亚马逊云科技 致力金融服务创新

借助亚马逊云科技安全性与合规性强化金融服务机构

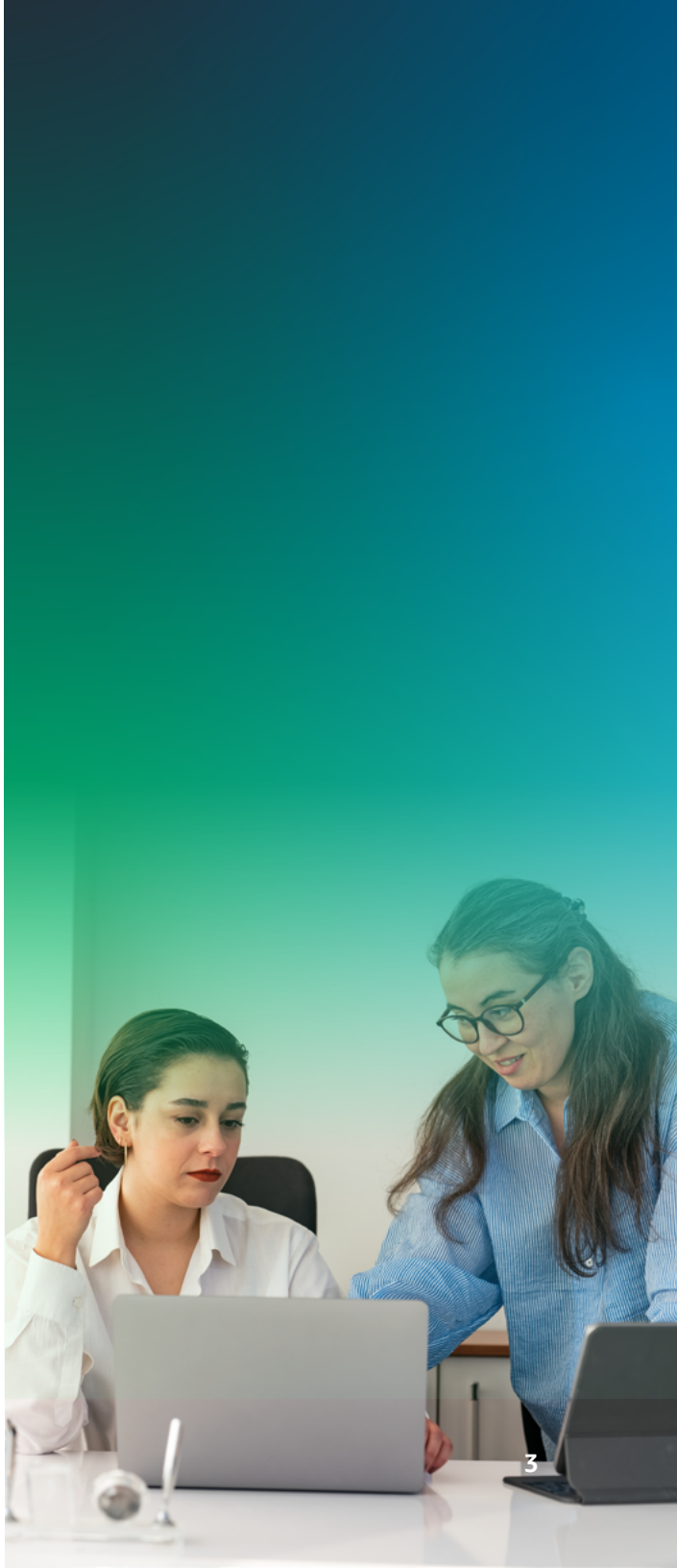
目录

简介

随着金融服务机构迁移到云并在云上进行构建，韧性、安全性、数据隐私和监管合规性依然是各机构需要关注的重要方面。

云技术在各种类型的企业中不断发展。金融服务机构越来越关注业务关键型应用程序的大规模云迁移，这些应用程序包括交易生命周期平台、核心银行和保险系统以及支付处理软件。

如果金融机构想要将业务迁移到云端，亚马逊云科技可提供多种优势。首先，亚马逊云科技支持采用持续的方法来实现安全性、合规性和韧性。亚马逊云科技的核心基础设施旨在满足高度敏感型企业（例如军事机构、全球银行等）严苛的安全要求。为了支持责任共担模式，亚马逊云科技提供了广泛的服务、工具、资源、最佳实践和指导，来协助客户实施应用程序级安全措施并实现合规性。亚马逊云科技专家可以协助金融机构，建立可满足甚至超额满足其控制要求的控制措施。此外，亚马逊云科技合作伙伴也提供了一些工具及功能，来协助金融客户实现其安全目标，包括网络安全、配置管理、访问控制和数据加密。



轻松应对变幻莫测的局面

数据、应用程序和基础设施的监管和安全要求千变万化，让如今的金融服务机构面临着一个非常复杂的局面。随着生成式人工智能（AI）的出现，安全威胁形势以及抵御这些威胁所需的要求和政策也进一步发生了转变。亚马逊云科技可以协助企业满怀信心地轻松应对这一复杂局面。

网络攻击的主要目标

金融服务行业一直是极容易受到网络攻击的行业之一。破坏分子会使用各种威胁媒介，包括网络钓鱼、勒索软件、拒绝服务（DoS）攻击和内部威胁。而且，威胁的数量和狡诈程度依然是有增无减。

64%

金融服务企业在 2023 年报告遭遇勒索软件攻击的比例，而在 2021 年这一比例为 34%[1]

2 倍

金融领域 2023 年第三季度相比于 2022 年第三季度网络事件数量的倍数[2]

分化且复杂的监管要求

围绕数据隐私和网络安全的监管环境十分复杂，而且越来越分化。

金融服务机构必须很好地满足各种严格的数据隐私要求。其中最突出且影响最深远的是欧盟的《通用数据保护条例》（GDPR）。在美国，加利福尼亚州、科罗拉多州、康涅狄格州、蒙大拿州、俄勒冈州、德克萨斯州和犹他州均正式通过了数据隐私要求。其它州也在考虑推进相关立法。[3] 这种千变万化的监管环境，为跨多个州开展业务的企业带来了复杂性。

此外，全球各国 / 地区的政府和监管机构正在研究信息和通信技术（ICT）在金融服务机构运营风险中扮演的角色。值得注意的是，欧盟数字运营韧性法案（DORA）扩大了对运营风险组成部分的规定，将 ICT 纳入其中。

生成式人工智能和风险管理

生成式人工智能可以自动化、加速并强化从合规到环境风险控制的方方面面，从而从根本上改变金融机构的风险管理方式。[4] 与此同时，生成式人工智能引发了人们对风险的担忧，一些政府也因此出台了相应的监管措施，比如《欧盟人工智能法案》（EU AI Act），以及美国最近签署的《美国人工智能行政命令》（U.S. Executive Order on Artificial Intelligence）。随着机构不断发展，他们就需要考虑数据隐私、安全性，并负责任地设计基础设施以及利用其数据的大型语言模型。

[1]《The State of Ransomware in Financial Services 2023》，Sophos，2023 年。

[2]《Cyberthreats to the financial industry: interim results for 2023》，Positive Technologies，2023 年。

[3]《US State Privacy Legislation Tracker 2024》，IAPP，2024 年。

[4]《How generative AI can help banks manage risk and compliance》，McKinsey，2024 年。

此外，在 2020 年，美国联邦储备委员会发布了《Sound Practices to Strengthen Operational Resilience》，其中概述了根据现有法规、指南、声明和行业标准提高运营韧性的步骤。这些实践以有效的治理和风险管理方法为基础，考虑第三方风险，还建立了具有韧性的信息系统。

在 2024 年 3 月，美国财政部发布了一份新的报告，名为《Managing Artificial Intelligence Specific Cybersecurity Risks in the Financial Services Sector》，该报告确定了具体的风险，并概述了管理威胁的最佳实践。具体到云这方面，财政部于 2023 年 2 月发布了《The Financial Services Sector's Adoption of Cloud Services》。该报告确定了金融服务机构使用云服务可以为消费者带来哪些好处，包括“降低成本、能够快速部署新信息技术（IT）资产、缩短开发新产品和服务的时间，以及增强安全性和韧性。”

此外，该报告还概述了财政部关于支持金融业利用云服务实现运营韧性的战略愿景，包括利用云服务提高金融业运营韧性的长期目标。这一战略愿景将指导财政部在未来几个月甚至几年内，与私营企业以及国内外同级企业的协作。

聚焦运营韧性

- **澳大利亚**发布了市场诚信规则，旨在提高证券和期货市场运营商及参与者的技术和运营韧性。
- **香港**推出了《监管政策手册》，要求金融服务机构制定实现运营韧性的框架和时间表。
- **新加坡**发布了关于运营风险管理以及外包和第三方管理的指南。该国还要求银行根据该指南对自身的行为进行评测。

云中的安全性：培养安全防御文化

云采用可以在很大程度上推动培养安全防御文化，并协助金融服务机构更轻松地实现合规性。

面对不断增加的威胁和风险，以及不断提高的运营韧性要求，企业将会继续向云迁移，因为在云端，企业所做的一切都可以实现安全性。通过与客户、合作伙伴以及内部构建者合作，我们发现，云安全服务的快速创新，令企业能够更轻松地将安全性落实到企业的方方面面，并推动实现持续改进。

云技术带来的好处可以延伸至运营韧性，云服务提供商可以有效地提供所需的地域多元化和基础设施冗余，从而实现韧性和业务连续性。对于金融服务机构而言，自行构建和管理这些冗余将需要大量的资本和资源，并且会导致机构无法专注于能够推动创新和业务增长的项目。亚马逊云科技提供了非常安全、广泛、且可靠的全球云基础设施。Gartner 已经确认了我们的市场领导地位，在 2023 年 Gartner 战略云平台服务（SCPS）魔力象限报告中，将亚马逊云科技评为领导者。在前 8 位供应商中，亚马逊云科技在“执行能力”衡量指标轴中名列前茅。

亚马逊云科技责任共担模式

安全与合规是亚马逊云科技与客户的共同责任。这种责任共担模式有助于减轻客户的运营负担，因为亚马逊云科技将负责运行、管理和控制各种组件，从主机操作系统和虚拟化层，一直到运行服务的设施的物理安全机制等。对于 Amazon EC2，客户负责和管理来宾操作系统（包括更新和安全补丁）、其它关联应用程序软件，以及亚马逊云科技提供的安全组防火墙的配置。对于 Amazon Simple Storage Service（Amazon S3）和 Amazon DynamoDB 等抽象服务，亚马逊云科技运行基础设施层、操作系统和平台，而客户负责访问端点来存储和检索数据。客户负责管理其数据（包括加密选项）、对其资产进行分类，以及使用 IAM 工具来应用适当的权限。

客户应慎重选择服务，因为他们所承担的责任因他们使用的服务、服务与其 IT 环境的集成以及适用法律法规而各异。这一责任共担模式还提供了支持部署的灵活性和客户控制能力。如下一页的图中所示，通常，亚马逊云科技与客户的责任分别被称为“云的安全性”和“云中的安全性”。

亚马逊云科技的责任：云本身的安全性

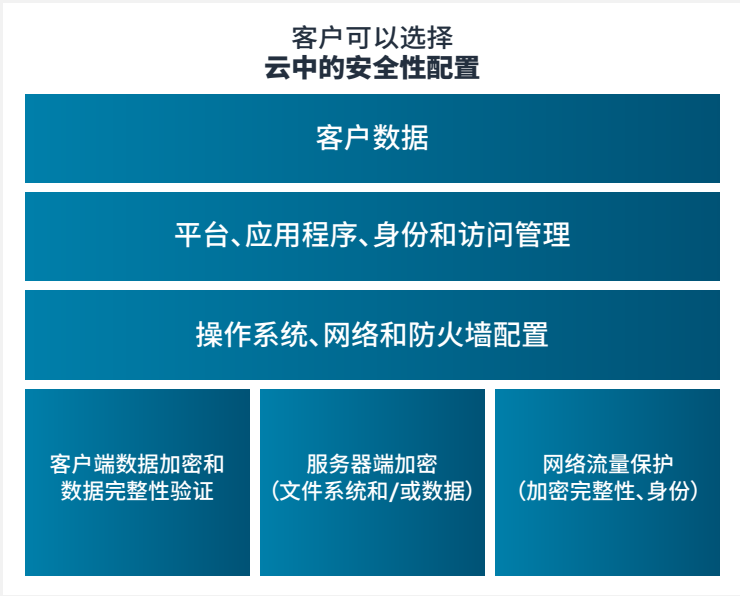
亚马逊云科技负责保护运行亚马逊云科技云中提供的所有服务的基础设施。该基础设施由运行亚马逊云科技云服务的硬件、软件、网络和设施组成。

客户的责任：云中的安全性

客户负责管理其数据（包括加密选项）、对其资产进行分类，以及使用身份和访问管理工具来应用适当的权限。

此外，这一责任共担模式还扩展到 IT 控制体系方面。正如亚马逊云科技与客户共同承担运行 IT 环境的责任一样，管理、运营和验证 IT 控制体系的责任也是由双方共同承担。亚马逊云科技可协助客户管理与部署在亚马逊云科技环境中的物理基础设施相关的控制体系，而这之前可能是由客户来管理的。

因为每个客户在亚马逊云科技中的部署均不相同，所以客户可以通过将管理特定 IT 控制体系的责任移交到亚马逊云科技，形成一个新型分布式控制环境。客户可以根据需要使用亚马逊云科技的控制和合规文档来执行自己的控制评估和验证流程。



采用亚马逊云科技最佳实践

在确保安全与合规，并推进这方面工作的发展上，并非所有云都做得一样好。使用亚马逊云科技，金融服务机构可获得所需的控制力和信心，利用当今高度灵活且非常安全的云计算环境来运营自己的业务，并可受益于亚马逊云科技区域和可用区的韧性，以及为保护其信息、身份、应用程序和设备而构建的基础设施。跨一个区域内的多个可用区运营便是一种最佳实践，有助于让客户实现非常高的可用性。借助亚马逊云科技，金融服务机构能够利用我们全面的服务和功能，提高自己满足核心安全与合规要求的能力，例如数据局部性、保护和保密性。此外，通过亚马逊云科技，金融服务机构可以自动执行手动安全任务，如检测和补救，从而可以将精力集中到扩展业务并实现创新上。

确保实现最高标准的安全性、合规性和隐私保护

亚马逊云科技经过精心构建，是当今非常安全的云环境，由一套云安全工具提供支持，拥有 300 多项安全性、合规性和治理服务及功能。这意味着亚马逊云科技客户将沿用最全面的安全与合规控制体系。

亚马逊云科技支持 143 项安全标准和合规性认证，包括国际标准化组织（ISO）、支付卡行业数据安全标准（PCI-DSS）、系统及组织控制（SOC）、FedRAMP、GDPR 等，有助于满足全球绝大多数监管机构的合规性要求。

亚马逊云科技拥有比其他云提供商更高的全球覆盖率，在 33 个地理区域提供 105 个可用区（已宣布计划在 4 个区域内再增加 12 个可用区），可支持不断变化的运营韧性要求。而且，亚马逊云科技全球基础设施也提供了比其他云提供商更高的网络可用性。

S&P Global
Market Intelligence

S&P Global Market Intelligence 为客户提供任务关键型应用程序，来处理大多数美国投资级债券的发行。因此，必须具备高可用性和出色的韧性。以前，公司为其每个客户分配自己的本地服务器，因而很难管理系统的小型更改。而后，公司在亚马逊云科技上构建了一个单租户系统，使用 Amazon Well-Architected Tool 对其基础设施进行改造，对照架构最佳实践来审查应用程序和工作负载的状态。如今，公司每年处理的债券发行量得以增加六倍，可用性也大大提高。

了解详情 ›

对数据保持有力控制

难以使用的数据没有太大作用。借助亚马逊云科技，金融服务机构可以基于高度安全的全球基础设施进行构建，知晓自己拥有和控制对数据的访问权限，并且能够加密、移动数据并管理数据留存。亚马逊云科技内置精细访问控制，让金融服务机构能够确保相应的资源对相应的数据拥有相应的访问权限。此外，亚马逊云科技基础设施让客户对其数据的物理位置保留完全控制权，从而有助于客户满足数据驻留要求。

JCB 是全球七大信用卡品牌之一，总部位于日本。公司选择将其本地业务系统迁移到亚马逊云科技，期望可以提高敏捷性、促进实现业务连续性并优化 IT 成本。借助 Amazon Web Services Cloud Adoption Framework（CAF）、Amazon Aurora、Amazon S3 和 Amazon Athena 等服务，JCB 得以将 80 个系统迁移到亚马逊云科技，推进通用基础设施和数据基础设施来应对业务环境的变化。公司预计，基础设施成本将降低 30%，并且运营负担也会减少。

了解详情 ›

通过自动化降低风险

金融服务机构渴望扩大安全流程的自动化，以满足业务要求和千变万化的监管要求，并应对不断扩展和演变的威胁媒介。自动化可减少人为配置错误，让金融服务机构变得更加安全，同时将资源集中投入到更具创新性且以增长为导向的项目中。

重要的是，要了解，整个安全生命周期的端到端自动化功能对于改善影响至关重要。亚马逊云科技让企业能够以在本地无法实现的规模，自动执行安全与合规方面的功能。

例如，Amazon Identity and Access Management Access Analyzer 有助于通过自动化，消除人工干预，从而让企业在对其 IT 基础设施进行更改之前，能够更多地了解其合规状况和权限级别。Amazon GuardDuty 和 Amazon CloudTrail 等亚马逊云科技服务能够根据组织的特定安全与合规需求，自动执行记录、监视和修复恶意活动等任务。Amazon Audit Manager 可以自动针对合规框架执行证据收集，让客户不再依赖基于时间点的人工评估。

此外，金融服务机构还可以使用 Amazon Systems Manager 在混合环境中自动执行基础设施和应用程序安全检查。这样一来，他们便可将亚马逊云科技作为无缝且安全的扩展，轻松与其本地环境集成。

而且，机器学习和人工智能（包括生成式人工智能）将在提高安全工程师的能力以及实现自动化方面发挥重要作用，可以协助安全工程师在云中创建更安全的架构和应用程序，并推动实现持续改进。面对千变万化的威胁形势，金融服务机构纷纷致力于打造更为主动的安全态势，而这些技术所带来的自动化和信息处理能力将有助于机构取得变革性的成果。

bitbank

随着分布式拒绝服务（DDoS）攻击的兴起，加密货币交易所 Bitbank Inc.（bitbank）利用亚马逊云科技，改变了其响应工作流并实现安全性升级。Bitbank 利用 Amazon Shield 等服务创建了一个新的 DDoS 攻击响应流程。最终，公司得以提高针对 DDoS 攻击的响应速度，确保客户不会失去任何机会，并实现安全的服务可用性和稳定性。

了解详情 ›

宏大愿景：
亚马逊云科技的强大之处——全球极其值得信赖的云

自信地加快创新速度，更快地将创意付诸实践

借助亚马逊云科技解决方案、服务以及非常大的合作伙伴社区，金融服务机构可以快速而自信地将创意付诸实践。我们的深度安全功能和对自动化的关注，为金融服务机构提供了从一开始就“正确构建”所需的资源，并优化了他们在创新方面的投入，同时也保持了最高的安全水平。

构建出色的运营韧性

鉴于金融服务机构在构建和运营（并展示）有韧性的应用程序方面往往面临着一些要求，亚马逊云科技无疑是其非常宝贵的合作伙伴。我们将防范业务中断和事故纳入我们的服务设计考虑因素中，并针对该问题进行了专门构建，以便在切实发生业务中断和事故时，将对客户和服务连续性的影响降至最低。Gartner 将亚马逊云科技区域和可用区模型评为运行需要高可用性的企业应用程序的推荐方法。

- 亚马逊云科技基础设施分布于五大洲，包括分布在 33 个地理区域中的 105 个亚马逊云科技可用区，而这些可用区又包括多个数据中心。
- 亚马逊云科技可用区在物理上相互分开、彼此独立，并采用高度冗余的网络连接，可承受局部业务中断。
- 亚马逊云科技区域相互隔离，每个区域都有专门的基础设施堆栈和服务，因此，一个区域的业务中断不会造成其它区域也出现中断的情况。与当今全球金融机构的本地环境相比，亚马逊云科技基础设施的地域多元化大大降低了地理区域集中的风险。
- 亚马逊云科技在基础设施和服务中启用了划分机制，并具有多种构造，可提供不同级别的独立冗余组件。
- 亚马逊云科技使用基于 cell 的架构，其中包含一个服务的多个实例，这些实例相互隔离。这种设计最大限度地减小了一个 cell 中出现中断进而造成其它 cell 也中断的可能性。

扩展网络事件恢复能力

金融服务机构正在亚马逊云科技上构建网络事件恢复平台，因为这样可以在几分钟内轻松构建网络数据保管库，而不像在本地构建那样，需要几个月的时间。公司可以从小规模开始，只为自己使用的资源付费，然后根据数据的增长进行扩展。而且，金融服务机构还可以使用多种安全服务来构建现代网络事件恢复平台。

了解详情 ›

更简单、更顺畅地实现安全与合规

自动化是更简单、更顺畅地实现安全与合规的关键，亚马逊云科技提供了业界极为广泛的解决方案，可大规模实现自动化。

亚马逊云科技在整个控制措施部署过程中为客户提供支持

身份与访问权限管理

检测

基础设施保护

数据保护

事件响应

合规性和治理

ekonoo

创新的实际应用

金融科技公司 ekonoo SA 曾力求在避免管理物理设备的复杂性的同时，保持安全性和合规性。为了寻求云原生工具，公司最后选择与亚马逊云科技合作。ekonoo SA 的 DevOps 负责人兼云架构师 Julien Del Piccolo 表示：“亚马逊云科技为我们提供了丰富的工具，让我们可以根据自身需求，利用这些工具实现几乎任何形式的安全或数据保护。”通过利用完全托管式亚马逊云科技服务，公司的养老金管理解决方案获得了监管部门的批准，从而让公司得以集中精力为客户创造价值。

了解详情 ›

亚马逊云科技为企业赋能

亚马逊云科技经过精心构建，是当今非常具安全性、可扩展性和韧性的云环境。借助最强大的一套云安全工具，企业将找到所需的技术、资源和行业专业知识，满怀信心地拥抱并体验云的灵活性。

立即增强您的云和应用程序

亚马逊云科技