

保護 API 並確保應用程式安全 方能讓業務蓬勃發展

現今的應用程式開發和生產變得無比靈活，而企業也面臨前所未有的巨大風險。雲端、API 採用，以及愈來愈低的安全性可見度，都讓應用程式更容易受到攻擊。Radware 最新的應用程式研究特別強調了這個狀況的嚴重性。

應用程式開發與 應用程式安全性 分離

92%

的組織中，安全人員無權過問
持續整合/持續部署的架構

在 89% 的公司中，
資訊安全團隊沒有
安全性解決方案的預算

89%

不同的威脅環境

API 現在是應用程式安全性的一大威脅



在 40% 的公司中，
約有超過半數的應用程式
因為 API 而暴露在網際網路
或第三方服務之下



表示 API 安全性現在是
「第一優先」



在 2021 年將
「大幅投資」API 安全性

重新利用 舊式網路攻擊

長期作為網路層級攻擊
方式的 DDoS，現在是
應用程式上最常見的攻
擊媒介

89% 的受訪者經歷過

DDoS
針對 Web 應用程式的 DDoS 攻擊

HTTP/S

洪水攻擊是最常見的應用程式層級 DDoS 攻擊

行動性 = 不安全

全球大流行的疫情讓人們更加依賴行動應用程式，但行動應用程式開發的安全性欠佳

36%

只有 36% 的應用程式具有完全整合的安全性方案

42%

只有「外掛」的安全性方案

22%

沒有任何安全性方案

由於資料和應用程式都移轉至雲端，而開發人員也愈來愈
依賴 API 來進行整合，因此確保安全性和資料完整性
變得愈發困難。

請參閱 2020-2021 Web 應用程式與 API 保護狀態報告，
了解如何克服這些挑戰