中国移动云安全白皮书

（2021 年）

中国移动通信有限公司研究院

前　言

随着数字化经济的飞速发展，云计算已成为新型信息基础设施建设的关键技术，是中国移动实现数字化转型，建设世界一流“力量大厦”的重要组成部分。中国移动经过十余年在云计算领域的深耕，目前已经形成移动云、IT 云以及网络云三类中国移动云服务。并且，随着边缘计算的发展，移动云和网络云按需下沉，形成边缘云，以快速、智能和安全的网络服务响应，满足行业客户在实时业务、应用智能、安全与隐私保护等方面的基本需求。

由于云计算具有硬件通用化、资源共享化、部署集中化、广泛基于开源组件等特点，使得通用软、硬件和开源组件的漏洞更容易被攻击者发现和利用，蠕虫等病毒更容易在集中部署的设备上进行快速传播。随着企业的业务以及运营商的系统、电信业务等逐步上云，攻击者将云作为重点攻击目标，一旦攻击成功，后果非常严重。目前，中国移动依据国家法律法规、相关技术标准以及中国移动的系统和业务的需求，从基础设施、网络安全、接入安全、应用安全、数据安全等方面对云服务进行了安全防护。但随着攻防对抗日益加剧，攻击技术迅猛发展，需不断完善中国移动的云安全防护，提升云安全服务能力，形成统一、主动、纵深的云安全防护体系。

为了保障中国移动云服务的自身资产与客户资产的安全，实现为行业客户提供安全的基础设施和稳定可靠的云服务，本文在全面分析云安全风险的基础上，提出中国移动云安全防护框架及安全防护要求，并对云安全关键技术进行了探讨，对云安全生态的思考进行了阐述，旨在为中国移动云安全的规划、建设和运营提供指引，与合作伙伴一起共同推进云安全产业发展。

得复制或拷贝本建议之部分或全部内容。

参与单位：中国移动通信有限公司研究院、中国移动通信有限公司网络事业部、中移(苏州)软件技术有限公司、中国移动信息技术中心

参编人员：何申、粟栗、谢懿、田峰、王浩硕、张文勇、秦尔楠、黄静、庄小君、侯艳芳、王旭、杨新苗、杨亭亭、陈佳、耿慧拯、陈敏时、王悦、罗志成、罗原、滕滨、刘天鹏、何亮忠、王庆栋

目 录

1 中国移动云现状及安全风险

1.1 中国移动云现状

根据业务发展需求，中国移动先后建设了移动云、IT 云和网络云三类云服务，分别用于承载租户业务、内部自有业务以及传统电信网络业务。中国移动严格执行“安全三同步”原则，在规划、建设和运营阶段，以法律法规和国内外标准、企业标准为依据，以业务需求为导向，不断完善中国移动的云安全能力，已经逐步形成基础的云安全防护能力、安全运维能力以及安全服务能力。

- **移动云**

移动云是中国移动基于云计算技术建立的云业务品牌，是中国移动的公有云，面向政府部门、企业和互联网等广大客户，为客户提供云网一体、安全可控的 IaaS、PaaS 以及 SaaS 类云服务，包括弹性计算、存储、云网一体、云安全、云监控、数据库、应用服务与中间件、大规模计算与分析以及海量优质应用等。移动云参考等保 2.0 的相关要求，分别在平台侧和租户侧构建了基本的安全能力。平台侧包括基线合规、防病毒、数据防泄漏、web 漏扫、系统漏扫等计算环境安全防护能力，和网络与边界的抗 DDoS、防火墙等安全防护能力。在安全管理方面，构建了安全运营管理平台以及网络空间测绘平台等，实现资源池的流量监测和暴露面检测的能力。租户侧已完成 Web 应用防护、漏洞扫描、抗 DDoS、云主机安全等相关产品的部署上线，能满足租户的基本安全防护要求，实现按需为租户提供安全服务。

- **IT 云**

IT 云承载中国移动全网各单位 IT 系统，支撑 IT 系统集中化。目前 IT 云已构建“网络产品能力、计算资源能力、容器云弹性计算能力、安全保障能力、同城双活能力”五类平台能力，为租户的业务系统提供更安全、更可靠、更多样的服务能力。在安全保障能力方面，IT 云依据国际、国内的行业安全标准和相关安全要求，制定了《中国移动 IT 领域云计算安全防护技术要求及实施指南》、《中国移动容器云安全规范》，并根据指南从安全防护、安全检测和安全监测层面开展了安全建设，结合全网安全运营管理平台、全网安全评估与检测平台、全网安

全威胁分析与预警平台、全网数据安全管控平台等集中化安全能力，形成一张安全、稳定、可靠的云安全保障网，增强了安全管控能力和业务保障能力。同时，在传统 IaaS 云资源上，还建设了以 Kubernetes 技术为基础的磐基 PaaS 云平台，并进行了 PaaS 平台的安全建设。经测评达到可信云容器解决方案评估标准，获颁可信云认证证书。

- **网络云**

网络云是一种新型的电信网络架构，通过云计算、网络功能虚拟化（NFV）、软件定义网络（SDN）等技术实现电信业务云化，可为传统电信业务提供一个资源可弹性伸缩、流量可全局调度、能力可全面开放的新型服务环境。当前网络云已具备基本的安全防护能力，包括基础设施、虚拟化网元以及 MANO 均进行安全加固，遵从最小化原则；虚拟网络以及资源池边界均进行逻辑或物理隔离；虚拟化网元之间的通信进行相互认证，传输的通信数据具有机密性和完整性保护；对所有设备的访问均进行认证，并通过 RBAC 等进行权限控制，对所有的操作进行日志记录和审计；对于敏感数据，传输、存储时进行加密和完整性保护，被访问时进行身份认证和授权；安全运维方面，周期性的进行合规检查和漏洞扫描，对不合规项进行整改，对漏洞和补丁进行管理，对安全风险进行监测。

虽然以上云业务已具备基本的安全防护能力，但随着各种开源组件的广泛使用、各类业务上线引入的 API 开放性以及攻击技术的日益发展、各种新型攻击的层出不穷，需要不断提升安全防护能力，为业务提供更安全可靠的云服务，重点包括：

（1）东西向流量防护能力：随着云原生化的发展，东西向流量会持续增加，而资源池内的横向攻击也会更加严峻，一旦资源池内遭受横向攻击，将影响所有业务。所以需进一步地梳理重要资产、业务端口开放要求、隔离要求等，完善东西向流量安全防护机制，对东西向流量实现精细化的控制；

（2）安全运维智能化能力：目前安全设备以手工配置安全策略为主，安全问题的定位也以人工排查为主，工作量大、耗时长、易出错，无法适应云化网络对高效运维的要求，需完善云安全管理中心的能力，实现安全自动编排和管理；

（3）主动防御能力：当前的安全设备均基于已有特征被动识别安全威胁，很难检测未知的安全威胁，以及主动识别和处置安全威胁。需基于威胁情报库、云安全管理平台以及安全监测组件等构建网络自检测和处置的主动防御能力；

（4）三云协同能力：由于三朵云的基础设施以及云管平台多使用通用的开源组件并具有类似的互联网攻击面，三朵云之间可相互借鉴和共享彼此的优秀经验，如威胁情报、安全解决方案等，实现协同发展、降本增效。

1.2 云安全风险

云服务因其总体架构、网络部署、运维服务具有相似性，面临着共性安全风险，以下从基础设施、网络部署、云上应用、运维服务四个方面进行安全风险分析。其中，基础设施是指为云上应用提供运行环境的软硬件及管理编排系统。

1.2.1 基础设施安全风险

在基础设施方面，面临以下安全风险：

- **物理环境及设备安全风险**

物理设备（如服务器、交换机等）被偷窃，机房遭受火灾、水灾等环境安全问题。物理设备的 WAN 口/LAN 口/串口无访问控制机制或使用弱口令被攻击者非法登录等。

- **虚拟化安全风险**

虚拟化软件或 Host OS、Guest OS、容器引擎漏洞被利用，虚拟机被非法迁移，虚拟机镜像或容器镜像被篡改、镜像漏洞被利用，虚拟机逃逸，容器逃逸等。

- **开源组件风险**

云服务使用了多种开源组件，如 Openstack、KVM、Kubernetes 等，由于针对开源组件具有公开的漏洞信息和攻击工具，所以开源组件的漏洞更易被攻击者成功利用。并且，漏洞一旦被攻击者利用，就会导致影响所有资源池的业务，如造成用户数据资产的损坏或泄露等。

- **配置与变更操作错误**

云服务承载的应用具有动态性，相应的配置与变更操作更加频繁，一旦对应用的资产进行了错误的配置与变更，可能会导致越权访问、数据泄露等。

- **带宽恶意占用**

恶意的虚拟机/容器可通过恶意占用网络带宽，导致其它虚拟机/容器无法正常通信，从而导致 DoS 等攻击发生。

- **资源编排攻击**

云平台通过编排实现计算资源的优化配置、存储和网络管理等，恶意攻击者一旦获取到管理员的权限，可通过恶意执行编排任务，对虚拟机/容器实施 DoS 攻击或非法访问等。

1.2.2 网络部署安全风险

在网络部署方面，面临着以下安全风险：

- **数据泄露**

云服务网络的复杂化与接口的多样化，增加了策略管理的复杂度，当接口访问的安全管控措施不严、安全策略不完善时，可能会导致用户数据被非法访问、窃取。

- **身份和密钥管理**

云服务中的用户具有多样性，云服务在进行身份识别与密钥管理时，如果缺乏可扩展的身份、凭据及访问控制系统，以及密码和证书的定期自动更新机制，会导致恶意用户读取或窃取、篡改、删除核心数据等，造成数据的破坏与泄露。

- **接入认证**

在向外部或内部提供云服务时，如果缺乏对访问服务的实体进行身份认证和授权，或者采用不安全的认证和授权机制，会导致攻击者非法接入、非授权访问等。

- **跨数据中心的横向攻击**

由于云基础设施使用 Linux、Openstack 等开源组件，各个数据中心之间具备一定的同质性，并且可能采用异地数据中心进行备份，如果恶意攻击者成功入侵了某个数据中心，可能通过承载网攻击其他相连的数据中心，实现跨数据中心的横向攻击。

- **APT 等新型攻击**

随着攻防对抗的日益激烈，APT、0 day 等新型攻击层出不穷。目前的边界安全设备基于已知特征进行安全检测，无法检测 APT 等新型攻击。

1.2.3 云上应用安全风险

在云上应用方面，面临着以下安全风险：

- **API 接口安全**

云服务使用 REST API、SOAP API 等类型的接口提供内部或外部服务，微服务的引入加剧 API 的频繁调用，当接口调用采用单一化的安全控制机制时，可能会面临缺少对客户端请求真伪进行识别，API 调用权限访问控制不足，以及缺少对 API 统一管理而导致的非法访问、数据泄露等的风险。

- **无服务器攻击**

无服务器应用程序能够快速启动云功能，而无需构建或扩展基础架构。这种“功能即服务”的方式为恶意攻击者创造了新的机会，也为网络维护者带来了新的挑战。例如，某些功能的权限设置不正确，恶意攻击者就有可能通过该功能执行非法访问或创建恶意账户等安全攻击。

- **(D)DoS 攻击**

来自单一来源，或多个不同来源的持续性恶意流量所实施的 DoS 或 DDoS 攻击，会淹没云上业务的正常流量，消耗云服务的可用系统与带宽资源，造成服务中断、宕机等问题，影响业务的连续性。在网络云中，还存在由海量的 UE 在同一时刻向网络云中的虚拟化网元发起访问，导致信令风暴的风险。

- **跨租户/跨省横向攻击**

在移动云和 IT 云中，如果租户之间的安全隔离、访问控制等安全防护策略配置不当，恶意租户可发起针对其它租户的攻击，比如利用虚拟机逃逸/容器逃逸攻击同主机上其它租户的虚拟机/容器，进而在资源池内横向扩展，实现对其它租户业务的非授权访问、恶意占用带宽导致 DoS 攻击等。在网络云中，同一资源池上部署多省业务，一旦攻击者攻击了资源池中某省业务，可横向攻击其他省的业务，造成各省之间的业务相互影响。

- **跨工作负载攻击**

在同一个租户中，恶意攻击者可以利用工作负载之间的相互通信发起攻击。例如，某租户使用不受信任的虚拟机浏览和下载在线内容时受到蠕虫感染后，该

蠕虫通过工作负载之间的通信传播给该租户上运行的其他具有敏感数据的工作负载。

- **云服务被滥用及违规使用**

恶意攻击者若伪装成正常租户使用云服务，在云上搭建恶意软件，并基于可信的中国移动云服务的域名，进行电子挖矿，向其他正常用户发起 DDoS、垃圾邮件、钓鱼邮件攻击，向关键网站发起暴力破解攻击，以及存储“九不准”内容数据等，会为中国移动云服务的正常运行与社会信誉造成很恶劣的影响。

- **用户账号管理安全**

云上应用的账号在整个生命周期中，可能存在账号信息未同步、权限控制粒度粗、访问控制覆盖面不全等问题，导致非法用户未授权访问、正常用户身份被仿冒等。

- **核心网攻击**

攻击者利用边缘云上的应用攻击 UPF 等网络设备，并进一步通过被控制的 UPF 等网络设备攻击 5G 核心网。

1.2.4 运维服务安全风险

在运维方面，面临着以下安全风险：

- **管理接口攻击**

恶意攻击者可通过管理接口存在的漏洞（如使用不安全的传输协议、使用弱口令等），非法登录设备，并进一步利用管理网络横向扩展，攻击云平台管理、服务器管理、网络管理和存储管理，从而控制整个云。

- **管理员权限滥用**

当对管理员的权限缺乏控制，且对管理员操作缺乏日志记录和审计时，恶意管理员进行非法操作并产生安全事件后，将无法有效地进行事件排查与溯源，影响业务正常运行。

- **漏洞和补丁管理安全**

管理员未定期对设备进行漏洞扫描，或者管理员对发现的漏洞未及时修复，导致漏洞被攻击者利用；管理员在给系统打补丁前未做与现有系统间的兼容性测

试，导致打完补丁后，业务中断等安全风险。

- **安全策略管理**

中国移动云中部署了多个厂家的安全设备，不同厂家的安全设备运维方式差异性大，而依赖人工进行安全策略的配置、优化等，存在工作量大导致配置错误，或者由于安全策略配置不及时，攻击者利用安全策略未有效配置的时间窗口入侵云数据中心的问题。

2 云安全目标及要求

2.1 云安全目标

随着云计算、5G 以及边缘计算的发展，云服务作为关键信息基础设施，其安全性关系到千行百业的安全。中国移动的移动云和 IT 云已经有十余年的发展，网络云从 2017 年试商用到正式商用也有近 5 年的发展。目前，每朵云均根据业务需求，在基础设施、网络部署、应用以及安全运维方面构建了各自的安全能力和一些安全工具。但是，随着攻击技术日新月异，攻防对抗形势异常严峻，网络开放性和暴露面日益增大，依赖当前基于已知攻击的被动式防御，无法有效应对 APT 等新型攻击，需在当前的安全防护体系的基础上，构建主动、纵深的云安全防护体系。并在此基础上，为用户提供灵活、可靠的安全服务。

因此，中国移动的云安全目标是基于三朵云的安全防护实践，面向共性安全需求，形成统一的具有主动、纵深防御能力的云安全防护体系，为业务提供可信的云基础设施和安全可靠的云服务。三朵云可相互借鉴优秀的安全防护经验，共享安全基线工具、扫描工具和安全情报等，打造统一的中国移动云安全能力，共同加强基础设施安全、网络安全、应用安全、数据安全和接入安全的同时，进一步完善云安全管理平台的安全管理和编排能力，统一安全设备的北向接口，实现智能安全检测、处置闭环，在现有被动安全防护的基础上，构建主动、纵深的云安全防护体系。

2.2 云安全防护要求

2.2.1 云安全防护框架

基于云安全目标，中国移动以法律法规及安全标准为依据，在加强基础设施安全、网络安全、应用安全、数据安全、接入安全的基础上，通过安全运维向自动化和智能化演进，逐步构建主动、纵深的云安全防护体系。

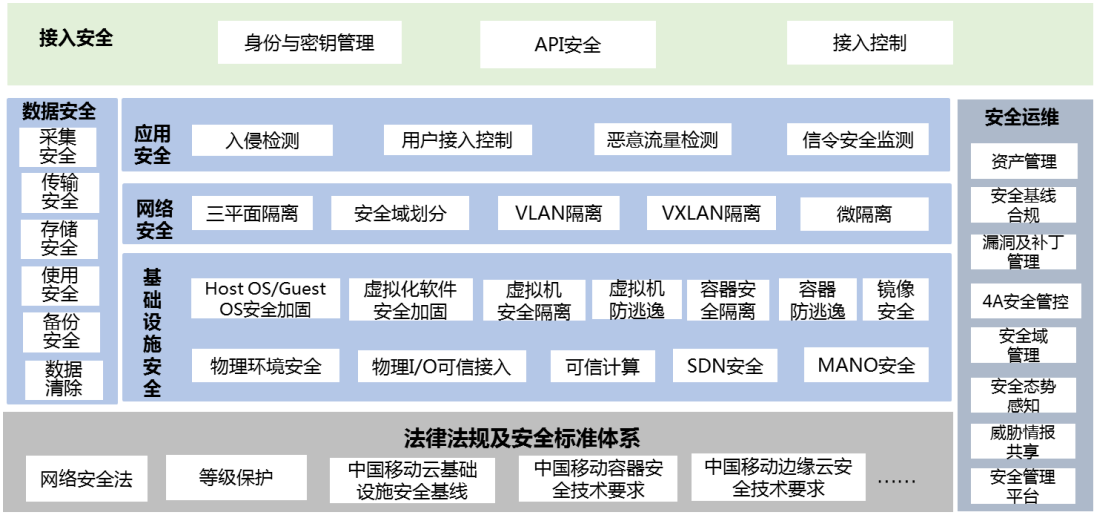

图 1 中国移动云安全防护架构

以下章节将基于中国移动云安全防护架构，对云安全防护要求进行阐述。

2.2.2 安全防护要求

2.2.2.1 法律法规及安全规范体系

中国移动云以法律法规和云安全技术规范的合规遵从为基础，在云安全规划、建设和运营全生命周期流程中，应对法律法规和云安全技术规范的符合度进行检查，及时整改不合规项。

2.2.2.2 基础设施安全

- **物理环境安全**

机房物理环境应遵从物理环境安全相关标准，如 GB/T 21052-2007《信息安全技术 信息系统物理安全技术要求》和 GB/T 31168-2014《信息安全技术 云计

算服务安全能力要求》等进行设计和部署。

- **物理设备安全**

服务器、交换机等设备的本地访问接口，如 WAN 口/LAN 口/串口等，应设计访问控制机制，如使用用户名和口令进行身份认证等。

- **系统安全**

应对物理服务器和虚拟机的操作系统、中间件和数据库，虚拟化软件等，进行安全加固，并采用安全的协议进行通信。

- **虚拟机安全**
  - 虚拟机使用的 vCPU，虚拟内存以及 I/O 等应进行安全隔离，虚拟机之间的相互访问应进行认证，授权和日志审计。
  - 虚拟机逃逸应进行监控。
  - 虚拟机迁移应授权，迁移数据应进行机密性和完整性保护。
  - 虚拟机销毁时，要保证数据的彻底清除。
- **容器安全**
  - 对容器运行时的组件（如 docker）等进行加固。
  - 对容器运行的资源和权限进行限制，采用最小授权的原则。
  - 容器所在的主机内核应进行安全加固。
  - 容器网络应进行隔离，支持南北向和东西向的隔离。
  - 容器运行时应支持安全检测和防护，包括不安全启动、逃逸攻击行为、宿主系统恶意访问容器、内部攻击、异常网络连接等进行监控，并支持入侵行为阻断等。
- **镜像安全**

（1） 镜像自身安全包括：

  - 应支持对镜像完整性保护，并对镜像的访问进行认证和授权。
  - 支持对镜像进行安全扫描（含基线检测、漏洞检测、恶意镜像检测），并根据扫描结果给出修复建议。
  - 支持镜像阻断，防止不安全的镜像上线运行。

（2） 镜像仓库安全包括：

  - 镜像仓库访问控制：镜像仓库需要对用户的身份认证，对访问的权

限控制，避免用户提权而访问其他用户的镜像资源。

- 镜像仓库安全通信：支持使用专门的认证和权限模型访问镜像仓库（例如：TLS），实现加密安全通信，防止信息泄露。

- **编排安全**

MANO 和云管平台、SDN 控制器、kubernetes 等负责对虚拟资源以及路由进行编排，应支持发现其存在的安全漏洞并进行安全加固，并对接口访问进行身份认证和授权，对传输的数据进行机密性和完整性保护。

2.2.2.3 网络安全

- **安全域划分**

安全域是中国移动云服务对网络进行安全建设的主要依据，应以边界接入、计算环境、网络基础设施、支撑性设施等维度，对云服务的网络进行安全域划分和隔离，防止安全风险扩散到重要系统及应用。

- **安全隔离**

中国移动云服务原则上应支持管理、业务、存储三平面物理隔离。资源池内应支持 VLAN/VXLAN 实现二层的隔离，支持微隔离实现端口级别的安全隔离，从而防止资源池内的跨租户/跨省的横向攻击。另外，在资源池的互联网边界，应通过传统的物理安全设备，如防火墙、抗 DDoS、IDS/IPS 等，构筑物理安全边界，防止来自互联网的攻击。

2.2.2.4 应用安全

- **入侵检测**
  - 支持为应用提供系统安全检测服务，防护远程连接 SSH 登录爆破、数据库登录爆破、服务软件漏洞被利用等系统入侵行为。
  - 对于 Web 应用，支持为应用提供 Web 应用防火墙（WAF）服务，防护 SQL 注入、XPath 注入、文件上传、CSRF、缓冲区溢出等 Web 入侵行为。
  - 支持为应用提供漏洞扫描和病毒检测服务，检测系统软件漏洞、应用程序漏洞、挖矿病毒、蠕虫等。

- **跨工作负载攻击防护**

为了降低跨工作负载攻击带来的风险，具有不同安全要求的工作负载应该工作在不同的安全域，并对工作负载之间的流量使用微隔离等机制进行控制。

- **恶意流量监测**

支持为应用提供恶意流量监测和防护，包括通过一键阻断来自指定区域的访问请求，解决部分地区高发的恶意请求问题或秒级阻断网站的恶意请求。

- **信令安全监测**

支持信令监测，对异常信令（如流量异常、报文异常等）进行告警。

2.2.2.5 数据安全

云平台数据安全可从采集、传输、存储、使用、备份、清除这六个方面入手，保证数据全生命周期的完整性、机密性和可用性。

- **数据采集**
  - 在取得用户同意授权的情况下，采用敏感数据自动识别等技术，对数据分类分级管理。
- **数据传输**
  - 在虚拟机迁移、网络配置、用户访问等相关数据的传输过程中，应提供数据完整性检测机制。并在数据完整性受到破坏时，提供数据完整性恢复功能。
  - 在虚拟机迁移、网络配置、用户访问等相关数据的传输过程中，使用加密传输机制或安全传输通道，保证数据的机密性。
  - 使用安全的密钥交换协议，保证密钥的安全性。
  - 应提供标准通用接口，确保业务系统及数据迁移的可移植性。
- **数据存储**
  - 敏感数据应根据相关要求进行分类分级。
  - 应根据业务场景及数据敏感级别，保证敏感性较高的数据加密存储，并支持 SM2/SM3/SM4 等国密算法。
  - 应提供虚拟机镜像文件完整性校验功能，当虚拟机镜像被恶意篡改时应能及时发现。
  - 进行密钥分层管理，并支持密钥替换。

- 完善数据备份存储及恢复机制，一旦数据损坏、丢失，能够及时恢复。
- 对虚拟机模版文件、配置文件等重要数据进行完整性检测。
- 应能针对平台内不同租户的存储数据进行有效隔离，防止不同租户间非授权访问。
- 不同云上应用数据，保证互相隔离，防止非授权访问。

- **数据使用**
  - 应对数据访问行为进行记录，并提供审计功能。应能对数据操作的访问流量进行保存，并能够提供流量回放功能。对流量保存的期限不少于 6 个月，对审计日志保存的期限不少于 6 个月。
  - 应对业务操作行为进行记录，并提供审计功能。应能够对业务操作的流量进行保存，并能够提供流量回放功能。对流量保存的期限不少于 6 个月，对审计日志保存的期限不少于 6 个月。
  - 应能够收集信息系统及相关网络设备、安全设备、主机、数据库、中间件等运行日志。
  - 在对云计算平台内敏感数据进行访问或分析时，应能根据业务场景及需求进行敏感数据脱敏处理。
  - 针对敏感数据的重要操作，使用多人审批-金库模式。
- **数据备份**
  - 应能够对被损害的敏感数据进行及时恢复。
  - 保证云上应用数据存在若干个可用的副本。
  - 各副本之间的内容应保持一致，当更新数据时，允许在一定时间区间内存在版本差异，但应保证在某个时间阈值后，各个副本之间内容应保持一致。
  - 采用数据周期性备份机制。
  - 数据备份可采用同步备份或者异步备份等方式，并应支持对数据的自动备份和手动备份。
  - 可通过虚机快照、数据快照、备份等方式进行数据恢复。
  - 对于物理网络或虚拟网络中的路由控制和云管理平台中的资源管理

等控制信息需做完整性校验，若发现完整性被破坏时可使用重传等机制进行恢复或数据修复。

- **数据清除**
  - 在清除敏感数据时，应确保敏感数据的所有副本都被同步清除，且被清除的数据无法恢复。
  - 针对个人信息超出存储期限的情况，可对个人信息进行删除或匿名化。
  - 生成相应的数据清除日志记录，包括删除时间、对象、请求的云上应用、删除副本数，及删除副本位置等。
  - 存放敏感信息的介质清理后不能用于存放公开信息。

2.2.2.6 接入安全

- **API 接口安全**
  - 对 API 调用进行强制访问控制，基于用户角色授权可调用的部分，确保用户使用的合法性，且方便进行合理的统计计费。设计独有的请求头、添加请求时间戳、校验 URI 的合法性、校验请求中的参数、标识 API 的版本号，确保客户端请求的可信度。
  - 所有授权调用的 API，均需在后台可查询管理，包括版本更新、参数映射配置、后端服务接口配置、API 操作（禁用、启用、修改、删除）、API 分组、API 级别等维度的管理。
  - 部署 API 网关，通过对 API 服务的统一接入、协议适配、流量管理与容错、以及安全防护，确保 API 接口服务的稳定性与安全性。
- **身份与密钥管理**
  - 对云服务用户及账号进行严格的身份访问控制，采用强密码验证与密码周期轮换等策略。
  - 身份管理系统需要提供用户身份的全生命周期管理，一旦检测到用户身份失效或发生变更，就需要同步、自动化地调整用户对资源访问的权限。
  - 基于业务需求，根据权限最小化原则，对账户及身份进行细分隔离。

- 加密密钥管理需要贯彻全生命周期，对密钥的生成、分发、存储、替换及销毁过程，进行定期地自动化更新，保证对用户资源的授权访问。

- **接入控制**

接入控制包括对用户接入应用的控制以及对运维人员接入设备的控制。当一个用户访问应用时，应由应用程序提供接入控制措施。如，移动云中的云游戏应用应对接入云游戏应用的用户提供用户名、口令或多因素认证等接入控制措施，并对权限进行检查。当研发人员或运维人员访问云基础设施或云管理平台等时，应对其设备、身份和权限进行检查。

针对高安全需求系统，应基于零信任来加强接入访问的安全性，即基于用户身份、设备、用户和设备行为等多认证因素对访问主体进行身份认证，并根据用户行为等安全上下文对访问主体进行持续信任评分，根据信任评分来动态分配访问权限。

2.2.2.7 安全运维

安全运维应做到设备资产清晰、网络运行稳定有序、事件处理处置有方、安全措施有效到位，具体包括如下要求。

- **资产管理**

中国移动云应支持准确识别所有资产。硬件资产应从“位置、型号、版本、访问 IP、入网时间、责任人”等维度进行描述；软件资产应从“承载设备、软件版本、维护地址、入网时间、责任人”等维度进行描述；检测类、防护类、监测及处置类的设备拓扑应进行描述，包括设备部署的位置、网络环境等；地址分配信息应进行描述，包括地址段申请情况、使用情况、VLAN 分配情况以及特殊接口上的信息等。

- **安全域管理**

隔离是任何安全的前提和关键。安全域管理应识别云中以及云间的安全域，包括安全域的名称、网段、划分时间、变更等。

- **变更与配置管理**

使用检测工具，对云服务的变更与配置操作进行监测，一旦发现错误的配置

与变更操作，立即进行告警通知，并对检测到的错误问题进行手动或自动修复。

- **安全基线合规及漏洞补丁管理**

应定期使用自动化检测脚本，对云服务的操作系统、数据库和中间件等的安全配置、变更操作进行核查，一旦发现错误的配置与变更操作，立即进行告警通知，并对检测到的错误问题进行手动或自动修复。应引入漏洞知识库，对漏洞发现、分析、整改、复核等全生命周期进行管理；应对补丁进行管理，只有经过测试验证，对业务没有影响的补丁才能入网。

- **4A 安全管控**

云网络中的应用资源、系统资源，均应纳入 4A 平台进行统一管理，通过使用账号管理、认证管理、授权管理、审计管理及金库管理等技术措施，确保云接入的安全性。

- **安全态势感知**

中国移动云支持根据收集的安全事件、安全日志、网络流量等，利用大数据、AI 等技术进行分析，形成云安全态势，从而实现安全威胁预判以及识别 APT 等新型攻击。中国移动的三朵云的安全态势感知平台可对接上一级安全态势感知平台，形成中国移动云安全态势。

- **安全知识管理**

基于内部获取到的威胁情报信息与外部共享的情报信息，定期更新包含 IP、域名、哈希值或 UserAgent 等在内的安全知识库，并建立三朵云的安全知识共享机制，保证安全知识在每个资源池内都能够有效使用。

- **安全管理平台**

安全管理平台支持对安全设备和安全策略进行统一的管理和编排。安全管理平台可对安全设备的安全日志、安全事件、可信完整性度量状态、云平台的异常行为等进行 AI/大数据分析，并给出安全处置策略，下发到安全设备和/或云平台上执行，实现智能检测、处置闭环。同时，安全管理平台支持对接安全态势感知平台或能力开放平台，接收安全服务请求并转化为安全策略下发到相关的安全设备，也可向安全态势感知平台上报态势。

3 云安全关键技术

3.1 基础设施可信

支撑移动云的主要基础设施可以划分为四个层面，包括物理层，资源虚拟化层、虚拟机层以及云管理平面。

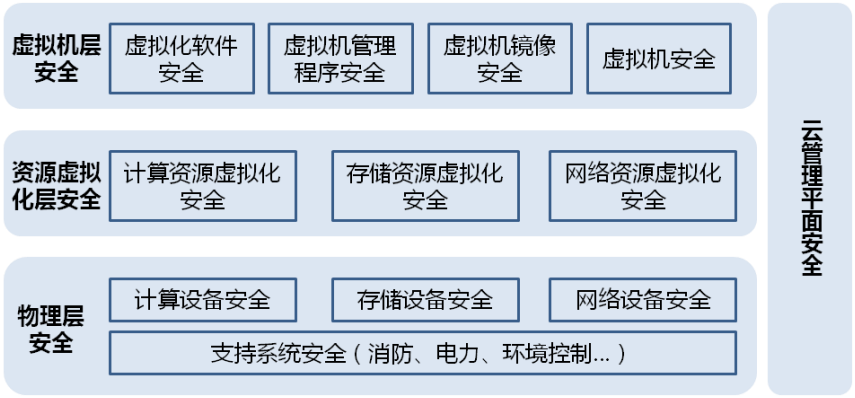

图 2 云基础设施安全层次

随着云化、软件化和虚拟化，以及云系统的开放性，云基础设施的暴露面日益增大，仅依赖当前的被动防御安全技术，难以应对层出不穷的新型攻击。随着等保 2.0 的正式发布和实施，可信验证被明确写入等保 2.0 的各级要求，利用可信计算技术，可对云基础设施四个层面中的设备和系统进行安全加固，为移动云系统构筑起主动的安全防护能力。

可信计算指在计算的同时进行安全防护，使计算结果总是与预期值一样，使计算全程可测可控，不受干扰。采用可信计算技术对云基础设施中的设备和系统进行主动防护的基本思路是：在设备启动的第一刻首先构建一个可信根，再建立一条信任链，从信任根开始到设备固件，BootLoader，操作系统，再到应用或虚拟机系统，一级认证一级，一级信任一级，把这种信任扩展到整个设备系统，从而确保整个设备系统的安全可信。其中主要涉及物理可信根、可信启动、可信度量、虚拟可信根、虚拟机可信启动、虚拟机可信度量、可信连接及可信证明等方面的技术。综合运用这些可信计算技术，可以实现对云系统的可信安全加固，具体如下表所示。

	物理层安全	资源虚拟化层安全	虚拟机层安全	云管理平面安全

可信连接及可信证明技术		*虚拟化控制连接及通信安全	*虚拟机管理连接及通信安全 *虚拟机迁移安全	*系统管理连接及通信安全
虚拟机可信度量技术			*云服务/云应用安全 *虚拟机关键数据安全	
虚拟机可信启动技术			*虚拟机 BIOS 及虚拟机 OS 安全	
虚拟可信根技术			*为虚拟机提供安全标识	
可信度量技术	*设备主体的应用程序及数据安全	*虚拟化控制程序安全 *虚拟化配置数据安全	*虚拟化软件安全 *虚拟机管理程序安全 *虚拟机镜像安全	*管理程序安全 *管理配置及数据安全
可信启动技术	*固件安全 *BootLoader 及 OS 安全	*控制器设备固件安全 *控制器 BootLoader 及 OS 安全		*管理设备固件安全 *管理设备 BootLoader 及 OS 安全
物理可信根技术	*为设备提供安全标识 *通过主动度量确保设备关键	*为虚拟化控制器设备提供安全标识 *通过主动度量		*为管理平面设备提供安全标识 *通过主动度量

	部件安全	确保设备关键部件安全		确保设备关键部件安全

表 1 可信计算技术与云系统的可信安全加固

此外还可在云管理平面构建一个可信安全管理中心，并通过可信连接的方式与云基础设施中的每一个可信设备建立起安全的管理通道，实现对设备的可信状态监测和安全策略管控，并进行动态关联感知，形成实时的安全态势，从而保证云服务系统整体的安全可信。

3.2 微隔离

当前资源池内的东西向流量已经成为资源池内的主要流量，而部署在边界的物理安全设备或虚拟化安全设备很难发现资源池内东西向流量的攻击（如资源池内跨租户攻击、跨省业务之间的攻击等），特别是同主机不同虚拟机之间不出物理网卡的东西向流量攻击。目前的 VLAN、VXLAN 等解决了租户、虚拟化网元的隔离，但没法对端口进行精细化的监测和控制。所以，需要使用微隔离技术对东西向流量进行全面精细的可视化分析，并进行细粒度的安全访问策略管理。

目前微隔离一般包括网络端口现状梳理、端口分析、端口监控和处置功能。其中：

- 端口梳理是通过端口扫描及流量分析的方式对资源池内的端口进行全面梳理，并发现网络端口中涉及敏感数据流转的端口以及敏感数据暴露面，根据敏感数据类型及严重程序对敏感数据端口进行敏感等级划分，针对不同敏感级别的端口制定差异化访问控制策略。
- 端口分析是通过机器学习和大数据算法对日志和安全信息的关联分析，对网络端口、访问 IP 及使用端口等建立正常网络端口和每个 IP、使用端口的行为画像，从基本业务操作、高频业务操作、业务操作稳定性（结合成为用户画像）等各维度构建特征工程，形成网络端口行为画像。
- 端口监控和处置是对网络端口异常流量、端口违规开放、异常操作行为、非授权访问等进实时监控、异常预警，并支持对异常业务系统及受影响的业务系统下发微隔离策略，可采用全量业务隔离或单项端口隔离。

端口梳理以及端口的监控均需基于端口、服务数据的采集，而处置策略也需

要由执行单元进行执行。目前的数据采集以及处置策略的执行方式主要由以下几种：

- 虚拟机上部署代理采集虚拟机流量，并执行处置策略。
- Host OS 上部署代理采集虚拟机网卡流量，并执行处置策略。
- 虚拟交换机镜像数据，虚拟交换机通过 ACL 执行处置策略。
- 单独虚拟机采集同主机虚拟机流量，执行处置策略。
- 采集容器与容器之间的连接，并执行处置策略。
- 采集 Pod 与 Pod 之间的连接，并执行处置策略。
- 采集微服务的连接，并执行处置策略。

3.3 应用安全

云服务与外部服务进行交互时，应通过使用端口白名单、脆弱性检测与安全加固、HTTP 请求内容检测及 DNS 安全等关键技术，确保云服务应用安全。

- **端口白名单**

云服务应根据业务需求，对端口进行统一梳理，集中管控，提供网络端口注册、系统登记、端口发布、端口有效性检测等管理能力。针对每一个白名单端口，建立访控列表（矩阵），仅允许访控列表（矩阵）中 IP 访问，并支持对端口启停状态、端口流量状态、端口网络数据内容等进行多维度的安全审计。

- **脆弱性检测与安全加固**

云服务应使用安全自动化运维工具，定期对应用程序的配置项、软件漏洞、微服务的列表和暴露端口等进行脆弱性检测，并根据检测结果，针对脆弱项进行配置变更、软件版本更新等安全加固操作，确保云服务的安全性。

- **HTTP 请求内容检测**

对于 HTTP 请求，应根据 HTTP 请求的 Referer 字段来对请求来源的域名进行筛选，包括对来源 Host 的地址进行识别和判断，防止产生盗链，使得云服务主机负载加重等。

- **DNS 安全**

基于正常访问网址的页面元素模板库，通过数据采集与异常行为分析技术，对 DNS 服务器解析后的 IP 地址进行分析，防止 DNS 被篡改、被污染、被劫持

等。

3.4 数据安全

基于云平台数据安全保护要求，应使用一定数据安全技术手段保障数据的机密性、完整性、可用性，典型手段包括数据脱敏、敏感数据自动识别、数据加密、日志审计等。

- **数据脱敏**

数据脱敏形态：按照实时性的不同，数据脱敏可分为静态脱敏和动态脱敏。静态脱敏适用于非实时场景，生产环境中的数据，脱敏后用于开发、测试、分析等用途。动态脱敏适用于生产环境等实时处理场景，当用户访问敏感数据时实时进行脱敏处理。

数据脱敏要点：

- 能针对不同用户和不同敏感数据根据需求设置不同的脱敏算法。
- 能支持动态添加或删除脱敏算法，同时确保系统平滑升级，应用无需中断。
- 能支持管理员配置用户查询特定数据库特定表、特定列的脱敏算法。
- 所选择脱敏算法具有一定的安全性、健壮性，不能被轻易破解或还原。
- 数据脱敏之后不影响业务连续性，不对系统性能造成较大影响。

- **敏感数据自动识别**

在对大量数据进行分类分级，寻找目标脱敏数据等过程中，可使用敏感数据自动识别技术，提高识别效率，可发生在数据采集到平台、数据存储、数据访问出平台等环节使用。

数据识别要点：

- 支持敏感数据定义，即可以配置敏感数据的匹配规则，当数据扫描时有数据匹配到该规则，该数据即判定为敏感数据。
- 可以灵活配置数据识别方式，具体识别方式包括基于数据内容的正则匹配、基于数据列名的识别、基于数据特征的匹配等。
- 支持黑白名单配置，运维人员可以手动配置黑白名单，提升数据识别效率。

- 数据识别需要考虑对线上系统的冲击，不能对正常业务有较大影响。

- **数据加密**

数据加密一般在数据存储、数据传输等阶段均有使用。

数据加密要点：

- 根据敏感数据的级别高低，对级别较高的数据采取加密存储。具体的数据加密存储方法包括应用层加密、数据库级加密、文件级加密、磁盘级加密和基于可信的加密方式等。
- 安全传输过程可采用 TLS/SSL 协议进行数据加密传输，也可采取建立 VPN 加密传输通道方式行安全传输。
- 所使用的密码算法、密码协议符合国家相关法律、行政法规和标准规范的要求，密码模块通过检测认证。

- **日志审计**

通过对日志数据的收集、积累和分析，能够发现系统内部用户的异常行为，并及时提醒审计人员。日志收集范围一般包括用户操作日志、运维人员操作日志等。

日志审计要点：

- 数据访问账号的创建、修改、查询、删除等；
- 账号是否最小化授权；
- 用户的登录、退出、数据查询、导入、导出等重要行为；
- 对涉敏信息处置环节开展审计，审计敏感数据未采用加密、模糊化、防拷贝等问题。

3.5 基于零信任的接入控制

为了保证云数据中心和用户业务的安全稳定运行，解决云计算带来的边界模糊、接入控制难等问题，在传统的 4A 接入管控之上，还可以基于零信任的理念，对接入的用户和设备进行联合身份认证、信任持续评级和动态自适应访问控制，并将审计结果作为信任评级的风险项，最终形成接入控制的闭环管理。

基于零信任的接入控制包括账户管理、身份认证、访问授权、操作审计四部分内容，示意图如下：

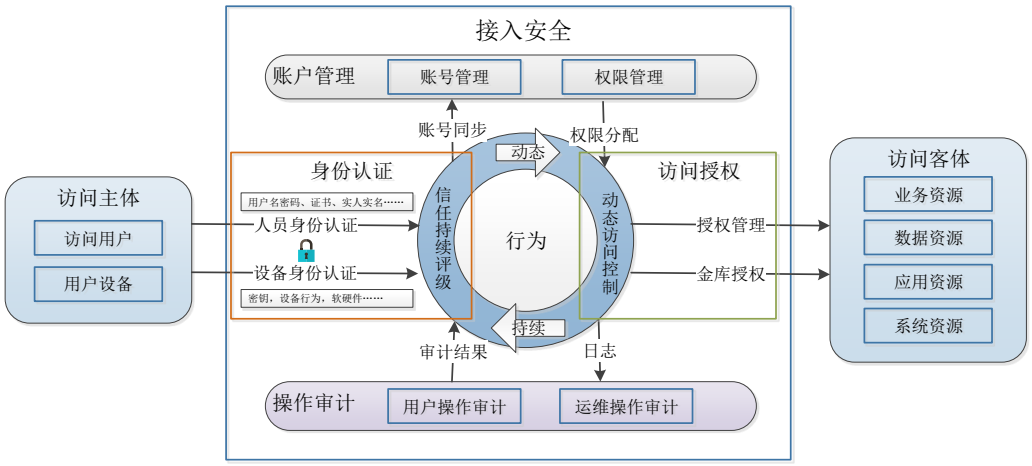

图 3 接入安全示意图

- **账户管理**

账户管理包括统一账号管理、权限管理两方面内容。

（1）统一账号管理：中国移动对主从账号生命周期、主从账号对应关系、账号密码策略和账号同步等进行统一管理。同时，应用 CAS、OpenID 和 OAuth2 等单点登录技术等单点登录技术，使用户只需登陆一次即能以不同的权限访问不同的资源，而无需重复登录多个系统。

（2）权限管理：中国移动根据不同业务维度和相同业务不同职责，实行 RBAC 权限管理。在此基础之上，还可以配合零信任架构的信任评级机制，对不同访问资源的权限进行动态管理。

- **身份认证**

身份认证包括设备、人员、设备+人员身份认证和信任评级四方面内容。

（1）设备身份认证：接入设备可以根据自身安全能力，使用基于对称密钥、非对称密钥、设备软硬件特征、设备行为特征、设备环境特征等因素以及多因素结合的认证方式。其中，基于设备行为特征的认证技术是重要的发展方向之一，即使用人工智能算法分析设备行为特征，判断设备行为与身份匹配程度，从而提高认证安全性又无需改造设备。

（2）人员身份认证：人员身份认证分为运维人员和用户身份认证，可基于用户名密码、手机验证码、用户证书、用户实人实名、临时用户凭证等因素来实现认证。其中用户实人实名认证是用户身份认证服务未来的重要发展方向，即基于人脸、指纹、指静脉等生物识别技术，配合身份证核验和手机号核验等技术进

行，自然人+有效证件+手机号+账号的用户真实身份验证。

（3）设备+人员身份认证：在传统的认证方案中，一般对设备和用户进行单独认证，但是设备和用户是访问请求中密不可分的上下文，应基于零信任中设备与人员配合认证的理念，将登录设备与用户身份进行绑定，作为整体进行认证，以加强身份认证的安全性。常见实现方式是在设备上安装专用浏览器、安全沙箱、Agent 等安全代理，安全代理会将用户和设备的绑定关系发送给云端，由云端判定两者绑定关系是否合法，最终实现设备+人员的身份认证。

（4）信任持续评级：在身份认证过程中，还可以持续采集用户的生物特征、操作行为、以及设备软硬件状态、行为特征和环境状态等相关信息，借助模糊综合评价，灰色系统综合评价等综合评价算法进行统一的风险分析和度量，并输出动态的信任评分，来实现信任的持续评级。

- **访问授权**

访问授权包括：授权管理、金库授权、动态访问控制三方面内容。

（1）授权管理：对访问主体的权限分配遵循最小权限原则，基于角色的访问控制允许该角色只能够访问特定的资源、只能够进行特定的操作。

（2）金库授权：对于高权限、高风险操作，采用金库式管理对申请人员进行审批和授权，通过多人制衡方式来实现监督和控制的效果。

（3）动态自适应访问控制：在 RBAC 权限管理基础上，还可以借鉴零信任的细粒度动态访问控制理念，依据信任的持续评级结果，对所有的访问请求进行细粒度的权限判定和动态授权。

- **操作审计**

操作审计包括用户操作审计和运维操作审计两方面内容。

（1）用户操作审计：中国移动为用户提供统一的云资源操作日志管理，记录云账号用户的登录登出和操作日志，使用户可以实现安全分析、事后追踪和合规审计。

（2）运维操作审计：中国移动对运维人员、运维行为进行审计，日志采集范围包括三部分：接入资源侧的原始日志、管控平台侧记录的维护人员对接入资源的操作日志、管控平台自身操作日志。

（3）审计结果上报：审计日志的审计结果也可以作为信任评级的打分依据，

实现身份和信任的闭环管理。

3.6 智能安全检测和处置

云化网络中应用动态上线，每个应用的安全需求也存在差异性，传统的在安全设备上手工配置安全策略的方式工作量大、易出错。并且，安全设备均基于已有特征被动识别安全威胁，无法检测未知的安全威胁。所以，应基于安全管理平台，协同云基础设施和安全设备实现主动、智能识别安全威胁和处置，从而实现安全运维的智能化和自动化应，具体包括：

- 云基础设施支持检测文件异常、进程异常、账号异常等异常行为，并将检测到的异常行为上报给云安全管理平台。
- 安全设备将安全日志和安全事件上报给云安全管理平台。
- 云安全管理平台使用大数据和 AI 技术，对收到的异常行为和安全设备的安全日志进行智能分析，预测安全威胁，提前预警，并给出处置建议。
- 云安全管理平台根据处置建议，结合网络拓扑，协同 SDN 控制器，对安全设备进行编排，实现对安全威胁的处置，从而实现主动、智能的安全检测和处置系统。

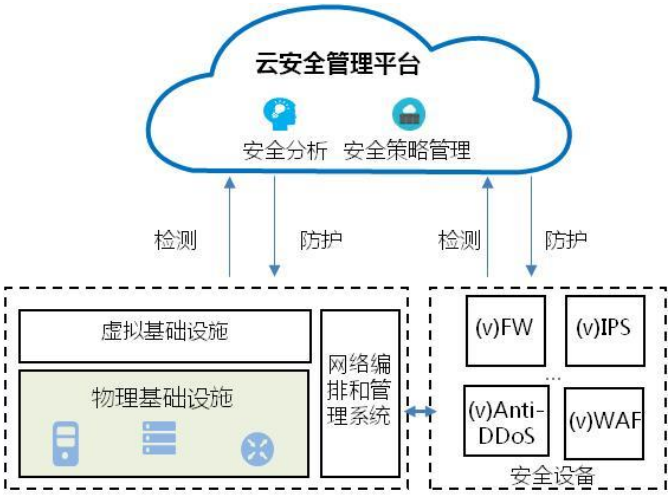

图 4 基于云安全管理平台的智能安全检测和处置

4 云安全生态

本章节介绍中国移动的云与用户之间的责任边界划分，以及为用户提供的灵

活安全服务。通过明确安全责任边界、提供云平台基础安全能力以及定制化的增值服务，与用户、第三方厂家构建共赢的云安全生态。

4.1 责任共担模型

信息系统在传统模式下，按照谁主管谁负责、谁运营谁负责的原则，有着明确的责任划分。然而，在云计算模式下，云计算平台的管理和运行主体与数据安的责任主体不同。云计算不同的服务模式和部署模式，以及云计算本身环境的复杂性，增加了云计算责任界定的难度。以云服务提供商、云租户为主要责任方，构建责任共担模型，明确云计算各个逻辑层次的安全责任人，可以有效划分责任边界。

中国移动作为云服务商，主要负责为云租户提供服务的实体，建设并管理用于提供服务的云基础架构，基于 IaaS、PaaS、SaaS 这三种服务模式，通过网络向云租户提供云服务。中国移动向云租户提供云服务，在确保云平台安全控制措施的有效性，重大变更风险的可控性，以及应急响应的时效性的同时，需要根据不同的服务模式，担负与之相应的安全责任。

- IaaS 服务模式：需要保证物理资源、网络资源、存储计算、Hypervisor 的安全性。
- PaaS 服务模式：需要保证物理资源、网络资源、存储计算、Hypervisor、虚拟化网络、操作系统、中间件、Runtime 的安全性。
- SaaS 服务模式：需要保证物理资源、网络资源、存储计算、Hypervisor、虚拟化网络、操作系统、中间件、Runtime、应用程序的安全性。

云租户是为使用移动云资源同中国移动建立业务关系的参与方。云租户可以直接作为用户使用移动云提供的云服务，也可以作为云代理商，为保证用户使用云服务的运行稳定而提供服务计量、计费与资源购买等运行管理服务。

云租户作为移动云的使用者，也需要根据不同的云服务模式，担负与之相应的安全责任。

- IaaS 服务模式：需要保证虚拟化网络、操作系统、中间件、Runtime、应用程序、数据的安全性。
- PaaS 服务模式：需要保证应用程序、数据的安全性。

- SaaS 服务模式：需要保证数据的安全性。

综上所述，中国移动的云服务安全责任共担模型如下图所示。

图 5 中国移动的云服务安全责任共担模型

4.2 灵活的安全服务

中国移动作为云服务商，通过建设云服务自身的安全能力，向云租户提供安全的云服务，保障云租户的业务正常开展。安全服务是以服务的方式提供安全能力。中国移动通过提供灵活多元的安全服务，协助云租户做好安全责任范围内的安全防护，来确保云租户的业务安全。

中国移动安全服务，可以分为基础安全防护与增值服务两大服务模式。基础安全防护嵌入到云服务中，开通即使用，为所有云租户进行免费开放。增值服务进行按需提供，只有云租户要求时才会开通使用。根据不同的场景需求，提供灵活的安全服务，可以提升云租户的体验，增强移动云的服务黏性。

中国移动在加强自身安全服务能力建设的同时，也会引入业界第三方安全服务企业，与之携手共同建设可持续发展的云安全生态，为用户提供安全可靠的云安全服务，保障用户业务安全的同时，促进云生态的健康发展。

5 总结与展望

本白皮书在分析中国移动云现状、安全风险的基础上，提出了中国移动的云安全防护框架，并描述了云安全要求以及相关的安全关键技术、云安全生态。随着云计算、5G 等的快速发展，中国移动云将以业务需求为导向，在遵从法律法规要求的基础上，不断提升云安全防护能力，协同发展三朵云，构建主动、纵深的云安全防护体系，为云上业务的安全运行提供有力安全保障。

未来，中国移动在加强自身云安全能力建设的同时，将携手业界的龙头云安全服务企业，构建具有统一认证、智能共识、智能防御等能力的主动、纵深云安全防护体系，实现云网、云数、云智、云边领域安全的深度融合，打造出数字化、智能化、原生化的云安全产品，为用户提供安全可靠、极致性能、按需供应的云安全服务。

缩略语列表

缩略语	英文全称	中文含义
4A	Account，Authentication，Authorization，Audit	账号管理，授权管理，认证管理，审计管理
API	Application Programming Interface	应用程序编程接口
CAS	Central Authentication Service	中央认证服务
CNCF	Cloud Native Computing Foundation	云原生计算基金会
CRSF	Cross-site Request Forgery	跨站请求伪造
DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
DNSSec	Domain Name System Security Extensions	域名系统安全扩展
DoS	Denial of Service	拒绝服务
GRE	Generic Routing Encapsulation	通用路由封装
IaaS	Infrastructure as a Service	基础设施即服务
IDS	Intrusion Detection System	入侵检测系统
IPS	Intrusion Prevention System	入侵防御系统
KVM	Kernel-based Virtual Machine	基于内核的虚拟机
LAN	Local Area Network	局域网
MANO	Management and Orchestration	管理和编排
NFV	Network Function Virtualization	网络功能虚拟化
OAuth2	Open Authorization	开放授权协议 v2
OpenID	Open Identity	开放身份鉴权
PaaS	Platform as a Service	平台即服务
RBAC	Role-Based Access Control	基于角色的访问控制
REST	Resource Representational State Transfer	资源表征性状态转移
SaaS	Software as a Service	软件即服务
SDN	Software Defined Network	软件定义网络
SDS	Software Defined Security	软件定义安全
SOAP	Simple Object Access Protocol	简单对象访问协议
SQL	Structured Query Language	结构化查询语言
SSL	Secure Sockets Layer	安全套接字协议
TLS	Transport Layer Security	传输层安全性协议
VIM	Virtualized Infrastructure Manager	虚拟化基础设施管理器
VLAN	Virtual Local Area Network	虚拟局域网
VM	Virtual Machine	虚拟计算机
VPN	Vitual Private Network	虚拟专用网络
VXLAN	Virtual eXtensible Local Area Network	虚拟扩展局域网
WAF	Web Application Firewall	Web 应用防护系统
WAN	Wide Area Network	广域网
XPath	XML Path Language	XML 路径语言

参考文献

[1]GB/T 21052-2007《信息安全技术 信息系统物理安全技术要求》

[2]GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》

[3]GB/T 22239-2019《网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求》

[4]GB/T 37092-2018《信息安全技术 密码模块安全要求》

[5]GB/T 38541-2020《信息安全技术 电子文件密码应用指南》

[6]GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》

[7]GM/T 0054-2018《信息系统密码应用基本要求》

[8]中国移动 《中国移动 IT 领域云计算安全防护技术要求及实施指南》

[9]中国移动 《中国移动网络云网络安全技术要求》