“云”原生安全白皮书

出品：

腾讯云计算（北京）有限责任公司

中国信息通信研究院

深信服科技股份有限公司

天融信科技集团

绿盟科技集团股份有限公司

发布时间：

2020年9月

腾讯安全 CAICT 中国信通院 SANGFOR 深信服科技 天融信 TOPSEC NSFOCUS

版权声明

前　言

云计算作为“新基建”中信息基础设施的重要组成，关键性得到肯定，是企业数字化转型的重要支撑，是实现产业互联网落地的必要途径。同时，云计算的广泛普及和重要价值也对其安全性提出更高要求，如何更加全面、有效的保障云上业务安全成为行业关注的重点。

云原生安全作为一种新兴的安全理念，并不是只解决云原生技术带来的安全问题，而是强调以原生的思维构建云安全，推动安全与云计算深度融合。本白皮书聚焦云原生安全，通过分析云原生安全定义与内涵，探究其在云安全领域的作用及意义。首先，白皮书从云平台安全原生化和云安全产品原生化两个方面对云原生安全体系进行定义，分析云原生安全体系如何促进云上安全的普及与实惠、助力所有云上用户实现全面的安全防护；继而，围绕计算环境安全、数据安全、网络安全和安全管理多个方面，探究云原生安全的应用场景和功能效用，为用户构建云上安全体系提供参考；最后，白皮书对云原生安全体系未来发展进行了展望。

本白皮书的核心观点与重要发现：

- 普惠安全以降低企业安全投入成本、提升安全成效为宗旨，缓解传统安全防护中设备昂贵、部署困难、数据流通差、联动性差等痛点，降低中小企业安全建设门槛，助力所有云上用户实现全面安全防护，提升云计算整体安全性。
- 云原生安全体系包括云平台安全原生化和云安全产品原生化

两部分。安全原生化的云平台，一方面通过云计算特性帮助用户规避部分安全风险，另一方面能够将安全融入从设计到运营的整个过程中，向用户交付更安全的云服务；原生化的云安全产品能够内嵌融合于云平台，解决用户云计算环境和传统安全架构割裂的痛点。

- 原生安全的云平台能够向用户交付更安全的云服务，一是云计算具备分布式存储、资源统一管理、网络虚拟化等特性，能够有效规避部分安全风险，实现数据高可靠性、安全管理统一化、流量隔离与管控精细化等能力；二是提倡云服务商从研发阶段关注安全问题，前置安全管理。
- 原生安全产品通过四大特性和优势，为用户云上安全建设提供更有力保障，四大特性和优势分别为：采用内嵌的方式而无需外挂部署；充分利用云平台原生的资源和数据优势；可以与用户云资源、其它原生安全产品有效联动；能够解决云计算面临的特有安全问题。
- 云原生安全体系能够有力促进普惠安全的实现，一是原生安全的云平台，深度融合云服务商安全技术和管理能力，成为客户云上安全的基石，以用户视角优化并设计的云服务原生安全属性可以满足客户的基本安全需求；二是原生安全产品依托其特性与优势，缓解企业因技术、人员、资源等条件受限而导致的云安全缺失，降低使用门槛，有效应对企业级客

户在计算环境、数据、网络、安全管理等不同安全场景下的需求与痛点。

- 依托云原生安全产品，企业级客户能够构建全面完善的云上安全体系，云原生计算环境安全产品适应云上主机、容器、应急响应和取证等计算环境新安全需求，数据安全分类治理、数据安全审计、敏感数据处理、密钥管理系统、凭据管理系统等云原生数据安全产品保障云上数据安全可靠，DDoS 防护、云防火墙、Web 应用防火墙等云原生网络安全产品有效抵御云上网络威胁，安全运营中心等云原生安全管理产品应对云上安全管理新挑战，原生托管安全服务等云原生安全服务缓解云上安全运营痛点。
- 云原生安全体系将更加成熟健全，体现在：云服务商与安全厂商联合建设云原生安全生态；产品趋于整合，形成综合的云原生安全解决方案；深耕行业，助力传统行业云上安全体系建设。

目 录

图 目 录

表 目 录

一、云计算安全态势严峻，云原生安全理念兴起

（一）云计算成为重要基础设施，安全性备受关注

1. 云计算助推数字化转型、新基建建设与产业互联网发展

云计算成为底层基础设施，帮助企业实现数字化转型。近年来，随着 5G、云计算、大数据、人工智能等新技术的持续发展，以数字化和智能化等为核心内容的第四次工业革命浪潮已汹涌而至。数字化变革将对经济和社会产生深远影响，越来越多的国家把发展数字经济作为推动经济增长的重要途径。中共十九大提出建设“数字中国”的宏伟蓝图，同时要求推动互联网、大数据、人工智能和实体经济深度融合。近两年，随着国家和各地相继发布推动数字化转型的政策文件，数字时代的到来，以及数字泛在化已经成为了一种必然的趋势。数字技术将深入改造企业生产、研发、销售、管理等各个环节，对于海量数据的采集、分析、挖掘、利用将为企业决策与运营提供重要帮助，数字资产将成为企业组织最重要的资产之一。数字化时代，数据信息在企业内部各业务模块、环节顺畅传递是企业实现数字化转型的必要条件。相比传统的本地部署模式，云计算具有快速部署、即接即用、弹性扩容、按需付费等特点，可以有效降低企业的使用成本，提升使用效率。针对海量数据处理所需要的巨大算力，云计算依托低成本、快速部署、弹性扩容等特点，可以随时提供强大的弹性伸缩的计算资

源。目前，云计算已经成为底层基础设施，企业实现数字化转型，离不开云计算等技术的发展，云计算、大数据等技术的大规模推广使用有助于实现企业内部的数字化改造，提升数据的运转效率，帮助企业最终实现数字化转型。

国家高度重视“新基建”，云计算成为新基建重要内容。基础设施的建设对于经济的发展至关重要，从 2018 年国务院在中央经济工作会议中第一次提出新型基础设施建设这个概念至今，已经累积超过 10 次中央级别会议或重要文件强调新型基础设施建设的重要性。进入 2020 年以来，国家关于新型基础设施建设的部署要求更加密集，政策路线更加清晰，其内涵也更加丰富。同时，全国各地也纷纷出台相关政策，不断加快“新基建”步伐，例如广东、湖南、浙江等省推进的云计算、工业互联网、物联网、5G、人工智能、区块链等重点项目，都在万亿规模。**“新基建”概念范畴广泛。**2020 年 4 月 20 日，国家发改委首次就“新基建”概念作出解释，新一代信息技术引领的新型基础设施建设也正式确定了其边界。“新基建”具体包含了信息基础设施、融合基础设施、创新基础设施三个方面。其中，**信息基础设施**主要是指基于新一代信息技术演化生成的基础设施，比如，5G、物联网、工业互联网、卫星互联网为代表的通信网络基础设施，以人工智能、云计算、区块链等为代表的新技术基础设施，以数据中心、智能计算中心为代表的算力基础设施等；**融合基础设施**主要是指深度应用互联网、大数据、人工智能等新技术，支撑传统基础设施转型升级，

进而形成的融合基础设施；**创新基础设施**主要是指支撑科学研究、技术开发、产品研制的具有公益属性的基础设施。

云计算是实现产业互联网落地的必要途径。产业互联网是互联网技术在特定产业领域的深度应用，其诞生打破了产业边界，实现了跨产业的网络连接、数据打通和业态创新。互联网概念早期应用于工业领域，随着扩展，有了产业互联网的概念，产业互联网是由互联网延伸出来的概念，是互联网技术与传统产业的结合，在传统产业间借助云计算、大数据、人工智能等，提升产业间的内部效率和对外服务能力，从而连接、重构传统产业，实现互联网+时代的转型升级。产业互联网的发展离不开各项互联网新技术的支撑，如物联网、云计算、大数据、人工智能、区块链等，云计算作为技术平台、基础设施，通过按需取用、按需付费、集中管理，使得 IT 对于业务的支撑更具弹性，技术壁垒和整体 IT 成本降低，为产业互联网云平台的搭建提供良好的基础。

2. 云计算威胁事件频发，安全建设需求迫切

安全性仍是云计算所面临的最大挑战。云计算出现以来，安全性一直是云计算所面临的最大挑战。数字化转型、新基建建设与产业互联网发展也对云计算的安全提出了新的时代要求。在云平台上，传统网络架构中的 DDoS、入侵、病毒等安全问题仍是常态；与此同时，针对云平台架构的虚拟机逃逸、资源滥用、横向穿透等新的安全问题

也层出不穷。数据安全是云计算安全的核心，云计算环境中，数据存储更为集中，一旦发生安全事件，后果影响重大。对于任何企业而言，数据都是最重要的资产，尤其是业务数据和用户数据，企业对于上云后数据的安全考量一直是在云中存储数据的主要问题之一。随着越来越多的企业将业务迁移到云上，将有更多的敏感数据驻留在云内，数据安全已经成为所有企业在产业互联网时代必须直面的挑战。目前，我国的云计算安全整体态势不容乐观，据国家计算机网络应急技术处理协调中心统计，2019 年，我国云平台网络安全事件或威胁情况进一步加剧，遭受 DDoS 攻击次数占境内目标被攻击次数的 74.0%、被植入后门链接数量占境内全部被植入后门链接数量的 86.3%、被篡改网页数量占境内被篡改网页数量的 87.9%。

重视云计算安全已逐步成为企业共识，根据信通院调查报告显示，私有云环境中，35.4%的企业在云安全上的投入占 IT 总投入的 10%-20%，7.6%的企业云安全投入占 IT 系统总投入的 20%以上；公有云环境下，42.4%的企业在选择云服务商时会考虑服务安全性。由于云计算架构的特殊性以及云计算平台安全的重要性，**普惠化将是云计算安全未来发展的必然趋势**。普惠具体指普及性与实惠型，随着安全新技术的演进，云计算安全防护的投入成本将会不断降低，帮助大规模云中中小企业，以可负担的成本，实现云中业务安全的运营，全面提升云计算行业整体安全性。

3. 传统安全防护有痛点，云上安全呈原生化发展趋势

云时代，上云成为大势所趋，各行各业在国家相关政策的推动下积极推进企业上云。与之相对，云上安全体系建设发展相对缓慢，企业在上云过程中，安全建设相对滞后，通常在云平台建设完成之后介入，作为补充措施保证云平台安全，仍以传统安全防护模式为主。传统的安全防护方案通过堆砌各类安全设备构建安全管理能力，存在硬件设备昂贵、安全资源利用率低、部署困难、云上数据难以获取、数据流通差、安全产品联动性差等弊端，安全的防护主要靠安全设备的叠加以及安全人员的投入，成本相对较高，尤其对于中小企业来说，安全成本相对较大。**云上安全原生化有助于实现普惠安全**，在企业上云，云平台建设过程中考虑融入安全建设有助于解决传统安全防护模式存在的弊端。云上安全原生化将安全能力内置于云平台，云产品云化部署，实现数据联通，安全产品联动，充分利用安全资源，降低安全解决方案使用成本，实现真正意义上的普惠安全。

（二）云原生安全理念兴起

为缓解传统安全防护建设中存在的痛点，促进云计算成为更加安全可信的信息基础设施，助力云客户更加安全的使用云计算，云原生安全理念兴起，国内外第三方组织、服务商纷纷提出以原生为核心构建和发展云安全。

Gartner 提倡以云原生思维建设云安全体系。基于云原生思维，Gartner

提出的云安全体系覆盖八方面，如图 1 所示。其中，基础设施配置、身份和访问管理两部分由云服务商作为基础能力提供，其它六部分，包括持续的云安全态势管理，全方位的可视化、日志、审计和评估，工作负载安全，应用、PaaS 和 API 安全，扩展的数据保护，云威胁检测，客户需基于安全产品实现。

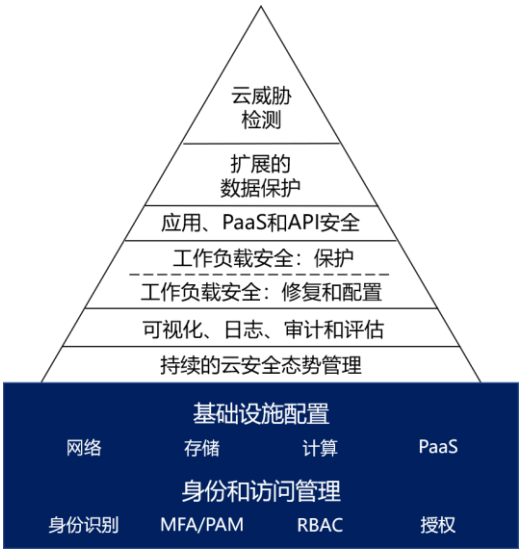

图 1 Gartner 云原生安全体系

Forrester 以 37 项指标评估公有云平台原生安全能力。Forrester 认为公有云平台原生安全（Public cloud platform native security, PCPNS）应从三大类、37 个方面去衡量，如表 1 所示。从已提供的产品和功能，以及未来战略规划可以看出，一是考察云服务商自身的安全能力和建设情况，如数据中心安全、内部人员等，二是云平台具备的基础安全功能，如帮助和文档、授权和认证等，三是为用户提供的原生安全产品，如容器安全、数据安全等。

表 1 Forrester 公有云平台原生安全能力指标

战略	已提供产品/功能	市场表现

物理安全计划	数据中心	总收入
认证计划	认证	PCPNS 收入
IAM 计划	用户管理	PCPNS 收入增长
Hypervisor 安全计划	授权和认证	PCPNS 直接的安装基数
Guest OS 工作负载安全计划	Hypervisor 安全	PCPNS 间接的安装基数
网络安全计划	操作系统和容器安全	北美表现
安全日志和审计计划	存储和数据安全	中南美表现
机器学习计划	网络安全	欧洲、中东和非洲表现
客户满意度	审计	亚太表现
供应商 RFP 响应	帮助和文档	
供应商 PoC 和展示	导航和综合环境	
服务和合作伙伴		
研发人员配备		
销售人员配备		
支持人员配备		
供应商透明度		
价格条款和灵活性		

VMWare 通过三大特征阐述原生安全理念。VMWare 认为原生安全探讨了信息安全建设与管理的转型，具备三大特征，一是内建而非外挂，二是主动而非被动，三是整合而非孤立。聚焦到虚拟化平台，原生安全理念有三大优势，一是对负载有更好的理解，基于负载的逻辑标识和虚拟化平台的逻辑分组来制定安全策略；二是无需部署额外的程序，独立于负载存在；三是通过与平台集成获得了更好的控制力，发现威胁后可以更积极主动应对。

深信服提出云原生安全体系应具备的三大基本能力。深信服认为云原生的安全体系应当是“全面面向云环境、基于云交付、可弹性扩展”的架构，应具备三方面的能力：一是能够对云环境下面临的新风险和威胁形式进行检测与响应，例如云的不当配置、云 API 恶意调用、云 API 密钥泄露等；二是云原生安全体系中各安全组件和能力，应支

持部署于云环境（云主机、容器等），以实现安全能力的服务化和弹性交付；三是覆盖私有云及各公有云环境，为企业级客户提供统一、有效和易用的云安全能力和解决方案。

二、云原生安全推动安全与云深度融合，促进安全普惠

（一）云原生安全定义

国内外各组织、企业对云原生安全理念的解释略有差异，结合我国产业现状与痛点，我们认为，云原生安全**指云平台安全原生化和云安全产品原生化。安全原生化的云平台，一方面通过云计算特性帮助用户规避部分安全风险，另一方面能够将安全融入从设计到运营的整个过程中，向用户交付更安全的云服务；原生化的云安全产品能够内嵌融合于云平台，解决用户云计算环境和传统安全架构割裂的痛点。**

作为一个全新的安全理念，云原生安全旨在将安全与云计算深度融合，推动云服务商提供更安全的云服务，帮助云计算客户更安全的上云。

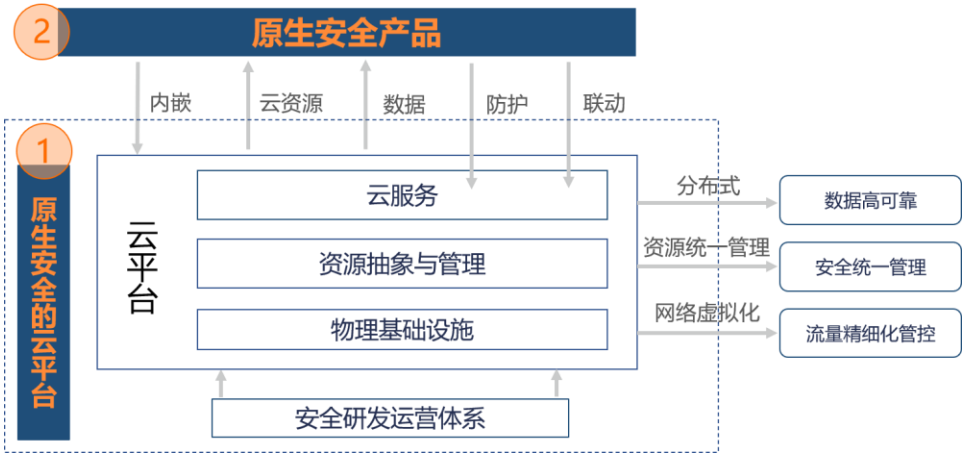

图 2 云原生安全架构

（二）原生安全的云平台，向客户交付更安全的云服务

云原生安全强调云平台安全原生化，一方面借助云计算特性，另一方面云服务商从云平台的设计阶段起考虑安全因素、纳入解决方案，将安全前置，让**云计算成为更安全可信的新型基础设施**。

云计算特性规避部分安全风险。与传统 IT 环境相比，云计算具备多种特性优势。上云后，借助和利用云计算特性，云计算客户面临的部分安全风险迎刃而解，主要体现在：1）云计算采用分布式存储的方式，保证了数据的高可靠性，降低数据丢失风险；2）云计算资源的统一管理助力企业摆脱复杂化、碎片化的安全管理模式，实现统一的安全管理；3）借助于云计算的网络虚拟化能力，企业可以更加清晰的掌握自己云环境内东西向流量的情况，实现更加精细化的流量隔离与管控。

从研发阶段关注云计算安全问题，前置安全管理。针对云服务的安全，通过在产品研发全生命周期便融入安全措施来提升云服务质量，覆盖云服务研发运营整个过程，降低解决安全问题的成本，具体措施如图 3 所示，包括：1）**管理架构**，建立合适的人员组织架构与制度流程，保证研发运营流程安全的具体实施；2）**安全培训**，针对人员进行安全培训，增强安全意识，进行相应考核管理；3）**明确安全要求**，前期明确安全要求，如设立质量安全门限要求，进行安全审计，对于第三方组件进行安全管理等；4）**安全需求分析与设计**，在研发阶段

之前，进行安全方面的需求分析与设计，从合规要求以及安全功能需求方面考虑，进行威胁建模，确定安全需求与设计；5）**安全研发测试**，搭配安全工具确保编码安全，同时对于开源及第三方组件进行风险管理，在测试过程中，针对安全、隐私问题进行全面、深度的测试；6）**安全发布**，服务上线发布前进行完整性审查，制定事先响应计划，确保发布安全；7）**运营安全**，上线运营阶段，进行安全监控与安全运营，通过渗透测试等手段进行风险评估，针对突发事件进行应急响应，并及时复盘，形成处理知识库，汇总运营阶段的安全问题，形成反馈机制，优化研发运营全流程。8）**服务停用下线，**制定服务下线方案与计划，明确隐私保护合规方案，确保数据留存符合最小化原则。

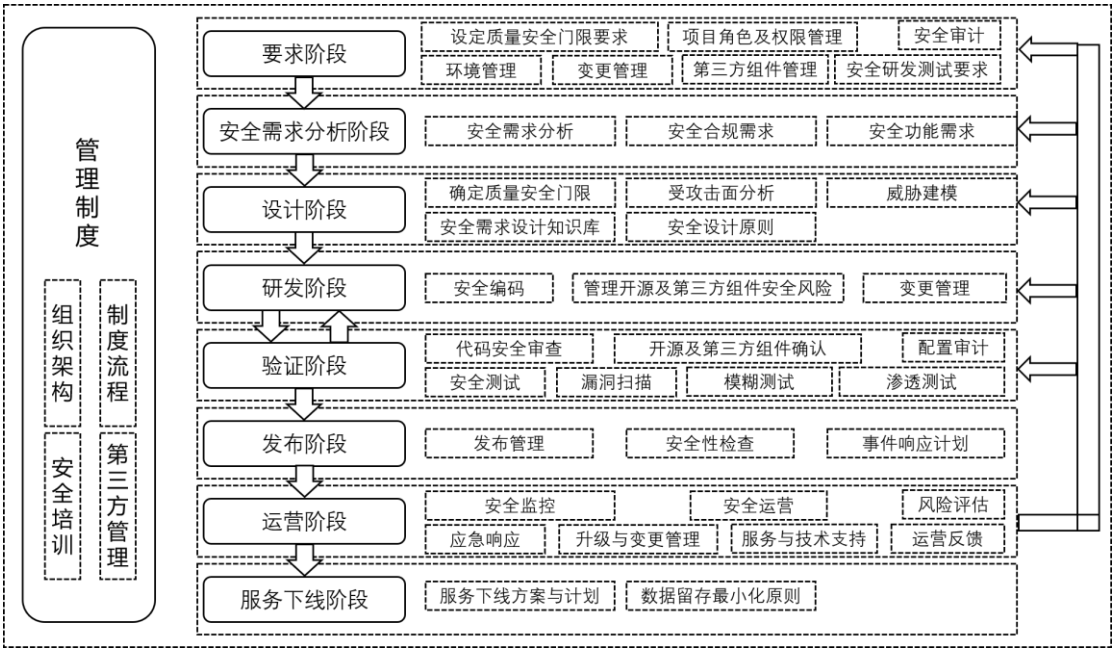

图 3 可信研发运营安全体系

关于安全前置的实现，目前业界的共识为通过安全解决方案将安

全融入现有研发流程，不破坏现有的研发环境。Gartner 也提出要使用安全测试工具和流程去适应研发人员，每个人为安全负责，不同角色协同共建安全；并通过构建安全工具链，整合安全流程，在 CI/CD 流程嵌入安全自动化检查等方式；使用工具和方法来最大程度降低对于研发人员的影响，提升安全效率，应对新的开发运维模型。核心的自动化测试能力主要包括**静态应用程序安全测试、动态应用程序安全测试、交互式应用程序安全测试、软件组成分析、运行时应用自保护**。

（三）原生安全产品，为客户云上安全提供更有力保障

云原生安全强调安全产品原生化。服务商提供内嵌于云、能够有效解决云上安全风险的原生安全产品；云计算客户能够利用原生安全产品，建设与云计算环境融合的安全体系与架构，规避传统安全架构与云计算环境割裂等问题，更加安全的使用云计算。

内嵌于云的原生安全产品，能够充分了解和利用云平台，最大限度发挥安全防护能力，极大程度提升云计算客户体验。原生安全产品特性和优势主要体现在四方面：

采用内嵌的方式而无需外挂部署。内嵌的方式具备多种优势，**一是无需安装**，云计算客户通过简单配置即可使用，与外挂部署相比更加便捷；**二是运行更加稳定和安全**，外挂部署通常基于代理实现，代理本身存在一定的安全和稳定性风险，同时代理的部署也可能对云上

IT 系统造成影响，而原生安全产品与云平台相融合，与外挂部署相比运行更加稳定和安全。

充分利用云平台原生的资源和数据优势。一方面，原生安全产品利用云计算的计算、存储、网络等资源，实现自身安全防护能力的弹性扩容，解决传统安全产品数据存储空间受限、计算能力不足等问题；另一方面，与传统安全产品相比，原生安全产品能够更便捷、全面的获取云平台内数据，通过整合、关联分析云平台内各类数据，深入挖掘潜在安全风险。

与客户云资源、安全产品有效联动，原生安全产品因与云平台深度融合，能够对云资源进行更有力的控制，各原生安全产品间能够有效协同，**一是能够自动识别云资源**，迅速感知云资源的状态和信息；**二是对风险资源进行主动处置**，在发现安全事件时，不仅仅生成告警信息，还能够自动联动相关云资源或其它原生安全产品，对安全事件采取处置措施和防护手段，实现从检测、告警到处置的安全运营自动化闭环。

解决云计算面临的特有安全问题。与传统 IT 系统架构相比，云计算因引入新技术、运营模式变化等原因，面临新的安全风险，如虚拟化、容器技术实现了 IT 资源的细粒度隔离，物理设备不再是资源承载调度的最小单元，物理安全边界消失，用户之间、用户与云平台间的安全隔离十分关键；云计算资源按需分配，可随时释放，动态性强，资源的迅速识别和有效管理成为难点；云服务的不当配置是造成

云上安全事件的重要原因……原生安全产品能够充分考虑云计算面临的新安全风险，为客户云计算环境提供更有力保障。

（四）云原生安全体系促进实现安全普惠

与传统 IT 系统架构相比，云计算将资源和数据的所有权、管理权和使用权进行了分离，云上安全由云服务商和云客户共同分担，云计算责任共担模式成为业界共识。只有云服务商和云客户双方切实承担云计算安全责任，才能确保云客户业务的安全运营。

云计算安全责任可分为三种，**一是由云服务商完全承担的责任**，云服务商承担保障云平台安全性的责任，包括数据中心、基础架构、虚拟化平台等云平台底层设施的安全责任，以及交付给用户的云服务、云服务 API、云控制台等自身安全性；**二是云服务安全属性与配置相关的责任，**云服务商主要承担着为云客户提供基础的云服务安全功能和属性的责任，云客户利用云服务商提供的云服务安全功能和属性，对其进行合理的配置，以更加安全的使用云服务；**三是云客户完全承担的责任，**云客户通过自建安全体系承担此部分安全责任，以保障自己云上业务和数据的安全。

目前，针对上述安全责任的承担，存在诸多问题。**一是云服务商在研发运营中安全介入相对滞后，无法有力保障云平台安全性。**为追求应用服务的快速研发部署，传统研发运营安全通常在应用服务构建完成及上线运营后才介入安全，进行安全扫描、威胁漏洞修复，研发

阶段代码层面的安全无法被覆盖，安全漏洞修复成本更大；**二是云服务原生安全属性有差异。**各云服务商提供的云服务原生安全属性，如 API 安全策略、控制台权限管理、安全组等，在精细化、灵活性、操作性等方面水平参差不齐，增加了云客户合理配置云服务安全属性的难度；**三是云客户自身安全能力不足。**云客户因安全技术薄弱、安全预算有限、安全建设与安全要求无法匹配等问题，导致自建的安全体系无法切实承担本该承担的安全责任。

云原生安全体系强调更安全的云服务和更安全的上云，能够有效缓解上述问题，全面保障三种云计算安全责任的落实，让安全惠及各类上云客户。

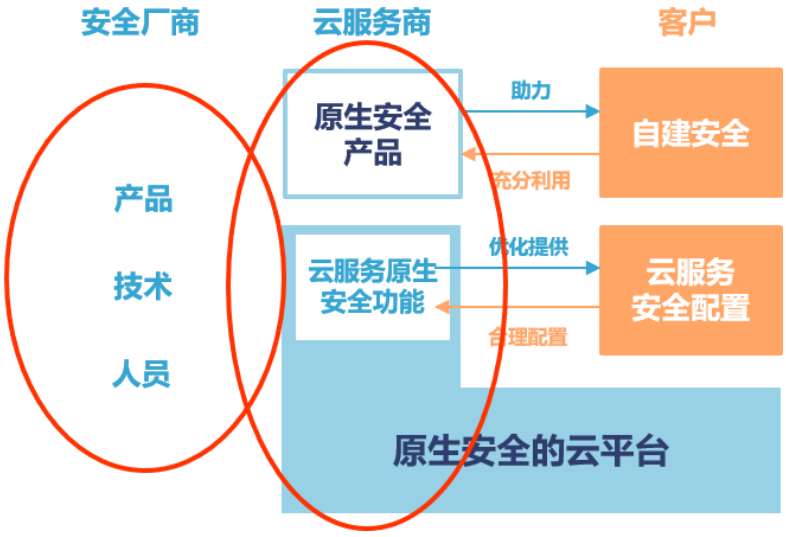

图 4 云计算安全责任与云原生安全体系关系

1.提升云平台整体安全性，满足客户基本安全需求

云平台安全原生化鼓励云服务商建立新型研发运营安全体系，进行安全左移，促进云平台整体安全性的提升。

一方面，**云平台安全性是客户云上安全的基石**。与大部分云客户相比，云服务商具备更强、更专业的安全技术和管理能力。当云计算平台深度融合了云服务商的技术与安全能力，云客户在此基础上使用云服务，一些安全责任由云服务商承担，部分安全问题已被云服务商解决，云客户无需再关注，与云客户以往自建 IT 架构相比，将更加安全便捷。尤其对于个人客户，可能更加追求云资源使用的快速便捷而没有资金和精力进行安全投入，选择一个深度融合安全的云平台，安全保障水平便能够满足大部分时间的要求。

另一方面，**云服务原生安全属性的发展将满足客户的基本安全需求**。安全左移强调云服务商在产品上线之前，更早的进行安全动作的执行，如在研发前进行安全方面的需求分析与设计，从用户视角优化设计并提供云服务安全功能，引导客户安全的使用云服务，让客户使用更加放心，配置更加便捷，丰富的云服务安全属性能够满足客户，尤其是个人客户和小型企业的基本安全需求；在研发阶段也需要做代码检查等，包含关注第三方组件安全；同时可以通过交互式应用测试等手段进行上线前的安全测试，将安全问题在上线前收敛，提供给用户原生安全的云服务。

2.原生安全产品不断丰富，解决客户多场景安全痛点

企业级客户往往安全要求高、业务场景复杂，云平台基本的安全性不足以完全契合客户实际需求，客户需通过采购安全产品构建自身

的云上安全体系。但传统安全产品使用复杂、成本高，增加了客户，尤其是中小企业的应用门槛。而原生安全产品依托其特性与优势，能够缓解企业因技术、资金、人员等条件受限而导致的安全缺失，有效应对企业级客户在主机、数据、网络、安全管理等不同安全场景下的需求与痛点。

云原生计算环境安全适应云上计算环境新安全需求。随着企业信息建设云化程度加深，云主机、容器等计算环境内部署的业务越加开放和复杂，固定的防御边界已不复存在，安全需求升级。1）**黑客攻击日益频繁，传统防护机制作用有限**。云主机、容器成为黑客入侵的主要目标，时刻面临暴力破解、加密勒索、挖矿等安全威胁，对黑客行为检测提出更高要求；2）**新漏洞层出不穷，安全漏洞应急响应难**。云主机、容器内部署的第三方软件、开源组件，新漏洞不断被发现且极易在短时间内被黑客利用，企业难以迅速获取重多来源的漏洞公告信息、对漏洞风险进行深入评估；3）**业务资产组件多，亟需有效清点和管理**。随着企业业务快速增长，云主机、容器中部署的软件版本类型众多，需对所有软件进行识别与管理，掌握软件安全现状，以在安全事件发生时，快速统计业务受影响情况。云原生计算环境安全产品能够有效适应上述云上计算环境安全新需求，帮助客户构建计算环境安全防护体系。

云原生安全发掘云上数据潜在风险。随着信息化深度日益加深，业务数据上线给 IT 信息化带来了高效便捷的好处，但同时也隐藏着

相应的数据风险。1）**数据系统分散，缺乏集中审计监控**。各数据库虽然有自己的日志，但数据内容无法统一，且各数据库访问行为之间无法做到关联分析，对全局数据安全态势没有整体了解，这将给信息系统管理带来巨大的隐患；2）**内部防范措施不到位，内网人员有机可乘**。内部人员更易接触企业敏感信息，了解企业在技术、管理等方面的薄弱环节，恶意内部人员可以利用相应漏洞对企业内重要系统、数据进行违规操作，造成数据泄露、删库等重大安全事件；3）**泄密事件追溯难**。企业发生云上重大数据泄露事件后，必须进行全面的事件还原和追责处理，但往往因数据访问者多、泄密途径不确定等原因，导致定责模糊、取证困难，无法进行有效的事件追溯；4）**数据安全管理需求迫切**。数据成为企业越来越重要的资产，随着企业业务向云上的迁移，大量敏感、重要数据分散的存储于云上，企业亟需对云上数据进行分级分类管理，掌握数据的流转情况，确保数据安全符合各种法律发规的要求。云原生数据安全产品能够有效发掘上述安全风险与隐患，为客户云上数据安全保驾护航。

云原生安全有效应对云上网络威胁。云计算促进企业数字化转型加速的同时，网络安全面临的威胁也在不断变化和升级。1）**DDoS 攻击泛滥，影响各行各业业务正常运营**。随着公网带宽逐渐增大，DDoS 攻击成本日益降低，而攻击技术也在不断升级，DDoS 攻击愈加频繁，游戏、互联网、金融、政务等重点行业遭受 DDoS 攻击后，对外业务受阻严重，用户体验；2）**大量公网端口暴露在互联网中，内外流量管**

控难。客户在云上可以快速便捷的申请公网 IP，尤其对于大型企业，公网 IP 数量庞大，导致大量公网端口暴露在互联网中，如何对公网 IP 地址进行统一管理，对由内到外或由外到内的流量进行有效管控，成为难题；3）**VPC 间流量控制成关键**。与基于安全域的传统网络不同，客户以 VPC 为基础构建云上网络结构，VPC 间细粒度的访问控制和流量可视化是云上网络安全的重点；4）**BOT 访问流量突增**。云时代，Web 应用或 APP 服务成为越来越多企业承载核心业务的选择，面临的 BOT 访问流量不断增加，若无法有效区分友好 BOT 和恶意 BOT，将对企业业务运营造成影响，导致信誉、经济等的损失。云原生网络安全产品能够有效应对上述网络威胁，全面保障客户云上网络安全。

云原生安全应对云上安全管理新挑战。云计算发展迅速，企业传统安全管理思路已无法有效应对云时代的安全新挑战。1）**资产管理范围变化，云上影子 IT 风险增加**。与云下传统资产相比，云上资产概念扩大，如对象存储、云数据库、容器等 PaaS 或 SaaS 层服务均在资产管理范围内，同时云资源灵活随需取用，资产无时无刻在发生变化，增加了客户的资产管理难度，易存在影子资产；2）**云产品配置风险隐患大，配置管理至关重要**。各类云产品的安全配置，是影响云产品安全使用的重要因素，但配置分散在各个云产品中，缺乏有效的统一管理和检查，容易产生配置风险隐患；3）**云上威胁概念扩大，安全事件检测与管理能待提升**。除传统的主机威胁、流量威胁、Web 安全威胁等，云上环境还面临新的威胁，如云服务 API 的异常调用、API

Key 泄露等，安全运营需覆盖云上新型威胁的检测与响应。云原生安全管理产品能够有效迎对上述新挑战，助力客户建设云上安全管理体系。

三、云原生安全助力企业安全体系建设

（一）云原生计算环境安全

1.原生主机安全

原生主机安全通过资产管理、漏洞管理、基线检查、病毒检测、入侵检测、威胁响应与处置，实现云上工作负载（Workload）的安全防护，主要具备如下原生特征:

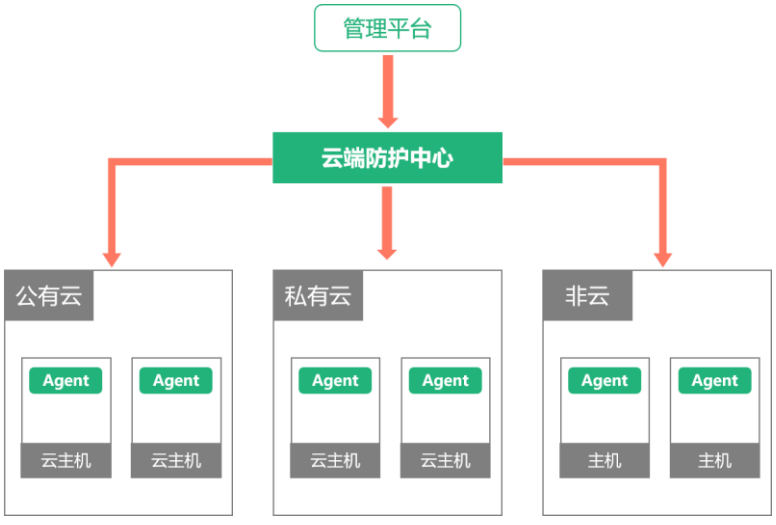

图 5 原生主机安全

轻量部署，便捷稳定。以轻量 Agent 与云端防护中心结合的方式实现主机安全，Agent 负责将主机内安全数据上报云端防护中心，同时响应云端防护中心下达的指令，绝大部分的计算与防护功能在云端

进行。Agent 采用稳定性高的数据采集与监控技术，对服务器的资源消耗低，不影响用户业务的正常运营。同时，以安装包、命令行、批量安装等多种方式，让用户更加便捷的实现在云主机或非云主机上的部署。

以工作负载为核心。随着云计算的发展，承载计算的节点不再仅仅是云主机和云数据库，容器、无服务成为越来越多用户的选择，安全防护不能仅关注主机层面的威胁。原生主机安全从云工作负载视角出发，对主机层面、容器层面及其上承载的数据库等工作负载进行全面的安全防护。

自动化获取信息，智能化主动防御。与主机进行联动，一方面自动化获取主机内各类资产的信息；另一方面，支持自动查杀病毒木马，主动防御入侵行为，自主完成漏洞基线修复，构建安全闭环和可感知能力。

海量数据关联分析。利用采集到的主机内各类数据，如进程、文件、系统、DNS 等的行为日志，结合云平台全网威胁情报数据，基于 AI 算法，实现多维度、高效的关联分析，提升威胁检测率与准确率。

表 2 原生主机安全产品主要功能

功能	详情
资产管理	能够对主机及主机内资产进行清点和管理，包括端口、账号、进程、软件、容器镜像等。
漏洞管理	能够对主机内系统、软件、Web 应用漏洞进行识别和预警，包括 Linux、Windows 操作系统漏洞，容器镜像漏洞，Apache、Mysql 等软件漏洞，Web-CMS 漏洞等。
基线检查	能够对主机内风险配置进行识别，包括弱口令、密码策略、

	影子账户等账号安全检测，注册表配置、Nginx 配置、数据库配置等配置检测。
病毒检测	能够对主机内的恶意文件进行扫描，包括 Webshell 后门、勒索病毒、挖矿程序等。
入侵检测	能够对主机的入侵行为进行实时预警，包括异地登陆、暴力破解、非法时间登录、非法 IP 登录等异常登录行为，提权、反弹、命令执行、关键文件变更、网页篡改等主机内异常行为。
威胁响应与处置	能够对主机内存在的威胁提供响应与处置手段，包括漏洞一键修复、系统加固建议、入侵行为自动拦截、恶意文件自动隔离和查杀等。
事件溯源	能够对安全事件进行详细记录，为用户追溯事件提供依据。

通过原生主机安全产品，可以有效保障云上主机及主机内资产的安全，原生主机安全的典型应用场景如下:

业务资产组件清点。对于业务增长快速、主机及内部组件繁多的企业，可以利用原生主机安全，实现云上主机和组件的快速识别和管理，构建企业资产组件全景图。

安全漏洞应急响应。对于没有专业安全团队，或安全团队人员不足的企业，可以利用原生主机安全，实现云上主机和组件的快速漏洞检测和修复，第一时间获取最新漏洞信息，提升漏洞应急响应效率。

互联网业务入侵行为检测。对于配置公网 IP、部署互联网业务的云主机，时刻面临黑客的渗透和自动化攻击，企业可以基于原生主机安全，对暴力破解、本地提权、高危命令等入侵行为进行检测和处置。

2.原生容器安全

原生容器安全通过安全策略、镜像检测、合规基线检测、运行时检测和防护、容器网络隔离、安全运行环境，实现云上容器的安全防

护，主要具备如下原生特征：

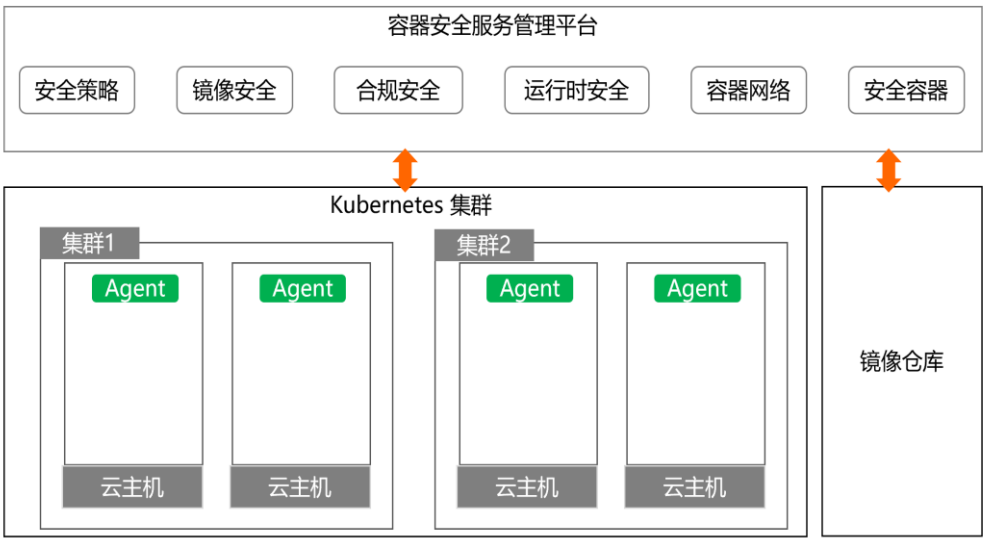

图 6 原生容器安全

轻量 Agent，快捷部署。用户根据业务的需要选择需要防护的集群节点，一键开通，以轻量 Agent 与云端容器安全服务管理平台结合的方式实现容器安全，占用低能耗，不影响其他容器的运行。Agent 负责接收管理平台下发的防护策略，实现用户节点的容器安全防护，并将告警数据上报到防护中心。

统一策略管理。统一管理用户容器的安全策略，用户自定义规则和一键下发，统一管理用户集群中所有节点上的容器和镜像防护状态。

丰富的漏洞库和规则库。包含有丰富的漏洞库并及时更新，有效发现镜像漏洞，内置常见的检测逃逸，帮助用户有效发现木马，提权等恶意攻击行为，并告警通知用户。

表 3 原生容器安全产品主要功能

功能	详情
安全策略	能够对容器的镜像、运行时、网络等设置安全策略，通过告警或者阻断的方式发现并修复风险。

镜像检测	能够对镜像仓库的镜像进行检测，识别镜像中的漏洞并预警。包括 OS 系统漏洞，应用漏洞（Nginx，Redis 等），恶意木马程序，不安全的配置等。
合规基线检测	能够对容器服务的合规配置、容器启动运行时的合规配置等进行合规检测，并输出检测报告，例如：Docker daemon，Audit rule 配置文件权限。 能够检测容器是否满足业界合规标准，例如：NIST-SP800-190，GDPR，HIPAA，PCI，CIS 等。
运行时检测	能够在容器运行过程中，发现容器内异常行为并进行实时告警，包括恶意木马/病毒程序运行，恶意文件访问，恶意系统 API 调用等行为，例如：Dirtcow 漏洞，敏感目录访问/etc/passwd，恶意系统调用 mount 等。
容器网络	能够自动发现网络拓扑并可视化展现，能够对容器间的东西/南北向访问进行访问控制策略控制，能否对容器间做 7 层的访问检测和告警。
安全容器	能够为容器提供安全的运行环境，在容器被恶意入侵时，防止入侵扩散和逃逸到主机。例如：kata/gvisor 容器。

通过原生容器安全产品，可以有效保障云上容器资产的安全，原生容器安全的典型应用场景如下：

CI/CD。在 DevSecOps 中将容器集成到 CI/CD 的原生工具中，而不是事后发现和修复安全漏洞，可以使开发人员能提前反馈其代码的安全状态。

部署。在 Docker Hub 下载的镜像也会存在漏洞，开源镜像的使用加剧了镜像漏洞的问题，通过镜像检测来发现镜像漏洞问题和快速修复，确保投入到生产环境的镜像是安全的。

运行。容器运行过程中，行为无法预测，存在木马、应用漏洞等风险，通过运行时监控发现和防御这些风险，实现容器上的漏洞快速检测和修复，提升漏洞应急响应效率。

3.原生应急响应和取证

原生应急响应和取证采用端上应急检测数据，结合安全运营中心、蜜罐、威胁情报等数据进行智能化数据分析，实现应急响应主动和被动流程、溯源取证的自动化。主要具备如下原生特征：

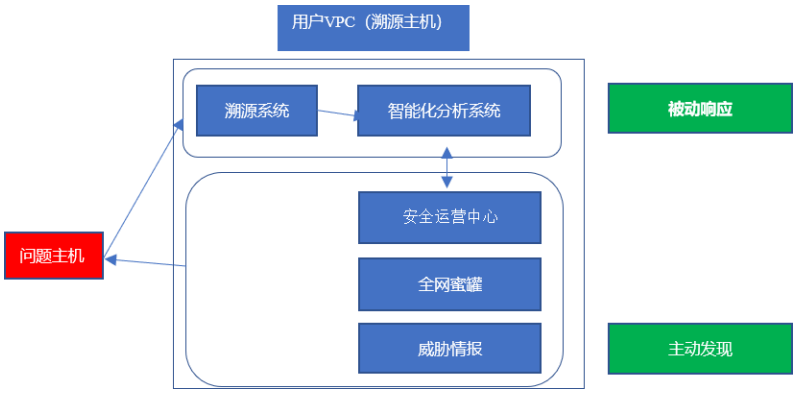

图 7 原生应急响应和取证

易于部署。用户无需关注硬件或软件的安全部署，可以通过统一控制台一键开启应急响应和取证功能。

易于扩展。用户通过提供云主机列表和授权秘钥，可同时对多台云主机进行溯源取证。

与云平台紧密结合。充分结合云平台特点，采取自动快照、数据镜像、加载快照、挂载镜像的方式突破网络限制、系统损坏等极端场景。结合云安全运营中心、全网蜜罐、云威胁情报数据提前感知威胁，并和后期智能化分析联动，突破无日志溯源取证场景。

自动化响应与取证。能够对整个入侵痕迹进行分析，输出可能的入侵途径和处置方案；根据分析结果输出格式化的证据链。

数据安全可靠。溯源操作由用户账号发起授权，系统运行环境和

资源均在用户 VPC 内，证据数据和分析结果也均保留于用户 VPC 空间之内。

表 4 原生应急响应和取证产品主要功能

功能	详情
溯源分析	通过对日志、数据进行分析，调查黑客入侵行为，完成安全事件的溯源取证。
智能化数据分析	基于云安全运营中心、全网蜜罐、云威胁情报等数据，进行自动化智能分析。
溯源报告与证据	根据分析和溯源结果，提供溯源报告，生成格式化证据链。

原生应急响应和取证的典型应用场景如下:

查找入侵原因，完成电子取证。对网络攻击、恶意程序、数据篡改与泄露、Web 恶意代码等黑客入侵事件进行分析，掌握黑客入侵手法和路径，实现电子证据的生成和留存。

降低应急时长，快速恢复业务。自动化、智能化进行海量数据分析，能够同时对大量被入侵主机进行响应和溯源，减少人工投入，通过标准化的应急响应流程提升响应效率，降低应急时长，帮助用户快速恢复业务。

（二）云原生数据安全

1.原生数据安全分类治理

数据分类治理是云原生数据安全的基础，包括对云上流转数据的发现和分类分级，并对敏感数据的泄露进行监测与拦截。主要具备如下原生特性:

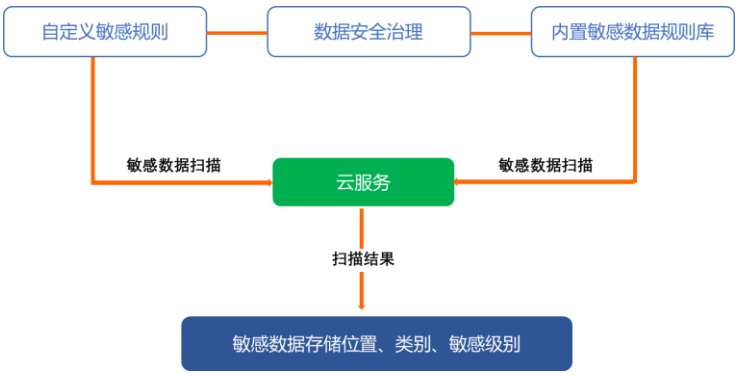

图 8 原生数据安全分类治理

云数据资产对接。深度对接云上各类数据库、存储产品，可完全适配用户云上数据资产，并从内核维度获取更详细的日志信息。

全面数据风险监控。对云主机中使用的数据进行深度内容分析，监控敏感数据泄漏和发现敏感信息隐患存储；对 API 接口数据进行监控，及时了解 API 接口安全状态及数据泄露风险，从事前-事中-事后三个维度实现对 API 接口风险的收敛。

表 5 原生数据安全分类治理产品主要功能

功能	详情
数据资产对接	在取得授权的前提下，深度对接云上不同类型的数据库、存储系统，从内核维度获取最及时的数据资产信息。
数据资产可视化	可结合已发现的敏感数据内容，针对性的审计并展示数据存储位置、访问者位置以及数据资产流动变化信息，定位敏感数据。
API 接口监控	采用自动化接口发现技术，能够将网络流量中大量的 URL 进行聚合归类，提取参数配置，还原接口的技术设计形式，同时按照接口资源类型展示各类接口。通过敏感数据识别引擎识别接口返回内容中包含的敏感数据类型并对接口进行打标。
数据风险监控	对数据行为建立基线，包括用户基线、接口基线、系统基线，并利用前沿的异常检测技术，从多个维度来识别异常数据访问行为，并形成最终的风险评分，对高风险行为进行预警。

原生数据安全分类治理的典型应用场景如下：

敏感数据发现与分类。云原生数据安全分类治理深度对接云上不同类型的数据库、存储系统，在取得授权前提下，从内核维度获取最及时的数据资产信息，并针对性的发现相关敏感数据，对其进行分类分级，帮助企业从安全角度梳理数据资产，并满足符合行业法规的相关要求。如自动提供各类存储实例清单，包括未加密的存储实例、可公开访问的存储实例以及共享的存储实例的列表，并将机器学习、模式匹配技术应用于目标存储实例，识别敏感数据，并发出警报，具体包括个人身份信息(PII)、财务数据、客户信息数据等。

API 接口安全监控。云上大量数据通过 API 应用程序接口流转，API 接口已成为云数据安全风险度最高暴露面之一。API 接口的开发、配置缺陷等问题将带来鉴权机制失效、敏感信息暴露、数据滥用或由漏洞问题带来的海量数据泄露风险。API 接口安全监控以事前-事中-事后模式，实现对 API 接口风险的收敛，事前，对暴露面进行全面分析，包括应用系统 API 接口梳理、API 脆弱性分析；事中，建立用户、接口、账号、系统多维度数据行为基线，识别异常数据访问行为；事后，通过接口级细粒度的访问日志，实现审计溯源及合规需求。基于 API 监控，用户可全面感知业务接口、重要程度、流动数据，及时了解 API 接口的新增、变更、失活等情况，并进行必要性和安全性评估。

泄露监控。通过数据防泄漏对云主机中使用的数据进行深度内容分析，监控敏感数据泄漏和发现敏感信息隐患存储。准确判定定位敏感数据，对敏感数据在传输中的使用行为及存储行为进行监控，实现

敏感数据的保护。数据防泄漏通过云管控中心统一下发策略，获取数据进行检测，并根据检测结果进行的处置，包括记录、告警、阻断、隔离、加密、分类、启动工作流审批等。

2.原生数据安全审计

原生数据安全审计系统可挖掘数据库运行过程中各类潜在风险和隐患，对企业网络中的数据库各类会话信息、访问操作、SQL 语句进行全量双向审计、分析、告警以及日志归档留存，保障数据库安全运行，主要具备如下原生特性：

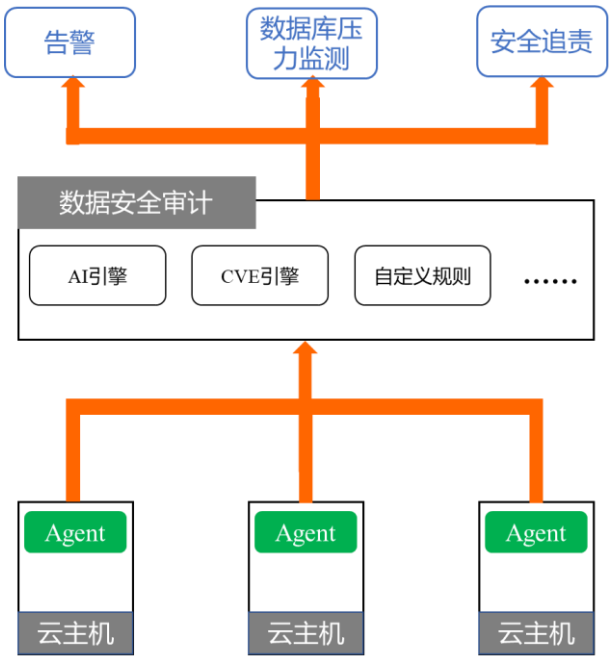

图 9 原生数据安全审计

一键开通，快速部署。用户只需根据自身业务数据库情况，一键开通数据安全审计服务，无需调整数据库属性或安装部署软硬件设备，通过简单配置 Agent 与数据库实例，实现各类数据库相关信息数据的获取，进行安全审计。

依托云计算资源，审计性能弹性伸缩。依托于云平台计算、存储、网络资源弹性扩缩容的特点，可以根据审计数据库台数、QPS 等数据情况，实现数据安全审计性能弹性扩展。

基于人工智能、威胁情报，进行威胁全方面识别。基于云平台丰富的样本训练环境以及共享的威胁情报等数据，对于威胁攻击、恶意操作以及各类变体攻击及非常见威胁操作实现监控。

支持各类数据库，实现数据系统统一管理。通过安装 Agent，配置数据库实例，设置审计组等方式，对于分散的数据系统进行统一集中审计监控。

表 6 原生数据安全审计产品主要功能

功能	详情
智能检测基线建立	依托深度学习技术与实时流量样本学习，能够应对变化多端的攻击场景，对各类变体攻击及非常见威胁操作自动识别，检测、记录，以及威胁告警。
数据库威胁防护	结合安全情报与 CVE 引擎，能够根据威胁攻击、恶意操作、SQL 注入的流量特征对安全事件进行告警。
自定义规则审计	支持按照库、表、访问源、数据库实例等多种维度进行审计规则设置，安全策略灵活自由，可实现精细化监控；还能根据不同场景不同类型的应用进行个性化定制，掌控数据库访问信息。
风险报表	基于总体概况、性能、会话、语句、风险多层面，结合图表统计和详尽展现。
语句压力预警	支持将动态会话信息整合成实时语句压力预警，从网络层面为管理员提供数据库语句压力与实时流量图标展现。
业务审计	支持全量双向会话审计功能，覆盖数据库所有的 SQL 操作。会话审计类别齐全，存储周期满足合规性要求，为各类数据操作行为进行详细溯源，对于数据库安全事件追责提供支持。
运维审计	审计业务系统与数据库之间的操作，能够对数据库日常运维的 DBA 进行审计。审计内容包括登录时间、所用账户、SQL 语句类型、SQL 内容等信息，以及

	常用运维协议，如：ssh、telnet、nfs 等，确保 DBA 的行为在受控范围内。
威胁告警	在威胁操作被识别瞬间，通过告警向相关管理员发送操作的源 IP、所用账户、操作语句等各项信息。支持多种告警途径确保警报能及时到达管理员处。

原生数据安全审计的典型应用场景如下:

感知危险操作。数据库可能面临来自内外网络的蓄意攻击，以及内部人员各类误操作导致的数据损失。当这些危险操作发生时，数据安全审计能够立刻检测出攻击源、攻击目标、攻击事件、操作的库表字段内容、所用语句、执行情况、返回信息与数据等信息，并且及时产生告警，确保管理员第一时间能够掌控威胁情报，应对数据库安全问题。同时，数据安全审计还能够将危险操作进行分类，按照影响范围、威胁程度分为高中低三级，让管理员在海量威胁告警中精准定位最紧急的事务，确保高威胁事件得到充分处理。

监控数据库压力。数据库风险除了恶意攻击和危险操作外，还来自于过高的 SQL 压力所导致的宕机等性能问题。数据安全审计能够全面监控当前各数据库的实时语句和流量压力，协助管理员了解当前数据库系统的网络性能概况，为管理员排查语句压力问题提供有力依据。

安全事件追责。当数据库系统出现数据被删除、信息被篡改、敏感信息被泄露等重大安全事件时，要进行全面的事件还原和追责处理。数据安全审计通过归档以及 SQL 语句存储，在发生安全事件时，通过对长时间跨度的历史信息进行深度检索，能够清晰的将安全事件进行

全貌还原，对安全问题进行溯源。

统计安全信息。通过自定义报告等功能，可从全局概况到每个实例的具体信息自由定制，满足企业个性化统计需求。为数据安全信息、运行信息提供详尽的分析依据。

3.原生敏感数据处理

原生敏感数据处理可为数据系统中的敏感信息进行脱敏处理并在泄漏时提供追溯依据，为企业核心数据提供有效的安全保护措施，主要具备如下原生特性：

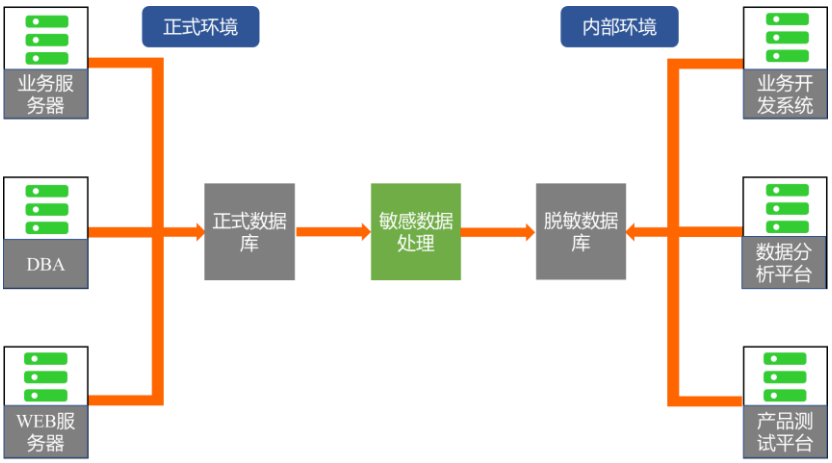

图 10 原生敏感数据处理

快捷开通配置。用户无需关注软件或硬件设备安装部署，使用控制台一键开通服务。通过 VPC 网络与数据库等配置，开启功能，进行敏感数据保护。

适配云平台原生网络架构。无需改变云平台网络架构，通过简单 VPC 网络配置、路由表配置等措施，实现与云平台原生网络架构适配，实现网络连通。

敏感数据处理性能支持弹性扩展。依托于云平台计算、存储、网络资源弹性扩缩容的特点，可以根据脱敏数据量、活跃任务数、存储空间等情况，实现敏感数据处理性能弹性扩展。

支持各类型数据库。通过统一的数据库配置模块，支持多种数据库类型，支持异构数据库之间数据同步，实现不同类型数据库之间的抽取、处理和装载数据。

解决云平台共享数据安全问题。通过敏感数据脱敏，泄密事件追溯、安全多方计算等技术解决云平台共享数据的安全性问题。

表 7 原生敏感数据处理产品主要功能

功能	详情
敏感数据自动发现	根据内置及自定义规则，对数据集的所有字段进行敏感属性识别，确保隐藏的敏感信息能被妥善处理。
敏感数据变形处理	支持屏蔽、变形、移位、格式保留加密、令牌化、洗牌、强加密算法等多种脱敏算法，可根据需求对敏感数据进行不同的脱敏处理。
异构数据库同步	支持对多种类型数据库的数据进行脱敏处理，并能完成异构数据库之间的同步。
敏感数据匿名化	支持通过匿名化方式，将部分标识数据进行泛化处理，使得某一段区间的数据行数一定不小于某个值。
敏感数据追踪	支持通过水印等相关技术，对于泄漏的数据集进行外泄时间和泄露者等的追踪操作，降低泄密事件影响。

原生敏感数据处理的典型应用场景如下:

内部数据脱敏。研发、测试、数据分析环境中，开发人员并不需要使用完全真实的数据，仅需要数据格式与生产环境一致即可。此时，如果数据系统提供的数据不经处理，那么会产生核心数据边界不可控

的问题。开发人员如果因为一已私利倒卖关键数据，将对企业造成不可估量的影响。敏感数据处理能够将研发、测试、数据分析环境中的数据进行脱敏处理，杜绝内部泄密。

泄密事件追责。当企业数据库出现重大敏感数据泄漏事件时，必须要进行全面的事件还原和追责处理。但往往因为数据访问者较多，泄密途径不确定，导致定责模糊、取证困难，最后追溯行动不了了之。敏感数据处理将泄漏的数据集进行外泄时间和嫌疑人的定位，缩小排查范围，保障泄密企业快速追查责任人，从而将泄密事件影响降到最低。

动态脱敏。将动态脱敏系统部署在访问终端和目标数据库之间，所用访问请求都要经过脱敏系统，基于数据库 SQL 协议的解析、改写和审计，完成数据动态脱敏，实现数据安全管理。对数据库中数据查询导出进行动态脱敏处理，实现未授权人员只能访问脱敏后的数据，并对操作数据库的行为进行审计，防止数据被滥用、或被非授权完整复制，导致敏感信息外泄。

4.原生密钥管理系统

原生密钥管理系统提供云平台集中的密钥管理服务，包括对称密钥与非对称密钥的生成、存储、分发、启用、更新、禁用、轮换、销毁、导入和导出、查询等生命周期管理，结合严格的密钥使用授权，保障密钥安全使用与隔离保护。，主要具备如下原生特性:

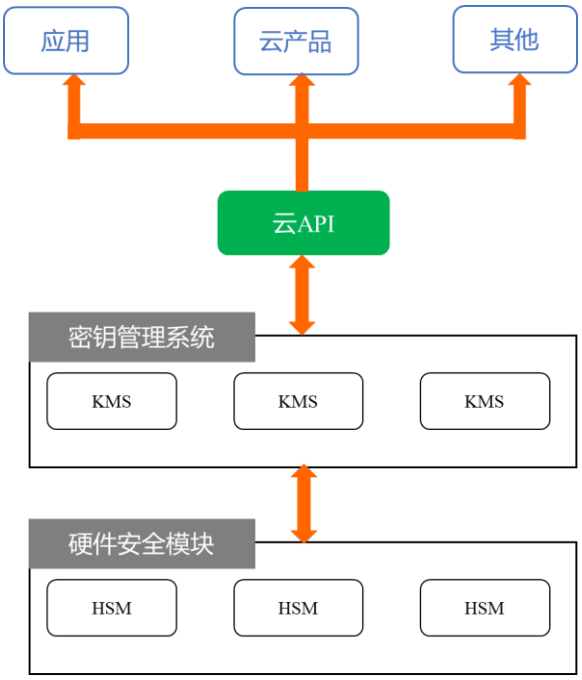

图 11 原生密钥管理系统

无缝集成云平台。与云计算架构里 IAM 身份认证服务集成，实现密钥资源级粒度鉴权，接入云审计实现密钥操作的流水审计，实现与云平台一体化的密钥权限管控及审计管理。

无缝集成云服务。用户无需配置部署，与对象存储、分布式数据库、云硬盘等服务的加密特性无缝集成，管理这些服务内所存储数据的加密。

支持云上 BYOK 架构。在云架构上实施 BYOK（Bring Your Own Key）方案，允许用户在云架构上使用自有的密钥材料进行敏感数据加解密服务，进一步提升用户对云上数据隐私的自主管控能力。

集群化部署与冷热备份，实现高可用。依托云计算底层资源，采用多机房分布式集群化的业务部署和冷热备份，确保密钥管理系统的高可用性。

表 8 原生密钥管理系统产品主要功能

功能	详情
托管式密钥管理	支持密钥创建、启用、禁用、轮换设置、别名设置、查看密钥详情、修改相关信息等，可以创建、保护以及执行各项密钥管理策略
密钥导入	支持导入用户自有密钥，通过 KMS 系统生成一个密钥材料为空的 CMK,并将自己的密钥材料导入到该用户主密钥中，形成一个外部密钥 CMK，再由 KMS 系统进行该外部密钥的分发管理。
密钥轮换	支持密钥轮换，开启后 CMK 会一年交换一次，轮换后使用该 CMK 加密的旧的密文依然可以解密，新的加密则使用新的 CMK
信封加密	对于较大的文件或者对性能敏感的数据加密，使用信封加密应对海量数据的高性能加解密方案。
敏感数据加密	加密接口（Encrypt）用于加密最多为 4KB 的任意数据，可用于加密数据库密码，RSA Key，或其它较小的敏感信息。
集中化密钥管理	通过 API、SDK、云产品等多种方式调用并集成密钥管理系统，实现对各类应用程序的密钥的集中管理

原生密钥管理系统的典型应用场景如下:

云上数据透明加密。云用户大量的业务数据在云平台上流转，云数据透明加密服务提供给用户数据落盘透明加密，保障用户数据的隐私安全。以云密钥管理系统为支撑，实现丰富的云数据加密方案，如块存储加密、对象存储加密、数据库加密、磁盘加密、文件加密等;用户在选择存储或数据库加密服务时，可选择一键加密，实现数据存储加密功能。

金融/政府敏感数据保护。金融和政府机构任何的通信和存储数据都具有高价值性和高保密性，通过信封加密对协议通信内容、重要

文件和资料提供加密服务及密钥保护和权限管理，满足安全性及合规性要求。

后台服务开发配置信息保护。应用开发配置文件需要进行加密以保护程序数据安全。通过密钥管理系统对敏感配置信息、数据库连接信息、数据库密码、登录密钥、后台服务的配置信息进行加密及完整性保护。

企业核心数据保护。核心知识产权、用户手机号、身份证号、银行账号、口令等隐私数据做严格保护，将敏感数据加密后保存，但是无法保证数据密钥的安全。以信封加密方式，将所有核心数据通过数据密钥加密，数据密钥再经过密钥管理系统加密，为核心数据提供双重保护。

网站或应用开发安全。提供 HTTPS 等服务时需要使用到证书、密钥，这些信息若以明文保存本地，攻击者可以轻易获取。通过密钥管理系统对密钥进行加解密，加密后本地保存密钥的密文文件，使用时解密且不保存本地，使得攻击者难以获取，从而保证网页和应用的安全性。

5.原生凭据管理系统

原生凭据管理系统对云平台、云产品以及云租户业务系统中存在的大量敏感凭证信息，如云计算架构中数据库凭证、API 密钥和其他密钥、敏感配置等进行集中查询、管理以及加密存储，所有的凭据由

密钥管理系统进行加密保护，并提供简单的使用接口和 SDK，实现云上敏感凭据及配置信息的集中管控与安全保障。主要具备如下原生特性：

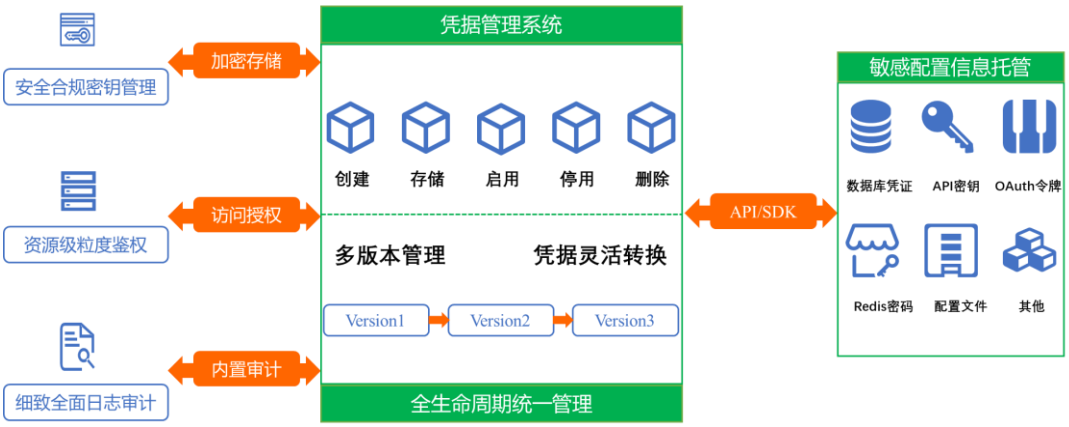

图 12 原生凭据管理系统

云平台无缝集成。使用被云密钥管理系统安全保护的主密钥作为加密密钥对凭据进行加密，实现凭据硬件级加密存储；与云平台访问管理 IAM 集成实现凭据管理系统访问精细化鉴权；与云审计结合，实现凭据访问监控审计、合规性检查、操作审核和风险审核的服务。

服务安全可靠。凭据管理系统架构采用集群化部署的方式，通过分布式数据库存储系统实现数据固化与容灾备份；主备 CMK 跨区域管理，加解密凭据密文多地域备份存储；业务侧用户可多地域内创建同样的凭据，实现业务侧的跨区域容灾。

凭据全生命周期统一管理。为用户提供凭据的创建、检索、更新、删除、权限管控等全生命周期的管理服务，结合资源级角色授权及全面细致的审计管控，轻松实现对敏感凭据的统一管理。

表 9 原生凭据管理系统主要功能

功能	详情
凭据检索	从应用程序的源代码中删除硬编码凭据，将代码中的硬编码凭据替换为 API 调用，以编程方式动态检索凭据
凭据存储	使用被云密钥管理系统 KMS 安全保护的主密钥 CMK 作为加密密钥，对所管理的凭据内容进行加密存储
多类型存储	存储多种类型数据，例如数据库连接、账号密码、IP 端口等
凭据轮换	凭据全量轮换：通过控制台或者 API 对当前使用的凭据版本直接更新内容，业务侧对 API 发起请求时将会获得最新凭据，实现凭据一次性全量轮换
	凭据灰度轮换：管理员对指定凭据增加新的版本，业务侧根据选择可以一次性或者灰度进行凭据版本的变更
权限控制	与访问管理集成，通过身份管理和策略管理确保只有授权用户可以访问或修改凭据
监管审计	与云审计结合，记录所有凭据管理操作和凭据使用情况
安全合规	凭据管理系统与密钥管理系统 KMS 相关联，KMS 底层使用经过第三方认证的硬件安全模块 HSM 来生成和保护密钥，符合监管和合规要求
统一的 API 接口	支持统一接口，提供包括凭据创建、删除、编辑、更新、检索等操作；支持 php、C++、python、java、.net 等多语言版本 SDK

原生凭据管理系统的典型应用场景如下：

凭据集中管控。为保障业务开发敏捷性，系统中存在大量的敏感账户信息、Tokens、证书、SSH 密钥、API 密钥等，通过凭据管理系统对敏感凭据进行统一的存储、检索、使用等全生命周期管控。

敏感凭据检索管理。当用户创建从数据库查询信息的自定义应用程序时，必须将访问数据库所需的凭证（密码）直接嵌入在应用程序的配置文件源码之中，通常情况下是明文显示，安全性较低。凭据管理系统可以将代码中的硬编码凭证（包括密码）替换为对 Secrets Manager 的 API 调用，以编程方式动态检索凭据，助于确保密钥以及

敏感凭据的保护。

应用层凭据轮换。为提升系统安全性，需要对敏感凭据进行定期更新，通过在凭据管理系统中更新目标凭据内容，实现依赖目标凭据的所有应用点的同步更新。

管理多类型敏感数据。除了用户名和密码以外，密钥通常还包含其他敏感信息。借助凭据管理系统，实现多种类型敏感数据存储，如数据库连接、账号密码、IP 端口等，确保可用于访问密钥中的凭证的敏感信息的安全。

（三）云原生网络安全

1.原生 DDoS 防护

原生 DDoS 防护体系通过对网络流量进行攻击检测和异常流量清洗，实现覆盖从网络层/传输层到应用层的 DDoS 攻击防护，主要具备如下原生特性：

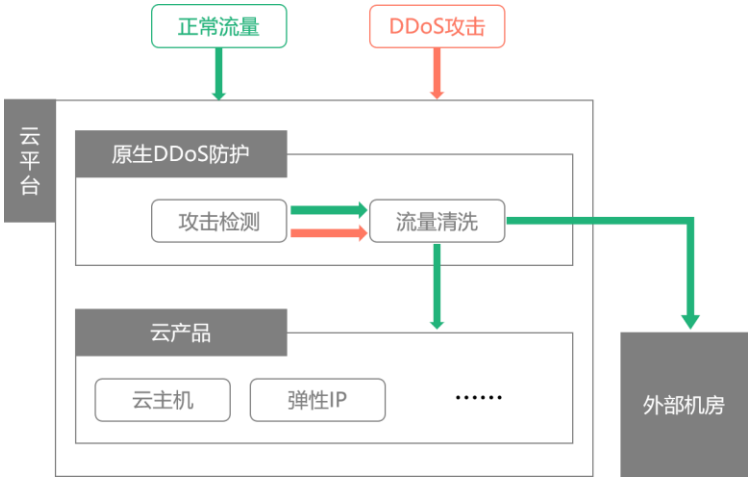

图 13 原生 DDoS 防护体系

便捷接入。通过云平台原生网络防护 DDoS 攻击，用户无需改变业务架构。云上用户可将待防护 IP 与原生 DDoS 防护绑定，无需变更已有 IP，即可开启防护功能。同时，云上用户或非云用户，也可通过简单的防护 IP 配置，利用防护 IP 将正常流量转发至已有 IP 或外部机房，实现源站隐藏。

与安全产品有效联动。通过与其它原生安全产品进行联动实现安全能力整合和纵深防御。如对大流量攻击进行清洗后，通过原生 Web 应用防火墙实现精细化应用层攻击的抵御。

防御能力弹性扩展。利用云平台计算、存储和网络资源，能够实现从 MB 级到 TB 级别的防护能力调度。

海量情报数据，算法持续迭代。利用海量威胁情报，尤其是云平台内高质量流量与攻击数据，为攻击检测提供有力支撑；通过规则策略与 AI 结合的方式，实现攻击检测的智能化。同时，对情报数据和算法进行持续迭代与更新，不断提升攻击检测能力。

运行稳定，低延迟。底层通过集群部署支持高可用，能够稳定持续为用户提供 DDoS 防护，用户无需购买备份以进行容灾；依托云平台流量调度、多线 BGP 等能力，保障用户防护访问速度，最大限度降低延迟，不对用户业务运营造成影响。

表 10 原生 DDoS 防护产品主要功能

功能	详情
网络层攻击防护	能够对 UDP Flood、SYN Flood、TCP Flood、ACK Flood、FIN Flood 等四层攻击流量进行检测和清洗。

应用层攻击防护	能够对 CC 攻击、HTTPS Flood、HTTP 慢速、Wordpress 反射攻击等应用层攻击流量进行检测和清洗。
自定义配置	支持用户根据业务需求自定义防护配置，包括 IP 黑白名单、清洗阈值、报文特征过滤策略等。
防护统计与分析	能够对各类攻击进行多维度数据统计和展示。

对于易遭受 DDoS 攻击的客户，可以通过原生 DDoS 防护产品，确保云上业务高可用，原生 DDoS 防护的典型应用场景如下:

游戏行业。一是在游戏运营过程中，遭受 DDoS 攻击和黑客敲诈勒索，导致游戏业务中断，影响玩家体验；二是当活动、新游戏发布或节假日游戏收入旺季时，DDoS 攻击导致营销策略受阻、用户流失，缩短游戏生命周期。

政务民生行业。政务网站遭受 DDoS 攻击，导致访问速度变慢，甚至网络瘫痪，影响民生正常生活及政府公信力，尤其重要敏感时期，政务网站是 DDoS 攻击的重要目标。

金融行业。金融业务因 DDoS 攻击造成不可访问，将影响用户线上交易，造成经济损失，产生用户信任危机，甚至面临用户的巨额索赔。

互联网行业。在促销、活动、新品发布等重要时间段极易遭受 DDoS 攻击，业务系统不能正常对外提供服务，势必影响企业正常的生产、企业公信力及品牌形象。

2.原生云防火墙

原生云防火墙通过对互联网与云上资产间的东西流量，以及云内

VPC 间的南北流量进行访问控制，实现云上流量的安全可信与可控，主要具备如下原生特性：

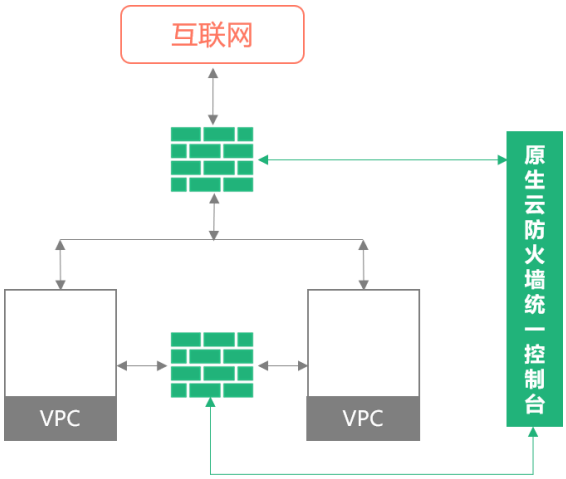

图 14 原生云防火墙

免部署与配置。用户无需关注硬件或软件的安全部署，可以通过云防火墙统一控制台，选择待防护资产，一键开启功能，自动将流量牵引至云防火墙。

集群化高可靠，性能弹性扩展。基于集群部署技术，用户无需部署双机热备系统，可靠性高，性能可以平滑扩展。

自动化响应与处置。一是能够自动识别用户公网 IP 及关联资产，在资产变更时能够自动同步；二是能够对来自互联网的入侵行为和云主机的主动外联行为进行自动拦截和管控。

云内流量精细化管控。不仅能对互联网与云上资产间的东西流量进行安全检测，还能对云内 VPC 间的流量、云主机粒度的外联行为进行精细化管控。

表 11 原生云防火墙产品主要功能

功能	详情
访问控制	基于访问控制策略，能够对经过互联网的、主机或 VPC 间的流量进行访问控制。
入侵防御	基于入侵防护规则，通过与威胁情报进行联动，能够对入侵行为进行发现和阻断，通过虚拟补丁实时修复高危、0-day 等漏洞。
溯源取证	能够提供日志存储与查询功能，协助用户运维人员进行审计和溯源，存储时间满足网络安全法和等保合规要求，日志类型主要包括流经云防火墙的所有流量数据日志，所有被执行云防火墙动作的事件日志，用户的操作日志。

原生云防火墙的典型应用场景如下:

主动外联管控。大部分的网络攻击和安全事件具备明显的回连特征，对于易被暴力破解、挖矿等的用户，应更加关注业务的主动外联，利用原生云防火墙发现和阻断异常外联行为。

互联网业务防护。对于在云上部署互联网业务的用户，应关注资产在互联网的暴露情况，利用原生云防火墙实现互联网业务的入侵检测和漏洞防护。

精细化隔离管控。对于业务种类多、业务间访问频繁的用户，可以利用原生云防火墙进行 VPC 间的细粒度隔离管控，实现传统网络中的 DMZ 区需求，将核心资产重点防护。

等保合规。利用原生云防火墙满足等保 2.0 中对互联网边界隔离、漏洞扫描、入侵防御、网络流量日志留存等方面的要求。

3.原生 Web 应用防火墙

原生 Web 应用防火墙(WAF)通过对云上 Web 应用的恶意流量、

访问行为进行检测和拦截，实现 Web 应用核心业务和数据安全，主要具备如下原生特性：

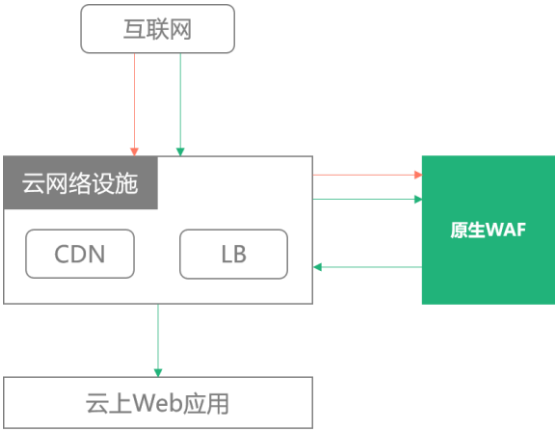

图 15 原生 WAF

便捷接入。用户无需调整现有网络结构，通过原生 WAF 统一控制台，配置待防护网站域名，一键开启防护功能。

原生集成云网络设施。与负载均衡、CDN 等云网络设施融合联动，对经过云网络设施的流量进行旁路检测与拦截，最大限度降低原生 WAF 对 Web 应用业务的影响。

集群化高可靠，性能弹性扩展。依托云平台主机、容器等计算资源，以集群方式提供服务，可靠性高，避免单点故障。同时根据实际流量情况，弹性缩减和增加集群规模，实现安全防护能力的平滑扩展。

形态向 Web 安全与 API 保护（WAAP）聚合转变。除具备传统 WAF 的安全防护能力外，聚焦 Web 应用面临的新安全风险，支持 API 保护、BOT 管理等功能，实现更加全面的 Web 应用安全防护。

表 12 原生 Web 应用防火墙产品主要功能

功能	详情
Web 攻击防护	能够防御 SQL 注入、XSS 跨站脚本攻击、非法

	HTTP 协议请求等 Web 应用攻击。
CC 攻击防护	能够在网络层和应用层阻断恶意请求，过滤 Web 应用垃圾访问，防御 CC 攻击。
漏洞虚拟补丁	能够在发现 0-day、高危等漏洞时，生成相应漏洞防护策略，在 Web 应用漏洞补丁发布和修复前，实现漏洞的快速防护。
网页防篡改	能够检测网页篡改行为，在网页被篡改后，以缓存的正常网页替代被篡改网页，避免篡改事件扩散。
自定义防护策略	支持用户根据业务需求，自定义防护策略，如黑名单封禁，基于 IP、URL 路径、POST 参数等的自定义防御规则。

对于云上部署 Web 应用的客户，可以通过原生 Web 应用防火墙产品，确保云上 Web 应用安全稳定运行，原生 Web 应用防火墙的典型应用场景如下:

电商/OTA/文创网站防护。一是在高并发抢购及各类营销活动场景下，识别垃圾流量访问，保障业务活动顺利进行；二是解决交易数据、商品信息和 IP 知识产权被恶意爬取问题，有效解决短信/营销接口滥用、恶意库存查询、黑产 SEO 等问题，确保营销策略有效开展，保护正常用户访问，节约服务器和带宽资源。

政务网站防护。一是提供 Web 攻击入侵防护；二是提供核心页面防篡改服务和敏感信息防泄漏功能，保证民生政务网站（政务、医疗、教育、社保、税务等）内容不被篡改，敏感数据不泄露；三是在重大活动或节日期间，能够根据需要进行弹性扩容，保护网站稳定运行。

泛互联网安全防护。一是有效防御常见的 Web 攻击，如 SQL 注入、XSS 和 Webshell 检测等；二是能够防御 Web 零日漏洞和未知威胁，

保护网站安全；三是用户可在营销、重大节假日等时段进行弹性扩容，节约成本。

（四）云原生安全管理

1.原生安全运营中心

原生安全运营中心通过对于云上资产进行统一安全运营与管理，提供资产自动化盘点、互联网攻击面测绘、云安全配置风险检查、合规风险评估、流量威胁感知、泄漏监测、日志审计与检索调查、安全编排与自动化响应及安全可视等能力，帮助云上用户实现事前安全预防，事中事件监测与威胁检测，事后响应处置的一站式、可视化、自动化的云上安全运营管理。主要具备如下原生特性：

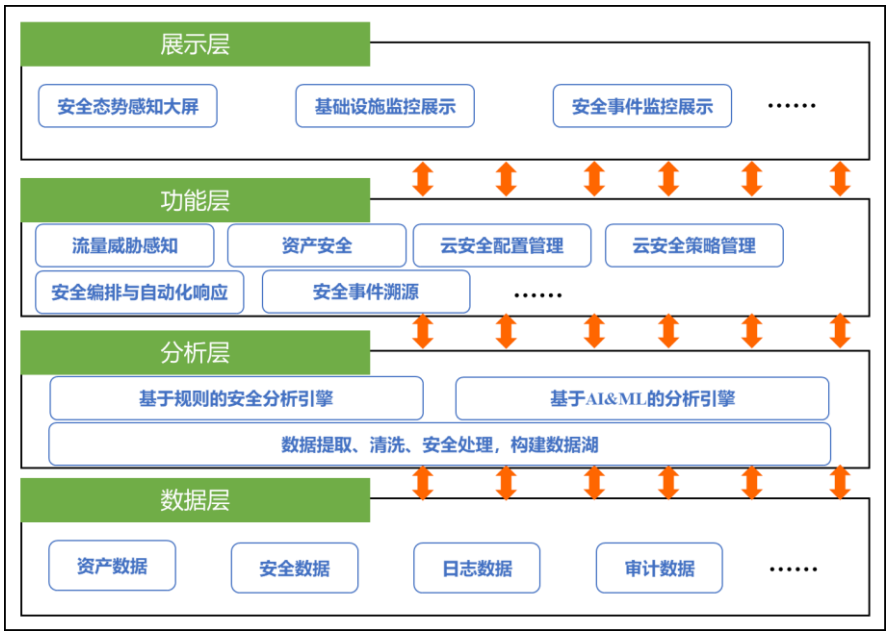

图 16 原生安全运营中心

免部署与配置。用户无需关注软件或硬件设备的安装部署，通过

控制台一键开通服务，对于云资产进行简单授权操作，快捷开启安全运营中心产品功能。

云上资产自动发现，统一管理。对于用户云上的资产进行自动化动态盘点，包括云服务器、对象存储、云数据库及云负载均衡等多种资产。同时通过云配置风险、漏洞及安全事件等多种安全维度，对资产安全风险进行统一管理，降低云上影子资产风险。

安全编排与自动化响应。通过自定义或内置安全编排策略，实现安全产品的联动处置，可针对多种安全事件实现自动化的响应处置，提升云上安全事件响应处置效率。

云内流量威胁感知，安全事件统一运营。提供流量威胁感知能力，实现云上流量由外到内及由内到外的双向攻击检测。同时解决云上安全事件处理割裂的问题，通过安全运营中心平台，对于安全事件统一运营，协作处理，提升安全事件的响应及处理效率。

表 13 原生安全运营中心产品主要功能

功能	详情
互联网流量威胁感知	针对互联网流量进行威胁感知，实现互联网对内攻击及内部资产向互联网异常外联行为的检测，检测内容包括漏洞利用攻击、命令注入攻击、暴力破解攻击、僵尸网络主机、主机挖矿行为、代理隧道行为等多种威胁的感知
资产安全中心	实现云上资产的自动化动态盘点，盘点内容包括云服务器、对象存储、云数据库及云负载均衡等多种资产。同时通过云配置风险、漏洞及安全事件等多种安全维度，对资产安全风险进行统一管理
云安全配置管理	提供自动化检查评估功能，覆盖云服务器、对象存储、云数据库及负载均衡等多种云产品，降低因云产品使用中的错误安全配置带来的安全风险，提升整体云上安全水平

云安全策略统一管理	对于云安全策略进行统一管理，包括自定义安全策略的创建以及安全策略启用、停用等
安全事件统一运营	将云上各个安全产品检测出的安全事件进行统一采集与存储，对于安全事件统一运营，协作处理，提升安全事件的响应及处理效率
安全可视化	通过安全仪表盘、安全大屏及安全报表中心实现云上安全的全局可视化，实现安全态势的实时监测及安全建设成果的直观可视化呈现
安全编排与自动化响应	通过自定义或内置安全编排策略，实现安全产品的联动处置，可针对多种安全事件实现自动化的响应处置，提升云上安全事件响应处置效率。

原生安全运营中心的典型应用场景如下:

统一安全管理。云上业务众多，若同时使用多种安全产品，需要构建云上统一安全运营管理平台，提升整体云上安全管理效率。安全运营中心以云上资产中心为基础，打通云上各类安全相关数据，为客户构建覆盖事前、事中及事后各个环节的统一安全运营管理平台。

统一威胁检测与响应。业务上云后，除了面对传统的主机安全威胁、网络安全威胁及应用安全威胁外，客户也需要面对云上特有的新的威胁类。各类安全威胁的检测与响应处置分散在各个安全产品上，造成安全事件处置效率低下，大大增加了云上安全风险。安全运营中心提供流量威胁感知功能，提供了有效的流量威胁检测能力补充，实现云上流量由外到内及由内到外的双向攻击检测。同时安全运营中心可针对云上特有的云产品配置风险、异常用户行为及异常 API 调用等进行检测，全面覆盖云上新增的各类安全风险及威胁。安全运营中心打通云上各类安全产品检测的威胁数据，并通过统一的响应中心实现对威胁统一的响应处置，针对部分威胁事件可通过内 置的安全编排

功能实现自动化响应处置，简化威胁管理难度，提升响应处置效率。

等保合规建设。等级保护 2.0 标准正式实施后，针对云上合规要求进行了进一步细化，云上资产对外发起的攻击检测、日志审计及集中管理等都需要客户采取相应技术措施进行满足。同时针对安全管理方面提出的各项管理要求，也需要有相应的工具和产品帮助客户更容易、更有效地落地。安全运营中心提供的流量威胁感知、UBA、日志审计与检索等功能，可以帮助客户有效满足等级保护合规要求，同时安全运营中心可帮助客户实现等级保护标准要求中关于安全管理中心相关的要求，在满足等保要求的基础上，切实提升客户云上安全水平。

资产安全管理中心。公有云上的业务更加弹性灵活，云资产的变化更加频繁，对资产的安全运营和管理要求更高，需要通过自动化的方式实现资产的统一安全管理。安全运营中心可为客户提供云上资产全流程的安全管理平台。从资产的自动化盘点，到资产各类安全风险的检测识别，再到资产安全风险的自动化响应处置，建立以资产为中心的统一安全管理平台，提升云上整体安全水平。

云上安全托管。随着攻击手段的不断升级和安全监管要求的不断提高，用户面临的安全形势日益严峻，对安全运营管理也提出了越来越高的要求，需要专业的托管服务来帮助实现安全体系的建设与运营管理。可以安全运营中心为核心载体，搭配服务厂商安全托管服务，实现云上业务的安全运行。

（五）云原生安全服务

1.原生托管安全服务

原生托管安全服务，**利用托管安全服务商丰富的 API 接口及安全数据优势，依托托管安全服务商专业人员的安全能力和实践经验**，为用户提供安全托管服务，缓解企业用户安全运营压力。原生托管安全服务主要包括:

安全评估服务。由托管安全服务商全面分析用户云上资产安全状况，对客户资产信息、业务架构、安全产品策略等开展安全评估，发现已有云产品安全配置风险、系统及应用安全风险，并开展受影响面评估，提供修复解决建议。

风险检测服务。由托管安全服务商在获取用户服务授权后，结合各类型漏洞扫描技术，为客户提供周期性漏洞检测、配置核查服务，并提供修复指导和风险管理最佳实践。

漏洞感知及风险监测服务。由托管安全服务商提供包括重大漏洞、数据泄露情报在内的多种最新风险信息，以及定向预警、专业分析和修复建议，帮助云用户快速掌握威胁信息及快速应对方案。

安全监控服务。利用云原生 API 优势，结合云上典型用户威胁处置场景，利用自动化编排技术，实现大部分风险事件告警的自动化闭环处置，针对云上各类高级别安全事件提供更快速、更高性能的处置服务能力。

风险处置服务。针对安全评估、风险检测和情报监测各阶段产生的事件信息进行分析处置，为用户提供云环境专业风险处置方案和建议，指导进行云端风险加固和收敛，通常包含产品策略加固、安全策略加固以及系统漏洞、配置等加固。

应急响应服务。提供全天候的安全应急值守服务，在业务遭受黑客攻击时，提供安全事件响应，协助业务恢复，提供安全防范指导。

知识情报管理。结合托管安全服务中积累的事件经验与云端威胁场景，构建的事件知识库。通常包括自动化处置流程库、解决方案、标签规则、漏洞库、补丁库、病毒库、安全要求、安全工具、应急预案库、威胁情报数据、漏洞情报数据、泄露情报数据。在服务实施过程中，利用云端攻击源恶意 IP 地址库、恶意样本信息库、钓鱼网站列表、垃圾邮件发送列表、全球被黑网站、代理服务器等信息，为用户提供更加精准的风险识别分析和安全运营服务，不断完善和提升托管安全服务运营质量。

四、云原生安全趋势与展望

随着云计算安全需求愈加迫切，云安全技术与产业不断发展，云原生安全体系也将更加成熟健全，具体表现为：

云服务商与安全厂商联合建设云原生安全生态。随着云计算的发展，客户类型日益多样，不同用户群体面临不同安全场景，安全需求差异大。同时，网络安全环境日益严峻，云安全所涉范围越来越广，

构成愈加复杂。仅凭一家厂商的技术与管理能力，云原生安全建设难以面面俱到，一些领域暴露短板。未来，云服务商与安全厂商势必加强深度合作，结合双方在技术研究、人才储备、产品应用等方面的积累和经验，建设一个更加完善、开放的云原生安全生态。

产品趋于整合，形成综合的云原生安全解决方案。目前，云原生安全已建立了包括云主机安全、敏感数据处理、DDoS 防护、云防火墙、安全运营中心等在内的较为丰富的产品体系，单个产品可以缓解用户在某些场景下的安全问题。但随着用户对云上安全体系建设全面化、完善化的不断追求，未来，云原生安全产品将趋于整合，各产品之间有效联动增加，以综合的安全解决方案的形式交付给用户，进一步降低用户安全建设复杂度，助力用户更加便捷、快速的构建云上安全体系。

深耕行业，助力传统行业云上安全体系建设。政务、金融、工业、农业等行业业务场景各有特色，上云后安全需求和痛点有差异，如政务云内跨业务区的数据同步和交换对安全性的要求，金融云面临高监管要求等。未来，云原生安全将更加聚焦行业，结合行业安全需求，精细化发展云原生安全产品功能。