Umeet 网络会议

——安全白皮书

2020 年 02 月

尚阳科技股份有限公司

目 录

文 档 信 息

文 档 名 称	**Umeet 网络会议安全白皮书**
文 档 编 号	
文 档 类 别	技术文档 ■ 服务文档 □ 其他 □
当 前 版 本	1.2
创 建 日 期	2020-02
文 档 作 者	曾成
联 系 方 式	zc@systec.com.cn

第 1 章 概况

Umeet 网络会议数据安全和用户隐私是尚阳最重要的原则。尚阳致力于打造公共、开放、安全的云视频平台。Umeet 云视频会议，在线会议，群消息，在一个易于使用的平台上提供软件定义会议解决方案。Umeet 网络会议可以在 Windows、Mac、iOS、Android 终端上提供最佳的视频、音频、无线分享自己电脑桌面。

Umeet 网络会议在公有云或混合云部署当中，始终将安全性放在最高优先级。Umeet 网络会议致力于不断提供健壮的安全特性来满足企业的安全合作需求。

而阿里云作为 Umeet 网络会议基础架构；竭诚为 Umeet 网络会议提供稳定、可靠、安全、合规的云计算基础服务，保护系统及数据的机密性、完整性、和可用性。

第 2 章 安全责任共担

基于阿里云的 Umeet 网络会议，其安全责任由双方共同承担:阿里云要保障云平台自身安全并提

供安全产品和能力给云上 Umeet 网络会议;尚阳负责基于阿里云服务构建的应用系统的安全。

阿里云负责基础设施(包括跨地域、多可用区部署的数据中心，以及阿里巴巴骨干传输网 络)和物理设备(包括计算、存储和网络设备)的物理和硬件安全，并负责运行在飞天分布式云操作系统之上的虚拟化层和云产品层的安全。同时，阿里云负责平台侧的身份管理和访问控制、 监控和运营，从而为客户提供高可用和高安全的云服务平台。

Umeet 网络会议负责以安全的方式配置和使用各种云上产品，并基于这些云产品的安全能力以安全可 控的方式构建自己的云上应用和业务，保障云上安全。阿里云基于阿里巴巴集团多年攻防技术 积累，为客户提供云盾安全服务，保护客户的云上业务和应用系统。阿里云建议客户选择使用 云盾安全服务或者阿里云安全生态里的第三方安全厂商的安全产品为其云上应用和业务系统提供全面的安全防护。

安全责任共担模式之下，阿里云保障云平台层面的安全并提供一方集成的云产品安全能力和云盾安全服务给客户使用，让客户降低对安全性的顾虑，更专注于核心业务发展。

2.1 尚阳安全责任

尚阳基于阿里云提供的服务构建自己的云端应用系统，综合运用阿里云产品的安全功能、 云盾安全服务以及安全生态提供的第三方安全产品保护自己的业务系统。

尚阳应对云上产品进行安全配置管理，保障云上业务的基础安全和数据安全。请注意，尚阳在阿里云上如果使用的是基础类服务(例如，阿里云提供的云服务器(ECS))，那么相关服务实例完由尚阳控制，尚阳对管理实例进行了安全配置，并应加固租用的云服务器操作系统、 升级补丁、配置安全组防火墙进行网络访问控制。

尚阳使用阿里云产品的原生加密能力或云盾加密服务对敏感数据进行加密，并对加密密钥进行妥善管理(例如，使用密钥管理服务(KMS)的托管 HSM 能力)。

尚阳阿里云上的应用和业务系统已通过使用云盾安全服务以及安全生态提供的第三方安全产品来保护。并使用云盾安全服务对云上应用和业务系统，包括云上资源进行有效的安全监控和运营。在账户安全层面，尚阳保护阿里云账户认证凭证(例如，开启多因素认证 功能)，并在账号设置上遵循最小权限原则，通过如群组授权等手段实现职责分离。尚阳使用阿里云操作审计服务(ActionTrail)记录管理控制台操作及 OpenAPI 调用日志，对账号操作进行审计。

2.2 阿里云安全责任

阿里云负责基础设施、物理设备、分布式云操作系统及云服务产品安全，并为 Umeet 网络会议提供保护云端应用及数据的技术手段。

阿里云保障云平台自身安全，包括但不限于:

- 保障云数据中心物理安全。
- 保障云平台硬件、软件和网络安全，包括操作系统及数据库的补丁管理、网络访问控制、DDoS 防护、灾难恢复等。
- 及时发现云平台的安全漏洞并修复，修复漏洞过程不影响 Umeet 网络会议业务可用性。
- 通过与外部第三方独立安全监管与审计机构合作，对阿里云进行安全合规与审计评估。

阿里云为 Umeet 网络会议提供保护云端信息系统的技术手段，包括但不限于:

- 提供多地域、多可用区分布的云数据中心以及多线 BGP 接入网络，利用阿里云基础设施构建跨机房高可用的云端应用。

- 提供安全的硬件基础设施和设备。
- 提供云上账户安全管理能力，包括但不限于云账号支持主子账号、多因素认证、分组授权、细粒度授权、临时授权等账户安全管控手段。
- 提供安全监控和运营能力，包括安全审计手段。
- 提供数据加密手段。
- 提供各类安全服务。
- 引入第三方安全厂商，提供个性化的行业安全解决方案。

第 3 章 Umeet 网络会议安全

3.1 个人信息保护

长期以来，尚阳坚持致力于保护每位用户的个人信息，保证用户对所有提供给 Umeet 网络会议的个人信息拥有所有权和控制权。与此同时，尚阳积极响应国家监管部门对企业承担个人信息 保护责任的号召，持续完善内部的个人信息管理和保护体系。尚阳设置了专业的个人信息保护团队，在隐私权政策、用户权利保障等方面持续优化，建立了内部整体的数据安全管理体系， 落地数据安全保护的核心技术，为用户个人信息提供了全生命周期的安全可靠的保护能力。

尚阳将持续建设个人信息 保护管理体系，除了关注尚阳作为控制者角色时云平台自身的个人信息保护能力之外，会进一步投入力量建设作为数据处理者的角色时个人信息保护能力。

Umeet 网络会议的隐私权政策可以在阿里云官网查看，有任何隐私相关的问题都可以通过邮件 umeet_support@systec.com.cn 或电话客服进行反馈。

3.2 基础架构

Umeet 网络会议是一个专有的全球网络,提供高质量沟通体验。Umeet 网络会议实时媒体服务器托管在阿里云一级数据中心。

在 Umeet 网络会议基础设施拥有一套低延迟的分布式网络多媒体路由器(软件)。使用这些低延迟多媒体路由器，所有来自主机设备和到达参与者设备的会话动态切换。

客户端与云端服务器通过 https（443 端口/TLS）建立连接。

3.3 客户端安全

基于角色的用户安全（端到端加密）；

- ✧ 开启端到端加密会议
- ✧ 使用标准的用户名和密码或 SAML 单点登录
- ✧ 密码保护的会议
- ✧ 可预约一场密码保护的会议

有选择性邀请参会者（email, IM or SMS.）；

会议详细信息存储在 Umeet 网络会议安全数据库；

高级加密标准（AES256）位算法加密所有的演讲内容；

使用加密标准（AES256）位加密聊天会话；

3.4 会议安全

- 基于角色的用户安全；

会议主持人拥有以下安全功能：

✧ 驱逐一个参与者或所有参与者

✧ 结束一场会议

✧ 锁定一场会议

✧ 与参与者或所有参与者聊天

✧ 静音/不静音一个参与者或所有参与者

✧ 启用/禁用一个参与者或所有参与者记录

✧ 当打开一个新窗口，临时暂停分享电脑屏幕

会议的参与者拥有以下安全功能：

✧ 静音/不静音

✧ 开/关视频

- 开放或拥有密码的会议；
- 编辑或删除会议；
- 会议中的安全；

使用 AES256 加密标准加密所有屏幕共享内容

使用 256 位 TLS 加密标准加密网络连接

- 客户端和会议服务器使用 256 位传输层 TLS 加密隧道

3.5 管理控制

以下是提供给管理员的安全功能：

-安全使用标准的用户名和密码登录选项或 SAML 单点登录。

-添加用户和管理员账户

-用户订阅级别升级或降级

-删除用户账户

-审查账单和报告

-管理账户仪表板和云录音

3.6 特殊的安全特性/API

- 会议服务器

会议服务器位于中国境内云端，服务器不记录、不向其他目标位置转发任何会议信息。也可以在客户指定的位置（内部网络）部署自己的会议服务器。

使用 256 位 TLS 加密标准建立安全的通信网络和使用 AES256 加密标准加密共享内容。

- 网络研讨会

可以使用 Umeet 网络会议召开 1000 人的高清视频会议，还可以召开 10000 人的视频大会（Video Webinar）!

- 记录存储

Umeet 网络会议为我们客户提供记录和分享他们的会议。录音可以存储在本地，也可以在 Umeet 网络会议云端。

记录发起者可以通过受保护的 Web 界面管理他们的录音。录音可以下载，分享或删除。

- Umeet 网络会议只有存储基本信息

。

第 4 章 Umeet 网络会议基础设施

Umeet网络会议是基于阿里云云主机方式部署，同时阿里云为Umeet网络会议提供全球部署、多地域多可用区的云数据中心;采用多线 BGP 网络提高网络访问体验;飞天分布式云操作系统为所有云产品提供高可用基础架构和多副本数据冗余;全球领先的热升级技术使得产品升级、漏洞修复都不会影响客户业务;高度自动化的运维及安全， 国内外相关权威机构的认可的合规性;高可用、安全、可信的云计算基础设施。

阿里云在全球部署数据中心，同地域支持多个可用区。客户业务跨地域、跨可用区部署，可实现高可用架构，例如同城应用双活、异地数据灾备、异地多活，两地三中心。

第 5 章 云安全架构

5.1 数据存储的持久性

Umeet 网络会议数据中心建设满足 GB 50174《电子信息机房设计规范》A 类和 TIA 942《数据中心 机房通信基础设施标准》中 T3+标准，其中包含本章以下物理与环境安全控制要求。

合同期内每月云主机和块存储的用户应用和用户的内容文件持久性为 99.99%，意为每月用户 10000 个存储的文件，合同期内每月数据不丢失的概率为 99.99%，即每月只有 1 个文件丢失的可能性。

阿里云块存储(Block Storage)，是阿里云为云服务器 ECS 提供的低时延、持久性、高可 靠的数据块级随机存储。块存储支持在可用区内自动复制用户的数据，防止意外的硬件故障导致数据不可用，以保护用户的业务免于组件故障的威胁。就像对待硬盘一样，用户可以对挂载 到 ECS 实例上的块存储做格式化、创建文件系统等操作，并对数据持久化存储。

5.2 数据可销毁性

安全擦除

Umeet 网络会议建立了对设备全生命周期(包含接收、保存、安置、维护、转移以及重用或报废)的 安全管理。设备的访问控制和运行状况监控有着严格管理，并定期进行设备维护和盘点。建立废弃介质上数据安全擦除流程，处置数据资产前，检查含有敏感数据和正版授权软件的媒介是否已被覆写、消磁或折弯等数据清除处理，且不能被取证工具恢复。当因业务或法律原因，不再需要某些硬拷贝材料时，将其物理破坏，或取得数据处理第三方的损坏证明，以确保数据无法重建。

云服务数据处置

尚阳在终止为云服务客户提供服务时，及时删除云服务客户数据资产或根据相关协议要求返还其数据资产。基于阿里云数据清除技术满足行业标准，清除操作留有完整记录，确保数据不被未授权访问。

运维人员未经客户许可，不得以任意方式访问客户未经公开的数据内容。遵循生产数据不出生产集群的原则，从技术上控制了生产数据流出生产集群的通道，防止运维人员从生产系统拷贝数据。

设备报废方法

第一，数据质量远比数据的数量重要，要注重有效数据的处理。所以任由数据量增长下去，数据中心会很快不断扩容，结果数据中心的规模越来越大，而数据中心业务并没有实质增长。数据切不可成为数据中心的负担，该清理时就清理，该销毁时就销毁。

第二，我们对数据进行销毁，这就要从数据产生的源头做起。管理这些数据是非常复杂的，涉及到数据辨识、清理、优化等等，而这些工作又是周期性，需要花费时间和一定的人力资源，且不会带来明显的收益，常常被忽视。其实，数据的有效存储工作将对数据中心的业务产生长期和正面的收益，且越早行动收益越明显。

第三，数据的销毁并不是简单的删除清空这样简单，销毁的手段也有几种，分为软销毁和硬销毁两种。软销毁是通过数据覆盖等软件方法数据销毁或者数据擦除。硬盘数据销毁中的硬销毁则通过采用物理、化学方法直接销毁存储介质，以达到彻底的硬盘数据销毁的目的。软销毁一般只是将数据文件进行销毁，并不能真正将磁盘区数据擦除，操作系统由于考虑到操作者操作习惯或者误操作，数据销毁后各种非常情况等诸多方面因素，用户所使用的删除命令，只是将文件目录项做一个删除标记，把它们在文件分配表中所占用的簇标记为空簇，并没有对数据区进行任何改变也就是没有对这些信息做任何数据擦除、数据销毁的操作，这样数据其实依然占用存储空间，没有达到节省存储空间的目的。所以数据中心的数据销毁都采用硬销毁的方式，真正将存储空间释放出来，用来存放更有意义的数据。硬销毁常用的方法有：格式化硬盘、硬盘分区、文件粉碎软件。还有一种硬销毁是采用专用的消磁硬盘机或者折弯机来彻底销毁数据，不管是直接对硬盘进行消磁，还是对硬盘进行折弯，都是破坏性的行为，硬盘将被损坏，不仅数据不能再还原，硬盘也无法再进行使用，这种硬销毁往往是用来对已经故障的硬盘进行处理，避免故障硬盘里存着的数据被外人还原出来，拿着数据去做坏事。

及时对数据中心中的无用数据进行销毁，不仅可以节省硬盘存储空间，还可以提升安全性，避免一些数据泄露，给数据中心带来安全隐患。所以对于无用数据要进行彻底销毁，不让任何人有可乘之机，更不能让人有机会再还原出来利用。

5.3 数据可迁移性

Umeet 网络会议基于阿里云主机搭建的软件应用，不管从软件层面或者是硬件层面，都能保证启用或弃用该云服务时，数据能迁入和迁出。

另外阿里云硬件架构通过了国内权威认证<<云计算服务认证>>，阿里云云主机、云数据库产品和服务对数据可销毁性、数据可迁移性、数据私密性、 数据知情权等进行了规范。

5.4 数据私密性

通过了国内权威认证<<云计算服务认证>>，阿里云云主机、对象存储、云数据库、内容分发等多款产品和服务获得可 信云全国首批云服务认证，对数据可销毁性、数据可迁移性、数据私密性、数据知情权等进行了规范。

5.5 数据知情权

通过了国内权威认证<<云计算服务认证>>，阿里云云主机、对象存储、云数据库、内容分发等多款产品和服务获得可 信云全国首批云服务认证，对数据可销毁性、数据可迁移性、数据私密性、数据知情权等进行了规范。

5.6 服务可审查性

依赖阿里云通过的国内权威中央网信办云服务安全审查 ， 成为全国首批通过中央网信办云计算网络安全审 查(增强级)的云计算服务 。

5.7 服务功能

尚阳承诺用户提供如下功能：

- ✧ 会议前基本功能

  固定 ID 修改

  安排会议

  设置主持人入会前，参会者可提前入会

- ✧ 会议中基本功能

  主持人清除并将所有注释

  会议通知（邮件、链接、QQ、微信）

  本地录制

  远程控制

  会议中聊天、保存记录

  一键静音

  共享屏幕

  多人屏幕共享

  主持人控制

  举手功能

  分组讨论

  在等候室允许所有参会者进入

  会议中文件传输

- ✧ IM 收发消息

  单聊发送/接收文本、表情、图片、消息；

  IM 邀请参会者（已安装 Umeet 网络会议客户端）

- ✧ 音视频会议-分别用音频、视频测试会议

  具体操作说明-参考 Umeet 网络会议操作手册

5.8 服务的可用性

尚阳承诺用户服务可用性：不低于 99.9%。

服务可用性的计算公式：实际可用性=（总时间-实际不可用时间）/总时间×100%

5.9 服务资源调度能力

尚阳承诺用户，可以满足业务资料的 30%的并发容量，24 小时完成；100%的并发扩容需要 2 天；每次最大可扩容 100%容量，最小 60000 并发参会者容量。

5.10 故障恢复能力

尚阳承诺由于统计或计费逻辑造成云服务不可用，可临时将统计计费下线优先保障客户的服务，系统架构设计上可以支持降级，保证服务运行。

5.11 网络接入性能

Umeet 网络会议目前使用的是阿里云的 VPC 的共享带宽包的方式，可根据业务的情况动态扩容；目前 Umeet 网络会议出口平均使用带宽是 8Gbps 的带宽左右。

5.12 服务计量准确性

线下付费方式，主要是根据用户沟通的会议并发方式-100 方、300 方、500 方、1000 方视频会议来计算费用，按年计费 。

参考<<CLOUD_Umeet 报价_20200511>> (因价格比较特殊，暂时不对外发布)

5.13 服务安全性

5.13.1 身份认证

身份认证是指通过凭证信息认证用户的真实身份。它通常是指通过登录密码或访问密钥(Access Key，简称 AK)来进行认证。请注意，用于身份认证的凭证信息对于用户来讲是秘密 信息，用户必须妥善保护好身份凭证信息的安全。

1） 账号密码认证

用户可以使用其云账号(即主账号)或其云账号下 RAM 用户的密码登录阿里云控制台并对 其云上资源进行操作。阿里云的账号密码规范、登录安全风控策略由阿里云统一管理。云账号 下子用户(RAM 用户)的密码策略则可以由客户自己设定，如密码字符组合规范、重试登录次 数、密码轮转周期等策略。例如，用户可以通过 RAM 控制台为 RAM 用户创建密码策略，以保 证各个子用户都使用定期轮转的强密码从而提高整体账户的安全性。

2) Access Key(AK)认证

阿里云的 Access Key(AK)是用户调用云服务 API 的身份凭证，用于在用户通过 API 访问阿里云资源时对用户身份进行认证。API 凭证相当于登录密码，只是使用场景不同。前者用于程序方式调用云服务 API，而后者用于登录控制台。

Access Key 包括访问密钥 ID(AK ID)和秘密访问密钥(AK Secret)。AK ID 用于标识用户，而 AK Secret 用来验证用户身份的合法性。用户在调用资源时会传入 AK ID，并使用 AK Secret 对请求进行签名(HMAC-SHA1 算法)。用户可以登录阿里云用户中心或 RAM 控制台来管理 Access Key，包括创建、冻结、激活和删除操作。Access Key 是可以长期使用的 API 访问密钥， 建议用户在使用时要考虑对 Access Key 的周期性轮转。

请注意，出于有效权限分割和降低风险的考虑，云上最佳安全实践中不建议用户为其云账 号(即主账号)创建 AK 凭证，而建议为其下属的 RAM 用户各自创建 AK 凭证。

3) STS 认证

阿里云 Security Token Service(STS)是为 RAM 用户、阿里云服务、身份提供商等受信实体提供短期访问资源的权限凭证的云服务。有时存在一些用户(人或应用程序)，他们并不经常 访问客户云账号下的云资源，只是偶尔需要访问一次，这些用户可以被称为“临时用户”;还 有些用户，例如运行在不可信移动设备上的 App，由于自身安全性不可控，不适合颁发长期有 效的访问密钥。这些情况下，可以通过 STS 来为这些用户颁发临时权限凭证。颁发令牌时，管 理员可以根据需要来定义令牌的权限和自动过期时间(默认为 1 小时过期)。

STS 访问令牌是一个三元组，它包括一个安全令牌(Security Token)、一个访问密钥 ID (Access Key ID) 和一个秘密访问密钥 (Access Key Secret)。用户在调用资源 API 时传入安 全令牌和访问密钥 ID，并使用秘密访问密钥对请求进行签名(和上述 AK 签名机制相同)。

4） MFA 认证

MFA 是一种简单有效的最佳安全实践方法，它能够在用户名和密码之外再额外增加一层安全保护。启用 MFA 后，用户登录阿里云时，系统将要求输入用户名和密码(第一安全要素)， 然后要求输入来自其 MFA 设备的可变验证码(第二安全要素)。这些多重要素结合起来将为用 户的账户提供更高的安全保护。阿里云可以支持基于软件的虚拟 MFA 设备。虚拟 MFA 设备是产 生一个 6 位数字认证码的应用程序，它遵循基于时间的一次性密码(TOTP)标准(RFC 6238)。 此应用程序可在移动硬件设备(包括智能手机)上运行。

5） SSO 认证

阿里云支持基于 SAML 2.0 的单点登录(Single Sign On，简称 SSO)，可以支持企业客户 使用企业自有身份系统(作为 Identity Provider)的登录服务登录访问阿里云(作为 Service Provider)。

为了满足不同企业客户的登录场景需求，阿里云提供了以下两种基于 SAML 2.0 协议的 SSO 机制:

- ● 用户 SSO:阿里云通过身份提供商 IdP 颁发的 SAML 断言(SAML Assertion)确定企 业用户与阿里云 RAM 用户的对应关系。企业用户登录后，使用该 RAM 用户访问阿里云 资源，对应的访问权限由 RAM 用户的授权策略所限制。
- ● 角色 SSO:阿里云通过身份提供商 IdP 颁发的 SAML 断言(SAML Assertion)确定企业 用户在阿里云上可以使用的 RAM 角色。企业用户登录后，使用 SAML 断言中指定的 RAM 角色访问阿里云资源，对应的访问权限由 RAM 角色的授权策略所限制。

6） SSH 密钥对

针对 ECS Linux 实例，阿里云提供了 SSH 密钥对作为认证方式。SSH 密钥对是通过一种加 密算法生成的一对密钥:一个对外界公开，称为“公钥”;另一个由用户自己保留，称为“私钥”。如果用户已经将公钥配置在 Linux 实例中，那么，在本地或者另外一个实例中，用户可以使用私钥通过 SSH 命令或相关工具登录之前有公钥配置的实例，而不需要输入密码。SSH 密钥对默认采用 RSA 2048 位的加密方式，相较于传统的用户名和密码认证方式，SSH 密钥对登录认 证更为安全可靠，同时便于远程登录大量 Linux 实例。同时，阿里云容器服务也支持通过 SSH 密钥对的方式远程登录集群。

5.13.2 用户授权

提供了多种工具和功能，用来帮助用户在各种情况下授权资源的使用权力。 其中，阿里云为客户提供 Resource Access Management(RAM)资源访问控制服务，用于用户身份管理与资源访问控制。RAM 使得一个阿里云账号(主账号)可拥有多个独立的子用户(RAM 用户)，从而避免与其他用户共享云账号密钥，并可以根据最小权限原则为不同用户分配最小 的工作权限，从而降低用户的信息安全管理风险。RAM 授权策略可以细化到对某个 API-Action 和 Resource-ID 的细粒度授权，还可以支持多种限制条件(例如，源 IP 地址、安全访问通道 SSL/TLS、访问时间、多因素认证等)。

RAM 是阿里云账号安全管理和安全运维的基础。通过 RAM 可以为每个 RAM 用户分配不同 的密码或 API 访问密钥(Access Key)，消除云账号共享带来的安全风险;同时可为不同的 RAM 用户分配不同的工作权限，大大降低了因用户权限过大带来的风险。

5.13.3 密码管理

Umeet 网络会议遵循一人一账号原则，每个账号都有明确的持有者。所有用户集中下发密码策略，强制要求设置符合密码长度、复杂度要求的密码，并定期修改密码且不能与上一次密码相同。同时，支持账号密码登录、SSO 单点登录等多种认证登录方式，会议中我们基于实名制认证，只有手机短信认证的用户才能参与会议。

5.13.4 软件代码漏洞

安全加固-是指通过各种技术手段减少虚拟化管理程序中可能的被攻击面。Umeet 网络会议基于阿里云使用轻量级和专门为云上场景开发的虚拟化管理程序(以 KVM 为基础的 Hypervisor)，并在设计之初即做到软硬件场景结合，专注于只支撑垂直的云上基础设施的硬件虚拟化。同时，为减少可能受 到 0day 漏洞的影响，阿里云虚拟化管理程序会在不影响功能和性能的基础上限制系统级别的 动态函数库的调用。简而言之，阿里云会最大限度的从虚拟化管理程序中裁剪一些与云上设备 无关的代码来降低攻击面，此外，所有虚拟化软件必须编译和运行在一个可信的执行环境上才 能保障每个二进制文件在执行时不被恶意篡改和替换。阿里云采用了一系列可信计算技术来保 障整个链路的安全，也有一整套完善的控制机制来保障这些虚拟化二进制文件不被外部恶意获 取分析利用。

在此之外，阿里云还对虚拟化管理程序和宿主机 OS/内核级别进行相应安全加固。例如， 对虚拟化管理程序在动态运行时进行降权，并阻止内核执行用户空间代码以增加逃逸后提权的 难度;开启内存地址随机化特性，并开启内核符号限制访问功能和内存保护页功能以增加内存 溢出类攻击的难度。阿里云不断引入新的安全特性到虚拟化管理程序和宿主机 OS/内核中，这 其中包括内部研发的和外部开源社区的最新安全功能。

逃逸检测-虚拟化层面的入侵事件主要体现为在虚拟机上的逃逸攻击，其主要包括两个基本步骤:首 先将攻击方控制的虚拟机置于与其中一个攻击目标虚拟机相同的物理主机上;然后破坏隔离边 界，以窃取攻击目标的敏感信息或实施影响攻击目标功能的破坏行为。

在 Umeet 网络会议中，基础架构阿里云虚拟化管理程序通过使用高级虚拟机布局算法以防止恶意用户的虚拟机运行在特定物理机上，且虚拟机无法主动探测自身所处的物理主机环境。此外，阿里云 在 Hypervisor 层面会对虚拟机异常行为进行检测，例如对 Coredump 文件实时分析监控、对 Hypervisor 加载和执行可疑代码段进行实时检测、对虚拟机的系统函数调用和 VM Exit 异常行为 进行审计、以及对宿主机的进程执行行为和网络行为等可能的异常场景进行实时监控和分析， 及时发现对虚拟化平台的恶意攻击事件。

当检测到恶意攻击时，阿里云会定位和处置发起恶意攻击的虚拟机，并对整个攻击链条进 行及时的采样还原，并对找到的漏洞进行补丁热修复。

补丁热修复-阿里云虚拟化平台支持补丁热修复技术，通过补丁热修复技术使得系统缺陷或者漏洞的修 复过程不需要用户重启系统，从而不影响用户业务。

5.13.5 数据传输加密

Umeet 网络会议传输加密是指为客户端与云端服务器提供了 SSL/TLS 协议来保证数据传输的安全。

例如，实际是在网络层（传输层）通过 TLS 进行加密，因此数据只有在通过网络发送前才会进行加密，保证在传输期间即使被截获数据，也无法读取里面的有效信息。

简单来说，音、视频数据从客户端发送到后台服务器这个过程是加密的。数据到达后台服务器后，只会向后台提供音、视频的质量信息（比如延迟、丢包、接入地区等信息），以便于在出现故障时运维人员进行排查。而会议中的音、视频流（实际的声音及图像信息），系统设计时没有预留任何接口让运维人员去获取这些音、视频流，因此 Umeet 网络会议无法获取用户的会议信息。

另外基础架构中阿里云的网关产品也提供传输链路的加密功能。VPN 网关(VPN Gateway)服务，可通过 传输链路加密通道将企业本地 IDC 和阿里云 VPC 安全可靠的连接起来。VPN 网关可建立 IPsec- VPN，将本地 IDC 网络和云上 VPC 连接起来;也可建立 SSL-VPN，将本地客户端远程接入 VPC。 阿里云也提供智能接入网关(Smart Access Gateway，简称 SAG)服务，企业用户可通过智能 接入网关实现就近加密接入，并在传输过程中通过使用 IKE 和 IPsec 协议对传输数据进行加密， 保证数据安全。阿里云 VPN 网关和智能接入网关在中华人民共和国国家相关政策法规内提供服务，不提供访问 Internet 功能。

5.13.6 数据存储加密

Umeet 网络会议提供云产品落盘存储加密能力给用户，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。阿里云的存储加密提供 256 位密钥的存储加密强度(AES256)，满足敏感数据的加密存储需求。

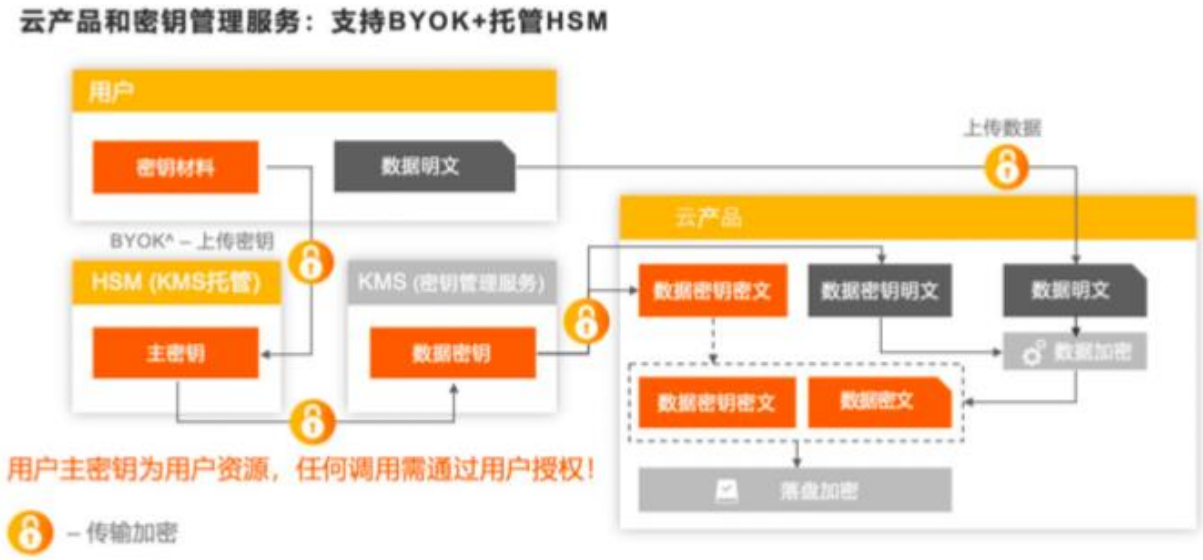
不同产品基于业务形态和客户需求，其存储加密的具体设计略有不同，但大体而言，存储加密中密钥层次会至少分为两层，并通过信封加密的机制实现对数据的加密。第一层为客户主密钥(Customer Master Key，简称 CMK)，第二层为数据密钥(Data Encryption Key，简称 DEK)，其中 CMK 为 DEK 进行加解密操作和保护，DEK 为真实数据进行加解密操作和保护。在数据落 盘存储时，云产品会将数据密钥密文(通过 KMS 使用 CMK 加密)在数据写入的时候，与密文数 据(云产品在存储链路上使用 DEK 加密)一同写入永久性存储介质中。顾明思义，信封加密中的“信封”指的是在概念上数据密钥的密文和数据密文被打包在一个“信封”(Envelope)中。 在读取加密数据时，数据密钥的密文也会一同被读取，并先于数据进行解密。只有在数据密钥 被解密后，密文数据才能够被正常读取。

在信封加密机制中，客户主密钥 CMK 受阿里云 KMS 提供的密钥管理基础设施的保护，实施强逻辑和物理安全控制以防止未经授权的访问。阿里云的密钥管理基础设施符合(NIST)800- 57 中的建议，并使用了符合合规要求的密码算法和硬件加密机(HardwareSecurityModule，简 称 HSM)。在整个信封加密过程中，CMK 的明文从不会在 KMS 托管的 HSM 之外进行存储和使用。KMS 也支持软件密钥托管，通过软件密码模块(Software Cryptographic Module)对密钥 进行保护。KMS 通过加固软件密码模块，保护软件密钥的明文材料不会离开软件密码模块的边界，仅能在模块边界内被加载于内存中。同时，数据密钥 DEK 明文仅会在用户使用的服务实例所在的宿主机的内存中使用，永远不会以明文形式存储在任何永久介质上。

云产品的存储加密功能支持使用托管给云产品的服务密钥作为主密钥实现。具体而言，当 用户在一个地域第一次使用某一个云产品服务的数据加密功能时，该服务系统会为用户在密钥 管理服务(KMS)中的使用地域自动创建一个专为该服务使用的用户主密钥(CMK)。本密钥会 作为服务

密钥且其生命周期是托管给云服务的。具体表现为用户可以在密钥管理服务控制台上 查询到该用户主密钥，但不能删除。

在存储加密功能中，阿里云也有多个产品支持用户自选密钥功能，包括支持用户自上传的 CMK(Bring Your Own Key，简称 BYOK，也称 Customer Supplied Key)或用户自己在 KMS 中生成的用户主密钥(CMK)作为主密钥对数据进行加密，并允许客户对 CMK 的生命周期进行全 程管理。需要强调的是，用户自选的 CMK 是用户的资产，云产品必须得到用户的授权(通过 RAM)才可以使用其对数据进行加解密操作。用户也可以随时取消相对应的 CMK 授权，达到对数据加解密操作的可控。



请注意，为了表达的简单扼要，在本白皮书中，如无特别说明，后续会使用“用户自选密钥”来泛指使用用户自上传到 KMS(BYOK)或用户在 KMS 自生成的 CMK 作为主密钥进行存储加密的功能。

阿里云已拥有不同的云产品支持数据存储加密功能:

- ● 块存储 EBS:支持虚拟机内部使用的块存储设备(即云盘)的数据落盘加密，确保块存 储的数据在分布式系统中加密存放，并支持使用服务密钥和用户自选密钥作为主密钥 进行数据加密。

- RDS 数据库的数据加密:RDS 数据库的多个版本通过透明加密(Transparent Data Encryption，简称 TDE)或云盘实例加密机制，支持使用服务密钥和用户自选密钥作为 主密钥进行数据加密。

- 表格存储 OTS:支持使用服务密钥和用户自选密钥作为主密钥进行数据加密。

- 文件存储 NAS:支持使用服务密钥作为主密钥进行数据加密。

5.13.7 数据备份

Umeet 网络会议提供一个扁平的线性存储空间，并在内部对线性地址进行切片，一个分片称为一个 Chunk。 对于每一个 Chunk，都会复制出三个副本，并将这些副本按照一定的策略存放在集群 中的不同节点上，保证用户数据的可靠。

5.13.8 数据删除保护

数据删除

在用户进行删除操作后，释放的存储空间由飞天分布式文件系统回收，禁止任何用户访问，同时进行内容擦除，最大限度保证用户的数据安全性。

数据保护

✧ 数据分类

云上环境中，时时刻刻都会有海量数据的产生。而在对这些数据进行处理和保护之前，如何从海量数据中发现并分类出各种需要被保护的敏感数据是后续数据保护机制能够有效运作的前 提条件。数据分类的第一步是对数据中的敏感信息，如个人验证信息(Personal Identifiable Information，简称 PII)，进行发现和检测。数据分类的第二步是针对数据中的敏感信息，根据 用户的使用场景、合规需求和安全要求，对数据进行分类分级，从而达到自知数据资产，并后续进行针对性保护的作用。

阿里云的敏感数据保护(Sensitive Data Discovery and Protection，简称 SDDP)产品，可以对用户云上数据进行发现和分类分级功能。SDDP 可在得到云上用户授权后，自动扫描和发现 授权范围内的新增实例/库/表/列、对象存储文件桶/文件对象等不同级别数据信息。通过关键 字、规则、机器学习模型算法，精准识别云环境内的敏感数据，并支持根据用户自身业务规则进 行敏感数据自定义。SDDP 根据敏感数据识别结果，可实现云上数据基于业务内容的分类以及基 于敏感程度的分级，以供后续根据敏感分类分级结果在云上系统中对用户数据实现相关的保护 机制。

✧ 数据脱敏

在发现和分类敏感数据后，为保护数据隐私，用户往往需要根据不同的业务场景对相关敏感数据进行脱敏后的使用。例如，用户往往希望能够在不改变数据结构和特征分布的情况下， 对生产数据进行脱敏，并用于测试、开发、分析和三方数据交换等场景中。

阿里云的敏感数据保护产品，提供 Hash、加密、遮盖、替换、洗牌、变换等六大类近 30 种 内置脱敏算法并同时支持客户自定义脱敏算法或者自定义脱敏参数，确保脱敏后的数据无需改变相应的业务系统逻辑，保留原有数据特征和分布，确保数据的有效性和可用性。用户可以低成本、高效率、安全地使用脱敏数据完成业务需求。

✧ 数据防泄露

用户数据的防泄露，主要体现在对数据的权限控制的完整度和数据使用中的监控和检测能力。如果想要防止数据泄露，首先需要实现对云上存储产品和传输产品权限的有效管控。Umeet 网络会议的敏感数据保护产品支持“数据、人、权限”三要素的即时查询，支持角色背后主账号权限映射解析，和全局数据权限统一查询。

其次，需要对用户数据的流转和操作过程有全面的监控和检测能力，及时发现数据使用中可能的异常行为。针对数据流转过程中的异常情况进行有效监控，实现数据流转链路动态展示，确保数据导出/数据传输合规有序。根据日志聚类分析，服务能有效识别人工操作与应用接口调用。基于机器学习和大数据分析能力，针对环境内各类数据流转、数据操作中产生的异常行为进行监控告警。

最后，在发现数据泄露告警后，支持对异常事件进行分析以供后续的处理响应。 其中，事件分析支持集中归集各类告警事件，并通过使用时序分析技术还原责任主体行为基线， 动态展示历史基线轨迹，从而有效的提升分析效率。同时，支持各租户事件隔离处理， 并支持处理结果自动回流机器学习样板库，从而使得异常检测能力日趋准确。

✧ 数据完整性

在数据传输和存储层面，Umeet 网络会议提供了全链路数据校验功能，且会定期对存储介质中的数据进行完整性扫描，以确保数据传输和存储过程中的数据可靠性需求。同时，在数据存储时也会有对应的校验码贯穿 始终，达到对数据进行细粒度的完整性校验保护。数据的完整性也通过访问授权功能得到保障。

✧ 数据高可用

Umeet 网络会议使用分布式存储，文件被分割成许多数据片段分散存储在不同的设备上，并且每个数据片段存储多个副本。分布式存储不但提高了数据的可靠性，也提高了数据的安全性。同时， 基于阿里云的云产品，为 Umeet 网络会议提供多副本、系统备份、故障热迁移、负载均衡、DDoS 防御等多重保护，保证用户在使用数据时的高可用性。