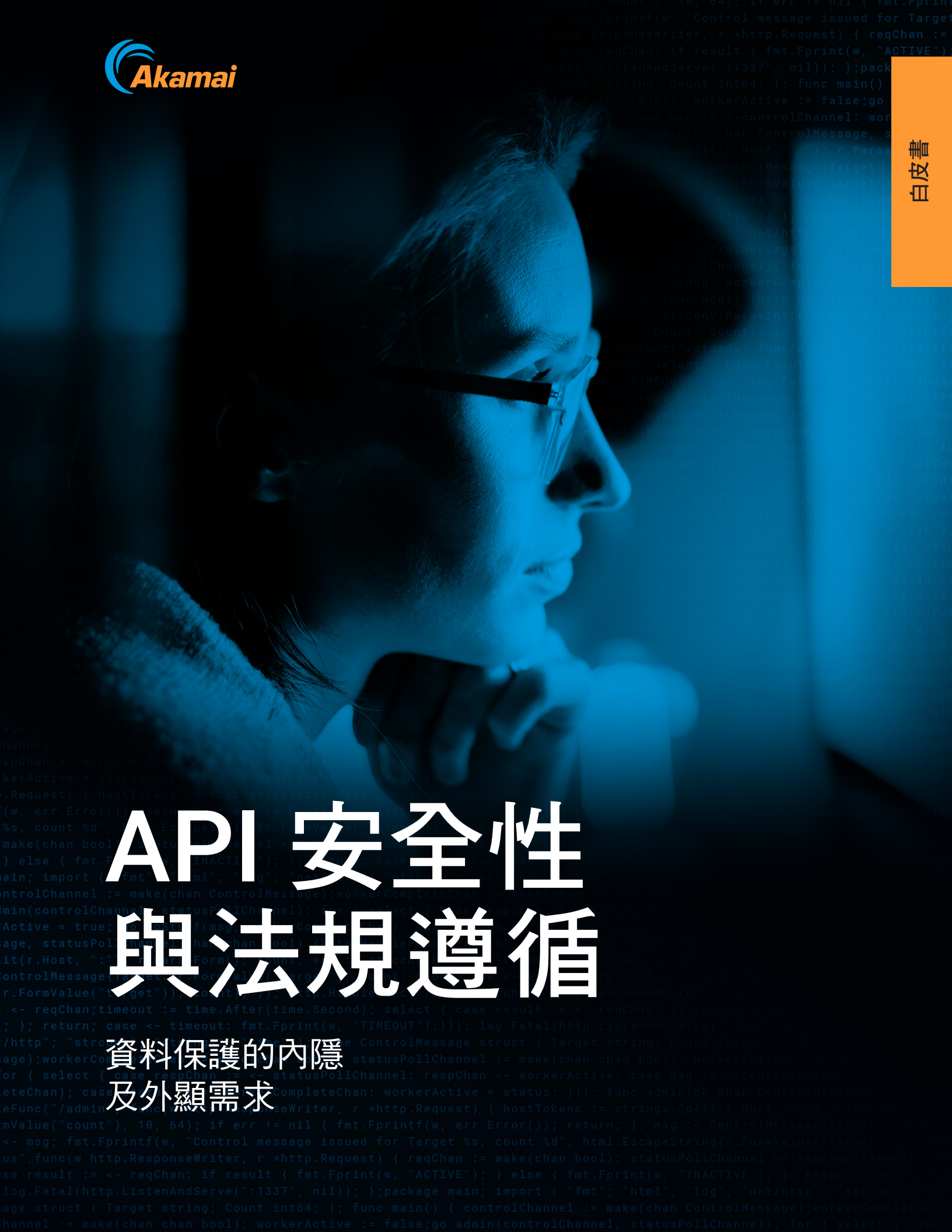
Akamai

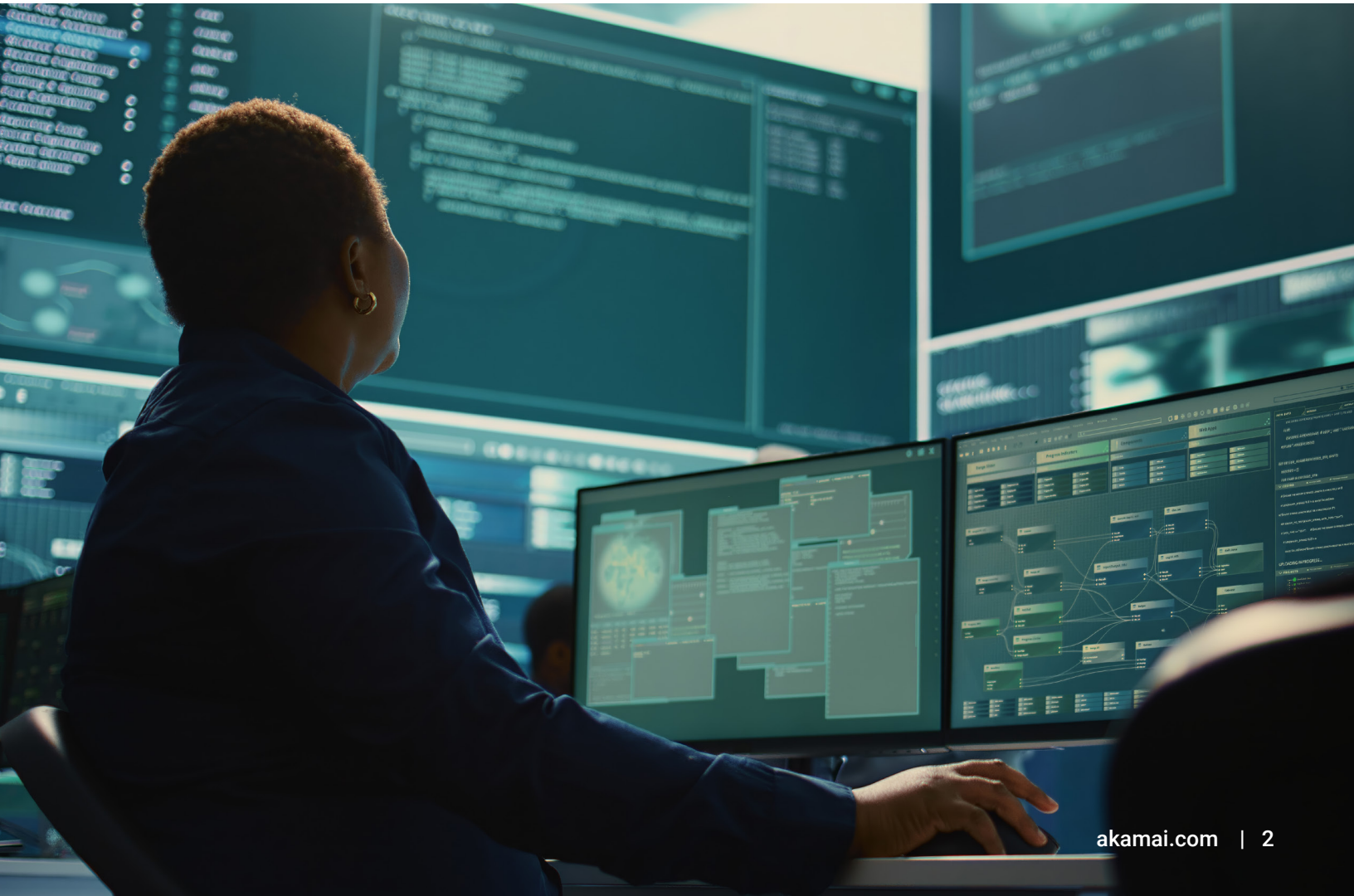
白皮書



API 安全性與法規遵循

資料保護的內隱及外顯需求

本報告內容



引言

傳統上，為了確保能符合資料保護法規，就需要花費大量心力和資源，以應對最常見的風險。但這種情況正在改變。現今的攻擊面正在快速進化，涵蓋了許多企業法規遵循計劃無法應對的威脅。部分原因在於監管機關難以跟上快速演變的攻擊技術，因此無法明確列出避免遭受入侵需要涵蓋的所有層面。

API 保護也遇到了這個狀況。每次客戶、合作夥伴或供應商以數位方式與您的企業互動時，都會有 API 在幕後快速處理資訊交換，其中往往包含機密資料。攻擊者現在意識到他們可以簡化策略，直接鎖定 API 來竊取資料。

法規中的許多措辭已經開始指出需要清查、評估或保護 API。而雖然法規尚未明確列出 API 專屬條款，由於 API 已經成為明確的攻擊方向，這就*表示*您必須有足夠的保護。

API 成為主要的法規遵循問題並不讓人意外。公開或設定錯誤的 API 相當常見、容易出現破口且通常未受到保護。只要任何一個 API 遭到入侵，就可能導致數百萬筆記錄遭竊。數字會說話：

- 百分之七十八的企業曾遭遇到 API 安全事件。[1]
- 百分之四十四曾經因為 API 安全事件遭到監管機關罰款。[2]

這對您的法規遵循計劃有何影響？監管機關需要看到您的企業正在採取措施，保護所有機密資料的存取點。這表示您必須證明您的企業可以：

- 掌握每個 API，包括難以察覺的地下 API
- 找出並修正所有 API 弱點
- 採用量身打造的控制措施，避免發生以 API 為中心的資料外洩

本白皮書將深入探討 API 風險日益增長的原因，強調六個涉及 API 保護的法規與架構範例 (無論是明確規定或間接要求)，並提供透過 API 安全最佳實務達到合規要求的建議。

1., 2. Akamai Technologies，《API 安全性歧見》，2023

瞭解 API 風險

API 位於企業數位產品、服務和雲端環境的核心。它對資料的持續存取雖然可推動營收成長，但也提高了營運風險。問題在於，大多數的企業，即使擁有成熟的安全計劃，也並沒有將 API 相關威脅的優先順序排到與網路釣魚或勒索軟體等其他威脅相等的程度。

有些企業仰賴 API 閘道與網路應用程式防火牆 (WAF) 提供基本的 API 保護，但這些工具的設計無法提供專業 API 安全解決方案所能提供的可視性、即時防護及持續測試能力。以下是這些工具不足以應對風險的原因：

- API 閘道和 WAF 只能觀察由這些閘道路由的*受管理* API 流量。
- 他們無法保護未受管理的 API，而根據分析師的預測，到 2025 年時，一般企業 API 生態系統中幾乎會有近一半是未受管理的 API。
- 因此，資安團隊並未做好充分準備，無法保護攻擊面中擴展最快的部分，並不十分清楚 API 的路由位置、設定方式，會交換哪些機密資料，以及其所造成的風險。

對監管機關來說，保護使用者資訊是最優先的要務，如果企業無法合理保護客戶的資料免於未經授權的存取，就會被處以嚴重的罰款。每 10 位擁有完整 API 清查資料的資安專家中，只有 4 位知道哪些 API 會傳回機密資料[3]，而且許多 API 呼叫都來自攻擊者試圖測試弱點，因此透過 API 進行資料駭侵情況只會不停增加，尤其是 API 攻擊目前相當容易執行。

3. Akamai Technologies，《API 安全性歧見》，2023

四種與法規遵循相關的 API 攻擊

API 漏洞會如何影響公司的法規遵循狀態？以下為幾個範例：

- 攻擊者利用缺乏驗證控制的 API 端點，入侵了熱門的專案管理應用程式。攻擊者入侵 API 後，未經授權即取得了數百萬名使用者的資訊，並在數個月後，在網際網路上洩漏了超過 21 GB 的資料，包括電子郵件地址和董事會成員等。
- 根據報導，某家大型電信公司超過 1,100 萬筆客戶記錄遭到暴露，報導指出這是因為有一個 API 暴露於網際網路中卻沒有被發現，而且它不需要驗證。攻擊者入侵這個 API，發現它沒有唯一識別碼，猜出它的 ID 號碼，輕易地要求到敏感資料。
- 據報導，一家社群媒體公司近年來因為不當使用 API，導致受到兩次資料擷取攻擊。在第一次攻擊中，有 5 億筆使用者檔案中的隱私資料遭到擷取和出售。在第二次攻擊中，攻擊者建立了一個資料庫，包括從 7 億名使用者擷取的電話號碼和薪資資料。
- 相同的攻擊手法也發生在其他社群媒體公司上，導致數百萬使用者的資料遭竊。由於第三方廠商使用該公司的 API 收集敏感資料，該公司遭到 50 億美元的罰款。罰款的重點原因並不是廠商濫用 API，而是該公司*本身*並未監控其應用程式。

六個與 API 安全性相關的法規與架構範例

在許多法規與架構中，並未明文指定 API，但其規定明確地重視保護應用程式和基礎架構，而這正是 API 運作所在。舉例來說：

- 「支付卡產業資料安全標準」(PCI DSS) v4.0 提供指引，確保企業的軟體能安全使用外部元件的功能。其中包括將付款資料從行動應用程式傳輸至銀行系統的 API。
- NIST 安全軟體開發架構為打造防禦良好的軟體提供指南，確保其持續性與對弱點的應對能力。API 位於軟體開發的核心。

在許多情況下，法規雖然沒有明確定義保護資料的目標，但例如「一般資料保護法規」(GDPR) 等法規會要求企業採取「適當的安全措施」。您的 API 每天可能會收到數百萬次來自客戶*和*攻擊者的呼叫，要求提供資料。您必須判斷需要使用哪些安全控制，然後證明這些控制有達到成效。

讓我們深入看看對 API 生態系統有直接影響的法規和架構。

1. PCI DSS v4.0

PCI DSS 由支付卡產業安全標準協會所訂定，已成為保護付款資料的全球標準。如果貴公司接受主要的信用卡，並以電子方式處理、儲存或傳輸持卡人資料，您就必須遵守其規定。

2006 年 PCI DSS 發布時的原始版本規定涵蓋了一些重要的安全原則，至今依然非常重要，例如根據「需要知道」的基礎，指派系統與持卡人的資料存取權限，以及根據依角色定義存取等。

然而，隨著 PCI DSS v4.0 生效，企業必須調整其法規遵循計劃，以應對經常鎖定支付技術中數千個 API 的威脅發動者。整體而言，PCI DSS v4.0 著重於四個主要目標：

1. 持續滿足支付產業的安全需求
2. 強調安全是持續不斷的過程
3. 為企業提供滿足要求的彈性 (例如新工具和新控制措施等)
4. 強化驗證方法與程序

PCI DSS v4.0 要求 6.2.3 著重於企業必須審查其客製化的應用程式代碼 (也就是由第三方廠商開發的程式碼，而非標準的市售現成應用程式)，以確保不會將弱點帶入生產環境。就 API 具體而言，這項要求提供了一個方向，需要確定企業的軟體是否能安全地使用外部元件的功能 (程式庫、框架和 API 等)。這樣的要求強調了 API 在廣泛軟體供應鏈中所扮演的關鍵角色，以及保護 API 的重要性。

在現代應用程式環境中，API 已成為連線和資料交換的預設方法。因此，在上線前 (左移式) 和上線後 (右移式) 都能妥善保護 API，就是讓數位業務能夠抵禦攻擊的關鍵。以下是一些達成 6.2.3 要求的 API 安全性最佳實務：

- 確認 API 元件的使用情形及其資安布局 (例如找出導致弱點的組態錯誤，包括使用弱式加密方式等)。
- 驗證 API 的正常及預期使用狀況，並實施控制措施，阻止可疑行為者濫用您的系統 (例如檢查應用程式行為以偵測邏輯弱點)。
- 偵測用於驅動 API 的第三方架構，判斷是否有任何過時且易受攻擊的架構。
- 建立所有 API 的完整清查，包括正在執行的不同版本。這可讓您了解是否有後門存在，以及您需要管理的潛在未記錄功能。
- 驗證 API 程式碼的安全性，避免讓任何 API 相關的弱點進入生產環境。
- 為 API 導入安全程式編寫最佳實務，讓您採用程式化的方法，持續安全地交付程式碼。

2. 一般資料保護法規 (GDPR)

GDPR 是一項歐盟 (EU) 的法規，目的在強化並統一歐盟內的個人資料保護。GDPR 不僅適用於歐盟內的公司，任何在歐盟提供消費性商品或服務的企業都必須遵守此法規。

該法規明確定義，個人資料指可連結或關聯至個人的資訊。GDPR 規範的資料包括個人姓名、聯絡資訊、銀行與財務資料，以及醫療資訊等。在技術性方面，規範的資料也包含地理位置資料，例如 IP 位址和網頁 Cookie 等。

這對 API 安全性代表著什麼？無論您是開發應用程式、微服務或物聯網 (IoT) 裝置，在您技術核心的 API 都可能會處理受到 GDPR 規範的資料。因此，開發網際網路 API 的企業從一開始就必須將資料保護納入 API 設計中，而不是事後才開始補救。

例如要考量最低權限原則，這個原則要求確保使用者只擁有執行工作所需的最低權限。

GDPR 的第 25 條便*源於*最低權限，要求公司實施「技術和企業措施，以確保根據預設，只會處理針對具體目的所需的個人資料。」這代表 API 開發人員也應導入使用者驗證與授權控制，以保護透過 API 傳輸的機密資料。API 開發團隊也必須使用安全通訊協定來加密用戶端與伺服器之間的資訊交換，確保資料在傳輸時保持機密。

然而，企業過去數年甚至數十年來所建立的現有 API 生態系統該怎麼辦？企業 API 中有一大部分未受管理、遭到遺忘，或一直在持續運行而沒有經過阻礙或制約。對於這些情況，GDPR 要求：

- 找出 IT 環境中的每個 API
- 評估這些 API 的風險因素 (例如所交換的資料類型，以及誰或什麼系統可以存取該資料)
- 修復所有弱點，例如組態錯誤或驗證機制薄弱等
- 持續測試 API，確保有韌性能夠應對傳統和新興的漏洞和攻擊方法

3. 數位營運復原力法 (DORA)

有鑑於歐盟金融產業在重要基礎設施營運中的角色，DORA 的要求是協助歐盟會員國內的企業承受網路攻擊，並從攻擊中復原。透過 DORA，該產業將擁有具約束力的全方位資訊與通訊技術 (ICT) 風險管理架構。該法案的目的是調和並加強對歐盟金融公司的要求，因為目前的環境涉及多種法規和標準。

歐盟共有超過 22,000 家金融機構和 IT 服務提供者受到 DORA 的影響。值得注意的是，這包括為歐盟金融公司提供 ICT 系統和服務的第三方廠商，包括雲端服務供應商。該法案要求金融機構制定 ICT 第三方風險策略，並進行盡職調查，以審核供應商的合適度。

DORA 規定了數項與 API 安全性有關的要求，包括數位營運穩定性，要求企業導入定期測試計劃，以識別數位營運穩定性中的潛在漏洞、弱點和/或缺失。這些測試包括網路安全測試、滲透測試，Web 應用程式測試等。依金融企業的規模、風險和業務概況而定，依據威脅領導滲透測試 (threat-led penetration testing，TLPT) 進行必要的審查是非常重要的。同樣重要的是定期測試 API 是否有弱點。

DORA 提供了安全測試範例，包括 Web 應用程式與 API 測試。包括利用公開的資源，如開放網路應用程式安全專案 (OWASP)。OWASP 10 大 API 安全風險對企業十分實用，能夠協助企業辨識可能導致攻擊者能夠存取、操控或以其他方式控制企業資源的組態錯誤、弱點、邏輯缺陷和程式碼問題。

4. 健康保險可攜性和責任法案 (HIPAA)

HIPAA 著重於資料隱私和安全性規則，以保護電子病歷 (EHR) 中的健康資訊 (PHI)、電腦化醫師醫囑輸入平台，以及其他醫療照護 IT 系統。任何以電子方式儲存或傳輸 PHI 的美國醫療業者、計劃管理者或資訊交換機構皆必須遵守 HIPAA 的規定。這包括確保 PHI 的機密性、完整性和可用性，以及避免未經授權的揭露和不當使用。

HIPAA 是一項對 API 有重大影響的法規範例，即使它在要求中並未明確指出 API。

以一家為 24 小時全年無休的醫療診所建立病患入口網站的技術廠商為例。這些入口網站的基礎功能之一，就是讓病患能更有效率且安全地存取醫師門診、測試結果和付款等行動。這些資料的交換都靠 API 協助，因此診所和廠商都必須遵守 HIPAA 的要求。

HIPAA 的隱私權規定明確指出「必須開發並實施政策和程序，根據員工的特定角色，限制對受保護健康資訊的存取和使用。」因此，企業的 API 開發人員必須導入技術防護措施，例如驗證、唯一使用者 ID 和以角色為基礎的存取控制，確保能實行最低權限原則。

對受 HIPAA 規範的企業來說，可視性也是不可或缺的，無論是由 IT 團隊自行開發 API，或透過廠商開發 API 的供應商。企業需要針對每個 API 的風險態勢進行即時評估與報告，包括他們傳輸的 PHI 類型。這不僅與法規遵循有關，也是為了履行 HIPAA 的要求，以回應個人要求關於何時、何地、為什麼及向誰揭露其 PHI 的資訊。

5. 網路與資訊安全指令 (NIS2)

歐盟於 2023 年 1 月通過了 NIS 指令版本 2.0，以原始版本的準則為基礎，進一步加強對 IT 基礎架構和報告事件的要求。雖然 v2.0 並未特別提及 API，但其要求對於 API 的保護和管理有著重大影響，因為對於受指令規範的企業來說，這些 API 是許多數位服務運作不可或缺的。值得注意的是，NIS2 包括：

- 更廣泛的產業範圍 — 現有的名單中加入了如雲端服務供應商和社群媒體公司等，其中也包括關鍵基礎架構營運商。在這些產業中，API 廣泛用於整合和服務遞送，而確保 API 安全就成為優先要務。
- 強調確保供應鏈安全 — 企業必須評估風險，並確保其 IT 供應鏈與第三方供應商關係的安全。由於 API 經常用於整合外部服務，因此確保其安全就是法規遵循的關鍵。
- 要求建置一套資訊安全管理系統，用於評估人員、規則和技術，以保護機密資源，並確保營運恢復力。由於 API 是成長快速的攻擊途徑，因此必須納入風險管理策略中。
- 回報重大網路安全事件，包括 API 漏洞。因此，企業必須建立機制，以監控、偵測和報告 API 相關事件。

6. 美國金融服務監管機構指引

聯邦金融機構檢查委員會 (FFIEC) 為聯邦監管機構制定了一份監督美國金融產業的指引和標準。這包括聯邦儲備金、FDIC、OCC 和 NCUA。該委員會的使命是保護消費者與投資人，避免遭受詐欺、濫用及其他不當行為。雖然這並非法規，但 FFIEC 的指引是確保金融公司瞭解如何符合建議安全措施的關鍵。

這是一份關鍵文件，其中包含如何保護 API 的具體指引，進而保護消費者免於詐騙和身分竊盜。以下為相關概覽：

- **清查：**FFIEC 建議建立包括 API 的所有資訊系統清查，這些系統需要具備驗證和存取控制。這不僅適用於金融機構，也適用於其第三方廠商，例如雲端服務供應商等。
- **驗證：**API 應僅允許經過授權的使用者存取。識別所有需要存取控制的使用者 (例如客戶) 是必須的。另外，也應識別需要加強控制 (例如多因素驗證) 的使用者。
- **授權：**API 應僅允許授權使用者存取特定資源。儘管如此，FFIEC 仍建議實施多層式安全機制，例如監控、記錄和活動報告，以識別並追蹤未經授權的存取。
- **風險管理：**FFIEC 在其最新指引中提出了多項有效的風險管理實務。其中，他們在「資訊系統」類別的「清查」下明確指出 API，這表示您需要準確的 API 清查。

企業可能已經很熟悉如何快速應對網路釣魚或勒索軟體等廣為人知的威脅，但 FFIEC 要求辨識「具有可能影響金融機構資訊系統的可能性」及其資料的*任何*網路威脅。如同簡介中所述，78% 的企業曾面臨 API 安全事件，因此您可以相信，即使金融監管機關的要求不斷進化，API 保護依然會是法規遵循的首要任務。

透過 API 保護的最佳實務應對法規遵循挑戰

現今的威脅情勢使企業需要完整的 API 安全解決方案，包括 API 探查、布局管理、執行時間保護，以及 API 安全測試。這樣的全方位方法可輔助現有的任何 WAF 或 API 閘道。

1. API 探查

出現沒有人認識的 API 其實並不罕見。大多數企業對其 API 流量的可視性比例極低，或完全沒有可視性。這通常是因為企業認為所有 API 都會透過 API 閘道路由。但其實並非如此。您的企業面對著各種風險，但缺乏完整且準確的清查。您需要的核心功能：

- 找到並清查您的 API，無論其組態或類型為何
- 偵測休眠、舊版和殭屍 API
- 識別遭到遺忘、忽略或其他未知的影子網域 (又稱「鬼域」(Shadow Domain))
- 消除盲點並找出潛在的攻擊路徑

2. API 布局管理

有了完整的 API 清查後，您必須瞭解哪些類型的資料流會經由 API 傳送，以及這如何影響您的法規遵循能力。API 布局管理可提供流量、程式碼和組態的全方位檢視，以評估企業的 API 資安布局。您需要的核心功能：

- 自動掃描基礎架構，找出錯誤組態和隱藏風險
- 建立自訂工作流程，通知重要利害關係人有關弱點的資訊
- 識別哪些 API 和內部使用者能夠存取敏感資料
- 為偵測到的問題指派嚴重性排序，以排定補救優先順序

3. API 執行時間安全性

您對「假設已經遭到入侵」的概念一定不陌生。API 的駭侵和攻擊事件也已經到了這種無可避免的程度。針對您在生產環境中的所有 API，您必須能夠即時偵測並封鎖攻擊。您需要的核心功能：

- 監控是否發生資料竄改和洩漏、違反原則、可疑行為和 API 攻擊
- 分析 API 流量，不需要額外的網路變更，或安裝困難的代理程式
- 與現有工作流程 (票證、SIEM 等) 整合，以警示安全/營運團隊
- 利用部分或全自動化的補救功能，即時預防攻擊與濫用

4. API 安全性測試

API 開發團隊面臨著速度上的強大壓力。速度對每個開發的應用程式而言都非常重要，因此更容易發生忽略弱點或設計瑕疵的狀況。透過在 API 進入生產環境前的開發階段中進行 API 測試，便可大幅降低風險與修正脆弱 API 的高昂成本。您需要的核心功能：

- 執行多種模擬惡意流量的自動化測試
- 在 API 上線之前發現漏洞，以降低攻擊成功的風險
- 根據既定的治理原則和規則，檢查您的 API 規格
- 以隨選或作為 CI/CD (持續整合和遞送) 管線的一部分，執行以 API 為重點的安全測試

Akamai API Security 如何簡化 API 法規遵循的複雜度

API 是現今法規試圖防範的安全漏洞的主要原因。隨著 API 與風險加倍成長，您該如何保護您的企業？許多企業目前現有的基本 API 保護工具能提供一些防護，但這遠遠不夠。如果您想要更完善保護企業的 API，並證明符合法規遵循，我們很樂意為您提供協助。

針對本白皮書中所述的每一項需求與指南，Akamai API Security 都能強化企業所需的保護，不僅符合法規，也能保護客戶的資料與信任。

Akamai 的全方位解決方案 能從 API 開發的初始階段到進入生產環境之後，全程為 API 提供保護，讓您能遵循核心最佳實務：

- API 探查
- 布局管理
- 執行時間保護
- 安全性測試

進一步瞭解 API，以及如何保護 API 免於遭受攻擊。

瞭解 Akamai API Security 能如何協助您的企業。