aws

亚马逊云科技白皮书

AWS 安全性简介

AWS 安全性简介: 亚马逊云科技白皮书

Table of Contents

AWS 安全性简介

发布日期：2021 年 11 月 11 日（文档修订）

摘要

Amazon Web Services (AWS) 推出了一个具有高可用性和可靠性的可扩展云计算平台，为您提供运行各种应用程序所需的工具。帮助保护您的系统和数据的机密性、完整性和可用性对 AWS 而言至关重要，维持您的信任和信心也是如此。本文档旨在介绍 AWS 实现安全性的方法，包括 AWS 环境中的控制措施，以及 AWS 为帮助客户实现安全目标而提供的一些产品和功能。

亚马逊云科技基础设施的安全性

AWS 基础设施经过精心构建，是当今最灵活、最安全的云计算环境之一，旨在提供一个可扩展性极强、高度可靠的平台，使客户能够快速安全地部署应用程序和数据。

此基础设施的构建和管理不仅基于安全最佳实践和标准，还考虑到了云的独特需求。AWS 采取冗余的分层控制措施、进行持续验证和测试并大量使用自动化，以确保底层基础设施全天候受到监控和保护。AWS 会确保这些控制措施将复制到每个新数据中心或服务。

所有 AWS 客户都将受益于专为满足对安全性最为敏感的客户的要求而打造的数据中心和网络架构。这意味着您可以获得高度安全且具韧性的基础设施，却无需耗费传统数据中心的资本支出和运营开销。

亚马逊云科技采用安全责任共担模式，即亚马逊云科技负责底层云基础设施的安全性，而您负责保护自己部署在亚马逊云科技中的工作负载（图 1）。这为您提供了您所需的灵活性和敏捷性，使您能够在 AWS 环境中对业务职能部门实施最适用的安全控制措施。您可以严格限制用户访问处理敏感数据的环境，或者对希望公开的信息实施相对没那么严格的控制措施。

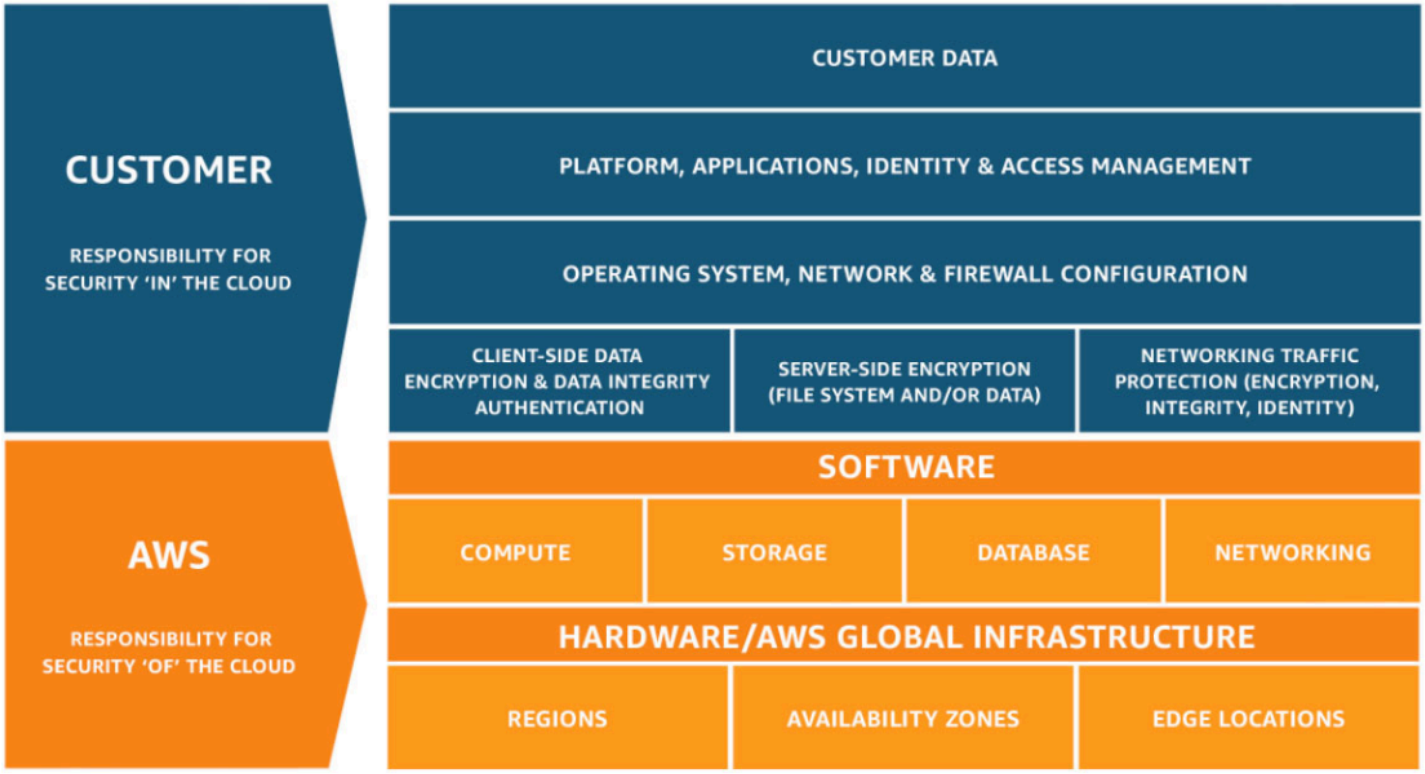

图 1：亚马逊云科技安全责任共担模式

安全产品和功能

AWS 及其合作伙伴提供了多种工具和功能，以帮助您实现安全目标。这些工具的控制措施与您在本地环境中部署的常用控制措施一摸一样。AWS 提供涵盖网络安全、配置管理、权限管控和数据安全性的安全工具和功能。此外，AWS 还提供了监控和日志记录工具，可供您全面了解环境中的实时情况。

主题

基础设施安全性

AWS 提供多种安全功能和服务，以提高隐私性、控制网络访问/使用权限，这包括：

- 内置在 Amazon VPC 中的网络防火墙，让您能够创建私有网络并控制对实例或应用程序的访问。客户可以在各种 AWS 服务中使用 TLS 控制传输中加密。
- 联接选项，支持您从办公室或本地环境建立私有或专用连接。
- DDoS 缓解技术，适用于第 3 层或第 4 层以及第 7 层。这些技术可用作应用程序和内容分发策略的一部分。
- 自动加密通过 AWS 全球和区域网络在 AWS 安全设施之间传输的所有流量。

库存和配置管理

AWS 提供一系列工具，让您能够实现快速发展，同时确保您的云资源符合组织标准和最佳实践。这包括：

- 部署工具，用于根据组织标准管理 AWS 资源的创建和停用。
- 库存和配置管理工具，用于识别 AWS 资源并跟踪和管理随着时间的推移对这些资源所做的更改。
- 模板设定和管理工具，用于为 EC2 实例创建经过强化和预先配置的标准虚拟机。

数据加密

使用 AWS，您可以在云中为静态数据添加一层安全保护，从而提供可扩展且高效的加密功能。这包括：

- 在大多数亚马逊云科技服务（如 Amazon EBS、Amazon S3、Amazon RDS、Amazon Redshift、Amazon ElastiCache、AWS Lambda 和 Amazon SageMaker）中提供的静态数据加密功能
- 灵活的密钥管理选项，包括 AWS Key Management Service，允许您选择是让亚马逊云科技管理加密密钥，还是让您能够完全掌控自己的密钥
- 使用 AWS CloudHSM 的基于硬件的专用加密密钥存储，可以帮助您满足合规性要求
- 加密消息队列，以便使用适用于 Amazon SQS 的服务器端加密 (SSE) 传输敏感数据

此外，AWS 还为您提供相应的 API，用于将加密和数据保护功能与您在 AWS 环境中开发或部署的任何服务集成。

身份与访问控制

AWS 为您提供了在各种 AWS 服务中设定、实施和管理用户访问策略的功能，这包括：

- AWS Identity and Access Management (IAM) 使您可以跨亚马逊云科技资源（适用于特权账户的 Amazon Multi-Factor Authentication）定义具有权限的各个用户账户，包括面向基于软件和硬件的身份验证器的选项。借助 IAM，您可以使用现有身份系统（如 Microsoft Active Directory 或其它合作伙伴产品/服务）向员工和应用程序授予联合访问AWS Management Console和亚马逊云科技服务 API 的权限。
- Amazon Directory Service 使您能够与企业目录集成并联合，从而减少管理开销并提升终端用户体验。
- Amazon Single Sign-On (Amazon SSO) 使您能够在 AWS Organizations 中集中管理所有账户的 SSO 访问和用户权限。

AWS 在其多种服务中提供原生身份和访问管理集成，以及与您自己的任何应用程序或服务的 API 集成。

监控和日志记录

AWS 提供的工具和功能使您能够了解 AWS 环境中的当前情况，这包括：

- 利用 AWS CloudTrail，通过获取您账户的亚马逊云科技 API 调用的历史记录，您可监控您在云上的亚马逊云科技部署，包括通过AWS Management Console、Amazon SDK、命令行工具、较高级亚马逊云科技服务进行的 API 调用。您还可以识别哪些用户和账户调用了支持 CloudTrail 的服务的 AWS API、调用的源 IP 地址以及调用发生的时间。
- Amazon CloudWatch 提供可靠、可扩展且灵活的监控解决方案，您可以在几分钟内开始使用。您不再需要设置、管理和扩展自己的监控系统和基础设施。
- Amazon GuardDuty 是一种威胁侦测服务，可持续监控恶意活动和未经授权的行为，从而保护您的 AWS 账户和工作负载。Amazon GuardDuty 通过 Amazon CloudWatch 发布通知，因此您可以触发自动响应或通知相关人员。

这些工具和功能可以提供您所需的可见性，使您能够在问题影响业务之前，就能发现问题，改进环境的安全状况，从而降低风险。

AWS Marketplace 中的安全性产品

组织将生产工作负载迁移到亚马逊云科技，可以在保持安全环境的同时提高敏捷性、可扩展性，并实现创新和成本节省。 AWS Marketplace 提供的安全性产品业界领先，且与您本地部署环境中的现有控制产品等效、相同或可与之集成。这些产品对现有亚马逊云科技服务起到补充作用，使您能够在云和本地部署环境中部署全面的安全架构，进而实现更无缝的体验。

安全指导

亚马逊云科技通过亚马逊云科技及其合作伙伴提供的在线工具、资源、支持和专业服务为客户提供指导和专业知识。

AWS Trusted Advisor 是一款在线工具，类似于定制的云专家，可以帮助您按照最佳实践配置资源。Trusted Advisor 会检查您的 AWS 环境，帮助弥补安全漏洞，并随时寻找可以节省资金、提高系统性能和可靠性的机会。

AWS 客户团队提供第一联系人，指导您进行部署和实施，并为您指出可以解决您可能会遇到的安全问题的正确资源。

AWS 企业支持承诺在 15 分钟内响应；提供全天候电话、聊天或电子邮件支持；以及配备专门的技术客户经理。这种礼宾服务可确保客户的问题尽快得到解决。

亚马逊云科技合作伙伴网络可提供数百个行业领先的产品，这些产品与您本地部署环境中的现有控制产品等效、相同或可与之集成。这些产品对现有亚马逊云科技服务起补充作用，使您能够在云和本地部署环境中部署全面的安全架构，进而实现更无缝的体验，以及通过全球数百家经过认证的亚马逊云科技咨询合作伙伴来帮助满足您的安全性与合规性需求。

亚马逊云科技专业服务可提供安全性、风险和合规性专业实践，可帮助您在将最敏感的工作负载迁移到亚马逊云科技云时增添信心并提升您的技术能力。亚马逊云科技专业服务可以帮助客户开发基于行之有效的设计的安全策略和实践，并且有助于确保客户的安全设计符合内外部合规要求。

AWS Marketplace 是一个数字目录，收录了独立软件供应商的数千种软件产品，让您可以轻松查找、测试、购买和部署在亚马逊云科技上运行的软件。AWS Marketplace 安全产品对现有亚马逊云科技服务起到补充作用，使您能够在云和本地部署环境中部署全面的安全架构，进而实现更无缝的体验。

亚马逊云科技安全公告提供关于当前安全漏洞和威胁的安全公告，并使客户能够与亚马逊云科技安全专家合作解决报告滥用、漏洞以及渗透测试等问题。我们还提供了关于安全漏洞报告的在线资源。

亚马逊云科技安全文档介绍了如何配置亚马逊云科技服务来满足安全性与合规性目标。亚马逊云科技客户可以从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

Amazon Well-Architected Framework 可以帮助云架构师为其应用程序构建安全、高性能、具有弹性且高效的基础设施。AWS Well-Architected Framework包含专注于保护信息和系统的安全性支柱。关键主题包括数据的机密性和完整性，识别和管理哪些人员可以通过权限管理进行哪些操作，保护系统以及建立控制措施来检测安全事件。客户可以通过AWS Management Console使用 AWS Well-Architected Tool，或者通过 APN 合作伙伴提供的服务来协助其使用该工具。

AWS Well-Architected Tool 可帮助您审核工作负载的状态，并将其与最新的亚马逊云科技架构最佳实践进行比较。这项免费工具已在AWS Management Console中推出，您在回答了一系列关于卓越运营、安全性、可靠性、性能效率和成本优化的问题后，即可使用该工具。回答问题后，AWS Well-Architected Tool 会提供一项关于如何使用成熟的最佳实践设计云架构的计划。

合规性

AWS 合规性计划可以帮助客户了解 AWS 用于维护 AWS 云中安全性和实施数据保护的强大管控措施。如果系统是在 AWS 云中构建的，那么 AWS 和客户共担合规责任。亚马逊云科技计算环境持续接受审计，并获得来自不同地理区域和垂直行业的认证机构的认证，包括 SOC 1/SSAE 16/ISAE 3402（以前是 SAS 70）、SOC 2、SOC 3、SO 9001 / ISO 27001、FedRAMP、DoD SRG 和 PCI DSS 级别 1.i。此外，亚马逊云科技还具有保证计划，这些计划提供模板和控制映射，以帮助客户确立其在亚马逊云科技上运行的环境的合规性。有关计划的完整列表，请参阅亚马逊云科技合规性计划。

我们可以确认所有 AWS 服务均符合 GDPR 的规定。这意味着，除了受益于 AWS 为维护服务安全性而采取的所有措施之外，客户还能将 AWS 服务部署为其 GDPR 合规性计划的一部分。AWS 提供了一项符合 GDPR 规定的数据处理附录 (GDPR DPA)，让您能够履行 GDPR 合同义务。AWS GDPR DPA 包含在 AWS 服务条款中，自动适用于全球需要 AWS 遵守 GDPR 的所有客户。Amazon.com, Inc. 通过了欧盟-美国隐私护盾认证，AWS 也通过了这项认证。这有助于那些选择将个人数据传输到美国的客户履行其数据保护义务。Amazon.com Inc. 的认证可在欧盟-美国隐私护盾网站上找到：https://www.privacyshield.gov/list

客户在经过认证的环境中运营，就能缩小审计范围并降低执行审计所需的成本。AWS 会持续评估其底层基础设施，包括硬件和数据中心的物理和环境安全性，以便客户能够利用这些认证并直接使用固有的控制措施。

在传统数据中心，常见合规性活动通常是需要手动定期执行的活动。这些活动包括验证资产配置和报告管理活动。此外，生成的报告甚至尚未发布就已过时。通过在亚马逊云科技环境中运行，客户可以利用嵌入式自动化工具（如 AWS Security Hub、AWS Config 和 AWS CloudTrail）来验证合规性。这些工具可以减少执行审计所需处理的工作量，因为这些任务已经成为持续自动执行的常规活动。由于花费在需要手动执行的活动上的时间减少，您可以帮助公司将合规性角色从必要的管理负担变成管理风险和改善安全状况的角色。

延伸阅读

有关更多信息，请参阅以下资源：

有关以下内容的信息...	请参阅
关于 AWS 云安全性的关键主题、研究领域和培训机会	亚马逊云科技云安全性学习
Amazon Web Services Cloud Adoption Framework，指导客户重点关注六大方面：业务、人员、监管、平台、安全、运营	Amazon Web Services Cloud Adoption Framework
AWS 上部署的特定控制措施；如何将 AWS 集成到您现有的框架中	《Amazon Web Services：风险与合规性》
安全、身份与合规性的最佳实践	安全、身份与合规性的最佳实践
安全性支柱 – Amazon Well-Architected Framework	安全性支柱 – Amazon Well-Architected Framework

文档修订

要获得有关此白皮书的更新通知，请订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
已更新白皮书	针对链接进行了更新以供延伸阅读。	2021 年 11 月 11 日
已更新白皮书	针对最新服务、资源和技术进行了更新。	2020 年 1 月 22 日
初次发布	发布了亚马逊云科技安全性简介。	2015 年 7 月 1 日

声明

客户负责对本文档中的信息进行独立评估判断。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。