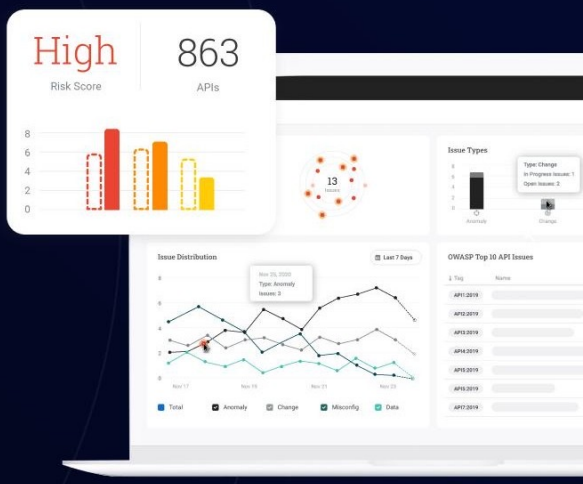
noname

產品簡介

完整且主動的 API 安全平台



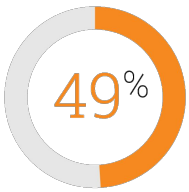
Noname Security 是唯一提供 API 安全狀態管理，提供 API 運行時安全性，保護您的 API 開發生命週期的公司。

數位化轉型同時需要 API 轉型

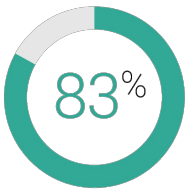
API 是數位化生活的核心。 API 是一種有效率且對開發人員友好的方式，使軟體和資料資產具有靈活性、速度和可移植性的互動能力，也因此更多人看見它的價值。因此許多數位化轉型計劃也加入了 API 的運用，包括:

- 公有雲服務
- 微服務應用程序設計
- Open banking
- 行動健康照護
- 新的業務和開發者生態系統
- 後勤系統數位化
- 大量使用 - GraphQL, gRPC, webhooks

API 使用量將在 2022 年繼續激增



2020 年
API 呼叫量增加



2019 年
透過 API 發起的web流量

隨著企業在 API 上開展業務，他們經歷了 API 安全事件的顯著增加。Gartner 指出，到 2022 年，API 將成為 Web 應用程式的主要攻擊媒介，IBM 指出，三分之二的雲端漏洞與 API 設定錯誤有關。

Noname Security 即時保護 API 並在存在弱點和設定錯誤被惡意利用之前偵測到它們。 Noname API 安全平台是一種 out of band 解決方案，可與您的 API 閘道器、負載均衡設備和 WAF 整合，以提供更深入的可視化和安全性。

API 安全狀態

使用資料**分類盤點每個 API**，包括舊有API 和影子 API。

識別原始碼、網路設定和安全政策中的**錯誤設定和漏洞**

API 運行時安全

使用基於行為的模型來進行**運行時 API 威脅檢測。**

自動化和半自動**阻擋和修復**威脅。

安全的 API 程式碼

持續測試 API 以在 API 風險出現之前辨識出它們。

自動化且動態測試開發並整合到 CI/CD Pipeline中

業界領先的 API 安全防護

找出所有 API、資料和 Metadata

查找並盤點各種 API，包括 HTTP、RESTful 、GraphQL、SOAP、XML-RPC 和 gRPC 。找出不受 API 閘道器管理的舊 API 和惡意 API，並對 API 資料和metadata 進行分類。

分析 API 行為並偵測 API 威脅

使用基於 AI 的自動化偵測來辨識最常見的 API 弱點，包括資料外洩、資料篡改、設定錯誤、違反資料政策、可疑行為偵測和攻擊偵測。

攻擊防護與 修復 API 漏洞

即時防護攻擊、修復錯誤設定、自動更新防火牆安全政策、Webhook 到您的 WAF 以增加新安全政策來阻擋可疑行為，並與現有工作流（問題處理和 SIEM平台）整合。

在部署至線上前 積極測試 API

大多數應用程式在部署到生產環境之前都經過測試。但 API 並未被一樣對待。作為軟體開發生命週期的一部分，更積極的測試 API ，並在正式部署至線上前找出問題是首要任務。

noname

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022 GOLD API Security category North America

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022 GOLD Fastest Growing Cybersecurity Company North America

關於 Noname Security

Noname Security 是唯一一家對 API 安全採取全面且主動做法的公司。Noname 與 20% 的財星全球 500 大企業合作，涵蓋整個 API 安全範圍的三大支柱 —— 狀態管理、Runtime 安全與 API SDLC 安全。 Noname Security 是一家私人控股公司，總部位於美國加州帕羅奧圖，並在以色列特拉維夫和尼德蘭阿姆斯特丹設有辦事處。

Nonamesecurity.com | taiwan@nonamesecurity.com |