IDC | 蚂蚁集团 ANT GROUP | AOTA 安全平行切面联盟 Aspect-Oriented Technology Alliance

安全平行切面

—— 数字时代的原生安全架构

致谢

在撰写期间，本白皮书得到蚂蚁集团韦韬、王宇、李婷婷、李宏宇、王珉然、程岩、吴飞飞、马传雷、郑旻，平安集团首席信息安全总监陈建，中国移动首席专家王晓征，红途科技CEO刘新凯，吉利汽车数字化中心CTO郑金伟的大力支持。

感谢刘宇江、党二升、徐子腾、莫书棋、庞培、黄文静、罗海棠、蓝潞、崔虹、顾为群、傅成彦、王延辉对于白皮书内容的指导，提供了宝贵的资源和素材。

感谢红途科技、浙江移动、平安科技等切面联盟成员单位，以及合作企业吉利汽车集团，作为受邀企业，贡献了关于安全平行切面实践落地的重要观点和宝贵经验。

特此致谢！

Contents

IDC观点

数字化优先时代，复杂性爆炸给未来信任体系的构建带来重重挑战

当企业数字化转型迈向纵深，从以开展数字化试点项目为主的实验阶段，发展至通过数字化手段与业务深度集成助力业务创新的高级阶段时，进一步践行数字化优先战略成为全球企业的必然选择，以进一步扩大技术使能范围，实现切实有效的规模化创新。在业务发展和政策驱动的背景下，企业领导者持续关注网络安全、数据安全的建设，以保护和扩大企业的可信度，构建更具竞争力的企业未来信任体系。在此过程中，数字化业务的蓬勃发展带来了更多的复杂性。伴随整个行业的技术演进，数字化企业逐渐出现了多代系统堆叠并存的局面，企业内部的应用、数据、访问主体和管理对象都在急剧增长，内部、内外部之间的数字化接口繁多，技术体制混杂，缺乏足够的标准规范约束。同时，企业在发展过程中引入了大量外部系统，一些系统呈现技术上的黑盒状态，其安全合规方面的风险很难得到准确评估。此外，数字化系统所支撑的业务流程也在持续迭代升级，导致复杂性进一步增加，企业的安全包袱越来越大，潜在隐患不容小觑。

安全平行切面支撑原生安全范式落地，让业务长出新的安全触角

数字化企业可被视为一个完整的数字生命体，能持续发展出有机生命所必须的成长进化、复杂交互和全局智能能力。在复杂性爆炸的背景下，企业亟需解决的核心问题，是如何对复杂的数字生命体实施全局性、持续性地保护，强化安全效能，提升安全效率，实施规模化的安全感知和干预。“原生安全范式”为企业安全发展提供了理想的目标和参考方案，帮助企业从复杂业务的本源出发，在系统设计时就全面考虑安全与业务的融合问题，从而实现分布式、实时化、工具化的企业安全防护能力。在支撑原生安全思想落地的过程中，安全平行切面作为理念、方法论、技术框架和工程化平台的集合，开始在企业安全实践中快速发挥效用。通过构建切点、切面和安全平行舱等方式，企业一方面可以实现面向业务的深度感知和干预能力，另一方面也为安全能力的迭代发展建立了较为独立的空间，体现出安全与业务之间的

高融合、低耦合。安全平行切面是支撑未来企业安全架构的重要技术方向，也是提升安全防护水平的全新方法体系。

安全平行切面有望创建更多的安全场景，为企业安全运营带来全新价值

安全平行切面作为一个基础技术框架和服务集合，具备区别于传统安全体系的一系列突出能力特性，包括多维深度感知、微观干预和编程扩展等。其重构了安全与业务的协同关系，让安全真正融入到业务本身，实现业务行为的可知、可见、可控。因此，安全平行切面有望为网络安全、数据安全、个人信息保护等领域带来**跨越式的变革，**也有望推动一大批安全、合规、攻防和安全保险等场景的创新发展。在面向当前和未来的应用场景落地时，安全平行切面的理念以及落地实践过程，能够在能力、效率和成本方面体现出显著的优势，为企业安全运营带来全新价值。

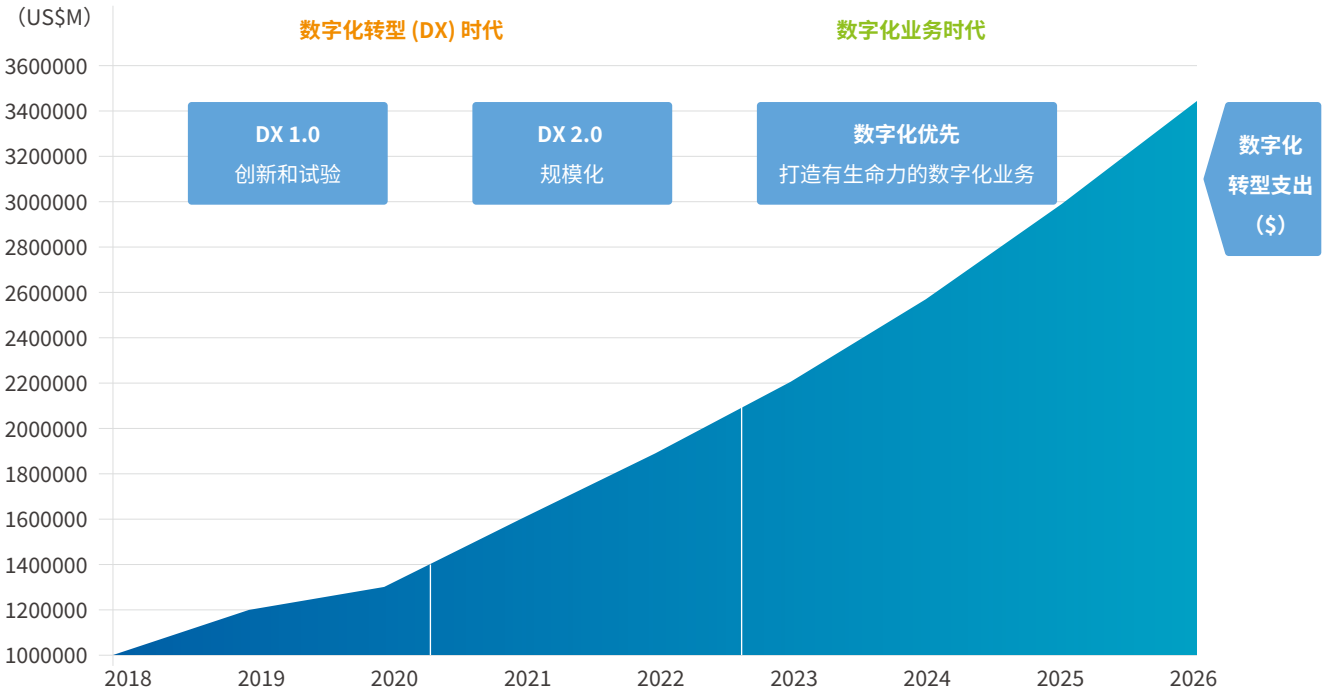
第一章

数字化时代下
安全能力是守护企业创新力的基石

1.1 围绕未来信任构建新一代安全体系，为企业创新保驾护航

数字化优先战略成为全球企业发展的确定性趋势，企业将持续增加数字化转型投资。伴随全球数字经济的蓬勃发展，云计算、大数据、人工智能、5G等信息与通讯技术的应用范围在不断扩大，推动了行业创新场景的规模化涌现。目前，全球企业的数字化转型已进入持续深化阶段，企业在不断进阶的过程中，切身感受到了数字化带来的巨大价值，也促使决策层更加坚定决心，逐年加大数字化转型的投入。IDC数据显示，2022年全球企业数字化转型投资规模超过1.5万亿美元，并有望在2026年超过3万亿美元，2021-2026年五年复合增长率（CAGR）约为16.7%。中国的数字化转型市场将保持高速增长态势，到2026年，中国数字化转型支出规模预计超过6,000亿美元，五年复合增长率达到17.9%，增速位于全球前列。

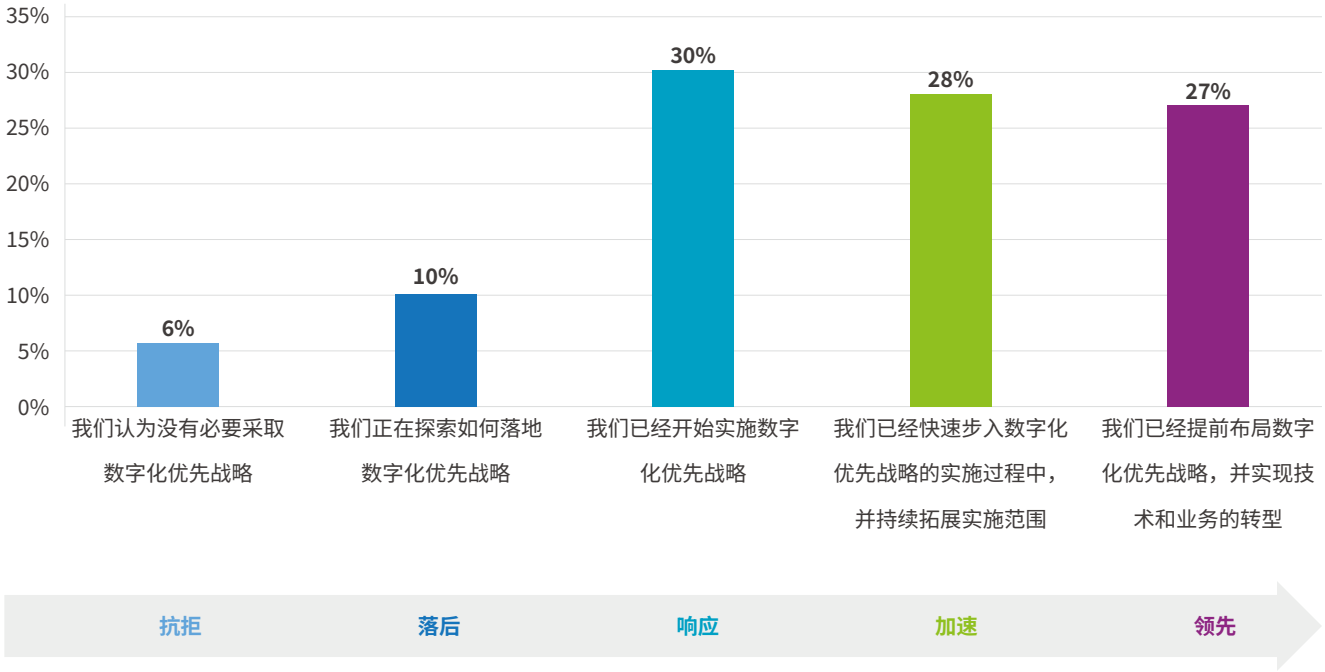
图1 IDC全球企业数字化转型支出预测



来源：IDC，2023

在数字化转型发展至高级阶段时，进一步践行数字化优先战略成为全球企业的必然选择。数字化优先是指一个组织为了实现业务目标，能够优先考虑各类数字技术的部署和应用，进而不断满足客户需求，提升组织竞争力，实现可持续发展。数字化优先的显著特征是企业开始全面利用数据驱动业务创新发展，进而构建一种自上而下的全新思维和行动模式。IDC企业数字化优先战略调研显示，大多数企业都已经开启了数字化优先战略的尝试，企业会根据自身的具体情况，全面或有重点地推动数字化业务的开展。

图2 全球企业对数字化优先战略的采纳程度



来源：IDC，2023

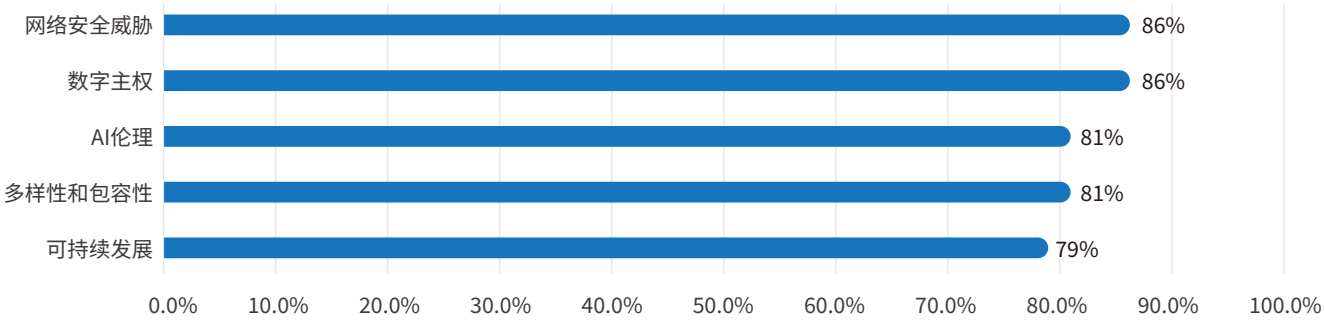
企业在数字化竞争中欲取得优势，必须对数字化业务和应用进行持续投入。大量的企业正在向实用可行的数字化业务阶段过渡。在实践数字化优先的过程中，企业需要依靠大量应用程序构建数字化业务大厦，以实现客户体验提升以及推动规模化共情、企业和生态系统智能、智能/自动化设备发展等。事实上，对于大型企业而言，当前的数字化应用发展速度已然令人震惊。例如，喜力在其全球运营中使用了4,500个应用程序；摩根大通仅在一个云应用程序平台上就运行了1,522个生产应用程序。IDC统计显示，仅2022年，全球就产生了3.1亿个新应用。IDC预测，到2023年，全球超过50%的GDP将依赖于已完成数字化转型的企业提供的产品和服务；到2025年，超过三分之二的G2000企业将成为高性能、大规模、基于软件的数字化创新生产商。企业希望依靠软件应用程序创造市场价值，获得可观的回报。

图3 应用成为构建企业与市场、企业内部、企业与上下游之间的价值创造纽带

来源：IDC，2023

业务发展和政策驱动背景下，企业领导者持续关注网络安全、数据安全的建设。数字化业务和应用的快速发展，带来数据量的激增，企业暴露的危险点也不断扩大。如何保护应用安全、数据安全以及业务安全，成为企业上下广泛关注的话题。Edelman的一份报告中对400名首席信息官的调查结果显示：“大多数首席信息官认为他们的领导地位与公司的声誉和形象直接相关。”IDC全球在2022年开展的一项针对CEO的调研表明，网络安全和数据主权是企业管理层最关注的发展议题。此外，“网络安全法”“ 数据安全法”“个人信息保护法”以及“欧洲一般通用数据保护条例（GDPR）”等一系列国内外安全法律法规的相继出台和落地，对企业数字化转型带来制度、组织、技术、预算等多个维度的影响，也让企业更加重视安全合规能力的建设。

图4 2022年全球CEO最关注的企业发展议题



来源：IDC，2023

信任是数字化业务健康运行的必要条件，企业领导者必须保护和扩大企业的可信度，构建更具竞争力的未来信任体系。面向全球数字化转型实践，IDC创建了完整的信任框架体系——未来信任。IDC认为，信任涉及安全、风险、合规、隐私以及商业道德，企业未来信任建设不仅需要保护企业免受攻击，建立更高的道德标杆，还需要对收入、支出和股东价值进行可量化的影响评估。因此，企业需要通过有效的风险管理、监管合规、安全管理以及宣传隐私保护、道德规范和社会责任，来建立与客户、员工、合作伙伴及业务生态系统之间的信任，这不仅有助于企业满足合规要求，更是为企业的长期发展和声誉建设提供坚实的基础。IDC认为，未来信任包含基础、义务、战略、实现四个层面的6个关键要素（也称信任支柱），并通过可信治理、可信生态和可信商务三个实施层实现信任的产出。以未来信任为基础的新一代企业安全体系，对于企业发展和业务升级具有极大的价值。

图5 IDC未来信任要素

来源：IDC，2023

1.2 复杂性爆炸是未来信任体系必须面对的核心问题

在构建信任体系的过程中，企业将面临一个极具挑战性的现状：数字化业务在提升创新力的同时也会带来更多的复杂性，大幅增加建立信任的难度。IDC针对全球不同行业代表性企业的长期研究发现：在企业数字化转型发展至一定阶段后，数据与业务相融合的运行形态将帮助这些数字化企业成长为一种不断演变进化的生命体；这种演进迭代是持续不断的，甚至还会呈现出加速的态势。

数字化企业伴随整个行业的技术演进，会逐渐出现多代系统堆叠并存的局面，且企业内部、内外部之间的数字化接口繁多，技术体制混杂，缺乏标准规范的约束。同时，企业在发展过程中引入了大量外部系统，一些系统呈现技术上的黑盒状态，其安全合规的风险很难被准确评估。此外，随着业务的快速发展，数字化系统所支撑的业务流程也需要持续迭代升级，导致复杂性进一步增加，企业安全包袱越来越大，潜在的隐患也不容小觑。

企业数字化业务发展所出现的复杂性覆盖以下六方面：

- **快速增长的应用数量：**如前文所述，企业越来越依赖软件应用来提升内部效率、增加营收以及获得其他战略业务成果，因此，应用程序的数量出现爆发式增长。全球企业上云的大趋势，进一步加速了新应用产生的速率，因为大量的云上平台和中间件能够让应用系统的建设更加快速和便捷。IDC预计：到2025年，全球将创建7.5亿个云原生应用程序。

- **海量的数据：**物联网和大数据等技术的快速进步，让数据的采集、开发和治理成为企业数字化转型的常规能力要求。一方面，企业数据规模出现接近指数级的爆炸性增长。IDC数据圈研究预测，2027年全球新产生的数据量将达到291ZB，近乎2022年的3倍，五年年复合增长率达到22.4%。另一方面，数据链路的覆盖范围持续扩大，数据全生命周期所触及的系统、平台、流程和角色更加广泛，数据形态变化频繁，数据的活跃度也在不断加强。

- **多样的访问主体：**企业业务的多元化、全球化趋势，伴随数字经济、线上经济的蓬勃发展，使企业的跨地域、跨行业交互成为常态。为了支撑业务的全球触达，数字化系统的开放性越来越强，边界也变得更加模糊，内、外部数据的交换需求和随时随地的登录请求，使各类系统的访问主体出现爆发式增长，用户的身份极为复杂，授权管理稍有不慎即会带来灾难性的后果。

- **不断增加的管理对象：**数字化业务所触达的对象也在快速增加。IDC预计，到2025 年，全球联网设备的数量将超过 420 亿台。企业云平台上汇集了极为丰富的PaaS组件和分布式中间件产品，大量的外部系统带来了快速膨胀的API管理规模，边缘设备和软件定义网络的使用也使运维形态发生了显著变化，数据要素和其所有者、使用者成为新的关注重点。企业数字化业务的管理对象呈现出类别多样、虚实融合的新现象。

- **更加严峻的威胁：**伴随数字化业务带来的在线、协同和智能化提升，各类攻击也随之变得更具规模化和组织化。大量增加的数字化系统暴露出更多的漏洞和风险，使攻击者有了更多可趁之机，攻击手段更加敏捷，攻击效率持续提升，给企业带来的损失与日俱增。国家互联网应急中心（CNCERT）发布《2021年上半年我国互联网网络安全监测数据分析报告》中的数据显示，2021年上半年，国家信息安全漏洞共享平台（CNVD）收录通用型安全漏洞13,083个，其中“零日”漏洞数量占比54.3%，同比增长55.1%；Web应用漏洞的影响持续上升，占比达到29.6%。根据美国商务部国家标准与技术研究所（NIST）国家漏洞数据库（NVD）的报告，2022年新增漏洞26431个，同比2021年增加25.87%。此外，伴随生成式人工智能的发展，企业亟需提升对未知威胁的检测、分析效率和准确性，通过自动化/半自动化的方式降低安全运营人员的工作负载。

- **日趋复杂的访问路径：**随着大量的应用由传统单体架构转变为以云为承载的微服务架构，应用软件呈现出更多的弹性和动态特征。传统单体架构下的程序主体数量有限，内部访问路径相对单一和固定；微服务的出现显著增加了应用内部受访主体的数量，软件交互的复杂度急剧攀升，访问路径呈现出指数级增加态势，导致应用防护出现更多的不确定性。

技术的演进、系统的升级以及数字化业务的快速发展，共同导致企业运行的复杂性出现爆炸性增长。这种复杂性将会给企业未来信任体系建设带来一系列难题。企业现有的安全管控措施日趋乏力，企业疲于应付各类安全事件，业务效率会受到极大影响，其在处置各类安全事件以及弥补安全事件所带来的损失时，将付出更多的被动成本。

整体安全局面失控的风险大增

- **安全需求超越企业安全能力上限：**未来企业将引入更多的第三方软件和开放源代码，因此，确保软件供应链的安全对于降低应用程序风险至关重要。威胁的多样性和应用系统的复杂性常常会超出企业安全能力的设定，让CIO/CISO和安全团队倍感分身乏术，技能的缺失和不全面的布局也会导致应用成为外部攻击的突破口。

- **数据资产管理和数据安全出现短板：**大量增加的企业数据使管理流程不堪重负，很多数据长期处于无序管理状态，数据流转路径复杂。企业缺少对数据资产实现全面盘点的手段，数据分类分级管理和全链路监控更是无从谈起，导致数据资产底数不清，数据泄露、丢失和损毁情况严重。

- **安全体系出现明显漏洞：**数字化环境的复杂性变化也会导致传统的安全体系出现薄弱区域。由于一些关键环节上缺乏安全日志数据和阻断手段，在遭遇新型攻击时，攻击者往往可以轻易绕过安全设置区域，使安全保障团队长时间不能明确攻击来源，也无法洞察攻击链路。大量云上应用在线访问所带来的AK滥用现象更是加剧了安全体系的崩溃风险。

安全管理效率显著降低

- **安全协同问题：**一方面，企业安全能力的迭代与业务创新能力的迭代不同步；另一方面，复杂性爆炸导致安全与效率的矛盾更加突出，企业在疲于应付安全威胁的过程中，采用了大量不科学的安全设置，经常导致业务在运行中出现严重阻塞，甚至自乱阵脚。

- **安全风险和安全事件处置不及时：**企业存量系统的安全改造占据了安全团队的绝大多数精力和时间，系统和漏洞修复速度经常落后于攻击方，使大量的工作成为无用功，不能及时对新威胁和新漏洞做出快速应急处理。例如，传统漏洞修复流程需要经历多个环节，包括确认是否做、做什么、如何做，以及执行补丁修复后的复杂测试和验证工作，这些工作动辄需要一个月的时间，远远落后于恶意代码的生成速率。

安全管理和运维成本疾速增加

- **安全产品成本：**传统安全保障模式下所采购的安全产品，已经愈发难以满足规模化扩展的需求，导致安全改造的成本居高不下。云上应用的弹性访问需求变化，常常使安全设施难以招架，而对这些安全产品进行云化改造，又会引起整体架构的一系列变化，让企业产生很多额外的顾虑。

- **运维和运营成本：**由于企业在安全集成模式下采购了多样化的安全产品，后期的运维成本也在持续增加，这其中既包括统一管理过程中的庞大开销，也包括各类产品长期升级特征库所带来的巨大支出。

- **现有系统修复成本：**企业在遭遇安全风险和安全事件时，往往面临经济成本和时间成本上的双重压力。IDC研究发现，2018年，单个关键工作负载的平均宕机修复成本为 48,700 美元/小时。以漏洞管理为例，根据Edgescan的报告，企业关键严重性漏洞的平均修复时间为65天。整体上看，IDC数据显示，2022年，全球应用漏洞管理市场规模超过25亿美元，同比增长13.5%。这意味着企业正在投入更多的成本来应对应用漏洞风险。对于大型集团性企业而言，漏洞管理工作可能需要覆盖几十、上百种应用，成本将会更高。随着应用复杂性的增加，这类修复工作将会变得更加困难，很多时候需要专业团队长期驻场，使之成为昂贵的定制化服务，给企业的成本管理带来无法承受的压力。

第二章

构筑安全平行切面
打造下一代原生安全

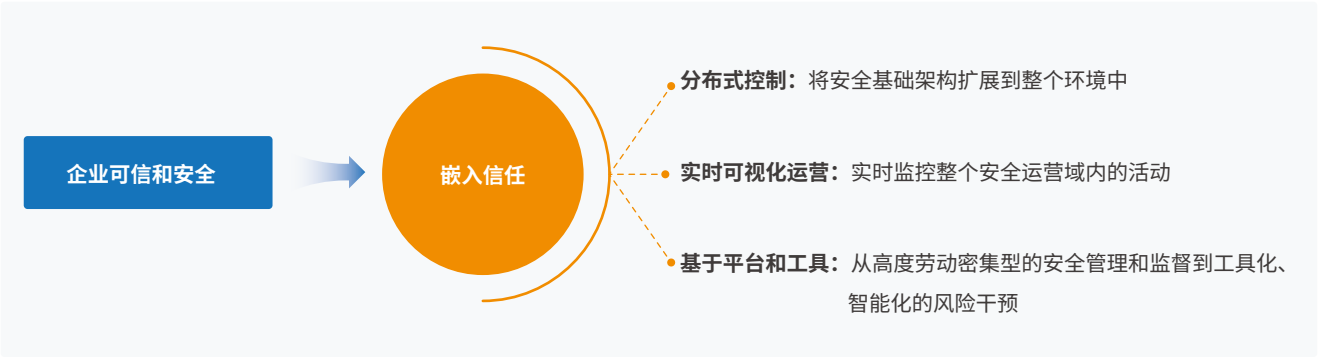
2.1 原生安全范式：企业安全建设应明确技术要求

在复杂性爆炸的背景下，企业亟需解决的核心问题，是如何面向完整的复杂数字生命体实施全局性、持续性保护。传统的安全防御往往依赖单点能力，以边界为重心构建防御体系，既看不到应用内部的数据流，也看不到外部数据在应用内部产生的变化和扰动，无法满足企业更细粒度、更高效、更规模化的防护需求。

为了消除复杂性爆炸带来的一系列安全隐患，企业应考虑如何引入安全领域的新理念和新成果，全流程优化安全服务体系，覆盖产品研发、交付、运维、运行等关键环节，推动安全实践过程从粗放式发展转向精细化发展。同时，企业也可将很多临时性的安全行动和零散的工具整合为平台化能力，实现对动态数据的可视化洞察和治理，以更加积极地应对多元风险造成的敞口，构建不断进阶的信任体系，强化综合决策能力，在新的安全理念、安全战略引导下，实现企业安全架构的全新进化。

新的企业可信和安全目标的达成，必须以正确的安全范式为顶层设计指引，逐步将安全能力融入到数字体系中，构建面向安全对象的分布式控制能力、实时可视化运营能力，以及基于平台和工具的自动化、智能化干预能力。

图6 将安全能力融入企业不断演进的数字体系



来源：IDC，2023

IDC认为，在向企业嵌入信任的过程中，企业应高度关注安全实践领域的几个重要演进趋势：

- **架构演进：**中心化部署的安全产品将向分布式部署的安全资源演进，确保安全能力与业务如影随形；
- **方法演进：**安全能力将从代码化向策略化演进，即从能力的迭代演进为策略的升级，使产品升级的时效性不断得到增强；
- **规模演进：**安全资源将从离散化向规模化演进，企业必须具备可大规模部署的安全运维、调度、干预（隔离）能力。

以此为依据，企业安全体系能力和服务升级目标可包括：

- **强化效能：面向当前和未来的业务发展设计敏捷安全架构。**在企业数字化转型的大背景下，数实融合进程快速推进，企业应用的规模和覆盖范围也越来越大。为了更好地支撑海量数据的管理和价值挖掘，满足应用的快速迭代要求，企业安全架构必须做出相应的变革：既要解决好安全与业务协同中长期存在的固有矛盾，也要关注海量数据资产保护、零信任体系构建等新的安全需求。

- **提升效率：适应数智化时代的变化节奏，提高安全攻防效率。**企业数字化应用的访问主体、管理对象等方面的复杂性爆炸问题，让安全威胁和安全事件所能带来的影响加速扩散。企业需要尽快建立起细粒度的实时感知、分析和快速干预能力，将安全事件的影响尽可能地化解于早期；同时，也需要提升安全领域的研发迭代效率，在保持防御体系先进性的同时，尽量减少安全事件对业务系统连续性的影响。

- **形成规模效应：构建高价值、资源池化的安全体系。**企业数字化资产的规模在快速提升，包括快速增加的基础设施、应用系统、终端以及呈指数级增长趋势的多模态数据。因此，企业在构建新一代安全架构时，必须考虑到对规模化数字资产的防护干预能力。例如，在发现新的安全漏洞时，企业应当能够在最短的时间里，最大程度地对可能遭遇威胁的系统进行修补，避免遗漏情况的发生。未来，安全资产的管理模式和安全能力的输出形式都将发生明显的变化，安全能力不仅要能快速调用，还必须做到统一管理，用平台化的方式，实现从中心化到资源化的转换，以满足复杂环境下对数据、系统、应用、设备、人员等的规模化防护需求。

如何实现上述目标？“原生安全范式”提供了一个极具价值的参考方案。“原生”体现出安全需求要从复杂业务的本源出发，从系统设计开始就全面考虑安全与业务的融合问题。“范式”则意味着将这样的安全能力整合输出为一套企业可遵循的规则和要求。“原生安全范式”旨在解决企业信息安全的本源问题：一是避免安全防护手段被绕过，二是避免受信任的权限被滥用。

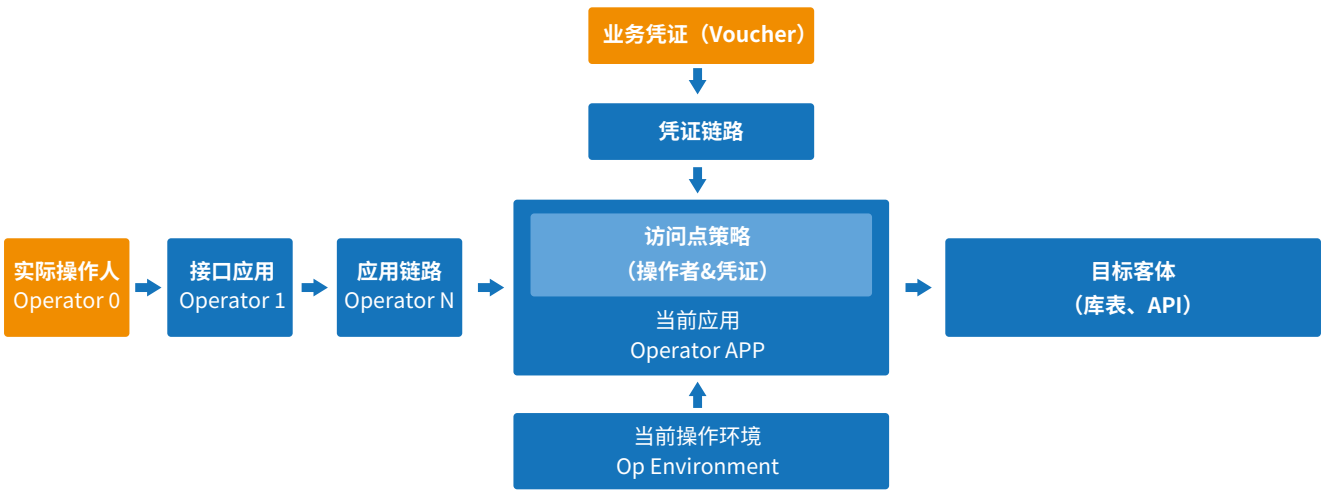
“原生安全范式”为企业安全发展提供了理想的理论依据、实践指导和实践经验归纳，可用于指导企业构建全领域、全周期、工具化、标准化的整体安全防护能力。例如，基于“原生安全范式”的规则要求，所有的认证都应该基于可追溯的凭据，即保证所有的验证过程都可被视为具有可靠性。在传统的安全体系中，仅验证身份的方式不足以满足日趋复杂的安全形势要求，访问者在什么场景下施加了什么行为、获得了什么资源，都需要被进一步验证，以确保访问行为的合理性、合法性和合规性。企业应建立起全方位的鉴权能力和链路追踪能力，明确由谁发起请求，明确用户访问链路，明确访问者权限范围，并确认其是否可以操作相应的资源。

安全范式作为重要的安全理念，体现为一套体系化的安全要求，是对安全问题本源认知的设计规范和参考架构。事实上，企业之所以在大量的攻击中遭受损失，往往都是因为没有达到安全范式的模式要求。违背安全范式是造成安全事件的主要原因，当企业缺乏明确的技术要求和整体性的防护思路时，非常容易出现越权访问和权限滥用的现象，使防御体系出现大量的薄弱环节。此外，在人工智能迅速发展的背景下，企业完成数据管理和价值挖掘的水平将很大程度影响对于人工智能的应用，在这个过程中，执行“原生安全范式”能够帮助安全团队更全面地探测和治理数据相关问题，进而为企业的智能建设奠定良好基础。

在探索原生安全范式的过程中，有两个典型范式具有代表意义，它们在传统安全思路中未被触达，但对安全结果会产生直接影响。

- **OVTP可溯范式：**基于对网络访问安全本源的认知辨析，完整准确地研判一个网络访问是否合法，应基于该访问操作者的访问链路信息(包括实际操作人、访问链路上的应用以及相关运行环境信息)与凭证（Voucher）的传递链路信息，即站在一个数字化企业的全局视角，对所有网络访问的合法性进行研判，确定应该获取和分析哪些因素。

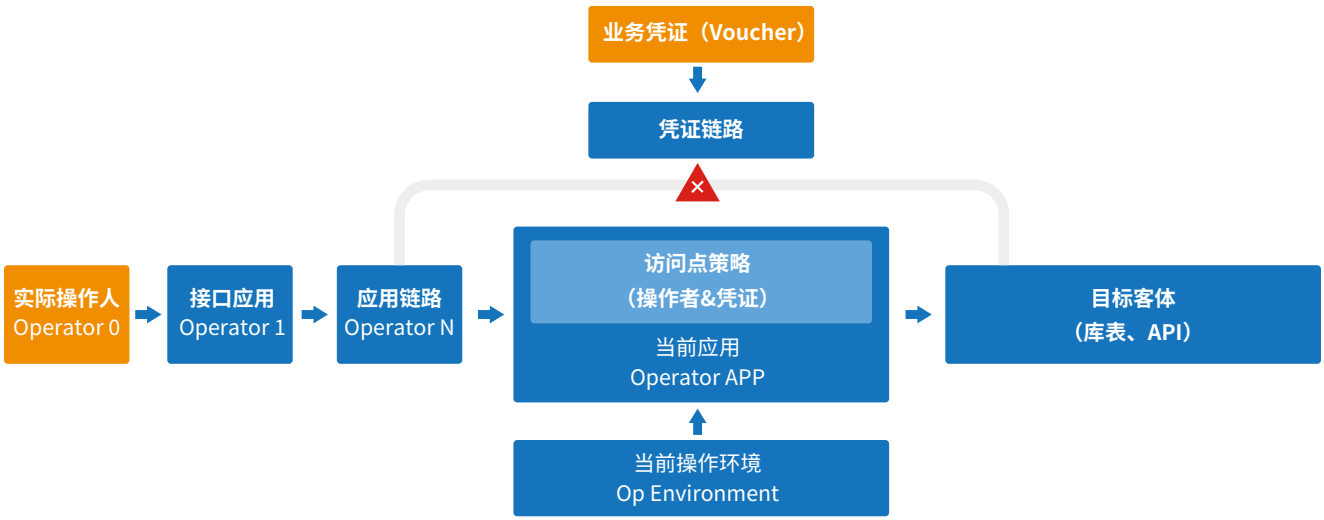
图7 OVTP可溯范式（Operator-Voucher-Traceable Paradigm）示例



来源：蚂蚁集团，2023

- **NbSP零越范式：**应确保关键安全检查点不可被绕过。当前，数字化系统的内部执行链路极其复杂，一些隐性链路或被滥用的链路，可以被攻击者用于绕过安全检查点，导致整个安全保障体系非常容易被击穿。对于新的核心系统，应通过模型检验等形式化验证方法来证明系统中不存在绕过安全检查点的执行路径。对于已有的业务系统，应用在主客体业务之间的关键核心节点上，动态增加策略执行的横切点，识别并阻断各类绕过关键检查点的非法行为。

图8 NbSP零越范式（Non-bypassable Security Paradigm）示例



来源：蚂蚁集团，2023

2.2 安全平行切面：为企业生命体注入“安全疫苗”

原生安全范式为新一代的企业安全架构设计提供了理想的目标指引。在支撑原生安全范式落地的过程中，**安全平行切面**的构想被适时提出，并开始在企业安全实践中持续发展迭代。原生安全范式是对安全问题本源的探索，安全平行切面则是支撑未来企业安全架构的重要技术方向，是提升安全防护水平的全新方法体系。二者相辅相成，让安全理念得以落地。

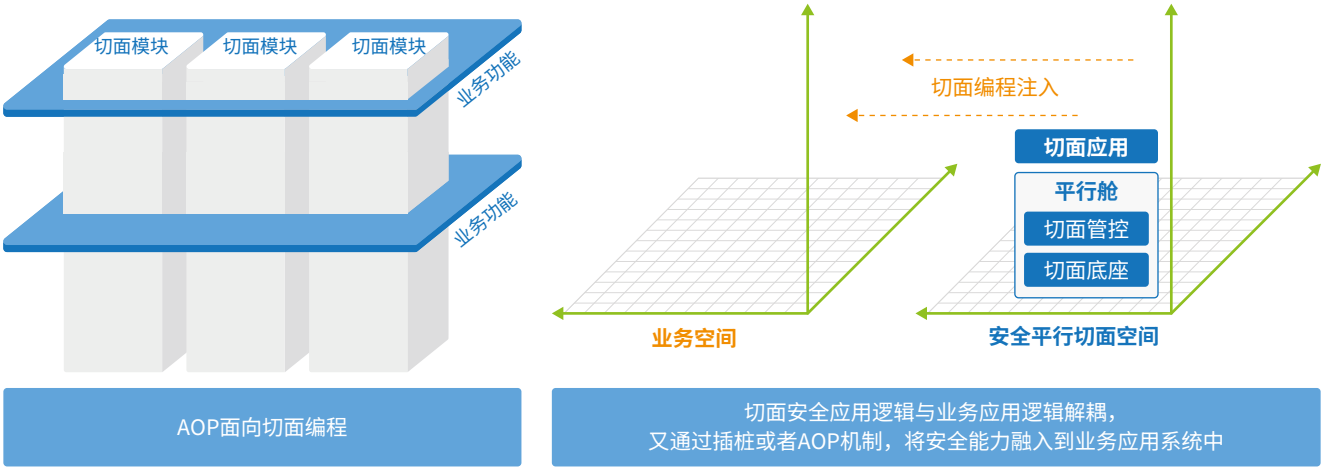
安全平行切面是一种面向未来安全、承载安全攻防对抗和安全治理能力的基础框架。它会通过构建与业务环境低摩擦的安全友好架构，带来攻防能力和安全治理效率的显著提升。**安全平行切面的核心思想是：**将编程语言环境下的Aspect-oriented Programming （AOP面向切面编程）推广应用到安全架构建设中，构建与业务正交融合的安全横切面，在不修改业务逻辑的情况下，通过横切面上的切点将安全能力系统化地融入到业务内部。此举有助于在保持安全响应能力和复杂业务逻辑解耦的同时，通过标准化的接口，为安全业务提供内视和干预能力。安全平行切面是一种创新的安全架构，是低成本实现“原生安全”、快速增强应用服务内在“安全体质”的可行路径。

安全平行切面像“疫苗”一样，伴随企业数字生命体的成长而不断演化，帮助企业以内生的方式应对复杂环境带来的安全挑战，成为企业数字化环境不可或缺的组成部分；同时，在不对企业数字生命体造成不利影响的前提下，帮助企业持续强化自身的安全基础，企业可以同时拥有多个安全切面，在互不干预的前提下，发挥出不同的“免疫”防护作用。

从实践层面看，“切面”是面向企业数字生命体的新一代安全基础平台定义，能够通过插桩或者AOP机制，将安全能力融入到业务应用系统中，同时又通过将切面安全应用逻辑与业务应用逻辑解耦，实现安全与业务的快速平行迭代。从某种意义上说，AOP是Object-Oriented Programming（OOP面向对象编程）的重要补充，两者相互影响，彼此延伸。

传统的安全实践一般以不同的业务系统为目标主体，将安全能力通过编排组合，附着在业务系统的各个环节中，形成“个体化”的设计。安全平行切面则把一些高频使用的安全模块抽象出来，形成独立发展的能力项，并以AOP机制为支撑，实现独立部署，使交付和运营过程更敏捷，安全代码复用性更强，如图9所示。安全平行切面能够将更多的安全能力转化为基础设施资源，以更加全局化、全链路的方式，为规模化应用提供安全保障。

图9 安全平行切面示意图



来源：IDC，2023

安全平行切面解决方案有助于企业发展出更加精细化的安全管控能力。依托平行切面思想和工程化手段，企业可以拥有一个独立的安全发展空间，将不断迭代的安全能力“编织”到业务系统内部。如图10所示，传统安全方案以外部防护为主，在业务系统从单机到集群再到微服务架构的演进过程中，难以伴随业务的精细化发展路径进行深入和细化，即：无论业务逻辑如何拓展，其安全管控措施都无法摆脱粗放的模式；而切面能力既解除了安全能力与业务系统之间的相互束缚，也为企业提供了深入业务内部的手段，业务中的每个新增细节都可以被切面有效观测到，并及时推动整体安全策略的动态调整。

图10 安全和业务颗粒度同步趋向细化

来源：IDC，2023

为了落实安全平行切面对业务空间的一系列感知和干预能力，其在工程化实践过程中，形成了以下几个关键概念：

- **切面：**是一系列动态逻辑的组合。在与业务空间的一个平行空间里，通过注入、代理等技术，在不修改源代码的情况下动态修改或添加新的逻辑，这些新的动态逻辑被称为切面应用。切面应用作用于不同的切点，为应用服务动态扩展出各种丰富的安全增强能力。

- **切点：**是切面应用在业务系统中的具体作用位置，即原有应用运行逻辑中的某一代码位置。在实践中，一个切面应用可以作用于一个或者一组切点，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。

- **平行舱：**平行舱是对切面应用进行的工程化封装，以构建一个与业务应用共同存在的平行空间，让各种切面应用能够平稳、有序、可控、安全地运行，控制各种安全能力，使其在合适的时间、位置，以适当的规模生效。

安全平行舱具备三大特性：隔离性、可调度性和可管控性。

- **隔离性：**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。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。

- **可调度性：**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，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，从而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。

- **可管控性：**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，因此必须进行合理的管控，避免切面自身被恶意利用。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，对于大部分观测类切面只赋予只读权限。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。

事实上，安全平行切面作为一个新的安全框架体系，与传统安全技术存在千丝万缕的延续关系。安全平行切面利用AOP、插桩技术、hook机制等，构建了一个新的安全能力发展空间，这种思路已在IT应用和运维侧实现成熟产品化应用，但在安全领域尚未实现系统级的应用。

> 计算机科学中的所有问题都可以通过增加一个间接层来解决。
>
> ——大卫·惠勒，计算机科学家，剑桥大学教授

安全平行切面的发展极大地改变了这种局面。**安全平行切面通过对“感知+干预”能力的强化，一方面促进了业务安全触角的延展，另一方面也构建了细粒度的管控体系。**相比于传统的安全技术，基于平行切面的安全技术在延续很多安全攻防技术的同时，又发展出更具先进性的特征。安全平行切面作为安全能力体系的基础平台，与上层业务应用之间实现了有效的解耦。基于高融合、低耦合模式，安全平行切面能够为安全产品、组件和安全能力的发展迭代提供一个独立空间。

- **融合+解耦：**切面既紧密作用于应用系统，又与应用系统解耦。切面将云管边端的不同环节有效地连接起来，实现安全作用力的组合输出；同时，它的解耦性又能让安全组件始终保持独立化发展迭代的局面，形成安全防护的敏捷性优势。

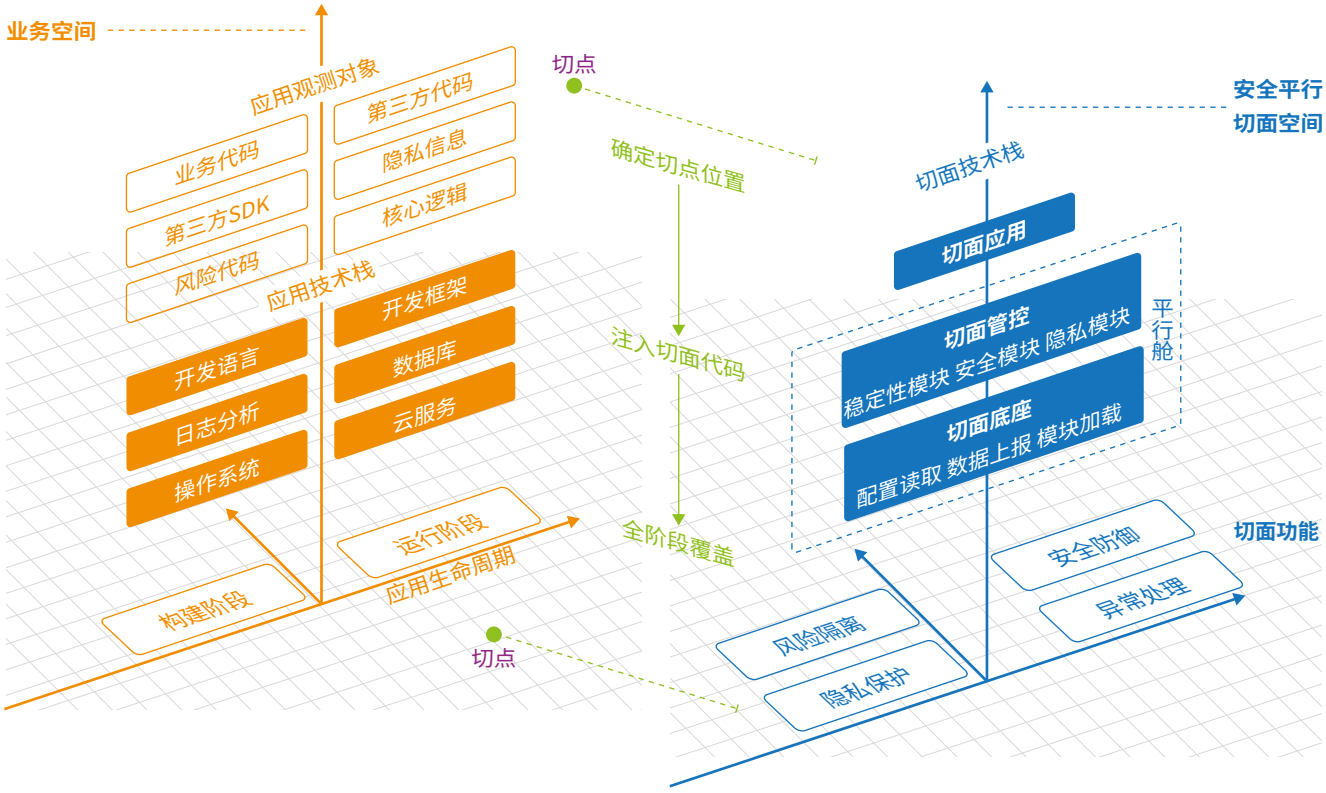
- **基础设施特性：**安全平行切面是面向下一代原生安全的基础设施，既与安全体系在构建过程中融合，又可充当一个底层的安全能力，形成基建化、共享化和服务化的优势。

- **原生安全处置能力：**切面和平行舱能够通过标准化接口的形式，规模化地输出安全能力，对业务系统进行组合干预。从业务视角看，这些安全干预举措实现了原生安全的保障和处置能力，这是传统安全保障体系所难以达成的目标和效果。

在实践中，安全平行切面有相当多的应用模式和作用范围。

- **在应用层面：**安全平行切面可以在业务逻辑和流量关键环节中构建切点组合，更快速地发现潜在威胁，实现对异常访问的精准感知和快速阻断。例如，切面可以提供针对企业自研或外采安全产品的管理机制，缓解外采给企业带来的技术挑战；切面通过平行的安全域对目标进行管控，无需修改代码和产品即可实现对攻击的感知和阻断；切面提供的规模化漏洞修复能力，改变了传统漏洞修复速度严重滞后于漏洞危害扩散速度的被动局面，可在极短时间内实现大量漏洞的自动修复。安全平行切面既能够适应传统的非云基础设施，也可以适应云和微服务架构。此外，在企业多云架构带来的多样化技术栈环境下，安全平行切面仍可以提供一体化的安全保障服务，帮助企业应对多云环境带来的复杂度挑战。

图11 移动应用端安全平行切面应用示意图



来源：IDC，2023

- **操作系统：**切面也可以针对操作系统内核提供热修复能力。例如Linux security module提供了一个跨内核的安全切面，但其尚未作为基础设施来实现，也缺少平行舱这样的服务层，无法主动与云平台等实现一体化安全管控。未来，基于安全管控的植入框架，安全平行切面有望在操作系统层面提供更多的安全服务能力。

- **网络：**相对于传统的防火墙、WAF层面的防护，安全平行切面可以在与网关、网格的结合中体现出更深入的优势，形成更具全局和更细粒度的网络安全能力集合。

2.3 安全平行切面的核心能力和特征

安全平行切面作为一个基础框架和能力集合，具备区别于传统安全体系的一系列突出能力，包括感知、干预以及快速扩展等核心和特性能力。

- **多维感知能力，还原事实本身：**感知能力是安全领域“看得见”的基础能力，做不到感知能力的覆盖就很难保障系统安全和数据安全。安全平行切面技术将安全基础设施融入应用和系统内部，能在业务系统中的任意位置进行深入的数据采集观测；同时，在端管云各层次切点之间，通过对运行时上下文数据的解析，可快速准确地串联起各层次切点的观测数据，极大地拓展安全感知能力可观测的数据维度，以全局视角还原攻击者的实际意图与结果，提高整体感知能力的准确性。

- **微观干预能力，精准高效防御：**由于安全平行切面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干预能力，其精度能细化到对业务系统内的任意一行代码进行干预的粒度。相对于传统的外挂式安全系统在宏观行为层面对攻击进行判定与防御，微观干预能力能让防御效果精准地作用于攻击生效点，并可通过上下文、执行链路等进行动态干预判定，进一步过滤正常的用户和系统行为，省去大量特征过滤的开销，提高防御的准确性与效率。

- **编程扩展能力，支撑快速创新：**安全平行切面是一套可编程的安全基础设施，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。不同领域的安全团队，比如数据安全、系统安全、攻防对抗等，可以各自独立地存在于平行空间内，实现、维护和部署各自所需的安全能力，为各团队的应急与安全创新提供了很好的基础保障。

安全平行切面在赋能业务系统开发、运维和运营的过程中，能够体现出以下显著特征：

- **稳定性：**切面和切点的设置不对业务系统代码产生实质性改变，可以最大化地减少对业务系统运行所产生的影响，保证企业整体运营的稳定。

- **有效性：**相对于传统的边界防护，安全切点深入到应用系统、网络和操作系统内部，对安全动态的感知、分析、阻断能力更有效，也更能体现全局联动的效果。

- **安全性：**安全平行切面实现了自身安全组件的独立迭代，其安全能力的规模化输出和对自身的安全性保障都在持续性地进步与完善。相较于传统安全体系，安全保障的质量有实质性的跃升。

- **隔离性：**由于安全平行舱所构建的安全能力集合，与业务实现了完全解耦，保证安全能力的升级迭代过程与业务系统完全隔离，确保安全能力与业务能力的独立发展。

- **易用性：**安全平行切面通过对典型切面构建过程的标准化定义和工程化平台支撑，使企业规模化的安全感知和干预工作变得更加轻松，平台的基础设施属性也便于其在提升易用性的同时，拓展安全措施的规模化影响力。

2.4 安全平行切面的应用价值

在面向当前和未来快速增加的创新业务应用时，安全平行切面的理念以及落地实践过程，能够在能力、效率和成本方面体现出显著的优势。

1、安全平行切面的能力优势

企业安全平行切面和安全平行舱的引入，重构了安全与业务的协同关系，让安全真正融入到业务本身，实现安全过程的可知、可见。例如，基于对业务行为和目的的感知、分析和判断，构建新的认证机制，并将其通过丰富的切点贯彻到所有业务系统的安全升级和改造过程中。从防护效果上看，安全平行切面推动了从传统外挂式防护到原生安全防护的转变，从而将安全影响力推进至业务系统的深层空间。

- **全面深入感知：**安全切面为安全攻防提供了强大的实战保障，其对应用系统的全面、深入感知能力，能够衍生出很多实战化的应用场景，实现从“以合规为导向”到“对后果负责”的转变。例如，面对日益严重的数据泄露问题，传统的安全模式仍注重外围环节的严防死守，对多重因素联合造成的数据泄露事件缺乏预判、跟踪、阻断和追溯能力。安全平行切面极大改变了这样的被动局面，也有望重塑数据管理的责权利机制。

- **安全日志自由：**传统安全产品所产生的安全日志，其覆盖率、准确率和知识性都有很大的局限性，切面提供了针对应用的细粒度观测能力，由于其深入应用内部，具备全方位的观测和干预能力，因此不需要通过安全产品的采集和授权访问，就可以自己获取海量的日志信息。在日志流转不及时的情况下，安全切面可以最大化保证安全日志的实时按需获取，这是安全切面最重要的底层能力体现。

- **对传统安全技术的一体化管理：**安全平行切面为企业自研或采购的其他安全产品提供了理想的管理机制，缓解外采安全产品带给企业的技术压力。应用内部的快速变化和复杂性爆炸因素，使外采安全产品的配置缺陷和协同不畅时常成为外部攻击的突破口，安全平行切面的切点管控能力使外采产品的一体化管控成为可能，从而更全面地管控风险。

- **打造新一代安全底层框架：**安全平行切面让企业安全防护的重心由边界向应用协同深层转变，形成了新一代安全基础设施。在这样的安全底层框架上，各类安全组件和安全产品将以新的模式发挥作用，安全生态能力也将依托新的框架，实现面向未来企业安全体系的创新与协同。

2、安全平行切面的效率优势

安全平行切面体现了安全能力共享化、资源化的发展趋势，可以在企业安全防护特别是规模化防护过程中显著地提升效率。企业数字化应用的快速发展和复杂性爆炸，使需要防护的对象成倍增长，防护重心也从边界转为应用内部更细粒度的关键节点，进而产生了普遍的规模化防护需求。

安全平行切面打造了一个具备多样化安全能力的基础设施，通过不断趋向标准化的切点和切面构建，全面融入至上层应用的业务逻辑中，既打造了原生安全，同时又利用平行舱的低耦合特性保证自身的独立性。在实现规模化防护的过程中，安全平行切面能够切实体现出以下效率优势。

- **敏捷化防御：**切点和切面的构建使安全防御能力能够快速触达规模化应用系统的每一个关键环节。安全平行舱所承载的多样化安全组件和产品在独立迭代的过程中，既保证了安全能力的先进性和时效性，也能够利用规范化的切面设计和丰富的切点设置，实现多个应用系统的快速并行干预，使防御体系的敏捷性和有效性获得数量级的提升。

- **实施更便利：**安全平行切面对业务应用的感知和干预过程，均无需修改原有业务系统的代码和产品配置，而只需按照设计要求，全面执行切面安全保障机制。这能够最大化地减少对业务系统的干扰，也显著抵消了传统安全与业务之间的相互影响。

3、安全平行切面的成本优势

企业应该从全局运营的视角，重新审视规模化安全能力带给企业的综合成本优势。这些成本包含了研发成本、运维成本和运营成本等。

- **研发成本：**企业的代码开发负责团队可以从切面设置中获益。由于切面有很强的内视能力，因此，一些内部研发过程和类似DevSecOps的实践都可以通过切面的植入来实现。切面的思想甚至还可以用于保障供应链安全等行业需求。在传统的供应链安全管理中，静态信息偏多，在用于实际的分析时，很容易发生遗漏，且不能充分反映线上的动态情况，切面的引入，则可以从根本上消除全局被动性所造成的影响。

- **运维成本：**安全平行切面可以有效解决安全的规模化防护问题，通过对安全资源统筹效率的革命性提升，实现基础安全资源对应用的快速影响力覆盖，从而显著减少安全人力、物力和财力的投入。

- **运营成本：**规模化安全防护的优势也体现在对企业业务运行的高质量保障中。在传统的安全防护模式下，企业安全团队针对所有应用系统梳理和修复一个漏洞，需要逐个执行修复和验证措施，无论是采用串行工作还是多人并行工作的方式，其包含停机时间、人力、物力因素在内的企业运营成本都很高。而在安全平行切面的干预模式下，针对应用的安全升级和干预过程几乎不对业务开展产生干扰，这受到了包括SRE团队在内的内部组织的广泛欢迎。

- **行业综合成本：**安全平行切面打造的安全日志自由，有助于实现“CT式”安全评估能力，为风险评估生态体系（包含企业上下游、安全厂商、安全保险企业等）提供丰富、可靠的安全态势参数。通过业务与安全相融合的新场景，涉及安全产品、运维、运营、保费在内的综合成本均可呈现出理想的优化效果。

第三章

安全平行切面的应用和构建

3.1 安全平行切面的应用场景

安全平行切面带来了创新性的安全可观测和可干预能力，为网络安全、数据安全、个人信息保护等领域带来了颠覆性变革的可能性，同时也有望推动一大批安全、合规和攻防场景的出现。

1、合规场景

- **数据资产精确测绘：**数据资产测绘是企业当前数据管理中的一个重要环节。在海量数据持续产生的背景下，数据资产的测绘过程普遍会遇到如何应对数据动态变化的问题。例如，在测绘过程中，测绘目标产生了增量，导致分类分级定义发生变化。网络中的动态流量也给测绘过程增加了复杂度。此外，传统的数据测绘过程会普遍出现越权现象，从而对数据资产的安全性产生威胁。安全平行切面为数据资产的动态、精确测绘提供了有效手段。针对海量数据，可以采用静态测绘与动态相结合的方式，通过在切点设置代理，获取相应的数据资产基础信息和分类分级结果，保证测绘过程的安全性和精准度。

- **数据流转全链路感知：**企业内部应用系统数量和各类终端用户数量的快速增长，使数据流转过程日趋复杂，数据在流转过程发生不可预知的泄露风险也大幅增加。安全平行切面的出现为跟踪数据流转全过程提供了有效的方法选择，通过在数据流转通道的关键环节设置切点，准确记录数据的传输、交换、存储过程，有助于建立对数据流转过程的全链路感知能力，发现数据在流转过程中的潜在泄露风险，及时阻断数据泄露行为。

- **场景化数据分类分级：**在数据驱动业务发展的目标指引下，企业内外部的创新应用场景层出不穷。为了在保障安全的前提下，充分发挥数据资产的价值，实现场景化数据服务，企业数据的分类分级策略将变得更加灵活多样。安全平行切面通过在数据管理流程中合理设置管理切点，可以对数据分级分类施加更细粒度的执行策略，从而使数据的组合、加工和处置过程更加贴近业务需要。

- **APP端个人信息合规保障：**企业在运营拥有海量用户的APP时，由于终端防护水平的参差不齐，因此经由终端输入的个人信息会面临多样化的威胁，也给企业自身的合规建设带来很大的隐患。企业可以通过安全平行切面的规模化干预能力，及时升级终端上的安全合规和安全防护策略，调整APP数据的权责管控模式，形成个人信息合规的动态保障能力。

2、威胁对抗场景

- **大规模1day漏洞防护：**企业在引入专有云和云原生架构的进程中，大量的应用系统架构采用了统一的架构和技术组件，也使新的漏洞爆发时所产生的影响范围变得更大。企业1day漏洞大规模修补和系统升级工作的时效性至关重要。基于企业现有的人力、物力资源条件，安全平行切面技术能够帮助企业实现规模化漏洞的批量快速修复，确保将1day漏洞对业务运行的影响降至最小。

- **-1day威胁感知与捕获：**切点的合理设置，还能够帮助企业发现潜在可利用的安全漏洞或攻击者的攻击尝试（即-1day威胁），及时对业务进行整改或更新安全策略，提升企业的防御性弹性，并在一定程度上对0day漏洞的未知风险产生预防作用。

- **细粒度攻击感知与阻断：**安全平行切面可在测试环境、仿真环境或真实业务环境中，动态地对关键sink点进行持续性监测，并实现对应用逻辑的细粒度刻画以及对NbSP异常行为的检测。相比传统的网络、系统层面的监测或静态扫描，通过切面实现的动态监测识别颗粒度更细，结果更为精准，其阻断措施也更加快速和准确。

- **精准根因定位与研判：**由于切点的设置深入应用、操作系统、网络的内部节点，因此对安全威胁和安全事件的过程信息掌控更加精准。同时，经过海量数据分析和训练形成的安全模型，能够帮助企业精准定位安全事件的根因，实时研判安全态势，大幅提升安全应急处置的水平。

3、网络保险场景

网络安全保险是面向企业安全保障的一项机制创新，通过产品、服务、保险的组合，强化企业安全运营成效，为企业因IT系统和网络攻击而产生的损失兜底。目前，网络安全保险市场正处于起步期，根据IDC调研，到2023年，全球网络安全保险保费将增长51%以上。按照保险的出险、定损、赔付等环节，安全平行切面有望支撑的场景包括：

- **全链路安全风险评估：**网络安全风险通常包括：由漏洞的直接和间接成本导致的财务风险，合规风险，保密性/完整性/可用性受损带来的声誉风险，安全事件造成的运营风险，以及威胁组织持续生存能力的战略风险等。当前行业中针对安全的评估判断主要依赖于调查表，其全面性和客观性有限。而切面可以透视整个系统，通过对系统的复杂性、脆弱性的度量，可以形成跨越当前技术的新体系，进而获得对风险的精确认知。

- **细粒度安全监测：**与威胁对抗场景类似，细粒度的安全监测可以帮助企业更精准地确定保单范围，评估潜在的事件损失成本、事件响应成本以及因业务停机产生的收入损失、声誉损失、系统恢复成本和法律成本等，进而形成多样化的安全保险赋能场景。例如，企业通过对安全动态的实时掌握，有效评估在投保项目方面的重心和规模，达成安全保险与安全投入的合理平衡，最终实现安全保费和安全投入的最小和。

- **高效安全响应与溯源：**通过安全切面可以实现访问链路的精确刻画，例如在应用空间内植入微网关能力，代理各类请求（包括HTTP、JDBC、RPC等），动态感知业务进出口流量，实现多协议流量按需采样，流量入口身份可进行身份鉴别，出口进行标识染色，从而实现OVTP链路刻画，帮助企业建立高效的安全相应和溯源能力。

3.2 建设安全平行切面的方法、步骤与应用指南

1、企业战略认知与顶层设计

企业以外挂式安全架构为核心的安全模型已经发展了多年，形成了相对稳定的运行环境和理想的性价比，被包括业务部门在内的企业各方所接受。但随着数字化环境日趋复杂，复杂治理环境和高强度的攻防对抗已成为常态，企业应认识到：传统安全架构在可观测能力和全局管控能力上存在局限性，无法有效应对未来安全态势的发展。

安全能力与业务逻辑的深度融合已成为大势所趋，在数据安全、网络安全、隐私保护等领域，严峻的攻防态势要求用户必须具备全局、深度的感知、防御和处置能力。与此同时，安全能力也需要突破与业务系统之间长期存在的制约关系，获得独立迭代的空间，以足够的能力应对快速增加的安全威胁。

安全平行切面以高融合、低耦合的方法，建立安全与业务的全新协同发展模式，为业务提供了更具良好体验的原生安全服务，为未来企业安全架构的发展提供了良好理念和方法论借鉴，也是企业构建未来安全战略时需要重点关注的目标。

以新的安全战略为指引，企业可以借鉴安全平行切面的思想，着手完成安全架构的顶层设计，形成安全体系建设的路线图、能力框架、技术架构、场景规划和运营模式。在这个过程中，企业需要根据自身的业务需求，形成有侧重的安全防护体系，例如，企业应围绕对数据要素的动态访问和数据驱动的业务场景，建立以数据要素为中心的安全架构，满足复杂的安全业务场景需求，包括对企业内网数据的安全访问、数据实时共享、隐私数据保护、移动终端防护等。

2、构建切面的底层能力框架

安全平行切面的底层能力框架是新一代企业安全防护体系的承载平台，体现了安全平行切面的思想和理念，也通过安全平行舱这样的工程化平台形成多样化的集成搭载能力。

- 安全平行切面能力框架旨在赋予企业强大的观测能力与精准的干预能力，实现感知能力与响应效率的跨越式提升，高效支持企业数字生命体中原生安全范式的实现。
- 能力框架通过可注入的基础技术，在不修改应用源码的情况下给程序动态添加或修改功能，并通过切面平行舱保证其有序运行，提供精准的安全观测与干预服务。在此基础上，安全平行舱打造了不同切面应用的执行环境单元，体现切面应用调度和管控的基本颗粒度。
- 在安全平行舱的支撑下，企业需要根据自身的需求，借鉴成熟的工程化模板，实现切面、切点的设计，形成应用切面、操作系统切面、终端防护切面等不同的防护组合。
- 基于安全平行切面能力框架，安全产品厂商和生态服务企业都可以发挥自身的优势，将各类安全能力通过产品、组件和服务的方式构建在框架中，形成持续迭代和深度协同的发展局面，使最终客户能够在多产品运维、多事件管理、多维数据融合等维度上实现真正的统一运维、统一管控和统一调度。

3、实现切面场景的持续拓展

对于大多数企业来说，从应用切入，分步实现切面场景的拓展是一个较为理想的选择，也是保证安全平行切面快速产生业务价值的必要路径。

安全平行切面通常首先用于解决企业安全攻防、数据治理等最根本的问题。作为未来安全对抗和安全治理的基础平台，安全平行切面会带来攻防对抗和安全治理效率的显著提升。传统的安全模式下，企业缺少对业务系统形成干预能力的技术平台，因此通过定制化安全开发所形成的业务系统外围和内部的安全措施缺少效能提升的空间。未来，预计30-40%的安全服务都会实现切面化改造，由此带来攻防效率和研发迭代效能的革命性提升。

企业在将切面技术用于安全对抗和安全治理的过程中，可以有效积累经验，打造标准化的模板、技术组件和服务，并通过安全平行舱实现安全能力的标准化沉淀和输出；在此基础上，根据企业各领域的安全需求持续拓展安全切面的应用场景，包括合规场景、安全对抗场景、保险场景等。

4、形成安全能力长期迭代提升的良性局面

企业安全能力的建设不是一蹴而就的短期过程。安全平行切面及安全平行舱的出现，创建了一个较为完整的技术框架和工程化平台，并通过高融合、低耦合特性，为各项安全能力的发展提供了独立空间。以此为基础，各安全系统、安全组件、安全服务的供应商有望加速自身的发展迭代速度，在统一的技术框架下，通过发挥各自所长，逐渐形成一个相互协同的生态体系，使安全能力基于生态基础实现相互协同，构建起全流程的安全能力闭环。

安全平行切面技术框架的隔离性，也有助于加快安全切面设计模式的标准化进程，将面向业务系统的安全能力更多地抽象出来，形成新的安全基础设施，并在原生安全范式下对不同层面的安全能力进行长期持续迭代，在产品和服务体验上获得持续提升，在商业模式上取得新的突破。

3.3 安全平行切面的实践应用

3.3.1 蚂蚁集团安全平行切面的内部实践

蚂蚁集团数字化业务体量大，发展快，为了应对企业数字业务的规模化安全保障过程中所面临的一系列现实问题，蚂蚁集团积极探索基于安全平行切面的实践活动，在应用场景、部署经验等方面积累了先进的经验，获得了可圈可点的成果。

应用背景

在传统架构下的安全左移实践中，企业需要在各类非真实的测试环境中依靠扫描工具做代码逻辑分析和业务行为模拟测试，并根据线上安全产品采集的业务流量与进程行为进行综合威胁研判。

面对未来的大规模安全治理与攻防对抗要求，传统架构下的检测、治理、防护手段单一，上下文逻辑缺失，数据可集成度低，规模化运维难度大。此外，传统模式的抽样观测效果不佳，抽样数据无法支撑链路追踪目标，安全事件的追溯范围也极为有限。据统计，传统的安全监控可覆盖高风险范围的比例平均只有29%，大量应用因技术栈陈旧、无人维护等原因处于观测盲区。

成效概览

蚂蚁集团的安全平行切面实践，极大提升了漏洞挖掘、实时防御、资产画像、隐私保护等行动的效率和准确性。目前，全集团的切面观测模块部署超过100万个容器，生产环境稳定运行了330多个注入点，日均观测量级70亿次。在前不久的log4j2漏洞发生期间，共拦截相关攻击40万余次，在小时级的时间内完成了全站精准止血，实现0误拦0漏拦，应急响应的人力需求从6000人日大幅降低到30人日。蚂蚁集团的安全平行切面助力集团有力应对双11、双12期间的流量洪峰，在平行止血加固的同时，极大程度减少对业务的干扰，并且做到服务不降级，安全策略检测速率达2.2亿次/分钟。

图12 蚂蚁集团安全平行切面应用实践效果

- 切面观测模续运行情况：部署100W+容器，生产环境稳定运行330+注入点，日均观测量级70亿次
- 拦截 40万+ 次 log4j2攻击，小时级完成全站精准止血，0 误拦，0 漏拦，应急人力从6000 人日降低到 30 人日
- 双12大促封网不受影响，平行止血加固，业务 0 打扰化解危机
- 双11、双12流量洪峰值不降级，安全策略检测 2.2亿次/分钟
- Spring4Shell超危漏洞应急，获得高度认可

来源：蚂蚁集团，2023

落地场景

1、安全治理场景

> **概要：**安全态势研判的复杂性会伴随数字化业务的复杂性增加而快速增长。业务场景的复杂导致需要判断的行为数量显著增加，进而打破原有的需求和能力平衡。安全切面能够基于更细粒度的数据，发现之前无法发现的问题，显著提升安全防护的效率和效果，为企业安全治理带来跨越式的变革。

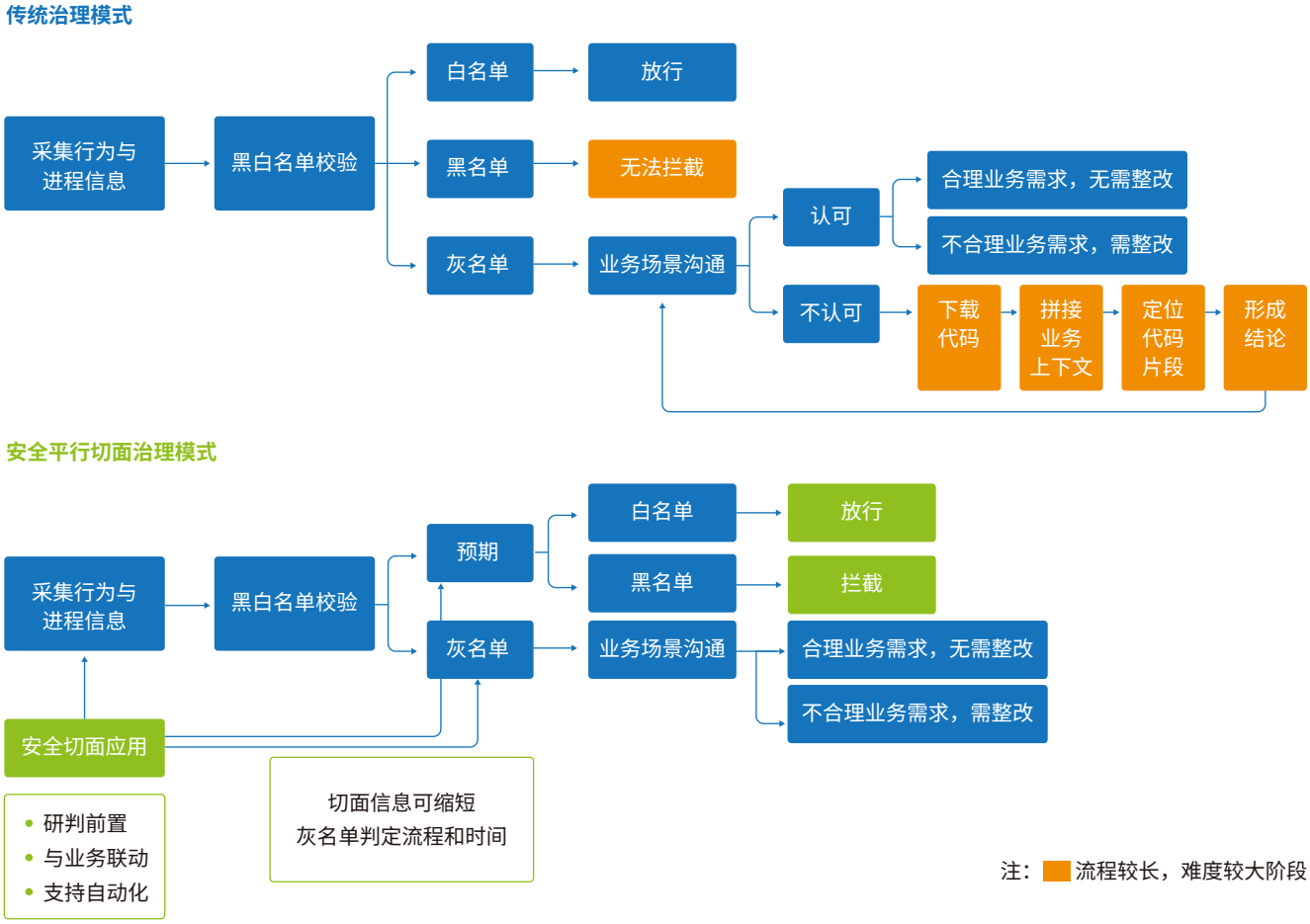
背景与挑战

复杂场景下的网络安全治理，从来不是非黑即白的简单判定过程。从已有的观测数据中，往往会发掘出很多未知行为（俗称灰名单）。在实际安全运营过程中，企业需要投入大量的时间和人力深入业务场景，联络业务责任人，梳理业务逻辑，研判系统行为合理性，最终对“未知行为”做出风险和合规认定。这一系列调查、取证动作会严重贻误战机，放任攻击者达成攻击目标。

例如，在蚂蚁集团安全团队治理过程中，安全系统发现某个应用频繁访问一些外部不可控的域名，并自动发出了告警。一般情况下，安全团队不能在第一时间阻断未知的请求，而是需要与业务团队进行确认，以防止误拦截所造成的严重业务影响。但业务方由于各种信息不透明，往往也无法给出及时而有效的判断。

在传统治理模式下，安全团队要完成业务应用的代码审计，定位可能发起网络访问行为的代码片段，再结合代码片段所引用的上下文研判问题根因。面对大规模的未知访问时、在安全团队规模远远小于业务团队规模的情况下，这样的治理模式在时效性方面不具备与攻击组织对抗的可能性。

图13 传统治理模式 vs 安全平行切面治理模式



来源：蚂蚁集团，2023

而在切面治理模式下，安全团队利用切面基础设施快速将切面应用部署至该业务所属的全量基础环境及业务上下游，开启切面对该应用的线上观察模式，实时获取行为日志。通过分析切面告警日志，可以快速锁定触发访问域名的行为在代码工程中的位置和堆栈信息，确认访问域名行为的发起者，并与业务方共同排查代码逻辑的合理性。经上下文分析确认：开发人员为实现日志打印，通过应用代码直接获取外部IP，导致在使用某个获取域名的方法做请求时，由于入参的变化引发了函数的异

常行为。经过上述分析，安全团队确认该异常访问行为并非安全漏洞引发，但仍存在一定的安全隐患。安全团队做出溯源排查结论后，业务方迅速完成了整改。

应用成效

在该案例中，整个未知行为的分析溯源过程非常复杂，且业务代码的调用链路长。通过对应用代码的执行过程进行细粒度的观测，安全运营人员快速识别了敏感行为，并进一步提供有效的止血手段，极大缩短了调查取证和做出威胁响应的时间。

2、-1day挖掘实践

> **概要：**-1day挖掘体现了安全行为的左移思想，能够将企业的安全对抗成本进行前置。基于新一代安全基础设施，可以更有效地发现-1day漏洞，从而大幅减少企业在面对0day时的应急响应投入。

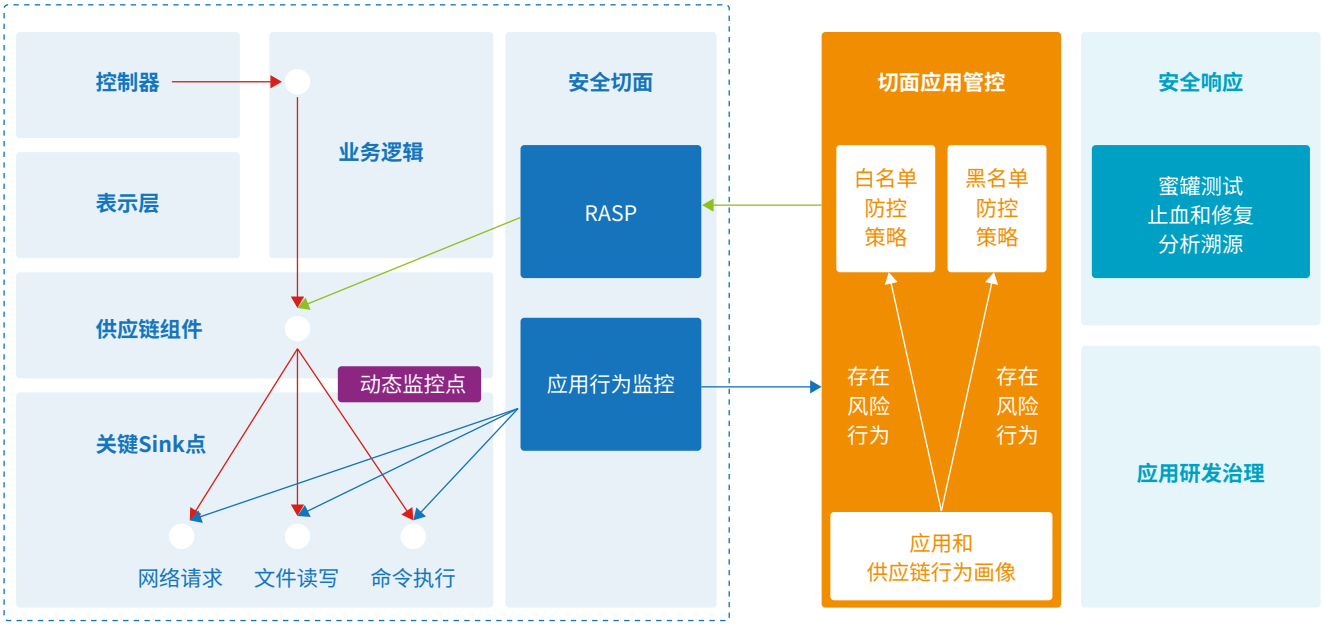
背景与挑战

在传统安全体系下，-1day漏洞的挖掘工作具有很高的综合门槛。例如，企业需要具备对高危命令的治理能力，深入理解高危命令和业务的实质关系，连续观测高危命令的执行情况。在一些业务场景中，攻击者通过修改Button背后的URL，达成其正向攻击探测的目标。而安全团队则可以根据代码进行反向分析，先于攻击者发现可能存在的问题，实现反向推测。

在企业纵深防御体系中，大量针对漏洞（尤其是边界公网可达的应用漏洞）的攻击行为最为致命，因此，对企业边界处的攻击探测与加固行动必须分秒必争。对-1day漏洞的检测与防护，本质上也是漏洞防护的“左移”，即：通过在日常治理过程中对应用行为的细粒度观测以及可信行为的建立，实现对潜在可利用漏洞的提前感知，大幅降低后续处置0day和1day漏洞的成本。

解决方案

图14 -1day挖掘实践程示意图



来源：蚂蚁集团，IDC，2023

蚂蚁集团安全可信技术团队通过应用安全切面，上线了面向命令执行的白名单策略，仅允许JAVA应用执行可信可控的linuxshell命令。在策略上线过程中，安全团队发现了若干应用存在自定义的shell命令，通过对这些命令的引入方式进行分析，发现某个应用执行的命令非常可疑，有潜在的存在命令注入风险。经过进一步的深入跟进，安全团队挖掘出一个互联网可达的远程命令执行（RCE）漏洞，攻击者利用该漏洞实施攻击的成本极低，危害极大。

在发现漏洞的过程中，安全团队首先根据切面模块（RASP）提供的非预期命令执行告警，查看到一个异常变化的URL。通过RASP详细告警信息中的堆栈，安全团队快速定位到了命令执行的位置。再经过进一步的源码解读和业务逻辑分析，初步判断存在远程命令执行（RCE）漏洞。经过WAF防护系统和蜜罐系统的协同验证，这个公网应用的-1dayRCE漏洞被正式确认，并迅速启动了后续的紧急止血和修复工作。

应用成效

在该案例中，切面应用和基础设施作为贯穿“命令执行可信行为治理”过程中的基础能力，覆盖了所有核心应用模块与检测策略要求。细粒度的观测数据为治理团队提供了详细的告警信息，有效支撑安全团队高效定位、溯源和排查可疑行为，助力安全团队在治理过程中挖掘潜在的高危风险，为企业全局性的攻防对抗争取了宝贵时间。

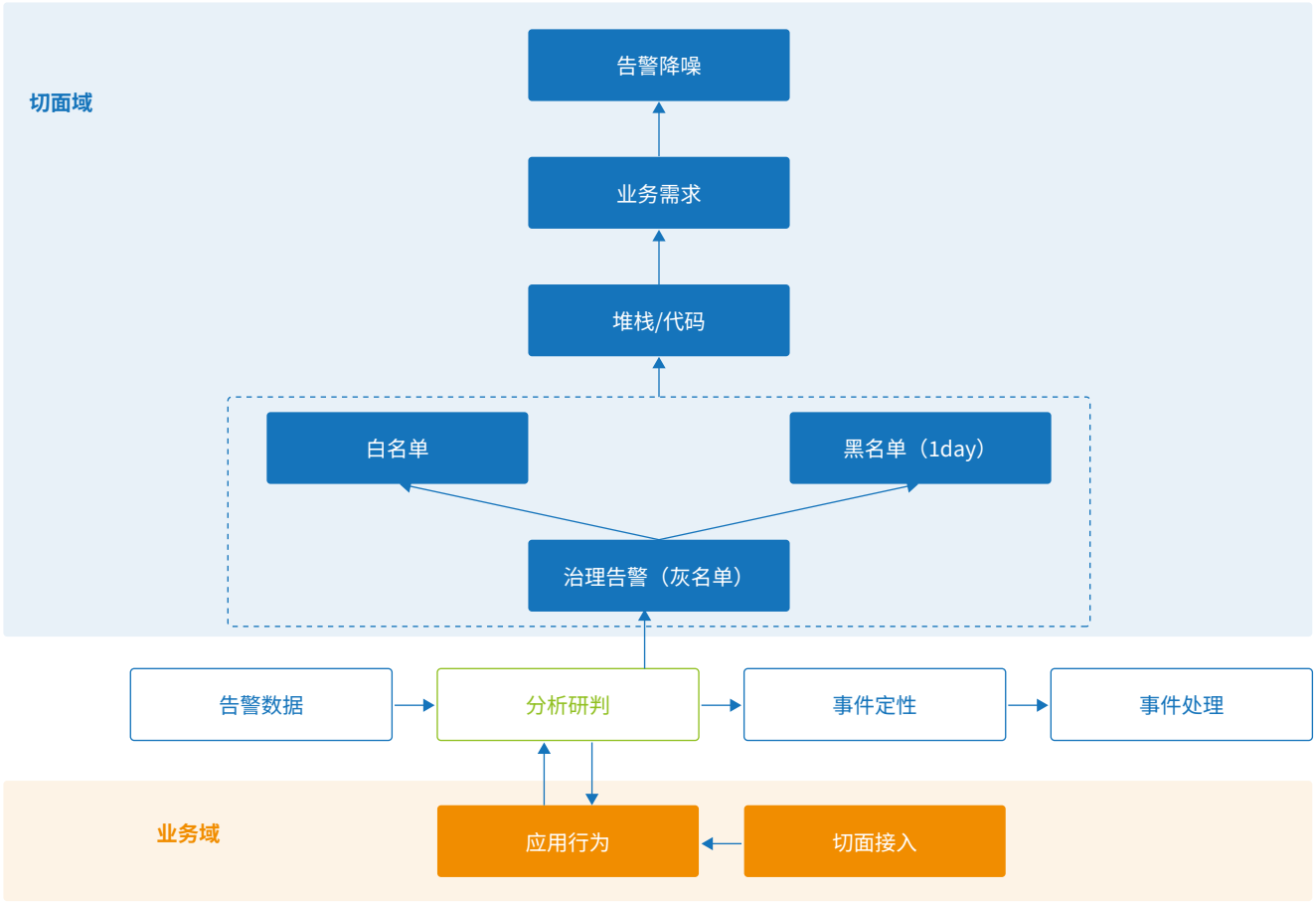
3、告警降噪场景

概要：在企业攻防对抗中，对海量告警信息的降噪非常关键且难度极大。传统模式下的简单降噪策略在降低告警量的同时，会导致一些关键信息的遗漏。安全切面模式基于细粒度的观测数据、自动化的研判规则以及对高等级威胁的学习，可以精准确认攻击行为，实现快速响应。

背景与挑战

在企业攻防对抗场景中，实施入侵检测与响应的过程可以抽象为获取原始数据、提炼告警信息、甄别真实事件、实施威胁响应等一系列关键举措。在蚂蚁集团的实践中，各类设备与系统日志上报形成了海量的原始安全数据，并经过一系列的规则策略过滤，形成待处理的告警信息。这些告警信息反映出大量不可预期的“异常”业务行为，但规模过于庞大，安全团队难以直接判断其中哪些是真实的攻击。

图15 基于安全平行切面的告警降噪实现过程示意图



来源：蚂蚁集团，IDC，2023

海量告警信息的降噪成为攻防对抗中的关键环节。安全切面模式以细颗粒度的观测数据为基础，通过切面提供的堆栈和代码，结合对风险引入方式的判断，对灰名单进行自动化的黑白判别，这其中包含了一系列规则、策略的设计编写工作，以及对更高等级威胁的学习和处理过程。例如，精准确定哪些未知的可疑行为由应用代码自身产生，哪些由未知的脚本或漏洞产生，进而从告警中有效甄别出真实的入侵事件。

应用成效

目前，蚂蚁集团的安全切面针对已知的攻击路径/检测策略实现了全面覆盖，对已知威胁场景的策略实现自动化执行。同时，对大量的未知攻击也做到了实时处理，大幅提升了安全攻防效率。

4、越权防护场景

概要：对越权防护场景的支撑是一项具有挑战性的全新能力。通过将水平越权SDK包装成切面应用，企业能够以基础设施的方式实现对业务的逻辑植入，进而发现和处置越权访问问题。例如，企业可以把OVTP票据逻辑集成到SDK逻辑里，实现水平越权行为的端到端检测，并对个人信息进行有效保护。

背景与挑战

水平越权是很多行业应用中存在的棘手问题，其风险占比高，危害大，且事前发现困难，持续治理成本无法预估。过去数年中，很多企业安全团队尝试了多样化的治理方法，但由于水平越权问题与业务强相关，因此一直缺少理想的根治手段，也间接导致企业数据泄露事件频发。在数据安全与隐私保护备受关注的情况下，水平越权可能引发企业无法承受的巨大数据风险。

传统的水平越权漏洞防治方法，一般基于外挂式与嵌入式两种安全架构：

- **外挂式安全架构：**基于旁路自动识别能力，利用扫描检测工具检查代码逻辑，但其无法自动化识别多样化业务之间的相关性，例如金融或交易属性之间的关联。而人工检测的方式又因代码变更量大，人工成本高，无法做到业务逻辑的全覆盖。
- **嵌入式安全架构：**通过代码规约和注解扫描的方式，将SDK集成到业务代码里，发现包括“接口忘记鉴权”在内的隐患问题。但该模式依赖业务系统改造，业务侵入性大，推广和升级非常困难，对于存量业务的实施难度更大，其鉴权正确性也无法得到保证。

解决方案

蚂蚁集团在2023年初启动实施了基于关系链的水平鉴权方案，通过提炼出业务代码中的主体、客体以及主体与资源间的逻辑关系，在业务运行过程中综合判定越权行为。为了让所有业务应用都快速具备鉴权能力，蚂蚁集团开发了水平鉴权切面应用，利用切面基础设施平台实现了业务侧的无感接入。在业务运行期，则可通过票据透传策略，鉴权计算所需的关系链和上下文。

应用效果

水平鉴权切面实现了安全策略与业务的无感融合，体现了切面的融合与解耦特性。基于票据透传的能力，有效实现了针对水平越权问题的端到端检测，突破了代码层面检测的局限性。在业务运行过程中，访问客体可以从票据中心拿到票据，并根据透传信息执行验证过程，有效确保了个人信息的安全。

图16 鉴权SDK效果总结

来源：蚂蚁集团，2023

5、高可用保障场景

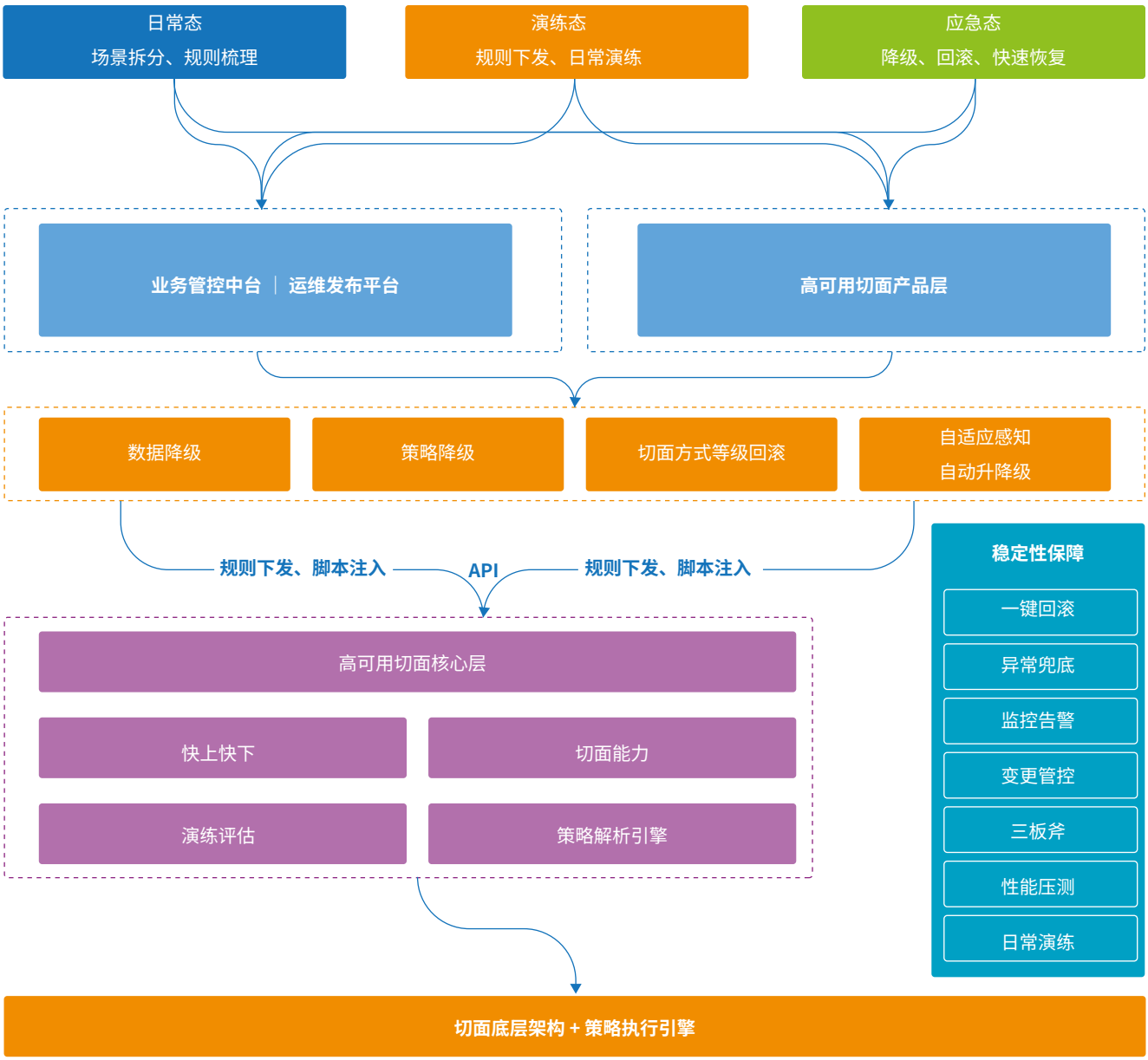
概要：通过切面快速完成异常行为定位和故障应急，确保线上业务的高可用，避免一般软件BUG对业务操作的影响，确保线上业务的高可用。线上故障的恢复时间可降至分钟级，故障影响也降至最小程度。

背景与挑战

在高可用保障场景中，涉及异常处理的两个最重要的环节是异常定位和故障应急。其中，故障应急的效率（即影响时长）非常关键，关系到最终的业务影响范围和损失规模。传统的高可用保障方案在面对未知风险造成的影响时，需要通过代码修复手段解决问题。代码发布后若再发现异常，则需要进一步进行回滚，使修复和发布时间十分不可控，经常会导致止血缓慢，损失范围持续扩大。

而在已知风险的应急场景中，如果一部分对外提供的SDK出现服务异常，企业需要快速进行服务降级。特别是在安全风控链路部分发生异常的情况下，业务方希望具备UID或业务域维度下的快速降级能力。此外，部分无人维护的应用缺乏降级能力，也希望通过切面注入的方式带来应急能力的提升。

图17 基于安全平行切面的高可用保障方案



来源：蚂蚁集团，2023

面对以上未知风险场景和已知风险场景的应急需求，业务高可用切面方案可以利用强大的注入能力和切面融合能力，提供三类高可用应急服务：

- **未知异常下的快速修复止血：**基于切面基础设施实现高可用切面模块的规模化部署，即可提前收集注入切点信息并通过编译部署方式生效，也可以针对即时发现的异常切点动态下发注入规则。快速构建切面修复策略，利用切面控制平台实现策略下发，并通过Pointcut切点的动态注入，快速实现异常修复止血。
- **已知异常下的快速应急：**利用切面基础设施进行高可用切面模块的规模化部署，梳理出与应用已知风险点相关的所有Pointcut切点集合，并通过切面控制平台对已知 Pointcut切点进行提前埋点检测，实现快速应急。
- **灵活的应急策略下发模式：**既可以将应急策略提前下发，实现有条件触发（即依赖已知异常信息进行触发)，也可以根据实际需求，在启动异常处理时动态下发应急策略。

图17 基于安全平行切面的高可用保障方案

来源：蚂蚁集团，2023

应用成效

基于安全切面底座构建的高可用切面架构，提供了一种新型高可用应急止损能力，能极大提升 部分场景的应急时效性，为业务团队提供了一种新的变更回滚思路即切面策略等效回滚方案。同时，高可用切面能力可以联动其他三方中台提供的多种场景的自愈降级方案；目前高可用切面产品能力已经完成全量铺面，覆盖内部数千应用，并且在SDK组件风险自愈、业务异常数据快速降级、全链路动态追踪、发布代码等效回滚等多类场景应急中取得很好的实践效果，部分应急场景止血时长从小时级降低至分钟级。

3.3.2 生态伙伴实践

为了更好地推广安全平行切面理念和框架，发展切面应用场景，2023年7月，在中国信息协会信息安全专业委会指导下，由蚂蚁集团牵头发起、近15家企业共同参与的安全平行切面联盟正式成立。联盟致力于安全平行切面技术的开源共建、标准共创和应用推广工作，不断向社会贡献创新技术和最佳实践，以此来推动提升企业安全架构的实战性、稳定性、安全性和易用性，推进企业安全架构的变革和可持续发展。

红途科技：基于生态伙伴 丰富切面应用

联盟成员的角色和价值

深圳红途科技有限公司是一家以技术驱动的创新型科技企业，致力于数据安全和隐私合规科技领域发展，首创全链路数据流转追踪技术，打造数据流转追踪地图的底盘能力，围绕数据安全治理、数据风险管理、审计溯源及隐私合规，帮助企业构建数据安全与隐私合规科技能力。蚂蚁集团和红途科技互为重要合作伙伴，双方就安全平行切面和全链路数据流转追踪技术进行深入合作，致力于面向广大客户提供新一代安全能力产品及服务。

依托安全平行切面提升整体安全治理能力与水平

在安全平行切面的基础上，除深化原有产品能力（如：网络安全—平行蜜罐、隐私保护—双重确权/尽责自证、运维—APM/日志标准化、稳定性—混沌工程、仿真测试—流量录制与重放、国密改造—透明加密等）外，红途科技还依托自身全链路数据流转追踪技术，从数据流转的角度，厘清数据源头、数据存储、数据被使用、数据被调用再存储等所有过程，自动刻画完整的数据流转地图，进而提供数据资产梳理、数据流转观测、数据风险监测和审计溯源等能力，最终从网络安全、数据安全以及数据合规等多维度整体提升企业数据安全防护水平。红途科技的数据流转观测底盘产品实现了全域数据属性、分布、流转及使用情况的自动化梳理，全局呈现数据运营情况。

提供多样化的场景服务

- **数据流转观测：**伴随企业微服务架构改造等技术的实施，企业内部业务系统日益庞杂，系统内部及系统间的数据流转情况愈发难以梳理。全链路数据流转追踪技术，可以自动绘制数据流转链路，帮助企业全面掌握其敏感数据流转和分布情况，避免数据黑盒式扩散带来的管控风险。

- **数据风险监测：**基于数据流转及使用过程，围绕数据、数据库、应用接口、用户账号及IP等要素进行多维关联分析，形成数据风险监测能力，有效应对敏感数据在流转及访问过程中出现的数据暴露风险和数据泄露风险。

- **定位溯源：**改变以往业务系统需要埋点改造，投入成本高、耗时长的现状，业务系统无需埋点改造即可灵活采集用户访问行为日志，审计对象涵盖用户、应用、数据库和数据，全面覆盖数据流转全链路上的重要对象，不仅可以作为数据访问过程自证清白的有力依据，通时一旦出现疑似安全事件时，可以基于访问对象或访问内容快速实现定位溯源。

作为首批成员单位和技术合作伙伴，红途科技将继续深化平行切面和数据安全这里的落地实践，助力安全平行切面联盟的共建、共创和推广工作，协助推进数字化转型背景下企业安全架构和企业安全建设的变革和可持续发展。

3.3.3 行业用户实践

对于多数企业来说，安全平行切面的实践过程可以首先从应用侧切入，重点关注在数据安全维度的应用场景，让业务部门从业务可用性、隐私保护、可追溯等方面认可新一代安全架构的价值。在组织形式上，可先采用安全部门牵头、多部门联合决策的方式推动试用场景落地。未来,随着安全平行切面框架的易用性和快捷部署能力的提升，以及相关平行舱安全组件的不断丰富，可以转由业务部门主导建设，探索更多安全创新场景。

实践1：某证券公司——数据安全治理

关键词

应用场景：数据安全与合规

应用目标：基于平行切面技术，实现数据流转可见，发现数据安全风险，为后续实现精细化管理提供技术支撑

主导团队：安全团队

某证券公司作为一家大中型综合类券商，其主交易系统对安全性、可靠性以及低时延的要求极高，在业务系统上施加任何改造都有可能影响系统的响应速度和运行平稳性。

与整个行业类似，该证券公司也面临着较大的数据安全与合规压力。在实现内部数据安全与合规以及个人信息保护的过程中，需要从组织、制度、技术等多个建设维度入手，落实相关的工作。此外，证券行业普遍重视网络和信息安全领域的快速响应处置能力。例如，一旦个人信息出现泄露，会迅速对客户端造成影响。因此，如何快速通过审计和溯源查找相关证据，定位和解决问题非常重要。

该证券借鉴了安全平行切面的建设思想，围绕大数据平台及下游应用系统，构建了数据流转监测分析能力，从而识别数据从用户到应用、从应用到数据存储层以及数据从存储层返回用户的链路全过程，实现数据流转过程可见，并实现用户风险监测、记录留痕、资产画像等关键能力。

该证券还将分类分级成果应用在数据流转监测过程中，对相应数据进行分类分级标记，从而进行差异化监测防护。此外，基于用户、应用、数据库、大数据平台的数据关联记录，可对数据链路进行审计溯源，提升数据安全风险事件的问题定位效率；通过数据分析，识别数据流动中的安全风险，降低数据被滥用或泄露的风险，从而持续推动数据安全管理的规范化和标准化。

实践2：浙江移动——漏洞批量修补和应用链路监控

关键词

应用场景：漏洞管理，运维场景

应用目标：基于平行切面技术，在安全事件、攻防事件以及漏洞事件中，提升采取行动的效率，降低成本，实现精准修复。

主导部门：研发效能部门

浙江移动正在探索如何将安全平行切面作为通用型的技术平台和组件，由研发效能团队牵头，通过组织决策、需求理解、部门协同和技术规划，共同推动安全平行切面的工程化解决方案落地。

目前，浙江移动已经在漏洞批量修补场景中，引入安全平行切面思想，测试相关技术路径，通过在应用程序上构建调用链和监控点，实现开源软件漏洞的批量快速封堵。同时，研效部门也开始考虑在运维场景中，通过构建监控切面以及调用链流量回放等方法，逐步推动运维的标准化、智能化水平。

未来，在增量场景需求的推动下，浙江移动还将利用平行切面的思想重构一些基础服务能力，利用标准化的切面应用提高安全事件行动效率，降低安全防护成本，实现精准防御、深度防御。

实践3：吉利汽车——平台化的数据安全治理和统一运营

关键词

应用场景：数据安全和合规（含网络传输层面、应用层面和数据库层面）

应用目标：基于平行切面技术，系统化构建数据安全运营平台，实现对数据安全风险的精准感知，实现数据资产的实时可视化，实现风险的实时阻断和控制。

主导部门：安全技术部门统筹，涉及业务、研发和产品、营销、大数据等多个团队

吉利汽车从合规体系管理出发，逐渐发展自身的安全技术体系平台建设工作。从2022 年开始，吉利汽车将安全工作的重点聚焦于安全运营，重点关注信息安全合规性建设和数据安全建设工作。近年来，行业内友商相继发生的数据泄露等安全事件，使个人数据和个人隐私保护成为行业重要的目标和共识之一，吉利也意识到，若缺乏健全的数据安全运营体系和平台，则难以对数据安全做系统化的管理和管控。

在与蚂蚁的合作过程中，吉利汽车尝试从多个层面构建数据防护切面，包括：从网络层面（利用网关方式构建数据管理切面）、应用层面（通过Agent与数据库建立连接）、数据库层面（从数据库自身存储的行为切入）入手，并把这些管理细节信息统一汇聚至数据安全运营平台上。

在上述基础上，吉利首先实现了统一的数据资产管理，进而通过数据分类分级策略

和技术手段对数据资产做初步的划分，再结合数据切面执行相关的分类分级规则和控制策略，实现数据风险管控和分析。

通过安全平行切面的初步实践，吉利汽车的数据分级分类准确率得到了大幅提升，同时在一定程度上实现了全链路跟踪和分析能力，能够做到风险可视化分析和识别。未来，吉利汽车还将不断完善风险规则，并在网络安全和数据安全两个重要维度持续投入研究实践，在风险识别与控制、数据脱敏、业务可用性等方面构建更多场景。

实践4：平安科技——隐私合规和RASP

关键词

应用场景：数据安全和合规

应用目标：基于平行切面技术，为应用动态添加功能，创建与业务原本功能相互独立的运行空间，平台化解决数据安全全流程管控。

主导部门：安全部门

近年来，平安科技安全团队非常关注安全攻防领域的实践，并涉及部分安全防御领域的产品开发等工作。作为一个大型金融公司，平安的业务系统非常复杂，同时也涉及大量敏感数据的使用，在法规监管日趋严格的大背景下，国家对行业内APP 隐私泄露在内的相关通报事件越来越多，平安科技也在隐私合规和安全管控方面积极做出了更多努力。

在服务务端应用方面，需要对应用数据、敏感数据使用情况进行标记和监控。在移动端应用隐私合规方面，也力求打造一个工具平台，用 SDK 的方式检测和管控 公司近 200 个 APP 的敏感API接口调用行为。这两项工作面临一个同样的难题：若要达到理想的防护效果，就需要一定程度上与业务实现绑定，这会给业务和安全的发展带来很多协同上的矛盾和问题。

通过技术、管理、开发和架构人员的共同努力，公司计划针对上述两项问题开展安全平行切面和平行舱建设的实践。目前整个集团已在进行与切面类似技术的安全管控系统的建设实践，通过代码注入，可以在不修改现有业务代码的情况下，实现服务间调用信息的采集和追踪。在此基础上引入平行切面方案，将底层代码注入功能与上层安全管控逻辑实现解耦，可以极大地减少代码注入类产品的重复性开发适配工作和注入兼容问题，并降低未来其他安全管控应用如RASP、权限访问控制等的集成接入门槛。平安科技的安全团队认为，安全平行切面作为一个新的技术框架，可以通过多方共同努力，实现很多具有想象力的场景。未来，平安也将基于自身现状，利用切面思想实现更多的应用模式，包括海量APP终端的隐私保护等。

第四章

IDC建议

安全平行切面能够帮助企业实现对安全问题本源的认知。切面跨越了应用、操作系统和网络等不同的架构设置，以深入业务全局的方式构建安全场景，实现一系列安全服务能力的抽象和标准化。IDC认为，安全平行切面对于未来企业安全架构发展具有重要的意义，企业和厂商需要正视安全平行切面的理念发展和技术进步，并在推进工程化实践的过程中，重点解决好好以下主要问题：

企业

- **战略、组织、文化的升级：**企业的决策层和执行层都需要认识到复杂性爆炸所带来的全新挑战，不断更新自身的安全认知。在引入新的安全体系建设思想的过程中，首先构建起具有前瞻性的新一代企业安全发展战略，形成上下一致的战略认知。在执行的过程中，企业的组织架构和安全文化都需要做相应的升级，以适应安全与业务之间新的协同发展关系。

- **原有安全体系的改造和融合：**企业在过去多年间建设的安全体系仍具有强大的基础防护作用和长期的生命力，在向新一代企业安全架构升级的过程中，企业可以基于统一的切面框架设计，将原有的安全能力逐渐实现平台化、资源化，并以组合服务的形式重新作用于应用系统。在这过程中，企业应面向业务端，选择较为急迫的安全需求场景进行试点，重点解决细粒度感知和规模化处置的问题，让各业务部门充分认可安全切面应用的价值，进而成为整个体系发展的重要参与者。

- **合理选择运营模式：**企业应该进一步关注对安全攻防能效比的提升，从投入和价值的角度衡量和规划安全运营工作，通过高效的安全运营全面提升安全交付效率、研发效率和产品成效，形成可持续发展的安全架构和安全团队。切面的构建可以为包括安全人员在内的企业IT团队提供多样化的运维/运营能力选择。例如，内部研发过程可以利用切面进行更好地管理，因为切面有很强的植入和内视能力，可以对研发过程的大量动态信息进行多维度的分析。同时，系统上线后基于DevSecOps的持续安全运维工作，以及运营时的供应链管理、软件清单管理等，都是切面应用最擅长的施展空间。企业可以根据自身情况，由不同部门牵头建立灵活的一体化运营模式，改变以静态信息为主、各自为战的运营局面。

- **统一规划，分布实施：**企业可以利用安全切面的可见性和可观测能力，首先选择问题集中且较容易上手的业务应用（特别是创新应用），通过对切面的合理配置，强化这些系统的安全感知和安全治理能力；当完成风险的识别后，可进一步通过安全切面对系统的安全防护能力，进行体系化的提升，这有助于企业在实践过程中获得内、外部的全方位支持。

安全厂商

- **自身能效的持续提升：**安全厂商同样需要升级自身的企业文化和发展战略，建立可持续发展的技术、产品、经营和市场体系。在实践安全切面技术的过程中，安全厂商应加大对平台和工具能力的打造力度，力求用自动化、智能化的能力夯实自身竞争优势，帮助用户提升攻防能效比，为用户提供更多类型的高质量服务。

- **生态合作伙伴体系建设：**安全平行切面和安全平行舱构建了一个理想的技术框架和工程化平台，也为安全能力的迭代发展拓展出更具想象力的空间。安全厂商可以利用切面体系实现更多的融合场景创新。因此，安全平行切面的能力发展，很大程度上也取决于其生态体系的丰富度和活跃度。各安全厂商可以根据自身的技术特性和服务定位，深度参与到生态体系的建设过程中，成为某一细分技术领域的佼佼者。

- **优化技术能力，探索更多落地场景：**切面模式提供了对业务系统深度感知和干预能力，使安全厂商更加关注企业业务的发展，在业务创新的过程中寻找新需求，解决新问题。本白皮书的3.1节提供了在切面模式下的部分潜在场景参考，在未来的发展过程中，各行业都会出现带有鲜明行业特征的安全深度融合场景，这些场景也会催生出更多小而专的技术服务团体，使整个安全平行切面体系的发展呈现出枝繁叶茂的局面。

关于 IDC

国际数据公司（IDC）是在信息技术、电信行业和消费科技领域，全球领先的专业的市场调查、咨询服务及会展活动提供商。IDC帮助IT专业人士、业务主管和投资机构制定以事实为基础的技术采购决策和业务发展战略。IDC在全球拥有超过1100名分析师，他们针对110多个国家的技术和行业发展机遇和趋势，提供全球化、区域性和本地化的专业意见。在IDC超过50年的发展历史中，众多企业客户借助 IDC 的战略分析实现了其关键业务目标。IDC是 IDG 旗下子公司，IDG 是全球领先的媒体出版，会展服务及研究咨询公司。

IDC China

IDC中国（北京）：中国北京市东城区北三环东路36号环球贸易中心E座901室

邮编：100013

+86.10.5889.1666

Twitter: @IDC

idc-community.com

www.idc.com