阿里云

阿里云 安全白皮书

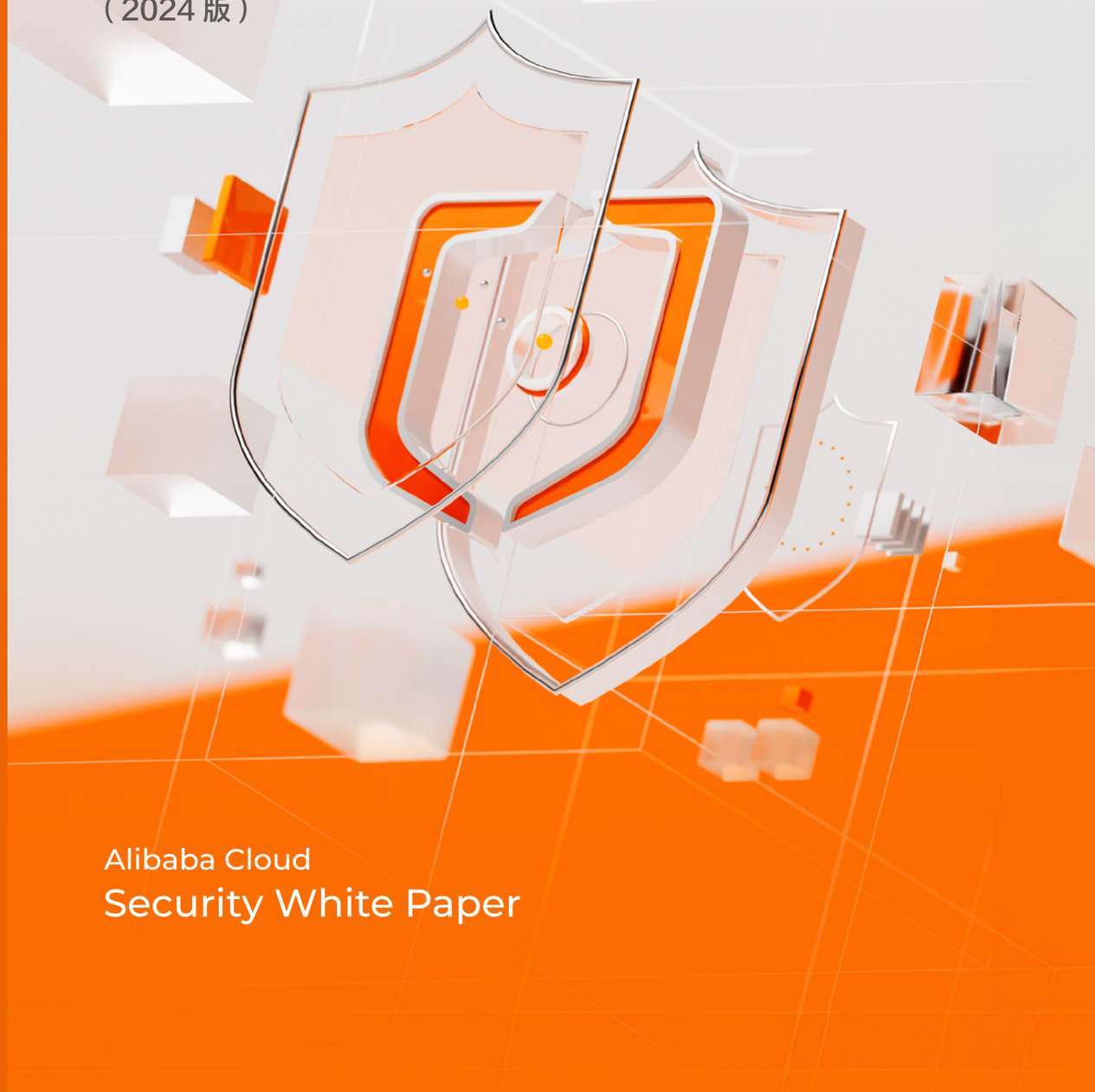
Alibaba Cloud Security White Paper

阿里云

阿里云

阿里云
安全白皮书

（2024 版）



Alibaba Cloud
Security White Paper

阿里云

编写单位

指导委员会

郑俊芳 阿里云智能集团首席战略官

钱　磊 阿里巴巴集团 & 云智能集团安全部总裁

周　拓 阿里云智能集团首席安全官

郑雅敏 阿里云智能集团租户安全负责人

编写组成员（以下按姓氏拼音首字母排序）

常　畅、陈迪思、陈雪琴、陈章炜、冯子强、贺　剑、黄昱恺、靳　滢、李　超、李国强、李海鑫、梁　雷、刘　迪、刘颖男、刘志辉、刘自慧、楼燕华、吕　光、敏　清、聂百川、彭玉轩、钱　岩、瞿孝志、孙戴博、童杰文、屠励杰、王灿鹏、王晓东、王艺颖、王　瑜、魏巍巍、肖　畅、肖　剑、熊自成、杨　磊、杨露佳、殷　慷、于国瑞、张崇臻、张　祺、张仕卿、张　威、张　瑜、张振尧、赵世然、赵　萱、周　颖、曾逸尘、朱　松

特别鸣谢（以下按姓氏拼音首字母排序）

蔡仁毅、晁　巍、崔立喜、高　阳、管　玥、何登成、何　欣、何延哲、郝伟刚、黄少青、黄正艳、季　凡、刘佳良、刘　珂、刘煜堃、马乐乐、马庆栋、欧阳欣、任　懿、石肖雄、谭冠群、唐　洪、徐方芳、许玉娜、汪圣平、王睿超、王云翔、魏朝龙、吴德新、杨杜卿、杨　永、尹　哲、张晓丹、郑原斌、钟　丹、祝建跃

扫码线上阅读

联系我们

cloud_product_security_team@alibaba-inc.com

阿里云
安全白皮书

Alibaba Cloud
Security White Paper

目录 CONTENT

为社会数智化保驾护航

各行业

互联网	金融	制造业	零售
能源	医疗	汽车	……

各地域

中国	新加坡	欧盟	美国
印尼	韩国	日本	……

29 Region　　3200+ 边缘节点　　89 可用区

阿里云　公共云

客户可管可控

身份	数据
RBAC & ABAC	操作可审计
无明文密钥	可信计算　机密计算
多账号关联	一体化解决方案

风险可防可治理

线上威胁感知	原生安全防护
联动防御	按需弹性伸缩
快速无损恢复	适配不同上云阶段

- 坚守数据主权的数据安全保护
- 全链路身份管控与精细化授权
- 面向攻击的安全高可用（稳定运行 / 容灾 / 快速感知 / 快速逃生）
- 全球化背景下的合规支撑（各地域 / 各行业 / 自身合规 / 助力租户）
- 安全防护能力高效弹性可扩展
- 面向线上威胁的快速响应与恢复
- 全流程产品安全保障建设
- 全方位红蓝对抗反向校验

更强安全性　**更低成本**

纵深防御体系　　反向校验

产品安全生命周期：立项 / 设计 / 编码 / 测试 / 发布 / 运营监控

- 白帽社区漏洞悬赏
- APT深入测试
- 三方机构渗透测试

零信任架构　　以攻促防

安全　机制

图：云上安全治理框架

前言 *PREFACE*

数智化技术的快速发展与广泛应用显著加快了社会创新的步伐，并深刻引领着产业升级变革的浪潮。伴随这一转型进程的推进，数智化系统及其所承载的数据资源的重要性急剧攀升，已然成为不可或缺的核心要素。

数智化价值日益凸显也吸引来更多的恶意攻击者，导致这些系统与数据所面临的安全风险与日俱增，为数字化业务运营者带来了前所未有的安全防护挑战。如何应对核心数据安全的严峻考验，如何有效抵御日益复杂的网络攻击，以及如何在追求业务高效稳定运行的同时确保安全合规性，已成为当前亟待解决的关键议题。

阿里云作为全球领先的云计算服务提供商，始终将安全置于战略高度，将云上客户的安全视为阿里云发展的基石。我们致力于不断强化云平台自身的安全防护能力，并通过创新技术和服务模式，助力云上客户构建更为坚固的安全防线，共同构建 “云上安全共同体”。

阿里云在持续加大对云上安全能力的投入、并力求在降低客户安全成本的同时，也提供了全方位、多层次的安全保障。依托云上安全八大支柱框架，我们专注于安全机制与安全能力的建设，为云平台及云上客户构筑起一道坚实的防护网，为各行业数智化转型的稳健前行保驾护航。从安全性的维度出发，我们旨在促进数智化进程中的互利共赢，为社会的和谐稳定与安全发展贡献积极力量。

01.

数智化趋势下的
发展机遇与安全挑战

Benefits and Security Risks in the Trend of Digital Intelligence

1. 数智技术驱动产业加快转型升级

当今世界，新一轮科技革命和产业变革方兴未艾，新一代数智技术得到蓬勃发展和深度应用，人类社会加速进入数字经济时代。

数智技术自身的产业化发展以及与实体经济的深度融合，形成了数字经济时代的新质生产力，不断提高生产、协同、交易、消费及公共服务和治理的效率。当前，数智技术已经与各行业深度融合，加速企业组织协同及研发设计、运营管理、生产制造、供应链管理、市场营销、客户服务等产业链各环节的数字化转型，推动各行业的质量变革、效率变革和动力变革。

在互联网领域，电商企业通过对历史销售数据和市场趋势的深度学习，实现个性化推荐系统的优化，提升产品体验及用户购买率，直接带动了销售额的增长；智能客服系统利用自然语言处理和机器学习技术，能够自动识别并回答用户的问题，提供 24 小时全天候服务。

在金融领域，银行通过大数据平台与智能风控平台进行数据整合加工与风控模型决策，打造普惠金融服务，提升了小微企业和个体工商户的金融服务可得性和服务质量；保险公司通过对海量数据的挖掘和分析，能够识别出不同客户群体的风险特征，从而提供更加个性化和精准的保险产品。

在制造业领域，汽车制造商可以通过部署数字工厂解决方案，实现对生产线的实时监控与智能化调度，传感器收集的海量数据被上传至云端，借助大数据分析，企业能够精准预测设备故障，提前安排维护，提高生产效率。

除了制造、零售、电商等各个行业的渗透和普及，数智技术也在逐步进入影响国计民生的关键领域。2023 年 3 月，国家能源局发布《关于加快推进能源数字化智能化发展的若干意见》，提出加快电力、煤炭、油气等行业数字化智能化转型，通过数字化、智能化技术融合应用，为能源高质量发展提供有效支撑。2024 年 4 月，财政部、交通运输部联合发布《关于支持引导公路水路交通基础设施数字化转型升级的通知》，提出加快公路水路交通基础设施的数字化改造，建设数字化感知网络、智能化管控系统和网络化服务体系；更加注重数据要素价值释放，以数字手段推动交通基础设施管理服务水平明显改进；更加注重融合创新，以应用场景规模化落地，促进产业协同创新水平显著提高。

随着 AI 大模型技术的兴起，生成式人工智能的自主生成创造和推理能力，为内容创作、图片设计、软件开发等任务场景带来强有力的工具更新，极大地提升了生产效率。生成式人工智能也逐步渗透进各个产业领域，指数级扩展了应用边界、加速了数智化转型进程，助力企业经营提效、业务创新、客户体验提升等。面向未来，各行各业都将进一步拥抱数智技术浪潮。

在业务的数智化转型中，云计算在其中起到了重要的底座支撑作用，并且满足当前发展阶段的更高要求。经过十几年的发展，云计算已经演变成体系化、多层次的技术和服务架构，覆盖更多传统行业，并向更多行业的核心生产环节迈进，从而助力千行百业加速转型升级，拥抱数字智能世界。

这里特别需要指出的是，得益于人工智能技术，尤其是深度学习等领域的快速发展，算力需求呈现出指数级增长，而公共云作为应对这一挑战的关键平台，正推动“云计算”向“云智算”转变。它不仅提供基础的计算、存储和网络资源，更整合了模型生态、数据治理和 AI 工具等与智能化发展密切相关的全方位服务。这种转变意味着公共云不仅满足基础 IT 需求，更成为支撑大规模人工智能应用、模型训练与推理的核心基础设施。

2. 数智化发展带来的隐患与挑战

2.1 信息系统安全性影响经济社会的稳定运行

在当今高度数智化的时代，信息系统已经渗透到社会生活的方方面面，包括政府管理、金融服务、交通运输、能源供应、医疗健康、教育科研等各个领域，信息系统的安全直接影响到社会的稳定、经济的繁荣和国家的安全。

政府管理与公共服务方面，政府信息系统承载着大量的政务数据和公共服务功能。如果政务信息系统受到攻击或泄露，可能导致政府决策失误、公共服务中断，甚至引发社会恐慌和不稳定。其中类似税务系统、社保系统等关键政务信息系统的安全一旦受到威胁，将对政府的公信力及民众的生活造成广泛而深远的影响。

金融信息安全方面，金融系统是国民经济的命脉，金融数据是推动金融业发展的核心要素之一，其信息系统安全直接关系到金融市场的稳定和经济的健康发展。黑客攻击、数据泄露等安全事件可能导致金融欺诈、资金流失、市场波动等严重后果，严重时可能引发金融危机。

其它关键信息基础设施，能源、交通、通信、医疗、教育等基础设施的信息系统安全也至关重要。这些系统的稳定运行是社会经济活动的基础。一旦这些系统受到攻击或瘫痪，将严重影响国计民生和公共利益，甚至可能引发灾难性后果。

就像硬币的两面，数智技术走进千行百业，与社会、与行业深度融合的同时，整体的数字系统的安全性也直接影响到国家、社会和企业的稳定，这是数智化发展到一定阶段的必然挑战。随着我们面临的安全挑战日益增多且变得更加复杂，我们需要不断提升安全防护、巩固安全机制、强化态势感知，全产业一起共同努力，确保数字世界的可持续与稳定性。

2.2 数据逐渐成为组织的命脉，但数据安全隐患愈发凸显

数字化转型已经成为企业及组织发展的“新动能”，数据作为核心资产，已经成为组织的新型生产力，在战略决策、产品创新、运营效率提升、客户管理等方面都起到了重要作用。但随着跨行业、跨部门、跨层级、跨地域、跨系统、跨业务的数据采集、存储、传输、使用等场景的与日俱增，数据在发挥更大作用、创造更大价值的同时，重要数据和个人隐私信息遭篡改、泄露等问题也越发突出，数据滥用、暗网交易等黑灰产活动日益猖獗，对企业和组织及社会公共利益带来了严重威胁。

全球数据泄露事件持续高发。根据 Forrester 的《2024 年网络安全 TOP 风险趋势》报告中显示，存在 78% 的受访者在过去 12 个月中敏感数据被泄露或系统被入侵过，数据泄露给受访者带来的经济损失平均高达 218 万美元。数据泄露对政府、企业和个人构成严重威胁。

加强数据治理、保护数据安全，为数字经济持续健康发展筑牢安全屏障，这是时代发展的客观需要。应加快建设全流程、全环节、全场景的数据安全管理体系，重视数据分级分类、数据角色授权、数据安全过程场景化管理，推动数据安全治理体系持续改善。

2.3 网络空间安全威胁日趋严峻

数智化趋势下，网络空间安全威胁的态势愈发严峻，网络安全已然成为数字时代国家安全战略的基石。当前，全球网络空间正面临着多方面的挑战，包括但不限于网络攻击规模不断扩大、新型网络攻击手段的层出不穷，以及国家级网络安全对抗日趋明显。

一是网络攻击规模扩大。越来越多的社会生产活动依赖数智化系统，这些系统的价值持续上升。进而促使在网络空间中，受利益驱动的攻击行为频繁发生，导致网络攻击规模持续扩大。根据 Veeam 的《2024 年数据保护趋势报告》，四分之三（75%）的组织去年遭受过至少一次勒索软件攻击。

二是新型网络攻击手段不断涌现。人工智能等新技术的发展同时也导致网络攻击成本进一步降低，勒索软件、APT 攻击等高级威胁正在经历一次“网络犯罪技术革命”，人工智能技术的恶意使用也成为 2024 年最主要的网络风险之一，攻击者通过使用恶意的大模型工具（如 FraudGPT、WormGPT），可以自动创建网络钓鱼电子邮件和恶意软件，使得网络钓鱼活动更加容易实施。小语种恶意软件威胁不断增加，使用 Go、Nim 和 Rust 等小语种编程语言开发的恶意软件增加，相应的安全分析工具较少，难以被检测和拦截，造成勒索软件飞速传播。

另外，国家级网络安全对抗日趋明显。国际网络空间安全威胁不仅影响世界形势，也对未来网络空间国际秩序的走势产生了深远的影响。一方面是网络战和信息战的对抗增加了网络空间的紧张局势，冲突双方利用网络进行攻击，包括黑客攻击、关键信息基础设施打击等动态效应，以及运用舆论手段巧妙影响公众心理效应。其次世界形势也揭示出网络空间武器化的危险性，表现为代码武器化、社交媒体武器化、以及互联网资源武器化。这种趋势对国际网络安全构成了严重威胁，破坏了互联网底层的信任基础，加强了网络空间碎片化趋势，并可能加剧网络空间的军备竞赛。在国际冲突中，非国家行为体如黑客组织等也参与其中，发起大规模的网络攻击。这些非国家行为体的参与使得网络空间的对抗态势更加复杂化，给国际网络安全带来额外的挑战。

综上所述，数智化转型加速推进，深刻改变了社会经济的运作模式，为企业发展和人民生活带来了前所未有的便捷和效率提升。然而，这种变革同样催生了一系列新的安全问题，使得系统安全、网络安全和数据保护成为数字时代必须直面的重大挑战。各行各业特别是承载关键数据资源和业务系统的云平台更应该发挥积极作用，强化安全治理体系，构建安全的环境。

2.4 数智化发展对安全提出更高要求

数智化发展不断加速，相较以往产生了一系列变化。日益增长的价值催生了更多的攻击，愈发深入的场景，增加了安全防护的复杂性。愈发白热化的竞争，要求企业能够同时保障敏捷与安全。

数智化时代因此对安全防护提出了更高的要求：

先进普惠的安全技术：严峻的安全威胁需要先进的安全攻防技术来保障，同时应当降低使用这些先进技术的成本，使其成为大多数组织可用、易用的技术。

敏捷高效的安全能力：由于快速发展的需求，要求安全防护能力能够随着业务的变化而弹性伸缩，并在业务的不同阶段支持高效地完成安全治理工作，维持业务的敏态。同时在业务的敏态下，保障业务运行的稳定性与合规性。

丰富全面的解决方案：场景的不断丰富和深入，要求安全防护能力也能够不断进化，适应不同的场景，并提供贴近于具体场景的安全解决方案。

02.

公共云安全治理愿景与框架

Vision and Framework for Alibaba Cloud Security Governance

1. 治理理念：云上安全共同体

随着数智技术的产业化发展及其与实体经济的深度融合，企业对云计算的需求日益增长。数字化转型的加速推动了企业上云用云的比例显著提升。“全面上云”浪潮愈演愈烈，“深度用云”特征日渐明显。

云上安全的建设，需要企业和云服务商之间秉承一致的安全理念。恰当的安全理念，能够促成上云企业与云服务商之间快速建立对云安全的理解和共识，解决云上业务流程与线下 IT 流程相异的安全管理问题；也能够帮助深度用云企业解决云上复杂生态系统带来的更高安全协作需求。

阿里云基于多年集中的安全技术投入、丰富的风险应对经验、完善的安全组织机构、灵活规范的安全措施落地机制，和为客户云上安全提供支持，为社会安全稳定贡献力量的不移决心，正式提出 “云上安全共同体”这一安全理念，以**驱动云上安全的建设。**

云上安全建设中，云服务提供者无疑是最关键的角色之一。在“云上安全共同体”理念的引导下，阿里云不仅会坚守安全责任共担模式云服务商的责任，搭建和提供“安全的云”，如基础设施、物理设备、分布式云操作系统及云服务产品安全，保障云平台基座的安全。与此同时，阿里云也会帮助客户“安全使用云”，从而优化云上安全的“最后一公里”，实现共同安全目标的治理理念。

“云上安全共同体”的安全理念，以实现保护云环境中数据和资产安全的共同目标，云平台发挥主观能动性，提供更多可供客户采取的安全保障措施，与云上客户一起形成一个紧密相连、互相支持的安全防护网络，构建一个多层次、相互协作的安全保障体系，促成深度用云安全，从而进一步造就云平台的运行安全。以云产品安全配置为例，客户需要根据上云数据、系统的定级决定安全策略，根据安全策略自行开启安全配置。在安全共同体理念的方向引导下，阿里云主动为客户提供了更多默认的安全配置与风险提示，支持客户实现配置安全。阿里云深知，如果我们的客户不安全，那么阿里云作为云平台就无法实现真正意义上的安全。

“云上安全共同体”理念的提出，标志着阿里云作为领先的云平台，不仅勤勉尽责地履行承担本职的安全责任，更致力于提供一系列切实可行的安全保障措施，这些措施旨在 帮助客户更深入地思考、制定、理解安全策略，并支持这些安全策略更顺畅、便捷地落地实施。

阿里云致力于从打造“安全的云”和赋能“安全使用云”两个核心维度践行云上安全共同体理念。

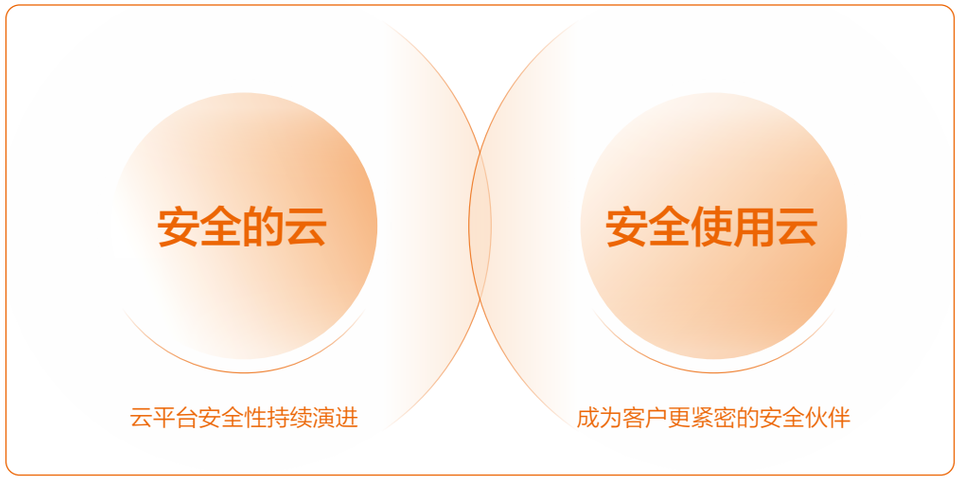


图 2.1.1：云上安全共同体

安全的云。阿里云坚持在云安全领域进行持续投入，促成云平台安全性的持续演进。如持续汇聚安全精英人才，建立全球顶级的安全团队；不断建立和完善原生先进的安全能力，提高云产品自身的安全能力和提供更丰富的云安全产品；通过制定有效的安全预案及通过实践充分演练，能更早地介入威胁发现和风险防范的过程，以确保在遇到各类网络攻击时，云平台能更快地响应、更有效地防护。

安全使用云。基于平台经验和能力的沉淀，阿里云围绕云租户的安全管理需求提供进一步的强化安全保障服务，致力于成为客户更紧密的安全伙伴。如对于云产品设置更高的初始安全水位，提高云产品使用的安全性；通过提供更普惠的安全能力，促成更低的用云安全成本；通过增强多方位的安全检测和防护能力，实现安全事件的主动响应，通过提供全面而易于理解的安全指南和最佳实践，推动安全科普与安全意识的培育，使用户能够清晰地了解云服务的安全性能和潜在风险，做出明智的决策。

阿里云希望能通过这些安全保障措施建设工作，展现我们对云上安全的坚定承诺，以及 为客户提供一个安全、可靠和合规云环境的决心。为了更清晰、具体地陈述相关工作，在本次安全白皮书中，阿里云会就构建平台核心安全保障的八大支柱进行呈现。如希望 查阅更多关于安全共同体理念的落地内容，敬请关注官网和阿里云发布的其他信息。

2. 治理目标：更强安全性与更低成本

在当今数智化时代，云计算正以前所未有的速度改变着企业的算力建设模式、IT 运营流程与业务支撑方式。其不仅为企业提供了前所未有的灵活性和可扩展性，更在安全性与成本效益方面展现出了显著优势。而全球头部云计算厂商通常具备绝对的规模优势和长期的运营经验，凭借深厚的技术积累、严格的安全标准遵循、以及持续的安全研发投入，构建了更加坚固的安全防护体系，确保了云计算环境相比传统 IT 架构具备更高的安全性。

2.1 云安全提升更强的安全性保障

阿里云不仅遵循国际 / 国家安全标准以及安全合规要求，还通过多层防御策略、数据加密、访问控制、安全审计与监控、以及实时的威胁检测与响应机制等方式，全方位保护客户系统与业务免受各类安全威胁，让云计算尤其是公共云成为企业数字化转型中更加值得信赖的选择。

- **全球顶级的安全团队**

  阿里云拥有专业的安全团队，这些团队具备行业领先的技术能力，并基于深厚的行业经验，不断地夯实云基础设施的安全防御能力，以“零信任”“纵深防御”的先进安全架构，应对层出不穷的安全威胁，并基于自身攻防对抗经验，为客户提供专业的安全解决方案。

- **原生安全能力支撑**

  原生安全是云计算安全性的重要组成部分，它强调从设计之初就将安全考虑融入应用程序和服务的每一个环节中。在一些核心攻坚类技术领域，阿里云将行业领先的防御技术（如 ECS/ 机密计算、ACK 机密计算）与安全用云策略（如配置审计与一键修复）融入到产品中，以方便云上客户使用，无需自行研发。

2.2 云安全保持更低的成本消耗

在不牺牲安全性的前提下，云计算可以有效降低安全成本和时间成本。企业无需自行构建和维护复杂的安全体系，也无需担心因资源闲置或过度安全配置而造成的浪费，从而能够更加专注于业务创新和发展，正因如此，云计算尤其是公共云以其卓越的安全性和显著的成本优势，正成为越来越多企业的首选。

- **经济成本优化**

  阿里云通过提供集中的安全资源、自动化的安全更新与监控以及规模经济效应，显著降低了企业的安全成本。相比传统 IT 环境，云计算服务商能够利用先进的安全技术和专业团队来保护其庞大的数据中心，这种集中化的安全管理方式不仅提高了安全性，还使得企业无需投入大量资金自建和维护复杂的安全体系，从而实现了安全成本的有效降低。

- **时间成本节约**

  阿里云通过提供即时可用的安全产品服务和自动化管理工具，大幅降低了企业在安全加固上的时间成本。企业无需从零开始构建和维护复杂的安全体系，而是可以直接利用云服务商提供的成熟安全解决方案，快速响应安全威胁，优化安全策略，从而节省了大量在安全建设、管理和维护上的时间投入。

3. 治理框架

从云上安全共同体的角度出发，为达成云上更强安全性、更低成本的目标，阿里云在安全机制、安全能力上做出了一系列设计与建设，共同构成了云上安全八大支柱，以保障云平台自身具备足够的安全水位，且能够最大化地帮助客户提升客户侧安全水位。

3.1 安全机制保障

云平台基座的安全，是云上安全的基础，为确保万无一失，阿里云建设了全生命周期的安全保障机制和全方位的红蓝对抗反向校验机制来保障云平台的安全。

- **全流程产品安全保障建设**

  阿里云在产品全生命周期中，通过多环节干预，以纵深防御、零信任架构设计理念为指导，并通过自动化、数字化安全分度量机制，切实保障安全要求的落地。最终，使云平台、云产品具备高安全水位。

- **全方位红蓝对抗反向校验**

  安全水位需在攻防对抗过程中不断提升，阿里云在内部建设了红蓝对抗体系，蓝军团队采用 APT 级强度对云平台开展渗透测试，从内部视角查漏补缺。 另一方面，阿里云拥有完善的外部白帽生态及漏洞悬赏机制，邀请第三方服务商来进行渗透测试、漏洞挖掘，从外部视角验证云平台安全防御水位。

3.2 安全能力支撑

云上安全需要云平台和云上客户的共同安全，在云平台安全基座的基础上，阿里云还将“保障客户安全”的设计融入到了方方面面，争取最大化地助力客户云上安全建设。

- **坚守数据主权的数据安全保护**

  在客户数据主权及机密性保护方面，阿里云从机制、技术架构角度，保障客户的云上数据仅用于符合客户自身意图的场景，不会挪作他用。同时，阿里云还具备各类数据安全保护机制，可默认提供比绝大多数自建环境更安全的数据存储、传输、使用环境，避免外部不法分子窃取数据。

- **全链路身份管控与精细化授权**

  在信息技术高速发展的今天，进行高效、灵活的数据流动、网络联通是云平台的优势所在。为了安全地达成这一目的，身份权限管理至关重要。阿里云提供了全链路身份授权与权限管控体系，支持客户按照“最小够用”原则，细粒度地按需分配云上权限，从而确保数据流动、网络联动符合客户场景需要的同时，不因过度授权而使客户系统安全性受到负面影响。

- **安全防护能力高效弹性可扩展**

  作为云原生时代的基础设施，阿里云所提供的安全防护能力，可随着基础设施的弹性伸缩而灵活调整，实现了安全防护能力的高效弹性，有助于降低安全防护的时间成本。阿里云在基础产品之上开放可扩展能力，便于三方安全厂商集成云上基础产品，并发挥出更好的性能与稳定性，提升云上客户安全防护的可扩展性。

- **面向线上威胁的快速响应与恢复**

  安全是持续对抗的过程，阿里云提供了风险感知、数据备份等服务，即使客户因外部入侵导致服务受损，对应的产品能力也能帮助客户达到快速感知、快速响应、快速恢复的目的。

- **面向攻击的安全高可用**

  阿里云建设了完整的安全高可用架构，如租户隔离、负载均衡等方式，并建设严密的监控发现能力、服务快速恢复能力，以保障云服务在面对安全攻击时的高可用性。

- **全球化背景下的合规支撑**

  阿里云积极拥抱监管合规，持续推动云平台与云产品自身符合各地区、各行业监管合规要求，并将共性合规要求融入到云安全产品功能设计中，以帮助客户按需地选用产品功能，来满足使用过程中的审计与合规需求。

阿里云坚定地与客户一起，迎接日益严峻的云上安全挑战，帮助客户以更低的成本具备更强的安全性。在后续章节，将详细展开阿里云安全治理框架，以帮助客户更好地理解和利用云上安全优势。

03.

云上安全重要支柱

Important Security Capabilities of Alibaba Cloud

1. 全流程产品安全保障建设

攻防对抗不是单一环节的较量，阿里云秉持“多层防护、全面覆盖”的理念，深入贯彻DevSecOps，将丰富的安全工具和安全管控流程无缝集成至产品研发的各个阶段。通过多环节协同合作，共同负责风险控制，从而确保安全效果不再依赖于任意单一环节。

在传统的软件开发生命周期中，安全检测和修复通常集中在发布阶段，这种方式容易导致工作积压，存在效率低下的弊端。阿里云通过产品设计阶段威胁建模、开发阶段提供安全编码 IDE 插件、测试阶段执行自动化漏洞扫描等方式，在前置环节发现风险，有效控制了安全治理成本。通过应用接入 RASP、WAF 的方式，提升了线上产品对外部攻击和新兴 0day 漏洞的免疫、防御、拦截能力。使安全治理流程更加高效、可持续。

在与全球顶级黑客团队对抗的过程中，阿里云贯彻纵深防御和零信任架构的设计理念，建设了世界领先的安全架构，这一架构通过多层次防御机制，不仅保障了云平台自身安全，还保障了客户数据及资产的安全性，不让任何一个环节成为安全漏洞的突破口。

安全架构设计和安全流程的关键在于实际执行，阿里云不仅在理论上进行了充分规划，还通过建设内部度量机制，确保安全流程在各个团队中得到严格遵循和执行，通过对流程的监控和评估，阿里云切实履行了其在安全保障方面的承诺，确保每一环节的安全措施都落实到位。

1.1 安全流程：产品全生命周期

阿里云通过将安全管控要素嵌入产品研发流程，实现了安全管控与产品研发的同步启动、同步实施以及同步完成。产品研发安全生命周期共分为六个关键环节：立项、设计、编码、测试、发布、运维 & 监控。阿里云在整个产品研发过程中内置标准化的审核流程和自动化安全工具，旨在将产品研发过程中的潜在风险扼杀在上线前，并在产品上线后及时发现和响应新的安全风险，这一全流程的安全管控机制，使得安全不再是最后的补丁，而是贯穿于整个研发生命周期的核心要素。

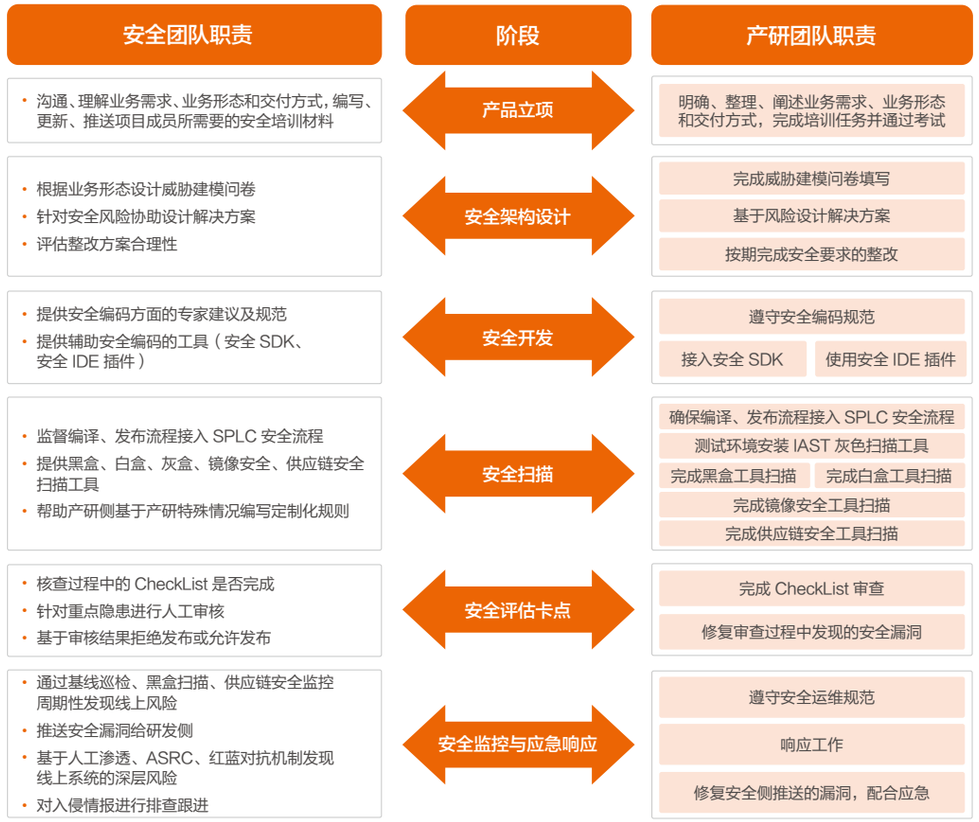


图 3.1.1：阿里云产品安全研发流程

1.1.1 立项环节

在产品立项环节，产品研发团队和安全团队将充分沟通，明确业务需求、业务形态和交付方式，确认双方可接受的风险程度，并明确安全责任边界。这种协同合作是确保产品安全的基础。

产品立项环节的目标是厘清该产品业务背景下云平台需实现的防护效果，并要求参与业务的各职责人员具备充足的安全知识及安全意识，避免因安全知识、安全意识不足，而引发线上风险。在立项环节中，阿里云要求产品线一号位、产品经理、项目经理、研发、运维、交付等相关人员必须完成安全培训考试，牢记产品安全红线和安全基线。

阿里云平均每年完成线上安全培训和考试数万人次，完成线下培训数千人次，并具备配套的数百份安全规范文档，覆盖产品研发全流程和全部岗位类型，以指引产品研发工作安全、合规地开展。

图 3.1.2：安全培训机制概览

1.1.2 设计环节

安全团队会在设计环节介入，辅助产品线完成安全架构的设计与评审工作。对产品的部署架构、网络架构、应用架构、接口交互逻辑和租户隔离架构进行完整的威胁建模，事前识别出产品的安全风险，并给出针对性整改建议。

安全是阿里云的生命线。因此在产品管理流程中，安全团队具备产品设计方案的一票否决权，并将安全审核作为产品上线的关键卡点，从而保障安全要求的落地。

阿里云产品的架构评审完成率均达 100%，威胁建模标准库中累积数百条风险判断规则，以全面发现各场景、各层级下的安全隐患。

针对云计算的特殊场景，阿里云重点关注租户隔离方面的风险治理，在不同层级实施了不同强度的加固措施。

针对云场景下的租户隔离问题，阿里云在虚拟化层、网络层、网关层、应用层、主机层架设了不同层面的纵深防御体系，在假设单层防御失效的情况下设计整体防御方案。

在虚拟化层，阿里云自研了 ECS 沙箱隔离、袋鼠安全容器技术，从架构角度解决云上资源共享及调度带来的租户隔离影响，并在容器集群内统一配置严格的 NetworkPolicy、WebHook 拦截能力，拦截集群内的异常访问请求。

在网络层，阿里云在不同类型业务间、不同产品间严格使用 VPC 进行默认隔离架构设计。对于核心生产网，额外实施内网 L4 层零信任隔离，具备机器、IP、端口粒度的动态隔离阻断能力；对于容器环境，使用自研的 SideCar 能力，对网络流量进行清洗和隔离；对于网络通道，在各类计算资源与公网资源之间，实行“非必要不互通”的策略，加大外部攻击者通过 C2 通道控制计算资源的成本。

在网关层，阿里云实施动态智能的流控策略，避免 A 客户的异常操作影响到 B 客户，并支持业务在网关层配置接口鉴权，避免因内部研发过失导致客户间越权访问资源及数据。

在应用层，阿里云除了通过产品安全研发全生命周期管控，最大化规避研发编码失误导致租户隔离被突破以外，还针对 0day 漏洞导致租户隔离被攻破的场景，提前部署了 Web 应用防火墙、运行时应用自我保护 RASP 工具，使应用具备应对 0day 漏洞的默认免疫力。

在主机层，阿里云通过自研工具安骑士，实时监控和响应主机上的异常行为，并及时处置。

不同层级的安全架构设计，共同组成了阿里云的纵深防御体系。阿里云的安全防护不仅仅依赖于单层的防御机制，而是永远在“单层防御已被攻破”的假设下，设计更深的防御机制。阿里云也基于“零信任”的理念，结合自身与顶级黑客团队的对抗经验，实施建设了一体化的零信任安全架构，这一架构的细节，将在 1.2 中详细阐述。

1.1.3 编码环节

所有产品研发人员在编码时，必须严格遵守安全编码规范，主动接入安全团队设计并封装的安全 SDK，使用统一、标准化的安全修复方案，安装安全 IDE 插件，在测试及预发环境安装 IAST 灰盒插桩程序，确保业务经过安全扫描等。

在编码环节，阿里云希望将多种风险扼杀在摇篮，核心措施包括：

针对潜在漏洞治理，通过编码规范、IDE 安全编码插件的方式，将诸如 SQL 注入、命令执行等基本漏洞，尽量在编码环节规避；

针对越权风险设计及实施鉴权切面机制，通过代码层切面的方式，控制研发编码失误导致的鉴权失效问题；

针对代码层 0day 风险，在编码环节内置运行时应用自我保护工具 RASP，使应用具备对 0day 漏洞的默认防御能力；

针对编码过程中极易出现的凭证泄露风险，阿里云提供了自研的零信任凭据轮转解决方案、动态轮转代码中关键凭据 (如 AccessKey)。与此同时，限制凭据的合法使用范围，一旦凭据泄露立刻轮转止血。

1.1.4 测试环节

阿里云自研了黑、白、灰盒安全扫描工具，并通过 SPLC 安全运营平台嵌入整个研发流程，对产品源代码、供应链组件、开源代码进行安全扫描。

产品研发工程师不需要单独提交扫描工单，在研发平台点击发布按钮后，自动进入白盒扫描，覆盖 100% 常见漏洞类型，这一过程对产品整体研发进度几乎无影响。

产品部署到测试环境后，会默认强制接受灰盒扫描，通过动态 Fuzz、模拟攻击行为的方式，准确地发现安全风险。

阿里云在产品上线前会对测试环境完成黑盒扫描，主要排查弱口令、1day 漏洞等风险。

1.1.5 发布环节

产品发布前，会进行默认配置检测，以保障产品遵循最小权限、最小暴露面、账号合理授权等基线要求；同时进行敏感信息检测，规避口令、AK 等泄露风险。

原则上，所有产品都需要接入运行时应用自我保护工具 RASP、Web 应用防火墙等安全工具，以构建产品自身的纵深防御体系。

针对产品上线前依然存在的疑似安全风险，由阿里云权威安全专家进行最终评估和确认后才能上线。

1.1.6 运维 & 监控

产品上线后，还涉及以下流程：

基于零信任可信的架构设计，在运维环节，对流量、资源配置、外部人员操作行为数据进行收集，并分析审计出潜在风险，按照相关规范制度规定的时间，及时推动解决。

进行日常运维和风险监控，一旦出现安全风险，立即启动应急响应。敏感数据在传输、存储过程中均为密态。若与客户业务相关，仅在获得客户授权的情况下开展处置操作。

通过红蓝对抗、产品众测、攻防比赛等形式，反向验证产品的安全性，主动发现产品迭代过程中出现的新风险，并及时加固和修复。

应急响应环节若发现流程、工具能力有不足之处，将尽快纳入到内部需求池中，排期进行优化；若发现新的威胁类型，会迅速上线防御策略。

1.2 安全架构：阿里云零信任体系

零信任的核心理念是不单纯依赖网络请求来源和单一身份凭证，而是通过各层、各场景的信息，综合分析潜在的风险，从而拦截可疑的攻击者，实现动态安全。对于云厂商而言，保护客户数据安全是其核心要务。从设计层面实现这一目标，需要从全链路的角度识别哪个环节对客户数据执行了操作，不仅要防止外部攻击者的渗透攻击，还需要预防内部员工被钓鱼所带来的操作风险。

安全可信：全链路可信身份传递，多层纵深防御，持续监控与响应

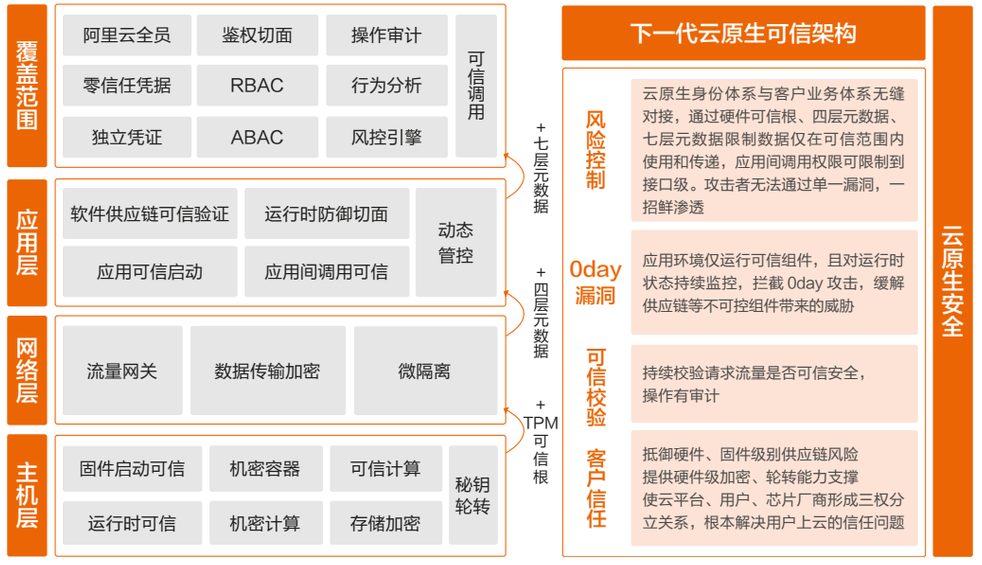


图 3.1.3：下一代云原生可信架构

阿里云平台将身份数据在全链路进行传递，包括主机层、网络层、应用层及业务层。其中主机层记录和传递主机硬件身份信息，网络层记录和传递网络 IP、端口等四层信息，应用层记录和传递进程信息、接口等应用运行时信息，而业务层记录和传递具备业务属性的访问者身份 ID 标识信息。

阿里云通过零信任体系的建设，实现了以下关键成果：

全链路风险控制：阿里云将云原生身份体系与客户业务体系无缝对接，通过硬件可信根、四层元数据、七层元数据，限制数据仅可在可信范围内使用和传递，应用间调用权限限制到接口级别。攻击者无法通过单一漏洞完成对云平台的渗透工作。

防御 0day 漏洞：阿里云平台的应用环境仅可运行可信组件，且持续监控运行时状态，从而大大缓解了 0day 漏洞与供应链组件带来的威胁。

防止内部误操作：阿里云通过持续校验请求流量是否可信，对内部操作进行充分审计，从而最大化避免误操作，确保内部操作安全规范。

1.3 安全制度：安全分机制

在安全实践中，“三分技术、七分管理”的理念至关重要。为持续性保障各个产线的安全水位，阿里云创造性的推出了针对各个产品线的安全评价体系，即“安全分”。

安全分覆盖了阿里云产品安全基线条例的大部分内容，如“公网服务未接入WAF”“ECS 实例未经安全审核开放公网”，其目的在于揭示隐藏于各类产品配置中的潜在安全弱点，使之显而易见。并且分数权重能够清晰地呈现出治理优先级，以帮助安全工程师和产线有序地完成改进措施。

安全分的计分逻辑是从阿里云整体安全建设角度出发，综合考虑不同问题的治理 ROI。这些逻辑由具备丰富实战经验的安全专家进行设置，并经过安全团队与产品线评审通过后正式确定。此外，在实际运行中，安全分会不断优化和迭代，以确保其有效性和适应性。

安全分的计算基于平台自动机制完成。在云资源安全配置、安全防御接入等领域，可以通过自动化巡检能力发现和清洗需要进行治理的数据表，并在配置完成后自动刷新数据。对于无法进行自动计算的部分，比如产品架构设计，在产品安全接口人上报后并通过安全团队审核完成后计分。这两部分数据源按预先设定的权重相加来得出每个产品的最终分数。所有关于安全分的动态变化都在统一的可视化平台上呈现。

通过内部的安全分平台，产线可以清晰感知到安全风险以及安全风险治理的优先级。此外，安全分平台还与内部流程平台联动，不仅提供了风险治理的针对性解决方案，而且还提供了治理入口和工单，从而极大地降低了产线内部以及产线和安全团队间的协作成本。这也提高了安全运营的效率，确保了安全治理目标的贯彻执行。

通过内部的安全分平台，产线可清晰感知到安全风险以及安全风险治理的优先级。并且，安全分平台还与内部流程平台联动，在提供风险治理的针对性解决方案的同时，也会给出治理入口和工单，极大地降低了产线内部以及产线和安全团队间的协作成本，提高了安全运营的效率，确保了安全治理目标的落地。

2. 全方位红蓝对抗反向校验

尽管阿里云已建立起一套系统化、立体化的全方位安全防护体系，但我们深知安全是一个动态对抗的过程。若仅从单一视角进行防御建设，可能会因单一参与方的盲区而在真实的对抗场景下被攻破。

为了防止可能发生的“安全策略失效”等问题，阿里云平台的安全能力持续保持在线状态，在动态对抗中持续提升安全水位，我们相信只有让“红蓝对抗”常态化，才能保持防御水位。一方面，阿里云在内部建设了“红蓝对抗”体系，蓝军团队不断研究新技术，保持与业内顶尖团队的交流，时常以“APT 级”的强度对云平台发起渗透测试。另一方面，阿里云拥有完善的“外部白帽生态”及“漏洞悬赏机制”，定期邀请高水平的第三方“安全服务商”针对云平台进行渗透测试、漏洞挖掘，从外部视角验证并加强云平台安全防御能力。

2.1 内部定向 APT 模拟实战

APT（高级持续性威胁）攻击在全球范围内对国家安全、经济稳定、基础设施安全以及个人隐私构成了重大威胁。这类攻击以其高度的技术复杂性、长时间的潜伏期和精准的目标选择为特点，对政府、大型企业和个人造成了深远的影响。从国家战略层面的机密泄露到关键信息基础设施的瘫痪，再到经济领域的商业机密被盗，APT 攻击已成为一个不容忽视的全球性问题。

阿里云作为国内市场份额最大的云厂商，内部业务结构多元、访问流量复杂、身份变动频繁，面临着超复杂的环境，涉及数百万服务器、数百个数据中心、PB 级流量、数万名员工、上百个全球办公场景、数万量级域名。如果仅以防守方思维去构建安全，难以面面俱到。由此，**阿里云基于攻防对抗思想，建立了内部红蓝对抗体系，常态化模拟最接近真实场景的**攻防对抗，**最大化提升平台安全性。**

图 3.2.1：阿里攻防对抗体系设计

阿里云攻防体系主要以“定向 APT 攻击”作为核心主旨，完成内部的攻防演练。攻击团队（以下简称阿里云蓝军）会以 MITRE ATT&CK 框架作为指导，系统地模拟外部攻击者的行为，而防守团队（以下称阿里云红军）会进行持续性防守。整个演练过程，主要包括以下几个阶段：

- **攻击规划阶段：**
  - 将以某个阿里云产品或内部系统系统作为演练靶标对象，进行定向目标的信息收集，包括但不限于 OSINT、网络扫描等。
  - 基于收集到的信息，分析目标的潜在攻击点和薄弱环节，选择攻击手法，构建复杂攻击链，设计完整的模拟攻击流程。
  - 由 APT 演练的项目负责人完成整体攻击方案的确认，编排攻击资源，包括但不限于定向挖掘 0day 漏洞、可控攻击链投毒、特定性远程控制攻击工具的编写与测试，形成攻击链路图。
- **攻击执行阶段：**
  - 阿里云蓝军成员将严格按照攻击链路图进行模拟定向 APT 攻击的实施工作，并记录阿里云红军对于攻击实施的实时反应。
  - 考虑到攻击行为可能被阿里云红军感知，阿里云蓝军还会选择特定攻击技战法，例如社会工程学攻击、中继攻击、隐蔽攻击等手法，建立稳定的攻击驻留点。

  - 当获得稳定驻留点后，会根据当前收集到的目标信息，尝试访问目标系统，并使用预先构建的武器化攻击工具定向攻击演练靶标系统，从获取系统普通权限到获取系统管理权限再到获取该系统主机权限，完成靶标系统的完全掌控，达到预先定型 APT 攻击的目的。
- **复盘修复阶段：**
  - 收集整理攻击反馈数据，包括成功和失败的攻击尝试、定向 APT 攻击目标的防御反应等。
  - 阿里云蓝军与阿里云红军，将共同完成最后的总结复盘工作。
  - 演练过程中所发现的漏洞及防御体系薄弱点，将由阿里云红军负责人带回，供设计形成解决方案并推动落地，并推动逻辑，以弥补防御体系的短板。

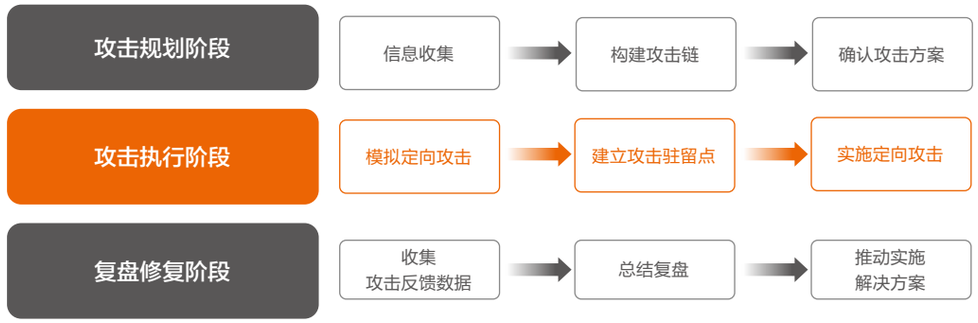


图 3.2.2：红蓝攻防演练流程

2.2 自动化红蓝对抗平台

为应对日益严峻的网络安全挑战，确保安全防御能力始终处于最优状态。阿里云构建了一套 7x24 小时全自动化红蓝对抗平台，

平台通过深度整合内部和外部的攻防案例，将多种攻击手法进行随机打散与重组，在阿里云全域内开展高频次、自动化的演练。该平台不仅提升了阿里云对复杂攻击的应对能力，还确保了安全防护体系能够持续优化，以应对不断变化的网络威胁。

图 3.2.3：自动化红蓝对抗平台流程

2.2.1 常态化安全对抗

1. 全自动化演练机制：通过深度整合外部 APT 事件、MITRE ATT&CK 框架和内部自编写攻击案例，平台能够实现全自动的在指定演练范围内进行攻防对抗，过程中无需人工进行介入，确保全天候攻击与防御能力验证。

2. 随机性与多样化：演练目标的生成过程是随机化的，结合历史安全攻防事件和公开工具攻击手法的随机组合，提升了对抗环境的多样性和真实感，确保能够覆盖多种潜在攻击情境。

3. 可视化输出与风险同步：每次演练后，平台会自动生成详细的攻击路径以及可视化评估报告，通过输出各个演练过程的关键节点，并实时同步安全风险，确保快速反馈和问题暴露。

2.2.2 防守过程稳定性

1. 节点负载智能控制：在多节点并行演练的过程中，系统会根据节点的负载情况自动调整演练规模，避免对生产环境造成过度影响，同时保证业务系统的连续运行。

2. 日志追踪与审计：平台具备全流程日志记录功能，任何演练操作都可以被详细追溯，确保事件的透明性和可审计性，以防止误操作或者不合理的攻击行为对系统产生风险。

3. 应急场景秒级熔断：当演练过程中出现异常情况时，系统能够在秒级响应并快速进行熔断，确保生产环境的稳定性，避免对核心业务系统造成影响。

2.2.3 复盘推修

1. 发现与问题反馈：演练结束后，平台会自动检测发现的安全问题，通过查看平台输出的报告内容以便同步对应的安全风险。

2. 持续验证机制：平台会自动化发起常态化验证，确保每个已修复的安全问题在不同场景下的持续有效性，防止已解决的漏洞再次复现。2.3 外部三方验证。

2.3 外部三方验证

为了进一步加固安全防线，阿里云积极引入国内外优秀的第三方渗透测试服务提供商，通过专业的外部验证手段，确保云平台及产品的安全性达到国际领先水平。

外部三方验证：是指聘请独立的安全专家团队，运用专业的渗透测试技术和工具，模拟黑客攻击行为，对目标系统进行深度安全检查的过程。这一过程旨在识别和评估系统安全控制的有效性，揭示潜在的安全弱点和威胁，最终提出改进建议和修复方案。

2.3.1 合作伙伴甄选与认证

阿里云在全球范围内精选具备深厚安全背景、技术实力与良好市场口碑的第三方渗透测试服务提供商。合作厂商需满足严格的资质要求，包括但不限于 ISO 27001 信息安全管理体系认证、CMMI 成熟度模型集成认证等，相关服务人员需要具备 CISP-PTE/PTS、CISM、OSCP 等专业认证，并通过阿里云内部的安全能力评估与认证流程，确保其服务的专业性与合规性。

2.3.2 测试范围与深度

第三方验证范围覆盖阿里云的全系列产品与服务，从基础设施层（如服务器、网络设备）到平台服务（如数据库服务、容器服务）、再到软件应用层（如 Web 应用、移动应用）。测试内容深入至黑白盒代码审计、网络渗透、逻辑漏洞挖掘等多个维度，确保全方位、无死角的安全验证。

图 3.2.4：外部三方验证

2.4 外部安全生态建设

我们深知只靠阿里云安全团队自己的力量无法保障绝对的安全。唯有阿里云安全团队与白帽社区携手并肩，方能形成有力的安全屏障。广大白帽群体和安全社区，是阿里云在安全道路上寻求突破、弥补短板、拓宽思路的关键支撑。通过鼓励白帽挖掘漏洞，刺激内部红军团队补齐短板，阿里云的安全防线才得以不断提升。

基于上述考虑，阿里云在 2013 年创立了阿里安全响应中心（ASRC），通过高额的赏金激励行业精英白帽，持续不断帮助阿里云发现安全防御中的薄弱环节，全面提升业务整体安全水位。为进一步帮助云上用户提升安全性，继而又在 2015 年创建了先知平台，通过安全众测等形式，方便客户集中高效地发现安全风险。

阿里安全响应中心（ASRC）

阿里安全响应中心（ASRC）针对阿里云及阿里集团其他所有业务的外部风险，通过提供漏洞赏金计划、开展安全众测项目，提前发现潜在的安全风险，避免阿里云业务漏洞被外部恶意黑客利用。

先知平台

先知平台服务于阿里云客户，一方面为客户提供针对企业特定产品的公开或私密的安全众测项目，另一方面通过通用漏洞收集计划，及时感知云上用户大量使用的通用软件产品的 0Day 安全风险，进而将两者转化为安全能力服务客户。

为了更好的服务阿里云及云上用户，ASRC 和先知平台进行了重大升级，整合双方资源，建立了统一的“先知 2.0”品牌，以提升用户覆盖、加速协同效率、拓展服务类目、共享安全技术为宗旨，与时共进，打造新一代互联网安全服务响应平台。

10 余年间，先知累计发布超过 1800 个项目，吸引了全球 30 多个国家的 17000 余名白帽黑客参与其中，一起保障了阿里云上亿用户和企业的安全。阿里云对白帽社群的价值高度认可，作为对安全社区的回馈，发放了超过 8000 多万赏金，单个白帽子最高获得了 500 多万。随着阿里云业务规模不断壮大和业务形态持续多元化，“先知”不仅成为吸纳各安全细分领域顶尖人才的平台，还通过举办众测活动、安全竞赛、行业沙龙等，将最前沿的攻防技术和研究成果融入阿里云的安全体系。在国际上，“先知”也积极参与各类安全行业大会、与 Top 白帽平台合作，获取全球最前沿的安全技术能力。

阿里云安全生态的繁荣，离不开安全社区的蓬勃发展。阿里云致力于共建一个更加开放、互助的安全社区，深化与高校、专业团队的合作，借助线下沙龙、阿里云 CTF 赛事、阿里云安全挑战赛、先知安全社区等多元化活动，培育新兴安全人才，激发技术创新活力，共同筑造安全行业的健康可持续发展之路。

3. 坚守数据主权的数据安全保护

从成立第一天起，“保障客户数据安全”就被阿里云列为最重要的事情。阿里云在数据安全保障上做出以下承诺：

客户掌权：客户完全拥有自身数据主权；未经授权，阿里云除执行客户的服务要求外不会访问、使用或移动客户数据。

先进的数据安全保护技术：云上提供各维度行业领先的安全能力，帮助客户提升数据安全水位。

3.1 客户数据主权保障原则与态度

3.1.1 数据是客户资产，阿里云不会移作他用

阿里云用户对自身数据具有完全的知情权和控制权。用户可自行选择其生产数据部署或存放的云服务可用区地点，未经用户授权 ，阿里云不会移动其生产数据的存储区域。

阿里云设计并实施了严格的租户隔离架构，不同用户之间都默认相互隔离，既看不到彼此的数据，也不会相互影响。

在阿里云的零信任架构中，为防止在内部员工被恶意攻击者钓鱼情况下，恶意攻击者通过内部员工身份开展的数据窃取行为，阿里云建立了严谨的授权机制。通过设置严格的客户数据访问控制策略，确保仅在客户明确授权的必要场景，方可允许内部员工访问客户数据。

3.1.2 夯实数据安全保障体系，全面保障客户数据安全

在云平台自身数据安全保护方面，阿里云严格遵守《数据安全法》《个人信息保护法》《一般数据保护条例》（GDPR）以及行业相关法律法规要求，构建数据安全和个人信息保护管理和技术体系：

建立数据安全管理组织，明确数据安全职责和分工，落实数据安全责任；

建立总纲、规范、指南和流程四级制度体系，覆盖数据采集、流动、存储、使用和销毁的生命周期各个环节，明确数据生命周期安全管理要求，确保数据安全管控措施到位；

建立数据安全风险运营机制，从人员管控、行为防护、安全监测和风险运营开展数据安全管控；

建立数据安全事件应急响应机制，制定数据安全事件分类分级标准，组织开展数据安全应急预案的制定和演练，全面保障数据安全风险治理和处置有序开展。

3.1.3 践行数据合规要求，验证数据主权与数据保护机制

阿里云严格遵循业务运营所在国家和地区的个人信息保护相关法律法规，尊重用户数据的归属权和控制权，严格保障用户隐私安全，未经用户授权，不会访问和披露用户业务数据和隐私信息。

为进一步验证阿里云在数据安全与个人信息保护方面的高标准和专业能力，阿里云通过了多项国内及国际权威机构的认证。阿里云先后通过了中国网络安全审查认证和市场监管大数据中心（CCRC）的数据安全管理认证、韩国互联网与安全局的信息安全管理体系认证（K-ISMS）、新加坡网络安全局的网络安全最高级别认证（Cyber Trustmark）、欧盟独立监督机构 SCOPE Europe 的 EU Cloud Code of Conduct 二级认证（符合 GDPR 要求）、英国标准协会 BSI 颁发的可信数字云最高级别钛金奖及其他全球性的数据安全管理体系认证，包括 ISO/IEC 27001:2022、ISO/IEC 37301:2021、

ISO/IEC 27040:2015、ISO/IEC 27701:2019、ISO/IEC 29151:2017、ISO/IEC 27018:2019、ISO/IEC 27799: 2016、BS 10012:2017 和 TRUSTe 等。阿里云已经获得包括 ISO/IEC 27701：2019、ISO/IEC 29151：2017、ISO/IEC 27018：2014、BS10012：2017 在内的所有关于隐私保护标准认证的“全满贯”。

这些权威的三方认证和审计报告，验证了阿里云在数据获取、传输、存储、处理、销毁过程中的合法合规性。

3.2 客户数据安全保护技术能力

阿里云提供多样的数据安全控制措施，如数据操作审计、加解密、细粒度访问控制策略、可信计算和机密计算、数据本地化存储等，为客户提供全面、完整的数据保护策略选项。

3.2.1 数据操作可审计

操作审计服务（ActionTrail）能够帮助记录用户的云账号资源操作，包括通过阿里云控制台、OpenAPI、开发者工具，记录云上产品和服务的访问和使用行为。用户可以将这些行为事件下载或保存到指定的日志服务 Log store 或 OSS Bucket，然后进行安全分析、资源变更追踪和合规性审计等操作。

阿里云数据安全中心（DSC）在云账号资源操作之外，还提供了面向数据实例内部操作的安全审计能力。例如面向数据库产品，该能力可针对数据库 SQL 注入、风险操作等数据库风险行为进行记录与告警。除云上数据库产品实例外，数据安全中心还可覆盖客户自建数据库实例。通过数据安全中心，可帮助客户记录、分析、追踪数据库安全事件，发现不安全操作并抛出告警，有效降低数据泄密风险，帮助企业满足数据安全保护及合规要求。

3.2.2 全链路数据加解密

数据加密是关键的数据安全保障技术，若数据在传输、存储、计算过程中以明文形式存在，将导致链路上的每一环节都存在数据被窃取的风险。

在数据传输环节，阿里云提供了标准的 TLS 加密传输协议，支持用户通过加密协议与云产品进行交互，从而保证用户请求数据在传输链路中的安全。OSS、全球加速等产品支持用户设定强制传输加密，并支持通过 RAM Policy 设定加密协议版本。

在数据存储环节，阿里云的数据存储类产品提供了可选的数据加密能力，与密钥管理服务（KMS）协同保障静态数据的安全；其中包括可一键开启的磁盘加密，以规避物理磁盘被窃取时可能导致的数据泄露风险，磁盘加密不影响对数据的正常读取使用。也包括覆盖使用链路的数据加密，可确保只有同时具备密文数据访问权限、密钥访问权限时，才可获取明文数据。

云上数据加密可基于 KMS 生成各类强度的密钥，若客户对于自身数据主权具备更高要求，可以使用 BYOK 能力，将自己生成的密钥导入到 KMS、数据类产品中，完成加密操作。同时阿里云还支持客户购买 Cloud HSM 硬件加密机或者使用客户自身拥有的加密机进行外部密钥管理（HYOK），以保障客户对密钥生成、访问的绝对控制权。通过对密钥的细粒度权限管控能力，客户可以将需要重点保护的数据进行加密，并只将密钥的访问权限授予可信的调用方、可信的使用环境，以此来保障自身对这些关键数据的控制力。

3.2.3 细粒度访问控制策略

当数据需要在云上环境进行流程和传输时，为保障客户能够掌控数据的访问权与流动方向，阿里云提供了细粒度的权限管控策略、网络访问控制策略，并在核心数据存储类产品上，提供了更为安全的私网访问通道。

阿里云的权限管控基于 RAM（Resource Access Management）机制，用于帮助客户管理身份和资源访问权限。RAM 机制同时具备基于角色的 RBAC（基于角色的访问控制）和 ABAC（基于属性的访问控制）能力，能够做到资源粒度的最小授权，并且可以为权限施加 Condtion 限制，如只有某特定可信网段来源的请求才允许访问。

除身份权限方面的限制外，对于 ECS、RDS 等资源，阿里云还提供了网络安全组能力，可限制只有特定网段才能访问资源，或限制 ECS 实例对外访问公网资源。以此来支持客户配置细粒度的访问控制策略，保护数据安全。

以 OSS 为例，OSS 提供了最细到 Object 粒度的访问控制策略，并提供私网连接（PrivateLink）通道，以保障 OSS 内的数据，仅可通过私网通信链路，在某个特定 VPC 内访问。

3.2.4 可信计算与机密计算

可信计算与机密计算是保障数据安全的高阶能力，能够保障客户数据主权及数据机密性，客户直接选用对应规格，并完成少量配置即可使用高阶功能，完成自身的数据安全加固。

– 可信计算

可信计算是用于实现云租户计算环境底层高等级安全的主要功能之一。通过虚拟化层面的可信能力 vTPM 作为可信根，构建涵盖系统启动和用户指定应用的信任链并实现远程证明机制，为用户提供了针对环境启动阶段和运行阶段的全方位可信保障。在系统和应用中加入可信验证，能够减少由于使用未知或遭到篡改的系统 / 软件遭到攻击的可能性。

可信计算技术为用户的 ECS 实例提供可验证的完整性，以确保实例未受到启动级或内核级恶意软件或 Rootkit 的侵害。可信实例通过使用 UEFI 安全固件、虚拟可信平台模块（vTPM/vTCM）、远程证明服务，实现实例启动度量和完整性校验，从而保障实例的安全可信。

– 机密计算

机密计算可为客户提供物理级的安全计算环境，以虚拟化 Enclave 为例，阿里云虚拟化 Enclave 在 ECS 实例内部提供一个可信的隔离空间，将合法软件的安全操作封装在一个 Enclave 中，保障客户的代码和数据的机密性与完整性，不受恶意软件的攻击。

阿里云为适配不同企业的不同场景需求，同时支持 Intel® SGX 机密计算技术、Intel® TDX 机密计算技术、海光安全加密虚拟化 CSV（China Secure Virtualization）技术，可供金融、医疗这类对敏感和机密数据有强保护需求的业务选择。

3.2.5 公共云形态下的敏感数据本地存储

对于敏感行业，既需要遵守数据本地机房存储的监管合规要求，同时又希望使用标准弹性的公共云产品。阿里云为满足此类业务需要，提供了专属区域、云盒两种形态，分别支持将小型化 Region、小型化 AZ 可用区部署到客户机房。

阿里云专属区域是阿里云公共云的小型化部署形态，提供面向客户的专属服务场景。专属区域可以在阿里云数据中心的独立物理区域或客户数据中心构建，提供与阿里云公共云相同的 IaaS、PaaS 云产品，并通过云服务方式为客户提供独占资源和统一运维服务，满足数据隔离和合规要求。

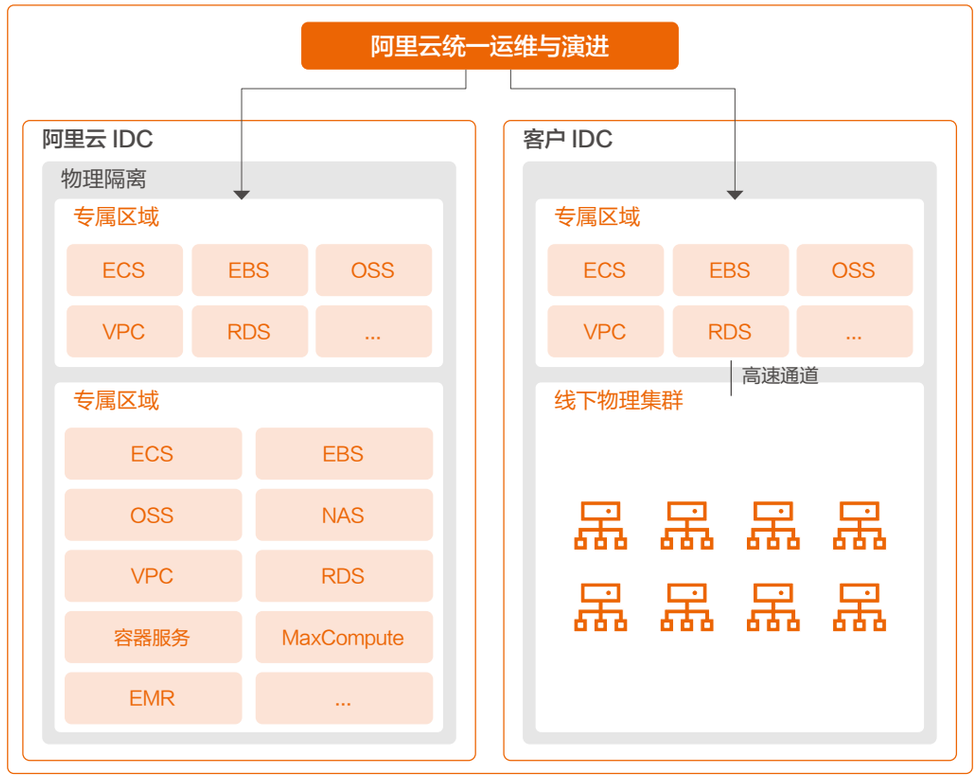


图 3.3.1：专属区域

云盒（CloudBox）是将阿里云公共云（下文也称为中心云，以突出与云盒的位置关系）的计算、存储、网络等技术以软硬一体方式部署到客户本地机房，客户可以根据需求选购具体的云产品，满足数据安全、数据本地处理、低延时等业务需求的全托管云服务。云盒通过上云连接与中心云相连，复用中心云管控基础设施和远程运维能力，允许云盒与中心云中的用户 VPC 互通。

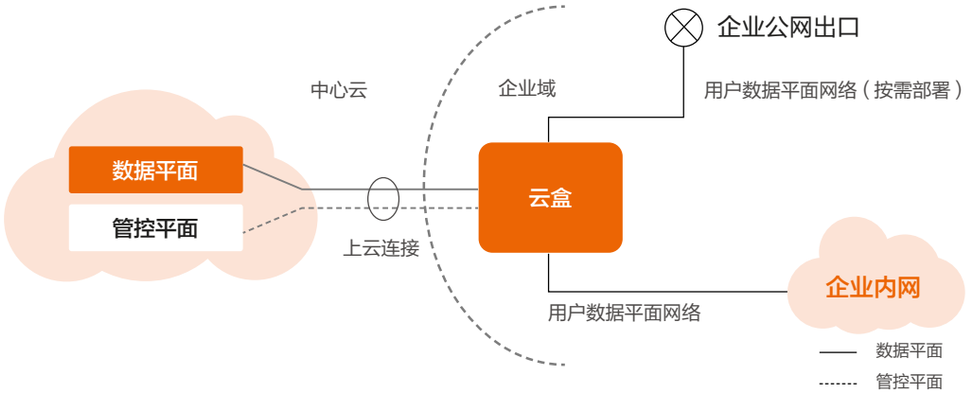


图 3.3.2：云盒

通过这两种形态，客户可将关键必要的数据保留在本地，通过物理层隔离的方式符合合规性，同时又可以在合规的前提下，便捷地与云上资源互访，兼顾便捷性与合规性。

3.2.6 从数据风险出发的数据安全解决方案

阿里云数据安全中心，可为客户提供一体化以数据为中心、风险为导向的数据风险全生命周期的安全解决方案。在满足等保 2.0 安全审计及个人信息保护要求的基础上，获取用户明确授权后，为客户提供敏感数据保护和数据库审计服务，提供敏感的数据资产安全的监控保障。具备敏感数据识别、细粒度数据审计、数据脱敏 / 列加密、数据泄露检测与防护四大功能。

图 3.3.3：阿里云数据安全治理架构图

- **敏感数据识别：**从海量数据中发现和锁定保护对象，通过内置算法规则和自定义敏感数据识别规则，对其存储的数据库类型数据以及非数据库类型文件进行整体扫描、分类、分级，并根据结果做进一步的安全防护，如细粒度访问控制、加密保存等。
- **细粒度数据审计：**细粒度行为审计追溯的能力，可审计用户终端信息、使用工具、数据信息、返回结果等详细信息，全场景还原用户行为轨迹，有效追踪溯源数据的访问行为。

- **数据脱敏 / 列加密：**支持通过灵活多样的内置或自定义脱敏算法或列加密，实现生产类敏感数据脱敏到开发测试等非生产环境使用的场景，并确保脱敏 / 加密后的数据保真可用。
- **数据泄露检测与防护：**通过智能化检测模型分析内外账号对敏感文件的访问行为，实现对敏感数据访问的异常检测，同时为数据安全管理团队提供相关告警。

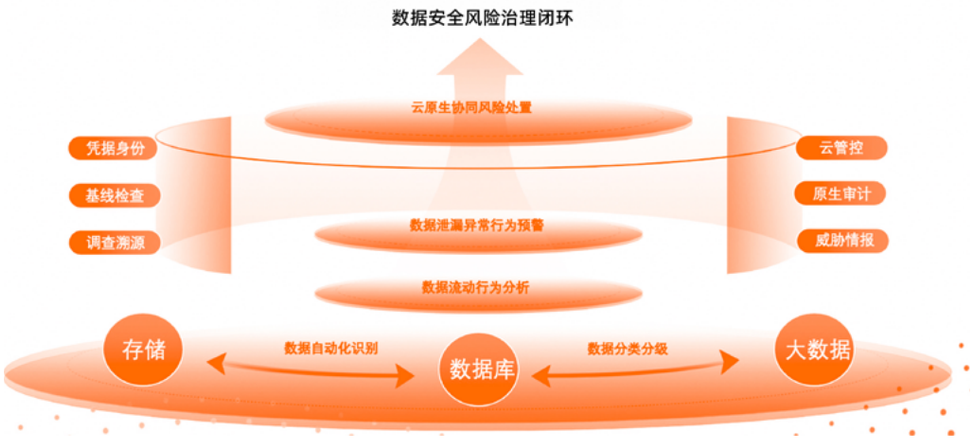


图 3.3.4：阿里云数据安全风险治理架构图

4. 全链路身份管控与精细化授权

随着数智化发展的深入，企业需维护大量的资产和数据。这导致访问和管理这些资产和数据的身份权限体系变得极其复杂。

阿里云提供了细粒度的权限管理能力以及完整的身份、凭证保护方案，覆盖了阿里云全链路的产品品类，以满足各种场景下、不同体量的客户对数据资产访问控制策略的需求，从而保护其数据资产的安全性。

同时云平台具备标准性、可扩展性，同时云平台具备标准性、可扩展性，能够帮助企业将云上身份与企业内部身份关联起来，构成一张身份网络。在提升企业安全效率的同时，又减少了风险暴露面。在提升企业安全效率的同时，又减少了风险暴露面。

4.1 云上身份与细粒度权限管理

阿里云的身份体系中，云账号为云上资源的载体，默认拥有账号内资源的所有管控权限，同时用户可以通过为员工和程序应用创建 RAM 用户、RAM 角色身份，并分配不同的权限，来满足不同场景的使用需要。身份与权限体系相当于云上资源的门锁，若门锁不安全，云上资源的安全性也无从谈起。

主账号及 RAM 用户支持通过用户名密码登录阿里云管理控制台，为避免账号密码泄露引入安全风险，用户可以对账号启用多重身份验证（MFA，Multi-factor Authentication），通过多因素核身的方式（如输入短信验证码），来帮助客户控制账号密码泄露的风险。拥有 RAM 访问控制权限的管理员还可以配置 RAM 用户的密码策略、MFA 验证规则，以及通过最小化权限授权，来进一步控制用户密码被盗带来的风险。

为进一步控制云上账号被盗后产生的风险，阿里云将陆续为所有 RAM 用户开启登录时强制进行 MFA 多因素认证，有效地阻止用户被盗用登录。当有迹象表明用户控制台密码存在泄露风险时，阿里云会对 RAM 用户进行临时限制登录保护，客户需要重置 RAM 用户密码后才能重新登录使用。

RAM 用户和 RAM 角色的权限，可以通过访问控制 RAM 来进行限制。访问控制 RAM（Resource Access Management）是阿里云提供的管理用户身份与资源访问权限的服务。客户可以使用 RAM 访问控制产品创建代表员工或应用程序的 RAM 用户，并可以控制这些 RAM 用户对资源的操作权限。阿里云支持客户为不同场景、不同员工创建不同的 RAM 用户，按需为用户分配最小权限，从而降低企业的信息安全风险。RAM 机制支持用户组功能，以支持对职责相同的多个 RAM 用户进行批量管理。

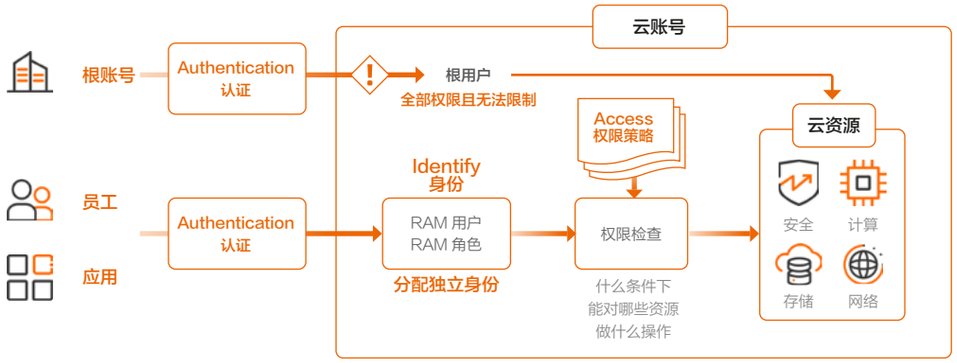


图 3.4.1：用户可通过 RAM 服务管理资源访问权限

RAM 机制同时具备 RBAC 和 ABAC 能力，RBAC 支持客户抽象出一些角色出来（比如运维角色），不需要再给每一个 User 来配置权限。ABAC 支持客户做到资源粒度的最小授权，并且可以为权限施加条件限制，如只有某特定可信网段来源的请求才允许访问。

在面对大量、繁杂的资源时，为了进一步提升客户细粒度权限管理能力，满足各场景访问控制策略需求，阿里云提供了 ResourceGroup 资源组和 Tag 标签能力。ResourceGroup 资源组适用于常规的资源分组管理场景，例如，企业将某一主账号下的资源，分配给不同的项目组。Tag 标签能力则可以实现“多对多”的复杂管控需求，也即一个资源可打多个标签，如资源同时具备项目标签和环境标签，通过标签的组合，便可以定位到 A 项目的生产环境对应的资源。

为了帮助客户达到“最小授权”的目的，阿里云提供了访问分析（Access Analyzer）服务，旨在帮助企业有效管理和持续检测企业云上身份的权限及其使用情况，识别过度授权的身份，并推荐最佳实践方案，帮助客户践行“最小授权”的原则。Access Analyzer 服务可以帮助分析企业和账号内的所有 RAM 用户和 RAM 角色，识别过度授予但未使用的权限，帮助企业优化权限的分配。Access Analyzer 还可以分析出企业内拥有高风险权限的身份，帮助企业集中管理特权身份，加强特权身份的安全水位，降低企业安全风险。

基于上述账号风控及细粒度的权限管理能力，用户可以根据自身使用场景构建合适的身份与权限管控策略。

4.2 云上凭证保护

凭证是身份的证明，一旦泄露，将可能导致数据泄露、服务器被入侵等后果。凭证分为长期有效的访问密钥（AccessKey，后文统一称作 AK）与短期有效的 STS Token。

图 3.4.2：AK 与 STS Token

阿里云提供了一系列保护机制，来帮助客户治理凭证泄露风险。

使用 STS Token 代替永久 AK

永久 AK 由于长期有效，泄露后会对云资源安全产生持续威胁。而 STS Token 到期后将自动失效，无需定期轮换。因此推荐用户使用 STS Token 作为程序访问凭证访问云资源，替代风险更高的永久 AK。

当客户的应用程序部署在阿里云 ECS 实例上，则可以通过“ECS 实例角色”功能，让 ECS 实例扮演具有某些权限的角色，获取到 STS Token 访问阿里云 API。ECS 实例角色功能允许客户将一个角色关联到 ECS 实例，在 ECS 实例内部基于 STS Token 临时凭证访问其他云产品的 API。出于安全性考虑，使用该功能时应当开启“仅加固模式”。

当客户的应用程序部署在阿里云 ACK 容器集群上，则可以基于 RRSA（RAM Roles for Service Accounts）功能，在容器集群内实现应用隔离的 RAM 角色功能，各个应用可以扮演独立的 RAM 角色，访问阿里云 API。基于 RRSA 功能，客户可以在集群内实现 Pod 级别隔离的应用关联 RAM 角色功能。各个应用可以扮演独立的 RAM 角色，并使用获取的临时凭证访问云资源，从而实现应用 RAM 权限最小化以及无永久 AK 访问阿里云 API，避免 AK 泄露。

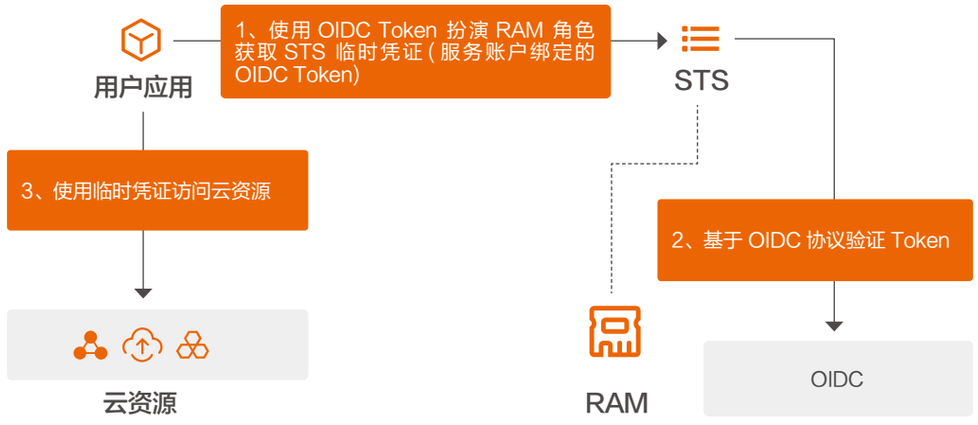


图 3.4.3：用户使用 STS Token 访问云资源

对于凭证方面的保护，用户可以通过使用 STS Token 代替永久 AK，实现“无永久 AK”的效果，根本性解决云上凭证泄露问题。也可以将凭证托管到 KMS 中，以控制泄露风险，便于凭证泄露后到快速轮转。

AK 凭证加密托管

尽管我们在先前的讨论中提倡采用 STS Token 作为授权手段，但在某些独特情境下，使用 AK 或许仍然在所难免。在此类情况下，云上客户可以使用 KMS 密钥管理服务管理及使用 RAM 凭据，以此来确保敏感凭证的安全保管。在客户授予 KMS 管理 RAM 用户 AK 的权限后，即可使用 KMS 提供的 RAM 凭据插件、阿里云 SDK 从 KMS 获取 RAM 凭据值并缓存在应用程序的内存中，然后向云产品发起请求。

选择将凭证托管到 KMS 上，而不是硬编码到代码中，可以规避代码传播过程中产生的泄露风险。并且一旦某把凭证泄露，可通过 KMS 立刻进行轮转。

AK 凭证安全审计

同时，阿里云也为客户提供了 AK 审计功能。通过该功能，客户可以对账号下的 AK 使用情况进行深度审查和管理。AK 审计用于查询 AK 的基本信息、访问的云服务及相关 IP 地址和资源，帮助客户追溯 AK 使用信息，以便快速应对 AK 泄露等异常事件，或者为轮换 AK 提供决策参考。

AK 泄露风控

长期不使用的访问凭据容易发生泄露，且闲置时间越长，暴露风险越高。为帮助控制 AK 泄露后产生的实际损失，若识别到 AK 泄露，阿里云会对该 AK 进行限制性保护，泄露期间访问阿里云指定高危 API 时会提示报错，防止风险进一步扩大。并会及时通知账号管理员，关注 AK 泄露风险。

同时，将针对长期未登录的 RAM 用户自动禁用控制台登录，针对长期未使用的 AccessKey 自动禁用使用。

4.3 企业多账号管理

当云上企业使用单账号承载云上资源时，企业内不同业务之间难以实现强隔离，且人员和权限管理复杂度极高。所以，企业通常会为每个独立的业务单元申请独立的云账号，实现安全隔离。

对于持有大量云账号的中大型组织，阿里云提供了资源目录（Resource Directory）产品，支持企业管理员将企业的众多账号按业务的层级结构有序地组织起来，形成组织的资源结构目录，进而以组织视角集中管理身份权限、安全、合规、策略等资源，满足企业资源在安全、审计及合规方面的管控需要。通过资源目录产品，企业可以利用账号作为逻辑边界提升资源安全状态，更清晰地管理用户对不同环境的访问权限。

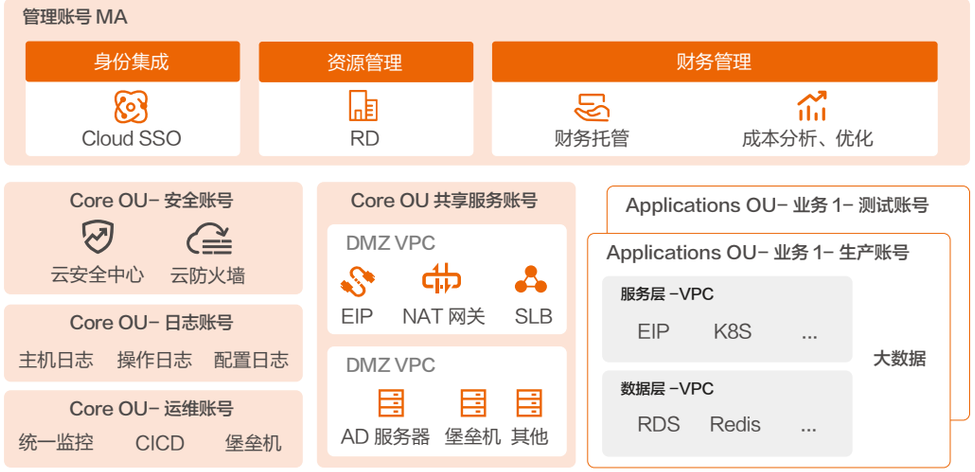


图 3.4.4：多账号环境最佳实践

“如何保障众多云账号遵守公司的安全合规基线？”是众多中大型组织云上资源管控的痛点。为了支持中大型客户解决此类痛点，阿里云基于资源目录产品提供了 Control Policy，可限制多云账号内的权限边界，以确保企业安全基线与合规性。

Control Policy 并不执行权限的授予，而是在整个组织树下，规划约定权限限制。即使云账号管理员为某个子用户分配了敏感的权限，该子用户由于受到资源目录管控策略的限制，也仍无法进行危险的操作。

举例来说，当安全合规管控团队希望禁止访问者与 OSS 产品间进行明文交互，要求强制使用 TLS 链路加密时，可以通过 Control Policy 进行限制。

```
{
  “Effect”: “Deny”, // 当权限满足该策略描述时，则拒绝访问
  “Action”: “oss:*”, // 针对 OSS 产品的所有 OpenAPI
  “Resource”: “*”,
  “Condition”: {
    “Bool”: {
      “acs:SecureTransport”: [
        “false” // 不使用 TLS 链路加密
      ]
    }
  }
}
```

Control Policy 还支持其它类似的场景，如禁止 ECS 开放公网、强制加密存储、禁止修改 ECS 镜像分享权限、禁止关闭 ActionTrail 日志审计。企业可以基于 Control Policy 的能力，用 RAM 的语法灵活地设置企业权限基线，以满足企业安全与合规管控需要。

4.4 身份关联与映射

企业内部由于内部管理需要，或考虑到云下历史架构，可能需要保留其它身份与权限管理体系，或建设专属企业内部的身份与权限管理体系，如传统的 Windows 域身份权限体系。企业自有身份体系与云上身份权限体系的映射，通过自有身份体系实现单点登录，以此来保障企业身份、权限系统的简洁性，同时降低密码泄露风险。

阿里云支持云上身份与企业内部身份权限管理机制关联，员工无需持有云上用户身份的登录密码，直接通过内部身份权限管理机制就能免密登录到云上控制台，这一关联机制能够有效控制多套账号密码管理混乱所导致的安全隐患。同时也可以更高效地解决员工转岗、离职所带来的云上账号转交及注销，大大降低了企业身份权限管理的复杂度。

单点登录（SSO）是一种身份验证解决方案，可让用户通过一次性用户身份验证登录多个应用程序和网站。SSO 是云上身份与企业自建身份权限体系互联的基本能力，基于标准的 SAML2.0 或 OIDC 身份协议，可以支持对接企业自建 IdP（身份提供商），使用户在通过企业内部账号认证后，就可以直接登录到云控制台的某个 RAM 用户或 RAM 角色身份。

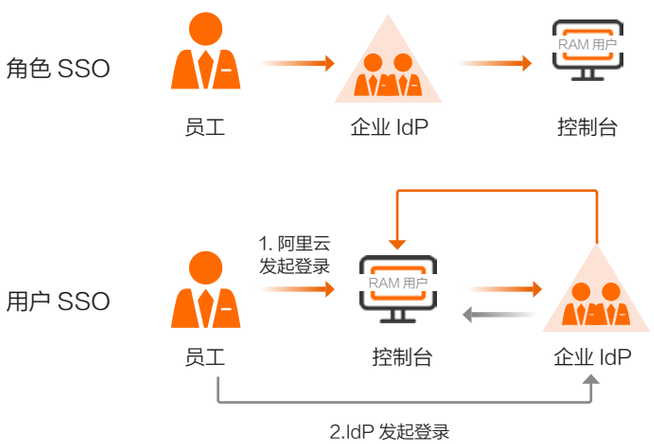


图 3.4.5： SSO 单点登录

如上一章节所述，中大型企业往往需要持有大量的云账号，这些云账号可以通过资源目录产品来进行统一管理。对于身份关联工作，阿里云基于资源目录产品，提供了云 SSO 能力，能够将企业中所有的身份在云 SSO 中进行统一的管理，支持多账号的 SSO 分配与管理，通过配置模版能力，能够大大加速配置速度，控制配置成本。

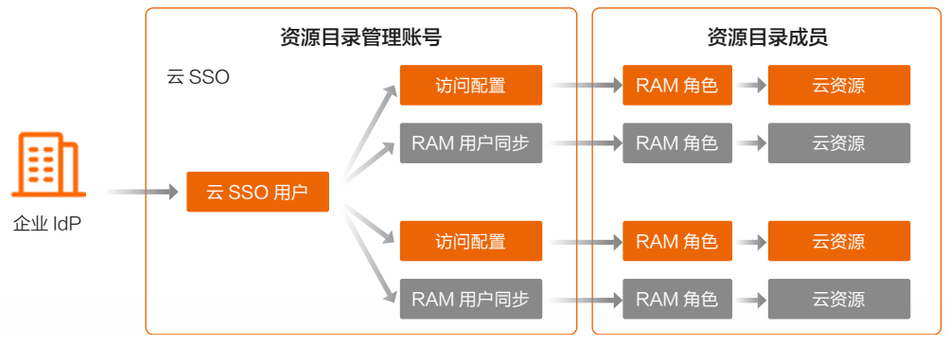


图 3.4.6：云 SSO– 多账号身份权限管理

通过上述一系列工具及能力，可以将云上身份与企业自建身份体系打通，便于企业级大规模身份与权限管理，帮助企业保护云上资源的安全。

5. 安全防护能力高效弹性可扩展

面对日益严峻的攻防态势和日益复杂化的系统架构，企业需要实施多方位的安全防护，如在网络层到应用层需要配置 DDoS 防护、云防火墙、WAF、RASP 等安全产品，如果这些安全防护能力完全由客户自建，将会产生大量的资源投入成本及时间成本。

在数智化转型趋势中，企业的敏态需求日益增长，云平台能够在确保这些需求得到满足的同时，助力业务实现快速的弹性伸缩与扩展。在安全领域，阿里云也致力于将安全防护能力融入到云产品中，以“原生安全”的理念，为客户提供内生、默认、可配置、可弹性伸缩、可扩展、生态友好的安全防护能力。

5.1 产品原生安全防护能力

阿里云希望所有将系统部署在云上的企业，都能够享有尽量高的默认安全水位，因此将安全能力默认融入到了产品设计中，为企业提供原生的安全防护。

- **数据保护层面，阿里云提供了默认的传输加密与存储加密**

  传输加密是指云产品为用户访问（包括读取和上传）数据提供了 SSL/TLS 协议来保证数据传输的安全。例如，当用户通过阿里云控制台操作时，控制台会使用 HTTPS 协议进行数据传输。所有的阿里云产品都为客户提供了支持 HTTPS 的 API 访问点，以满足敏感数据的加密传输需求。对象存储 OSS、全球加速产品还提供了 TLS 版本控制能力，以满足客户多样化的安全合规需求。

  阿里云为用户提供云产品落盘存储加密能力，并统一使用阿里云密钥管理服务（Key Management Service，简称 KMS）进行密钥管理。云上关键存储产品，如云盘、数据库 RDS、对象存储 OSS，均实现了一键加密能力，客户可免费一键开启，以满足敏感数据的磁盘加密存储需求。

- **网络安全层面，阿里云提供了默认额度的流量攻击防护额度**

  阿里云云安全中心提供了免费版的漏洞检测、安全告警和基线检查服务，还帮助客户收集并呈现安全日志和云上资产指纹。客户可以在 ECS 管理控制台的概览页面或者云安全中心控制台查看相关安全信息。

  客户创建弹性公网 IP（EIP，Elastic IP Address）资源时，阿里云将默认开启 DDoS 基础防护能力，免费提供最大 5 Gbps 的基础 DDoS 防护能力，以抵御小规模攻击。

- **访问控制层面，阿里云提供了默认最小够用的产品配置**

  为防止企业无意间配置错误的访问控制策略，导致严重的数据安全隐患，阿里云在产品中提供了默认最小够用的产品配置，并提供充分的风险提醒。例如，OSS Bucket 配置了“阻止公网访问”，防止使用者误操作，导致敏感数据非预期对外暴露。

图 3.5.1：OSS Bucket 管理

- **应用层防护层面，阿里云提供了可选的安全防御与扫描能力**

  应用实时监控服务是阿里云的一款应用性能管理（APM）监控产品，整合了 RASP（Runtime Application Self-Protection）防护能力。当企业有代码层入侵拦截的需求时，可以通过 ARMS 控制台一键接入应用安全，接入后重启目标应用对应的实例即可，无需对任何应用代码进行修改。

云效作为阿里云提供的 DevOps SaaS 产品，在代码检测环节提供了安全扫描能力，客户可按需使用该功能，提升应用代码的安全质量。

图 3.5.2：云效的安全扫描功能

阿里云还将在更多的产品上，推动更多的原生安全设计落地，保障企业的安全水位。

5.2 按需使用与弹性伸缩

企业所需要保护的资产规模、需要实施的具体安全防护级别会动态变化。考虑到企业的快速迭代、扩展需求，阿里云提供了按需使用、一键接入、按需扩展的安全能力，旨在帮助企业同步实施安全防护策略。

高昂的接入成本也是影响安全防护实施敏捷性的一个关键因素，阿里云通过一系列产品改造与建设，帮助客户实现低成本、高质量的接入体验。

以阿里云的流量防护产品为例：

图 3.5.3：阿里云流量防护产品的按需使用与弹性扩展

在企业原本的接入流程中，会遇到诸多障碍，影响抗 D 能力的有效接入：

- **配置繁琐：**企业业务有大量 IP 资产和端口资产，代理模式防护部署需要维护多对多转发配置。
- **协同链路长：**代理模式防护部署涉及串联部署、DNS 接入需要企业内部运维流程协同。
- **架构改造复杂：**代理模式防护部署需要修改入口到高防 IP，会改变企业的业务流量架构。

为了帮助企业快速按需接入抗 D 能力，阿里云提供了“原生接入”方式，可抵挡高达数百 Gb/s 级别攻击，一键接入，不需要侵入业务。

5.3 云上安全生态共享

安全不是闭门造车，云上企业众多，场景千变万化。为促进云上安全生态，阿里云通过云市场形式引入了众多安全产品，为客户提供了丰富的选择，并通过优化产品设计，便于三方安全产品在云基础产品上提供更优质的服务。

阿里云云市场是云上的软件交易及交付平台，通过赋能生态伙伴，引入三方生态产品，以实现客户、阿里云、生态伙伴之间的共赢。截至 2024 年 8 月，阿里云云市场已引入包含国内外主流安全厂商的 358 款三方安全产品，为企业的安全解决方案提供更多的选择。

图 3.5.4：云市场三方安全产品

除此之外，阿里云在自身云产品设计上，为生态集成留出了接入扩展点，为三方安全设备提供更稳定、可靠、安全的接入体验。

网关型负载均衡（Gateway Load Balancer，GWLB）是阿里云提供的一种负载均衡服务，专为网络虚拟设备设计，旨在简化在阿里云上部署和管理第三方网络虚拟设备（如第三方防火墙、DPI 设备等）的过程。

GWLB 与阿里云云市场上的众多安全和网络供应商产品集成，如 FortiGate、Palo Alto Networks 等主流安全厂商，使得这些设备可以在阿里云上高效部署和管理，轻松实现云原生安全和网络策略。GWLB 为这些设备提供了高可用性和扩展性、灵活的流量分配、基于 Private Link 的私网安全数据传输能力、易用的配置与管理能力。另外，GWLB 还支持统一的安全策略，使用户在复杂的网络结构下，同时保持高性能及高安全性。

在拥抱安全生态的路上，阿里云还将继续砥砺前行，未来会引入更多的三方企业共同加入到云上安全生态的大市场中，共同为用户的安全水位保障添砖加瓦。

云上安全重要支柱 阿里云安全白皮书

6. 面向线上威胁的快速响应与恢复

在严峻的攻防态势下，综合业务灵活性、成本的考虑，很难做到绝对安全，但是需要追求风险可控的安全。因此必须要考虑线上出现风险后，如何动态地控制风险。阿里云为了帮助客户控制风险，建设了一体化的安全运营能力，帮助客户在极端威胁下快速感知风险、响应风险、恢复数据及服务。

安全对抗不是单个系统、单个组织、单个国家的事情，只有将各方关联起来，进行联动防御，才能取得更好的效果。为履行数字基础设施的社会责任，阿里云还推出一系列机制，压制黑灰产的云上行动，为社会的安全稳定做出贡献。

6.1 安全运营能力一体化

软件实施的疏漏或云资源的不当配置会引发线上安全漏洞，外部恶意攻击者便有机会利用这些漏洞侵入系统，进行数据盗窃、植入勒索软件等非法活动，严重威胁企业信息安全。漏洞类型错综复杂，而攻击手法又变幻莫测，成为了当前企业在安全领域中的一大严峻挑战。

“如何将线上威胁检测能力全面覆盖企业资产”“如何精准识别具体风险点”“如何快速、稳定、无损地完成风险治理”，这是对企业安全响应能力的严峻挑战。

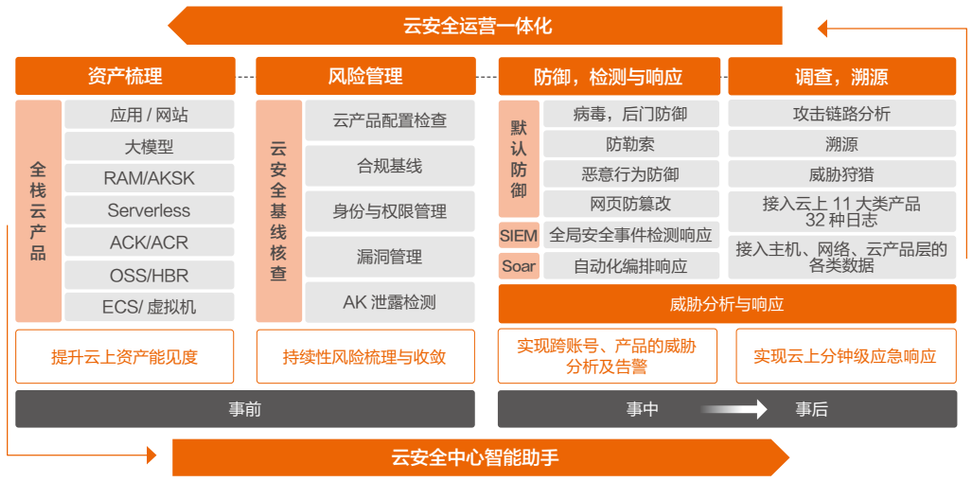


图 3.6.1：一体化安全运营能力体系

阿里云云安全中心从事前、事中、事后全流程的角度出发，以资产数据、风险识别、风险治理为重点建设方向，建设了一体化的安全运营能力体系。为企业克服上述挑战，提供了强大的能力支持。

6.1.1 全面可视的资产梳理

基于阿里云标准化的资产定义、API，阿里云可以帮助客户自动化地生成云上业务的架构图。客户可通过该架构图分析云上应用的互联网暴露情况、云内的 VPC 内部的流量、云服务的调用关系。解决了风险管理中的“影子资产”痛点问题，为下一步的风险管理、检测与响应、安全加固打下坚实的基础。

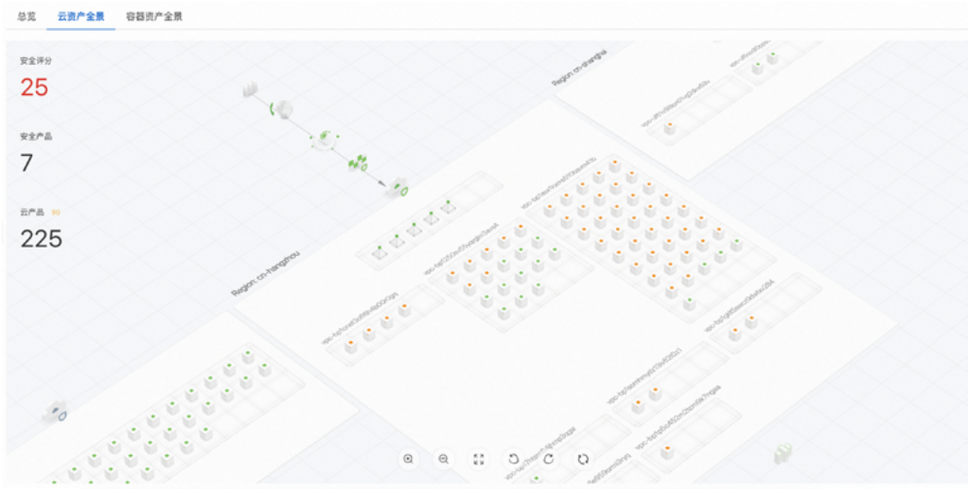


图 3.6.2：可视化资产梳理

注 *： 影子资产，指那些在资产统计中没有明确列出，但对机构的风险水平有一定影响的资产。

6.1.2 及时联动的威胁情报分析

面对严峻的安全威胁，阿里云建设了一系列安全能力，能够帮助客户集中处理来自多云环境、多账户和多产品的告警和日志数据，并从中分析出潜在威胁，通过 SOAR（威胁分析与响应服务响应编排）完成自动化、流程化安全响应。

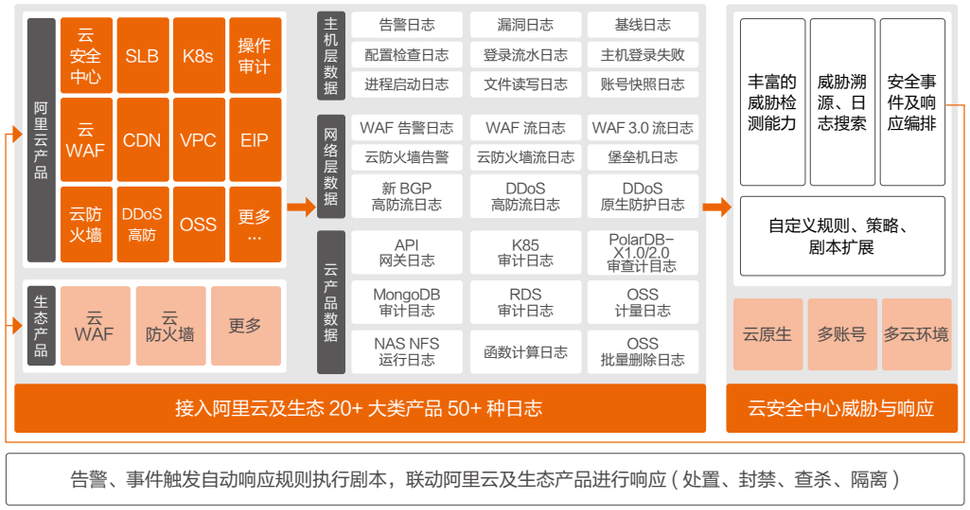


图 3.6.3：威胁情报联动分析与响应

– 威胁情报共享

威胁情报不只需要关注自持资源的常规安全威胁，还需要能够结合全球威胁情报，进行跨产品的综合评估。客户可在阿里云获得最新的安全情报，并通过云上安全产品，即时具备检测与防护能力。

为面向社会共享威胁情报，阿里云建设了公开的 AVD 漏洞库，将全球开源安全漏洞情报及其分析结果向社会公开分享。针对重大安全缺陷，会及时将检测规则集成到云安全中心，并推动告警信息到客户侧，帮助客户更好地应对安全威胁。

– 联动防御威胁

阿里云还具备跨产品联动防御、防御策略辐射多客户的能力。举例说明，众多客户均授权了云安全中心来分析日志、执行防御动作，当其中某客户被新型勒索病毒入侵后，阿里云能够从该用户主机行为日志中识别该病毒，并拦截其进一步横向移动。这一入侵特征在经过分析后，会进入到安全策略库中，其它客户也可以基于云安全中心的能力，快速识别此类新型勒索病毒。该策略也会同步到云防火墙规则中，能够通过云防火墙标记、告警、拦截连向病毒控制中心的请求。通过这样的联动防御，可以大大提升云上众多客户的安全威胁防御能力。

6.1.3 高效的风险识别

基于全面的资产梳理，阿里云利用其技术领先的安全扫描与巡检能力，建立了一套高效的风险识别与治理体系，能够自动帮助客户定期检查云资源，包括识别互联网暴露风险、配置风险、漏洞风险及身份权限管理风险。另外还通过无代理技术等方式，规避了风险识别阶段的稳定性风险。

在风险识别和分析过程中，阿里云不仅仅依赖单一信息来源，而是整合多方面的信息进行综合分析。当存在漏洞的服务被暴露于互联网上时，该风险的预警级别会因为同时满足“存在漏洞”和“对外开放于互联网”这两个条件而显著提高，这样有助于客户科学合理地确定风险治理的优先顺序。

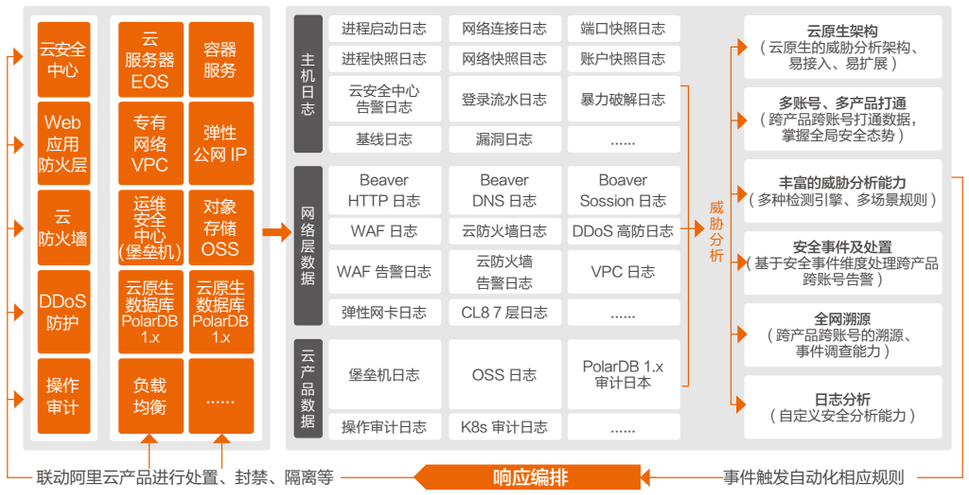


图 3.6.4：云上威胁日志联合分析

6.1.4 精准、稳定的风险治理与业务恢复

在基础安全领域，安全专家们面临着诸多日常而琐碎的简易任务，诸如进行安全审查、处理木马与挖矿软件等事宜。这些繁杂的工作大幅度占用着高级安全专家的时间和精力。因此，那些对于企业内部环境了如指掌、熟练掌握竞争对手信息、并能深入分析攻击者行为模式的专家们，难以腾出更多资源聚焦于至关重要的网络攻防对抗及深度安全研究领域。

基于自动化响应编排 SOAR 能力，可以将安全事件运营自动化、流程化，从而提升安全响应速度。自动化编排系统将安全专家从日常繁重琐碎的工作中解放出来，集中精力应对真正需要处理的安全事件。自动化剧本也可积累安全运营的经验，将人员的经验转化为可解释、可执行的自动化剧本沉淀在企业内，更利于经验的传承。响应编排 SOAR 能够以比人工快得多的速度对大量的攻击告警事件和其他数据进行初步处理，并从中过滤出真正需要人员关注的重点事件，以进一步跟踪处置。

响应编排 SOAR 能力适用于安全运营过程中的调查、检测、响应、溯源、经验积累等各个环节，并不限于事件响应。自动化剧本支持对安全事件进行信息富调查、联动处置等流程，减少重复性劳动，提升安全事件的平均响应时效。响应编排 SOAR 可以定期执行任务剧本，可以设定定期运行巡检任务。人工运行剧本可以按需手动执行特定的任务。企业可通过响应编排 SOAR 的各种安全组件，调用云防火墙、云 WAF、主机安全以及本地威胁情报等各种安全设备的安全能力，进行调查、分析、处置等动作。云安全中心支持一键修复能力，能够自动修复云资源错误配置、账号身份权限错误配置等问题。通过这一系列机制和能力，云上客户可实现人与工具、工具与工具之间的有效协作，将安全设备作为一个完整的整体，可以节约人效 120 倍，防御效果提升 10 倍以上。

除响应速度的提升以外，阿里云提供了一系列能力支持客户进行风险行为拦截。如支持安装 RASP 工具来保障业务“带洞运行”时的基本安全水位，动态无损地防御恶意行为；统一的 one-agent 防护架构，还可以通过日志与流量结合分析，发现恶意攻击行为，并自动化拦截恶意命令。

遭遇攻击后，迅速恢复业务运作十分重要。云备份（Cloud Backup，原混合云备份 HBR）作为阿里云统一灾备平台，是一种简单易用、敏捷高效、安全可靠的公共云数据管理服务，可以为阿里云 ECS 、RDS 数据库等敏感资料，提供备份、容灾保护以及策略化归档管理能力。客户可以针对敏感资产，开启对应产品的自动备份功能，一旦被入侵或蠕虫攻击，立刻恢复正常业务运行。

6.1.5 专业的安全服务

阿里云提供了完整的方案，帮助企业解决不同场景下的安全专家资源不足的困境。

在日常场景下，阿里云提供了渗透测试服务，以攻击者思维，模拟黑客对业务系统进行全面深入的安全测试，帮助企业挖掘出正常业务流程中的安全缺陷和漏洞，助力企业先于黑客发现安全风险，防患于未然。

图 3.6.5：阿里云渗透测试服务

同时，阿里云可支持企业组织与协调红蓝对抗，由蓝军负责发起攻击、红军负责内部防御，通过对抗的形式深入挖掘企业内部的安全风险。

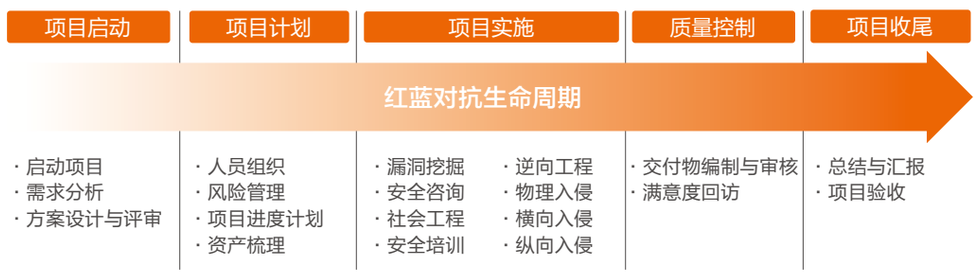


图 3.6.6：红蓝对抗项目

针对重点业务的重保时期，可采购阿里云的“重保护航服务”，由专人在特定时间段，提供 7*24 的全方位守护。通过重要时期安全保障运营服务，开展梳理筹备、摸底评估、布防加固、模拟演练、值守保障、整改优化等一系列安全工作，能够系统化提升企业整体的安全防护监测、应急响应、分析溯源能力。

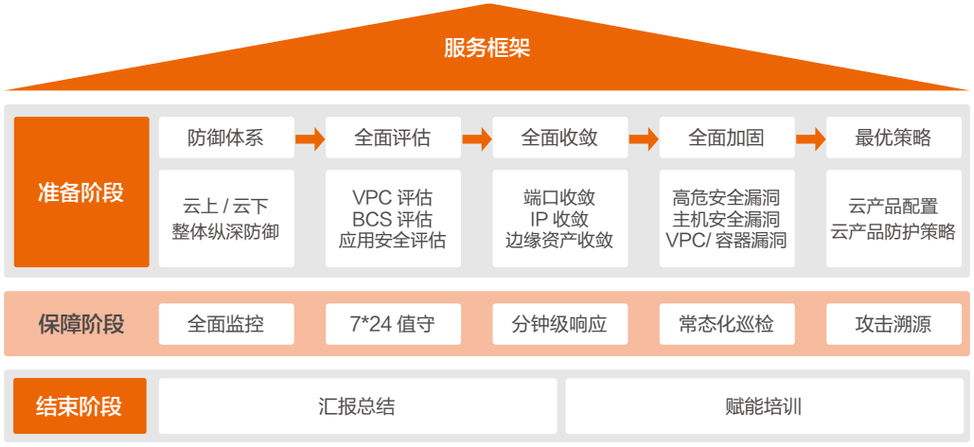


图 3.6.7：重保护航服务

阿里云在安全服务领域具备深厚的积累与丰富的实践经验，曾承担过 2023 杭州亚运会、2024 巴黎奥运会等重大国际体育赛事的安全保障工作，并成功保障 0 安全事故。

6.2 场景演练：防勒索病毒

借助比特币等数字货币的匿名性，勒索攻击在近年来快速兴起，给企业和个人带来了严重的威胁。越来越多的勒索病毒集成了丰富的攻击模块，在业务场景复杂多样的背景下，企业常因口令管理、访问控制等原因而遭受勒索病毒的攻击。勒索病毒会严重影响用户业务，带来严重的数据泄露、业务中断、经济损失，为此阿里云提供了完整的防勒索解决方案。

- **服务器安全加固：**支持服务器漏洞、弱口令的检测及一键修复，协助用户做好服务器的安全加固，避免用户服务器被入侵。

- **勒索病毒查杀：**支持对大量已知勒索病毒的实时防御，在企业主机资源被病毒感染的第一时间进行拦截，避免文件被加密勒索。
- **诱饵目录：**针对新型未知的勒索病毒，通过放置诱饵的方式一旦识别异常加密会立刻拦截同时触发告警，通知用户进行防御。
- **关键文件备份：**和文件备份服务合作，定期对指定文件备份，在文件被加密时能通过文件恢复的方式找回，做到万无一失。

基于上述一体化的安全运营能力，云上客户可高效地发现、响应勒索攻击事件，并快速恢复业务系统。

6.3 联合对抗黑灰产

阿里云作为基础设施提供商，正在积极承担社会责任，为云上租户提供多种产品能力和解决方案，从而帮助租户应对黑灰产对云上资源的威胁。

除网络攻防领域的对抗外，阿里云也在响应国家的相关法规要求，与监管部门紧密配合，建立了一套对云上黑灰产团伙的联合压制措施，全力守护一个健康、有序、安全的云环境。

在“云上安全共同体”的理念引导下，阿里云还将持续投入对黑灰产攻击态势的研究工作，持续优化安全解决方案与产品能力，为云上租户着想，保障云环境的安全与稳定，也为社会的稳定运行贡献一份力量。

7. 面向攻击的安全高可用

随着攻击态势的加剧和攻击规模的扩大，部分攻击已威胁到云服务的可用性，而云服务的可用性直接关系到用户数据的完整性和可用性。具体而言，特定类型和规模的攻击能够严重地破坏流量通道、业务集群乃至机房的物理基础设施，这不仅威胁到业务系统的持续运行能力（即数据可用性受到威胁），还极易导致数据在传输、存储或处理过程中受损或丢失，导致数据的完整性受到破坏，给用户带来难以估量的损失。

长期以来，阿里云持续开展着系统化的安全高可用架构设计，并进行相关的能力和机制建设工作，以守护用户数据完整性与可用性。其目标是构建一个既安全又高度可用的云环境以确保用户数据在面对攻击威胁时始终保持安全可用的状态，并随时供用户调用。

7.1 面向攻击的安全高可用设计

7.1.1 多维度隔离机制

云上基础产品采用多租户的架构。以 ECS 举例，同一物理机上的 ECS 实例会分配给不同的用户。因此，实例之间的隔离对各个用户来说是重要的安全保障。阿里云在计算、存储、网络等方面建立了多维度的隔离机制，充分实施租户间隔离架构，以确保在面对攻击时各个用户之间不会相互影响。

7.1.1.1 计算资源的隔离

阿里云提供的计算能力采用多种安全加固方式进行计算资源隔离，包括：

- **虚拟化隔离：**使用自研 Hypervisor 和 MoC 设备将单一物理主机切分为多个相互独立的虚拟机。通过限制虚拟机之间可使用的资源，如操作系统、CPU 份额、内存空间和磁盘资源，能防止单一用户在物理机上消耗大量资源导致的性能影响。

- **容器隔离：**容器技术（如 Docker）通过操作系统级别的虚拟化，在单一操作系统内核上运行多个隔离的用户空间实例。容器共享主机的操作系统核心，但通过命名空间（Namespace）对文件系统、网络设备、进程 ID 空间等进行隔离，通过控制组（Cgroups）对资源使用（如 CPU 时间、内存）进行限制，实现了轻量级的资源隔离。

7.1.1.2 存储的隔离方式

存储资源的隔离主要是为了保护数据的隐私和安全，具体方式包括：

- **多租户架构：**云存储服务通过逻辑上的多租户架构，确保不同用户的存储资源在逻辑层面完全隔离，即使存储在相同的物理设备上，也通过访问控制和身份验证机制确保数据不会被非授权用户访问。
- **加密存储：**对存储的静态数据进行加密处理，支持选择主流加密算法，密钥管理独立于存储服务，进一步增强数据的安全性。

7.1.1.3 网络的隔离方式

网络隔离是确保云环境中服务间安全交互的关键，具体实现方法有：

- **虚拟私有云（VPC）：**为每个用户创建一个逻辑上的隔离网络环境，用户可以自定义 IP 地址范围、子网、路由表和网络访问控制列表（ACL），实现网络流量的细粒度控制。
- **安全组和网络 ACL：**安全组工作在网络层，根据端口和协议控制入站和出站流量；网络 ACL 更侧重于子网级别，提供更基础的防火墙规则，两者结合使用能有效控制网络访问。
- **私网连接：**云产品提供服务时，通过 PrivateLink 等方式，提供从企业内部网络到云服务的专用、高带宽、低延迟的网络连接，数据不在公共互联网上传输，提高了数据传输的安全性和可靠性。

7.1.2 动态负载均衡及弹性扩展

阿里云建设了实时容量管理能力，能够预测和调整系统资源，以确保满足当前和未来的业务需求，在避免资源过剩造成浪费的同时，防止系统因资源耗尽而过载，导致性能下降、响应时间延长甚至服务中断。此外，容量管理提倡采用弹性架构，使系统能够根据负载自动扩展或收缩资源。这种设计确保了系统在面对突发负载和恶意攻击时仍能保持稳定，避免因固定资源限制造成的性能瓶颈。

基于阿里云内部快速全面的容量监控，云平台可以根据负载情况动态对云服务进行扩缩容。借助阿里云底层的海量资源进行弹性扩展，不仅能够根据业务需求和资源使用情况合理规划和调整资源分配，还可以有效抵御 CC 攻击或其他资源耗尽攻击。

7.1.3 数据冗余及同步方案

在架构设计阶段，我们为内部各类系统的数据存储设计了数据冗余和多级备份方案，通过数据复制和备份，确保用户资料数据的安全性。

- **数据冗余**

  所有数据的读写最终都会被映射为对阿里云数据存储平台上的文件的读写。阿里云提供了一个扁平的线性存储空间，在内部会对线性地址进行切片，一个分片称为一个 Chunk（中文含义为块）。每一个 Chunk，阿里云都会复制成三个副本，并将这些副本按照一定的策略存放在存储集群中的不同数据节点上，保证数据的可靠性。

- **数据同步**

  阿里云服务即时或定时地将运行时关键数据传输到其他位置进行冷热备份。在出现数据遭遇删除、丢失或损坏时，我们可以将云服务当前使用的数据直接切换到备用实例上，减少故障影响时间，同时最小化潜在的数据丢失量。

对于用户侧存储的数据，阿里云通过建设一系列可选的数据冗余能力，支持用户保障数据的完整性与可恢复性，数据冗余能力因产品品类不同存在差异，以数据库为例：

- **主从复制：**将操作数据实时同步到多个 region，例如将利用数据库 binlog，将数据库数据实时同步至其他数据库实例，在主数据库存在异常时，从数据库能够迅速接管，确保服务的连续性。
- **分布式数据库：**通过将数据分布存储在不同集群的多个节点上，防止由于单一节点被攻击导致的全局性问题，提高云平台可用率。
- **定期备份：**按照设定的时间表自动执行数据备份，确保在数据丢失或损坏时能够快速恢复。通过在地域间的数据同步，实现数据的分布式存储，降低访问延迟 ，并为数据容灾提供解决方案。

7.2 严密的安全和可用性监控

7.2.1 全方位物理安全监控

在物理安全方面，我们的数据中心配备了先进的安全监控设施，包括全天候的视频监控、入侵检测、防火墙等。通过多层次的物理安全防护，以确保数据中心的安全性和可靠性。具体措施包括：

- **视频监控与入侵检测：**在数据中心内外安装高清摄像头，实施 24/7 的视频监控，实时监测异常活动。同时，配备入侵检测系统，识别并阻止未经授权的访问。
- **严格的访问控制：**实施严格的访问控制政策，包括生物识别技术、智能卡等，确保只有授权人员能够进入敏感区域。所有进出记录均被保存，以备审计和追溯。
- **环境监测与灾害预警：**配备环境监测系统，实时监控数据中心的温度、湿度、电压等环境参数。同时，建立灾害预警机制，及时应对自然灾害、火灾等突发事件，保障数据中心的安全运行。

7.2.2 全链路攻击行为监控

在阿里云内部，我们在多个位置部署了多种网络防护设备，以防止来自互联网的各类攻击对云平台可用性带来的问题。

- 在云网络各个出入口，阿里云部署了自研的 Beaver，Beaver 是集流量检测、安全编排、流量日志等功能为一体的高性能云安全平台，发现及处置云上僵尸网络、蠕虫攻击、0day 漏洞、Web 攻击、Webshell、反弹 Shell、暴力破解、内部 DDoS、挖矿、数据泄露、信安等各类安全事件，为阿里云、公有云租户及专有云客户提供基础的入侵检测和默认防御等安全能力。
- 阿里云通过各类防火墙，限制用户可访问的网络区域，将用户必需的服务暴露到公网，降低云平台自身供给面，防止各种入侵行为可能导致的阿里云业务受损。
- 云平台各个应用访问入口，都部署了自研的 WAF，在用户请求真正到达服务端进行处理前，提前解析业务请求，识别恶意攻击行为，提前完成对 Sql 注入、SSRF、XSS 攻击的阻断，防止由于系统漏洞影响其他系统。
- 阿里云与全球威胁情报平台合作，获取最新的攻击信息和防护措施，不断更新和优化内部安全策略，提高系统的防护能力。

7.3 健全的应急响应机制

7.3.1 有效的攻击阻断机制

在面对攻击时，我们设计了一套高效的阻断机制，能够迅速隔离受影响的部分，防止攻击扩散。自动化的安全策略调整和实时的系统修复，确保业务中断时间降到最低。具体措施包括：

- **自动化攻击阻断：**通过自动化工具和脚本，系统能够在攻击发生时自动执行阻断操作，如调整防火墙规则、限制流量、隔离影响设备等，迅速阻止攻击的扩散。
- **快速响应团队：**建立快速响应团队，负责监控和处理安全事件。团队成员具备丰富的实战经验和专业技能，能够在短时间内做出准确判断和有效处置。
- **持续改进与优化：**在每次攻击后，我们都会进行详细的事件分析和总结，不断改进和优化我们的防护策略，提高系统的防御能力。

7.3.2 灵活的迁移策略

阿里云的计算与网络服务深度融合智能运维技术，在故障发生，或攻击行为影响其他用户时，能主动发现性能劣化、网络拥堵等场景，此时，阿里云服务将主动发起业务无感的迁移策略。阿里云常用的迁移策略有以下几类：

- **主备切换：**通过配置主备服务器，当主服务器出现故障时，系统会自动将业务切换到备服务器，确保服务不中断。主备切换可以在秒级甚至毫秒级内完成，极大地减少了故障对用户的影响。
- **多活数据中心：**多活数据中心是指两个或多个数据中心同时处理业务，并且相互备份。当其中一个数据中心出现问题时，其他数据中心可以立即接管所有业务，确保服务的高可用性。
- **沙箱流量迁移：**当检测到恶意流量时，系统会将这些流量迁移至沙箱环境中，而不影响正常的业务流量。同时，阿里云安全服务将通过监测沙箱中的流量行为，获取攻击者的攻击模型，为后续的安全防御提供数据支持。

7.3.3 快速数据恢复机制

我们依托高度自动化的备份与恢复机制，确保在数据遭遇意外丢失或损坏的紧急情况下，能够迅速恢复业务运作。我们精心设计了多维度的数据恢复策略，覆盖从细粒度的文件级别到全面的应用级别，全方位保障恢复的高效性与数据的完整性。具体策略如下：

- **无缝主从切换策略：**实施高效的 IP 切换机制，当主数据库系统遭遇故障时，系统自动将访问流量无缝转移至备用数据库，确保系统服务不间断，快速恢复稳定运行状态。
- **智能自动化备份体系：**集成先进的自动化备份工具，定期对核心数据进行全面扫描与备份，确保在数据丢失或损坏时，能即刻启动恢复流程，最小化对业务的影响。
- **精准多版本数据回溯：**运用多版本数据恢复技术，能够在数据发生错误或被篡改时，快速恢复到正确版本，保障数据的完整性和准确性。
- **实战化灾难恢复演练：**定期组织灾难恢复实战演练，全面检验并优化恢复预案，不断提升系统的恢复能力与响应速度。

8. 全球化背景下的合规支撑

在数智化和全球化的趋势下，信息基础设施必须满足不同地区和行业的监管合规要求。这些要求既包括对云服务提供方在基础设施和云平台安全性上的规定，也包括对客户使用云服务过程中的要求，涵盖客户的自身数据、应用和账户安全等方面。

为帮助企业高效且低成本地实现安全合规的目标，阿里云高度重视云平台自身的安全合规建设，确保来自不同地区和行业的客户在选择阿里云服务时，能够满足他们所需遵循的安全合规要求。同时，阿里云致力于将共性合规要求融入到云安全产品功能设计中，以便客户可以按需选用合适的产品功能，以满足使用过程中的审计与合规需求。

8.1 云平台自身合规

8.1.1 全球安全合规领先的云服务商

阿里云基于完整的平台与产品管理机制，结合自身合规治理经验，推动内外部合规标准在云平台与产品中落地，确保云平台与产品在基础设施安全、网络安全、身份安全、主机安全、数据安全与个人信息保护、云产品安全等方面均符合海内外合规标准。

阿里云致力于加强全球化业务布局的合规体系建设。作为全球安全合规水平领先的云服务商，阿里云通过独立第三方机构验证其安全合规的符合性，并在全球范围内通过了 140 多项安全合规认证。这些认证展现了阿里云在各体系标准下的全面安全能力。阿里云不断提升云平台安全合规水位，以此支持云上客户及组织高效满足所在地区和相关行业的安全合规要求。

中国		全球通用	境外区域及行业	
网信办	云计算服务安全评估： 电子政务云（增强级） 金融云（增强级）	ISO 9001 ISO 27001 ISO 27017 ISO 27018 ISO 27701 ISO 29151 ISO 20000 ISO 22301 ISO 27799 ISO 27040 ISO 37301 ISO 42001 BS 10012 CSA STAR PCI DSS/PCI 3DS SOC1/SOC2/SOC3 CyberGRX CyberVadis GxP	**欧盟** EU Cloud CoC GDPR 合规评估 **美国** NIST 800-53 NIST CSF SEC Rule 17a-4(f) TRUSTe **德国** C5 TISAX AIC 4 Trusted Cloud **阿联酋** NESA/ISR **菲律宾** BSP 合规评估 **马来西亚** BNM&SC 合规评估	**新加坡** MTCS Cyber Trust Mark OSPAR DPTM CBPR/PRP **印尼** OJK 合规评估 **韩国** K-ISMS **中国香港** HKMA 合规评估 HKIA 合规评估 SFC 合规评估 SRAA 合规评估 **中国澳门** AMCM 合规评估
公安部	网络安全等级保护： 金融云（IaaS/PaaS，四级） 公共云（IaaS/PaaS/SaaS，三级） 电子政务云（IaaS/PaaS，三级） 安全产品销售许可证 网络安全专用产品检测			
工信部	可信云安全评估 产品安全能力评估			
国家市场监督管理总局	中国网络安全审查认证和市场监管大数据中心 网络安全专用产品认证 数据安全管理认证			
国家密码管理局	密码应用安全能力评估： 公共云（IaaS，三级） 政务云（IaaS，三级）			

图 3.8.1：阿里云海内外安全合规资质

更多关于阿里云的安全合规信息以及合规文档，可参见阿里云官网“阿里云信任中心 – 阿里云合规”。

8.1.2 满足高合规要求行业的客户需求

阿里云支持云上客户及组织高效满足金融行业的安全合规要求，已经通过了多项国内及国际权威机构的认证。在国内，阿里云按照网络安全等级保护制度的要求，对金融云平台开展网络安全等级保护定级备案，并由第三方权威机构进行网络安全等级保护测评，金融云平台（IaaS/PaaS）通过等保四级测评；按照网信办《云计算服务安全评估办法》要求，金融云平台在 2020 年作为首个通过云计算服务安全评估（增强级）的具有金融行业属性的云平台，为金融行业客户提供安全可控的云计算服务。

国际上，阿里云通过了支付卡行业安全标准委员会的支付卡行业数据安全标准（PCI DSS）、美国证券交易委员会（SEC）17a-4(f) 记录保存规则评估、香港金融管理局（HKMA）合规评估、香港保险业监管局（HKIA）合规评估、香港证券及期货事务监察委员会（SFC）合规评估、香港保安风险评估及审计（HKSRAA）、澳门金融管理局（ACMA）合规评估、新加坡银行业协会的 OSPAR 、菲律宾中央银行（BSP）合规评估、马来西亚国家银行（BNM）和马来西亚证券委员会（SC）合规评估、印尼金融服务管理局（OJK）合规评估、印尼金融行业 ISAE 3000 认证。

8.2 助力租户侧合规

为满足客户应对监管合规要求及内部安全管理的需求，阿里云持续支持客户的安全合规需求，并提供等保、密评、数据安全等安全合规咨询服务和解决方案，助力客户获取合规资质。同时，阿里云还提供强有力的产品安全审计和合规能力，协助客户准备并配合审计与检查，开展有效的安全合规治理。

8.2.1 全面专业的安全合规服务

阿里云及时响应客户的合规需求，持续协助客户安全合规文档的提供。阿里云通过官网合规文档中心、客户服务支持中心、对接销售人员服务等渠道为客户提供安全合规资质、安全合规审计报告、平台和产品的合规证据等。通过安全合规文档的提供，阿里云协助客户迎接监管检查，获取等保、密评、ISO 等资质认证以及通过公司内部审计等，以支持客户业务安全合规性证明，同时提升客户市场竞争力。阿里云支持客户通过官网合规文档中心自助下载文档，可参见**阿里云合规文档中心**。

同时，阿里云组织行业资深安全合规专家，为客户提供安全合规咨询服务。

等保咨询服务整合云安全产品的技术优势，联合优质等保咨询、等保测评机构等合作资源，为客户提供了一站式等保咨询服务，全面覆盖等保定级、备案、建设整改以及测评阶段，帮助客户高效地通过等保测评。关于更多阿里云等保合规服务的信息，可参见**阿里云等保合规解决方案**。

密评合规服务是阿里云依托云平台密评经验和云密码产品优势，联合第三方测评机构等合作资源，提供一站式密评合规方案，覆盖差距分析、方案设计、建设整改、密码测评及密评备案等阶段，助力客户快速完成密评合规。关于更多阿里云密评合规服务的信息，可参见**阿里云密评合规解决方案**。

阿里云在云平台提供更为安全便捷的数据保护能力的同时，根据自身多年的经验积累，基于数据安全法律法规及国家标准等，结合大量云上客户的最佳实践，提供了一套完整的数据安全合规解决方案，帮助企业提升云上数据风险防御能力，实现企业核心及敏感数据安全可控。关于更多阿里云数据安全合规服务的信息，可参见**阿里云数据安全合规解决方案**。

8.2.2 便捷高效的安全合规产品

阿里云为帮助客户在云资源管理过程中更好地满足安全合规要求，定义了三个关键环节：事前限制、事中及时发现和修复、事后审计记录。阿里云针对每个关键环节均提供匹配的安全合规产品和服务，提升客户对云资源管理的合规与审计能力。

在事前限制环节，资源管理服务中资源目录的管控策略能力支持按照合规要求执行针对资源的访问控制，实现预防性管控。在事中及时发现和修复环节，配置审计（Config）服务支持持续评估云上资源配置合规性，实现发现性管控。在事后审计记录环节，操作审计（ActionTrail）服务支持对云上操作日志的集中管理收集和持久化存储，实现对操作日志的追溯分析。

阿里云的安全合规产品通过限制和持续监控以确保 IT 配置始终符合合规预期，提供合规能力；通过客观记录云上 IT 运维的全过程并做长期留存，提供审计能力。基于强有力的合规与审计能力，阿里云为客户构建一个可见、可控、可追溯的安全运维环境，降低客户安全合规风险。

图 3.8.2：云上资源管理关键环节

8.2.2.1 管控策略

通过资源管理服务中资源目录的管控策略能力，定义组织最大的权限边界。策略决定了组织中哪些行为允许发生。用户使用管控策略，将合规基线按照策略语法编写对应的 Policy，然后将 Policy 附加到期望生效的组织节点上，那么此节点下所有账号（包含未来新增账号）都会继承到这个父节点的 Policy。被附加了这个 Policy 的业务账号，即使业务开发具有 Admin 权限，也依然无法做突破 Policy 的操作。管控策略自上而下的继承性确保策略不会被业务部门所篡改，保证了企业安全红线、合规基线的强制实施。

8.2.2.2 配置审计

用户使用面向云上资源的配置审计（Config）服务，实现对于海量云上资源合规性的持续监控和自动修复，满足客户内外部合规的需求。

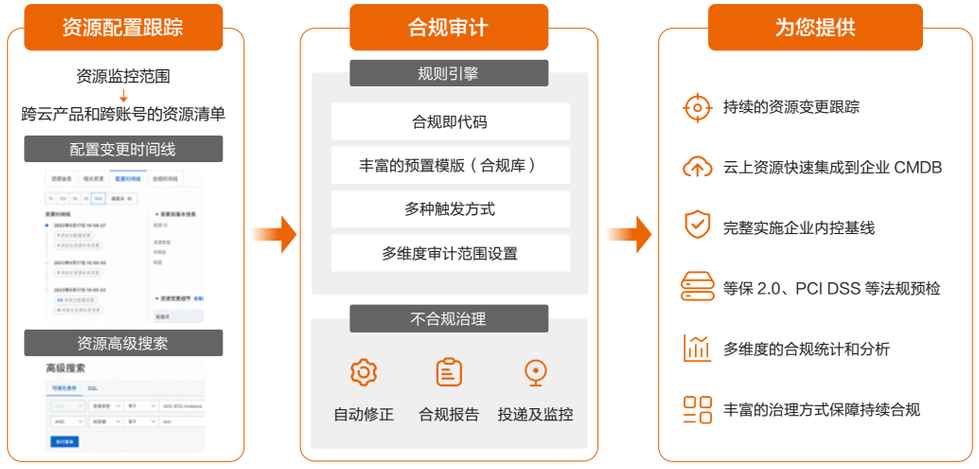


图 3.8.3：配置审计服务

同时，配置审计（Config）帮助用户记录云上 IT 资源的配置变更历史，并通过审计规则持续地评估云上资源配置的合规性，通过使用自动修复模板或者自定义修正，自动对云上不合规资源完成修复。当资源配置变更时，通过触发配置审计规则来判断某个资源配置是否合规；或将审计规则设置为周期性触发，定期为用户执行合规评估。配置审计（Config）支持客户按照企业实际场景自定义审计规则，也提供累计 400+ 审计规则模板；同时基于法律法规和最佳实践，提供了 20+ 合规包模板，并支持用户从规则、资源和成员（仅用于多账号模式）维度查看检测结果。其中，法律法规合规包模板涵盖了 GxP 欧盟附录 11 标准合规包、ISO27001 安全管理标准合规包、等保三级预检合规包、RMiT 金融标准检查合规包等；最佳实践类合规包模板涵盖了 AccessKey 及权限治理最佳实践、资源稳定性最佳实践、多可用区架构最佳实践、网络及数据安全最佳实践等。用户可以通过快速启用合规包，多维度进行合规统计和分析，推动云上 IT 合规治理。

8.2.2.3 操作审计

通过使用阿里云操作审计（ActionTrail）服务，用户可以利用云上操作日志查看账号行为、进行问题溯源、构建安全分析等，可以满足客户合规审计需求，助力提升租户侧合规能力。

操作审计（ActionTrail）默认为每个阿里云账号记录最近 90 天的管控事件，如用户为了满足内外的合规要求需要对事件记录留存更长时间，可以通过操作审计（ActionTrail）的跟踪服务实现事件记录的持久化存储。

操作审计（ActionTrail）为用户提供统一的云资源操作日志管理，可通过多账号跟踪功能实现将多个账号日志集中收集。通过阿里云资源目录（Resource Directory）的管理账号或操作审计的委派管理账号，可配置对整个资源目录中多账号跟踪，其记录的操作日志通常包括操作人、操作时间、源 IP 地址、资源对象、操作名称及操作状态等，这样资源目录中所有成员账号的事件记录被集中投递到指定的存储服务中，便于企业的审计管理员统一对云上所有账号的操作记录进行合规审计和安全分析。

通过对操作日志进行分析，可以应用到安全监控与保障、合规审计、资源变更管理、故障诊断与运维等多个合规应用场景。

04.

云上安全建设最佳实践

Best Practices for Alibaba Cloud Security Construction

1. 全面上云：淘宝云上安全建设实践

淘宝作为全球最大规模、峰值性能要求最高的电商交易平台，基于公共云底座成功通过了多年双 11 峰值的考验。系统及业务的稳定运行离不开安全性的保障，淘宝长期以来将安全性保障视为重要目标，基于公共云的安全能力支撑，在云上系统安全、网络安全、账号 & 凭据安全、云资源安全等领域积累了丰富的经验和最佳实践。

1.1 系统与网络安全体系：构建坚不可摧的企业安全防线

业务上云后，机房物理环境安全交由阿里云保障，淘宝无需投入人力资源，更多地把重心投入系统与网络安全建设中。

1.1.1 系统安全保障

淘宝建设了完整的系统安全保障体系，控制系统被入侵的风险，并减少入侵行为对业务的损害。在建设过程中，使用了阿里云所提供持续更新的操作系统安全版本，并使用云安全中心来进行主机上的防护，如漏洞检测、安全威胁态势感知、病毒检测、防勒索、入侵检测与响应。

在漏洞检测与风险态势感知方面，能够及时、清晰地了解到系统安全所面临的风险。

在病毒检测与防勒索方面，能够做到全面、准确地识别病毒，并通过数据备份恢复等能力，控制入侵行为对业务的影响。

在入侵检测与响应方面，通过智能学习应用白名单的能力，能够识别可信和可疑 / 恶意程序形成应用白名单，防止未经白名单授权的程序悄然运行，可避免主机受到不可信或恶意程序的侵害，并及时将攻击者驱逐出生产环境。

1.1.2 网络安全保障

淘宝在“最小化暴露”“纵深防御”的设计思想下，设计了整体的网络安全架构，以保障淘宝数据和资产安全。

淘宝将网络安全防御分为南北向防御与东西向防御，南北向防御主要针对内外部流量传输进行防御。DDoS 风险是淘宝面临的核心风险，一旦因 DDoS 攻击导致服务中断，每分每秒都将面临巨额损失。淘宝使用阿里云的 DDoS 防护能力，可随淘宝业务流量峰值、威胁情况不同而弹性伸缩，从而保障了南北向的流量安全。

东西向流量是指企业内部网络中的不同设备或应用之间的流量，是企业生产网络中主要的流量类型。东西向流量的安全防护一直是企业网络安全建设中的难点。传统的安全防护手段，如防火墙、IDS/IPS 等，主要针对南北向流量进行防护，对东西向流量的防护效果有限。基于阿里云标准化、可扩展的云资源，针对企业内的痛点，淘宝设计了网关安全防护能力，以满足保障需要。

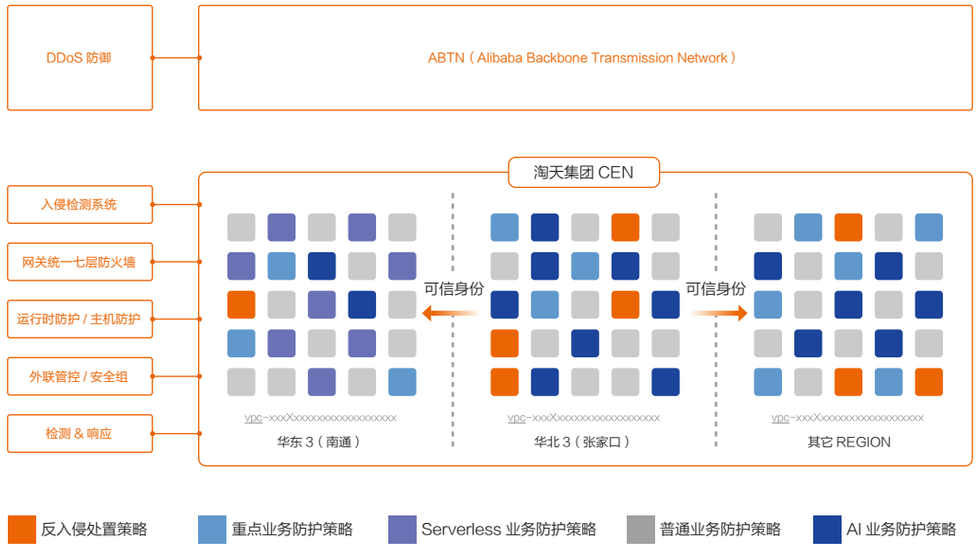


图 4.1.1：淘宝网络安全架构

1.2 账号与凭据安全体系：保障业务生产安全运行的坚实堡垒

随着越来越多的系统在云上部署、越来越多的数据在云上存储，账号与凭据作为权限的载体，其安全保障就变得尤为重要。一旦账号、凭据丢失，将可能导致数据泄露、服务中断等严重后果。

淘宝作为一款大型国民级产品，拥有庞大的研发团队，持有上千云账号，数以万计的云资源，如何保障在复杂、长期的研发过程中，控制账号与凭证泄露风险，是一项巨大的挑战。淘宝的安全团队与 TRE 团队一起，基于阿里云的多账号管理、身份关联扩展能力，采用了资源目录（RD）产品、云 SSO（CloudSSO）产品，建设了适合于大型组织的云管平台，构建了一套完善的云账号 / 凭据安全管理体系。

在云账号安全管理体系中，所采用的关键设计有：

- **禁用账密：** 对内部员工屏蔽账号密码登录，通过云 SSO 将办公 BUC 身份与云账号身份关联起来，实现免密登录，使云账号账密的风险敞口能够通过统一办公 BUC 的身份管理体系来收敛、控制。
- **明确账号管理流程与责任：** 制定清晰的账号申请、审批、使用、变更、注销等流程，并指定专人负责账号管理工作，确保账号安全责任可追溯。
- **禁用主账号日常操作：** 默认只允许使用子账号、RAM Role 执行管控操作，降低主账号被盗用的风险。
- **细粒度权限控制：** 遵循最小授权原则，通过 RAM 所支持的资源组、Tag 等细粒度控制能力，授予用户和应用最小必要的访问权限，避免过度授权带来的安全风险。
- **统一账号行为审计：** 通过阿里云 RD 将所有账号的操作审计进行汇总分析，集中监控账号行为，及时发现可疑操作，快速响应安全事件。

在凭据安全管理体系中，所采用的关键设计有：

- **避免明文接触：** 彻底消除业务员工接触、存储、明文使用云账号凭据的可能性，从源头上杜绝 AK 泄露风险。
- **运维统一管理：** 由运维系统统一管理 AK，降低运维成本和复杂度，提升安全性。
- **动态获取凭据：** 应用在运行时通过自身身份和资源标识动态获取所需的云资源凭据，实现凭据不透出、不落盘。
- **定期轮转凭据：** 为应用使用的云资源凭据指定轮转周期，定期更换凭据，降低凭据泄露风险。

淘宝通过这一套完整的云账号 / 凭据安全管理体系，有效提升了云账号的安全性，筑牢了云安全堡垒。

1.3 云资源安全管理体系：默认配置安全与巡检审计

淘宝上云后，需要管理数以万计的资源，资源类型也种类繁多，管理复杂度极高。而在全面上云后，通过云平台的标准化设计，大大降低了管理复杂度，使得安全妥善管理具备可行性。

为了管理如此大规模的云资源体量，淘宝基于阿里云资源中心的能力，获取到了近实时的云产品配置数据，并基于该数据实现了 CSPM（Cloud Security Posture Management）云资源安全管理平台。

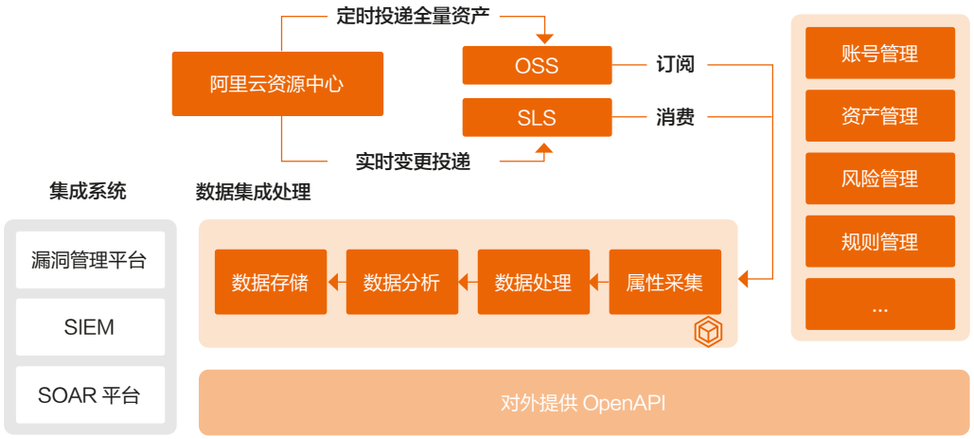


图 4.1.2：CSPM 云资源安全管理平台

一旦云上资源出现配置错误问题，可能会带来安全风险，比如存储了敏感信息的 OSS Bucket 允许外部匿名访问。在出现此类问题时，需要能够立刻响应并通过内部漏洞管理平台推动风险的修复。

1.4 总结

淘宝作为国民级大型应用，结合自身电商领域的安全痛点，基于阿里云的基础设施及安全能力，构建了高效弹性的安全保障体系。克服了 DDoS 攻击、大型企业多账号管理困难、大型组织资源安全管理复杂等痛点，为保护淘宝用户的数据安全、保障淘宝服务安全稳定运行提供了强有力的支撑。

2. 助力发展：关键行业云上安全最佳实践

阿里云作为数智化趋势下的基础设施，逐渐在各行各业成为了数智化系统的底座系统，从数字而生的互联网行业，到国计民生的金融行业，再到从传统行业转型的制造业，阿里云在满足客户业务高速发展的同时，也在利用云平台安全性优势，为各行各业的“安全行驶”保驾护航。

下文将从行业中的经典案例入手，分享阿里云如何帮助行业内的客户，克服安全方面的挑战。

2.1 互联网行业云上安全最佳实践

2.1.1 行业安全需求洞察

数智化时代，互联网行业作为数字经济的主力军，正面临着前所未有的安全挑战与机遇，其安全需求分别由“风险”“合规”两大要素驱动。一方面要防范不法分子的攻击，一方面要符合各类监管合规要求。

图 4.2.1：互联网行业安全需求

2.1.2 典型案例

某头部电商创立于2016年，之后经历了8年的快速发展，已经在纳斯达克上市。在他们8年的发展历程中，安全的发展迅速，期间遇到了不少安全痛点及威胁。

2.1.2.1 业务痛点

- **大促期间业务被黑洞风险：**“双 11”“双 12”等电商大促期前，客户花费了大量的营销资金进行铺垫，客户非常担心在大促期间因为 DDoS 攻击导致业务被黑洞，这样营销资金就会被浪费，并对业务造成巨大影响。
- **安全合规风险：**合规是客户对于安全建设的基本诉求，这对于客户在国内拓展电商业务，在美国谋求上市都至关重要，对应就是参照等级保护三级标准进行建设，满足监管要求。
- **数据爬虫风险：**电商行业竞争激烈，客户的竞对经常会利用爬虫，批量获取商品价格后制定商品定价策略，这样就会对客户的商品价格及销量造成巨大冲击。
- **业务安全威胁：**客户在拉新及用户运营时经常会有现金或红包奖励，他们的活动经常会被外部薅羊毛党盯上，通过注册大量僵尸账号发起薅取营销资金，给客户造成较大损失；最终用户留言、评论等 UGC 内容也时常会出现内容违规情况。

2.1.2.2 解决方案

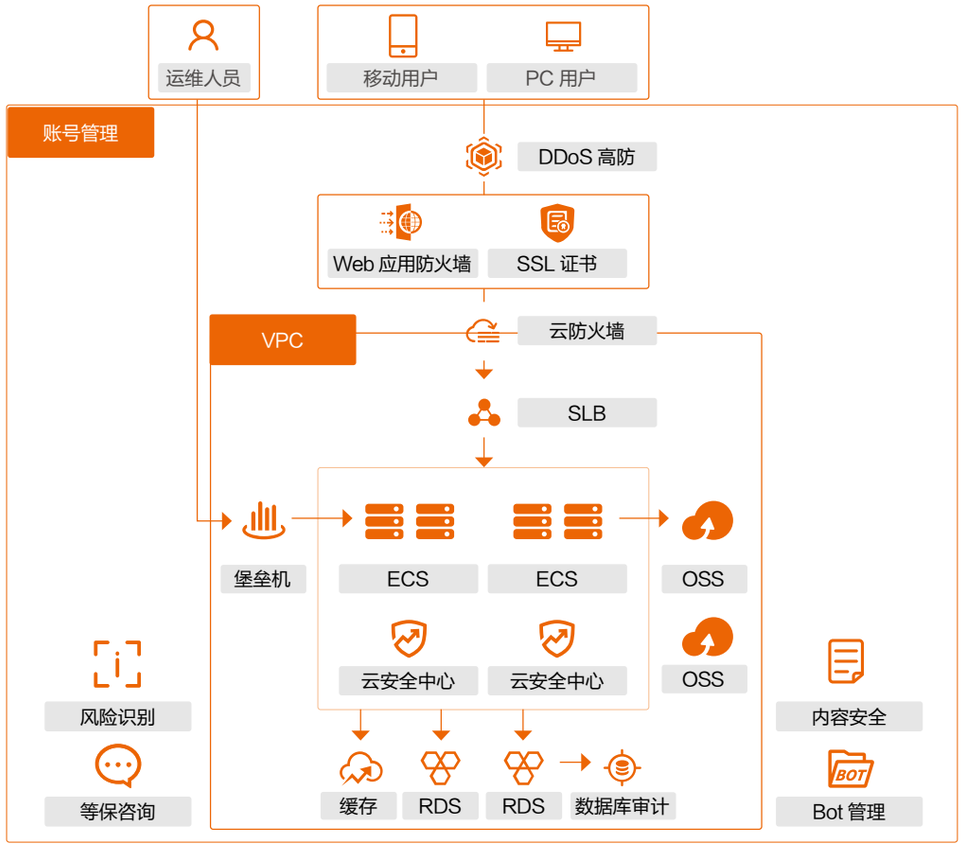


图 4.2.2：该公司解决方案

- **业务高可用保障：**通过 DDoS 高防产品，协助客户构建了业务高可用架构，过滤攻击流量，保障电商系统持续平稳对外提供服务。
- **合规及安全架构搭建：**通过 WAF、云防火墙、云安全中心、堡垒机、数据库审计以及等保咨询服务，协助客户构建了整体安全体系，并通过了等级保护三级测评；在满足等级保护合规要求的同时，有效对各类型攻击进行识别及阻断。
- **爬虫风险管理：**通过 BOT 管理，协助客户从海量请求中对自动化工具（例如脚本、模拟器等）流量进行识别和阻断，有效降低了数据爬取、撞库、垃圾注册、短信接口滥刷等情况的出现。

- **业务安全保障：**通过风险识别能力，帮助客户对 C 端用户的注册、登录及交易行为进行风险研判，提前发现潜在的薅羊毛党，降低业务损失；通过内容安全，对用户的 UGC 内容进行识别，提前发现内容违规风险。

2.2 金融行业云上安全最佳实践

2.2.1 行业安全需求洞察

金融行业是社会的核心行业，在数智化不断深入的今天，金融行业也在不断地将核心业务数字化，这也带来了新的安全隐患。

- **数据安全关乎企业命脉**

  金融行业的数据承载了核心价值，若数据可被非法篡改，可带来直接经济损失，造成企业破产等灾难性后果。若敏感信息数据被非法泄露，将可能导致 C 端用户的关键隐私泄露，严重损害用户对企业的信任感，造成企业经营困难。

- **丰富场景下的身份安全管理困难**

  随着金融业务数字化的发展，销售模式和产品更加丰富，参与人员大规模扩张，外包开发和合作伙伴协同模式逐渐多样化，叠加远程办公趋势的演进，越来越多的数据泄露是由于设备和人的行为管理不规范造成的。

2.2.2 典型案例

某财险类公司自 2020 年与阿里云签订全面战略合作协议后，持续使用阿里云的安全解决方案，为其数字化加速转型保驾护航。

2.2.2.1 业务痛点

- **系统安全风险：**在业务数字化后，若承载关键数据的系统不够安全，将可能因外部攻击而数据泄露。
- **数据安全泄露风险：**同时，在办公方面，研发员工开发用电脑缺乏安全管控工具，容易造成被动或主动数据泄露。普通员工桌面环境安装大量个性化软件，系统、电脑问题逐渐增多，办公安全风险过大。
- **身份安全管控困难：**员工电脑自设密码，登录公司内网后可访问大部分的业务系统，没有权限管控。

2.2.2.2 解决方案

图 4.2.3：该公司安全解决方案

系统安全

基于 WAF、云防火墙、云安全中心构建基础安全防护体系，持续检查并优化现有防护体系，针对防护薄弱点，定制攻防能力成熟度评估服务（如：渗透测试、红蓝演练等），提升险企内部人员的安全技能水平，优化应急保障。

数据安全

该财险公司，基于统一终端系统（UEM）和数据丢失防护产品（DLP）建立研发人员终端与数据安全解决方案，进行数据治理，消除“数据管理孤岛”。并建立完整的数据分类分级、全生命周期管理机制，并通过数据安全中心综合分析入网用户异常行为，感知如外包人员异常囤积客户账户信息、越权登陆核心数据库、员工离职带走用户保单等风险意图，在可能发生数据泄露风险之前感知并预警，将泄露风险限制。

身份安全加固

阿里云将 IDaaS 身份认证服务平台内嵌至该财险公司业务中台，一个账户打通企业内外部所有业务应用，大幅提升员工工作效率，改善用户保险购买和出险体验。

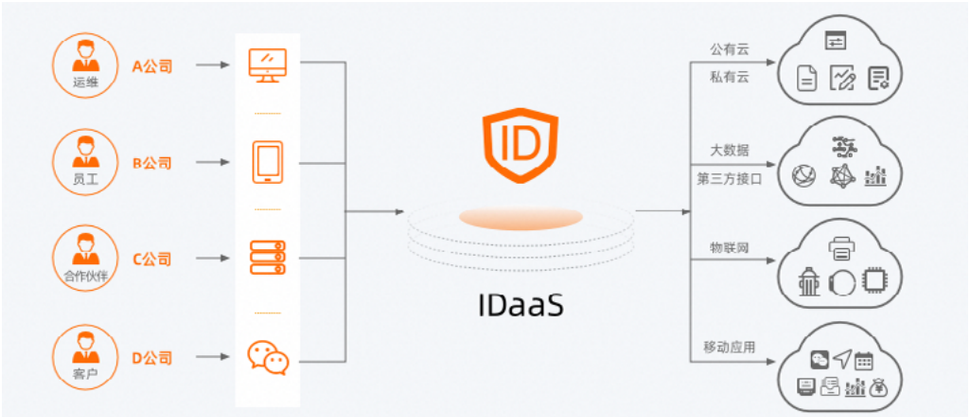


图 4.2.4：阿里云 IDaaS 管理理念示意图

IDaaS 结合 SPG 与 UEBA 技术的动态分析，帮助该财险公司的各运营支撑域清晰界定信息技术部门和不同子业务部门的运行维护职责，简化员工登陆与业务操作流程，强化用户行为管控。

在办公身份方面，使用了无影云桌面产品，能够有效实施针对剪切板、外设、水印、录屏的安全管控策略，满足集中运维、高效资产管理的需求。

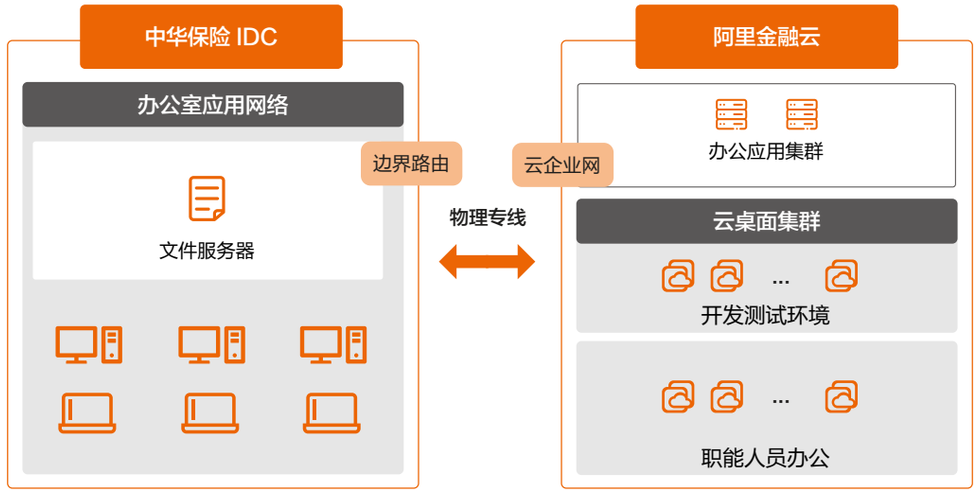


图 4.2.5：该公司安全解决方案

规范化员工身份与终端后，可以基于可信及白名单机制管理险企员工或外包开发人员异地登陆、异常登陆行为，并根据人员状态变化（离职、调岗等）对账号进行通知下发，冻结等操作。身份安全解决方案投入使用后，大大节省了该财险公司的身份安全管理成本。

2.3. 制造行业云上安全最佳实践

2.3.1 行业安全需求洞察

近年来，制造行业数字化转型收益显著。这一转型不仅提升了企业的生产效率、降低了运营成本、缩短了产品研制周期，还显著激发了产业新活力。但传统制造业数字化转型在实现工业全要素、全产业链、全价值链深度连接的同时，也带来新的安全挑战。

核心的挑战包括：

- 数字化转型促使基础设施云化，引入了很多新技术，传统安全（滞后的检测能力、碎片的安全体系、被动的防护能力）的安全防护思路难以应对不断变化的新威胁。
- 混合云、多云战略，带来暴露面扩大，安全防护水位难以拉齐，管理成本非常高。

制造行业需要一套云原生、一体化的安全解决方案，来应对这些挑战。

2.3.2 典型案例

某全球领先的制造业企业专注于工业、基础设施、交通和医疗领域的科技公司。其经营范围从更高效节能的工厂、更具韧性的供应链、更智能的楼宇和电网，到更清洁、更舒适的交通以及先进的医疗系统。自身业务系统经历多次迭代发展，当前面临企业数字化转型中的多种挑战。

2.3.2.1 业务痛点

- 大量历史系统存量 IDC、并运营多个公有云，管理成本高、防护效果差，安全策略难以拉齐。
- 业务分散，系统管理分散，管理成本高；。
- 安全事件频发，监管、合规要求提高。
- 企业数字化转型加速，安全拓展性和适应性要求高。
- 业务精细化管控，安全成本降低。
- 该企业携手阿里云，构建新一代云原生 IT 架构，并将安全方案进行落地。

2.3.2.2 解决方案

- **基础设施管理一体化**

  为了应对多云及线下 IDC 多形态资产，该企业采用阿里云原生安全防护，实现对多资产统一安全管理，统一管理互联网边界与主机、容器资产。

- **监控与安全技术一体化**

  为了应对复杂的业务系统形态，阿里云进行了监控升级，实现了安全日志的统一收集、安全告警的集中分析以及安全事件的统一管理。 结合一体化可观测监控，实现了对健康状态和安全事件的立体化监控。另外，还建立了自动化安全运维能力，以提升效率。

- **安全能力高弹性**

  通过对业务系统的微服务化改造，实现业务的灵活部署，提供更好的业务弹性与安全性，适配业务系统更加灵敏、灵活的要求。通过云上跨账号管理能力，提升了安全部门对集团账号统一管理、监控的效率。

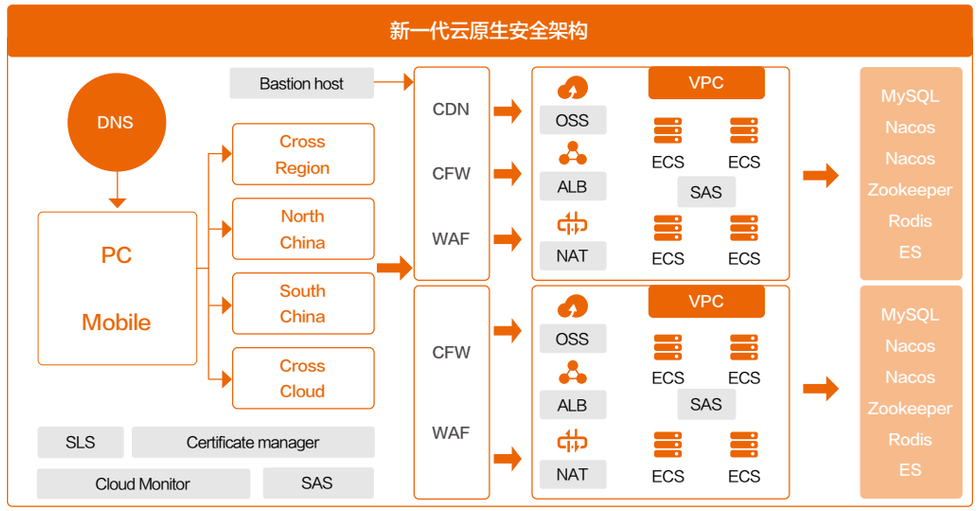


图 4.2.6：该企业新一代云原生安全架构

3. 迎接未来：AI 大模型云上安全最佳实践

ChatGPT 的问世和成功引领生成式人工智能的蓬勃发展，各类 AI 大模型产品如雨后春笋般涌现，正在各行各业积极探索应用落地场景。其中不乏 Perplexity 这样挑战 Google 搜索地位的新星、妙鸭相机这样的爆火应用。

在 AI 大模型产品快速发展的前提下，如何保护各方数据安全与主权，并有效地帮助客户应对由这些技术带来的算法安全和内容安全风险，已成为 AI 大模型时代云平台面临的关键命题，也是对数智化基础设施的重大挑战。

3.1 AI 大模型关键安全风险

阿里云同时拥有领先的云计算业务与先进的大模型技术，基于自身 AI 大模型的安全建设实践，阿里云希望能将这一未来重点领域的安全风险洞察、解决方案分享给社会。

一款 AI 大模型产品需经历数据准备、模型训练与微调、模型部署、模型运行阶段，在这些阶段过程中，面临着众多威胁与挑战，其中四项关键挑战为：

- **数据安全挑战：**

  为了使通用模型在特定领域实现更好的智能，企业需要对其自身业务数据进行提炼，并通过微调等技术将这些数据融入到模型中。鉴于这类数据对企业至关重要，在数据的收集、清洗、分析及存储过程中，都需要有完善的安全机制进行保障。

  模型在线上运行服务期间，用户的 Prompt 输入及其返回的内容可能涉及用户的隐私。因此，如何保障用户隐私不被侵犯成为 AI 大模型类产品的核心挑战之一。

- **模型安全挑战：**

  模型承载了对数据的“记忆”，因此模型一旦泄露，等同于训练数据的泄露。而模型在研发、部署阶段，大量的一线员工具备模型的访问权限，同时生产环境也面临着与传统信息系统一样的外部入侵威胁。一旦系统存在可被入侵的漏洞，就可能导致模型被外部攻击者窃取，从而间接导致参与训练的敏感数据泄露。

- **内容安全挑战：**

  生成式人工智能如果训练不当、使用不当，可能造成虚假信息与违法不良信息的传播，甚至成为诈骗分子的非法牟利工具。其输出内容也可能存在违法违规、违背道德伦理、内容失实、偏见歧视等问题。

- **合规性挑战：**

  在全球监管合规体系逐渐健全的趋势下，AI 大模型应用要遵守各地域各行业的合规要求，由于训练推理过程中需接触大规模数据，其在数据隐私合规领域的挑战尤为明显。除此之外，由于其技术的独特性，全球各国监管仍在积极探索针对 AI 大模型的监管合规政策，AI 大模型需及时响应最新的监管合规要求，在监督下有序发展。

  为了帮助客户快速且安全地发展，我们也在关键环节推出了一系列产品功能，以助力企业更好地应对 AI 大模型时代的安全挑战。

3.2 安全解决方案

3.2.1 数据安全

数据是实现 AI 大模型应用成功的三要素之一，要开发出强大的大模型应用，就需要将场景相关的数据投喂给 AI 大模型应用来进行训练、对齐、微调。因此，保护这些数据的安全性以及确保数据持有方通过云平台进行模型训练过程中的数据主权就变得尤为重要。

3.2.1.1 百炼推理链路加密

为实现对数据安全的保护，阿里云基于百炼 MaaS 平台，设计实施了一系列数据安全防护方案，包括专有网络访问通道、Prompt 加密、数据存储、应用层传输加密、存储加密：

- **私有链接传输**

为保障传输过程中网络信道安全问题，防止公网传输数据泄露，用户的推理调用、数据访问使用阿里云 Private Link 在用户自己 VPC 和百炼间创建私有链接，通过专网即可访问用户的存储实例完成训练、微调、推理等任务。且 VPC 提供网络流量监控与接口日志审计能力，可结合网络安全设备监控异常调用、专网攻击等恶意行为，提供专网保护。

- **Prompt 加密**

针对模型推理服务（纯模型调用、RAG 应用、Agent 应用）提供全链路的加密方案。用户输入提示词 prompt 和模型生成的答案全程不可见。解密只会发生在两个地方：根据用户输入 prompt 进行 RAG 片段召回、大模型用 prompt 生成答案时。百炼保证在客户授权情况下，遵循最小必要原则对 prompt 进行解密和使用，并且该过程只在内存中瞬间存在，不做任何的持久化存储。整体加密过程如右图所示：

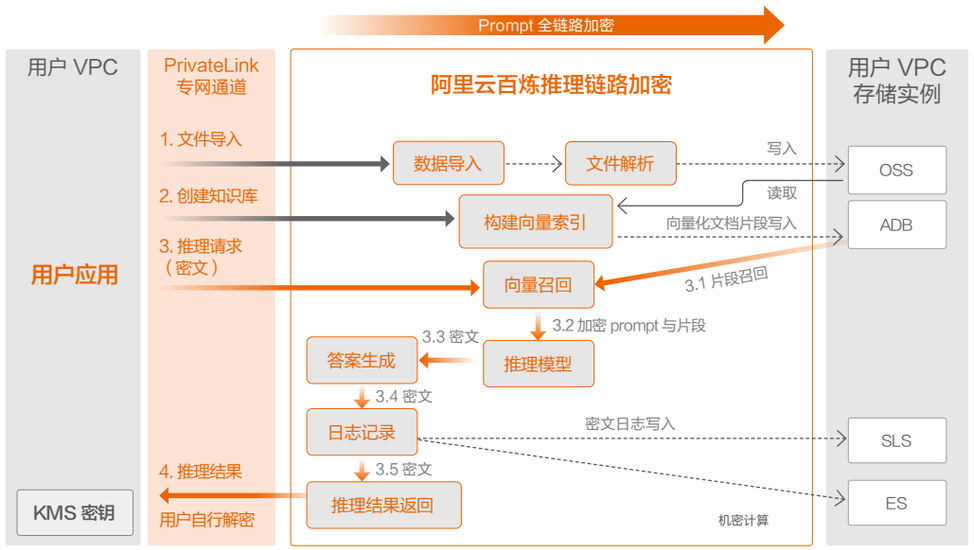


图 4.3.1：阿里云百炼推理链路加密

- **应用层传输加密**

在安全网络协议方面，为防止中间人、嗅探等网络攻击手段获取到用户与大模型服务，阿里云百炼通过支持应用层使用 HTTPS 协议进行安全数据加密传输以及采用传输层安全性 TLS 协议，为云服务和用户之间的数据传输提供保障。TLS 可提供严格的身份验证、消息隐私性和完整性保障，能够有效检测消息篡改、拦截和伪造行为。

- **存储加密**

百炼平台模型推理、训练、RAG 应用的用户数据均支持外接存储部署方式，支持外接 OSS、ES、ADB、SLS。数据采集过程支持外接归属于客户的数据库实例，用户对数据 100% 完全自主可控。这些产品支持使用服务密钥和客户自选密钥作为主密钥进行数据加密，满足敏感数据密态存储的需要，可降低数据泄露。

3.2.2 可信计算与机密计算能力

客户将数据托管到云平台，背后意味着对云平台的信任。阿里云承诺保障客户数据主权，并积极探索从技术角度，根本性保障客户数据主权及机密性的机制。

阿里云具备完整的可信计算、机密计算基础储备，产品技术矩阵如下：

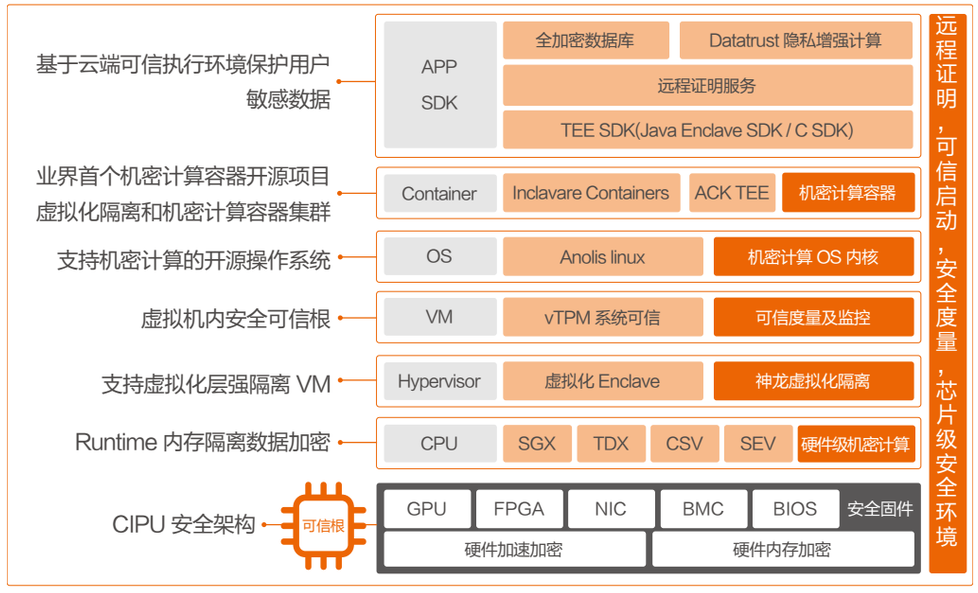


图 4.3.2：阿里云机密计算产品技术矩阵

通过利用 IaaS 层级的机密计算能力，可以为大模型服务提供端到端的、覆盖模型数据全生命周期的通用数据保护方案，保护客户运行时的数据机密性。在机密计算能力的保护下，阿里云内部的管控服务、运维人员等也无法看到用户输入的提示词 prompt、RAG 文档、微调后的模型等。

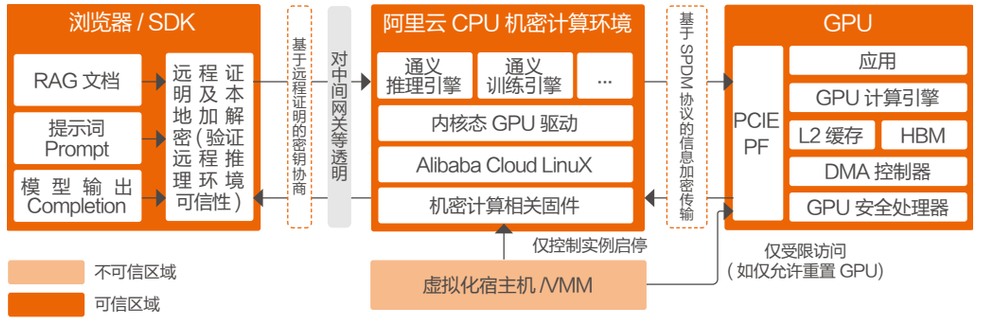


图 4.3.3：机密计算保护模型数据安全

在先进的技术基础上，阿里云还与生态伙伴一起探索更上层的合作伙伴。蚂蚁数科团队基于阿里云 ECS 机密计算、计算巢等基础能力，提供了面向 LLM 的大模型密态计算基座产品 MAPPIC，进一步为 AI 大模型应用安全提供支撑。

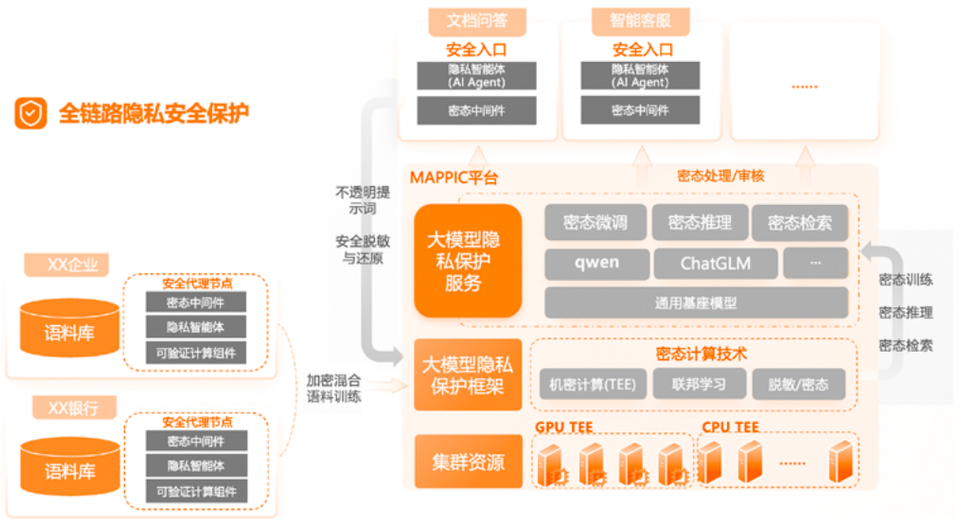


图 4.3.4：全链路隐私安全保护

3.2.3 内容安全

目前，AI 大模型技术在自然语言对话场景中得到了广泛的应用。在内容安全方面，需要确保输出内容的社会安全性，包括是否合法合规、是否遵守道德伦理和公序良俗等，具体表现在防止出现违法不良信息、内容失实、偏见歧视以及违反伦理道德等。

阿里云为此建立了完整的大模型内容安全解决方案：

- **训练语料数据去毒**

  为进一步提升定制用户的模型训练和测试、知识库数据及模型训练微调质量，防止针对模型数据集投毒攻击，除百炼内置阿里绿网提供内容安全能力，支持对用户自有的 OSS 资源中多种违规内容（例如涉黄、暴力、违法等）的实时监控、检测和拦截。

  此外，数据安全中心 / 内容安全提供了覆盖图片、视频、语音、文字等多媒体的内容风险检测的能力，帮助用户发现暴恐、色情、涉黄、暴力、惊悚、敏感、禁限、广告、辱骂等风险内容或元素，支持对训练语料进行拦截或清洗。

- **Prompt 问答护栏**

  为了满足更高安全需求的用户，数据安全中心（sddp）/ 内容安全可进一步提升实时提问管控能力，进行风险异常识别，支持意图识别，实时过滤伦理、价值观、个人敏感数据，进行安全问答阻断。可根据用户需求，构建安全知识库与专项知识库，实现数据安全规则灵活自定义与风险决策。

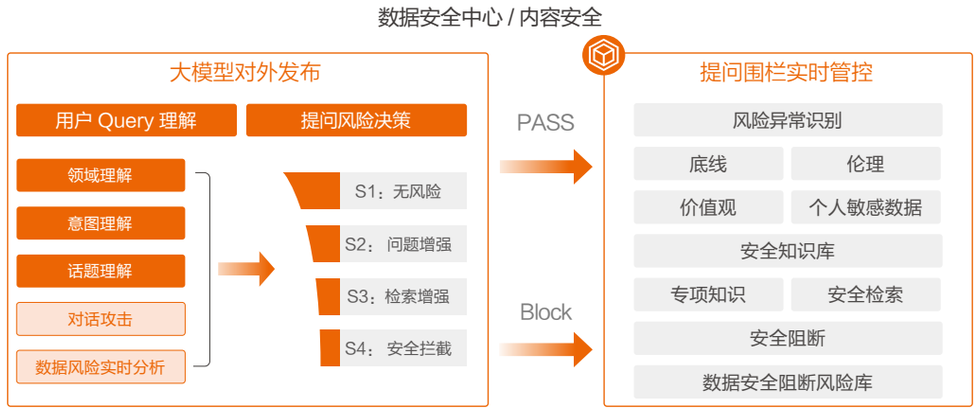


图 4.3.5：Prompt 问答护栏

- **全流程内容安全保障**

  若企业对于内容安全防护具备更高的定制需求，也可以使用阿里云的大语言模型内容安全解决方案，在自建系统中集成内容安全产品 API，实现覆盖“样本和训练管理”“模型应用”“举报与处置”“审核优化”四大阶段的内容安全整体治理。

3.2.4 模型安全

保护模型本身的安全，与其它信息系统的基础安全保障类似，需通过一系列流程与解决方案，确保系统漏洞不被外部攻击者恶意利用。

对于云平台，阿里云通过“全流程产品安全流程”与“红蓝对抗”切实保障了云平台本身的安全水位。

对于部署在云上的大模型系统，可使用云上弹性可扩展的安全防护能力，体系化地完成生产网、办公网安全建设。并通过云安全中心等产品，及时发现并治理线上风险。

3.2.5 合规性

阿里云同时拥有先进的大模型 AI 技术与云平台产品，在合规性建设方面，一方面积极跟进自身合规性建设，另一方面也在帮助云上客户完成大模型服务合规性建设。

为了进一步帮助客户更好满足《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》等监管要求，阿里云通过安全产品为客户提供算法及模型备案需要的安全技术能力，同时为客户提供作为服务提供者的互联网信息服务算法备案、生成式人工智能服务备案两项咨询服务，帮助客户更好合法合规开展互联网信息服务业务。

针对用户使用百炼进行微调后的模型，阿里云内容安全产品在模型评测阶段，提供安全性专项测试服务，帮助用户了解大模型对输入、输出内容的风险防控水位。另外可提供内容安全算法备案号，帮助客户简化备案过程。

05.

总结与展望

Summary and Prospect

总结与展望

数智化技术的发展和应用，已深刻重塑了社会生产模式，显著提升了生产效率并优化了资源配置的精准度。这一变革对基础设施设定了全新标准，要求具备高度弹性、敏捷响应、卓越性能、成本效益及更低门槛等特性。随着数智化系统成为支撑国家经济、企业经营与民众生活不可或缺的基石，保障其系统安全与数据安全的任务变得尤为紧迫与重要。

在确保系统具备弹性、可扩展性和敏捷响应等关键生产特性的同时，维护并提升其安全性，犹如在确保一辆汽车在高速公路上疾驰时，得到全方位的安全性保障，这无疑是一项极具挑战性的任务。阿里云希望从基础设施层面出发，通过不断深化安全机制的研究与安全能力的建设，为客户和社会构建一个安全、高效的云生态系统。这样不仅能保障云服务的稳定运行和客户的业务安全，也为推动数字经济的可持续发展贡献重要力量。

为有效应对挑战，阿里云积极倡导并推动云上安全共同体的建设，旨在联合社会各界力量，依托强大的公共云平台，共同追求更高水平的安全防护，同时降低客户的维护成本与时间消耗。通过实施“云上安全八大支柱”策略，阿里云不仅将安全理念深植于产品设计与服务全周期，还借助红蓝对抗等先进机制，持续优化与提升云平台的安全防线。此外，阿里云始终坚持保护客户数据主权，并实施严格的身份认证与权限管理，为客户提供既高效又灵活的安全防护方案，确保云平台在极端情况下也能快速响应与恢复，能够满足全球范围内的合规要求，全面强化云安全生态体系的建设。

展望未来，阿里云深知安全没有终点，只有不断地进步，才能满足数智化时代对安全保障的需求。

在云平台自身安全性层面：阿里云将不断深化零信任架构的实施，强化纵深防御体系，并持续加强红蓝对抗演练及第三方校验的力度，以此来有效应对日益复杂多变的网络攻击威胁。同时，阿里云将加强系统的稳定性和高可用性建设，确保客户在享受灵活弹性的云服务的同时，其业务服务的可用性得到持续保障。

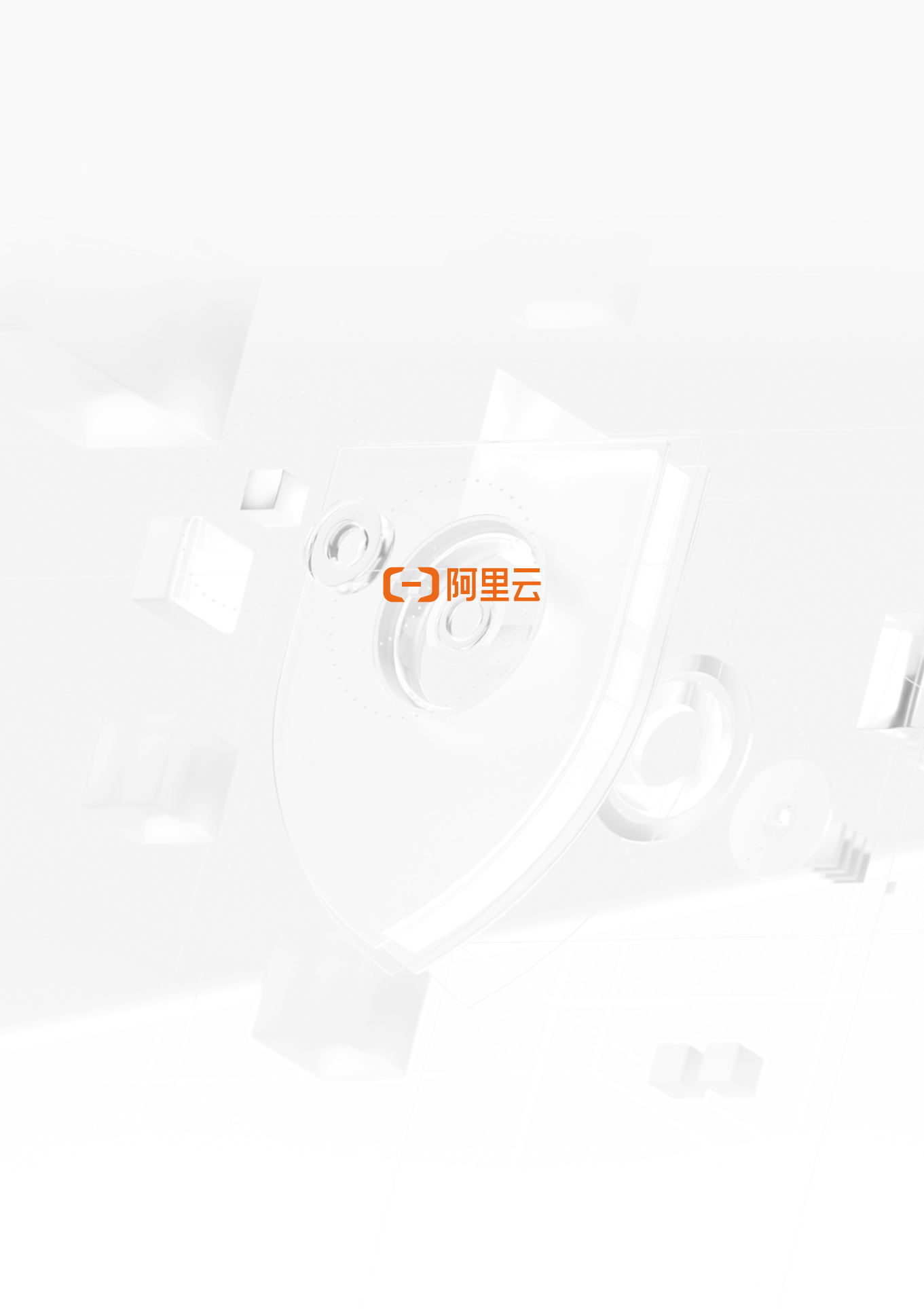
在数据安全保护层面：阿里云将始终坚守客户数据主权底线，不断探索，从技术创新及机制优化角度保障客户数据主权。阿里云将持续建设完整的、一体化的云上数据安全解决方案，最大化助力云上客户应对数据安全挑战。

在产品安全能力方面：阿里云将深入挖掘各行各业的用云场景，致力于提供更易用、更强大、更适用于企业的身份管控与权限管控方案。阿里云不断将安全功能内嵌于产品设计之中，确保产品具备默认安全和原生安全的特性，同时提供更完善的解决方案、更易用的扩展能力、更开放的生态、以及更强大的能力。

在合规支撑方面：阿里云将紧跟时代步伐，面对社会数据流通加速和智能化技术普及的新形势，积极参与合规制度的探索，致力于使云平台符合数智化时代高标准的合规要求。阿里云将积累并提炼各行各业的合规解决方案，为云上客户提供更加坚实的支持，助其构建健全的合规体系。

云上安全命运共同体不仅需要阿里云的持续努力与实践，更需要整个行业的广泛参与和共同推动。有鉴于此，阿里云呼唤云计算产业链上下游企业、行业协会、研究机构、云上客户乃至监管部门的广泛参与和深度合作。每个参与者都将被视为这一安全网络中的重要节点，共同织就一张紧密联结、互信互助的安全防护网。

阿里云作为全球领先的数智化基础设施提供商，将紧抓数智化发展的历史机遇，不断发挥自身安全优势，为企业、行业乃至整个社会的数智化转型提供更加坚实可靠的支撑与保障，携手共创更加智慧、安全、繁荣的未来。


阿里云