AWS 白皮書

AWS 安全簡介

AWS 安全簡介: AWS 白皮書

Table of Contents

摘要 1
摘要 1
AWS 基礎架構安全 2
安全產品和功能 3
基礎架構安全 3
庫存和組態管理 3
資料加密 4
身分與存取控制 4
監控和記錄 4
AWS Marketplace 中的安全產品 5
安全指導 6
合規 8
深入閱讀 9
文件修訂 10
聲明 11

AWS 安全簡介

發佈日期：2021 年 11 月 11 日 (文件修訂)

摘要

Amazon Web Services (AWS) 提供了一個實現高可用性和可靠性的可擴展雲端運算平台，並提供方便您執行各種應用程式的工具。對 AWS 而言，協助您保護系統和資料的機密性、完整性和可用性，和讓您保有信任和信心一樣至關重要。本文件旨在提供 AWS 安全方法簡介，包括 AWS 環境中的控制項，以及 AWS 提供的某些產品和功能，從中協助客戶符合其安全目標。

AWS 基礎設施安全

AWS 基礎架構是現今最具彈性且最安全的雲端運算環境之一。其設計旨在提供可極度擴展、高度可靠的平台，讓客戶能夠快速又安全地部署應用程式和資料。

此基礎架構不僅是根據安全最佳實務和標準來建置和管理，且設計時也考量到雲端的獨特需求。AWS 使用冗餘的分層控制、持續驗證與測試、以及大量的自動化來確保全年無休的監視和保護基礎架構。AWS 確保會在每個新的資料中心或服務中複製這些控制項。

資料中心和網路架構都是為滿足客戶最敏感的安全要求而建置，而所有的 AWS 客戶均能從這樣的資料中心和網路架構中獲益。換句話說，您可獲得一個專為高度安全而設計的彈性基礎架構，而且沒有傳統資料中心的資本支出和營運費用。

AWS 在共同安全責任模型之下運作，其中 AWS 負責基礎雲端架構的安全，而您負責保護在 AWS 中部署的工作負載 (圖 1)。這賦予您針對 AWS 環境中的業務功能，實作大部分適用安全控制項所需的彈性和敏捷性。您可以對處理敏感資料的環境嚴格限制其存取，或針對想要公開的資訊部署比較不嚴格的控制項。

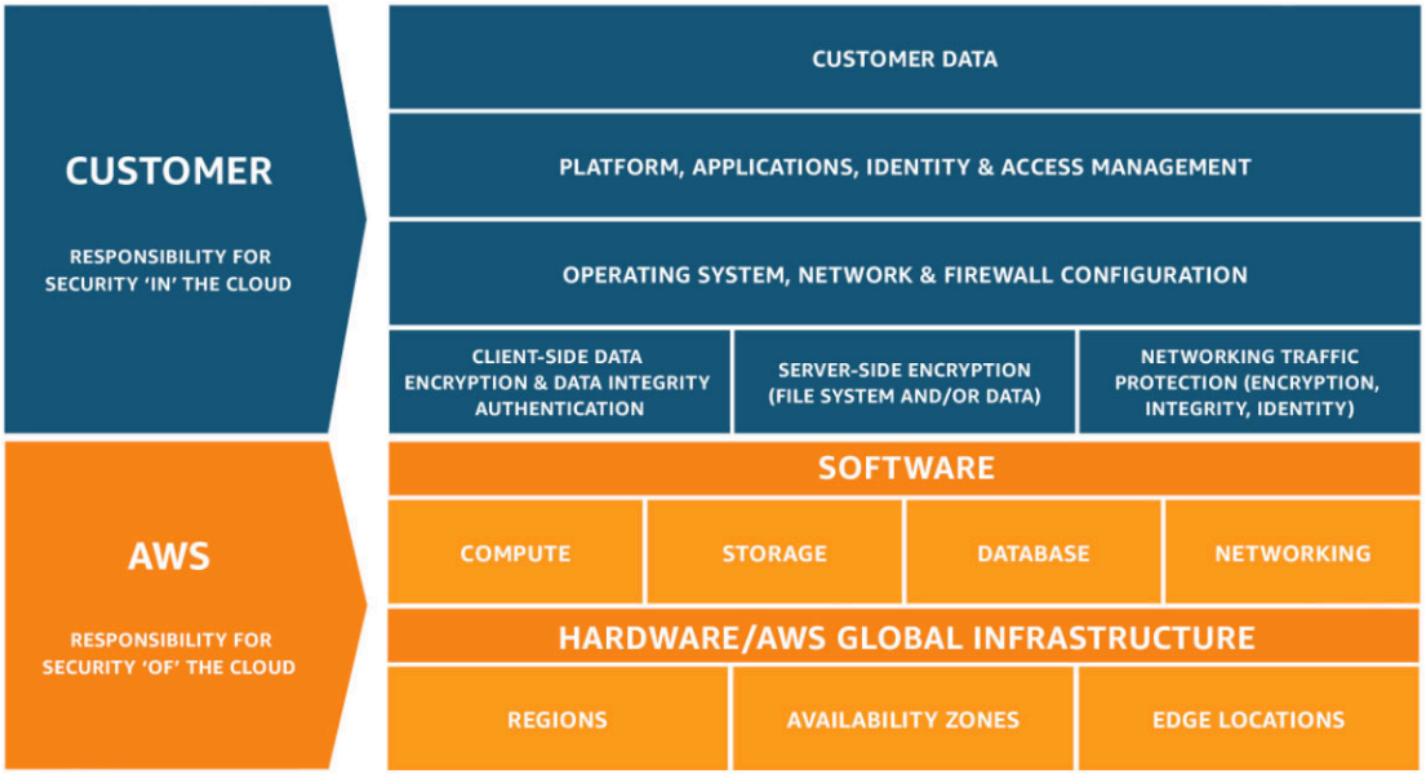

圖 1：AWS 共同安全責任模型

安全產品和功能

AWS 及其合作夥伴會提供各種工具與功能，協助您達成心目中的安全目標。這些工具可反映您在內部部署環境中部署的熟悉控制項。AWS 提供了安全專屬工具與功能，涵蓋網路安全、組態管理、存取控制及資料安全。此外，AWS 還提供監控和記錄工具，讓您完全掌握您的環境中所發生的一切事情。

主題

- 基礎架構安全
- 庫存和組態管理
- 資料加密
- 身分與存取控制
- 監控和記錄
- AWS Marketplace 中的安全產品

基礎架構安全

AWS 提供數種安全功能和服務，以提升隱私保護及控制網路存取。其中包括：

- Amazon VPC 內建的網路防火牆可讓您建立私有網路及控制執行個體或應用程式的存取。客戶可以跨 AWS 服務透過 TLS 控制傳輸中的加密。
- 連線選項可以讓您從辦公室或內部部署環境進行私有或專用連線。
- 套用於第 3 層或 4 層，同時也套用於第 7 層的 DDoS 緩解技術。這些技術可作為應用程式和內容交付策略的一部分。
- 自動對 AWS 安全設施之間 AWS 全域和區域性網路上的所有流量進行加密。

庫存和組態管理

AWS 提供的各種工具可讓您快速移動，同時仍可讓您確保雲端資源符合組織的標準和最佳實務。其中包括：

- 部署工具，用以根據組織標準來管理 AWS 資源的建立和除役。
- 庫存和組態管理工具，用以識別 AWS 資源，然後隨時間追蹤及管理這些資源的變更。
- 範本定義和管理工具，用以建立 EC2 執行個體的標準、預先設定、強化虛擬機器。

資料加密

AWS 讓您能夠為雲端中的靜態資料新增安全層，並提供可擴展且有效的加密功能。其中包括：

- 大多數 AWS 服務中可用的靜態資料加密功能，服務包括 Amazon EBS、Amazon S3、Amazon RDS、Amazon Redshift、Amazon ElastiCache、AWS Lambda 和 Amazon SageMaker
- 彈性的金鑰管理選項可，包括 AWS Key Management Service，可讓您選擇由 AWS 管理加密金鑰或由您完全控管自己的金鑰
- 使用 AWS CloudHSM 的專用、硬體型密碼編譯金鑰儲存，可協助您滿足合規要求
- 已加密的訊息佇列，可供使用 Amazon SQS 的伺服器端加密 (SSE) 進行敏感資料傳輸

此外，AWS 為您提供了 API，供您將加密和資料保護與您在 AWS 環境中開發或部署的任何服務整合在一起。

身分與存取控制

AWS 讓您能夠定義、強制執行及管理跨 AWS 服務的使用者存取政策。其中包括：

- AWS Identity and Access Management (IAM) 可讓您使用跨 AWS 資源的許可、適用於特殊許可帳戶的 AWS Multi-Factor Authentication (包括軟體和硬體型驗證器)，定義個別的使用者帳戶。IAM 可讓您使用現有的身分系統 (例如 Microsoft Active Directory 或其他合作夥伴產品)，對員工和應用程式授與 AWS Management Console 和 AWS 服務 API 的聯合存取權。
- AWS Directory Service 可讓您整合及聯合企業目錄，以降低管理費用及改善使用者體驗。
- AWS Single Sign-On (AWS SSO) 可讓您集中管理在 AWS Organizations 中所有帳戶的 SSO 存取和使用者許可。

AWS 提供其多項服務的原生身分和存取管理整合，以及與您自有應用程式或服務的 API 整合。

監控和記錄

AWS 提供各項工具和功能，讓您能夠查看 AWS 環境中所發生的一切事情。其中包括：

- 使用 AWS CloudTrail，您可以取得帳戶的 AWS API 呼叫歷史記錄，包括透過 AWS Management Console、AWS 開發套件、命令列工具和更高等級 AWS 服務發出的 API 呼叫，以便監控雲端的 AWS 部署。您也可以識別哪些使用者與帳戶呼叫 AWS API 來取得支援 CloudTrail 的服務、發出呼叫的來源 IP 地址，以及發生呼叫的時間。

- Amazon CloudWatch 提供可靠、可擴展的彈性監控解決方案，可讓您在短時間內立即上手使用。您再也不需要設定、管理和擴展自己的監控系統與基礎架構。
- Amazon GuardDuty 是威脅偵測服務，可持續監控惡意活動和未經授權的行為，以保護 AWS 帳戶和工作負載。Amazon GuardDuty 透過 Amazon CloudWatch 公開通知，以便您觸發自動化回應或通知相關人員。

這些工具和功能讓您可以在問題影響業務之前發現它們，使您改善安全狀態，並降低環境的風險狀況。

AWS Marketplace 中的安全產品

將生產工作負載遷移到 AWS 可以協助組織提高敏捷性、可擴展性、創新和成本節約，同時維護安全環境。AWS Marketplace 提供領先行業的安全產品，其會與您內部部署環境中的現有控制同等、相同或與整合。這些產品可補充現有的 AWS 服務，讓您能夠在雲端和內部部署環境中部署全方位的安全架構，以及擁有更流暢的體驗。

安全指導

AWS 透過本身及其合作夥伴提供的線上工具、資源、支援和專案服務，為客戶提供指導和專業知識。

AWS Trusted Advisor 是一項線上工具，如同客製化的雲端專家，可協助您設定資源以遵循最佳實務。Trusted Advisor 會檢查 AWS 環境，協助您消除安全落差及尋找節省金錢、改善系統效能及增加可靠性的機會。

AWS Account Teams 提供第一個聯絡點，引導您進行部署和實作，然後將您指向適當的資源，以解決您可能遇到的安全問題。

AWS Enterprise Support 提供 15 分鐘的回應時間，可經由電話、聊天或電子郵件提供全年無休的支援，並配有專屬技術客戶經理。這項專員服務可確保盡可能迅速地解決客戶的問題。

AWS 合作夥伴網路提供數百種領先業界的產品，這些產品與您內部部署環境中的現有產品在功能上相當、相同或者可以相互整合。這些產品可補充現有的 AWS 服務，讓您能夠在雲端和內部部署環境中部署全方位的安全架構，以及擁有更流暢的體驗，而全球有數百個經過認證的 AWS 諮詢合作夥伴可協助您符合安全和合規需求。

AWS 專業服務包含安全、風險和合規專業實務，可協助您在將最敏感的工作負載移轉至 AWS 雲端時建立信心和技術能力。AWS 專業服務可協助客戶根據備受證實的設計來發展安全政策和實務，並協助確保客戶的安全設計符合內部和外部合規要求。

AWS Marketplace 是包含了獨立軟體開發廠商的數千種軟體列表的數位目錄，易於尋找、測試、購買與部署運作於 AWS 上的軟體。AWS Marketplace 安全產品可補充現有的 AWS 服務，讓您能夠在雲端和內部部署環境中部署全方位的安全架構，以及擁有更流暢的體驗。

AWS 安全公告提供有關目前漏洞和威脅的安全公告，並讓客戶能夠與 AWS 安全專家一起解決報告濫用、漏洞和滲透測試等問題。我們也有適用於漏洞報告的線上資源。

AWS 安全文件顯示如何設定 AWS 服務，以滿足您的安全性和合規性目標。AWS 的客戶能從資料中心和網路架構中獲益，這些都是專為最重視安全的組織而建置。

AWS Well-Architected Framework 可協助雲端架構師建置安全、高效能、有彈性又有效率的應用程式基礎設施。AWS Well-Architected 架構包含著重保護資訊和系統的安全支柱。重要主題包括資料的機密性和完整性、透過權限管理來識別和管理有哪些人員可以執行哪些工作、保護系統，以及建立控制項以偵測安全事件。客戶可以從 AWS Management Console 使用 AWS Well-Architected Tool 服務，或利用其中一個 APN 合作夥伴的服務來協助他們。

AWS Well-Architected Tool 會協助您審查工作負載的狀態，並與最新的 AWS 架構最佳實務相互比較。在回答一組有關卓越運營、安全、可靠性、效能效率和成本最佳化的問題之後，可以在 AWS Management Console 中取得這項免費工具。AWS Well-Architected Tool 會隨即提供一個計劃，規劃如何使用所制定的最佳實務來針對雲端建構。

合規

AWS 合規可讓客戶了解 AWS 在維護 AWS 雲端安全和保護資料方面所具備的強大控制能力。當系統內建於 AWS 雲端時，AWS 與客戶會分擔合規責任。AWS 運算環境經過持續稽核，獲得來自各地區和行業認證機構的認證，包括 SOC 1/SSAE 16/ISAE 3402 (之前稱為 SAS 70)、SOC 2、SOC 3、ISO 9001 / ISO 27001、FedRAMP、DoD SRG 和 PCI DSS Level 1.i。此外，AWS 還提供保證計劃，提供範本和控制映射，以協助客户建立其在 AWS 上所執行環境的合規性。如需計劃的完整清單，請參閱 AWS 合規計劃。

我們可以確認所有 AWS 服務均在符合 GDPR 規範的情況下使用。這表示，除了受惠於 AWS 為了維護服務安全而已經採用的所有措施以外，客戶還可將 AWS 服務部署為其 GDPR 合規計劃的一部分。AWS 提供符合 GDPR 的資料處理增補合約 (GDPR DPA)，讓您能夠遵守 GDPR 的合約義務。AWS GDPR DPA 整合於 AWS 服務條款，並自動套用到所有需要它來符合 GDPR 的全球客戶。Amazon.com, Inc. 已依據「歐美隱私保護盾」協議 ((EU-US Privacy Shield) 取得認證，而 AWS 則涵蓋在此認證之下。這可協助選擇將個人資料轉移到美國的客戶符合其資料保護義務。在「歐美隱私保護盾」 (EU-US Privacy Shield) 網站上可找到 Amazon.com Inc. 的認證：https://www.privacyshield.gov/list

在認可的環境中運作，客戶可縮小其必須執行稽核的範圍和成本。AWS 會持續經歷其基礎架構的評估 (包括其硬體和資料中心的實體和環境安全)，因此客戶可以利用這些認證且只要繼承這些控制項即可。

在傳統資料中心，常見的合規活動通常為定期的手動活動。這些活動包括驗證資產組態及報告系統管理活動。此外，結果產生的報告甚至會在發佈前過時。在 AWS 環境中運作，客戶即可利用內嵌的自動化工具來驗證合規性，例如 AWS Security Hub、AWS Config 和 AWS CloudTrail。這些工具可減少執行稽核所需的付出，因為這些任務會變成例行、持續和自動的任務。在手動活動上花費較少時間，有助於將貴公司的合規角色從其中一個必要系統管理負擔，演變成可管理風險及改善安全狀態的角色。

深入閱讀

如需其他資訊，請參閱以下資源：

如需相關資訊...	請參閱
AWS 上雲端安全的重要主題、研究領域及培訓機會	AWS 雲端安全學習
AWS 雲端採用架構可將指導方針整理成六大重點領域：業務、人員、治理、平台、安全和操作	AWS 雲端採用架構
在 AWS 設置特定控制項；如何將 AWS 整合到現有架構中	Amazon Web Services：風險與合規
安全、身分與合規性最佳實務	安全、身分與合規性最佳實務
安全支柱 - AWS Well-Architected Framework	安全支柱 - AWS Well-Architected Framework

文件修訂

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

update-history-change	update-history-description	update-history-date
白皮書已更新	更新深入閱讀的連結。	2021 年 11 月 11 日
白皮書已更新	針對最新的服務、資源和技術進行更新。	2020 年 1 月 22 日
初次出版	發佈 AWS 安全簡介。	2015 年 7 月 1 日

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 協議之約束，且本文件並不屬於 AWS 與其客戶間之任何協議的一部分，亦非上述協議之修改。