阿里云
通用解决方案

安全解决方案

文档版本：20190329

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 静态数据加密

阿里云提供了多种静态数据的加密方式，如下表所示。

产品	加密方式	
OSS	OSS 客户端加密	OSS 服务器端加密
RDS	SSL 加密	TDE 加密
ECS 云盘	您可以使用ECS云盘加密功能加密云盘上的数据。	

OSS 数据加密

OSS 支持客户端加密和服务器端加密。

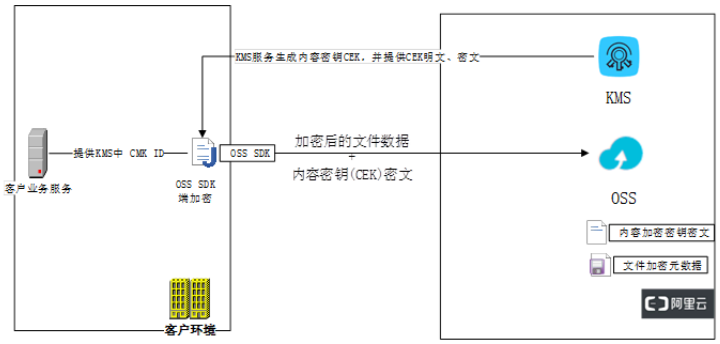
OSS 客户端加密

客户端加密是指将数据发送到OSS之前在用户本地进行加密，对于数据加密密钥的使用，目前支持如下两种方式：

- 使用KMS托管用户主密钥
- 使用用户自主管理密钥

使用KMS托管用户主密钥

当使用KMS托管用户主密钥用于客户端数据加密时，无需向OSS加密客户端提供任何加密密钥。只需要在上传对象时指定KMS用户主密钥ID（也就是CMK ID）。其具体工作原理如下：



1. 上传对象。

   通过使用CMK ID，客户端首先向KMS发送一个请求，申请1个用于加密对象的数据密钥（Data Key）。作为响应，KMS会返回一个随机生成的数据明文密钥（Data Key）以及一个数据密文密钥（Encrypted Data Key）。

2. 本地加密数据。

   本地客户端接收到KMS返回的数据明文密钥以及数据密文密钥后，将使用数据明文密钥进行本地加密，并且将加密后的对象以及数据密文密钥上传至OSS；

3. 下载对象。

   客户端首先会从OSS服务端下载加密的对象以及作为对象元数据存储的数据密文密钥。

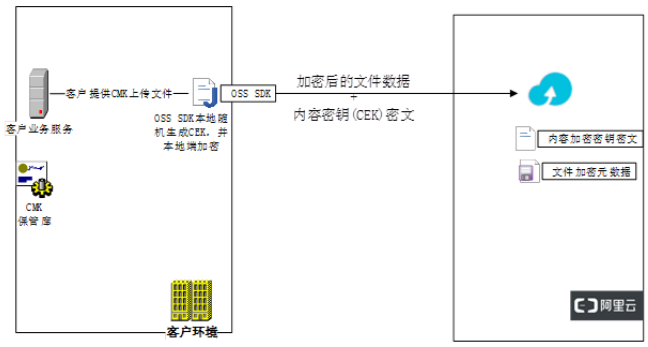
4. 解密数据。

   客户端将数据密文密钥以及CMK ID发送至KMS服务器。作为响应，KMS将使用指定的CMK解密，并且将数据明文密钥返回给本地加密客户端。

> 说明:
>
> · 本地加密客户端为每一个上传的对象获取一个唯一的数据加密密钥。
> · 为了保证数据的安全性，建议CMK定期轮换或者更新。
> · 客户需要维护CMK ID与对象之间的映射关系。

使用用户自主管理密钥

使用用户自主管理密钥，需要用户自主生成并保管加密密钥。当用户本地客户端加密时，由用户自主上传加密密钥（对称加密密钥或者非对称加密密钥）至本地加密客户端。其具体加密过程如下：



1. 上传对象。

   用户首先向本地加密客户端提供1个用户主密钥（对称密钥或者非对称密钥）。客户端只使用此主密钥加密其随机生成的数据密钥。该过程如下：

   a. OSS本地加密客户端在本地生成一个一次性的对称密钥，即数据密钥（Data Key）。它将用于加密单个对象（针对每个对象，客户端都会随生成1个数据密钥）。
   b. 客户端使用数据密钥加密对象。
   c. 客户端使用用户提供的主密钥来加密数据密钥。
   d. 客户端将加密的数据密钥（Encrypted Data Key）作为对象元数据的一部分上传至OSS。

2. 下载对象。

下载对象时，客户端首先从OSS下载加密的对象以及元数据。通过使用元数据中的材料，客户端将授权确定使用哪个主密钥来解密加密的数据密钥。客户端使用解密后的数据密钥来解密对象。

说明:

- OSS本地加密客户端不会将用户主密钥以及未加密的数据发送至OSS。所以，请务必妥善保管加密密钥，如果密钥丢失，将无法解密数据。
- 数据密钥由本地加密客户端随机生成。

OSS 服务器端加密

OSS支持在服务器端对上传的数据进行加密编码（Server-Side Encryption）：上传数据时，OSS对收到的用户数据进行加密编码，然后再将得到的加密数据持久化保存下来；下载数据时，OSS自动对保存的加密数据进行解密并把原始数据返回给用户，并在返回的HTTP请求Header中，声明该数据进行了服务器端加密。

OSS服务端加密主要应用场景

OSS通过服务端加密机制，提供静态数据保护。适合于对于文件存储有高安全性或者合规性要求的应用场景。例如，深度学习样本文件的存储、在线协作类文档数据的存储。针对不同的应用场景，OSS有如下两种服务端加密方式：

- 使用KMS托管密钥进行加解密（SSE-KMS）

  上传文件时，可以使用指定的CMK ID或者默认KMS托管的CMK进行加解密操作。这种场景适合于大量的数据加解密。数据无需通过网络发送到KMS服务端进行加解密，这是一种低成本的加解密方式。

  注意:
  使用KMS密钥功能时会产生少量的KMS密钥API调用费用，费用详情请参考KMS计费标准。

- 使用OSS完全托管加密（SSE-OSS）

  基于OSS完全托管的加密方式，是Object的一种属性。您可以在上传object或修改object的meta信息时，在请求中携带`X-OSS-server-side-encrpytion`并指定其值为AES256，阿里云oss服务端加密使用AES256加密每个对象。OSS会为每个对象使用不同的密钥进行加密，作为额外的保护，它将使用定期轮转的主密钥对加密密钥本身进行加密。该方式适合于批量数据的加解密。

服务端加密选项

服务端加密-OSS完全托管

OSS的服务器端加密是Object的一个属性。用户创建一个Object的时候，只需要在Put Object的请求中携带`x-oss-server-side-encryption`的HTTP Header，并指定其值为`AES256`，即可以实现该Object的服务器端加密存储。

服务端加密-KMS托管主密钥

RDS 数据加密

RDS 支持 SSL 和 TDE 加密。

SSL 加密

RDS提供MySQL和SQL Server的安全套接层协议（Secure Sockets Layer，简称SSL）。您可以使用RDS提供的服务器端的根证书来验证目标地址和端口的数据库服务是不是RDS提供的，从而可有效避免中间人攻击。除此之外，RDS还提供了服务器端SSL证书的启用和更新能力，以便用户按需更替SSL证书以保障安全性和有效性。

需要注意的是，虽然RDS提供了应用到数据库之间的连接加密功能，但是SSL需要应用开启服务器端验证才能正常运转。另外SSL也会带来额外的CPU开销，RDS实例的吞吐量和响应时间都会受到一定程度的影响，具体影响与您的连接次数和数据传输频度有关。

具体操作请参见*设置SSL加密*。

TDE 加密

RDS提供MySQL和SQL Server的透明数据加密（Transparent Data Encryption，简称TDE）功能。MySQL版的TDE由阿里云自研，SQL Server版的TDE是基于SQL Server企业版的功能改造而来。

当RDS实例开启TDE功能后，您可以指定参与加密的数据库或者表。这些数据库或者表中的数据在写入到任何设备（磁盘、SSD、PCIe卡）或者服务（表格存储OSS、归档存储OAS）前都会进行加密，因此实例对应的数据文件和备份都是以密文形式存在的。

TDE加密采用国际流行的AES算法，秘钥长度为128比特。秘钥由KMS服务加密保存，RDS只在启动实例和迁移实例时动态读取一次秘钥。您可以自行通过KMS控制台对秘钥进行更替。

具体操作请参见设置透明数据加密设置透明数据加密。

ECS 云盘加密

更多云盘加密的信息，请参见*ECS云盘加密*。

2 等保合规安全解决方案

2.1 背景信息

近期网络安全事故频发，法规制度对网络安全机制的建立、完善提出了更高、更明确的要求。企业在拓展网络应用的同时，应当将网络安全作为业务发展的重点考虑内容之一。

法规制度背景

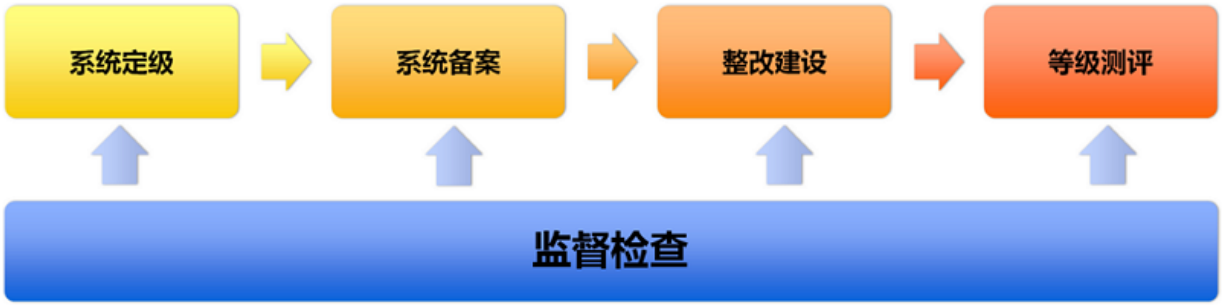
2016年11月7日上午，十二届全国人大常委会第二十四次会议表决，正式通过了《中华人民共和国网络安全法》，网络安全法将于2017年6月1日起施行。

根据网安法，企业需履行一定的义务并承担网络安全相关责任，网安法的重点解读请参考 《网络安全等级保护基本要求》 重点解读 章节。

其中，网安法第二十一条为：国家实行网络安全等级保护制度（下文简称：等保安全制度），等保安全制度适用于境内所有信息系统。企业需按照网络安全等级保护制度履行安全保护义务，按照等保安全制度申报完成网络安全等级评定，根据各级保护制度的要求整改、建设信息系统，是企业应履行的义务，同时可发现自身系统的安全隐患及不足，以及时整改，进而可提高企业整体的行业竞争力。更详细的等保安全制度介绍请参考 等保安全制度简介 章节。

等级保护制度实施流程

根据系统保护等级和各地政策的不同，申请等级保护认证的实施流程顺序略有区别，但基本都包括：系统定级、整改建设、等级测评、系统备案和监督检查等五项工作。以申请等保三级认证为例，标准实施流程如下：



流程解读：

- 系统定级：信息系统运营使用单位（企业）要按照《信息安全等级保护管理办法》和《网络安全等级保护定级指南》，初步确定定级对象的安全保护等级，起草《网络安全等级保护定级报告》，三级以上系统，定级结论需要进行专家评审。

- 系统备案：信息系统安全保护等级为第二级以上时，备案时应当提交《网络安全等级保护备案表》和定级报告；第三级以上系统，还需提交专家评审意见、系统拓扑和说明、安全管理制度、安全建设方案等。
- 建设整改：依据《网络安全等级保护基本要求》，利用自有或第三方的安全产品和专家服务，对信息系统进行安全建设和整改，同时制定相应的安全管理制度。
- 等级测评：信息系统建设整改完成后，运营使用单位应当选择合适的测评机构，依据《网络安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。
- 监督检查：公安机关及其他监管部门会在整个过程中，履行相应的监管、审核和检查等职责。

阿里云平台已完成等保三级认证，阿里金融云已完成等保四级认证。阿里云平台等保现状可参考 附录 3 阿里云等保安全现状 章节。

结合阿里云平台自身及客户等保认证经验，阿里云为企业提供一站式等保安全解决方案，助力企业完成等保安全评定，提供更专业、更高效、更便捷的等保安全解决方案。

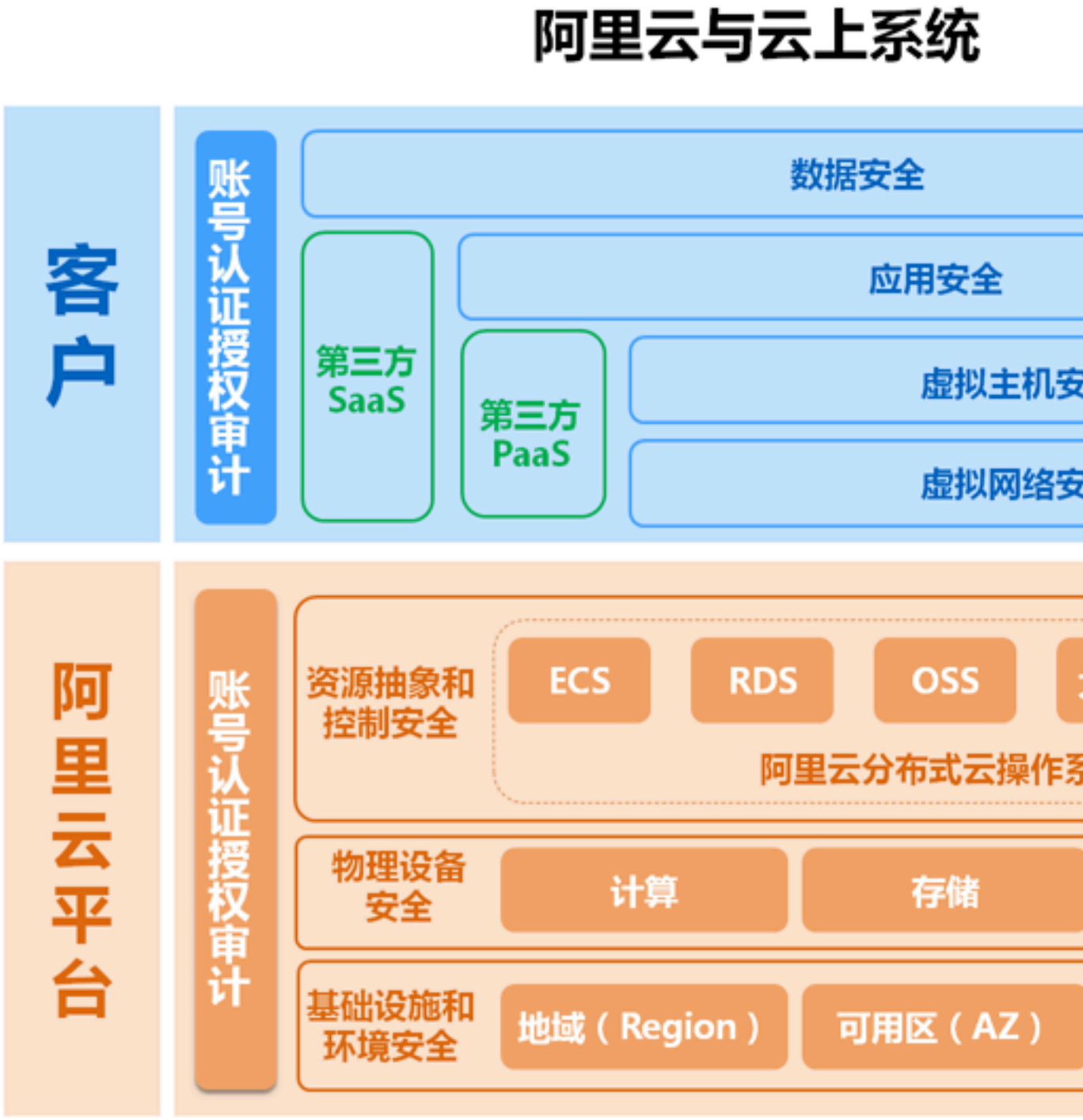
2.2 阿里云等保安全解决方案

阿里云提供一站式等保安全解决方案，助力企业更高效、专业地完成等保认证。

云上系统责任共担

企业申请云上系统的等保认证时，使用的云平台及企业部署在云上的系统应用均需满足等保认证的要求，云上系统的合规性由阿里云与企业共同承担。

图 2-1: 云上系统责任共担



等保合规生态

为了助力企业云上系统能够快速满足等保合规的要求，阿里云通过建立等保合规生态，联合阿里云合作伙伴咨询机构、各地测评机构和公安机关，向运营单位（阿里云客户）提供一站式、全流程等保合规解决方案。

根据等保实施流程，阿里云等保安全解决方案的实施过程中，各角色及责任分工如下。

机构	系统定级	系统备案	建设整改	等级测评	监督检查
运营单位	确定安全保护等级，编写定级报告	准备备案材料，到当地公安机关备案	建设符合等级要求的安全技术和管理体系	准备和接受测评机构测评	接受公安机关的定期检查
阿里云	协调第三方机构为运营单位提供辅导服务	协调第三方机构为运营单位提供辅导服务	提供符合等级要求必须的安全产品和服务	提供云服务商安全资质、云平台通过等保的证明材料	-
咨询机构	辅导运营单位准备定级报告，并组织专家评审（三级）	辅导运营单位准备备案材料和备案	辅导运营单位进行系统安全加固和制定安全管理制度	协助运营单位参与等级测评过程并进行整改	协助运营单位接受检查和进行整改
测评机构	-	-	-	测评机构对系统等级符合性状况进行测评	-
公安机关	-	当地公安机关审核受理备案材料	-	-	公安机关监督检查运营单位开展等级保护工作

说明:

测评机构可以提供咨询服务。

责任分工说明：

- 阿里云：整合服务机构能力，并提供安全整改方案
- 咨询机构：提供全流程技术支撑和咨询服务
- 测评机构：可提供等保咨询和测评服务
- 公安机关：负责备案审核和监督检查

建设整改方案输出

建设整改阶段，需要运营单位根据相应的安全保护等级要求，对信息系统进行建设和整改，建立完善的安全管理和安全技术体系。

安全管理体系	安全技术体系
安全策略和管理制度	物理和环境安全
安全管理机构和人员	网络和通信安全
安全建设管理	设备和计算安全
安全运维管理	应用与数据安全

阿里云等保安全解决方案除整合周边角色资源外，在建设整改阶段可根据企业自身业务特点，结合阿里云自身安全等保认证经验，输出安全等保技术体系，根据企业认证要求，给出基础合规方案及增强合规方案建议。

详细的建设整改阶段的安全技术体系方案请参考 安全合规架构 章节。

2.3 安全合规架构

安全技术体系

安全技术体系建立的主要手段包括使用安全产品、加固系统配置和开发安全控制，通过使用成熟的安全产品，可以快速满足合规要求。

为满足各个层面的等保安全测评项要求，您可以组合使用阿里云安全产品：

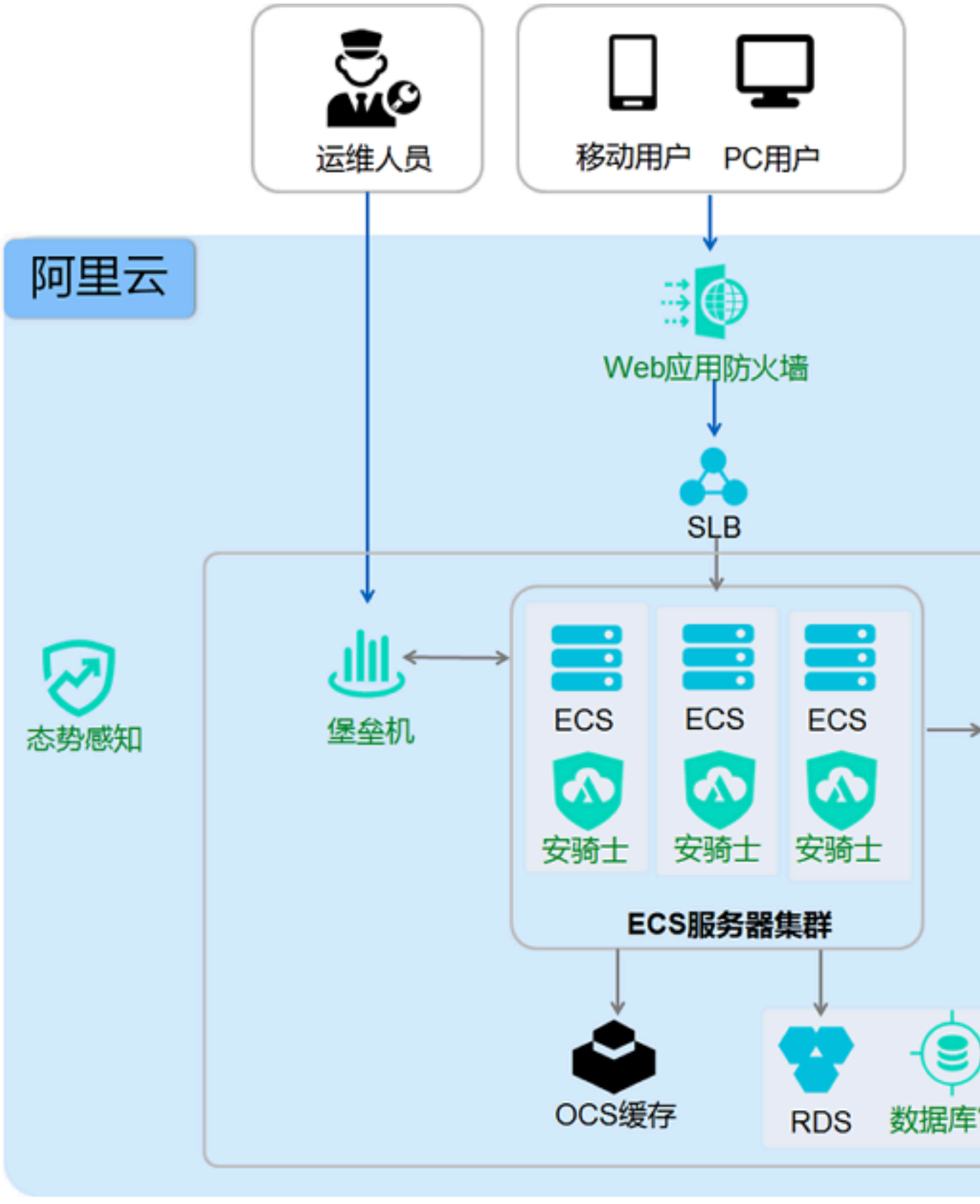
安全层面	类别	阿里云产品
物理和环境安全	-	直接复用阿里云等保测评结论即可
网络和通信安全	网络架构	· VPC · 云盾.云防火墙/安全组
	通信传输	云盾.证书服务/VPN
	边界防护	· VPC+NAT网关 · 云盾.云防火墙/安全组
	访问控制	云盾.云防火墙/安全组
	入侵防范	· 云盾.态势感知 · 云盾.DDoS高防IP · 云盾.Web应用防火墙

安全层面	类别	阿里云产品
	恶意代码防范	云盾.Web应用防火墙
	安全审计	云盾.态势感知
	集中管控	· 云监控 · 云盾.态势感知
设备和计算安全	身份鉴别	云盾.堡垒机
	访问控制	云盾.堡垒机
	安全审计	· 云盾.堡垒机 · 云盾.数据库审计/RDS.SQL审计
	入侵防范	· 云盾.先知 · 云盾.安骑士
	恶意代码防范	云盾.安骑士
	资源控制	云监控
应用与数据安全	身份鉴别	主要功能需要应用系统开发商解决Actiontrail审计阿里云控制台操作 云盾.安全众测
	访问控制	
	安全审计	
	软件容错	
	资源控制	
	数据完整性	· 云盾加密服务/系统开发商实现 · 云盾.证书服务 · 云盾.Web应用防火墙（防篡改）
	数据保密性	· 云盾.加密服务/RDS.透明加密 · 系统开发商实现
	数据备份恢复	RDS异地容灾实例或其他异地备份措施
	剩余信息保护	主要功能需要应用系统开发商解决
	个人信息保护	

更多阿里云安全产品及可满足的等保要求请参考 阿里云安全产品 章节。

基础合规架构

为满足等级保护的基本测评要求，建议您参考基础合规架构建设整改您的基础IT系统，提高整体安全性。基础合规架构可基本满足等保三级测评要求，提升整体安全防护水平。

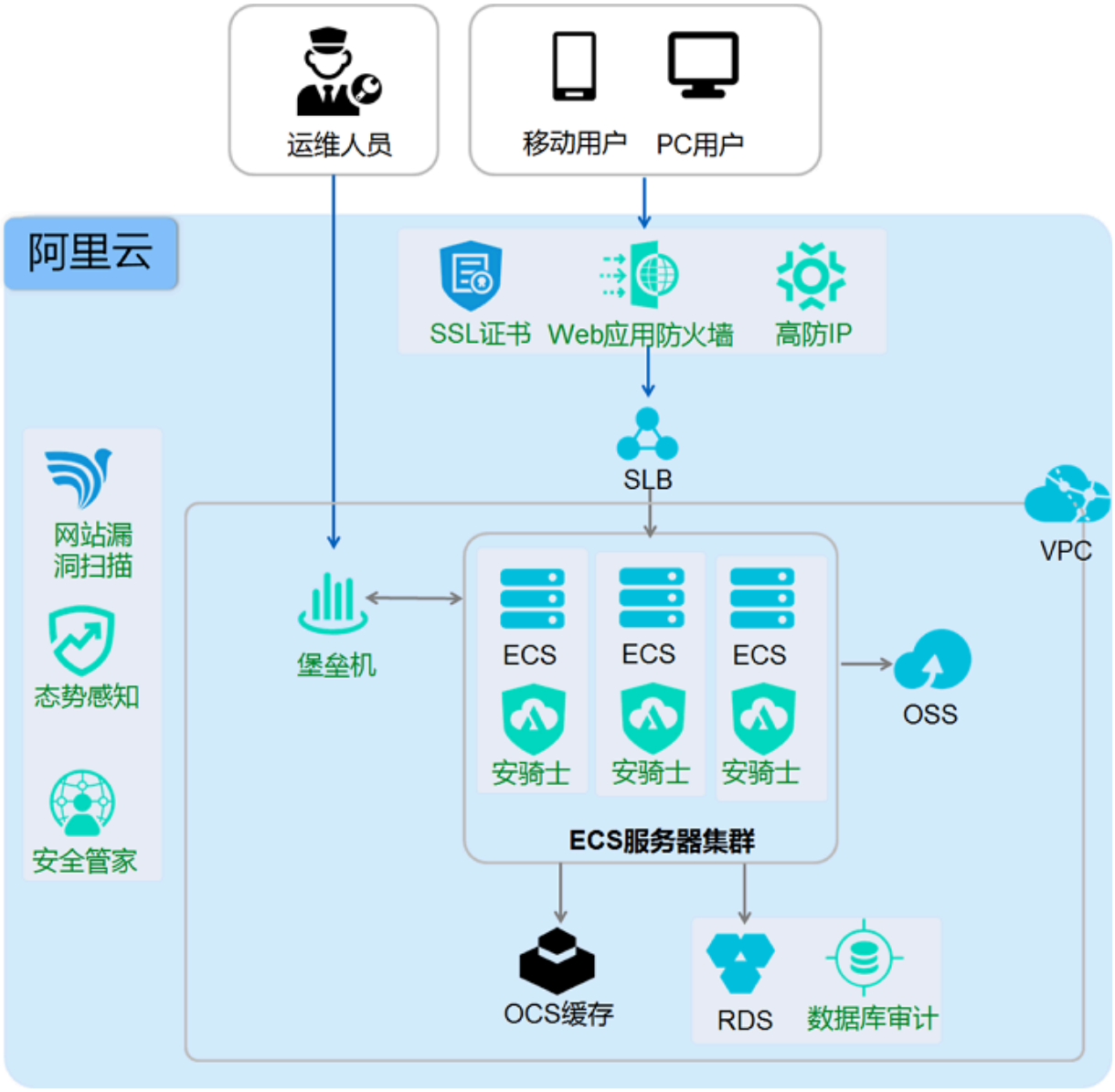


架构说明：

安全领域	服务名称	安全设计
网络安全	云防火墙	使用云防火墙实现业务分区分组，管理员可以清晰的甄别合法访问和非法访问，从而执行安全隔离和访问控制策略。
	VPC	使用阿里云VPC，隔离本系统网络与外部网络环境，并可自主规划网络内的业务网段，实现VLAN级别的网络隔离。
服务器安全	安骑士	通过安骑士实现对服务器的入侵防范和恶意代码防范。
应用安全	Web应用防火墙	部署Web应用防火墙防护恶意应用攻击，保障移动、PC等互联网用户的接入安全。
数据安全	SSL证书	使用SSL证书服务，为HTTP网站提供转向HTTPS，加密应用层数据。
安全审计	堡垒机	使用堡垒机管理运维ECS，实现云上服务器的操作运维审计和账号权限管理。
	数据库审计	使用数据库审计服务，实现对RDS数据库、ECS自建数据库的审计功能。
安全管理	态势感知	使用态势感知服务实现流量监控、整体安全监控，实现安全审计与集中管控。

增强合规架构

满足等级保护的基本测评要求之余，如果您对系统安全有更高要求，或希望更安全的系统来保障业务的稳定运行，建议您参考增强合规架构建设整改您的基础系统。增强合规架构在基本满足等保三级的要求之余，搭建更安全的系统，保障业务稳定运行，获得更好的测评结果。



架构说明：

安全领域	服务名称	安全设计
网络安全	DDoS高防IP	使用DDoS高防服务提供网络链路可用性保证，提升DDoS防护阈值，提升业务连续性。
	云防火墙	使用云防火墙实现业务分区分组，管理员可以清晰的甄别合法访问和非法访问，从而执行安全隔离和访问控制策略。
服务器安全	安骑士	通过安骑士实现对服务器的入侵防范和恶意代码防范。
应用安全	Web应用防火墙	部署Web应用防火墙防护恶意应用攻击，保障移动、PC等互联网用户的接入安全。

安全领域	服务名称	安全设计
	网站漏洞扫描	满足等保要求中关于及时发现漏洞和进行漏洞升级要求。
数据安全	SSL证书	使用SSL证书服务，为HTTP网站提供转向HTTPS，加密应用层数据。
安全审计	堡垒机	使用堡垒机管理运维ECS，实现云上服务器的操作运维审计和账号权限管理。
	数据库审计	使用数据库审计服务，实现对RDS数据库、ECS自建数据库的审计功能。
安全管理	态势感知	使用态势感知服务实现流量监控、整体安全监控，实现安全审计与集中管控。
安全专家服务	安全管家	阿里云安全管家服务是阿里云安全专家基于阿里云多年安全最佳实践经验为云上用户提供的全方位安全技术和咨询服务，为云上用户建立和持续优化云安全防御体系，保障用户业务安全。

2.4 解决方案优势

阿里云为企业提供一站式、专业、产品合规的等保安全解决方案，助力企业完成快速、高效、合规、安全的等保安全认证。

一站式

阿里云联合各地多家咨询和测评机构，为企业提供一站式合规解决方案。企业无需多点沟通，可借助阿里云平台一站式完成等保安全认证，省时省力省心。

专业

阿里公共云平台已通过等保三级认证，阿里金融云已通过等保四级认证，并助力很多客户成功完成等保认证。因此阿里云有丰富的实践经验，可以更专业的为企业提供等保安全解决方案。

产品合规

阿里云提供公安部认可的安全产品和服务，通过阿里云云盾和安全生态产品，可助力企业构建全面满足合规要求的信息系统，利用丰富、合规的阿里云产品建设、完善企业的信息系统。

客户价值

- 快速：通过阿里云等保安全解决方案，可平均缩短企业50%的整改及测评时间。
- 高效：阿里云提供一站式申请等保安全认证服务，避免企业多点沟通，减少企业沟通成本。
- 合规：针对行业监管，可以满足等保90分要求
- 安全：阿里云提供整改建设阶段的技术架构建议，并注重防护效果，在云端可加持大数据能力，保障架构的安全性。

2.5 客户案例

阿里云等保合规安全解决方案已成功助力多位客户完成等保合规认证。

智融集团

智融集团专注于以人工智能为核心的新金融技术，旗下包含为非传统金融机构目标人群提供小额周转的金融服务APP“用钱宝”，基于机器学习及大数据计算的人工智能风控引擎“I.C.E.”，以及信贷过程管理体系“慧诚帮帮PaaS”三大业务版块。

闪银奇异

北京闪银奇异是中国第一家互联网信用评估公司，其开发的Wecash闪银奇异是目前国内最先进的大数据信用评估平台。Wecash闪银是中国首家互联网信用评估平台，依托数据挖掘分析和机器学习技术，实现快速精准的信用评估。

斑马智行

斑马智行是上汽集团和阿里巴巴集团共同打造的互联网汽车解决方案。 现在已登陆全球首款量产互联网汽车荣威RX5。主要功能有旅途记录、远程车辆控制、车辆报警、道路救援。

全球影像

全球影像网以医疗影像的采集、传输、云存储为基础，满足医院远程会诊、双向转诊，医生移动阅片、远程影像诊断/示教、远程视频问诊等一系列医疗综合应用需求，为当下“看病难、看病贵”等社会问题提供解决之道。

2.6 附录 1 网络安全法简介

《网络安全等级保护基本要求》重点解读

根据网安法，企业需关注：

- 义务：按照网络安全等级保护制度履行安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露、篡改。
- 责任：网络运营者应对保障用户信息安全负有主体责任。
- 措施：
  - 制定网络安全事件应急预案，及时处理系统漏洞、计算机病毒、网络攻击、网络入侵等安全风险、并按照规定向有关部门报告。
  - 加强对用户发布信息的管理，及时消除法律、行政法规禁发的信息，建立网络信息投诉、举报制度、并及时受理。
  - 对收集的用户严格保密，并建立健全用户信息保护制度，不得非法收集、提供、获取、 使用用户信息。
- 维护：做好公共通信和信息服务、能源、水利、金融、公共服务、电子政务等重要行业的数据备份、防篡改、防泄漏、容灾措施，尤其是国家关键信息基础设施系统。

2.7 附录 2 等级保护简介

等级保护是什么

- 制度要求
  - 《中华人民共和国网络安全法》：“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。
  - 《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）：“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。
  - 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）规定：“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度”。
- 工作依据
  - 《警察法》规定：警察履行“监督管理计算机信息系统的安全保护工作”的职责。
  - 国务院令第147号规定：“公安部主管全国计算机信息系统安全保护工作”，“等级保护的具体办法，由公安部会同有关部门制定”。
  - 2008年国务院三定方案，公安部新增职能：“监督、检查、指导信息安全等级保护工作”。
- 监管范围与力度
  - 信息安全等级保护的适用范围：中华人民共和国境内的计算机信息系统。
  - 监管力度：二级及以上系统均纳入公安机关监管范围，其中三级系统至少每年测评一次。
  - 三级系统对安全产品主要要求：境内独立法人、自主知识产权、信息安全产品认证证书。
- 地位和作用
  - 国家信息安全保障工作的基本制度、基本国策。
  - 开展信息安全工作的基本方法。
  - 促进信息化、维护国家信息安全的根本保障。

等级保护分级说明

等级	等级定义	适用系统
第一级	信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益	不重要系统

等级	等级定义	适用系统
第二级	信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全	一般重要系统
第三级	信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害	比较重要系统
第四级	信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害	非常重要系统
第五级	信息系统受到破坏后，会对国家安全造成特别严重损害	极度重要系统

《网络安全等级保护基本要求》重点解读

网络与通信安全

表 2-1: 安全要求

类别	安全要求
网络架构	应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
访问控制	· 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。 · 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。
通信传输	应采用校验码技术或加解密技术保证通信过程中数据的完整性。
边界防护	应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信。
入侵防范	· 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。 · 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

表 2-2: 条款解读与应对政策

条款解读	应对政策
· 根据服务器角色和重要性，对网络进行安全域划分。 · 在内外网的安全域边界设置访问控制策略，并要求配置到具体的端口。 · 在网络边界处应当部署入侵防范手段，防御并记录入侵行为。 · 对网络中的用户行为日志和安全事件信息进行记录和审计。	· 推荐使用阿里云的VPC和安全组对网络进行安全域划分并进行合理的访问控制。 · Web应用防火墙防范网络入侵。 · 态势感知的日志功能对用户行为日志和安全事件进行记录分析和审计。 · 对于经常面临DDoS威胁系统，还可使用DDoS高防进行异常流量过滤和清洗。

设备与计算安全

表 2-3: 安全要求

类别	安全要求
身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性。
访问控制	应根据管理用户的角色建立不同账户并分配权限，仅授予管理用户所需的最小权限，实现管理用户的权限分离。
安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
入侵防范	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
恶意代码防范	应采用免受恶意代码攻击的技术措施或采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性检测，并在检测到破坏后进行恢复。

表 2-4: 条款解读与应对政策

条款解读	应对政策
· 避免账号共享、记录和审计运维操作行为是最基本的安全要求。 · 必要的安全手段保证系统层安全，防范服务器入侵行为。	· 推荐使用阿里云的堡垒机、数据库审计对服务器和数据的操作行为进行审计，同时为每个运维人员建立独立的堡垒机账号，避免账号共享。 · 使用安骑士对服务器进行完整的漏洞管理、基线检查和入侵防御。

应用和数据安全

表 2-5: 安全要求

类别	安全要求
身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求。
访问控制	应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
安全审计	应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
数据完整性	应采用校验码技术或加解密技术保证重要数据在传输过程中的完整性和保密性。
数据备份恢复	应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

表 2-6: 条款解读与应对政策

条款解读	应对政策
· 应用是具体业务的直接实现，不具有网络和系统相对标准化的特点。大部分应用本身的身份鉴别、访问控制和操作审计等功能，都难以用第三方产品来替代实现。 · 数据的完整性和保密性，除了在其他层面进行安全防护以外，加密是最为有效的方法。 · 数据的异地备份是等保三级区别于二级最重要的要求之一，是实现业务连续最基础的技术保障措施。	· 在应用开发之初，就应当考虑应用本身的身份鉴别、访问控制和安全审计等功能。 · 对已经上线的系统，通过增加账号认证、用户权限区分和日志审计等功能设计满足等保要求。 · 数据的安全，推荐使用成熟的云盾CA证书服务实现HTTPS，确保数据在传输的过程中保持处于加密状态。 · 数据备份，推荐使用RDS的异地容灾实例自动实现数据备份，亦可以将数据库备份文件手工同步到阿里云其他地区的服务器。

安全管理策略

表 2-7: 安全要求

类别	安全要求
安全策略和管理制度	应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的信息安全管理制度体系。
安全管理机构和人员	应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权。

类别	安全要求
安全建设管理	应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，并形成配套文件。
安全运维管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

表 2-8: 条款解读与应对政策

条款解读	应对政策
· 安全策略、制度和管理层人员，是保证持续安全非常重要的基础。策略指导安全方向，制度明确安全流程，人员落实安全责任。 · 等保要求提供了一种方法论和最佳实践，安全可以按照等保的方法论进行持续的建设和管理。	· 安全策略、制度和管理层人员，需要客户管理层根据本企业的实际情况，进行梳理、准备和落实，并形成专门的文件。 · 漏洞管理过程中需要用到的技术手段，推荐使用阿里云的安全管家和先知众测服务，快速发现云上系统漏洞，及时处理。

2.8 附录 3 阿里云等保现状及安全资质

阿里云公共平台已完成等保三级认证，阿里金融云已完成等保四级安全认证。

阿里云等保现状

2016年9月，阿里云通过新的云计算安全等级保护三级要求的测评，是国内首个通过国家权威机构依据云等保要求联合测评的公共云服务平台。

按照新的云等保要求和监管部门的意见，在具体的云上应用等级保护合规和测评中，涉及阿里云平台侧的相关要求不再进行单独测评，可以直接引用阿里云平台的测评结论。

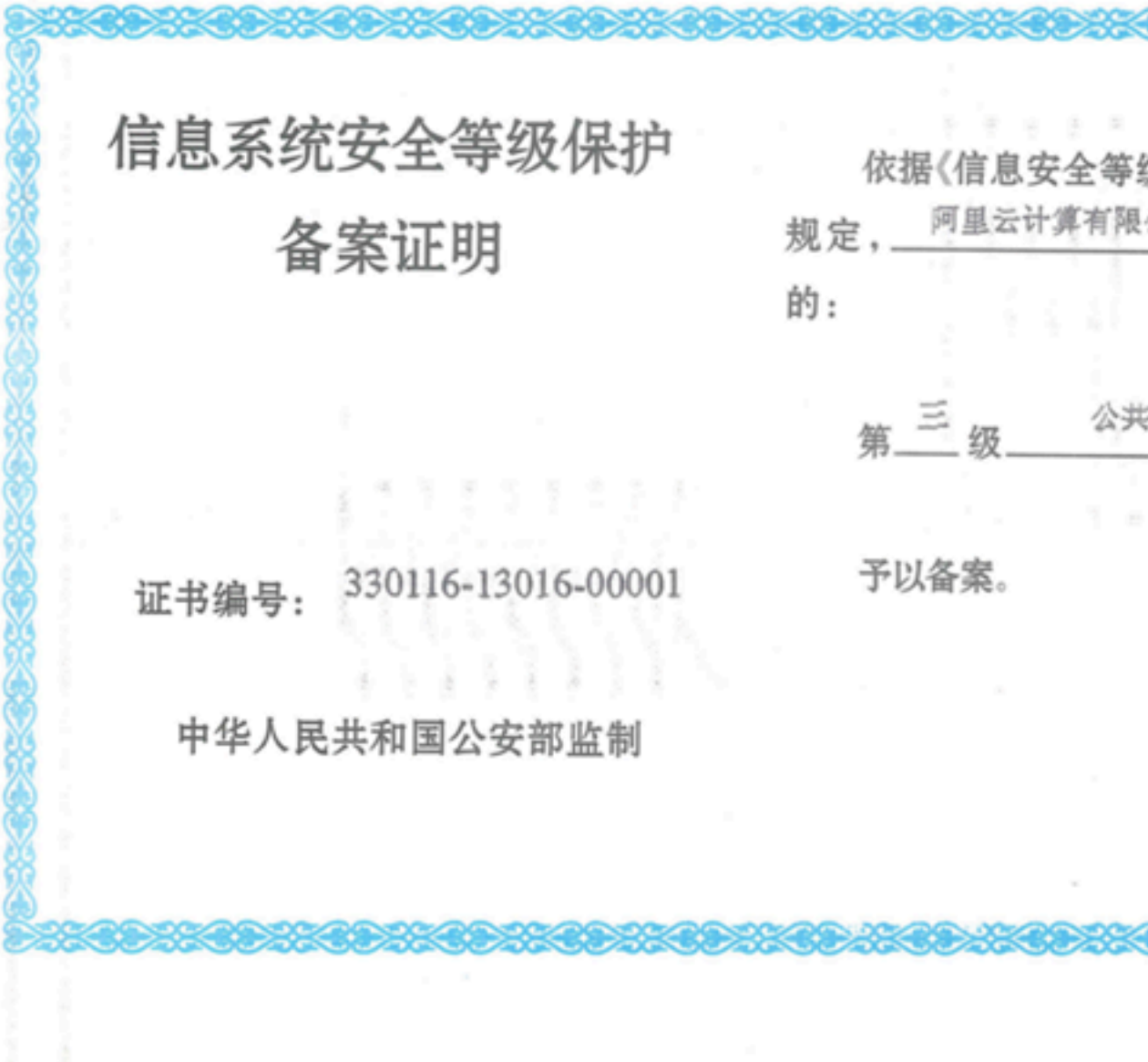
阿里云将提供以下材料，协助租户云上系统通过等保测评：

· 阿里云等保备案证明

· 阿里云测评报告封面及结论页

· 阿里云安全产品销售许可证（公安部）

图 2-2: 阿里公共云平台三级等保认证


信息系统安全等级保护
备案证明

依据《信息安全等
规定，阿里云计算有限
的：

第三级 公共

证书编号：330116-13016-00001

予以备案。

中华人民共和国公安部监制

图 2-3: 阿里金融云四级等保认证

阿里云安全产品

阿里云利用云盾、云防火墙和其他安全生态产品，可以提供完整的安全技术解决方案，相关的阿里云安全产品及其满足的等保要求如下。

领域	安全产品	功能简介	合规对应要求
网络和通信安全	VPC	阿里云专有网络，可以实现VLAN级隔离，并自定义IP地址分配（可选）。	满足等保要求中的网络架构、边界防护和访问控制等要求。
	DDoS高防	提供网络链路可用性保证，提升DDoS防护阈值，提升业务连续性（必选）。	满足等保网络安全中访问控制和机构安全的要求，20G以上防护。
	云防火墙	相比于传统防火墙以及安全组策略，云防火墙可以基于业务可视化、实现业务分区／分组，管理员可以清晰的甄别合法访问和非法访问，从而执行安全隔离和访问控制策略（必选）。	满足等保要求中的边界防护和访问控制等要求。
	Web应用防火墙	可防护应用攻击、CC攻击等，可根据网站实际防护场景需求实现精准防护，多种防护算法结合防御，实现业务风控，并可快速更新漏洞补丁，保障您的网站业务不被侵害受损（必选）。	满足行业自身的安全需求且满足等保要求中的入侵防范等要求。

领域	安全产品	功能简介	合规对应要求
	态势感知	· 实时全球访问流量监控。 · 实时监控整体安全。 · 云上服务器全端口扫描、应用漏洞扫描、0day漏洞扫描、CMS漏洞扫描。 · 服务器、数据库和应用后台弱口令探测。 · 通过大数据分析的方法发现隐藏的入侵安全事件，并回溯入侵点。 · 黑客恶意行为回放，对黑客入侵后的操作行为进行取证和记录。 · 高级威胁检测，如：定点web攻击，针对性ECS密码爆破。 · 利用社会工程学，对撞库攻击进行识别，保证业务账号安全。 · 利用全网威胁情报对异常登录事件、非常用IP连接数据库进行识别。 · 拖库行为发现，对数据库的异常下载进行告警。 （必选）	满足等保要求中安全审计和集中管控的要求。
	云堡垒机	实现云上服务器的操作运维审计和账号权限管理。支持100资产和100会话。	满足等保要求中身份鉴别、访问控制和安全审计等要求。

领域	安全产品	功能简介	合规对应要求
设备和计算安全	安骑士	· 跨平台支持配置四层（tcp、udp）七层（http）的自定义访问策略。 · 共享云盾恶意IP库，实时拦截全网威胁访问源。 · 全流量日志审计，秒级发现非法访问、主动外连等行为。 · 扫描第三方应用（wordpress、discuz等）及windows系统漏洞信息。 · 网站后门文件（webshell）检测及隔离。 · 恶意进程检测及病毒、木马查杀。 · SSH、RDP登录日志审计，异地登录提醒。 · 对暴力破解密码的行为进行拦截。 · 对服务器常见系统配置缺陷进行检测，包括可疑系统账户、弱口令、注册表等进行检测。	满足等保要求中关于入侵防范和恶意代码防范的要求。
	数据库审	数据库审计，同时支持RDS云数据库、ECS自建数据库，符合等级保护二级标准，帮助用户满足合规性要求，支持3个数据库（RDS）实例。（必选）	满足等保要求中安全审计的要求。
应用与数据安全	数据加密	加密服务基于国家密码局认证的硬件加密机，提供了云上数据加解密解决方案，用户能够对密钥进行安全可靠的管理，也能使用多种加密算法来对云上业务的数据进行可靠的加解密运算。	满足等保中对于数据保密性要求。
	SSL证书服务	为HTTP网站提供转向HTTPS，加密应用层数据（必选）。	Globalsign通配符域名证书，满足等保要求中数据完整性和数据保密性的要求。

领域	安全产品	功能简介	合规对应要求
安全运维管理	漏洞扫描系统	满足等保要求中关于及时发现漏洞和进行漏洞升级要求（必选）。	定期进行全网络的扫描，及时发现各种漏洞包括主机、网络和应用漏洞，以便进行系统加固。

3 新零售安全解决方案

3.1 背景信息

新零售的衍生

2016 年“双 11”上，阿里巴巴集团 CEO 张勇首次系统地对新零售进行了阐述，他认为，新零售就是通过大数据和互联网重构“人、货、场”等商业要素而形成的一种新的商业业态。2017 年 4 月，马云在 IT 领袖峰会再次提及新零售，他谈到，线下与线上零售深度结合，利用大数据、云计算等创新技术，构成未来新零售的概念。

在此基础之上，众多学者和经营者对于“新零售”的概念和含义进行了讨论和解读，新零售研究风生水起。新零售的产生，有其特定的背景基础——“双升”驱动，在技术升级与消费升级驱动下，新零售应运而生。更多新零售行业介绍请参考 附录 1 什么是新零售 章节。

新零售的安全挑战

新零售与我们每个人的生活息息相关，电商交易系统不仅存有海量的用户敏感数据，而且直接涉及到资金交易。新零售在迅速发展过程中，线上平台与传统电商一样，面临严峻的安全态势，线上系统几乎每天都会面临新型0day攻击：

- 线上系统多数使用通用Web组件，如apache、iis、phpcms等，这些组件几乎每天都有新型漏洞爆发。
- 此类漏洞危害性巨大，甚至可以直接控制服务器权限。例如：Heart Blood(Openssl高危)、Struts2系列(s2-045、s2-048等)等类型漏洞。
- 线上系统攻击工具脚本化，流水线的黑产行业极大降低了入侵成本，加快了入侵速度（爆发当天全网扫描）。

典型的安全威胁有：

- 数据泄露：服务商的销售业绩、用户资料、订单信息等数据泄露，不仅容易被竞争对手进行商业分析构成商业威胁，还可能由于用户数据的泄露违反《网络安全法》，更进一步如果用户因此受诈骗，服务商需承担刑事任。
- 业务欺诈：业务场景成为黑产重点攻击目标，通过Bot伪装、风险欺诈对服务商的业务进行攻击欺诈。例如：
  - 商品抢售
  - 克隆网站
  - 恶意下单、刷单
  - 营销作弊、抢红包
  - 恶意好评、刷榜
- 恶意注册/登录：通过网站侦查、访问伪装，黑产可消耗大量服务商的短信注册接口与短信费用，甚至拿到消费用户数据，构成商业威胁或进行定向欺诈。

- 比价爬虫：通过网站侦查、准备爬虫，黑产可爬取线上系统的商品价格，进而可能引起价格策略的恶性竞争，此外线上系统被爬虫恶意海量爬取信息时，会导致资源消耗，消费用户访问卡顿变慢。

法规监管要求

随着近年新零售的逐步发展和国家相关法规的逐步完善，新零售行业融合线上线下业务，面临着更严格的法规监管要求。例如：

- 《网络食品安全违法行为查处办法》：要求线上电商平台需要对所售食品安全负责，如果未履行相关义务导致严重危害后果的，可能需停业并接受通信主管部分处理。
- 《烟草专卖法》：要求线上电商平台不允许销售烟草产品。
- 《中华人民共和国刑法》：规定售卖发票为违法行为。
- 新《广告法》：明确广告中禁用词。

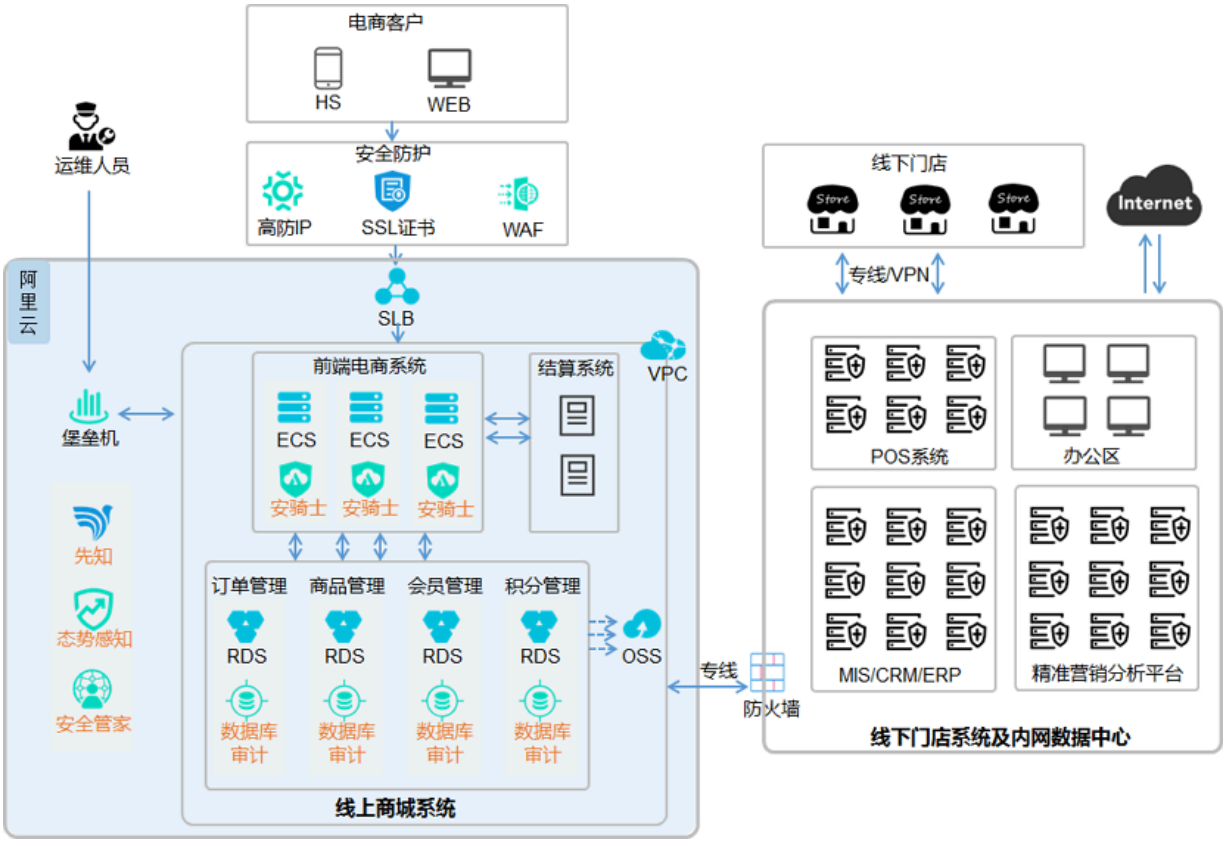
种种法规从系统、业务、内容各个层面对新零售的线上、线下业务提出了严格的安全要求。

3.2 阿里云安全解决方案

阿里云以“系统-业务-内容”全方位防护、完善的云端纵深防御、线上线下一体化、全生命服务周期为设计理念，为新零售提供一体化的安全解决方案。

系统安全架构

新零售的线上系统建议参考以下系统安全架构进行安全防护，以保障线上系统的安全性。



架构说明：

- 新零售包含线上业务与线下实体店，阿里云针对新零售的业务形态，建议将线上商城系统部署于阿里云上，线下门店系统及内网数据中心部署于客户线下机房，线上、线下业务相对隔离。
- 云上系统与云下系统通过专线、VPN连接。
- 云下系统部署防火墙产品，保障云下系统安全。
- 云上系统使用以下阿里云安全核心产品保障安全性。

安全域	服务名称	安全设计
网络安全	DDoS高防IP	使用DDoS高防服务提供网络链路可用性保证，提升DDoS防护阈值，提升业务连续性。

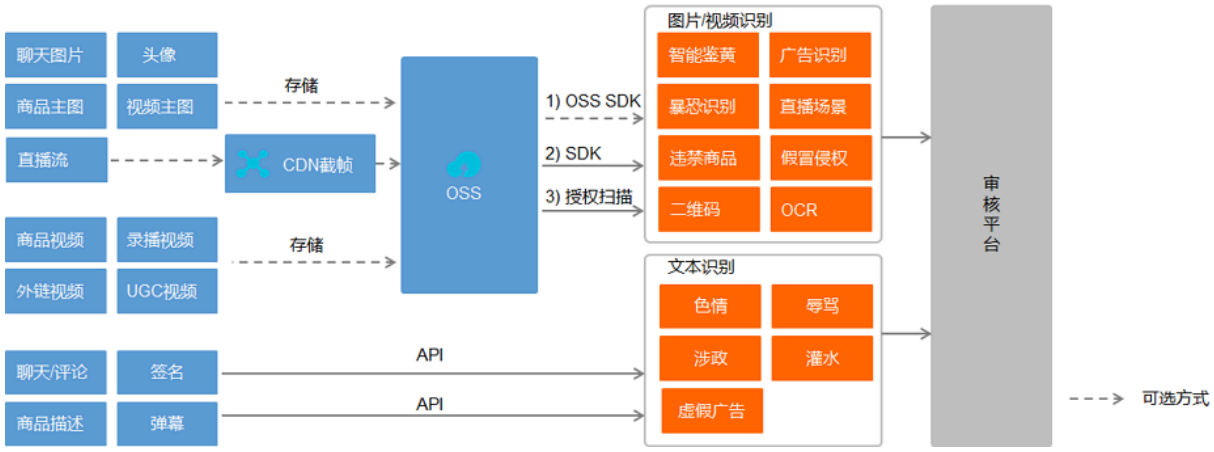
安全域	服务名称	安全设计
	VPC	使用阿里云VPC，隔离本系统网络与外部网络环境，并可自主规划网络内的业务网段，实现VLAN级别的网络隔离。
应用安全	Web应用防火墙	部署Web应用防火墙防护恶意应用攻击，保障移动、PC等互联网用户的接入安全。
	漏洞扫描	满足等保要求中关于及时发现漏洞和进行漏洞升级要求。
数据安全	SSL 证书	使用SSL证书服务，为HTTP网站提供转向HTTPS，加密应用层数据。
服务器安全	安骑士	通过安骑士实现对服务器的入侵防范和恶意代码防范。
安全审计	数据库审计	使用数据库审计服务，实现对RDS数据库、ECS自建数据库的审计功能。
	堡垒机	使用堡垒机管理运维ECS，实现云上服务器的操作运维审计和账号权限管理。
安全专家服务	安全管家	阿里云安全管家服务是阿里云安全专家基于阿里云多年安全最佳实践经验为云上用户提供的全方位安全技术和咨询服务，为云上用户建立和持续优化云安全防御体系，保障用户业务安全。
安全管理	态势感知	使用态势感知服务实现流量监控、整体安全监控，实现安全审计与集中管控。

内容安全架构

对新零售的线上电商平台、线下门店，阿里云提供内容安全服务。

- 线上电商平台：可对图片、视频、文本、语音等对象（例如会员昵称/头像、商铺名称/推广图片、视频直播等）进行多样化场景检测，有效帮助您降低内容违规风险。违规检测包括：涉黄、涉政、暴恐、违禁、敏感人脸、侵权等。
- 线下门店：通过内容安全服务，可对线下门店中的客户做客户群体画像分析、客户行为识别、异常人群/行为监控等。

加强内容安全防护时，推荐参考以下内容安全架构，以保障线上线下内容安全。



方案思路与优势

阿里为新零售行业提供一体化的安全解决方案。

- “系统-业务-内容”全方位防护
  - 系统安全：“云管端”整体安全防护
  - 业务安全：实人认证、业务风控、手机号情报
  - 内容安全：图片、视频、音频、文字全面防控
- 完善的云端纵深防御
  - 云上业务整体态势感知，实现潜在威胁可视化
  - 针对数据库SQL注入、风险操作等数据库风险操作行为进行记录与告警
  - 云主机全量漏洞管理、基线检查和入侵告警等
- 线上线下一体化
  - 线上线下全方位态势感知，构建全景威胁可视化
  - 云下生产系统主机漏洞管理、基线检查和入侵告警等
- 全生命服务周期
  - 事前：安全威胁可预警及可预先决策防御
  - 事中：威胁风险控制，减少攻击面
  - 事后：合规审计、攻击溯源

3.3 客户案例

阿里云等保合规安全解决方案已成功助力多位客户完成等保合规认证。

智融集团

智融集团专注于以人工智能为核心的新金融技术，旗下包含为非传统金融机构目标人群提供小额周转的金融服务APP“用钱宝”，基于机器学习及大数据计算的人工智能风控引擎“I.C.E.”，以及信贷过程管理体系“慧诚帮帮PaaS”三大业务版块。

闪银奇异

北京闪银奇异是中国第一家互联网信用评估公司，其开发的Wecash闪银奇异是目前国内最先进的大数据信用评估平台。Wecash闪银是中国首家互联网信用评估平台，依托数据挖掘分析和机器学习技术，实现快速精准的信用评估。

斑马智行

斑马智行是上汽集团和阿里巴巴集团共同打造的互联网汽车解决方案。 现在已登陆全球首款量产互联网汽车荣威RX5。主要功能有旅途记录、远程车辆控制、车辆报警、道路救援。

全球影像

全球影像网以医疗影像的采集、传输、云存储为基础，满足医院远程会诊、双向转诊，医生移动阅片、远程影像诊断/示教、远程视频问诊等一系列医疗综合应用需求，为当下“看病难、看病贵”等社会问题提供解决之道。

3.4 附录 1 什么是新零售

2016 年“双 11”，阿里巴巴集团 CEO 张勇首次系统地对新零售进行了阐述，他认为，新零售就是通过大数据和互联网重构“人、货、场”等商业要素而形成的一种新的商业业态。2017 年 4 月，马云在 IT 领袖峰会再次提及新零售，并对新零售进行了比较详细的阐述。他谈到，线下与线上零售深度结合，再加智慧物流，服务商利用大数据、云计算等创新技术，构成未来新零售的概念。

在此基础之上，众多学者和经营者对于“新零售”的概念和含义进行了讨论和解读，新零售研究风生水起。新零售的产生，有其特定的背景基础——“双升”驱动，在技术升级与消费升级驱动下，新零售应运而生。

技术升级为新零售提供发动机

云（云计算、大数据）、网（互联网、物联网）、端（PC 终端、移动终端、智能穿戴、传感器等）构建起“互联网+”下的新社会基础设施，为新零售准备了必要的条件。

一直以来，零售商依赖于数据塑造与顾客之间的互动，通过信息技术推动商业向顾客深度参与的方向发展。最初阶段是 POS系统引入店铺，获得基础数据，并在此基础之上发展会员制度。

第二阶段利用互联网的发展，通过移动端和社交媒体获取有效的消费者信息。

第三阶段，伴随近场感应终端、应用场景定位、虚拟试衣镜、传感器、大数据、移动终端等技术，完善商户线下应用场景，实现设备与人之间的实时互联。

第四阶段，通过远程无线技术（LoRT）搭建物联网，并通过物联网将信息实时传输给有关系统和终端用户，使得无论消费者身在何方，都处于智能设备访问范围之中，从而使得零售商能够从互联的零售系统和设备之中采集数据，并通过智能系统驱动优化操作。

我国目前的零售业发展正在跨过第二阶段，很多企业进入第三阶段：通过场景服务运营商提供整套“互联网+”的解决方案，实现Wi-Fi 覆盖和i-Beacon 应用进行场景定位，并通过近场感应终端、传感器等技术，实现对消费者购物轨迹的全流程追踪。

伴随着物联网技术的成熟以及在零售领域的应用，零售业对技术的应用将进入第四阶段，即物联网+零售，零售行业的服务边界进一步扩展。以天猫为代 表的新零售平台，通过其云计算、大数据、人工智能等互联网底层技术能力，链接品牌商、供应商、分销商、服务商等零售业生态伙伴，向着自助化、智能化发展，形成全新的商业基础设施，全面赋能合作伙伴，与消费者产生全新的链接和互动。技术发展为新零售产生提供了土壤，新零售沿着如上轨迹产生、发展、成熟。

消费升级为新零售增强牵引力

居民消费购买力日益攀升，消费主体个性化需求特征明显，消费主权时代到来，对商品与消费的适配度提出了更高的要求，同时对零售升级产生了巨大的牵引力。

消费购买力提升、消费主体更加个性化。

目前，18-35 岁的新生代和上层中产及富 裕阶层构成了我国的消费主体。他们更加注重商品和服务的品质、品牌，以及生活质量与效率。消费的档次被拉开，消费的“羊群效应”逐渐消失，排浪式消费基本宣告终结。与之相对应，个性化、多样化消费需求大规模兴起，渐成主流。消费者更加看重商品的个性特征，以期展示自我，而不只限于满足对物的需求。

个性化消费需求特点有三：注重心理满足，追求个性、情趣；强调商品或劳务内在的质的要求，如商品的时尚性、独特性和安全性；关注消费的文化内涵，如商品的欣赏价值、艺术价值和文化特质等。多样化消费需求主要体现在两方面：一是不同个体表现出越来越多样的消费需求；二是同一个体在不同生活场景或领域的消费需求可能存在较大差异。总体上，其特点可概括为“广泛性、个体性、情感性、多样性、差异性、易变形和关联性”。

新零售是我国零售业多年创新积累后降生的新生命，其着眼点是全球商业在互联网和大数据时代的未来图谱。在天猫等电商平台带动下，经历了一段时间的快速成长，目前已初具全球竞争优势。未来要小心呵护，保障其健康成长，在前进的道路上走得更稳、更远。

更多新零售发展现状的学习请参考 商务部发布首个“新零售”报告#一文读懂中国新零售现状 一文。

3.5 附录 2 网安法重点解读

《网络安全等级保护基本要求》重点解读

根据网安法，企业需关注：

- 义务：按照网络安全等级保护制度履行安全保护义务，保障网络免受干扰、破坏或未经授权的访问，防止网络数据泄露、篡改。
- 责任：网络运营者应对保障用户信息安全负有主体责任。
- 措施：
  - 制定网络安全事件应急预案，及时处理系统漏洞、计算机病毒、网络攻击、网络入侵等安全风险、并按照规定向有关部门报告。
  - 加强对用户发布信息的管理，及时消除法律、行政法规禁发的信息，建立网络信息投诉、举报制度、并及时受理。
  - 对收集的用户严格保密，并建立健全用户信息保护制度，不得非法收集、提供、获取、 使用用户信息。
- 维护：做好公共通信和信息服务、能源、水利、金融、公共服务、电子政务等重要行业的数据备份、防篡改、防泄漏、容灾措施，尤其是国家关键信息基础设施系统。