2023 年 11 月

機密運算 SI 支援套件

系統整合商如何利用 Intel 解決方案因應客戶的業務挑戰

什麼是機密運算？

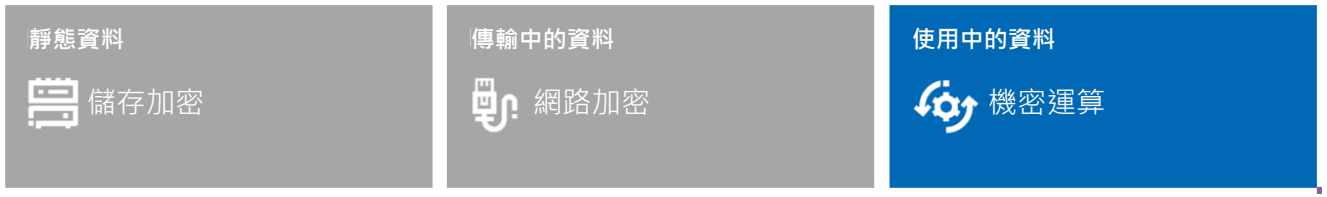
什麼是機密運算？

機密運算允許使用敏感資料擷取深入解析或訓練 AI 模型，而無須將資料暴露給其他軟體、合作者或雲端供應商
這開啟了無窮的可能性，可讓企業善加利用以前過於敏感或受監管的資料，進行分析和其他目的

機密運算軟體市場預計將是**規模最大**且**成長最快的市場區隔**，緊接在後的則是硬體與服務

短短幾年內，**機密運算作為一種為使用中的程式碼與資料提供端對端保護的強大新方法，獲得了廣泛的關注與氣勢如虹的發展衝勁**

機密運算的需求
填補資料保護持續性的重大缺口

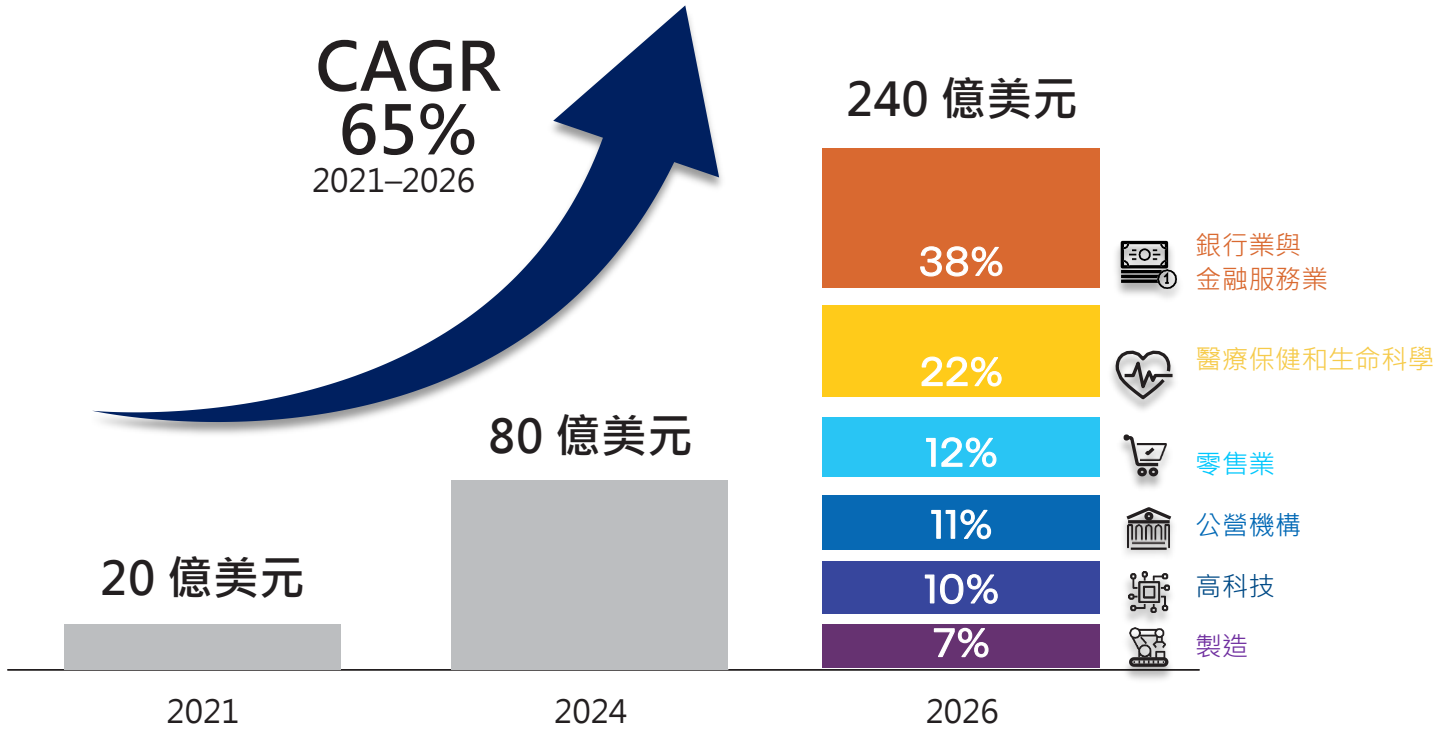


Everest Group®

Everest Group 認為：
「資料安全性的下一個新領域……即將實現指數級成長。」
2021 年價值為 19 億美元的全球市場在雲端與安全性專案的推動下，預計到 2026 年將以 40% 至 95% 的複合年成長率成長。

機密運算市場預測

預計將在雲端安全性與隱私保護多方運算的推動下，實現指數級成長



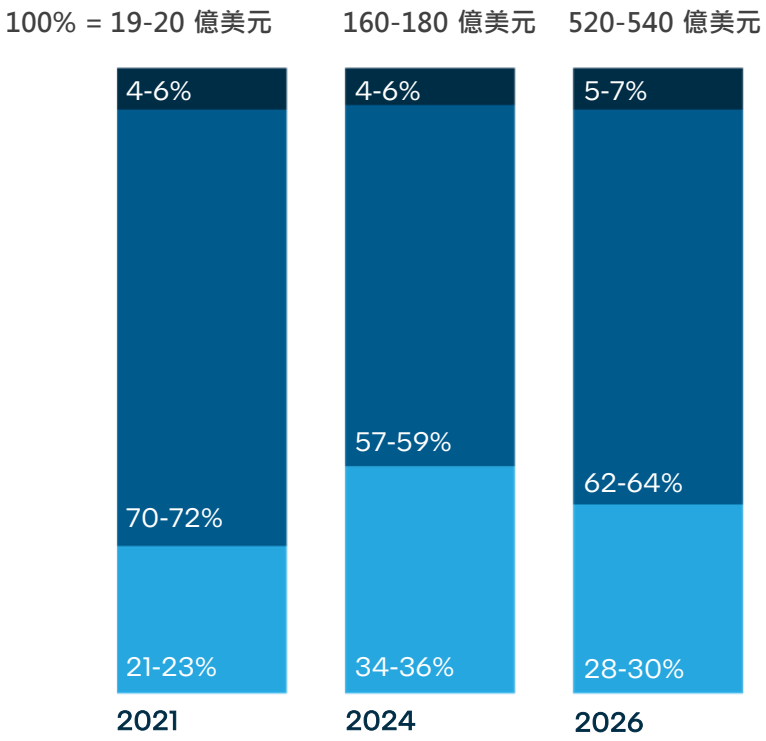
網路資料中心市場
深入解析

來源：2021 年機密運算聯盟

機密運算市場

機密運算軟體市場預計將是規模最大且成長最快的市場區隔，緊接在後的則是硬體與服務

機密運算 TAM，依技術領域劃分
百分比，2021-26 日曆年度



硬體 軟體 服務

服務子市場區隔 CAGR = 100-105%

全球系統整合商（貢獻率百分比）	ISV 的內部服務實務（貢獻率百分比）
8-10%	90-92%

- 服務仍侷限於早期驗證概念，解決方案或服務產品最少
- 大部分服務需求可能由 ISV 的內部服務實務來滿足

軟體子市場區隔 CAGR = 90-95%

雲端服務供應商（貢獻率百分比）	支援軟體 ISV（貢獻率百分比）
83-85%	15-17%

- 支援軟體市場區隔包含用於採用及管理 TEE，以及採 TEE 為基礎的應用程式的技術
- 隨著市場的成熟，支援軟體的貢獻預計會上升
- 假設 2021 年 CSP 的定價溢價為一般運算的 1.5-2 倍，並且隨著時間推移進行標準化

硬體子市場區隔 CAGR = 100-105%

矽晶片組 OEM（貢獻率百分比）	組裝伺服器 OEM（貢獻率百分比）
51-53%	47-49%

- 由於機密運算與一般運算相比，運算硬體的定價差異有限或沒有差異，因此將繼續推動需求
- 由於雲端環境的採用率增加，預計 2024 年後，矽晶片組的貢獻率將超越組裝伺服器市場

檢視完整報告：https://bit.ly/3GofM1d

機密運算成果

在確知掌握主控權的情況下移轉至雲端及啟用資料

即使包含機密或受監管的資料也不例外

RBC Bank / Microsoft Azure

與多方合作，進行有益的共享分析

同時維護隱私並遵循法規

Novartis / BeeKeeperAI

加強法規遵循與資料主權計畫

利用技術防護措施

Deutsche Telekom Sovereign Cloud

強化應用程式安全性與 IP 保護

硬體型隔離與存取控制

「社群媒體與廣告巨頭」

機密運算

產業和使用案例

產業

使用案例

客戶案例研究

醫療保健

採用受監管資料的協作運算

BeeKeeperAI™ NOVARTIS

情境

Novartis Biome 開發罕見疾病的診斷模型與療法。罕見疾病的資訊稀少且分散於多家醫院和研究機構

挑戰

患者資訊具私密性且屬於高度監管。醫院不希望資料外流或將私人記錄揭露給 BeeKeeperAI 或 Novartis

解決方案

每家醫院現場安裝搭載 Intel® Software Guard Extensions (Intel® SGX) 的 BeeKeeperAI 節點，分析私人資料並更新雲端的主模型權重。Novartis 和 BeeKeeperAI 人員都無法看到或儲存受監管的健康記錄

BeeKeeperAI™

「[機密運算平台] 可讓我們將演算法驗證時間縮短一半，同時成本也幾乎減半。這些省下來的費用可讓我們更迅速地訓練、驗證可通則化的演算法，並將其更快推向市場。而且，隨著 CCP 基礎技術與流程的成熟，速度會變得更快，成本也會更低。」
BeeKeeperAI, Inc. 共同創辦人暨商務長 MaryBeth Chalk

白皮書

加速臨床人工智慧演算法的發展

客戶案例研究

高度安全性金鑰保護

Fortanix®

情境

快速激增的金鑰和憑證需要強大的保護與集中管理。HSM 解決方案要價不菲，雲端解決方案則仰賴 CSP 安全性與法規遵循

挑戰

建構具有類似 HSM 安全性、可擴充的軟體型金鑰管理系統，且在技術上與雲端主機隔離

解決方案

Fortanix 採用基於 Intel® SGX 的自主防禦 KMS 軟體，保護金鑰和憑證免受外部對手和雲端供應商的侵害，並協助確保機密始終處於擁有者的掌控中

Fortanix®

啟用 Intel® SGX 後維持高效能

實施多個執行個體設定，可顯著提高輸送量。啟用 Intel® SGX 後對這些效能增強功能的影響極小，這表示組織可以同時提高安全性與效能。

解決方案快照

機密人工智慧資料 Intel 安全解決方案 - Fortanix

PRC 客戶案例研究

挖掘資料價值

創鄰科技

情境

如何確保企業資料與隱私的安全性，是資料庫與硬體製造商常面臨的問題

挑戰

傳統資料加密技術僅對硬碟儲存與網路傳輸加密，其效力前提為伺服器控制權限並未洩露。如果伺服器的控制權遭到攔截，則第三方可能會竊取或修改使用中的資料

解決方案

創鄰科技與 Intel 聯合推出採用 Intel® SGX 記憶體加密的圖形資料庫資料加密解決方案。保證了 Galaxybase 的極致效能，進而打造記憶體安全的圖形資料庫產品

相信在 Intel® SGX 記憶體加密技術的協助下，創鄰科技打造的新一代圖形資料庫 Galaxybase 可為客戶提供高品質且更安全的資料服務，高效實現資料互連，讓企業以穩健的方式實現資料資產的價值。

新聞稿

利用機密運算實現主權登陸區域

Intel® Xeon® 可擴充處理器實現機密運算

Intel 的機密運算技術產品組合豐富，可讓組織選擇需要的安全等級，妥善滿足業務需求及符合監管規定

Intel 是唯一一家同時提供應用程式和 VM 層級機密運算解決方案的公司

intel　accenture　SCONTAIN

Intel、Accenture、Scone 和雲端服務供應商的強大實力，可實現：

- 業務轉型：COE 打造的專門用途解決方案設計
- 增強的機密性、完整性、一致性、可擴充性和彈性
- 安全無虞的登陸區域執行個體化，包括 Scone CAS 與安全防護機制
- 在部署管道各自的登陸區域，將管道自動部署到登陸工作負載

白皮書

Intel 為機密運算提供什麼

4 大事實：Intel 為機密運算打下根基

2018

Intel® Xeon® 處理器上的 Intel® Software Guard Extensions（Intel® SGX）是引進資料中心的第一個機密運算解決方案

300+

已與 Intel 合作開發及部署機密運算服務的組織

3 億美元

在 Intel® Xeon® 處理器上使用 Intel® SGX 部署之基礎架構的估計價值

4

全球雲端供應商承諾將於 2023 年在第 4 代 Intel® Xeon® 處理器提供 Intel® Trust Domain Extensions（Intel® TDX）

Microsoft Azure　IBM Cloud　Google Cloud　Alibaba Cloud

檢視影片：這裡

Intel 提供最全方位的安全產品組合

Intel® Software Guard Extensions (Intel® SGX)

應用程式隔離

Intel® Trust Domain Extensions (Intel® TDX)

虛擬機器隔離

Intel® Trust Authority

適用於多雲和混合雲的獨立信任驗證服務

軟體解決方案、雲端、OEM 與系統整合商生態系統

Intel 安全至上開發與生命週期支援

*特定雲端供應商提供 Intel® TDX

Intel® Trust Authority

利用私有雲安全機制讓零信任唾手可得，並且擁有公有雲的靈活彈性

Intel® Trust Authority 這個全新的軟體與服務產品組合，採用零信任原則，
為機密運算強化安全與保障機制
Intel® Trust Authority 的第一代提供證明可信賴執行環境（TEE）的獨立證明服務，
採用 (Intel® SGX) 與 (Intel® TDX)

既可實現零信任原則，又不會產生自行建置證明服務的成本，
還可降低複雜度

獨立

可擴充性

部署容易

進一步瞭解
機密運算支援套件

產品簡介

noname 案例研究

Thales 案例研究

Zscaler 案例研究

What That Means 影片

機密運算

適用於 Intel® SGX 的軟體與解決方案生態系

商業支援解決方案

自行打造

商業解決方案供應商

anjuna
cosmian
decentriq
EDGELESS SYSTEMS
CYBERNETICA
Fortanix
Mithril Security
Opaque
enclaive
SCONTAIN
HUB SECURITY
secretarium

精選的部署就緒容器（2023 年第 1 季整季）*

PyTorch
redis
scikit learn
Spark
TensorFlow

開發人員工具

GRAMINE
SCONE
Occlum
Mystikos
Teaclave
Open Enclave SDK
intel Intel SGX SDK

系統整合商

accenture
KPMG
Capgemini
IBM
Atos
leidos
avanade

Hypervisor (SGX)

KVM 5.13 及更新版本
vmware vSphere 8

* 於 Azure Marketplace 提供

Intel® TDX 可用性

Intel® TDX 可搭載於第 4 代 Intel® Xeon® 可擴充執行個體，可透過三大雲端供應商取得公開預覽

如需各雲端供應商產品選擇的詳細資訊，請按一下下方的圖誌

Microsoft Azure　Alibaba Cloud　Google Cloud

IBM Cloud
*公開預覽待公佈

以下客體作業系統供應商支援 Intel® TDX

Red Hat　SUSE　Canonical Ubuntu

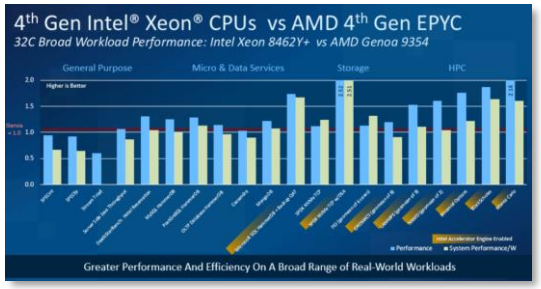
*Intel® TDX 於 2024 年透過第 5 代 Intel® Xeon® 可擴充處理器全面上市

競爭比較

	Intel® SGX	Intel® TDX	AMD SEV-SNP	AWS Nitro Enclaves	NVIDIA H100 GPU 上的機密運算
雲端基礎架構供應商的硬體/韌體、虛擬機器管理程式與雲端管理堆疊排除在信任邊界之外	●	●	●		●
透過多個雲端供應商提供，促進多方供應	●	●[1]	●		●
旨在適應低或無移植、重新設計或重新包裝的舊型應用程式		●	●		◎[2]
硬體真實性證明與正確的 TEE 啟動	●	●	●	●	●
TEE 中載入的軟體映像完整性證明	●	◎[3]	◎[3]	●	
機密資料僅由指定的應用程式代碼存取；VM 管理員、訪客作業系統、其他應用程式和雲端堆疊排除在存取之外	●				
無需虛擬化即可部署在「裸機」伺服器	●				●
硬體型加密記憶體完整性選項，提供額外的 Rowhammer 保護	●				
與代號為「Project Amber」的 Intel 獨立信任服務相容	●	●			
截至 2023 年 3 月的競爭資料來源			連結、連結	連結、連結、連結	連結

[1] Intel® TDX 執行個體將於 2023 年在特定雲端供應商上線；可用時間會有所不同
[2] 在 GPU 上執行的舊程式碼無變更或變更很少。使用 CPU 的部分工作負載必須包含搭載 CPU 的 TEE 和保護 PCIe 通訊的方法。
[3] 不是可用硬體技術的固有功能，但作為雲端或證明服務供應商提供的增值功能是可行的。

第 4 代 Intel® Xeon® 競爭力分析



第 4 代 Intel® Xeon® 可擴充處理器處理實際工作負載的效能超越競爭對手

intel XEON 相較於 EPYC AMD

第 4 代 Intel® Xeon® 可擴充處理器採用專為 CPU 最佳化的軟體，比 NVIDIA A100 GPU 快達 2.5 倍

intel XEON 相較於 NVIDIA

利用第 4 代 Intel® Xeon® 可擴充處理器，實現位居領先地位的資料中心效能

intel XEON 相較於 EPYC AMD

為什麼選擇 Intel 進行機密運算？

為什麼選擇 Intel 進行機密運算？

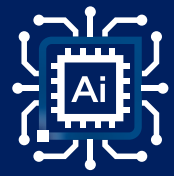
滿足不同安全性需求的技術選項

只有 Intel 提供應用程式隔離（Intel® SGX）和 VM 隔離（Intel® TDX），可讓客戶精確調整解決方案，滿足不同等級的安全性

廣大的解決方案生態系統

Intel 與數十家 ISV 和雲端供應商合作，提供託管服務與軟體解決方案，包括機密 AI、分析、區塊鏈、資料庫等

聯絡 Intel 和解決方案夥伴的專家



Intel 專家準備好利用解決方案架構、夥伴配對、POC 資源與部署疑難排解，為客戶提供幫助

與您的 PSAM 聯絡，獲得更多資訊

後續步驟

教育

瞭解機密運算的價值，以及許多終端使用者應用程式如何利用以確保環境安全並實現多方運算

顧客互動

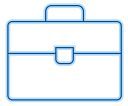
與您的 Intel PSAM 聯繫，深入瞭解生態系統中的 Intel 機密運算技術產品組合

Intel® 夥伴聯盟能如何協助

加入 Intel® 夥伴聯盟來開始

Intel® 夥伴聯盟會員資格為您提供專屬的業務擴展機會
（例如進入全球市場、進階訓練和促銷支援），
完全根據您的需求量身打造

訓練與技能

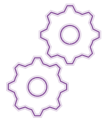


進入 Intel® 夥伴大學，
可獲得進階技術的專業訓練、
技能計畫和學習獎勵

行銷資源

進入 Intel 解決方案市場和
Intel 行銷工作室，協助您為
產品和服務創造更多需求

寶貴獎勵



為合格的活動賺取點數、
升級會員狀態，並取得其
他資源來拓展業務

如果您還不是夥伴
立即參加

會員福利

賺取點數

Intel® 夥伴聯盟最受歡迎且與眾不同的一大福利就是我們獎勵夥伴的點數，藉此表彰他們與 Intel 合作的業務成果，以及對高優先等級活動的踴躍參與。

Intel® 夥伴聯盟有超過 1,000 種賺取點數的方式以及超過 100 種兌換機會。

Cloud Insider 社群

Intel® Cloud Insider 社群提供持續更新、世界一流的雲端內容與工具。夥伴有機會與同行建立人脈，並與生態系統串連，將創新的共同雲端解決方案推入市場

進一步瞭解

產業深入解析

黃金級會員和鈦金級會員可以存取特別策劃的季度產業深入解析，讓業務更上一層樓

進一步瞭解

財務獎勵措施

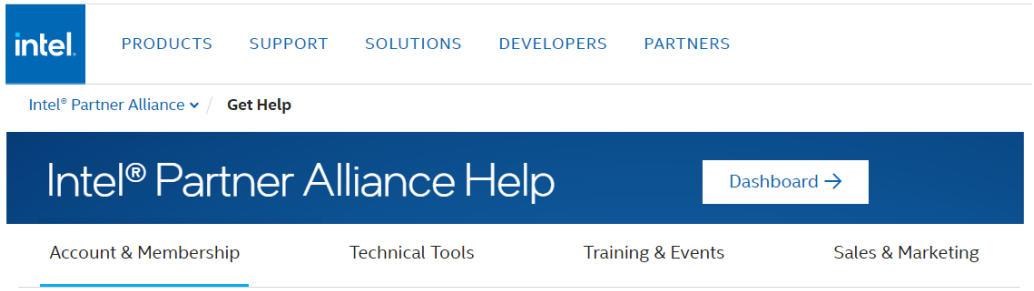
只要具備會員資格，即可利用強大的行銷開發基金與獎勵計畫，幫助您的產品行銷早日達成目標

請與您的 PSAM 聯絡，深入瞭解 Intel® 夥伴聯盟躍升計畫和更多財務獎勵措施

intel partner alliance
如何取得客戶支援

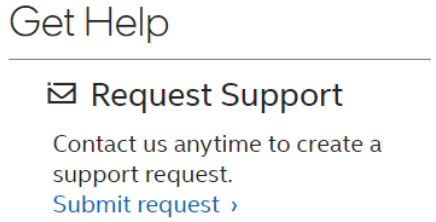
Intel Virtual Assistant
這個聊天機器人位於每個合作夥伴聯盟網頁右下角，為多數問題提供自助解答，或是即時支援代表的快速連結。

夥伴聯盟「取得協助」頁面
取得協助頁面針對多數工具提供詳細的自助指南，詳述合作夥伴聯盟會員享有的福利。



取得協助「滿版廣告」
提交線上支援要求。

這個連結位於合作夥伴聯盟網站多數網頁的頁尾。



相關資源

Cloud TV

Intel® Cloud TV 探索雲端運算最新消息、趨勢與策略，
助您一臂之力、馬到成功

雲端中的 Sapphire Rapids

瞭解如何保護雲端資產

雲端安全防護

雲端的安全性挑戰

機密運算
資訊與資源

30-3-30

機密運算 30-3-30

影片

機密運算概要

安全性是一項挑戰

新特色

資訊圖表

如何克服雲端安全性威脅

研究論文

保護新興 AI 工作流程中的資料與模型

技術文章

機密運算的現狀

雲端安全性簡介

部落格

效能與網路安全性的新典範

Intel 是安全性的起點

其他資源

效能指數

[第 4 代 Intel® Xeon® 可擴充處理器]

直播網路研討會

[雲端解決方案架構師（CSA）技術講座：利用第 4 代 Intel® Xeon® 可擴充處理器降低 TCO 並改善效率]

網路研討會錄製影音

[雲端解決方案架構師（CSA）技術講座：利用第 4 代 Intel® Xeon® 可擴充處理器加速關鍵工作負載]

其他訓練

[技能與認證]

機密運算
訓練連結

安全性訓練連結

課程/訓練

主題 - 目標族群
提高網路安全性韌性的 3 大技術 開發維運、雲端架構師 – 機密運算
物聯網解決方案的端對端安全 DevOps
邊緣到雲端安全性 開發維運、雲端架構師
虛擬私有雲、雲端網路與雲端安全性 DevOps
Intel® 產品與解決方案的安全價值 全部
保護雲端中的應用程式 DevOps
雲端運算的安全性 DevOps/雲端架構設計師

主題 -目標族群
虛擬私有雲、雲端網路與雲端安全性 開發維運、雲端架構師
商務對話的安全性 雲端架構師、高階主管
Intel 架構的加密入門指南 DevOps
Intel® 產品與解決方案的安全價值 開發維運、雲端架構師


intel

備份

機密運算

關鍵 AI 使用案例

多方機器學習

利用機器學習的威力，而不損害敏感客戶資料的機密性與隱私

企業簡介

採用機密運算的多方機器學習在以下領域尤其有用：

醫療保健

利用資料的威力進行更進階的研究，而無須公開機密的患者資訊

金融服務業

可以更佳預測潛在的詐欺活動，同時打擊洗錢和資助恐怖主義

Intel 的安全優先承諾

「產品的安全性是我們的優先要務之一。我們致力於設計、製造及銷售全球最安全的技術產品，並且持續創新及增強產品的安全功能。」

執行長 Pat Gelsinger

93%

2022 年處理的漏洞中有 93% 直接源於 Intel 在產品安全性保障方面的投資

56%

2022 年發佈的 243 個 CVE 中有 56% 是由 Intel 員工在內部發現

93%

自 2019 日曆年的首份產品安全性報告以來，發佈的所有 CVE 中平均有 93% 來自 Intel 在產品安全性保障方面的投資

85%

2022 年外部研究人員報告的 106 個漏洞中有 85% 的漏洞（即 90 個漏洞）都是透過 Intel Bug Bounty Program 回報

檢視完整報告：這裡

第 4 代 Intel® Xeon® 競爭力分析

主流運算領導地位

75%
更高的效能

50%
更高的效能/瓦數

20%
節約的二氧化碳公斤數與
節省的擁有權總成本

AI 領導地位

80%
推斷傳輸量更高

HPC 領導地位

40%
在各個工作負載
展現更高的效能

按一下瞭解雲端事實