亚马逊云科技 | Deloitte.

打造安全合规的数字化底座

2021 企业中国发展建议白皮书

2021.9.26

本白皮书由德勤企业咨询（上海）有限公司（“德勤企业咨询”）和 Amazon Web Services, Inc. 或其关联方（“亚马逊云科技”）分别撰写，双方就各自撰写的内容分别、独立享有相关知识产权。其中德勤企业咨询负责第一章、第二章和第三章 a 部分，单独享有该部分的知识产权；亚马逊云科技负责第三章 b 部分（即“技术平台搭建建议”部分），单独享有该部分的知识产权。

关于德勤部分的声明

关于德勤企业咨询部分的声明：本白皮书中所含内容乃一般性信息，任何德勤有限公司、其全球成员所网络或它们的关联机构并不因此构成提供任何专业建议或服务。在作出任何可能影响您的财务或业务的决策或采取任何相关行动前，您应咨询合资格的专业顾问。 我们并未对本白皮书所含信息的准确性或完整性作出任何（明示或暗示）陈述、保证或承诺。任何德勤有限公司、其成员所、关联机构、员工或代理方均不对任何方因使用本通讯而直接或间接导致的任何损失或损害承担责任。德勤有限公司及其每一家成员所和它们的关联机构均为具有独立法律地位的法律实体，相互之间不因第三方而承担任何责任或约束对方。德勤有限公司及其每一家成员所和它们的关联机构仅对自身行为及遗漏承担责任，而对相互的行为及遗漏不承担任何法律责任。德勤有限公司并不向客户提供服务。请参阅 www.deloitte.com/cn/about 了解更多信息。

关于亚马逊云科技部分的声明

关于亚马逊云科技部分的声明：本部分内容陈述了亚马逊云科技在封面页所示日期的有关服务产品及实践，该等信息可能变化且我们不会另行通知。客户对于本部分的信息以及亚马逊云科技的产品或服务应自己做出独立的判断，该等内容都是“依现状”提供，不包含任何明示或者暗示的保证。本部分内容并没有创设来自亚马逊云科技、北京光环新网科技股份有限公司（“光环新网”）、宁夏西云数据科技有限公司（“西云数据”）、或其各自的关联方、提供方或许可方的任何保证、陈述、合同性承诺、条件或者担保。亚马逊云科技、光环新网、西云数据对其各自的客户的义务和责任均由适用的客户协议管辖。本部分内容不是亚马逊云科技、光环新网、西云数据和其各自的客户之间任何协议的组成部分，也不构成对任何协议的修改。

前言

数字化经济在云计算、人工智能、机器学习、区块链、物联网等新兴技术的推动下，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。而数据是这一切的关键生产要素和核心驱动力。数据资产作为人类最新最有活力的资产形式将成为企业最核心竞争力的来源。同时，数据的流动性、共享性为如何保护这核心资产，如何在统一的规则和共识下进行数据确权、数据估值以及最终的数据贸易带来了巨大的挑战。

“合规是红线，安全是底限”，中国在不断通过各种立法来规范数字化经济的发展，确保对于数据的主权、维护核心数据资产的安全、保护个人隐私、促进数据必要的合法流动和共享、以及减少广义供应链风险。《网络安全法》，《数据安全法》，《个人信息保护法》都是这方面典型的代表。

虽然受疫情的影响，全球化的进程似乎受到了阻碍放慢了步伐。但全球化是数字化经济的必然趋势，不少著名跨国公司依然在加大对于中国市场的投入，这是一个更加理性和有规划的过程。对于跨国公司进入或拓展中国市场来说应该充分理解中国政府出于对国家安全、社会稳定和公众利益的考虑而构建的法律体系（网安法 + 数安法 + 个保法），积极拥抱监管要求，主动合规。

本白皮书旨在为跨国企业数据安全本地化数据安全，解读相应的法律法规，分析面临的问题和挑战，并提出应对策略以建立相应管理体系和构建数据安全技术平台，从而建立有效的数据安全合规保障体系。

德勤中国风险咨询全国主管合伙人

吴苹

亚马逊云科技大中华区产品部总经理

顾凡

Contents

目录

一 . 国内数据与安全合规趋势综述

a. 国家对重要数据及系统管控的要求 6

数据安全法中有关数据本地化的要求 6

个人信息保护法中有关数据本地化的要求 7

等保管理规范（草案）对安全运维本地化的要求 7

二 . 跨国公司新合规形势下的挑战

a. 重点行业对数据本地化的特殊要求 8

汽车行业 8

金融行业 9

医疗健康行业 9

高科技行业 10

b. 跨国公司应对难点分析 12

个人信息与重要数据跨境 12

数据出口管制 12

公司及法人责任 13

安全及合规人力资源 13

三 . 跨国公司新合规形势下的应对建议

a. 管理体系建设建议 14

组织架构 14

流程制度 14

意识培训 15

b. 技术平台搭建建议 16

安全责任共担模型 17

云的安全 18

亚马逊云科技云上的数据安全 20

数据分析中的安全 24

机器学习的安全 25

第三方解决方案 25

国内数据与安全合规趋势综述

a. 国家对重要数据及系统管控的要求

数据作为 21 世纪的基础性战略资源，有着新“石油”的美誉，对于企业乃至国家具有举足轻重的意义。因此，许多国家或地区相继出台一系列法律法规，旨在规范本国或本区域内数据的跨境流动。

我国数字经济走在世界前列，其发展过程中产生的海量数据亦受到了国家的重视。目前，我国数据安全相关的法律体系正快速构建成型，已发布了《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》和《关键信息基础设施安全保护条例》。通过对该系列法律法规的解读，我们不难看出，目前我国数据安全管控的基本原则是要求重点行业（如汽车业、金融业、医疗健康业）的重要数据和达到一定规模的个人信息进行“本地化存储”，同时将“数据出境安全评估”作为向境外提供数据的基本条件。

数据安全法中有关数据本地化的要求

作为数据安全领域的基础性法律，《中华人民共和国数据安全法》（以下称《数安法》）已于 2021 年 6 月 10 日正式通过，将于 2021 年 9 月 1 日正式实行。《数安法》距其草案第一次提请全国人大常委会审议（2020 年 6 月 28 日）到正式通过不到一年，立法急迫性可见一斑。

《数安法》第三十一条明确规定：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中国人民共和国境内收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。《中华人民共和国网络安全法》（以下称《网安法》）与之相关的规定为第三十七条，即“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。”由此可见两部法律都将数据本地化聚焦在了“关键信息基础设施的运营者”这一“关键少数”。但同时角色为网络运营者的企业，一旦处理或持有重要数据，仍然需要关注后续监管部门对重要数据的定义和本地化的相关要求。因此相关企业必须提前准备，以防止一旦被认定为“关键信息基础设施的运营者”或者处理了重要数据，如应对不当将会出现的重大合规性风险，甚至被迫中断业务的可能。

“关键信息基础设施的运营者”中有两个关键词。首先是“关键信息基础设施”，《网安法》中第一次正式明确了“关键信息基础设施”的基本概念，即“一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施”。但是由于该定义具有一定的模糊性，因此《网安法》举例了可能会涉及“关键信息基础设施”的重点行业或领域，如公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等；其次是“运营者”，根据《网安法》中的定义，“运营者”即为指网络的所有者、管理者和网络服务提供者，鉴于当前大多的企业无论是内部日常运营管理或是为外部客户提供服务都对网络具有极高的依赖程度，因此大部分企业都属于“运营者”的范畴。

© 2021. For information, contact Deloitte China.

“关键信息基础设施的运营者”在境内收集和产生的重要数据和个人信息本地存储是数据本地化的核心要求。（本节将重点介绍“重要数据”部分，关于个人信息的相关详细阐述可参见下一小节。）无论是《网安法》还是《数安法》，均未对“重要数据”进行明确的定义或举例。但参考 2017 年 5 月全国信息安全标准化技术委员会发布的《信息安全技术 数据出境安全评估指南（草案）》（以下称“评估指南”）所附“重要数据识别指南”中对重要数据的定义，重要数据是指“我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据），一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能对国家安全、国家经济和金融安全、社会公共利益、个人合法权益等造成相关严重后果的数据”。与此同时，“评估指南”附录 A 列举了包括能源、化工制造业、军工业在内的 27 个行业（领域）中的重要数据范围与对应主管部门。但是根据附录最后的兜底条款，重要数据的范围仍然可能根据行业发展出现变化。因此相关行业的企业对于“重要数据”的评估除参考“评估指南”中所列示的内容以外，还需持续监控本行业相关法律法规的发展，及时识别本行业所涉及的重要数据，从而更好地管理企业日常数据活动。这里需要特别提醒的是，即使企业自身未被认定为“关键信息基础设施的运营者”，但是如果向“关键信息基础设施的运营者”提供网络产品和服务，那么根据 2020 年 8 月出台的《网络安全审查办法》，“关键信息基础设施的运营者”会要求企业向其提供的网络产品或服务应当满足“关键信息基础设施的运营者”相关的合规要求。

个人信息保护法中有关数据本地化的要求

如今，企业对于用户个人信息的收集变得越来越普遍，通过对个人信息的加工分析，企业可为用户提供更为优质的产品和服务。但与此同时，由于对于个人信息的不当使用造成个人财产、精神损失的情况屡见不鲜。我国近年来正在加速推进个人信息保护的法律体系建设。2021 年 8 月 20 日《中华人民共和国个人信息保护法》（以下称《个保法》）人大常委会审议通过并正式发布，并在 2021 年 11 月 1 日正式生效。《个保法》详细规定了个人信息处理者在进行“个人信息处理活动”时需要遵循的合规要求。

《个保法》将“个人信息”定义为“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”，将“处理活动”定义为“个人信息的收集、存储、使用、加工、传输、提供、公开等”。《个保法》第四十条提到：关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的， 应当通过国家网信部门组织的安全评估。由此可见，这两类角色在境内收集和产生的个人信息被《个保法》纳入本地化存储的要求范围中，即 “关键信息基础设施运营者”和“处理个人信息达到国家网信部门规定数量的个人信息处理者”，但是对于“规定数量”在《个保法》中目前并没有量化指标，尚需相关部门后期进一步明确。

等保管理规范（草案）对安全运维本地化的要求

《中华人民共和国网络安全法》（以下简称《网安法》）于 2017 年 6 月 1 日开始实施，首次将网络安全等级保护制度上升为法律要求。次年，公安部于 6 月 27 日发布了《网络安全等级保护条例（征求意见稿）》（以下简称“条例”），该条例规定了等级保护三级及以上系统不得境外远程技术维护，当因业务需要而实施境外远程技术维护时，需进行网络安全评估以及采取风险管控措施。实施技术维护应当记录并留存技术维护日志，并在公安机关检查时如实提供。根据经验，对于收集、存储大量个人信息特别是敏感个人信息的系统，或非常重要的系统，往往会被认定为等保三级系统，因此需要确保满足安全运维本地化的相关要求。因此，企业需谨慎对待其所拥有系统的境外运维。

© 2021. For information, contact Deloitte China.

跨国公司新合规形势下的挑战

a. 重点行业对数据本地化的特殊要求

汽车行业

汽车行业特别是新能源汽车是中国目前实现刺激经济发展的重要行业，发展新能源汽车成为了大势所趋，各个传统车企，甚至是互联网公司都纷纷布局造车，掀起了新一轮的造车潮流。而与此同时汽车行业以及车联网等技术的发展也为数据安全保护带来了影响和挑战。汽车行业的运营者如汽车制造商、经销商、维修机构、网约车企业、保险公司等往往都会涉及大量的个人信息和重要数据。由于汽车行业中数据收集的方式存在行业特性，使得对相关个人信息和重要数据的安全管理措施与其他行业有所不同，应该针对具体数据收集处理的情况进行客制化。此外，国家正在加紧汽车领域的各项安全管理规定的健全，已陆续发布多项行业管理规定，办法和标准草案。

- 2021 年 4 月 28 日全国信息安全标准化技术委员会发布关于征求《信息安全技术网联汽车采集数据的安全要求》标准草案意见的通知，被视为我国首个网联汽车采集数据国家标准，对数据传输，数据存储，数据跨境等多种场景下的数据安全管理提供了指引。在《个人信息安全规范》中，当个人信息主体提出删除信息请求，应在 30 天内或法律法规规定的期限内作出答复及合理解释，并告知纠纷解决途径，而在《信息安全技术网联汽车采集数据的安全要求》中要求网联汽车采集的车辆位置、轨迹相关数据在车内存储设备、远程信息服务平台（TSP）中保存时间均不得超过 7 天，较前者，对数据存储的管理更为严苛。

- 2021 年 7 月 5 日，国家互联网信息办公室公布了《汽车数据安全管理若干规定（试行）》，又一部对汽车数据安全的管理办法。该规定明确了个人信息，重要数据，汽车数据处理者等定义，提出了汽车领域的个人信息和重要数据四项管理原则，1. 车内处理原则，要求除非确有必要不向车外提供；2. 默认不收集原则；3. 精度范围适用原则；4. 脱敏处理原则。另外对处理重要数据的汽车数据处理者提出了更严格的管控要求，即提出了应当在每年十二月十五日前进行自主数据安全管理情况申报，对于该适用范围内的运营者而言，数据安全管理报告将成为避无可避的常规工作。

- 多个法律法规，如《个人信息保护法》、《信息安全技术网联汽车采集数据的安全要求》、《汽车数据安全管理若干规定（试行）》等都多次提到并强调对于数据出境的管理，其中《个人信息保护法》明确指出个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的身份、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式等事项，并取得个人的单独同意；《汽车数据安全管理若干规定（试行）》指出个人信息或者重要数据应当依法在境内存储，确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。

在技术上，汽车行业对使用云的汽车企业来说，需要注意数据保存的位置，时限，保存方法，数据访问控制等方面有具体的要求。亚马逊云科技的账号管理服务 IAM，数据存储服务 S3，支持各类应用的数据库如 Amazon RDS、Amazon DynomaDB、Amazon Aurora、数据仓库 Redshift 等有有关于安全方面的加强和特性帮助客户遵守各类合规要求。

© 2021. For information, contact Deloitte China.

金融行业

金融行业，主要由银行业、保险业、证券业、信托业等细分行业组成，其所涉及的数据，可以从各个角度分析、反映国民经济的整体和个体状况，是国民经济发展的晴雨表，因此金融行业的数据具有极大的价值。

目前金融行业主要监管部门为中国人民银行、银保监会、证监会，其针对数据本地化提出一系列的要求，除了目前境内已颁布实施的《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《个人信息安全规范》等通用的法律法规标准以外，下面是对于金融行业对于数据本地化要求的摘录：

《中华人民共和国证券法》第一百七十七条 境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料。

《反洗钱法》第二十八条 国务院反洗钱行政主管部门根据国务院授权，代表中国政府与外国政府和有关国际组织开展反洗钱合作，依法与境外反洗钱机构交换与反洗钱有关的信息和资料。

《商业银行信息科技风险管理指引》“第二章 信息科技治理（十一）确保本法人机构涉及客户信息、账务信息以及产品信息等的核心系统在中国境内独立运行，并保持最高的管理权限，符合银监会监管和实施现场检查的要求，防范跨境风险。”。

《个人金融信息保护技术规范》
7.1.3 安全准则 - 使用在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，应在境内存储、处理和分析。因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，具体要求如下：

- 应符合国家法律法规及行业主管部门有关规定；
- 应获得个人金融信息主体明示同意；
- 应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；
- 应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。

基于以上行业监管要求和标准，在落地执行过程中，企业面临最关键的挑战在于投入适当的资源，满足合规和业务双需求，例如在反洗钱、信用风险、客户服务等领域，相关数据在中国境内产生、收集，但出于集团统一管理需要、客户全球化服务需要或系统历史原因部署在境外等原因，数据存在跨境场景。这就意味着从中长期来看，其系统本地化 / 数据本地化工作势在必行，也将产生一定的投入，但也会对业务流程或策略产生一定的影响，目前众多外资金融机构也逐步意识到了这一问题，在向管理部门申请业务牌照的同时，也在提前规划向中国境内规划部署本地化系统战略。

技术上来说，金融行业上云对于云的安全合规要求更高，除了保障数据流动过程中的合规，在敏感数据和隐私数据的发现、处理、监控方面也有很多要求，当前金融行业的很多新型业务，都在结合人工智能和大数据分析技术的应用。亚马逊云客户在这方面有得天独厚的能力，大量数据的交流和分析等活动对于数据的安全有更高的要求。亚马逊云科技的人工智能平台 SageMaker，本身就建立在严格的权限管控的基础上，并从基础架构到应用各个不同层面提供安全机制确保机器学习的整个流程中的数据安全。

医疗健康行业

医疗健康行业是关系到国计民生的重要行业，其产生或涉及到的数据往往数量及为庞大，且范围十分广泛，如健康医疗产业数据、个人健康数据、临床试验数据等。医疗健康相关的数据一旦发生泄露或滥用，对于人们的人身、财产安全甚至国家安全都会造成重大影响。因此，与其他行业相比，医疗健康行业对本行业数据的本地化要求也更为严苛。由于医疗健康行业受监管数据的定义及其对应的本地化要求在我国的不同法规、规章以及标准中都有被提及，因此下文将对医疗健康行业受监管数据的定义及本地化要求进行系统性梳理。

© 2021. For information, contact Deloitte China.

- 2014 年 5 月，国家卫生计生委员会（现为“国家卫生健康委员会”）发布的《人口健康信息管理办法（试行）》中提出了“人口健康信息”的概念。该办法所称人口健康信息，是指依据国家法律法规和工作职责，各级各类医疗卫生计生服务机构在服务和管理过程中产生的人口基本信息、医疗卫生服务信息等人口健康信息。该办法明确规定了“不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器”。
- 医疗健康行业中存在着大量被归为“重要数据”的数据。在 2017 年 8 月全国信息安全标准化技术委员会发布的《信息安全技术 数据出境安全评估指南（草案）》中所附的“重要数据识别指南”中明确举出了人口健康行业涉及的八大“重要数据”种类，如在药品和避孕药具不良反应报告和监测过程中获取的个人隐私、患者和报告者信息、生命登记信息等。根据《网安法》和《数安法》相关规定（前一节已阐述），这些“重要数据”必须满足本地化存储的要求。
- 2018 年 8 月，国家卫生健康委员会发布的《国家健康医疗大数据标准、安全和服务管理办法（试行）》提出了“健康医疗大数据”的概念，即“在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据”。该办法亦明确规定了此类数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。

2019 年 7 月起正式施行的《中华人民共和国人类遗传资源管理条例》中又引入了“人类遗传资源信息”这一概念，人类遗传信息指利用人类遗传资源材料产生的数据等信息资料。而该条例也明确禁止了外国组织、个人及其设立或者实际控制的机构向境外提供我国人类遗传资源的行为。

从技术角度看，在医疗监控行业，涉及到基因，医疗健康等不同类型的数据，医疗健康行业对数据除了对数据本地化的要求之外，还对数据在本地的建立，保存和使用全生命周期要做到可跟踪和审计，对于使用云平台的运营者，亚马逊云的安全合规服务和管理服务如 Amazon Cloudtraill、Amazon Config、Amazon GuardDuty、Amazon IAM 等对数据的全生命周期做到全面监控和控制。

高科技行业

近年来互联网及高科技行业飞速发展，在新生企业中，互联网及高新科技企业占比重大。在华的跨国互联网及高科技公司在原本的业务运营以及数据管理模式下，由于业务需求需要将数据跨境传输，现在也因此不可避免地面临着数据本地化的挑战。

- **高科技行业数据安全本地化法规要求**

互联网及高科技行业以技术为驱动，除个人信息之外，根据《信息安全技术 数据出境安全评估指南（征求意见稿）》中的“重要数据识别指南”，该行业还涉及大量“重要数据”，例如产品技术方案、设计图纸、源代码、研发数据、工艺参数、通信类信息以及收集的地理信息等，一旦泄露、丢失或被滥用，将对个人、社会经济乃至国家安全造成危害。因此根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》和《信息安全技术 数据出境安全评估指南（征求意见稿）》相关规定，互联网及高科技行业所涉及的这些“重要数据”必须满足本地化存储的要求。

- **电信和互联网行业数据安全监管趋势**

在物联网、人工智能等高新科技快速发展的同时，对于行业内企业所涉及的“重要数据”和个人信息及隐私，其数据安全风险场景也随之变得更加复杂、多样，因此，监管机构对于互联网及高科技行业的数据安全要求日益严苛，对于数据保护的重点领域提出了明确要求。工信部于 2020 年印发了《电信和互联网行业数据安全标准体系建设指南》，要求企业“结合新一代信息通信技术发展情况，主要在 5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等重点领域进行布局，并结合行业发展情况，逐步覆盖其他重点领域”。此外，顺应互联网及高科技行业发展趋势，行业网络数据安全保护的对象也逐渐发生变化。自 2019 年开始，根据《电信和互联网行业提升网络数据安全保护能力专项行动方案》，5G 网络基础设施已被纳入检查和保护的对象，确保企业有能力提供安全的服务，并且保证用户的个人信息和隐私。尽管《中华人民共和国网络安全法》举例了可能会涉及“关键信息基础设施”的重点行业或领域，并未对“关键信息基础设施”的定义提供更进一步的明确指导，但根据互联网及高科技行业在数据保护方面关注的重点领域，我们不难

© 2021. For information, contact Deloitte China.

看出，这些重点领域的信息基础设施运营者将是监管合规的重点关注对象，因此相关企业必须满足监管合规要求，将数据本地化存储。

- **互联网及高科技行业跨国公司在华数据本地化动向**

为了响应《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》、《信息安全技术数据出境安全评估指南（征求意见稿）》等法律法规的要求，同时满足企业自身业务需求，众多在华开展业务的跨国高科技企业已陆续开始落实数据本地化要求，在中国建立数据中心，掀起了“数据本地化”浪潮。苹果公司已联合云上贵州，在中国境内建立了数据中心，并已于今年 5 月 25 日正式投入运行；微软在建立了位于北京和上海的两个数据中心之后，又将在中国建立第三个数据中心，以满足日益增长的业务需求。除此之外，还有众多跨国高科技公司选择与数据中心位于中国境内的云服务提供商合作，将企业的数据中心搬迁至位于中国境内的云上，以此实现“数据本地化”。

因此，“数据本地化”已经成为跨国互联网以及高科技公司在华开展业务所面临的挑战。除此之外，在落实数据本地化的同时，数据安全管理依然是企业重点关注的任务之一。依照《电信和互联网行业数据安全标准体系建设指南》，除了建立数据安全框架以及数据分类分级标准外，企业还应制定关键技术标准，在数据生命周期各阶段（包括数据采集、传输、存储、处理、交换以及销毁），对数据清洗对比、数据传输完整性保护、数据加密传输、数据安全审计、数据防泄漏、数据脱敏、匿名化 / 去标识化、应用接口安全、数据销毁等各项操作的技术要求进行明确和规范。

企业在迁移业务系统到境内实现本地化的过程中，由于无法依赖原有企业中心化的安全运维解决方案，因此也需要同时考虑安全相关解决方案的本地化配套落实并满足境内的相关安全合规要求，安全运维落地的重点包括：

- **关注法律法规，确保本地化运行合规** – 所有的业务运营都应建立在合规的基础上，因此企业需要密切关注国内及行业监管动向，识别并落实本地的相关法律法规要求；此外，企业应按照《中华人民共和国网络安全法》的要求对位于中国境内的系统进行定级，并按照等级要求对系统提供相应的保护；
- **加强数据安全保护** – 近年来，数据泄露造成的信息安全事件频发，监管力度日益加强，随着《中华人民共和国数据安全法》的发布，保障数据安全对企业本地化运营至关重要。企业需要在数据迁移过程中以及完成本地化部署后的日常运维工作中持续关注数据安全，包括数据资产盘点、数据传输和存储加密、数据脱敏、数据备份、日志和审计等，以确保企业数据的安全性、完整性和可用性；
- **保障本地化系统的安全运行** - 由于《中华人民共和国网络安全法》以及网络安全等级保护制度的要求，企业应履行其网络安全保护义务，在系统落地的同时，通过技术措施与管理流程相结合的方式，提升信息安全能力，为系统自身以及其所在的网络环境提供有效的安全保护，抵御外部攻击；
- **提升企业网络预警能力，实现风险监测、事件响应，和威胁防御** – 在本地化运行模式下，企业需要建立安全运营中心，通过集中管理的方式，对系统和网络运行情况进行 7x24 监控，及时发现潜在安全风险或异常并快速响应；同时，应将各类日志和事件数据进行归集、关联和分析，以识别信息安全事件或潜在的安全问题；网络威胁是企业一直面临的安全挑战，在新冠疫情的背景下，大量企业启动线上远程办公模式，对信息基础设施的依赖程度剧增，直接扩大了网络攻击面，勒索软件、数据泄露等网络威胁泛起，为了防范日趋严峻的网络威胁，企业应建立平台收集威胁情报，并利用大数据分析、机器学习等技术对网络威胁的发展趋势进行预测，从而更加有效地对威胁进行防御。

© 2021. For information, contact Deloitte China.

b. 跨国公司应对难点分析

个人信息与重要数据跨境

在华跨国企业因为业务需要不可避免会涉及数据跨境活动，因此需要寻求数据跨境流动与合规之间的平衡。

根据 2017 年 5 月全国信息安全标准化技术委员会发布的《信息安全技术 数据出境安全评估指南（草案）》（以下简称“《评估指南》”），“数据出境”是指网络运营者通过网络等方式，将其在中华人民共和国境内运营中收集和产生的个人信息和重要数据，通过直接提供或开展业务、提供服务、产品等方式提供给境外的机构、组织或个人的一次性活动或连续性活动。数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（公开信息、网页访问除外）也属于数据出境的一种。这一点值得引起大部分跨国企业的重视，因为在跨国企业的日常运营中，常常采用由境外 IT 团队统一负责对分布在各个国家或地区的应用系统或数据库进行维护与调用，按照前述定义，这一行为也被认定为数据出境。

如前一章“本地合规化趋势”中所述，《数安法》和《个保法》中都明确了对于个人信息和重要数据的本地化要求。但对于确需向境外提供的数据，则应当通过国家网信部门组织的安全评估。目前国家网信部门并没有发布明确的安全评估流程，但是国家推荐性指南《评估指南》可以作为目前企业数据跨境合规风险管理的指引。《评估指南》详细描述了数据出境安全评估流程、评估要点、评估方法等内容。具体来说，数据跨境评估可以分为两部分，第一部分是对于出境目的的合法性、正当性、必要性评估；第二部分是针对出境安全风险是否可控进行评估，该部分又需要综合考虑出境数据的属性和数据出境发生安全事件的可能性。当数据出境安全风险评估的最终结果为极高或高时，个人信息和重要数据就将被禁止出境。因此，对于跨国企业，目前需考虑对企业自身数据出境情况进行系统性梳理，建立完善的数据出境安全评估管理机制，以应对势在必行的数据出境安全评估要求。

数据出口管制

根据 2020 年 12 月 1 日正式生效的《中华人民共和国出口管制法》（以下称“出口管制法”），我国目前对两用物项、军品、核以及其他与维护国家安全和利益、履行防扩散等国际义务相关的货物、技术、服务等物项实行统一的出口管制制度，通过制定管制清单、名录或者目录、实施出口许可等方式进行管理。其中，技术出口根据《中国禁止出口限制出口技术目录》（以下称“技术目录”）分为自由、限制和禁止三大类：禁止类不得出口，自由类技术实行事后合同登记备案制，限制类技术实行许可管理。相关企业如果需要将限制类技术转移出口至海外必须到省级商务主管部门申请技术出口许可，获得批准后方可对外进行实质性谈判或签订技术出口合同。该“技术目录”会根据我国科技、经济发展由商务部和科技部不断更新，例如在 2020 年 8 月更新的最新一版“技术目录”中，在限制出口类技术中新增了 23 项限制出口的技术条目包括“基于数据分析的个性化信息推送服务技术”、“人工智能交互界面技术”、“漏洞发现和挖掘技术”、“网络攻击追踪溯源技术”等与数据分析、网络安全相关的最新前沿技术。

即将生效的《数安法》也将管制物项的数据纳入了出口管制对象，明确提出“国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制”。这也就意味着企业待出境的数据一旦被认定为出口管制清单物项的数据，就也需要和“限制类出口技术”一样获得国家出口管制管理部门许可后才能进行数据出境。

因此，在华企业在涉及技术转移时应当及时关注“技术目录”的更新，确保存储管制类技术的信息系统位于中国境内，避免发生转移禁止出境类技术或在未获得许可下直接转移限制出口类技术的情况，特别是通过系统直接传输出境或境外远程访问境内系统的方式。

© 2021. For information, contact Deloitte China.

公司及法人责任

《网安法》、《数安法》以及《个保法》均明确了违反数据出境相关条款的法律责任。根据《网安法》第六十六条，关键信息基础设施的运营者违反相关规定在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。根据《数安法》第四十六条，关键信息基础设施的运营者违反数据出境相关规则时，可由有关主管部门责令改正，给予警告，并处十万元以上一百万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。根据《个保法》，由履行个人信息保护职责的部门责令改正，没收违法所得，给予警告；拒不改正的，并处一百万元以下罚款；情节严重的，由履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。

同时，《网安法》、《数安法》以及《个保法》《关键信息基础设施安全保护条例》也均对违反数据出境相关条款的机构的责任人的法律责任做出了相应的规定。根据《网安法》，直接负责的主管人员和其他直接责任人员可被处一万元以上十万元以下罚款；根据《数安法》，直接负责的主管人员和其他直接责任人员可被处一万元以上十万元以下罚款；情节严重的，直接负责的主管人员和其他直接责任人员可被处十万元以上一百万元以下罚款。根据《个保法》，直接负责的主管人员和其他直接责任人员可被处一万元以上十万元以下罚款；情节严重的，直接负责的主管人员和其他直接责任人员可被处十万元以上一百万元以下罚款。根据《关键信息基础设施安全保护条例》第四十一条 运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额 1 倍以上 10 倍以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

安全及合规人力资源

根据米高蒲志最新发布的《网络安全人才发展报告》，中国政府 2019 年在网络安全方面投入 79 亿美元，位居世界第二。但是，根据 BOSS 直聘研究院《2021 网络安全人才趋势报告》统计显示，目前中国网络安全专业人才的缺口在 50 万人以上，每年网络安全相关专业的高校毕业生仅两万多人，且仅有少部分毕业生进入了网络安全领域并从事相关工作。因此，中国网络安全人员储备极度短缺也是跨国企业在境内经营面临的众多挑战之一。

© 2021. For information, contact Deloitte China.

跨国公司新合规形势下的应对建议

a. 管理体系建设建议

组织架构

建议企业可根据《网络安全法》的要求网络运营者应确定网络安全负责人，落实网络安全保护责任，设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查。《个保法》中规定了处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。另外《数据安全法》也要求重要数据的处理者应当明确数据安全负责人和管理机构。因此建议企业在岗位设置上，一是要明确网络安全负责人和数据安全负责人，并考虑到需要与监管机构进行沟通，建议尽量安排中文母语人士担任；二在条件许可的情况下，设立包括风控、审计在内的多道防线，并将安全合规相关的事宜建立直接的汇报渠道，使得高级管理层可以直接获取安全合规方面的最新状态。

流程制度

大部分的跨国企业虽然通常都已经有全球统一的信息安全制度，但是大部分是基于国际通用的信息安全体系标准比如ISO27001 或者 NIST800 等标准，在这些大而全的安全管理体系里面，仍然有下列领域需要考虑满足中国本地的监管和合规的特殊要求，比如：

1. **个人信息保护方面：**《网安法》和《个保法》对个人信息保护提出明确要求，一是要收集、使用个人信息，应当遵循合法、正当、必要的原则，保障个人信息主体的权利，二是要建立健全用户信息保护制度。

2. **风险评估方面：**关键信息基础设施的运营者应当对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送主管部门。

3. **互联网安全及内容监督检查方面：**明确定义办理联网单位备案流程，并报送接入单位和用户基本信息及其变更情况；明确定义按照法律规定的为公安机关依法维护国家安全、防范调查恐怖活动、侦查犯罪提供技术支持和协助的管理流程；明确定义履行法律、行政法规规定的网络安全等级保护等管理流程。

4. **漏洞和脆弱性管理方面：**需要建立制度流程覆盖下列方面，一、网络运营者在发现其产品或服务存在安全漏洞时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。二、应定期对进行风险评估和安全检查，加强安全入侵检测监控，及时发现并处置安全事件。三、建立有效可靠的安全情报获取渠道，获取与信息系统运营相关的外部安全预警信息，并汇总、整理企业内部安全信息，形成有效的安全态势情报，进一步发现和预防潜在风险。

5. **备份与恢复管理：**企业应按照有关法

© 2021. For information, contact Deloitte China.

律法规要求保存交易记录，采取必要的程序和技术，确保存档数据的完整性，满足安全保存和可恢复要求。一方面需要确定数据的全面性，即保留的数据应至少包括业务交易数据、系统操作记录，以及系统运行记录。另一方面，需要确切遵照各自所属行业的具体要求，如金融行业明确要求备份所保存的物理位置、不同等保级别的系统所应遵循的备份要求等。

6. **应急预案与事件管理：**企业应根据自身业务的性质、规模和复杂程度制定适当的业务连续性规划，确保在出现无法预见的业务中断时，系统仍能持续运行并提供服务；定期对规划进行更新和演练，以保证其有效性。应急响应预案除应考虑信息系统发生故障时的预案情况，同时应该考虑当发生重大突发事件时预案场景。当发生或者可能发生个人信息泄露、毁损、丢失的情况时，除采取补救措施外，按照规定及时告知用户并向有关主管部门报告。根据《网络安全法》的要求，需要留存相关的网络日志不少于六个月。《公安机关互联网安全监督检查规定》也要求应采取记录并留存用户注册信息和上网日志信息的技术措施。

7. **数据安全义务方面：**《网络安全法》要求企业采取数据分类、重要数据备份和加密等措施。因此企业应当制定全面科学有效的数据管理制度，包括但不限于组织管理、部门职责、协调机制、安全管控、系统保障、监督检查和数据质量控制等方面。考虑到目前各个行业的重要数据定义并未正式发布，因此建议未来根据监管要求和实际需要，持续评价更新数据安全管理制度。

8. **数据出境管理：**根据目前的法律要求，在中国大陆境内运营中收集和产生的（达到一定量的）个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。因此企业需要考虑建立数据出境管理流程，规范数据本地化和出境风险评估的流程。

意识培训

企业应对所有员工进行必要的培训，使其充分掌握网络安全管理制度和流程，了解违反规定的后果，并对违反安全规定的行为采取零容忍政策。企业要建立和实施网络安全意识培训流程，使所有员工都了解网络安全与合规的重要性，并组织必要的培训，让员工充分了解其职责范围内的管理流程。

首先从全员层面，提升企业内部员工认知可能存在的安全问题，认识信息安全事故对组织的危害，通过培训或者模拟实战演练来达到认知和恪守正确的行为方式；再次，通过持续及循序强化的宣传教育方式，使用多种类型多种渠道，将安全意识进行输入形成员工的普遍认知，以达到巩固强化并践行到行为层面，通过全员安全意识的持续强化及关键行为上的督促转化，实现网络安全的高效稳定运行。

© 2021. For information, contact Deloitte China.

b. 技术平台搭建建议

亚马逊云科技于 2006 年建立，是一家成熟的云服务提供商，提供诸多基于订阅的基础设施产品，这些产品从美国、澳大利亚、巴西、中国、德国、爱尔兰、日本、韩国和新加坡的数据中心通过互联网按需提供。自成立以来，亚马逊云科技致力于通过快速将新产品交付到客户手中，然后根据客户反馈快速迭代和改进这些产品，保持着定义云计算的创新者的身份。创新的节奏和持续的服务改进是越来越多的组织为其关键任务系统 选择使用 亚马逊云科技的产品的原因。

亚马逊云科技的云平台在中国大陆地区由光环新网运营的亚马逊云科技中国（北京）区域和由西云数据运营的亚马逊云科技中国（宁夏）区域组成（下面对两家公司及其他亚马逊云科技区域的运营者各称为“云服务运营者”）。在此前提下，亚马逊云科技服务于各种客户，通过安全责任共担模型，使客户能够在 IT 环境中有效和高效地管理风险，并通过我们遵守已建立的、广泛认可的框架和程序，提供有效的风险管理的保证。

类别	产品
计算	Amazon EC2、Amazon EC2 Container Service、Amazon Elastic Beanstalk、Amazon Lambda、Amazon Auto Scaling
存储	Amazon S3、Amazon CloudFront、Amazon EBS、Amazon EFS、Amazon Glacier、Amazon Storage Gateway、Amazon Snowball
数据库	Amazon RDS、Amazon DynamoDB、Amazon ElastiCache、 Amazon Redshift
网络	Amazon VPC、Amazon Direct Connect、Amazon Elastic Load Balancing
开发人员工具	Amazon CodeCommit、Amazon CodeBuild、Amazon CodeDeploy、 Amazon 工具和软件开发工具包
管理工具	Amazon CloudWatch、Amazon CloudFormation、Amazon CloudTrail、 Amazon Config、Amazon 管理控制台、Amazon Service Catalog、Amazon Trusted Advisor
安全和身份	Amazon Identity & Access Management、Amazon Directory Service、Amazon KMS、Amazon WAF、 Amazon Cognito
分析	Amazon EMR、 Amazon Elastisearch Service、Amazon Kinesis、Amazon Kinesis Firehose、Amazon Machine Learning
移动及物联网 (IoT)	Amazon IoT 、Amazon FreeRTOS、Amazon IoT Device Management、Amazon IoT Event、Amazon IoT GreenGrass、Amazon IoT Analytics、Amazon IoT Device Defender
应用程序服务	Amazon API Gateway、Amazon SNS、Amazon SQS、Amazon SWF

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

安全责任共担模型

本部分描述亚马逊云中用于管理共享责任模型亚马逊云科技方面的风险的机制，以及客户可以利用的工具。

云服务运营者及其客户共享对 IT 环境的控制。因此，安全是一项共同的责任。当谈到管理云服务运营者中的安全性和遵从性时，各方都有不同的责任。客户的责任取决于他们使用的服务。然而，通常情况下，客户负责以与其特定的安全性和遵从性需求相一致的方式构建其 IT 环境。

本文详细介绍了各方的安全责任，以及客户可以从亚马逊云科技风险与合规计划中获益的方式。

安全性和遵从性是云服务运营者和客户之间的共同责任。根据所部署的服务，此共享模型可以帮助减轻客户的操作负担。这是因为云服务运营者操作、管理和控制从主机操作系统和虚拟化层一直到服务运行的设施的物理安全的组件。除了云服务运营者提供的安全组防火墙的配置外，客户还负责客户操作系统 (包括更新和安全补丁) 和其他相关应用软件的管理。

我们建议客户仔细考虑他们选择的服务，因为他们的职责取决于所使用的服务、将这些服务集成到他们的 IT 环境中以及适用的法律和法规。客户可以通过利用诸如基于主机的防火墙、基于主机的入侵检测和防御、加密和密钥管理等技术来增强其安全性和 / 或满足更严格的遵从性需求。

这种共享责任的性质还提供了灵活性和客户控制，允许客户部署满足特定行业认证需求的解决方案。

这个共享的责任模型也扩展到 IT 控制。正如云服务运营者及其客户共享 IT 环境的运营责任一样，IT 控制的管理、运营和验证也是共享的责任。云服务运营者可以通过管理那些与部署在亚马逊云科技的云环境中的物理基础设施相关联的控件来帮助客户。然后，客户可以使用可用的亚马逊云科技控制和合规性文档，根据需要执行其控制评估和验证程序。举例来说，某些控制的责任是如何在云服务运营者及其客户之间共享的。

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

云的安全

亚马逊云科技云上的隐私保护

客户的信任是亚马逊云科技的第一要务。我们为 240 多个国家和地区的数百万个活动客户提供服务，包括企业、教育机构和政府机构。我们的客户包括金融服务提供商、医疗保健提供商和政府机构，他们将一些最敏感的信息托付给我们，给予我们充分的信任。

我们知道，客户十分注重隐私和数据安全。因此，亚马逊云科技通过简单而强大的工具让您拥有和控制自己的内容，这些工具可以让您确定内容的存储位置、保护动态和静态内容，并为用户管理对亚马逊云科技服务和资源的访问权限。我们还采取了可靠而完善的技术和物理控制措施，防止您的内容被非法访问或披露。

亚马逊云科技持续监控不断变化的隐私监管和立法领域，以识别变更并确定我们的客户可能需要哪些工具来满足其合规性需求，具体取决于他们的应用程序。我们建议在亚马逊云科技和数据保护法规方面有问题的客户和 APN 合作伙伴先联系自己的亚马逊云科技客户经理。注册了企业支持的客户也可以联系自己的技术客户经理 (TAM)。TAM 会与解决方案架构师合作，帮助客户确定潜在的风险和可能的缓解措施。TAM 和客户团队还可以根据客户和 APN 合作伙伴的环境和需求，为其指明特定资源。亚马逊云科技无法提供法律建议，我们建议客户在遇到法律问题时咨询其法律顾问。

维护客户信任是一项持续的承诺。我们力求让您了解我们实施的隐私和数据安全政策、实践和技术。这些承诺包括：

- **访问：**作为客户，您可以完全控制自己的内容，并负责配置对 亚马逊云科技的云服务和资源的访问。我们提供了一系列先进的访问、加密和日志记录功能（例如 Amazon Identity and Access Management、Amazon Organizations 和 Amazon CloudTrail），可以帮助您有效达成这一目标。我们为您提供了 API，以便为您在亚马逊云科技环境中开发或部署的任何服务配置访问控制权限。未经您的同意，我们不会出于任何目的而访问或使用您的内容。我们绝不会出于营销或广告目的而使用您的内容或从中提取信息。

- **存储：**您可以选择存储自己的内容的北京区域或宁夏区域及其存储类型。您可以在多个区域中复制和备份您的内容。未经您的同意，我们不会将您的内容移到或复制到您所选择的区域之外，除非法律要求或者政府部门发布有约束力的指令要求。

- **安全性：**您可以选择自己的内容的保护方式。我们为您的传输中和静态内容提供强加密功能，而且您可以选择自行管理自己的加密密钥。这些数据保护功能包括：
  - o 在 100 多种亚马逊云科技云服务中可用的数据加密功能。
  - o 使用 Amazon Key Management Service (KMS) 的灵活密钥管理选项，让客户能够选择是让亚马逊云科技管理加密密钥还是自行完全控制密钥。

- **安全保证：**我们制定了一项安全保证计划，使用全球范围内的隐私和数据保护最佳实践来帮助您在云上安全运行，并充分利用我们的安全控制环境。这些安全保护和控制流程分别通过多个第三方独立评估进行了验证。

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

合规计划

合规计划可以帮助客户了解云服务运营者用于维护亚马逊云科技云中安全性和实施数据保护的强大控制措施。如果系统是在云中构建的，那么双方将共同承担合规性责任。通过将以治理为中心、便于审计的服务功能与适用的合规性或审计标准结合起来，合规性工具（如 Amazon Config、Amazon CloudTrail、Amazon Identity and Access Management、 Amazon GuardDuty 和 AmazonSecurity Hub）基于传统流程构建，可以帮助客户建立亚马逊云科技的安全控制环境并在该环境中运营。云服务运营者为客户提供的 IT 基础设施的设计和管理方式符合安全性最佳实践和一系列 IT 安全标准，包括：

北京区域的合规：

- ISO9001，ISO20000，ISO27001，ISO27018 和 ISO22301 认证
- 等级保护 2.0 MLPS 2.0 level 3
- PCI DSS
- SOC 1 Type 1 Type 2
- SOC 2 Type 1 Type 2
- SOC 3
- 可信云评估
- TISAX

宁夏区域的合规：

- ISO9001，ISO20000，ISO27001 ISO27018，ISO23301 和 ISO27701 认证
- 等级保护 2.0 MLPS 2.0 level 3
- SOC 1 Type 1 Type 2
- SOC 2 Type 1 Type 2
- SOC 3
- 可信云评估
- TISAX

此外，亚马逊云科技平台提供的灵活性和控制让客户可以部署符合多项行业特定标准的解决方案 。云服务运营者通过白皮书、报告、认证、评估认证和其他第三方证明向客户提供与 IT 控制环境相关的各种信息。

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

亚马逊云科技云上的数据安全

亚马逊云科技提供很多安全服务，帮助客户实现云端的数据安全，以满足各类数据保护，隐私保护相关的合规。这些服务涵盖数据访问的数据资产识别与发现、身份与权限管理、数据加解密、探测与分析、响应与处置、持续合规检查等几个方面。

数据资产的识别与发现

云上的数据分布关系型数据库 Amazon RDS、非关系型数据库如 Amazon DynamoDB、大数据分析服务如 Amazon EMR、数据仓库 Amazon RedShift、存储服务 Amazon S3、Amazon EBS 和 Amazon EFS 等。

我们可以通过 Amazon Config 发现云端的数据资产，并实现配置管理和变更管理。Amazon Config 服务可供客户评估、审计和评价亚马逊云科技上的资源配置。Amazon Config 持续监控和记录云上资源配置，并支持自动依据配置需求评估记录的配置。借助 Amazon Config，客户可以查看配置更改以及云上资源之间的关系、深入探究详细的资源配置历史记录并判断您的配置在整体上是否符合内部指南中所指定的配置要求。这样客户能够简化合规性审计、安全性分析、变更管理和操作故障排除。

身份与权限管理

云上的数据访问，需要有合理的使用账号管理与权限控制。身份管理服务 IAM 和目录服务 Directory Service 可以帮助客户在云上建立和管控对数据访问的权限管理。

Amazon Identity and Access Management (IAM) 使客户能够安全地管理对亚马逊云科技服务和资源的访问。客户可以使用 IAM 创建和管理 亚马逊云科技用户和组，并使用各种权限来允许或拒绝他们对亚马逊云科技资源的访问。

借助 IAM，客户能够控制对亚马逊云科技服务 API 和特定资源的访问。这类控制能力已经达到了操作级别，也就是对云资源的操作权限，都可以通过 IAM 的策略控制权限。在 IAM 的访问策略中添加特定的条件（例如时间，IP 等），以控制用户使用云服务的方式、其来源 IP 地址、是否使用 SSL，或是否通过多重验证设备进行身份验证。

IAM 还允许创建角色。通过角色定义一组权限，然后让通过验证的用户或 EC2 实例承担这些角色，通过授予对定义资源的临时访问权限改善安全状况。

IAM 支持多因子身份认证 MFA，提供除用户名称和密码凭证外的更多的验证

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

方式来保护客户的亚马逊云科技云环境。通过 IAM，客户还可以使用现有的身份验证系统（如 Microsoft Active Directory）向员工和应用程序授予对云管理控制台和云服务 API 的联合访问权限。使用任何支持 SAML 2.0 的身份管理解决方案都可以实现这类功能。

Amazon IAM Access Analyzer 功能，可以帮助客户分析其账号的用户访问权限使用情况。IAM 访问分析器提供超过 100 个策略检查，可帮助您在策略编写期间主动验证策略。这些检查将分析您的策略并报告错误、警告和建议，并提供指导您设置安全和功能权限的可行建议。IAM 访问分析器还可使您在部署权限更改之前验证对资源的公有访问权限和跨账户访问权限。您可以在 Amazon S3 控制台中或使用 IAM 访问分析器 API 预览访问权限。当客户需要实施最小权限原则时，最大的困难是如何确定当前使用的权限是最小的并且是够用的，IAM 访问分析器可以帮助您检查现有的访问，从而使您能够识别和删除意外的外部权限或未使用权限。为了使您能够识别具有公有或跨账户访问权限的资源，IAM 访问分析器生成全面的结果，访问分析器持续监控新资源策略或更新资源策略，并分析针对 Amazon S3 存储桶、Amazon KMS 密钥、Amazon SQS 队列、Amazon IAM 角色、Amazon Lambda 函数和 Amazon Secrets Manager 授予的权限。为了帮助您删除未使用的权限，IAM 还会提供最后一次访问的信息，以指定 IAM 实体最后一次使用服务或操作的时间。这可以帮助您轻松识别和删除未使用的权限，从而减少访问，并帮助您设置权限边界。

数据加解密

亚马逊云科技云上数据加解密是保证数据的重要手段，其中包括对保存在各种存储和数据库中的静态数据加密和对传输的动态数据进行加密。

Amazon Key Management Service (KMS) 可让您轻松创建和管理加密密钥，并控制其在各种云服务和应用程序中的使用。Amazon KMS 是一种安全且有弹性的服务，它使用已经过 FIPS 140-2 验证或正在验证的硬件安全模块来保护您的密钥。Amazon KMS 还能与 Amazon CloudTrail 集成，从而为您提供所有密钥的使用记录，帮助您满足监管和合规性要求。

Amazon KMS 与 Amazon Encryption SDK 集成，使您可以使用受 KMS 保护的数据加密密钥在应用程序中进行本地加密。使用简单的 API，您还可以在自己的应用程序中构建加密和密钥管理，无论应用程序在何处运行。Amazon KMS 与亚马逊云服务集成，可简化密钥使用以加密亚马逊工作负载中的数据。客户可以选择所需的访问控制级别，包括在账户和服务之间共享加密资源的能力。KMS 会将密钥的所有使用记录到 Amazon CloudTrail，以便为您提供访问加密数据的用户的独立视图，包括代表您使用这些数据的亚马逊云科技服务。

针对传输中的数据，亚马逊云科技上提供的 Certificate Manager 可帮助您轻松地预置、管理和部署公有和私有安全套接字层 / 传输层安全性 (SSL/TLS) 证书，以便用于 Amazon 服务和您的内部互联资源。SSL/TLS 证书用于保护网络通信的安全，并确认网站在 Internet 上的身份以及资源在私有网络上的身份。

亚马逊云科技加密开发工具包是一个客户端加密库，旨在让每个人都可以使用行业标准和最佳实践轻松加密和解密数据。它使您能够专注于应用程序的核心功能，而不是关注如何最好地加密和解密数据。亚马逊云科技加密开发工具包是根据 Apache 2.0 许可证免费提供的。

使用亚马逊云科技加密开发工具包，您可以定义主密钥提供程序（Java 或 Python）或密钥环（C 或 JavaScript），用于确定用于保护数据的主密钥。然后，您可以使用亚马逊云科技加密开发工具包提供的直接方法对数据进行加密和解密。其余的是亚马逊云科技加密软件开发工具包。

Amazon KMS 推出了多区域密钥，这项功能允许您将一个区域的密钥复制到其他区域。借助多区域密钥功能，您可以更轻松地在区域之间移动加密数据，同时无需在各个区域使用不同的密钥进行解密和重新加密。使用

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Aamzon 加密 SDK、Aamzon S3 加密客户端和 Amazon DynamoDB 加密客户端的客户端侧加密都支持多区域密钥。此功能简化了将受保护的数据复制到多个区域的过程，例如灾难恢复 / 备份、Amazon DynamoDB 全局表或者需要在多个区域使用同一签名密钥的数字签名应用程序。KMS 可让您轻松创建和管理加密密钥，并控制其在各种亚马逊云科技 服务和应用程序中的使用。

探测与分析

Amazon CloudWatch 是一种面向开发运营工程师、开发人员、站点可靠性工程师 (SRE) 和 IT 经理的监控和可观测性服务。CloudWatch 为您提供相关数据和切实见解，以监控应用程序、响应系统范围的性能变化、优化资源利用率，并在统一视图中查看运营状况。CloudWatch 以日志、指标和事件的形式收集监控和运营数据，让您能够在统一查看在亚马逊云科技和本地服务器上运行的资源、应用程序和服务。您可以使用 CloudWatch 检测环境中的异常行为、设置警报、并排显示日志和指标、执行自动化操作、排查问题，以及发现可确保应用程序正常运行的见解。

Amazon GuardDuty 是一种威胁检测服务，可持续监控恶意活动和未经授权的行为，从而保护您的云账户、工作负载和在 Amazon S3 中存储的数据。迁移到云后，账户和网络活动的收集与聚合变得异常简单，但安全团队对事件日志数据进行持续的分析以发现潜在的威胁，则可能十分耗时。Amazon GuardDuty 为您提供了经济高效的智能选项，从而持续检测在亚马逊云科技中发生的威胁。此服务使用机器学习、异常检测和集成威胁情报等手段，识别潜在的威胁并确定优先级别。GuardDuty 对来自多个亚马逊云科技上的数据源（例如 Amazon CloudTrail 事件日志、S3 数据访问日志，Amazon VPC 流日志和 DNS 日志）的数百亿事件进行分析。只需在云管理控制台中几次点击，就可以启用 Amazon GuardDuty，无需部署或维护任何软件或硬件。Amazon GuardDuty 警报与 Amazon CloudWatch Events /Event Bridge 集成，具有极好的可行动性，并且可以直接推送到现有的事件管理和工作流程系统。

响应与处置

Amazon Security Hub 可让您全面查看亚马逊云科技账户中的高优先级安全警报与合规性状态。客户可以任意使用一系列强大的安全工具，从防火墙和端点保护到漏洞和合规性扫描程序。但是，这通常会让安全或运维团队在这些工具之间来回切换，每天处理数百甚至数千个安全警报。借助 Amazon Security Hub，客户现在可以设置单个位置，对来自多个云服务（如 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie），以及来自合作伙伴解决方案的安全警报或检测结果进行聚合、组织和设置优先级。Amazon Security Hub 的检测结果可在具有可操作图形和表格的集成控制面板上进行直观汇总。客户还可以使用自动合规性检查（基于您的组织遵守的 亚马逊云科技安全最佳实践和行业标准），持续监控您的环境。Amazon Security Hub 的集成控制面板将所有账户的安全检测结果汇总起来，向您显示当前的安全性与合规性状态。客户可以基于此采取必要的后续步骤。例如，使用与 Amazon CloudWatch Events 的集成，您可以将检测结果发送到开单、聊天、电子邮件或自动修复系统。

同时，围绕 Amazon Security Hub，我们也构建了一个生态，很多安全公司的如防火墙，漏洞发现与管理工具等可以使用 Amazon Security Hub 开放的接口标准，把安全相关的发现和信息发送到 Amazon Security Hub 中。Amazon Security hub 作为云端安全运维管理的集成服务，也可以把发现的威胁与安全

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

风险信息，通过 Amazon CloudWatch Event 或 Amazon Event Bridge 发送到其他安全相关服务中，如通过 Amazon SNS 发送邮件通知相关人员，通过 Amazon Lambda 自动在工单系统中创建工单。通过 Kinesis 把发现发送到类似 Splunk 这类 SIEM 平台，调用安全自动化响应的 Lambda 函数，实现安全的自动化响应。

Amazon Lambda 是一种无服务器的计算服务，让您无需预置或管理服务器、创建可感知工作负载的集群扩展逻辑、维护事件集成或管理运行时，即可运行代码。借助 Lambda，您几乎可以为任何类型的应用程序或后端服务运行代码，而且完全无需管理。只需将您的代码以 ZIP 文件或容器映像的形式上传，Lambda 便会自动、精确地分配计算执行能力，并根据传入的请求或事件运行您的代码，以适应任何规模的流量。您可以将您的代码设置为自动从 200 多个亚马逊云科技服务和 SaaS 应用程序触发，或者直接从任何 Web 或移动应用程序调用。您可以使用自己喜欢的语言（Node.js、Python、Go、Java 等）编写 Lambda 函数，并使用无服务器和容器工具（例如 Amazon SAM 或 Docker CLI）来构建、测试和部署您的函数。Amazon Lambda 通过和 Amazon Security Hub，Amazon CloudWatch 或 Amazon Event Bridge 集成，可以实现安全的自动化响应。

持续合规检查

Amazon Security Hub 为您提供了一组称为亚马逊云科技基础安全最佳实践标准的自动安全控制措施。这是一套高度精心策划的安全最佳实践，由我们的亚马逊云科技安全专家审查，它们可以在相关资源发生变化时持续运行，或按固定的定期计划运行。每个控件都有特定的严重性分数，以帮助您确定修复工作的优先级我们建议在所有账户和地区启用此标准，并且我们将继续使用新的控制措施和额外的服务范围对其进行更新。Amazon Security Hub 还提供了与行业和监管框架相一致的其他标准，例如支付卡行业数据安全标准 (PCI DSS) 和互联网安全中心 (CIS) 的安全基线。这些标准还由连续、自动化的安全检查提供支持。

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

数据分析中的安全

亚马逊云科技的数据分析服务，主要在数据湖，数据仓库等上面，其中数据湖又是各个行业用户以及跨国公司重要的分析工具。

亚马逊云科的技数据湖的安全主要分为两个方面：一个是数据本身的安全，另一个是访问权限的安全。企业无论是为了内部合规还是符合外部监管，会有对于当前收集到的数据做分级。一些关乎客户个人信息的数据会被分类为 PII 高度敏感数据如姓名、身份 ID、电话等，需要最高级别的安全管控。亚马逊云科技的分析服务提供各种安全功能来满足客户对于数据安全的需求。

传输中加密

数据从客户端到服务器端加密可以更好的保证传输过程中不被篡改和窃取。大数据服务一般是集群模式以保证大数据量下的计算性能，集群节点之间的数据传输也非常的频繁。集群节点间的传输加密也很重要。亚马逊云科技的大数据托管服务全部提供传输中间加密的功能 :Amazon EMR、Amazon Redshift、Amazon Elasticsearch、Amazon Kinesis Amazon Glue、Amazon Athena、Amazon Quicksight、Amazon Managed Streaming for Apache Kafka。

数据存储加密

数据存储在云上，要保证数据不被窃取则需要数据存储加密。亚马逊云科技的托管服务提供多种不同的数据存储加密方式以满足不同数据分级的要求。不同的服务支持的数据存储加密种类会不同，具体请参照服务的加密选项。例如 Amazon EMR 的存储加密选项。

访问控制

大数据服务会有很多终端用户访问，不同用户的访问级别不同，需要表级别的访问控制的机制来满足安全合规需求。所有大数据服务都使用 IAM 的细粒度权限管理可以管理用户在 API 级别的操作权限，Amazon Lakeformation 可以提供基于 Amazon Glue、Amazon Athena、Amazon EMR 数据湖之上 S3 数据存储、表级别、字段级别和行级别的细粒度权限控制。其他服务如 Amazon Redshift、Amazon Elasticsearch 都提供类似的用户权限体系细粒度的管理用户访问权限。

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

机器学习的安全

Amazon SageMaker 通过整合专门为机器学习构建的广泛功能集，帮助数据科学家和开发人员快速准备、构建、训练和部署高质量的机器学习 (ML) 模型。SageMaker 使用专用工具为机器学习开发的每个步骤加速创新，包括标签、数据准备、功能工程、统计偏差检测、自动机器学习、训练、调优、托管、可解释性、监控和工作流。作为托管服务，Amazon SageMaker 自动继承亚马逊云科技的全球基础设施及其网络安全功能。Amazon SageMaker 还提供全面的功能集，因此客户可以运行机器学习工作负载灵活而安全的机器学习环境今天可用。Amazon SageMaker 的安全功能很容易满足客户面临的数据安全与合规的挑战。

基础架构和网络安全：控制跨越的数据流量，Amazon SageMaker 组件超过私人网络。确保合适单租户的入口 / 出口，所以你的数据和资源是安全的。

认证与授权：定义、执行和审谁可以进行身份验证并授权使用 Amazon SageMaker 资源。

数据保护：获取灵活的，自动的加密能力，包括对数据静态和传输中的数据，支持自带密钥。

监控与审计：跟踪、跟踪和审核所有 API 调用、活动、数据访问、和互动直至用户和 IP 级别。

合规：继承最多全面的合规控制并轻松与客户所在行业的监管要求。

第三方解决方案

亚马逊云科技在中国区域云市场 Marketplace 上，已经为客户提供了来自大量本土安全厂商和国际安全公司提供的有数百种产品，其中有大量的安全产品，包括主机安全，网络安全，数据安全，安全运维，合规检查，网络等级保护等。同时中国区 Marketplace 也支持 SaaS 的安全方案的部署。

©2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

致谢

编写指导

德勤中国：薛梓源 江玮 张震 石沛恩 阎光

亚马逊云科技：顾凡 王晓野 江学森

主编人员

德勤中国：须文东 何智聪 申燕茹 傅栌峰 李颖 王嘉晖

亚马逊云科技：韩旭明 贺浏璐

协助编辑

亚马逊云科技：王焘 张亮 李昕 吴佳敏