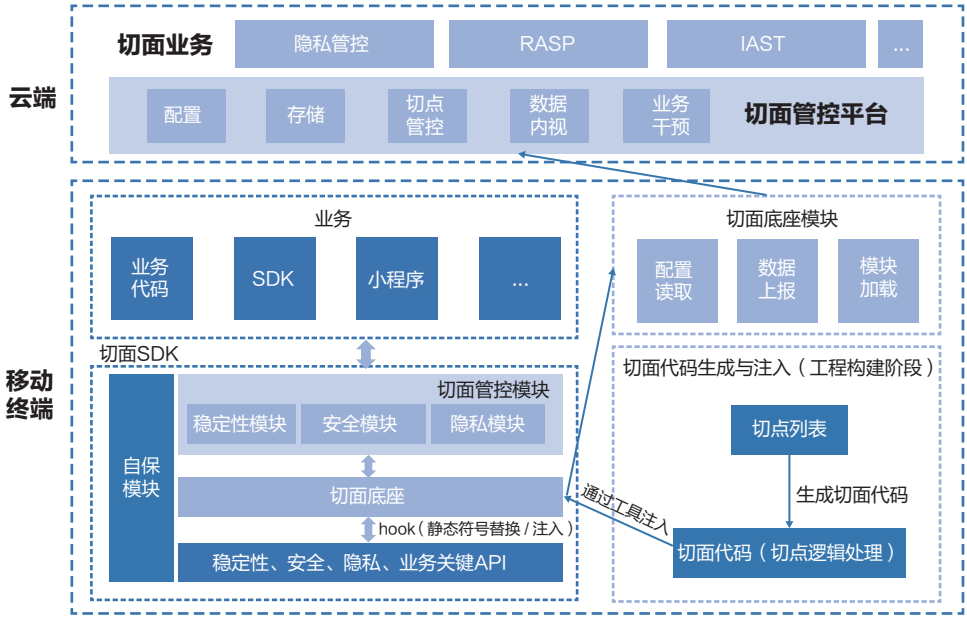

图 7　移动应用 APP 端的安全平行切面架构图

在 APP 构建阶段，切面工具链会根据切点列表生成对应的切面代码，并在 APP 预编译期间对 APP 的二进制文件进行自动化的静态符号替换 / 注入；或者在运行时对目标 API 进行动态代理，整个过程可以无感接入到业务的研发流程中。此外，切面工具链还可以对编译后的 APP 进行切点校验、性能评估和业务影响评估，从而保障切面在线上运行时的性能和稳定性。

在 APP 运行阶段，被插入的切面代码主要分为切面底座和切面管控模块，其中切面底座主要负责配置读取、数据上报和模块加载等功能，切面管控模块负责 具体的切点处理逻辑。不同的管控模块负责不同的业务场景。在 APP 运行期间，切面管控模块通过调用栈、函数参数、返回值和上下文等信息可以获取到每

一条调用链路的详情，针对不同的安全业务场景比如隐私 API 调用、数据和网络请求等做出对应的分析判断和信息上报。

在管控方面，云端在获取到上报的调用链路数据后，可通过大数据分析和算法刻画出业务的行为特征并筛选出异常的行为，并可下发对应的配置到切面模块，对有风险的隐私泄露或漏洞攻击链路进行管控。

2.1.4 服务端应用安全平行切面

服务端或云端是非常重要的安全战场，所有业务数据主要是在云端流转、计算、处置，有非常多的挑战。服务端或云端应用层的缺陷和漏洞是造成信息安全风险事件的主要原因之一。当前数据治理进入深水区后，个人身份识别信息、敏感图片、隐私数据，每一个都是很难啃的骨头，用“绑腿走路”可形象地反映企业应用安全所处的困境。因此企业迫切需要通过服务端应用安全切面技术来解决以上问题：既深入应用逻辑，又和应用解耦，实现安全团队独立维护和管控。

（1）关键技术

以 Java 应用为例，应用安全切面关键技术包括：

1）切点植入

可基于 Java 虚拟机底层字节码修改机制来进行切点植入。选取业务代码中特定函数 / 方法作为切点，在其进入、返回、抛出异常位置注入实现安全逻辑的字节码。在 Java 下有多种字节码修改机制可供选择，比较著名的有 ASM/BCEL 库。

2）数据内视

在切点处，能够获得的被注入函数 / 方法的上下文信息，包括调用栈、入参、返回值等。切点上下文很重要，有了完整的上下文，切面可以支持精确的实时攻击识别和拦截，也可以精确记录和采集数据流动。安全平行切面区别于外挂式安全的主要优势是能够获取细粒度上下文。

3）干预阻断

在切点处，安全逻辑可以过滤和改变函数调用的入参，可以改变函数调用的值和抛出异常，甚至可以在函数执行之前直接返回自定义的对象，也可以在方法

体抛出异常之后重新抛出新的异常，或者改变为正常返回。通过此能力实现对攻击的拦截。

4）模块隔离技术

框架内各个切面模块实现了各自的独立，模块之间互不干扰。类加载阶段，module 优先从自己的路径下进行类查找，如果找不到，则交由上层进行加载，实现类空间的隔离。

（2）架构

服务端应用的安全平行切面主要由切面业务模块、切面底座、切面底座 API、切面业务模块管理、运维管理平台、监控平台组成。下图是服务端应用安全平行切面的架构图。

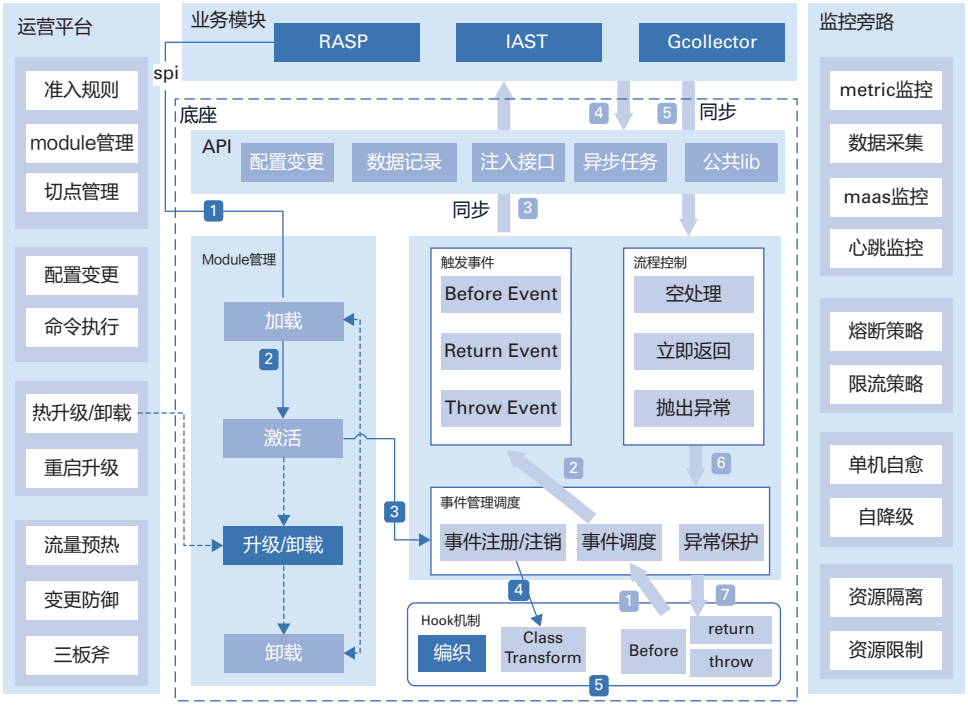

图 8　服务端应用的安全平行切面架构图

切面业务模块：承载安全业务的核心组件，本质是利用切面底座 API 编写的一组切点及对应增强的集合，组合实现特定安全业务能力。比如 RASP 作为切面业务模块存在，实现应用运行时的安全防护能力。

切面底座：封装底层字节码修改机制，提供切点注入、获取切点上下文、日

志统计、配置变更等 API，并负载加载和管理具体的切面业务模块。在 Java 下以 Java Agent 方式实现，实现和目标业务代码运行时融合。

切面底座 API：切面底座暴露给切面业务模块的编程 API，一般包括切点注入、获取切点上下文等切面管理 API，以及日志统计、配置变更等 API。

切面业务模块管理：切面底座的核心部分，实现对切面业务模块的加载、激活、升级、冻结、卸载等等管理动作的支持。

运维管理平台：面向安全技术运营人员，提供对切面业务的运维管理能力：安装 / 升级 / 卸载部署、配置变更等切面模块管理功能。

监控平台：主要承载切面稳定性相关的功能，包括各类监控、熔断、降级、资源隔离等功能。

切面模块的加载流程参考上图绿色序号部分，卸载流程为先冻结后卸载，升级流程为先卸载后加载。各生命周期执行的任务如下：

1）加载：进行切面模块的发现与加载，每一个切面模块拥有独立的类加载器；

2）激活：执行切点注入，将注入点与注入动作进行绑定，切面开始工作；

3）卸载：关闭内存资源与线程资源，需要业务模块确保资源被正常关闭和释放，不引发稳定性问题。

2.1.5 操作系统安全平行切面

操作系统安全的重要性无需赘言，但其面临的挑战却不容乐观。以云端最常见的 Linux 操作系统为例，其复杂度导致近年来各种安全严重漏洞层出不穷，攻击者能够利用这些漏洞实现权限提升、数据窃取、拒绝服务攻击，严重破坏了操作系统的机密性、完整性和可用性。具体来说，当前 Linux 操作系统安全管理上存在如下挑战：

1）Linux 操作系统漏洞曝出的频率越来越高。Linux 的广泛使用吸引了越来越多的安全研究人员进行研究，通过更深入的代码审计以及不断完善的模糊测试工具，发现 Linux 操作系统漏洞的频率越来越高，对漏洞修复带来了更大挑战，在被攻击者利用之前及时完成修复；

2）Linux 操作系统漏洞修复周期长。Windows 和 MacOS 等闭源的操作系统厂商会为用户提供稳定的升级补丁，用户在修复成本投入少。与闭源的操作系统不同，开源 Linux 的漏洞修复往往需要用户深度参与。特别是大型企业会开

发和使用自己的 Linux 内核代码树，导致企业在漏洞修复方面投入大量成本，整个修复过程会涉及到安全评估、代码编写、测试等，周期比较长，留下了很长时间的安全敞口，存在很大的安全风险；

3）Linux 操作系统漏洞修复之后的稳定性难以保证。Linux 采用开源的开发模式，对代码修改的测试要求更高。当漏洞刚被发现时，第一时间的修复代码可能并不完善，如果在测试不充分的情况下，贸然进行修复可能会给系统造成稳定性风险；

4）Linux 下的新型攻击不断出现。一种新型攻击方式是容器逃逸。云计算成为主流部署方式，各类 IT 基础设施迁移到容器系统中运行。但是由于 Linux 下的容器技术是一种弱隔离的技术，容器与宿主机进程共享同一个内核，攻击者一旦进入容器，就可能进行容器逃逸，得到宿主机权限，发起对操作系统内核的攻击。另一种新型攻击方式是无文件攻击。Linux 系统上可以直接执行内存中的恶意代码，无文件攻击方式能够绕过传统的安全软件监测，威胁巨大；

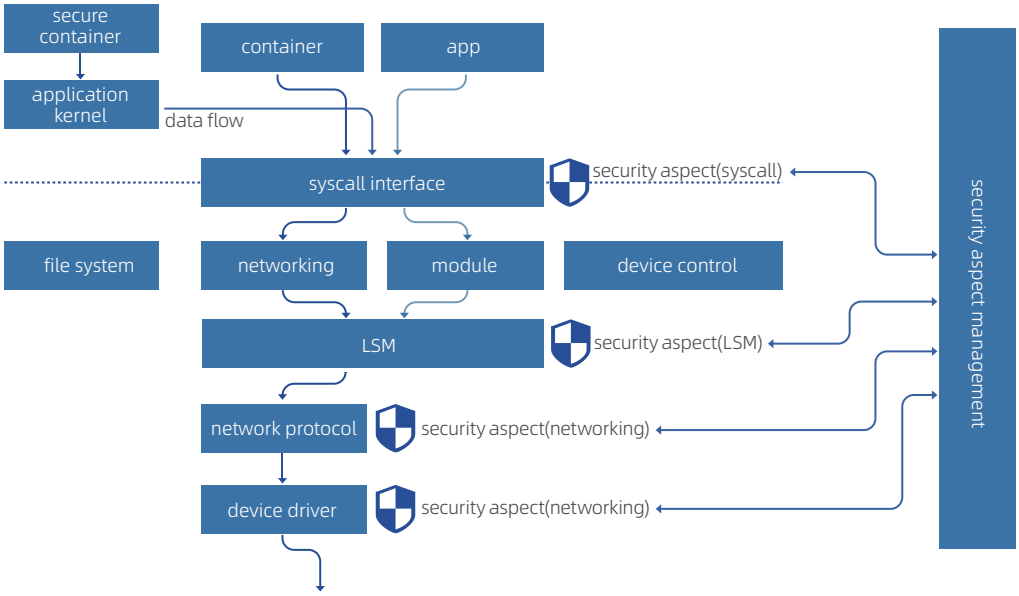

图 9　Linux 操作系统的数据路径

5）Linux 操作系统碎片化严重。Linux 碎片化的问题不仅体现在各个发行版使用不同的 Linux 内核版本上，也体现在即使是同一个发行版，由于内核的升

级推进，企业内部使用的各种 Linux 版本会呈现碎片化分布，给统一的安全管理带来了极大的挑战。

根据数据的流向，Linux 操作系统用户态的应用程序与内核通信会依次经过系统调用层 (syscall)、各种子系统层如文件系统 (file system)、网络 (networking)、内核模块 (module)、Linux 安全模块层（LSM），对于跟硬件交互的 IO 操作还会进一步经过 IO 层、设备驱动层、硬件层等。

在操作系统层引入安全平行切面，将安全能力系统化、透明的注入底层基础设施，在操作系统的整个数据路径上进行切入，既能够实时阻断各类攻击，也能够完成各种安全治理工作。典型的操作系统切面在操作系统内核态和用户态可以植入切点，包括如下几个层次：

系统调用切点层：因为系统调用是应用程序与内核交互的最基本原语，所以在系统调用处植入切点，实现粒度最细的切点管控。

LSM 切点层：内核会在 LSM 定义的各个安全点上调用自定义的 LSM 模块。在 LSM 定义的各个安全点上植入切面插桩程序，可以实现对内核的监控。由于 LSM 的各个调用点表示了程序的行为语义，该层的切点个数大大少于系统调用层切点。

网络切点层：Netfilter 框架在网络协议栈特定的 Hook 点会调用回调函数，用来对网络包进行处理。在内核注册回调函数或者通过 iptables 过滤方式，实现内核网络协议栈的切点植入。在 TC、XDP 相关点上加载 eBPF 程序，可以实现功能更加强大的切点。

驱动切点层：在网卡上注册 eBPF 程序，实现网卡的驱动层 XDP，从而实现切点植入。

安全容器切点层：每个容器都有自己的应用内核，容器中的应用运行需要系统调用层支撑。应用内核实现了应用程序运行所需的系统调用。容器安全切面将安全能力透明的注入容器，作用于应用内核的系统调用层，在重要的系统调用处会记录运行时的关键数据，包括进程启动、文件访问、网络连接、DNS 请求等行为。

（1）关键技术

操作系统的安全平行切面最重要的技术为内核插桩，需要灵活的切入复杂的操作系统内核，并且根据安全策略改变插桩程序，从而构建安全防御能力。在

Linux 操作系统安全切面中，涉及到如下几个关键技术：

1）基于 LSM 的切点植入技术

LSM（Linux 安全模块，Linux Security Module）是一组子函数接口，Linux 内核在执行过程中遇到安全相关的敏感访问时，会调用这些接口函数。根据安全策略实现 LSM 模块的部分或者全部函数，从而实现切点植入。

2）基于 Linux BPF 的内核行为监控和审计技术

BPF 架构的 Linux 内核在接收包时，会以数据包为输入，执行过滤指令。通过允许用户态程序在内核各个 BPF 加载点加载 BPF 程序，用户态的工具可以非常方便的对内核的行为进行监控与审计。

3）安全容器应用内核技术

安全容器应用内核指的是为容器安全运行的独立内核，每个容器都有属于自己的应用内核。应用内核可以使用内存安全的语言编写，从而增强其安全性。应用内核提供了容器应用运行所需的类 Unix 系统调用界面，使得应用无需修改即能够运行在应用内核中。应用内核能够非常方便对系统调用实现进行修改与定制，从而实现安全监控。

（2）架构

操作系统的安全平行切面主要由内核态安全切面、用户态安全切面、容器安全切面组成，安全平行切面的架构图如图 10 所示。

操作系统的安全平行切面作用于系统内核层，通过在各个切点加载对应的安全策略来限制、监控应用程序和容器的行为。

切点包括 LSM、syscall、network 以及能够进行 kprobe 插桩的内核函数等，其中 LSM、syscall、networking 的切点具有监控和拦截能力，内核函数的切点只具有监控能力。

切点作用的范围包括应用和节点的进程、文件、网络、能力、系统调用。通过灵活的在相应的内核子系统切点上加载切面代码，能够精细化的控制应用和节点的行为。

容器安全切面作用在安全容器上。每个安全容器都有自己专属的应用内核。应用内核运行在用户态，实现了传统的类 Unix 系统调用接口，能够非常方便与灵活的对系统调用实现进行修改与定制。为了增强安全容器的监控能力，可以在

应用内核的系统调用层增加统一的监控能力，对重点系统调用进行统一的监控。这些重点的系统调用包括进程创建类如 execve、文件访问类如 open、网络连接类如 connect。

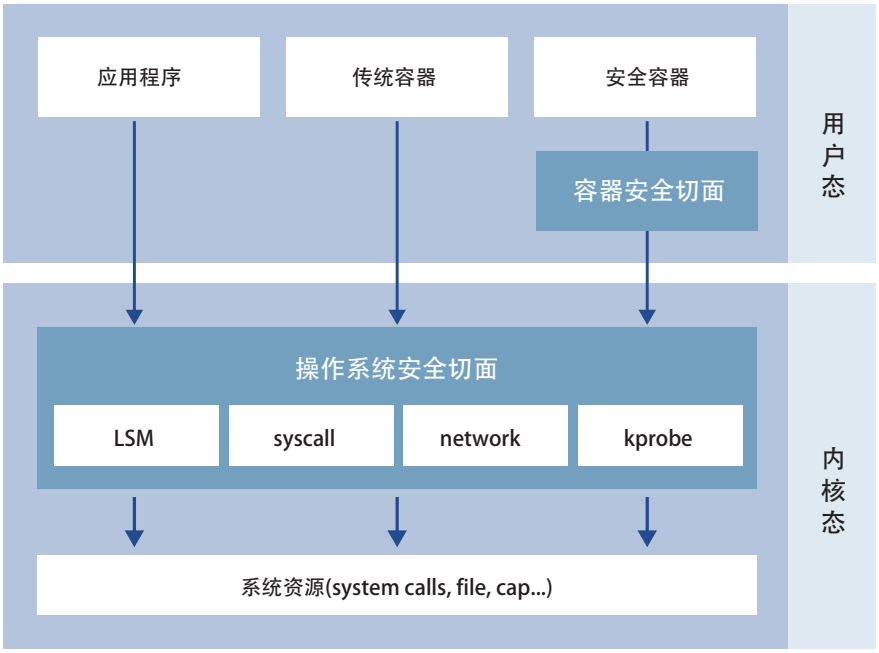

图 10　操作系统的安全平行切面

操作系统的安全平行切面具备多个方面的应用场景：

1）漏洞快速止血：当 Linux 系统中软件或内核曝出漏洞时，可以根据漏洞利用的方式提取相关的缓解特征，生成对应的 BPF 程序，实现快速止血；

2）保护线上业务：出于兼容性和稳定性考虑，线上业务有时不得不带病运行。通过操作系统安全切面，可以在关键路径上进行保护，具备一定的安全防护能力；

3）入侵检测：一般安全工具无法检测一些新型的漏洞攻击。操作系统的安全切面可以通过定制各类安全规则进行检测；

4）数据采集：操作系统的安全切面可以灵活加载相关 BPF 程序实现对资产的信息采集，比如应用端口监听；

5）混沌工程：由于切面的拦截能力，操作系统的安全切面可以用在混沌工程中主动为应用注入网络、系统等相关故障，考验应用的健壮性；

6）支持国产操作系统的安全增强：国产操作系统基本都是 Linux 操作系统，采用高强度的访问控制在安全机制上有所增强，但是在纵深防护以及新型漏洞攻击的防护方面有短板。安全平行切面同样支持在国产操作系统上部署，能够在细粒度高安全访问控制系统的基础上，显著增加系统的纵深安全防御能力，做到快速的漏洞止血、阻断攻击代码。由于安全平行切面的灵活性策略，实现在不升级系统的基础上加载新的安全防护策略，达到安全增强的目的。

2.2 安全平行切面的技术保障

2.2.1 性能保障

安全平行切面会带来一定的性能开销。在实践中一般会要求安全组件 CPU 占用不超过 5~10%，对在线业务响应延时在毫秒量级，线下场景可视情况放宽。不过需要说明，机构和企业不应过度追求极致性能，要为安全治理和应急需求留下空间。

在安全平行切面实践中，主要从以下几个方面控制和优化性能开销：

1）不论在系统层还是应用层，优先选择使用原生的，以及经过实践验证过的轻量级植入机制或框架，将植入动作所带来的开销降到最低；

2）权衡和控制切点处植入代码的复杂度和收益。不过度追求内视和安全能力的最大化，从而避免引入非常复杂的安全逻辑；

3）在线上环境避免引入超高频次调用的切点，通过关注和实测切点被调用的频次，来选择合适粒度的切点。线下环境根据需要可适当放宽；

4）建立安全切面模块能力分级分类管理，区分不同切面组件在线上、线下环境的能力边界，并把能力分级分类管理融入切面业务模块的研发上线流程中，防止切面能力被安全组件滥用。

蚂蚁经过长期优化实践，安全平行切面的性能开销表现良好。以不降级方式通过了最严苛的双 11 流量峰值压力的考验，启动延时、切点耗时、CPU 消耗都完全满足业务要求。

2.2.2 稳定性保障

安全平行切面将管控逻辑嵌入应用和系统，其稳定性会影响到宿主应用和系统的稳定性，所以稳定性保障至关重要。

首先在研发阶段加强质量管理，建立研发标准规范，标准化的 CI/CD 和自动化测试能力，收敛研发过程中出现的稳定性风险；然后在切面上线前、上线后，重点通过故障预防、故障主 / 被动发现、故障处置等方面工作机制，保证安全平行切面及业务系统的运行稳定。

1. 故障预防

基于大多数故障由变更引起的实践认知，安全平行切面进行发布变更或策略变更时，引入相关方交叉评审，确保充分评估风险，控制影响范围；建立前后置立体防御机制，有效避免单层击穿，支撑运维部署、版本发布和安全策略下发等变更场景；变更操作应严格遵循可灰度、可监控、可回滚的要求进行审查。

2. 故障主动发现

通过链路压测、故障演练、预案演练等手段模拟真实流量压力和故障，在模拟故障产生后，全面评估各项告警的可靠性、应急处置动作的及时性、故障预案执行的有效性，从而检验安全平行切面的稳定性和有效性。

3. 故障被动发现

在运行时，通过监控切面指标（如切面注入点耗时、切面抛出异常数、切面拦截量等）和业务进程自身的系统指标（CPU 占用、内存消耗、服务耗时等），进行多层次的综合判定安全平行切面运行稳定性。

4. 故障处置

通过统一的切面基础设施为各个层级的切面提供统一的故障处置应急机制，支持自动降级、模块降级、注入底座降级等多级预案，共同支撑起安全平行切面的故障快速处置，保障业务可用性和稳定性。切面降级功能，即关闭切点处的安全逻辑，以保障业务运行的稳定性。安全平行切面能够根据告警和异常情况有层次地执行降级预案。只有在主机负载过高或安全情况持续恶化的情况下，切面才会开启自动降级。

2.2.3 安全保障

安全平行切面是一个横跨所有应用、所有基础设施的超级管控平面，所以安全平行切面自身的安全防御也至关重要。

在研发阶段需要加强安全质量管理，建立黑白灰盒自动化安全测试能力，研发过程收敛安全漏洞风险。线上运行面临的威胁主要包括攻击者非法获得控制权和敏感数据泄漏，安全平行切面从以下 3 方面措施进行安全保障。

（1）防范潜在攻击者获得控制权的机制

对于上层安全业务和底层基础设施建立分层防御机制，其中切面底座具备切面加载管控和切点权限管理的能力。

1）切面模块的上线发布，必须经过签名验证才能发布，做到安全可控；

2）只有经过合法性验证，切面底座才能加载和启动切面模块；

3）在移动应用 APP 等不可信环境下，开启切面模块的自保护，采用代码混淆技术，加大攻击者的攻击难度；

4）只有通过企业统一的身份管理系统 IAM 才能访问切面管控平台，对所有操作施行严格的账号和权限管理。权限检查内置于安全平行切面中，并可授予针对安全平行切面对象（切面业务模块、宿主应用、安全策略）的细化权限，保障切面策略下发来源合法；

5）所有平台侧和端上的配置变更、状态变更都记录日志，并提交日志审计系统，进行安全审计。

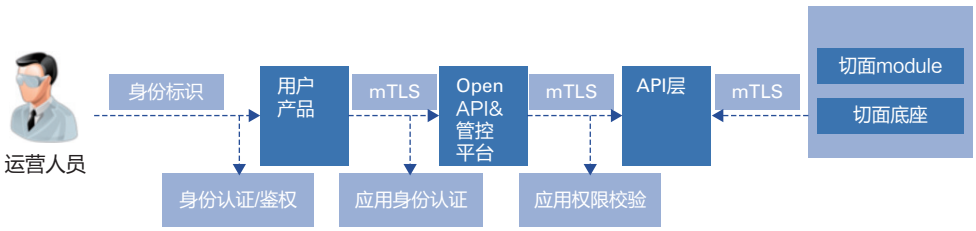

图 11　身份和权限管控机制

（2）对敏感数据进行管控

由于安全策略可能反向推导出攻击手段，所以安全策略内容按照敏感数据进行管控，涉及到敏感数据的切点只允许在同步单元内部操作，不允许明文传输和落盘。

（3）常态化攻防演练发现自身脆弱性

定期开展针对安全平行切面的攻防演练，通过真实的渗透攻防，有效地评估系统的脆弱性，采取有效措施提升安全水位，主动降低风险。

3. 安全平行切面实践案例

下面介绍安全平行切面在相关应用场景下的具体实践案例。

3.1 应急攻防实践

在安全应急攻防时，往往需要快速阻断攻击链，并在有条件的情况下向主动蜜罐引流。让业务团队快速修补漏洞并不现实，在大型复杂环境中一个漏洞修复往往需要大量的测试、灰度工作，甚至有十几个碎片化版本匹配测试，注定修复时间比较漫长。在应急攻防方面，正交融合的安全平行切面能够在各种场景下，实现快速阻断攻击链，具有很好的应用效果。

3.1.1 漏洞“止血”

（1）需求

应用层的缺陷和漏洞是造成信息安全风险事件的主要原因之一，主要面临注入攻击、身份认证、敏感数据暴露、访问控制、跨站脚本攻击、远程代码执行等安全威胁。防范应用层的威胁，仅依靠边界防护是不够的。例如，传统网络防火墙无法有效检测到对 Web 应用程序的恶意输入，而 Web 应用防火墙的误报率高且容易被绕过。

防范应用层安全威胁，安全防御机制需要深入应用的内部，和业务深入耦合，但这样一来安全和业务团队的工作节奏又经常冲突，常给业务开发人员带来较大负担，安全漏洞也常不能及时得到修复。在企业内部部署了大量应用的时候，一旦出现安全漏洞，及时有效地修补安全漏洞将会是投入巨大的事。以某大型互联

网企业修复 Fastjson 的安全漏洞为例，为了彻底修复 Fastjson 漏洞，投入了大量的人力，并对业务产生比较大的干扰。而且一些历史遗留业务代码，甚至可能存在无人维护的状态。

当生产环境的应用出现安全漏洞时，第一时间需要解决的问题便是漏洞防护，实现止血。如何在发现安全漏洞时及时大规模止血？如何确保所有应用的漏洞都可以及时修复？如何降低投入成本？

（2）解决方案

基于安全平行切面构建应用运行时安全防御系统 RASP，将检测和防护策略直接植入到被保护应用的服务端应用或移动 APP 中，以提供函数级别的实时保护能力，达到有效防御应用安全风险、发现潜在安全威胁的目的，具备流程控制、多元化注入、配置变更等能力。应用运行时安全防护架构如下图所示：

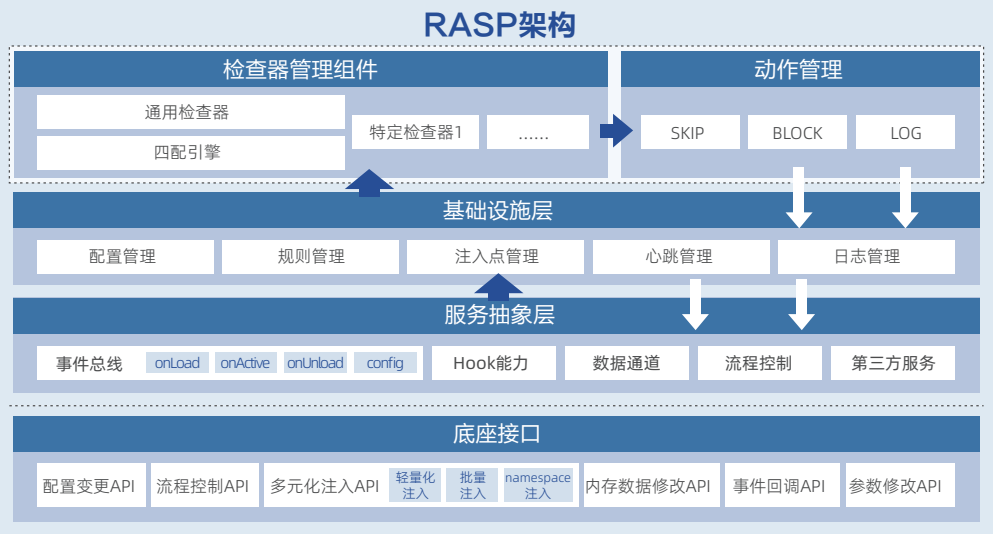

图 12　应用运行时安全防护（RASP）架构

安全平行切面可以针对多种类型的漏洞（远程命令执行、敏感数据泄露、非法文件 / 网络访问、SSRF、XXE、以及各种反序列化漏洞），提供了检测和加固方案；针对各种常见的 Payload 行为（数据库访问、文件操作、命令执行、以及内存驻留等），提供了监控、识别和检测能力。安全平行切面与应用解耦，具备后续独立升级能力，对业务的影响降到最低。

以 2021 年 12 月肆虐互联网的 log4j2 漏洞（CNVD-2021-95914）为例，使用安全平行切面进行应急止血，选择 log4j2 下 JndiLookup 等相应切点，开启阻断即可。相比传统修复漏洞方式有以下显著优势：

1）在官方补丁发布前，就可提前下发策略，实现及时止血，避免了漏洞爆发后的慌乱，影响业务安全运行；

2）止血方案适配各种环境，不用考虑与 log4j2 版本兼容问题；

3）实现精确匹配，既不会误拦截，也不会被绕过；

4）由于安全和业务解耦，止血方案不需要业务的过多参与，缩减应急时间和人力投入，保证了业务系统持续稳定运行，体现了应对危机的强大能力。

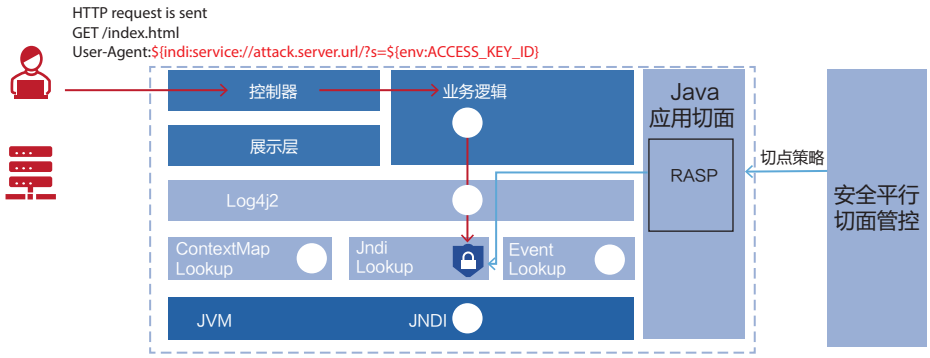

图 13　log4j2 漏洞止血方案

（3）效果

安全平行切面深入业务内部，具有业务内视能力，使得安全切面的数据能够一定程度刻画业务的行为特征，对应用代码安全分析也有很大帮助。

相比于 WAF，安全平行切面带来明显的益处，主要体现在以下几个方面：

1）不受网络协议限制，可以支持多种协议；

2）极低的误报和漏报，RASP 运行在应用内部，监控底层危险操作，和上层业务解耦，上层业务的复杂度不会影响检测质量，失败的攻击不会触发检测逻辑，触发到检测逻辑的攻击必然是有效攻击；

3）具备对抗未知漏洞的能力，RASP 运行在应用内部，可以获取运行时上下文，能够识别异常的上下文数据（堆栈等），可以对抗未知的漏洞。

3.1.2 主动蜜罐

（1）需求

蜜罐技术通过设置一些作为诱饵的主机、系统、虚拟主机或信息，诱使攻击者发起攻击，从而捕获到黑客信息进行分析，了解攻击使用的工具或方法，推测攻击目的和动机，能够让防御者了解所面临的安全威胁，进而通过自我防御手段增强系统网络安全防护能力。

在现实场景中，由于蜜罐一般是守株待兔被动等待攻击者的入侵，蜜罐的诱骗成功率不能完全保证，需要一种更高效的手段将攻击者诱骗进入到蜜罐中。

（2）解决方案

被保护业务部署切面，开启攻击检测和拦截。蜜罐控制系统接入攻击日志，在提前部署好的蜜罐中重放攻击流量，蜜罐收到请求后会响应攻击者的流量，诱骗攻击者以为蜜罐是用户内部的真实业务，攻击者会在蜜罐中“继续”入侵行为。

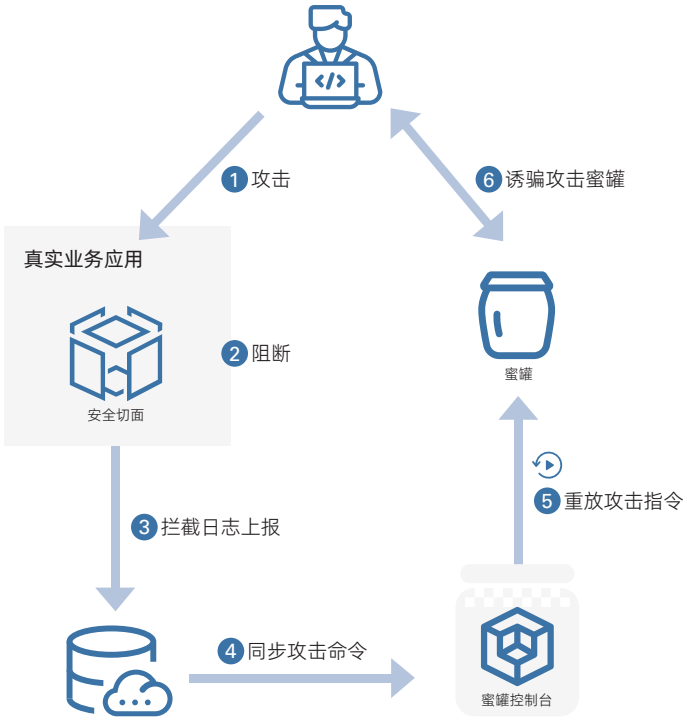

图 14 主动蜜罐

（3）效果

利用安全平行切面的优势，当检测到攻击尝试后，会对攻击进行阻断并将攻击行为在蜜罐中重放，攻击者会被迁移至蜜罐中“继续”入侵行为，起到主动诱敌深入效果。这样既为安全人员采取应急响应措施争取了宝贵的时间，同时可以继续对真实攻击行为进行记录观察、分析和溯源。

3.1.3 安全组件大规模快速升级

（1）需求

大型互联网企业的办公应用大规模部署了统一身份鉴权安全组件（IAM SDK）实现用户权限整个生命周期的管理，如创建权限、角色并授予用户以及回收。但是该 SDK 依赖于开发框架，当框架存在漏洞问题时，将面临安全风险。

传统修复方式不仅需要 SDK 提供方进行研发升级，还需要全部业务方共同改造代码上线才能完成修复升级，牵一发而动全身。如果问题严重要求在短时间内完成升级改造时，不仅打乱了业务的开发进度规划，而且涉及业务研发人员众多，导致人力和沟通成本高涨，修复周期漫长，严重影响修复进度。这是典型的业务和安全“绑腿走路”遇到的困境。迫切需要一种方法，能有效提高修复效率，由安全团队单独完成修复升级，缩短修复周期。

（2）解决方案

安全平行切面采用代码动态注入技术，横切入全部业务使用的 IAM SDK 代码中，进行热补丁修复，实现无需业务参与的安全组件统一升级。安全平行切面支持对类似的关键性安全组件提供新代码修复渠道，具备线上线下统一的安全漏洞修复能力、修复过程监控能力、故障及时回滚能力。

（3）效果

安全平行切面利用一整套流程保证业务不参与修复的情况下，独立实现安全组件升级，兼顾高效性、低成本、安全性和技术稳定性。在此案例中，由 SDK 提供方（安全团队）完成研发和上线，业务方仅关注业务的稳定性即可，实现了安全和业务的解耦。业务方几乎零投入，整体上实现了在较短时间内高效完成漏洞修复升级的任务，同时最大限度实现了低成本，达到预期目标。

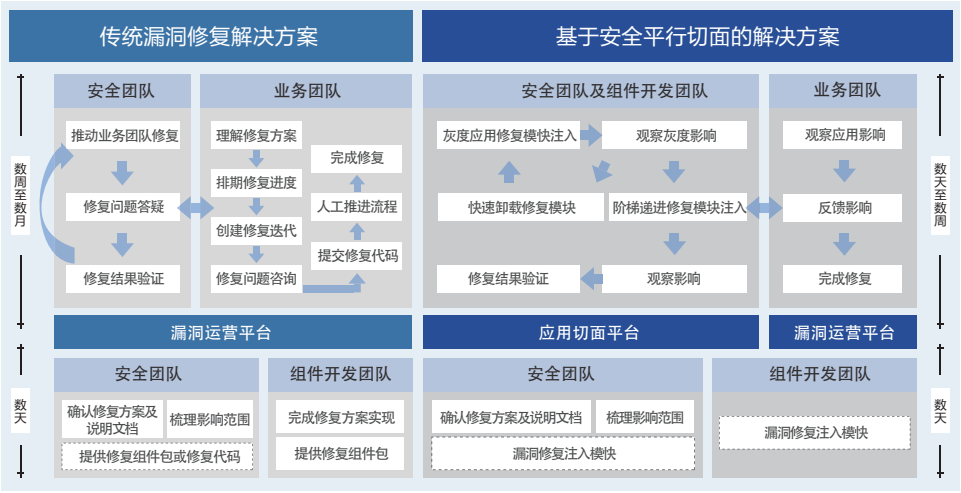

图 15　安全组件升级对比图

表 2　使用安全切面进行补丁升级成本对比

	传统修复方式	安全平行切面
技术要点	工单驱动业务团队修复	统一切面植入修复
人力投入	安全团队和相关业务团队	安全团队
时间成本	数周至数月	数天

3.1.4　操作系统内核漏洞应急防护

（1）需求

大型数字化企业拥有数量庞大的服务器集群，服务器上的基础组件如 Linux 内核不时曝出各种高危漏洞，各种新的入侵手法层出不穷。海量服务器全量内核版本的升级需要较长的时间周期，如何安全、高效、稳定地进行快速灵活地应急防护是安全团队的强烈需求。

（2）方案

操作系统的安全平行切面将可编程安全能力横切入系统内核中，构建切面基础设施，支撑 HIPS（主机入侵防御系统，Host Intrusion Prevention System），从而实现更快的漏洞修复时间和极大的灵活性。HIPS 可以监控系统中的文件、进程、网络的异常行为，识别入侵事件，完成攻击阻断。安全切面基础设施为 HIPS 提供了规则下发、安全策略加载、日志采集、稳定性保证等能力支撑，使得 HIPS 只需要专注于策略实现，极大地简化策略更新与加载过程，达到快速更新的目的。

操作系统的安全平行切面中的 LSM 层切面，通过在 LSM 层面的文件、进程、网络等切点加载插桩程序，使得 HIPS 可以获取到所有应用层的异常行为，通过与事先加载的策略对比，可以准确地判断出攻击事件，并进行阻断，从而实现应急防护。

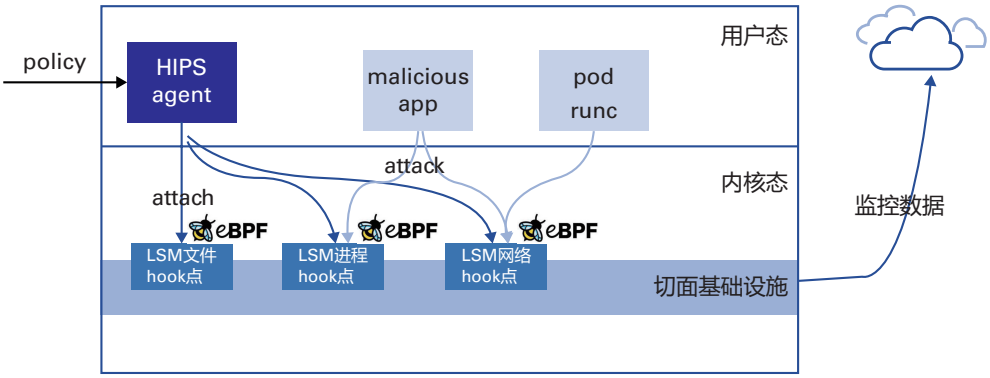

图 16　基于安全平行切面的 HIPS 架构

（3）效果

下面以文件保护为例，说明 HIPS 如何利用切面基础设施进行文件的防删除保护，如下图所示。

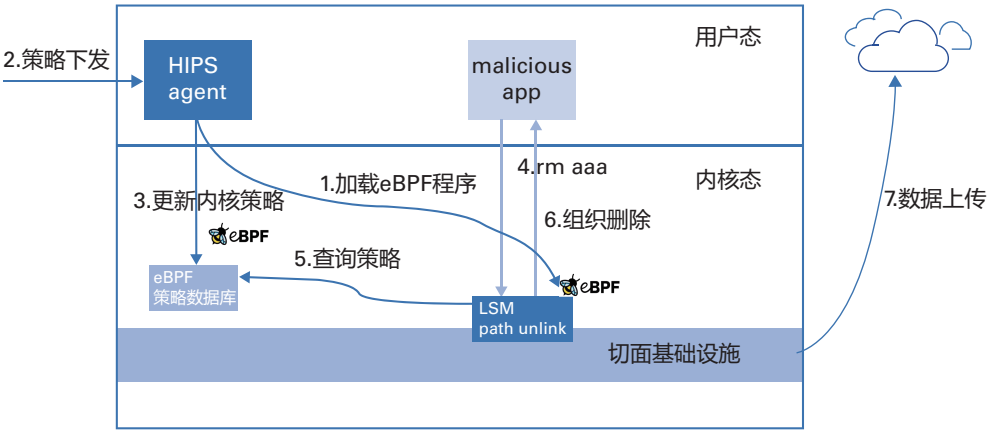

图 17　HIPS 的文件防删除保护框架

1）HIPS 的 Agent 通过操作系统切面基础设施提供的接口将 eBPF 程序加载到 LSM 的 Hook 点上；

2）用户通过 HIPS 提供的策略接口下发策略：禁止删除 aaa 文件；

3）HIPS Agent 通过操作系统切面基础设施提供的接口更新内核中的策略

数据库信息，添加步骤 2）中的策略；

4）攻击者对 aaa 文件进行删除；

5）步骤 4）中的执行流进入内核 LSM path_unlink hook 点，触发对应的 eBPF 程序，eBPF 程序查询策略数据库，发现 aaa 文件不能被删除；

6）path_unlink 对应的 eBPF 程序将删除 aaa 文件的请求阻止；

7）操作系统切面基础设施将这一触发规则的事件上报到日志采集服务器。

采用内核驱动模块的传统修复方式，存在以下问题：策略更新周期长，并且对系统的稳定性影响比较大。基于操作系统的安全平行切面的 HIPS 在攻防对抗方面具有如下优点：

1）安全稳定，通过使用 eBPF 插桩程序，极大的增加了系统的稳定性；

2）策略快速更新，通过使用操作系统安全切面基础设施，HIPS 能够快速地进行策略的更新，第一时间防御新型攻击；

3）监控点更加丰富，通过使用操作系统安全切面基础设施的丰富切点，HIPS 能够更快对异常行为进行监控，从而更加准确、快速地判断出入侵事件；

4）安全切面基础设施提供了规则下发、安全策略加载、日志采集、稳定性保证等能力支撑，HIPS 只需要关注自己的策略逻辑，更加安全、灵活。

3.1.5 挖掘 -1day 漏洞

（1）需求

传统上漏洞分 Nday、1day 和 0day，分别指已经公开的漏洞且有修补方案、已经公开但尚未有修复方案、攻击者掌握利用方式但尚未公开的漏洞。针对 Nday 漏洞，往往通过及时升级漏洞补丁，实现亡羊补牢式的修复。针对 1day 漏洞，只能通过业务和基础设施的升级换代进行解决。针对 0day 漏洞，由于防守方不掌握漏洞信息，只能依赖纵深防御体系，防守效果差，存在严重的不对称性危害。防守方完全处于被动局面，急需扭转被动挨打的局面。-1day 漏洞是指攻击者正在挖掘但尚未得手，防守者原来不知道，但由于有安全平行切面的内视能力，顺着攻击者的方向，利用更多的先验知识抢在攻击者前发现的漏洞。-1day 的价值不只是发现了原来不知道的漏洞，而是抢在攻击者前发现漏洞。捕获 -1day 的能力使防守者重新获得主动权，大幅度降低防守压力。

表 3　不同漏洞的攻守双方操作

漏洞	防守方	攻击方
Nday	资产盘查，安全治理	大范围扫描
1day	推动业务方和基础设施升级	抓紧写 exploit，抓紧去扫描
0day	强依赖于纵深防御体系，如履薄冰	保护 0day 不被暴露，一般只用于重要行动，重要目标
-1day	原来不知道，但顺着攻击者方向，利用更多的先验知识抢在攻击者之前发现漏洞	正在努力挖掘，但还没得手

（2）解决方案

如何发现 -1day 漏洞，给防守方提出了很大挑战。安全平行切面首先利用强大的内视能力，可以观察攻击者的行为，并通过算法筛选出异常行为，然后顺着攻击者的方向，结合自身的先验优势，完全有可能在攻击方发现漏洞之前发现自身产品的漏洞，掌握 -1day 信息，从而扭转攻守不对称态势，为在攻击之前完成修复提供宝贵的信息和时间。

（3）效果

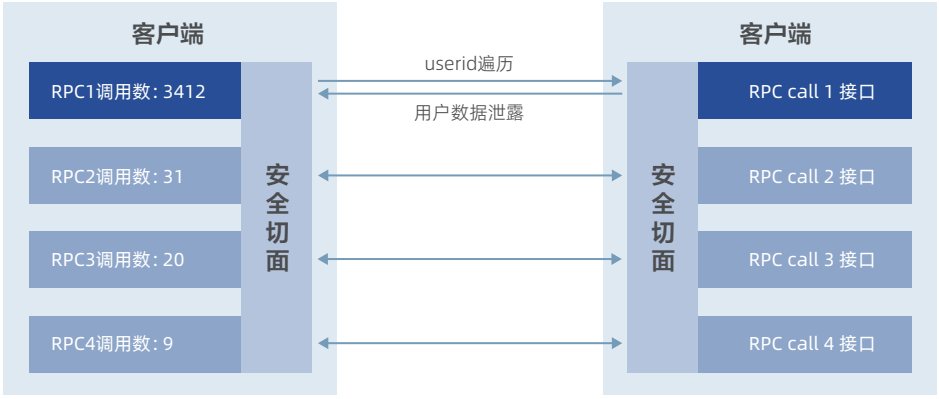

图 18　-1day 漏洞发现案例

在某案例中，安全平行切面在 APP 端通过调用栈和关键 API 参数等信息，发现攻击者对某敏感 RPC 调用 API 进行了注入，并存在枚举遍历用户信息的可疑行为（在短时间内发送大量 userid 遍历请求）。在造成实际损失之前，安全平行切面迅速阻断了攻击行为，将攻击者的账号加入了黑名单，并有针对性地对被攻击的敏感 RPC 调用 API 进行了安全加固，从而实现了零损失的巨大效果。

综上所述，安全平行切面在漏洞检测和加固，异常行为监控、识别和检

测，攻击快速阻断等应急攻防方面有很好的应用效果，可以实现漏洞快速止血、安全组件大规模快速升级、内核级漏洞应急防护，甚至可以先敌一步提前挖掘出 -1day 漏洞，扭转被动防守的局面，提前修复，防范于未然。

3.2 安全治理与布防实践

在复杂性爆炸的场景下，在安全治理上的投入经常远大于做安全攻防的投入，甚至超过 80% 的安全成本是治理投入。现在治理的效率往往非常低，正交融合的安全平行切面可以有效的改变这一现状。再进一步，安全需要灵活部署安全阵地。攻防是人与人的对抗，核心是知己知彼。如果所有的防御体系都一样，那么有经验的攻击者总能找到机会来绕过这样僵化的防御体系。先进的防御体系一定要有差异化的机制才能有效的进行防御。这些都要求安全防御阵地能够与应用解耦，并独立升级。

3.2.1 身份认证和鉴权能力快速接入

（1）需求

企业内部在最初设计或使用通信框架时，往往会忽略最基础的身份认证功能的设计，导致后续在做内部应用间的访问控制时，缺乏最基础的身份认证能力。但是通信框架的升级成本高，周期长。与之类似的情况，企业内部的接口调用往往不具备访问控制的能力，当某些接口存在敏感信息或者属于高危操作时，一般需要业务方自己设计认证机制和权限模型，来解决鉴权能力不足的问题。

传统的应用服务间的认证鉴权，通过 SDK 的方式接入，对于存量治理阶段，服务提供方需等待调用方全部接入改造完成，才可开启鉴权，而上游过多的情况下，改造周期难以协同，这导致多数时候鉴权仅具备审计能力。

（2）解决方案

安全平行切面可以方便、低成本实现身份认证和鉴权，通过安全平行切面将应用的身份信息通过协议扩展的方式融入到通信框架中；通过安全平行切面将通用的鉴权能力前置到接口数据的处理流程中，配合动态的鉴权策略配置，实现灵活的鉴权策略管控。

（3）效果

在此案例中，通信框架的维护方只需要通过安全平行切面，在业务方无感的情况下，以极低的成本即可完成身份认证能力的快速接入。首先鉴权 SDK 提供通用的权限模型，然后通过安全平行切面的能力，将接口请求的上下文信息与权限模型进行决策，实现鉴权能力的快速接入，业务方只需要关心授权关系，不需要关心策略引擎决策的细节。

3.2.2 DevSecOps 实践

（1）需求

随着互联网行业的快速发展，软件的研发模型从传统的瀑布研发模型到高效的敏捷研发模型转变。云计算被普遍的运用，微服务等基础架构的成熟，颠覆了原本笨重的运维部署模式，变得更加敏捷，形成了开发部署一体化的模式 DevOps。在敏捷的 DevOps 的模型下，传统的安全模型 SDL 降低了研发的敏捷度。Garter 在 2012 年提出了 DevOps 模型下的安全概念 DevSecOps，核心理念是人人为安全负责，让业务、技术和安全协同工作以生产更加安全的产品。

让安全研发变得敏捷和高效是 DevSecOps 落地的核心，也是 DevSecOps 落地的最大挑战，主要体现在以下两个方面。

1）DevSecOps 强调更前置的安全，在上线前提前发现和解决安全风险，将面临以下挑战：

- 如何在上线前自动化发现风险，且有较高的检出率和较低的误报率。
- 安全能力如何融入到研发流程中，且不给业务增加额外的安全负担。

2）安全是对抗中不断变化的过程，特别是在复杂的业务场景下，线上也会存在各类安全漏洞，那么在 DevSecOps 中漏洞的快速止血显得尤为重要，所以也面临很大的挑战：

- 传统的止血手段，例如 WAF 都是基于请求特征检测攻击，判断因子单一，原本误报和漏报就很难权衡，在互联网敏捷研发模型下，权衡误报和漏报更是难上加难，业务对接口的简单迭代可能就会造成误报或漏报；
- 当下的互联网业务除了 HTTP 协议，还有 IoT、移动端私有协议，传统的止血手段无法覆盖；

- 互联网企业往往使用了大量三方库，存在很多未知漏洞，此类漏洞的止血和对抗是个难题。

（2）解决方案

安全平行切面技术可以很好的应对 DevSecOps 的挑战，一站式完成 DevSecOps 的落地。交互式应用安全测试 (Interactive Application Security Testing，简称 IAST) 是一种 DevSecOps 落地的实现形式。交互式应用安全测试是一种将检测探针植入应用程序内部，在程序运行时采集各种信息进行漏洞检测的技术。由于 IAST 能非常精确的采集应用运行时的各种信息，可以有效的检测任意代码、命令执行、SSRF、水平越权、XXE、XSS、SQL 注入等多种漏洞，成为与白盒测试、黑盒测试并列的应用安全测试技术之一，并且具备更高的检出率和更低的误报率。

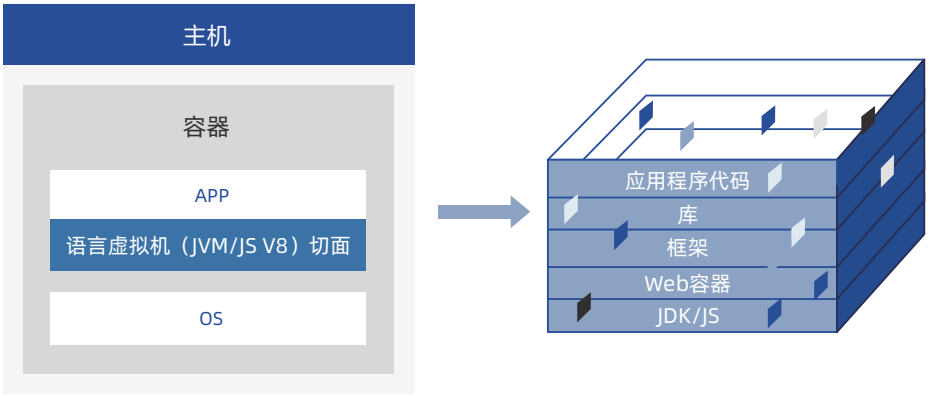

图 19　交互式应用安全测试

针对交互式应用安全测试 IAST 一些切点较为底层，程序运行过程中会被大量调用的场景，安全平行切面为 IAST 提供了轻量级注入能力，解决了 IAST 注入底层带来的性能问题。

交互式应用安全测试 IAST 作为安全平行切面的一个模块，安全平行切面为 IAST 提供了字节码 /JS 注入、规则下发、可信数据通信、监控和告警、部署等各种基础能力，使 IAST 只需聚焦自身业务实现，极大的简化了开发、部署和运营的难度。在语言虚拟机的切面层，通过对 JDK/JS、Web 容器、框架和应用程序各切点的切入，使 IAST 可以精确的获取到请求和响应信息、污点数据流、控制流、运行时配置等漏洞检测所需的多种信息。

（3）效果

目前交互式应用安全测试 IAST 已经在蚂蚁的开发和测试环境大规模部署，融入蚂蚁的研发流程，不需要投入额外的安全测试，业务测试就是安全测试，在开发和测试阶段成功地检测出数以千计的漏洞，使这些漏洞可以在研发过程第一时间被发现和修复，降低了业务上线的安全风险，也降低了漏洞修复的成本。

3.1.1 节介绍了使用安全平行切面对 Log4j2 漏洞（CNVD-2021-95914）攻击实施阻断的方案。应急之后仍需要检测和修复相关漏洞，例如为检出其他类似的 JNDI 攻击面，可在测试环境中使用 IAST 对 JNDI 的调用链路进行分析，一旦分析发现被污染的调用链路，即识别为风险并上报。这里需要注意的是，在研发测试环境也需要部署应用运行时安全防御系统 RASP 的切面模块，因为这也是一个重要的渗透攻击面。

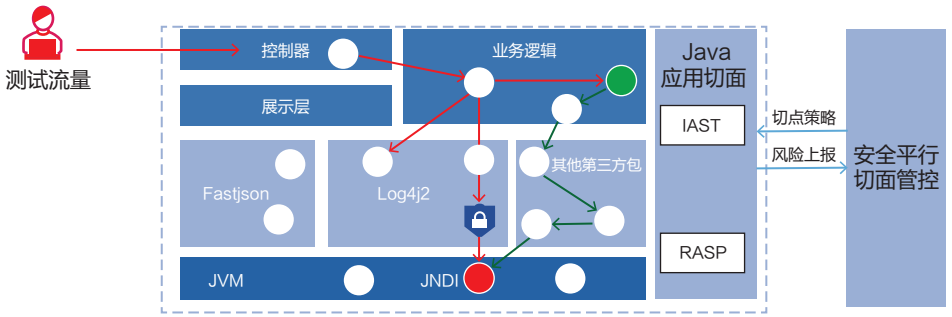

图 20　测试环境同时开启 IAST 检测和 RASP 阻断

3.2.3　移动应用隐私风险发现和管控

（1）需求

对于移动应用特别是平台型 APP，存在大量第三方 SDK、小程序等第三方代码，由于缺少运行时监测和管控的技术，无法对线上的实际调用行为进行观测，导致 APP 行为记录、解释和追溯极为困难，出现问题之后，也很难进行紧急阻断。

传统方式下，应用安全风险分析主要针对缺少安全管控或者管控存在疏漏的输入与输出，但是存在一些困难：

1）难以枚举应用的输入与输出。静态分析可以枚举出一部分，但是覆盖率

有限且存在一定程度误报；

2）复现困难。应用的某些行为，仅在特殊场景下才会触发，安全分析人员难以了解每个业务的细节，这些仅在特殊场景下触发的行为难以发现和评估。

比如第三方 SDK 会在某些特殊时段针对特定用户（三四线城市特定老年机）推送恶意逻辑，包括盗取用户敏感数据、推送恶意广告等。如果恶意代码隐藏足够深，只能在数天甚至数周后，当出现较多用户投诉时，才可能意识到这个风险；并且恶意行为在测试机环境上难以触发，定位和排查也很困难。

（2）解决方案

安全平行切面突破应用隐私威胁智能挖掘技术、运行时监测技术，通过移动端、流量端和云端构建全时态精准检测与追溯能力。安全平行切面通过给输入输出接口增加切面来实现，比如网络、文件、组件入口等接口，能够枚举应用的输入输出（大部分信息）；一定程度上能够判断输入与输出内容的安全属性、敏感程度、合法性等；通过切面的场景、参数、调用栈等信息能够快速找到触发路径，复现输入输出行为。

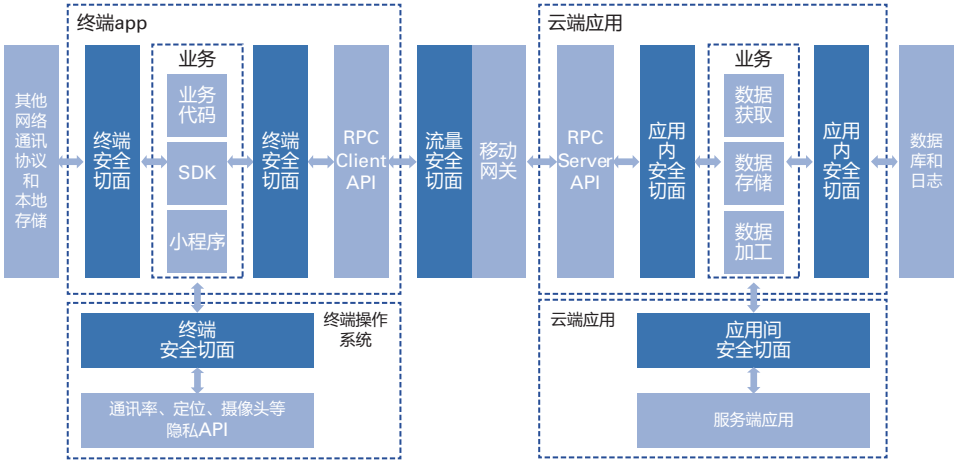

图 21　方案部署架构图

移动应用 APP 的安全平行切面，可以实现对隐私 API（通讯录、定位、摄像头等）调用链路、网络和文件操作、以及终端和云端之间通讯的监测和管控；通过流量安全切面可以实现针对移动网关中隐私数据分发的监测和管控；通过云端的应用内以及应用间安全切面可以实现对 RPC 通讯、数据库和日志操作、以

及与其他应用间通讯的监测和管控。安全平行切面具体可以提供的安全服务如下：

1）终端隐私风险发现

通过终端切面可以获取到隐私 API 的调用链路并上传到云端，通过算法分析可以快速发现异常，并可以定位哪些第三方 SDK、小程序窃取了用户隐私数据，以及是否通过网络、文件等方式对用户数据进行外发；

2）数据链路刻画

通过对 RPC 进行切面可以打通整个终端到云端的链路，从用户隐私数据获取和存储的角度看，通过切面可以知道用户的数据是从哪里获取的，以及怎么在云端落盘；从云端获取数据角度来看，可以知道哪些用户数据从数据库或者其他应用中进行了获取，并通过 RPC 返回到了终端的哪个模块；能够帮助业务方理清应用所属业务归属关系，业务之间数据使用不合规等情况；

3）服务鉴权

通过切面可以实现应用间服务鉴权的能力，当某个应用的服务被调用时，切面可以对调用者的身份进行验证和授权，从而限制非法的数据获取接口被调用；

4）数据泄露风险发现

通过在终端和云端对 RPC 进行监控和 IAST（交互式漏洞挖掘）的检测，可以在应用上线前或运行时发现越权信息获取的漏洞，从减少数据泄露和被爬取的风险；

5）细粒度隐私管控

通过对终端、网关和云端切面下发管控配置，可以在不需要业务修改代码的情况下，针对终端上特定的模块（小程序、第三方 SDK 等）和云端特定的应用接口进行细粒度（函数级别）的管控，避免了一刀切的防控，减少了对业务影响，并能够极大地加快止血速度。

（3）效果

目前通过对安全平切切面获取的数据进行挖掘和测试，已经发现并推动修复了十多个移动应用的脆弱性或风险，涉及隐私泄露、权限绕过、签名绕过、以及任意代码执行等多种类型，支撑了移动应用长时间的稳定安全合规运营。

3.3 数据安全治理实践

（1）需求

当前随着大数据、人工智能等信息技术飞速发展，企业在享受技术进步带来的发展红利时，也面临着重要数据与个人信息泄露的巨大风险。传统的技术、业务及企业架构，具有数据流动边界固定、数字资产量少、业务复杂度低的特点，依靠网关侧的流量采集再加上人工手动梳理基本可完成数据分类分级、访问权限管理、安全审计等数据治理工作。但随着企业数字化转型，企业业务数据及生产要素逐步成为数量庞大的数字资产，因为流动的数据才有生命力和业务价值，因此数据边界也在动态发生变化。

但数据的高速流通性让信息系统、网络区域之间的边界越发模糊。除了自身业务中产生的数据之外，企业也普遍采集或与外部第三方交换数据来丰富自己的数据资源，数据在不同组织和应用间的流通和加工成为不可避免的趋势。但数据流动普遍存在服务调用无授权、敏感数据过度输出、敏感数据违规使用和违规二次扩散、使用用户数据未经用户授权等数据安全风险。

随着《数据安全法》、《个人信息保护法》的施行，数据安全治理成为数字化时代的一道必答题。《数据安全法》规范数据生命周期过程中的数据安全，要求建立健全数据安全治理体系，实行数据分级分类制度，对数据全生命周期加强管控，不断提升数据安全保障能力，切实履行数据安全保护义务。根据《个人信息保护法》的规定，生物识别信息被划为敏感个人信息，只有在具有特定目的和充分必要性，并采取严格保护措施的情形下，个人信息处理者才能收集。为了打赢数字化时代数据安全保卫战，不仅要从法律上筑起数据安全防护网，也要从技术上打造数据安全的坚实屏障。

（2）解决方案

为了提升数据安全与个人信息保护能力，蚂蚁集团基于安全平行切面技术建立“蚂蚁数据服务海关体系”（以下简称“数据服务海关”），通过数据使用观测、数据使用监管、数据隐私保护、数据尽责审计四大功能实现对数据互通的安全治理。数据服务海关体现了大数据时代下蚂蚁集团数据安全治理理念的升级，是保障企业经营数据产权和用户数据产权安全的重要举措，为数据安全流动构建了新“边界”，确保数据的每一次使用都在数据服务海关的监管之中，从关注数据流入

和流出的渠道安全转移到关注数据全生命周期安全。

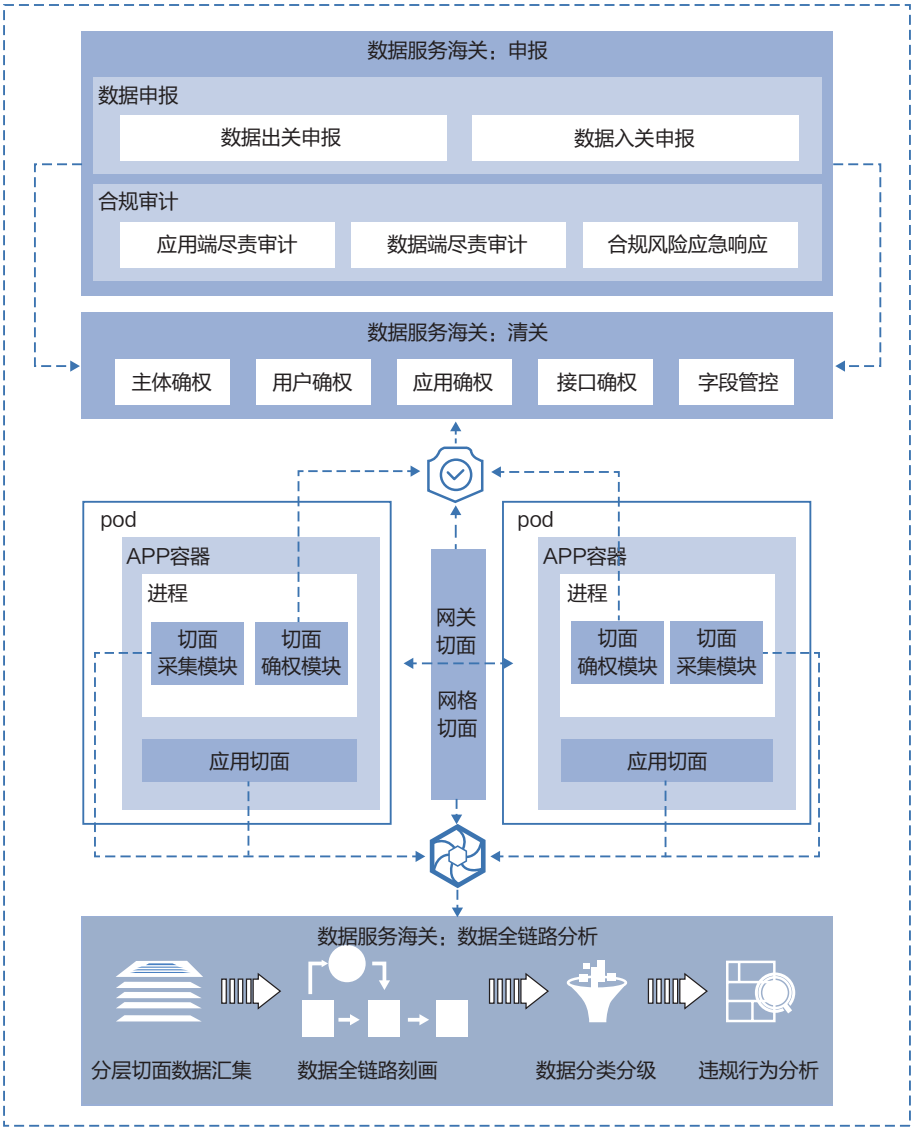

图 22　蚂蚁数据服务海关体系

数据服务海关针对数据流动与共享场景，通过可信身份验证、合法性依据管理、合理场景授权、目标资源范围最小化管控等技术机制，确保每一次数据流动均具有可追溯的用户授权和合规场景标识，保证数据流动满足安全合规要求。同时，数据服务海关联动安全平行切面、全息资产画像、实时授权策略引擎等技术功能，提供包含“资产采集 – 流转分析 – 风险处置 – 尽责审计”的一体化数据

合规管控能力，并对数据流动过程进行调查和分析，科学、准确的反映数据在线使用的态势，实施有效的统计监管和尽责审计。

相比于传统的仅基于用户授权处理数据的方式，数据服务海关引入数据出关与入关申报机制，使得业务所有对外提供的在线服务都需要在确保双方具备授权和合法性依据基础上明确使用场景和数据使用范围，如果涉及用户信息则需要获得用户授权，最终基于实际合作的业务主体、业务场景、数据内容、数据范围、授权协议等关键信息，共同构成数据出关与入关的申报要素，作为数据合规流动的证据材料，形成全局统一的数据服务海关监管管控策略。

通过出关与入关申报机制，使得相关治理团队能够掌握企业数据的流入和流出情况，并形成统一的管控策略：在运行时通过分层控制的原则，在各“边境”网关完成合法性依据、应用身份、场景合理性等验证；数据提供方则需要对接口输出的字段范围及是否已获得用户授权进行校验。

如果采用传统的安全技术来实现“数据服务海关”，对已有业务系统改造的成本极高。基于安全平行切面技术，在业务侧无需改造的情况下，就可以实现在关键的敏感接口位置实施用户确权校验，有效形成在“数据服务海关架构”下实施数据安全保护的纵深防护体系。

当前复杂的业务环境下，数据会有较多的融合汇集、跨主体 / 跨境流动，并会衍生出一系列的数据消费服务和潜在的数据要求，对数据安全的可观测性、访问控制能力等提出了更高的要求。数据服务海关具备以下能力：

1）数据使用观测

所谓可观测性即对海量、异构、复杂数据的采集、分析和展示能力，要求能够在流转的复杂结构数据中识别敏感数据，并能够对敏感数据进行准确分类分级，基于敏感数据传输的上下文呈现数据血缘关系，最终基于实际血缘关系完成数据使用的观测。

基于安全平行切面实现的数据采集能力，具有与业务独立且解耦的巨大优势，以精准的数据采集能力和采集数据具有关联性为特点，大大提升了数据安全治理的可观测性；能够按照应用类型和数据采集需求，动态下发采集规则，实现对所有接口请求与返回情况的采集，以及对所有应用读写数据源的行为采集，通过信息融合技术，拼接数据从采集到处置的全生命周期行为；结合图分析技术，将关联信息进行串并，对相似调用关系进行合并、对缺失信息进行补全，从而完

成整个数据处理流程的还原，在此基础上建设数据流转链路的可观测能力。

2）数据使用监管

在数据访问前，业务通过数据出关与入关申报完成数据使用权限的申请，并通过安全平行切面技术传递可信身份和申请数据的使用权限，申请内容包括应用所在企业主体、是否跨境传输、数据使用场景和字段范围，申请信息交由安全团队审批，审批通过后授权信息将作为策略下发到策略执行点中。在数据使用过程中，对服务的每次请求和数据获取请求进行可信验证，验证维度包括身份是否可信、使用字段是否超出授权范围、数据使用是否超出安全基线要求等，致力于消除应用对高敏数据的非授权使用，确保业务在授权范围内使用数据，避免应用违规扩散数据，且数据授权和使用过程可审计。

如果应用需要访问资源（可能是数据，或通过调用服务接口获取数据）时，安全平行切面技术在网络和应用侧提供的策略执行点，将向策略决策点描述应用的属性，请求安全决策，并根据策略决策点返回的信息执行决策。就某一个单一请求而言，需要考虑以下因素，包括应用身份是否可信、所在物理机环境是否处于安全状态、应用可使用的数据敏感等级是多少、对数据的使用是否获得企业主体授权、获得的字段范围是否在授权范围内等。

图 23　数据访问的安全管控

3）数据隐私保护

随着国家对数据隐私保护要求的提高，访问个人信息不仅要获得业务主体的授权，还要获得用户的授权。业务主体的授权通常跟随法律框架协议而生成唯一的接口调用场景码，通过场景码来关联指定接口的调用权限，而用户数据则在接口实时返回的行级数据中。传统的访问控制体系只能管控到接口粒度的鉴权，即鉴别调用方是否保护可信身份且拥有场景码对应的调用权限，但对于数据交换中涉及的行级敏感、隐私数据，却没有现成的用户确权方案。

数据服务海关对数据流动做到行级字段级别的监控，建立行级数据鉴权体系，

通过切面技术打造的隐私确权模块实现个人信息保护法中要求数据获取方获得个人授权的要求。

以用户开通信用卡为例，在用户开通信用卡并获得额度时，需要调用多个跨业务域的在线数据服务，获取用户信息用于实时的额度计算。当调用开通信用卡服务接口时，因为开通信用卡服务接口属于高敏接口管控名单，所以所有接口调用都需要执行同步 / 异步的确权判断，加载隐私确权模块能够在运行时实时查询远端用户协议中心的用户授权信息，并返回用户授权查询结果。如果查询用户已授权对其他跨业务域的信息查询，则继续调用接口获取信息来计算额度，否则终止此次开通信用卡业务的操作。

通过安全平行切面技术对行级数据的确权管控，使得数据安全治理从应用粒度、接口粒度深入到行级数据和字段级别粒度，提升了数据安全治理的可观测细粒度与合规水位，更好地支撑了安全治理团队对隐藏在行级数据中的安全风险治理和溯源能力。

4）数据尽责审计

尽责审计能力建设的初衷来源于监控部门提出的“穿透式监管”要求。穿透式监管另一个叫法是看穿式监管，出自于证监会公告 [2013]30 号《关于加强证券期货经营机构客户交易重点信息等客户信息管理的规定》的有关要求，目的是加强期货市场看穿式监控要求，指导期货公司按照要求规范客户交易重点信息的采集、记录、存储和送达等工作，所谓看穿式监管就是以投资者账户为核心，清楚掌握每一个账户的交易情况。2018 年 3 月银发 [2018]106 号文《中国人民银行关于规范金融机构资产管理业务的指导意见》中明确了实施穿透式监管的要求，按照穿透方向可分为向上的资金端穿透和向下的资产端穿透。资金端穿透是指：穿透识别标的资产的资金来源，审查投资项目的投资者和资金来源是否符合监管规定或合同约定；资产端穿透是指：穿透识别资金投向的底层资产，审查资金的投资范围和底层资产是否符合监管规定或合同约定。

对比数据安全保护与资产合规交易管控的业务场景，一个是对敏感数据的合规流动管理，另一个是对金融资产的合规交易管理，都需要完整记录和刻画数据流动（资金交易）的全链路信息，以实现数据流动的实时监管，对敏感数据的产生、

使用、流动、扩散、存储等各环节进行全面监管，建立数据安全合规流动管控制度。

数据服务海关的尽责审计能力可感知敏感数据从创建 / 采集、使用、流动、扩散、存储等环节以及各个环节涉及的应用信息，能够可视化的呈现敏感数据使用的链路，并根据敏感数据类型或应用实施数据段穿透和应用端穿透。在端到端的链路中能够刻画具体的合规风险并生成工单完成后续安全运营。同时能够配合监管检查，审计指定类型信息的使用是否符合监管要求。

其中，数据端穿透是指识别敏感数据的来源和扩散方向、途径应用 / 接口和最终的存储位置，审核敏感数据流动是否合规。应用端穿透是指查看应用对外开放了哪些敏感接口、敏感接口的上下游应用分别是哪些应用 / 接口、审核敏感接口调用是否合规。

（3）效果

蚂蚁集团于 2019 年首次在业界提出了安全平行切面，并于同年在蚂蚁集团内部应用基于安全平行切面技术的数据安全防护体系。该体系是应对业务复杂性爆炸带来的数据安全治理难点，具备可广泛部署且减少对业务连续性造成影响的创新性解决方案，有效覆盖中长尾数据中结构化与非结构化数据的数据生命周期治理场景，具备集数据采集、数据识别、血缘分析、风险感知和风险处置于一体的检测、分析与响应能力，在不影响业务连续性的情况下快速响应数据安全治理需求，使得安全治理目标与业务发展目标既融合又解耦。

安全平行切面技术体系改变了传统基于企业资产和静态存储数据的数据安全事后治理模式，利用切面基础设施与业务部署的正交融合，能够在业务的全生命周期、数据的全生命周期提供如影随形的数据安全管控能力；提供细粒度的采集和行为分析能力，能深入了解数据流转情况，克服资产与行为数据的缺失带来的治理盲区；在端、管、云协同作战，实现一体化、能力闭环的纵深防御。安全平行切面打通了各个应用之间的数据使用关联，正是有了这种关联，才能够回答：业务采集了什么数据，对外共享了什么数据，合法基础是什么，最终建立满足持续治理需求的数据安全管控体系。

表 4　安全平行切面对于数据安全治理效果的对比

	传统外挂式安全防御	安全平行切面
数据采集	旁路数据采集方式； 能否采集到数据依赖于终端、应用、网关、数据库等应用提供的原始日志作为数据源，缺乏业务上下文信息，数据采集可用性无法保证；	原生数据采集方式； 覆盖终端、应用、网关、数据库等多类实体的全域数据采集，深入业务逻辑内容，准确性、可用性更高；
数据识别	缺乏对上下文信息理解的识别语法，无法识别日志中数据的真实含义；	语义识别算法对带有上下文信息的数据信息的识别结果更加丰富；
分类分级	支持少量数据类型；	支持多种数据类型；
溯源分析	依赖终端、应用、网关、数据库等应用原始审计日志的溯源无法定位到风险责任主体；	通过终端、应用、网关、数据库等应用的行为日志且带有上下文信息的数据溯源可以定位风险责任主体；
风险感知	事后感知能力； 只能从采集的流量中尝试对已知的风险进行感知，缺乏事中感知能力，往往事后审计中才发现风险；	事中感知能力； 深入应用逻辑内部，实时感知敏感数据的违规使用、隐私数据的非授权使用等异常行为；
风险处置	缺乏对感知到的风险进行实时处置的能力；	能够实施对感知到的风险进行告警、审计和拦截；

4. 总结与展望

安全平行切面就像程序里的平行空间，与业务逻辑交织在一起，又相互独立；切面防御贯穿整个程序，可以有效地管控整个程序，同时又不被业务研发周期所束缚。在复杂安全风险场景下，安全平行切面防御体系将安全能力系统化地融入基础设施与应用内部，同时保持安全响应能力与复杂业务逻辑的解耦，形成独立的安全切面。在推进业务高速演进的同时，可以独立、高效、精确地在应用内部直接检测和阻断各种复杂攻击，并支持透视业务 / 应用以完成全方位的安全治理工作。安全平行切面防御体系在准确性、效率、通用性等方面超越了传统安全基础设施。

蚂蚁集团将安全平行切面作为下一代金融级基础安全防御体系，在多个云和端的重要技术基础设施上，超过 100 个场景下完成了研发和部署，每天可对千亿级的技术行为进行全程安全保护和管控。蚂蚁的实践表明安全平行切面是一个非常有前景的新兴安全体系，能够有效缓解大型数字化业务面临的严峻安全挑战，在应急攻防、安全治理与布防、数据安全治理方面发挥重要作用。

蚂蚁集团愿意把安全平行切面的建设和实践经验与业界分享，将以开源方式把成果分享到行业，包括完整的多层次切面基础设施和安全应用示例，也希望和业界朋友们一起构建更完善的安全平行切面生态，保障数字化产业的顺利发展。

参考文献

序号	文献名称	出处
1.	数字中国建设发展报告（2020 年）	国家互联网信息办公室，2021
2.	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	十三届全国人大四次会议，2021
3.	中华人民共和国网络安全法	全国人民代表大会，2016
4.	中华人民共和国密码法	全国人民代表大会，2019
5.	中华人民共和国数据安全法	全国人民代表大会，2021
6.	关键信息基础设施保护条例	国务院，2021
7.	中华人民共和国个人信息保护法	全国人民代表大会，2021
8.	网络数据安全管理条例（征求意见稿）	国家互联网信息办公室，2021
9.	数据出境安全评估办法（征求意见稿）	国家互联网信息办公室，2021
10.	数据安全治理白皮书	中国电子信息产业发展研究院、赛迪智库网络安全研究所，2021
11.	平行空间和高维正交 - 移动端安全切面体系架构设计与实践	Xcon，2021
12.	Aspect-oriented programming	ECOOP’97，1997
13.	内生安全：新一代网络安全框架体系与实践	奇安信战略咨询规划部 & 奇安信行业安全研究中心，2021
14.	SP 800-207：Zero Trust Architecture	美国国家标准与技术研究院，2020