京东智联云

京东智联云

数据安全白皮书

2019

版权声明

商标声明

京东智联云及其它京东智联云服务相关的商标均为北京京东叁佰陆拾度电子商务有限公司及其关联公司所有。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

法律声明

本文档仅供用户使用京东智联云产品及服务的参考性指引，本文档中的所有陈述、信息和建议以及内容的准确性、适用性等不构成任何明示或暗示的担保。任何主体和个人因使用和信赖本文档而发生任何差错或经济损失的，京东智联云不承担任何法律责任。
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。京东智联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。
本文档未授予用户任何京东智联云产品的任何知识产权的法律权利。

引言 Introduction

伴随云计算、大数据、人工智能等新兴技术的飞速发展，数据作为支撑这些前沿技术存在与发展的生产资料，已经成为组织的核心资产，并且受到了来自个人、组织乃至国家前所未有的重视与保护。在大数据时代，个人信息保护和监管已受到各国的高度关注， 如何确保数据的安全已成为个人隐私安全、企业资产安全、甚至国家和社会安全的核心问题。

近年来云计算市场规模持续增长，但数据泄露等安全事件频发不断，给国家和人民造成了巨大的经济损失。工信部于 2017 年发布的《 云计算发展三年行动计划（ 2017-2019 年 ）》中，将多租户数据保护列为云计算环境下产生的新型安全问题，并在《 云计算综合标准体系化建设指南 》中强调“ 云安全是影响云计算发展的关键因素之一”，且把“ 数据和隐私保护 ”纳入云安全标准规划中。各国都相继出台了大量与数据安全有关的法律法规，对个人、企业和国家重要数据进行保护。这些重要的法律法规包括： 我国在 2016 年出台，2017 年 6 月 1 日正式生效的《 中华人民共和国网络安全法 》。欧盟在 2015 年出台，2018 年 5 月正式生效的一般数据保护条例《 General Data Protection Regulation 》（ 简称 GDPR ）。我国在 2018 年正式出台，同年 5 月 1 日正式生效的个人信息安全规范，GB/T 35273《 信息安全技术 个人信息安全规范 》。与此同时，我国正在制定即将颁布的《 数据出境管理办法 》、《 重要数据管理办法 》、《 中华人民共和国密码法 》等。这些法律法规及标准，从数据处理合法、用户权利、数据安全、事故披露、跨境传输等方面对数据保护提出了更高更严格的要求。

越来越多企业和政府客户将业务部署到云环境上，在云服务模式下如何保障云上数据安全，成为大多数企业和客户的非常关注问题。

京东智联云以“ 让云端数据更安全 ”为目标，践行“ 尊重数据主权不碰用户数据，提供安全保障保护用户数据安全，保护隐私对用户透明可信 ”的理念。籍此白皮书发布，将京东智联云多年在数据安全领域的实践和经验，分享给客户，分享给业界。同时京东智联云，严格遵守国家法律要求，依托京东集团及京东智联云特有技术优势，打造可信的云服务，与客户及合作伙伴共建数据安全能力。并将持续提升数据安全防护能力，不断推出可靠的安全服务产品，保障客户云端数据安全。

目录 Contents

01

概述

数据安全是云服务商最为关注的安全问题，也是用户选用云服务时的关键考量。为此，京东智联云对用户关心的云上数据安全问题进行了深入剖析，通过以“让云端数据更安全”为目标的安全体系方法论及可靠的数据安全框架，完善的数据安全管理方法、先进的技术支撑、丰富的数据安全合规实践，实现对用户数据安全的承诺，为用户云端数据安全保驾护航。

京东智联云以安全为基准生命线，将保障用户在京东智联云上的数据安全、业务安全作为第一要务。京东智联云，作为京东集团旗下的全平台云计算综合服务提供商，凭借京东集团多年的数据安全管理经验和技术积累，为云平台搭建了强大的纵深安全防御体系，将数据安全理念融入每一个产品的需求设计和开发过程中，并贯穿产品运营的每一个环节。建立了集主动风险感知、智能协同防御、多维关联分析和溯源取证于一体的安全管理闭环。在保障云平台安全的同时，全力协助京东智联云用户保障其云端数据的安全。

02

京东智联云数据安全观

02/1 数据安全框架

京东智联云尊重用户的数据主权，提供安全保障措施及服务，供用户安全地处理数据，协助用户发挥数据价值。用户拥有其云上数据的所有权、控制权和知情权。京东智联云不接触用户数据，用户可以用任何方式管理自己的私有数据，按用户所希望的格式保存其数据，选择任何方式加密自己的数据，在指定的任何时间移动或者删除它。并且用户有权利了解数据存储、传输、访问、使用、销毁等机制。

图 1 京东智联云数据安全框架

京东智联云数据安全是以“让云端数据更安全”为目标的安全体系构建的方法论及实践，核心内容包括：

（1）满足安全合规性、数据安全保护、隐私及敏感数据管理三个需求目标；

（2）核心理念：数据主权、安全保障、透明可信；

（3）数据安全治理：数据安全人员组织、数据安全使用的制度、策略和流程、数据安全技术及工具支撑；

（4）京东智联云数据安全保护体系： 京东智联云践行**“尊重数据主权不碰用户数据，提供安全保障保护数据安全，保护隐私对用户透明可信”**的理念，以满足合规监管要求和用户业务需求为出发点，严格贯彻数据安全治理的执行要求，结合积累的云安全实践及安全运营保障经验，构建数据全生命周期安全保护体系。

02/2 数据安全合规

京东智联云持续努力完善标准认证体系，参与业界数据和隐私保护标准化工作，致力于数据安全能力建设和数据安全治理成效，务求更好地向用户展示京东智联云的合规实践并帮助用户保护云端数据安全。

京东智联云权威数据安全相关的认证：

> ISO27001 信息安全管理体系国际认证

> 公安部信息系统安全三级等保认证

> 中国信息通信研究院可信云服务认证

> 工业和信息化部云计算服务能力标准符合性证书

> 支付卡行业数据安全标准认证（ PCI DSS ）

> CSA STAR 云安全认证

> C STAR 云计算安全评估认证

ISO27001
信息安全管理体系
国际认证

公安部
信息系统安全三级
等保认证

中国信息通信研究院
可信云服务认证

工业和信息化部
云计算服务能力标准
符合性证书

支付卡行业数据安全
标准认证
（ PCI DSS ）

CSA STAR
云安全认证

C STAR
云计算安全评估认证

图 2 京东智联云安全资质认证

02/3 数据保护承诺

从京东智联云安全视角，用户在使用京东智联云服务时，通常提供或产生以下两类数据：账户信息（用户账户的创建或管理相关的用户信息）和用户内容（用户使用京东智联云服务过程中存储或处理的内容）。京东智联云将采取最高级别的安全措施保护这些数据的安全。

京东智联云在遵从国家法律法规要求的前提下，会收集用户的账户信息，包括但不限于用户的注册信息、操作日志等，京东智联云将依照《用户服务协议》、《隐私政策》予以尊重和保护，在处理过程中，遵循数据最小化原则收集、存储和使用用户的账户信息，并通过全面的数据保护措施确保用户的账户信息安全。对于用户内容数据，京东智联云采用符合业界标准的安全防护措施，为用户提供数据保护的服务和工具，保障数据的机密性、完整性、可用性、可追溯性等多种安全特性，为用户打造值得信赖的云服务环境，确保坚守不触碰用户数据原则之上，帮助用户保障数据安全。

03

云端数据保护职责

03/1 数据安全责任共担模型

京东智联云在《京东智联云安全白皮书》中详细介绍了京东智联云信息安全责任共担模型。就数据安全而言，用户对其托管于云端的数据拥有完全的控制权，并负责自身云端业务数据的安全管理，包括收集与识别、分类与分级、权限与加密等。

图 3 数据安全责任共担模型

03/2 用户的责任

用户是其数据的拥有者。用户依据自身业务发展的需要以及面临的数据安全风险，制定数据保护策略，并采取适当的措施，保障云上数据安全。

用户可以自行配置京东智联云提供的数据加密手段、访问管理功能、用户验证机制、数据备份与恢复工具等，以确保其对云端数据的保护并满足业务和合规的要求。

03/3 京东智联云的责任

京东智联云作为云服务提供者，负责基础设施、云平台的安全，并帮助用户保障其云端数据的安全，向用户提供丰富的数据安全服务产品和解决方案，服务和方案的选择由用户自主完成。

04

京东智联云数据安全实践

京东智联云遵循数据安全生命周期管理的业界先进标准，采取管理和技术两方面的手段进行全面数据安全体系建设。数据安全管理遵循“责任明确、授权合理、流程规范、技管结合”的工作方针。在安全通信、身份认证、访问控制、权限管理、数据隔离、数据加密、数据安全审计等方面，保证用户数据的隐私权、所有权和控制权不受侵犯，为用户提供最切实有效的数据保护。

04/1 京东智联云数据安全保护体系

京东智联云建立了完整的数据安全保护体系（如下图所示）。

图 4 京东智联云数据安全保护体系

数据安全保护体系是以合规监管要求和用户业务需求为输入，结合数据安全在人员组织、制度流程、技术保障的执行要求，通过技术工具的使用，贯穿整个数据全生命周期过程域的安全能力建设。

人员组织：是数据安全组织的架构建立、职责分配管理工作。分为决策层、管理层、执行层及监督层，分别负责制定数据安全的目标和愿景、制定数据安全管理策略和管理规范、保证数据安全工作推进落地。

制度流程：是安全具体管理制度的建设和执行，包括数据安全总纲、安全制度、安全指导手册、执行过程文档。

技术保障：确保平台和服务的自身安全并持续保障用户终端数据安全所做的措施。

技术工具： 针对数据全生命周期安全保障有效执行的技术和工具，包括独立的系统平台、功能、工具或算法技术等。

04/2 网络与基础设施保障

网络安全是保证数据安全传输和交换的基础，基础设施安全是数据安全的基石。京东智联云网络与基础设施提供了强大的保护措施来保护用户数据及业务。京东智联云为用户提供全球部署、多地域、多可用区的云数据中心，实现了 Region 区域级、AZ 可用区级、FD 故障域级容灾能力。采用多线 BGP 网络提高网络接入体验，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。保证云计算整个基础框架的高可用性、高可靠性以及云主机的高可用性，同时确保云平台提供不间断的服务，不但提高了数据的可靠性，也提高了数据的安全性。

4.2.1 对云平台的安全保障

云端数据的安全需要安全可靠的云平台环境。京东智联云提供成熟的网络安全架构及多层防护安全方案，对生产网络与非生产网络、业务网络和管理网络、虚拟网络和物理网络进行了安全隔离和严格的访问控制。为了保障云平台的安全，京东智联云从底层云平台基础架构安全性入手，结合大数据处理的能力，以及业界优秀的第三方安全厂商打造完整的安全生态体系，实现云平台、网络、系统、数据和应用系统安全的全面覆盖。

· 网络安全保障

在 Internet 与云平台服务、资源组之间的边界区域提供可靠的安全组件，可防止不受信任的网络访问内部网络资源。云平台使用抗拒绝服务 (DDoS)、应用安全网关、Web 应用防火墙、以及 VPN 设备防护，同时实施防火墙策略、访问控制列表 (ACL) 或特定路由等安全策略。

· 安全隔离保障

云平台网络隔离，各级网络以及虚拟设备之间的有效隔离是确保用户数据安全的关键控制。京东智联云通过网络访问控制列表(ACL)技术将对外提供服务的“云服务网络”和支撑云服务的“物理网络”进行安全隔离。

网络隔离服务，京东智联云私有网络（VPC）是用户在京东公有云上自定义的逻辑隔离的网络空间，此私有网络空间由用户完全掌控，用户在京东智联云上构建逻辑隔离的网络环境，可以自主规划网络部署，并通过安全组和网络 ACL 等实现多级安全防护。实例默认部署在用户自定义的 VPC 私有网络内，在 TCP 层直接进行网络隔离保护，确保数据安全。

用户隔离，用户实例隔离基于硬件虚拟化技术的虚拟机管理，在系统层面将多个虚拟机进行隔离。通过对服务器物理资源的抽象，将 CPU、内存、I/O 等物理资源转化为一组统一管理、可灵活调度、可动态分配的逻辑资源，并基于这些逻辑资源，在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。在虚拟化层，保证虚拟机只能访问分配给它的物理磁盘空间，从而实现不同虚拟机磁盘空间的安全隔离。

· 云平台监测与防护

京东智联云安全运营机制可以及时获知并解决外部安全威胁及内部安全漏洞，云平台利用安全自动监测系统，搭配威胁情报、反欺诈功能以及态势感知分析模型，有效阻止黑客入侵、恶意攻击等问题，并会在第一时间处理相关安全事件，保证京东智联云平台的安全稳定及用户数据业务安全。

· 云平台安全审计

京东智联云审计机制进行监控、审计、分析，及时发现异常数据流向及操作行为，一旦出现可能导致数据外泄、受损的恶意行为时，审计机制可以第一时间发出威胁告警。生产环境的运维操作通过堡垒机进行，后台运维操作记录均有统一的日志记录，并进行自动化安全审计。同时操作记录实时传输到集中日志平台，通过违规事项审计规则，主动发现异常或违规行为。

4.2.2 对用户提供的安全服务

为了确保用户在使用云服务的过程中数据受到实时的保护，京东智联云在云平台的各个层面提供了用户能够感知和应用的云安全产品及服务，以帮助云用户快速高效地部署云端安全防护。

图 5 云安全产品服务

· 网络安全

京东智联云免费为用户提供最高 2Gb 的默认 DDoS 基础防护能力，针对遭受大流量的 DDoS 攻击的用户，机房集群高达 1.5T 的清洗能力，能从容应对各种大流量 DDoS 攻击，保证用户的业务能够平稳安全地运行。VPN 连接利用公网架设专用网络，通过加密通道实现外部用户内网访问、跨地域内网互通等。私有网络支持用户在京东智联云上构建逻辑隔离的网络环境，用户可以自主规划网络部署，包括网络范围、子网网段、路由策略等，并通过安全组和网络 ACL 等实现多级安全防护。

· 系统安全

主机安全为用户提供的云主机安全管理，采用轻量级安全防护进程实现主机风险实时监测、安全威胁及时预警，恶意入侵精准防护，有效提升主机安全防御能力，保障用户云主机业务安全。

· 应用安全

Web 应用防火墙，针对网站业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障用户业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。

应用安全网关，是对网站或 APP 服务进行可视化安全分析和应用层威胁防护的产品。通过提供 WAF、用户访问审计、业务安全可视和合规性检查等功能，保障业务稳定可持续运行，提升用户体验，为网络服务提供者解决 HTTP/HTTPS 业务因攻击导致的异常或合规性问题。

· 数据安全

密钥管理服务 KMS（Key Management Service），为用户提供的一款数据安全管理产品，使用硬件安全模块（HSM）来保护用户的密钥安全。用户可安全、可控、便捷的使用托管密钥，专注于开发需要加解密功能的场景。

SSL 数字证书，为用户提供安全套接层（SSL）证书的一站式服务，包括证书上传、下载、管理、申请购买等功能，基于京东智联云与顶级数字证书授权（CA）

机构和权威经销商合作，为用户提供数字证书的全生命周期管理，实现网站的可信身份认证及数据安全传输。

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。

· 安全管理

态势感知系统，为用户提供大数据安全分析。通过数据建模、行为学习、情报关联分析，全面洞悉安全全景、发现入侵和攻击威胁，帮助用户建设自己的安全监控和防御体系。对多维度海量安全和业务数据进行快速、自动化的关联分析，通过图形化、可视化的技术将威胁和异常的总体安全态势呈现给用户。

· 安全服务

基线检测服务，在用户充分授权的情况下，对用户云上系统进行全面的安全基线检测，帮助用户掌握云上系统整体的安全脆弱性状况，并依据检测结果与用户业务模式特点，提供有针对性的安全修补建议，降低系统的安全威胁。

漏洞扫描服务，在用户充分授权的情况下，对用户指定的操作系统、Web 服务、数据库等提供全面的漏洞扫描服务，由京东智联云安全专家对扫描结果进行解读，并提供专业的漏洞扫描报告和修复指导建议，帮助用户有效地降低业务安全风险。

渗透测试服务，对现有系统不造成任何损害的前提下，以攻击者视角，模拟黑客入侵的技术手段对用户指定系统进行全面深入的攻击测试，发现系统中潜在的风险威胁，帮助用户降低因黑客入侵带来的经济损失。

应急响应服务，当用户遭遇网络攻击、木马病毒、数据窃取等黑客入侵事件时，京东智联云能够提供包括抑制止损、事件分析、系统加固、事件溯源等应急响应服务，帮助用户降低安全事件对自身造成的影响与损失。

04/3 身份与访问控制

有效的身份认证与访问控制是确保用户数据不被非授权访问的关键，同时促进合法用户的可用性。这些技术包括认证机制，数据和资源访问控制，供应系统和用户账户管理。对于云平台自身，京东智联云构建了基于内控要求的账号与授权管理系统和员工身份识别机制。对于用户，京东智联云提供了身份管理与访问控制服务 (IAM)。

· 云平台身份与访问控制

京东智联云结合自动化的运营管理机制，统一的云安全运维规范，所有对产品的运维操作都受到严密的权限控制和监控。云平台帐号的权限分配遵循“权限明确、职责分离、最小特权”的原则。一个帐号对应一个用户，而一个帐号拥有的权限是由其被赋于的岗位角色所决定的，按照角色或用户组进行授权。结合人工和静态扫描技术，对现有账号情况进行详细梳理，梳理结果形成账号和权限基线，通过扫描技术对所有账号及权限进行变化监控。

· 用户身份与访问控制

用户可以通过身份管理与访问控制(IAM)服务创建、管理子用户账号，并控制这些子用户访问京东智联云资源的权限。使用访问控制，用户可以向他人授权管理账户中的资源，而不必共享账户密码或访问密钥 , 按需为用户分配最小粒度的操作权限，从而降低主账号的信息安全风险。

> 集中管理 IAM 子用户及其安全凭证：在访问控制中创建子用户，可以控制子用户的控制台登录或者 Open API 访问权限，进行统一的虚拟 MFA认证，操作保护和访问密钥(AK/SK)管理。

> 对云资源进行精细访问控制：为每个用户或用户组绑定一个或多个权限策略，限制用户对特定资源的特定操作权限，也可以使用 IAM 添加特定的条件，以控制用户是否在特定的时间，特定的源 IP 地址，是否使用 SSL，是否通过虚拟 MFA 设备进行身份验证等。

> 集中管理用户角色和服务角色：用户可以在 IAM 中创建角色并管理权限，以便控制扮演该角色的子用户或服务可以执行哪些操作。也可以定义有哪个子用户扮演该角色，也可以使用服务角色或者服务相关角色，指定相应的服务扮演该角色，代表管理和操作云的其他资源。

04/4 数据全生命周期安全保障

为保障用户安全的处理云上数据，京东智联云对数据全生命周期的数据生产、数据存储、数据传输、数据访问、数据使用、数据销毁各阶段应用不同安全措施，配合京东智联云全流程数据安全保护体系，提供系统化的安全防护，并通过友好的操作界面和接口，方便用户使用与集成，满足不同行业用户对数据安全的个性化需求。

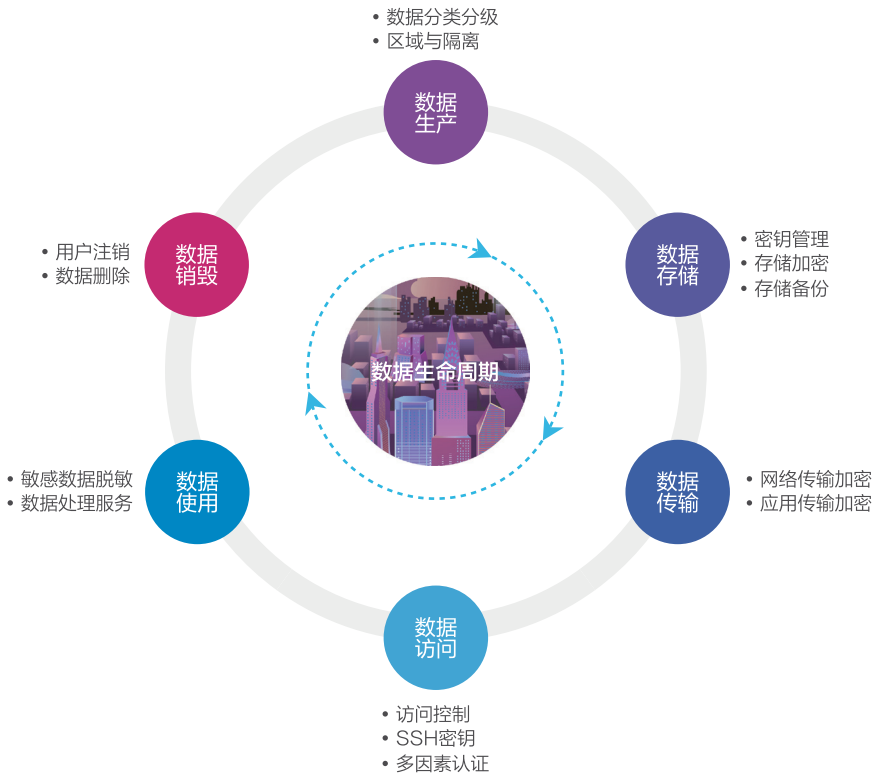

图 6 数据全生命周期安全保障

4.4.1 数据生产

数据生产是用户产生新的内容，或对已有内容的替换、更新或修改。针对这一阶段，京东智联云建议用户首先做好数据分类，并进行风险分析，再根据风险分析结果，明确防护数据的存储位置、存储服务和安全防护措施，在数据全生命周期的起始阶段就做好数据的区分与隔离。

· 数据分类分级

在使用京东智联云服务时，用户是其数据的控制者、拥有者，建议由用户自行对其数据资产进行分类分级管理。用户可依据数据安全需求，对数据进行分类分级化管理，识别敏感数据，对各类别级别的数据实施差异化的保护、细粒度的管控，有助于满足合规要求，防止敏感数据泄露。

建议每一个用户对其云端数据进行完整的风险评估。对于识别出的重要或敏感数据，用户可以按需要选择额外的数据保护措施。基于敏感数据发现的结果，京东智联云可以帮助用户进一步分析数据间的关系，输出数据分类和风险定级的信息，并推荐数据分类分级的架构方案。

· 区域与隔离

用户自主选择内容数据存储区域，可根据自己对地理位置的具体要求选择地点部署京东智联云服务。用户在区域中复制和备份自己业务数据，京东智联云未经用户授权，不会跨区域移动或复制用户的内容数据。

用户数据一般存储于数据库中，为保障账户数据安全，基于数据库存储对用户数据进行隔离存储，即与用户业务数据及京东智联云平台自身数据等不同类别的数据相隔离，并等同享受数据库存储数据的安全保障措施。

4.4.2 数据存储

数据存储是将数据提交到某种存储库中，通常在数据生产时发生。对于云端存储的敏感及重要数据，建议用户使用加密措施进行防护，降低数据泄露的风险。京东智联云通过安全策略及工具让用户拥有和控制自己的数据，确定内容的存储位置、保护动态和静态内容，并为用户管理对云服务和资源的访问权限。京东智联云为用户提供符合国家商用密码管理要求的加密服务，用户可轻松构建其安全应用。

· 密钥管理

京东智联云密钥管理服务KMS（Key Management Service）帮助用户管理及备份其加密密钥，提供云上密钥创建、禁用、轮换、删除等全生命周期管理。KMS 与云上多种产品集成，用户可以使用自己的 CMK 对云上 EBS 云硬盘、OSS 对象存储、RDS 关系型数据库进行加密，即可实现云端数据的加密存储。KMS 通过完善的技术方案，保障服务的高可用性，并且拥有完善的容灾与备份措施，以保障密钥不会因为不可抗力而丢失。

· 存储加密

云硬盘加密对存储在云硬盘上的数据进行加密，从而保障云硬盘中静态数据的安全性和数据在云主机实例和云硬盘间传输的安全性。

保护存储在对象存储服务（OSS：Object Storage Service）数据中心的磁盘上数据，用户可以对存储空间设置默认加密，从而对其中默认加密生效期间存储的对象进行服务器端加密。在使用服务器端加密时，OSS 将对象保存到其数据中心的磁盘上之前对其进行加密，并在下载对象时对其进行解密。

数据库 RDS 支持使用透明数据加密（TDE）来加密运行 Microsoft SQL Server 的数据库实例中存储的数据。TDE 会在数据写入存储前自动加密这些数据，并在从存储中读取时自动解密这些数据。数据库文件的加密在页级别执行，已加密数据库中的页在写入磁盘之前会进行加密，在读入内存时会进行解密。

· 存储备份

京东智联云的存储容灾服务为弹性云服务器、云硬盘和专属存储等服务提供容灾能力，通过存储复制、数据冗余和缓存加速等多项技术，为用户存储数据提供可跨区域复制功能并实时同步到指定区域，实现数据异地容灾，从容应对极端灾难并保证业务流畅，为重要数据加上多重保险。

数据备份服务拥有完善的数据备份机制，支持自动备份和手动备份，每个实例默认每天自动备份一次，也可以根据业务情况随时创建备份，备份文件以三副本的形式保存在京东智联云对象存储中，无需担心数据丢失。

4.4.3 数据传输

京东智联云对于数据的交换、转移和分享提供标准的传输加密协议，满足云平台以及系统间传输敏感数据的需求。

· 网络加密传输

针对用户业务混合云部署和全球化布局的场景，可以使用京东智联云提供的虚拟专用网络（VPN）、云专线服务，实现不同区域之间业务的互联互通和数据传输安全。

> VPN 连接利用公网架设专用网络，VPN 使用 IPSEC、IKE、预共享密钥方式对数据进行加密，基于公网提供安全可靠的通信隧道，实现外部用户内网访问、跨地域内网互通等。

> 专线服务 (Direct Connection) 提供高速、安全、稳定的网络接入服务。实现京东智联云网络与用户的 IDC、合作伙伴等网络环境进行内网通信、数据备份及跨机房容灾，为用户提供混合云解决方案。

· 应用加密传输

京东智联云支持 HTTPS 安全数据加密传输，并使用传输层安全性 (TLS) 协议，在云服务和用户之间传输数据时提供保护。TLS 提供严格的身份验证，消息隐私性和完整性强（允许检测消息篡改、拦截和伪造），具有良好的互操作性，算法灵活，易于部署和使用。

当用户通过互联网提供 Web 网站业务时，可以使用京东智联云联合全球知名证书服务商提供的证书管理服务。通过给 Web 网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。

4.4.4 数据访问

数据访问是指用户对云端数据的访问。建议用户对数据的访问和传输进行严格的管控及安全防护。为保证数据的合法访问，京东智联云提供身份鉴别、授权管理、权限鉴别三合一的用户业务访问控制。

· 访问控制

京东智联云提供了用户身份管理与访问控制服务（Identity and Access Management，IAM）。用户可以通过 IAM 服务创建、管理子用户账号，并控制这些子用户访问京东智联云资源的权限。

· SSH 密钥

对于用户登录使用 Linux 主机，SSH 服务可以对所有传输的数据进行加密，提供比传统 Telnet 服务更高的安全性。而基于密钥认证的 SSH 自动化登录，在保障用户安全性的同时，可以简化登录过程，降低运维成本。

· 多因素认证

MFA (Multi-Factor Authentication) 是一种简单有效的最佳安全实践，它能够在用户名和密码之外再额外增加一层安全保护，并且在京东智联云进行敏感操作时，进行身份验证防止误删。启用 MFA 后，用户登录京东智联云时，系统将要求输入用户名和密码，然后要求输入来自其 MFA 设备的 6 位动态验证码，即使他人盗取用户的密码，也无法登陆用户的账号，多因素的安全认证将最大限度地保障用户的账户安全。

4.4.5 数据使用

数据使用过程中，对其中的敏感数据进行数据脱敏、水印等处理可以确保数据合规使用，并规避信息泄露和法律法规遵从风险。

· 敏感数据脱敏

针对用户敏感数据，采用适当的脱敏算法进行处理，防止敏感数据被滥用和泄露，实现敏感隐私数据的可靠保护。

· 数据处理服务

用户上传文件到对象存储后，京东智联云提供丰富的数据处理服务，可以在云端实现图片的缩放、裁剪、水印、鉴黄、格式转化和样式管理，视频转码工作流等

丰富的数据处理功能，满足各网络场景下多终端设备的访问需求，同时提供数据安全性、透明性、可溯源性。

4.4.6 数据销毁

在用户提出请求和合同终止时，京东智联云会严格遵循数据销毁标准与用户之间的协议约定，执行用户注销和数据删除。

· 用户注销

京东智联云账户注销后，用户个人信息会在京东智联云系统中去除，使其保持不可被检索、访问的状态，或对其进行匿名化处理。根据相关法律规定，相关交易记录须在京东智联云后台保存一定时间。用户在操作之前，将自行备份京东智联云账户相关的所有信息和数据。

· 数据删除

当用户删除数据或离开京东智联云时，京东智联云会对指定的数据及其所有副本进行全面的清除，包括删除用户与数据之间的索引关系，并将内存、块存储等存储空间进行清零操作。在一定条件下，对退役的磁性存储设备进行消磁和物理销毁，确保其数据无法恢复。

04/5 安全运营保障

安全运营机制可以及时获知最新网络安全动态、安全情报，并在第一时间处理相关安全事件，保证平台的安全稳定及用户数据业务安全。安全运营团队依托安全产品服务和安全运营标准，为用户提供安全监测、安全预警、安全响应、安全运维全方位的安全保障。

· 安全监测

京东智联云构建了安全自动监测系统，监测范围覆盖内部、外部的关键服务组件，关键上下游服务组件等。联动分析各安全设备的告警信息、日志记录，结合机器学习技术和专家经验构建相应模型，检测已知、未知的数据安全威胁与风险。

监测对不同的服务组件设置了内存、磁盘、网卡等核心资源使用率等监控，设置严格的异常阈值线。及时告知运营团队通过错误统计结果，快速评估解决问题。监测的新增、删除、编辑具有明确的流程，监测明确监控等级、目标、监控接收人、异常处理预案，确保警报发生时的应急响应计划能第一时间进行。

· 安全预警

京东智联云构建了统一分析和预警云安全运营平台。通过对京东智联云安全各维度数据进行统一采集、处理和分析，使得管理人员能够实现全网的资产监控、事件分析与审计、风险评估和度量、预警和响应、定位并处置，并通过标准化的流程进行持续性的、实时的安全运营工作。

京东智联云构建了资产弱点监控系统，实现资产信息的关联分析及风险评估，漏洞发现、漏洞处理、漏洞披露等全流程的跟踪与管理，并结合入侵检查和威胁情报，通过态势感知产品，分析云内部网络和资产。确保云平台各服务产品和组件的漏洞得到及时的发现与修复，降低漏洞被恶意利用所带来的风险。

· 安全响应

在云平台及服务日常运行过程中，进行主动的风险管控，利用安全专家团队及云平台及服务自愈恢复能力，在紧急情况进行存储、应用等不同级别的数据与业务恢复。

安全运营团队会从事件发现之前，对入侵的可能：隐患、漏洞、风险、盲点做整改并推进，减少安全事件的发生。一旦安全事件发生，安全运营团队将快速发现、

分析定级并快速响应。事后评估事件的影响范围和危害程度，深入分析安全事件的根本原因，针对存在问题和隐患的系统，进行安全修复及复测。京东智联云配置了7*24 的安全事件响应专家团队，执行应急预案及恢复流程，安全漏洞通告并进行风险整改，帮助用户快速解决安全问题并降低对业务的影响。

· 安全运维

京东智联云安全团队为保障云平台的平稳运行，建立了一套严格的、细粒度的权限管理机制，要求运维管理人员始终坚持“与用户数据有关的操作需获得用户授权，不进行有损用户数据的操作”的基本原则。对于与用户数据安全直接相关的虚拟机迁移、数据搬迁、业务扩容关键运维操作，京东智联云制定了明确操作规范，规范化要求运维人员。

为保障用户数据安全、可靠，京东智联云开发运维平台与工具，使运维自动化、流程化降低人工干预。例如，利用堡垒机统一管理生产环境的所有运维账号，运维登录入口，使得所有的运维操作只能通过堡垒机进行。统一日志审计系统将运营管理团队的所有后台运维操作记录安全存储，内部审计团队定期对运维操作记录进一步审核。

05

结语

京东智联云一直以来以用户数据安全为核心，构建全链路安全产品与服务，化理念为实践，保障用户云上业务、网络和数据的安全，让攻击者进不去、数据看不到、拿不走。京东智联云通过针对安全开发成熟度模型进行深入解读，为用户提供安全编码、安全测试、安全部署等指南与规范，确保用户在安全可靠的架构设计之上完成应用开发和实践工作，最大程度保证从应用开发到上线运营的全生命周期安全。

面对数据及隐私保护的法律监管要求，京东智联云采取多种措施规范自身行为，组建数据安全合规团队，建立标准化的隐私协议、数据处理协议，严格实施云端个人数据保护措施和数据处理措施，规范第三方合作，积极推动业界关于数据安全或隐私保护的认证评估。

未来，京东智联云将继续加强在云安全方面的不断研究与探索，致力于为用户与合作伙伴提供安全、稳定、高可用的基础设施，专业、全方位的安全产品，完善、可靠的安全服务。帮助用户保护其系统及数据的安全，提升用户数据的可用性、保密性和完整性。

京东智联云坚持以保护用户云端数据安全为己任，利用在用户数据保护方面的优秀实践，通过智能化的安全大数据分析和业务层面的安全态势分析，为用户提供优质的数据安全解决方案。京东智联云希望通过与政府和企业携手并肩，助力其业务安全上云，实现“互联网+”的转型，并积极联合全球安全伙伴打造一个开放、协作、共赢的云端安全生态圈。

06

参考文献

参考文献

[1]《京东智联云安全白皮书》，2018 年；

[2]《京东集团数据安全管理规范》， 2018 年；

[3]《京东集团数据分类分级标准》， 2019 年；

[4] GB/T 31167-2014《信息安全技术 云计算服务安全指南》；

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

[6] GB/T 35279-2017《信息安全技术 云计算安全参考架构》；

[7] GB/T 22239.2《信息安全技术 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；

[8] GB/T 35273《信息安全技术 个人信息安全规范》；

[9] YD/T XXXXX-XXXX《云服务用户数据保护能力评估方法第 1 部分：公有云》（送审稿）；

[10] YD/T XXXXX-XXXX《云服务用户数据保护能力参考框架》（送审稿）；

[11]《数据安全治理白皮书》，数据安全治理委员会，2018 年；

[12]《大数据安全白皮书》，中国信息通信研究院，2018 年。

京东智联云

关注社交平台：

京东智联云微信　京东智联云微博

如欲了解更多信息：

欢迎登陆：www.jdcloud.com

咨询热线：400-615-1212