安全平行切面：面向企业数字生命体的安全基础设施

Aspect-Oriented Security: Security Infrastructure for Enterprises as Digital Lifeforms

韦韬/WEI Tao，顾为群/GU Weiqun，刘宇江/LIU Yujiang
（蚂蚁集团，中国 杭州 310013）
(Ant Group, Hangzhou 310013, China)

DOI：10.12142/ZTETJ.202206011
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221209.1058.003.html
网络出版日期：2022-12-10
收稿日期：2022-10-16

摘要：现代数字化企业是一种不断演变进化的生命体。它的架构复杂性会爆炸性增长，不断引入的外部数字化产品服务和行业技术体系演化，会推动其形成内部数字化基因的代差积累。为了应对严峻的网络安全攻击威胁，符合严格的数据安全合规要求，保障企业数字生命体的健康发展，现代企业安全基础设施必须更加适应这种动态复杂性。阐述了安全平行切面，其核心思路是把安全能力融入企业基础设施中并与业务解耦，使安全能力深入业务逻辑，同时实现双方的独立高速发展，在更高维度上实现持续的动态安全防护。

关键词：安全平行切面；内生安全；原生安全；企业安全架构；企业数字生命体

Abstract: A modern digital enterprise is a living organism that is constantly evolving. The complexity of its architecture will grow explosively, and the continuous introduction of external digital products and services and the evolution of industrial technologies will promote the accumulation of internal digital genes. In order to deal with severe threats of network security attacks, comply with strict data security compliance requirements, and ensure the healthy development of enterprise digital lifeforms, modern enterprise security infrastructure must be more adaptable to this dynamic complexity. The aspect-oriented security is described. The core idea is to integrate security capabilities into enterprise infrastructure and decouple them from business, so that security capabilities can penetrate into business logic, and at the same time both parties can achieve independent and rapid development, and ensure continuous dynamic security in a higher dimension.

Keywords: aspect-oriented security; endogenous security; security-native; enterprise security architecture; enterprise as digital lifeforms

随着“十四五”规划的发布，中国正式提出“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”的发展目标。这标志着中国“加快数字化发展，建设数字中国”的目标正式启航。习近平总书记指出，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。当今世界，以互联网为代表的新兴技术日新月异，对人类社会的发展进程产生深刻影响。同时，网络安全问题也相伴而生。世界范围内的个人隐私侵犯、知识产权侵犯、网络犯罪等时有发生，网络监听、网络攻击、网络恐怖主义活动等成为全球公害。网络安全已经成为中国面临的最复杂、最现实、最严峻的非传统安全问题之一。网络安全是经济与社会发展的基础保障。如何通过创新架构、创新理念和创新技术等方式突破现有困境，成为当前网络和信息安全建设的重要工作。

安全架构是网络和信息安全建设成果的重要体现。虽然近几年零信任、纵深防御、网络安全滑动标尺等安全架构和理念相继产生，但并没有根本性地改变安全建设与业务发展之间的生产关系：长期以来，安全架构建设由安全团队独立完成，被认为与企业架构及企业经营业务流程相对独立；因为安全架构需要建立在企业架构相关可用信息之上，所以安全架构建设常常滞后于企业架构的动态演进。经历数字化转型后的企业架构就像复杂的企业数字生命体（以下简称数字生命体）一样，会为了适应竞争环境而不断“进化”。每一次进化都可能会给安全架构带来巨大冲击。静态安全架构无法适应企业架构的动态变化，最终导致传统架构下的安全能力无法动态贴近业务，应对更深层的复杂性安全风险。面对数字生命体的不断进化，本文尝试将数字生命体与“人类复杂有机体”（以下简称有机体）进行比较，思考安全架构建设的困境与愿景，探究数字生命体在进化过程中，如何通过创新技术来实现安全架构与企业架构的常态化融合，并保持安全架构的一致性、连续性、低侵入性、有效性、稳定性和

友好性。

数字生命体中众多面向公网开放的互联网业务就像有机体的呼吸系统一样。当前开源软件的大规模引用和软件供应链安全威胁的加剧，使得类似新冠病毒这样的未知0day攻击日趋常态化，并通过“呼吸系统”感染数字生命体内部。结合外部风险态势和蚂蚁集团自身的安全需求，我们看到：随着业务复杂度的提升，已有的安全架构建设及单点安全能力显得力不从心，在面对内外部环境时不断爆出漏洞，在对抗、溯源、治理方面仍面临巨大挑战。因此，蚂蚁集团对安全理念和安全架构进行了全面升级。其中，安全平行切面与平行舱是安全理念和架构的具体体现。安全平行切面是中国在国际安全领域首创的创新安全理念及技术。

1 安全建设的困境与愿景

据统计，2022年网络与信息安全产业共包含94个细分安全领域[1]，比2021年增加7个。近几年，安全产业细分领域的快速增加在某种程度上表明，企业架构和业务逻辑复杂性的急剧增加也不断催生新的安全需求。为满足前期业务快速发展的需求，安全能力大多采用外挂式的架构模型保障业务发展。这种外挂式安全架构的部署成本和对业务的侵入性都较低，所以被各类企业所接受。但是在高强度对抗与复杂治理场景下，外挂式安全架构的业务效果受限于可观测能力，已经无法满足更深层次的对抗和治理需求。例如，在数据安全治理领域，过往对抗和治理的对象往往是内部结构化数据的非法泄漏风险。但如今数据已成为生产要素，数据要素的流动会潜藏数据非授权共享、个人隐私泄漏、敏感数据违规扩散等重大经营风险。企业不仅仅要在边界层查看数据流出的一跳链路，更需要将整条数据传输链路及传输内容进行精细化审计和实质性管控。外挂式安全架构在高强度对抗与复杂治理场景下已显得力不从心。

随着网络安全、数据安全、个人隐私保护等监管要求的加强，安全能力与业务逻辑相融合所产生的价值愈发凸显，但彼此融合后又面临严峻挑战：融合升级后的安全防护效果优于外挂式安全架构，但在对抗方面基本无法发挥作用。其中，融合的形式包括安全团队为满足防护需求而开发的各种软件开发工具包（SDK），以及需要与中间件深度集成的安全组件。受限于业务方的研发集成、发布和升级等工作，安全与业务相互间制约着各自的发展。例如，安全团队需要小时级甚至分钟级的止血响应，而大型业务团队经常面临着十几个版本的碎片化测试和稳定性灰度上线压力，无法满足安全应急要求；更有甚者，安全团队辛苦推动各基础设施和应用服务集成一个关键安全增强组件，但基础设施的一个小缺陷或者业务的一个需求变更回滚，导致安全团队前功尽弃。

当前企业架构和业务逻辑呈现复杂性爆炸态势。作为企业经营战略的组成部分，安全架构应以低侵入而非捆绑的方式集成到企业架构中，以改变企业经营发展受到安全架构发展滞后影响的现状，为业务提供体验友好的原生化安全服务。这既是未来企业架构与安全架构共同的演进趋势，也是安全架构建设的愿景。

面对数字生命体的进化和安全建设愿景，如何在动态过程中实现安全架构与业务架构的无缝融合，是蚂蚁集团在新形势下面临的挑战。蚂蚁集团逐渐形成了以数据要素为中心的网络安全架构。业务云化、数字化转型等技术变革带来了企业服务和数据要素的动态访问需求，而动态访问需求又产生了更为复杂的安全业务场景和需求，例如员工在任意空间对企业内网的安全访问、在线数据要素的实时共享和确权、个人隐私信息保护、生产网访问流量鉴权、多类型移动应用漏洞检测等。面向复杂和动态的业务场景，灵活、快速地部署安全能力和响应安全需求，既是对已有安全架构和单点安全产品的挑战，也是蚂蚁集团新安全架构的建设诉求。蚂蚁集团在2019年提出了安全平行切面的理念和技术体系[2]，安全平行切面技术能够在高强度对抗和复杂治理背景下，将安全能力深入到业务内部，从根本上解决问题。该技术不仅可以确保安全逻辑和业务逻辑各自独立、平稳演进，避免出现绑腿走路的困境，还可以让企业快速具备精准的感知和干预能力，同时实现安全能力和效率的跨越式提升。

2 安全平行切面的定义

我们通过类比的方式来描述什么是安全平行切面。在新冠病毒防控过程中，佩戴口罩和接种疫苗是非常重要的。（1）佩戴口罩的作用是防止空气中的病毒通过呼吸系统进入体内。理想情况下，如果每个人都佩戴了口罩就相当于达到了微隔离的效果。但口罩不是完全封闭的状态，病毒总会绕过口罩进入体内。（2）经过科学论证，接种疫苗是抗击新冠病毒的最佳途径。但在应对新冠病毒全面爆发这样的突发事件时，疫苗的有效性、疫苗自身的安全性、与体内其他疫苗的兼容性、疫苗的规模化接种等变得非常关键。可以想象，对于不同国家来说，为1 000万人口、1亿人口和14亿人口大规模接种疫苗的难度是完全不同的。

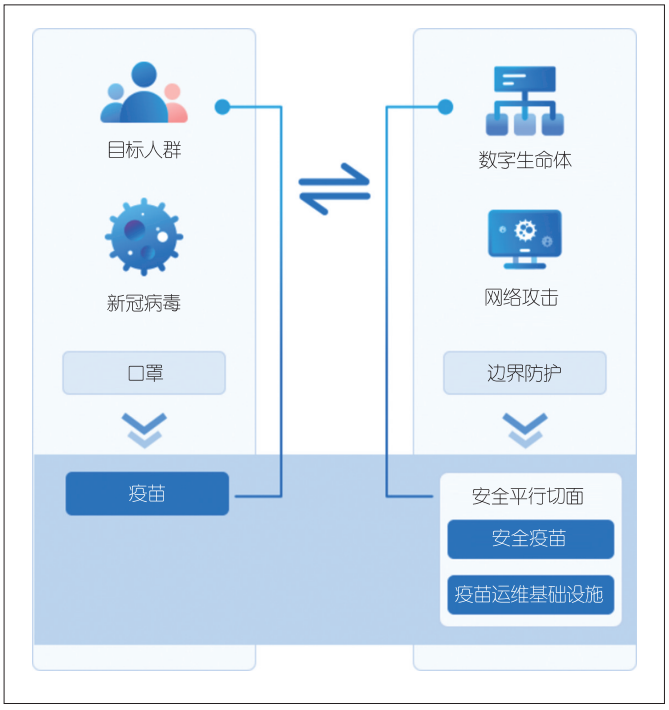
上述两个阶段恰好与企业在高强度对抗与安全治理的过程十分相似。企业首先通过入侵防御系统（IPS）/Web应用防火墙（WAF）/防火墙等对企业边界进行防护。有效的边界防护非常重要，它能够防护大部分的外部攻击。但防护能力始终存在被绕过的可能，所以企业开始考虑通过运行时插

桩手段对正在运行的业务进行像疫苗一样的保护。这种技术方式将安全逻辑注入到业务内容，形成一种以上下文分析和异常行为检查为基础的“抗疫”能力。这种植入“安全疫苗”的方式在蚂蚁集团内部多个0day应急场景中被证明是有效的。因此，蚂蚁集团自研了诸如运行时应用自我保护（RASP）、交互式应用安全测试（IAST）等安全疫苗产品。但在应急响应过程中，这同时也带来了诸多问题：

- “安全疫苗”本身也是由代码构成的，如何快速验证疫苗能够发挥预期的安全作用？
- 如何确保疫苗自身足够安全，不会被攻击绕过或被动失效？
- 如何确保疫苗自身足够稳定，不会在出现异常的情况下影响宿主正常运转？
- 企业可能拥有几万甚至几十万台机器，那么如何在短时间内为每台机器都注入疫苗？
- 每台机器不会只注入一种疫苗，那么疫苗和疫苗之间如何进行有效的隔离，以确保不存在兼容性异常？

解决上述问题是蚂蚁集团提出并打造安全平行切面架构的初心。我们发现：为安全疫苗在业务空间内提供一个可持续进化的安全平行空间，是未来高强度对抗与安全治理背景下安全能力建设的普遍需求和唯一方向。这样的平行空间需要完备的稳定性、有效性、安全性、隔离性保障，不仅能够帮助安全疫苗快速部署到离业务会话最近的地方，还能够随着业务的动态扩/缩容而动态部署，实现中心化安全能力向分布式安全资源的演进。

那么什么是安全平行切面？安全平行切面是一套由安全疫苗和疫苗运维基础设施组成的安全架构。它首先在移动应用程序（APP）、云端应用、操作系统等应用与基础设施中注入安全疫苗，形成端-管-云立体安全防护架构，通过安全逻辑与业务逻辑解耦实现网络安全、数据安全的微观和宏观感知覆盖，满足应急响应、漏洞止血、数据安全、隐私保护等高强度对抗和安全治理需求。疫苗运维基础设施则从研发、测试、验证、监测与控制、稳定性保障等方面确保安全疫苗产品符合各类准入要求，并帮助各类安全疫苗实现全生命周期运维和大规模覆盖。所以，安全疫苗（例如RASP、IAST或其他具备运行时安全特性的产品）与疫苗运维基础设施共同构成了安全平行切面，如图1所示。



▲图1 安全平行切面为数字生命体提供疫苗保障

3 安全平行切面架构与平行舱

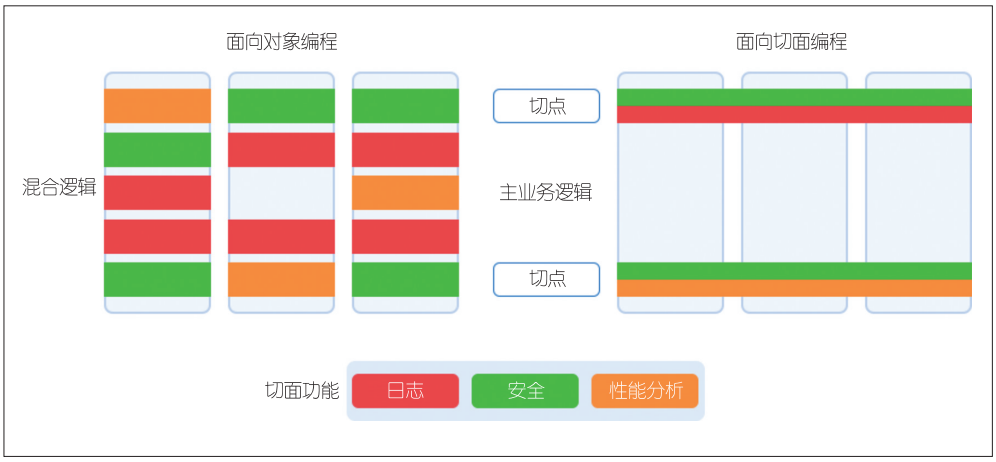
3.1 面向切面编程（AOP）与安全平行切面

1997年施乐帕洛阿尔托研究中心的Gregor等学者在著名的欧洲面向对象编程（ECOOP）会议上提出AOP的概念[3]。研究发现，面向对象编程（OOP）不能解决所有的问题，特别是涉及大量类的横切系统性功能问题很难用OOP来解决。而AOP能够很好地解决这一问题，它可通过预编译、运行时动态代理、注入等方式，在不修改原码的情况下，给程序的正常业务逻辑动态添加或修改功能，如图2所示。AOP已在AspectJ和Spring等项目中得到应用。

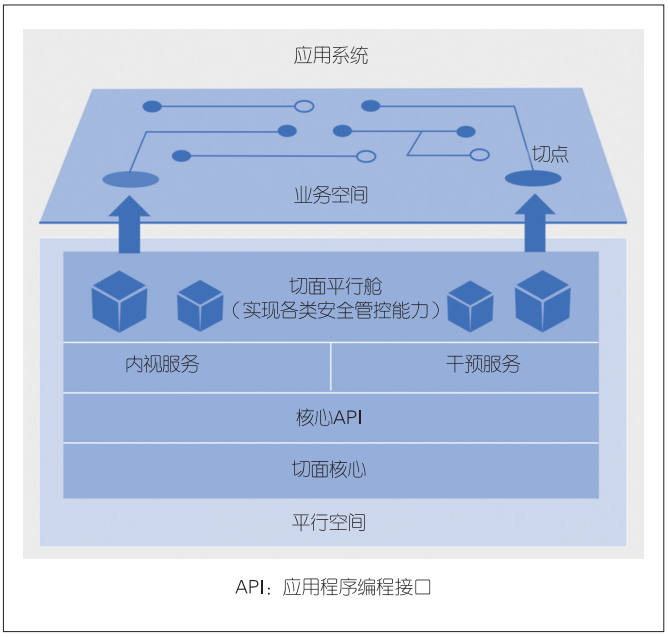
安全平行切面的核心思想是：将编程语言环境下的AOP推广应用到安全架构建设中，构建与业务正交融合的安全平行空间，在不修改业务正常逻辑的情况下，将安全能力系统化地融入到技术基础设施和应用服务的内部，从而实现更高维度的安全防护，在保持安全响应能力和复杂业务逻辑解耦的同时，通过标准化的接口为安全业务提供内视和干预能力。安全平行切面是一种创新的安全架构，是低成本实现“原生安全”、快速增强应用服务内在“安全体质”的一条可行路径。

3.2 安全平行切面基本架构

图3是安全切面的基本结构，上方是业务空间，下方是平行空间。在平行空间里面，安全平行切面通过注入、代理等技术，可以在不修改源代码的情况下动态添加新的（或修改程序原有的）逻辑。这部分动态逻辑称为切面应用。切面应用的作用位置（切点）是应用原有运行逻辑中的某一代码



▲图2 面向对象编程与面向切面编程



▲图3 安全切面的基本结构

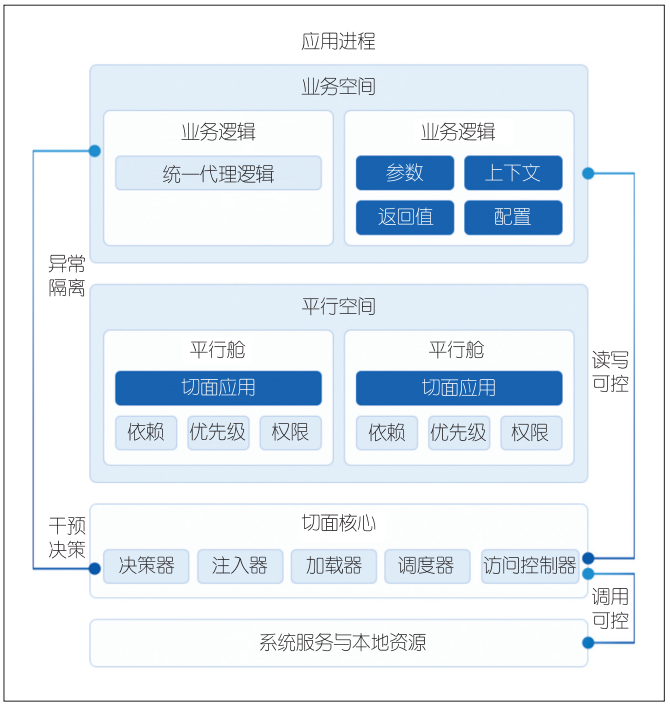
位置。一个切面应用可以作用于一个或者一组切点。类似于AOP的机制，安全切面可以将切点位置的代码执行流程引至切面应用中，并对其原有逻辑进行观测或干预。安全团队可以通过研发部署各种作用于不同切点的切面应用，来为应用服务动态扩展出各种丰富的安全增强能力。这就像如同通过应用注射各种疫苗来提升应用服务自身应对安全风险的“抵抗力”。

切面应用的动态扩展能力能够很好地降低日常安全治理成本，实现高效的安全响应能力。对切面应用模块化的管理方式，不仅能使各类安全能力实现独立开发，还可使不同的切面应用研发人员之间相互解耦，互不影响。但是便捷是一把双刃剑，其背后隐藏着巨大的隐患。例如，随着各类切面应用的不断增多，切面应用的质量参差不齐导致各类系统故障，不同切面应用之间的相互影响导致功能异常。如果被恶意人员所利用，切面应用反而会成为应用服务的安全短板。因此，如果不加以合理管控，安全切面会成为安全和稳定性的短板，无法被大规模推广使用。

3.3 平行舱：安全平行切面的稳定保障

为了保障平行空间内各种切面应用能够平稳、有序、可控、安全地运行，在系统运行时我们对切面应用进行了一层封装，即切面平行舱。这就像给疫苗加上一层“胶囊”一样，能够控制其在何时、何处、以何种规模生效。平行舱有三大特性：隔离性、可调度性和可管控性。借助平行舱可以对切面应用的作用和影响范围、组件依赖、可执行动作等进行相应的隔离与管控，如图4所示。

切面应用通过切面核心的加载器加载到平行空间中，在属于其自身的平行舱中运行，并通过各平行舱命名空间的隔离，来确保其依赖作用域只限于自身，不会污染业务空间。切面核心通过统一注入的代理逻辑接管切点的处理流程，并根据各种切面应用的优先级进行统一的调度管理。当最终各



▲图4 平行舱与切面应用

切面应用的处置逻辑执行完成之后，根据不同切面应用的执行结果，决策器会给出对业务逻辑所需要执行的干预行为。当切面应用出现异常时，切面核心可作为异常缓冲；而当切面核心出现异常时，统一的代理逻辑可提供异常兜底机制，避免对业务产生影响。这极大地提高了切面基础设施对切面应用和业务应用的运行保障能力。

此外，由于切面应用可以对业务执行流的上下文等数据进行修改，并且能和应用服务一样访问系统资源和服务，如果不加以限制，一旦被恶意利用，切面应用自身将成为安全短板。平行舱的访问控制能力可以限制切面应用对业务上下文的读写，默认其只有只读权限。这对于大部分观测类的切面应用来说已经足够使用。此外，对系统资源和服务的访问，也可以通过平行舱限定在有限的范围内。每个切面应用默认只能访问属于自身的资源目录和提供有限的系统服务。只有经过许可的切面应用，才能执行额外的操作。

安全平行切面是一套安全基础设施。通过提供统一的干预与内视能力，安全平行切面可实现丰富的安全能力。同时平行舱可确保整个架构平稳、可靠地运行，进一步提升了整个架构的安全性和稳定性，为各类切面应用与应用服务之间和谐有序共存提供了必要的基础保障，为安全平行切面的大规模应用奠定了基础。

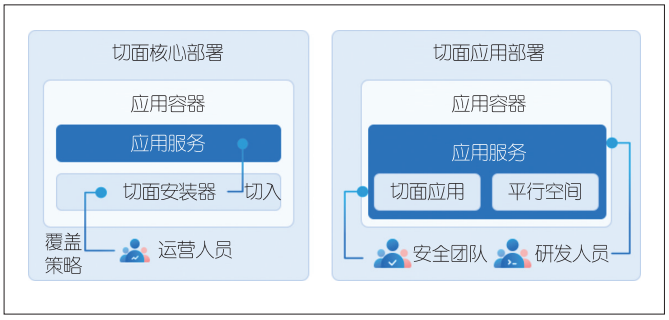
4 安全平行切面的规模化应用

4.1 基本部署结构

在安全平行切面大规模落地的过程中，为了降低推进成本，减少不同语言、框架应用带来的差异性，我们将安全平行切面的部署结构分为3个基本组成部分：切面安装器、切面核心和切面应用。切面安装器在接收到安装指令后，会将指定版本的切面核心包下载，并在应用启动阶段，对应用执行注入动作，进而完成切面核心的部署。切面核心部署与切面应用部署如图5所示。不同领域的安全团队，比如数据安全、系统安全、攻防对抗等，可以各自独立地对平行空间内的切面应用进行维护，从切面应用仓库中，选择并部署它们所需要的能力。整个过程不需要应用做任何提前准备和代码修改。在这种解耦的工作模式下，各个团队的效率都可以得到跨越式的提升。

4.2 切面规模化部署

安全平行切面是一个面向多语言、多框架异构应用的安全基础设施。不同语言和框架的差异性使切面核心的注入方式、启动方式等有所不同。为了尽可能降低由碎片化场景带来的运维交付成本，满足大规模部署要求，我们必须对适用于各类异构应用的切面进行运维操作统一化处理。因此，切面安装器应运而生。



▲图5 切面核心部署与切面应用部署

切面安装器是一个纯系统软件，可广泛应用于各类操作系统。在切面大规模部署之前，切面安装器需要先安装在所有目标应用容器之内。整个过程所需要的仅仅是系统软件的批量安装能力（在绝大多数云和企业中，这是一个比较常规的能力），并且这一过程通常是一次性的，成本相对可控。

在当下复杂的企业环境中，往往运行着各种基于不同语言和框架开发的应用服务。由于需要针对不同的应用服务决策下发不同的部署策略，因此切面管控管控端需要有足够的信息依据，以便判定一个应用是什么语言类型、适合部署什么版本的切面。由此可见，在切面安装器部署完成之后，首先要解决的是应用资产信息的收集问题。通过切面安装器自带的进程和环境信息上报能力，云端可以快速获取每个容器中运行服务的基本情况。结合配置管理数据库（CMDB）、代码仓库、平台即服务（PaaS）等，我们可以很方便地识别出容器内运行应用服务的基本信息，例如所属应用、开发语言、服务框架和负责人等，自动化地完成应用服务摸底任务。当然，对于一些元数据缺失的应用，我们也可以通过人工打标的方式完成资产判定。但是这对于存量应用的覆盖是有限的，无法实现增量应用服务的自动识别与覆盖，会产生一定的维护成本。

不同语言应用在切面核心注入逻辑上的原理与实现方式是有差别的。为了消除不同语言（或框架）切面核心的差异性，切面安装器定义了一套统一的安全平行切面部署执行标准。无论哪种语言类型的切面核心，都使用同一个安装包格式。安装包内除了有切面核心具体代码之外，还包含相对应的初始化脚本、注入脚本和启动脚本等。针对不同语言类型的切面核心，切面安装器只需要进行统一解压、校验，并按流程依次执行相应的脚本即可。标准化的运维操作可以让我们很方便地实现面向任意语言切面的统一部署流水线，配合

相应的监控、变更防御策略等，可以稳定、高效、自动化地完成大规模切面部署。

经过我们的实践测算，在确保稳定性的情况下，平均每1 000个应用服务在完成日常安全能力升级时仅需要10人日（紧急情况下，甚至可以在小时级时间内完成），而传统的强耦内嵌式的安全能力升级往往需要以月为单位计算。安全切面带来的效能和安全敞口收敛效果的提升是跨越式的。在整个体系验证完成后，蚂蚁集团就很快完成了全站95%以上应用的接入，并完成了核心业务全覆盖。整个系统非常稳定，至今未发生过故障，具有很好的推广价值和借鉴意义。

5 安全平行切面架构的收益

安全平行切面给企业数字生命体带来的最大收益是：能够在企业动态进化的架构中构建与业务逻辑平行的原生安全空间，将“疫苗”快速、稳定、高效地注入给受保护的目标。安全平行切面架构能够将安全逻辑深入到应用服务内部，天然具备更细粒度且更为精准的感知和干预能力。同时由于安全平行切面架构具有与业务解耦的特性，因此在效率与成本方面，优于很多传统的内嵌安全架构。使用不断扩展的切面应用可以实现各种丰富的安全能力。经过不断探索，蚂蚁集团目前已经拥有40多种切面应用，包括负责对抗和漏洞感知的切面应用（RASP、IAST等），以及和数据与隐私保护相关的切面应用（隐私数据的流转和血缘分析、敏感接口的确权控制等）。

5.1 运行时安全防护

2021年底，Log4j被爆出存在命令执行漏洞，影响范围广泛。因攻击难度低、变种多、内网穿透强性，log4j危险性极大。一方面，当时蚂蚁集团正处于双十二购物狂欢节（以下简称“双十二”）大促业务稳定性保障的关键时期。在大促封网的关键时期，启动全局范围的修复阻力非常大，会耽误最佳的应急时间。另一方面，由于log4j的攻击变种比较多且具有相当强的内网穿透性，所以边界层Web应用防护系统（WAF）的止血效果也十分有限。而基于安全平行切面实现的、大规模部署的RASP应用，可以很好地防御此次漏洞攻击：只需要在漏洞执行链的关键切点进行阻断即可，精准且高效。借助安全平行切面的快速部署能力，安全团队在小时级的时间内就完成了全站数千个应用、几十万容器的防护升级，最终阻止了40多万次真实外部攻击，实现了0漏报和0误报，使应急人力投入从预期的6 000人日降到30人日，大大提升了安全防护效率，缩短了安全风险的暴露时间，顺利抗住了“双十二”的流量洪峰。这个案例很好地体现了安全切面应用的精准感知和管控能力，即安全切面应用可以在非常细粒度的关键点上进行布防。不管外层如何变化和隐藏，都绕不过最终的执行点。同时，整套架构和业务自身是解耦的，不需要业务感知，极大提升了整体的应急效率。

5.2 数据要素流转治理

在业务运转过程中，数据就像血液一样流动。敏感数据伴随着普通数据在应用及数据存储间快速流转。基于敏感数据传输的上下文最终呈现数据血缘关系。基于切面体系实现的数据采集能力发挥其与业务融合又相对解耦的巨大优势，大大提升了数据安全治理的可观测性。可观测性是指对海量、异构、复杂数据的采集、分析和展示能力，即不仅能够在流转的复杂结构数据中识别敏感数据，还能够对敏感数据进行准确分类和分级。基于安全平行切面的数据安全应用能够按照数据类型和采集需求动态下发采集规则，实现对指定接口读写数据的行为采集。后继结合图分析技术，将信息进行融合分析，可以还原整个数据处理流程，构建完善的数据链路血缘。通过安全平行切面架构对数据要素共享治理体系进行升级后，数据要素的分类分级识别能力、数据采集的可达范围均可产生显著提升，并将风险感知和处置的时效提升至分钟级以内。

5.3 移动应用隐私风险治理

移动应用特别是平台型APP存在大量第三方SDK、小程序、H5页面等。由于缺少运行时的监测和管控技术，线上实际调用行为无法被观测到。这导致APP的行为记录、解释和追溯变得极为困难。当出现问题之后，系统很难进行紧急阻断。传统方式下，应用的安全风险治理主要通过APP上架前的安全研发生命周期管理（SDL）和上架后的APP发版对漏洞进行修复。这种方式存在一些问题：

（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，但误报率高，且无法检测动态加载的行为；动态检测可以模拟的环境有限，只能触发有限的业务场景。

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

（3）难以修复。从发现问题到发布修复版本往往耗时数个月（3～4个版本），这给研发带来巨大负担。

利用代码植入技术、运行时函数信息监测技术、风险行为检测算法和运行时函数行为管控技术，移动端安全平行切面架构可以提供移动应用数据内视、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。目前通过对安全平行切面获取的数据进行收集和挖掘，我们已经发现多个日活跃用户数达到亿级的移动应用的数十项隐私合规风险，包括隐私泄漏、后台调用异常、超频次使用、未授权调用等。这些风险可通过动态下发切面管控配置进行修复，不需要通过APP进行重新发版。

6 结束语

本文中我们将当前企业信息架构类比为数字生命体，将数字生命体的网络攻击防护与新冠病毒的防护进行类比，阐述了安全平行切面的内涵，并总结了网络与信息安全形势面临的3个趋势：企业数字生命体持续动态进化、业务规模及业务逻辑复杂性爆炸、高强度攻防对抗及安全治理日趋常态化。在这样的背景与趋势下，传统静态安全架构已显得力不从心，原生安全架构比“口罩”的静态安全架构有更加理想的安全效果。安全逻辑与业务逻辑紧密结合所带来的巨大收益逐渐被人们重视。我们认为安全架构与企业架构实质性融合的时代即将到来。如何将安全逻辑像疫苗一样安全、稳定、可靠、大规模地注入到应用内部是安全平行切面需要应对的挑战。此外，本文还介绍了蚂蚁集团安全平行切面架构和平行舱技术，阐述了如何通过疫苗运维基础设施对安全疫苗实施全生命周期的运维保障。蚂蚁集团应用安全平行切面所取得的收益或许能够为安全行业带来新的建设思路。

致谢

在本文撰写过程中，蚂蚁集团郑旻、王少宇、李婷婷给予了大力支持，特此感谢！

参考文献

[1] FreeBuf 咨询 . CCSIP 2022 中国网络安全产业全景图（第四版）[EB/OL]. (2022-07-21)[2022-10-15]. https://www.freebuf.com/articles/339788.html
[2] 蚂蚁科技集团股份有限公司, 中国电子科技集团第十五研究所(信息产业信息安全测评中心). 安全平行切面白皮书 [R]. 2021
[3] KICZALES G, LAMPING J, MENDHEKAR A, et al. Aspect-oriented programming [EB/OL]. [2022-10-15]. https://www. cs. ubc. ca/~gregor/papers/kiczales-ECOOP1997-AOP.pdf

作 者 简 介

韦韬，蚂蚁集团副总裁、首席技术安全官，浙江省科学技术协会委员，北京大学客座教授；20多年来一直致力于让各种复杂系统变得更加安全可靠，牵头和推动了多项知名开源项目的研发工作，在全球首创了安全平行切面、可信密态计算等重要安全技术体系，在安全攻防、隐私保障、合规治理等领域有着丰富的实战经验，2022年入选IDC“中国CSO名人堂（十大人物）”。

顾为群，蚂蚁集团安全平行切面产品经理；深耕网络与信息安全产品领域10余年，致力于通过产品与解决方案链接创新技术和复杂业务场景，主导和参与蚂蚁集团在安全平行切面、生产网零信任、应用安全、威胁对抗、数据安全等多个领域的产品体系建设。

刘宇江，蚂蚁集团安全平行切面架构师；长期从事企业基础安全领域的体系架构与建设工作，具备丰富的大型互联网企业安全建设实践经验，先后负责蚂蚁集团的安全感知、威胁对抗、零信任与安全切面等安全体系的设计与落地，深度参与了蚂蚁集团历代基础安全能力的架构演进升级工作。