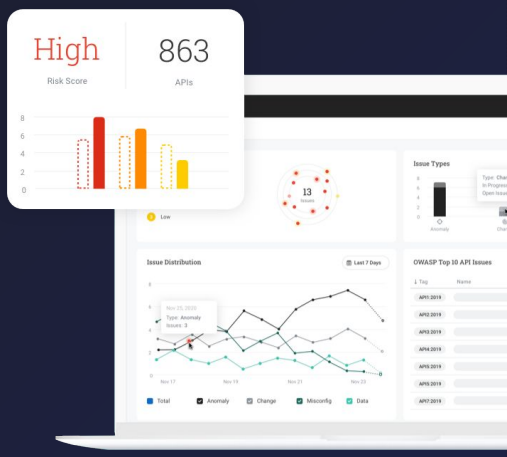
noname

解決方案簡介

# 閘道器、WAF 和 API 安全

## 使用 Noname Security 來彌補不足




數位化轉型的步伐從沒有放緩的跡象。在考量勞動力的需求和增加收入來源的創新要求推動下，IT 領導團隊的首要任務依舊是數位化轉型。而這些數位化轉型計劃都與 API 息息相關 。

雖然 API 是實現數位化轉型的關鍵，但在確保 API 得到充分安全這方面，IT 安全團隊仍然缺乏熟練度和成熟度。API雖然不完全是"新技術"，但 API 在數量、資料量和普遍性方面的巨量增長讓應用程式安全團隊備感壓力。所造成的結果就是 API 的可視化能力以及針對API 的特定安全控制應用存在明顯差距。

許多新的 API 的分佈式特性是導致既有 API 安全性和成熟度不足的原因。 API 安全控制分佈在包括 API 管理、API 閘道器、Web 應用程式防火牆 (WAF) 的部署技術棧之間。雖然技術棧中還有其他元件，但這些是執行安全政策和控制最顯著且最依賴的元件。

## API 管理和閘道器

API 管理和 API 閘道器在確保 API 部署方面發揮著非常重要的作用。兩者都扮演重要的角色，並與控制平台上的 API 管理（管理和安全政策）和數據平台中的 API 閘道器（具有安全政策執行的代理）緊密結合。 API 管理和閘道器的主要功能是在部署 API 時確保 API 可用性、監控使用情況和實施存取控制。

API 管理通常作為入口網站服務，開發人員和 API 管理員可以在準備部署至正式環境時檢視他們的 API。 API 管理用於管理和監控 API 的操作。

顧名思義，API 閘道器充當 API 端點前面的存取控制點。 API 閘道器的核心功能是確保 API 可供其預期使用者使用。 API 閘道器也是 API 管理安全政策的控制點，存取控制和使用（例如速率限制和總量限制）。透過 API 閘道器做流量傳導是一種最佳作法，尤其是對於開放 API（暴露於互聯網），但並非所有 API 都位於閘道器後方。這些 API 就無法納管於閘道器和管理功能提供的控制和可視化中。

# Web 應用程式防火牆(WAFs)

專為 Web 應用程式設計的 WAF 已成為應用程式和 API 保護核心的一部分。 WAF 是所謂代理伺服器的工具，用於檢查傳入的 http(s) Web 和 API 請求是否存在攻擊或不需要的流量。 WAF 功能各不相同，但基本功能是為 Web 和 API 流量提供應用層過濾器。此過濾器在傳入請求(表頭和內文/本文)中查找惡意/不需要的內容，還用於確保只能執行批准的操作(透過安全政策) 。

WAF 用於為應用程式和 API 提供基本保護。他們非常擅長檢測已知攻擊（帶有簽署）和惡意腳本。高級 WAF 增加了反自動化功能，更廣泛地覆蓋了 OWASP Top 10 for Web 應用程式。與 API 閘道器一樣，WAF 只能將安全策略套用於經過它的流量。

# API 安全漏洞

API 閘道器和 WAF 都是部署 API 時的重要組件，但提供充分保護 API 所需的安全控制和可觀察度都不是兩者主要功能。

### 完整的可視度：

API 閘道器和 WAF 都只能觀察經由它們路由進出的 API 流量。 Gartner 預測，到 2025 年，50% 的企業 API 將會是 “未受管理”，這表示可視度將會是有限的。雖然一些非託管 API 是僅在企業內部部署的，但其他未知的“影子”或“殭屍”API，將可能會使組織風險提高。即使所有 API 都透過閘道器和 WAF 進行路由進出，大多數企業組織也只能看見部分可能跨越多個團隊或業務部門的 API 資產.

### 精準的盤點資訊：

僅僅了解組織內的 API 數量對於安全和 IT 團隊來說並不是很有用。準確的清單需要包含 API上下文資料，其中包括處理的資料類型、身份驗證控制、設定、流量映射、路由詳細信息、互聯網暴露以及所有其他相關metadata。 API 閘道器和 WAF 都無法提供完整的 API 盤點總表和目前最新的盤點資訊.

### 安全態勢管理分析：

如果沒有完整的上下文感知可視化， API 閘道器和 WAF 的組合根本無法對 API 進行狀態的詳細分析。狀態管理分析可幫助 IT 團隊有效地找出和解決可能導致安全風險或違反法規的錯誤設定。例如，錯誤設定可能包括身份驗證不完整、不必要的暴露（互聯網）、缺少速率限制或加密等等.

### API 特定的 runtime 安全控制：

閘道器和 WAF 的組合提供了基本的 API 安全控制，閘道器可以執行速率限制和身份驗證控制，WAF 可以偵測基於簽名的攻擊和基於用戶的會話行為。這些控制是非常需要的，但無法充分保護業務免於遭受特定的 API 攻擊和濫用。例如，損壞的對象級授權 (BOLA) 攻擊看起來像閘道器和 WAF 的“普通”API 流量，這使得它們能夠躲過這些控制而不被檢測到。API 閘道器和 WAF 缺乏 API 請求和回應之間的上下文感知。這功能缺口讓 API 容易遭受 BOLA 攻擊，而且容易受到其他攻擊和業務邏輯濫用的影響，這些攻擊和業務邏輯濫用僅僅使用標準閘道器和 WAF 設備根本無法輕鬆辨識.

# 使用 Noname API 安全性彌補不足

Noname API 安全平台有助於彌補 API 閘道器和 WAF 功能缺口而造成的安全弱點。該解決方案有助於準確盤點所有 API，包括內部和影子 API，並主動保護您的環境免於遭受 API 安全弱點、錯誤設置和設計缺陷的影響。 Noname API 安全平台還可與現有 API 閘道器、WAF 和其他 API 部署元件整合，以自動偵測和回應 API 特定威脅，否則這些威脅將無法偵測到。

### 全面的可觀察性和準確的盤點：

Noname API 安全平台自動搜尋、收集和整合來自多個來源的 API 詳細資訊，包括網路流量分析、API 管理和閘道器、WAF、應用程式部署控制等。 API 清單內會自動分類包括流氓/影子和殭屍 API ，因而實現更高效率的 API 資產管理。

### 安全態勢管理分析：

Noname API 安全平台對 API 清單執行狀態管理分析。該分析會自動辨識設定相關的弱點，例如，如果處理敏感或受監管資料的 API 沒有足夠的身份驗證控制。高風險問題會被自動標示，以便安全團隊可以優先考慮首要的工作或最需要的地方。態勢分析可主動完成降低風險，並有助於減少潛在的 API 攻擊面。

### 特定的 API runtime 安全控制：

Noname API 安全平台提供 runtime 攻擊檢測以補充現有的安全控制。該平台使用人工智能 (AI) 和機器學習 (ML) 建立 API 行為基線。如果有異常行為，例如 BOLA 攻擊或商業邏輯濫用，會被自動偵測和標示。補救措施可以透過安全政策自動化或透過與現有 IT 工作流程的整合來啟動。

# 更好的結合：透過 Noname Security 從 API 閘道器和 WAF 中獲得更多效益

網路安全是一項需要團隊合作的運動，保護 API 也不例外。沒有單一的解決方案可以充分滿足全面 API 可視度和安全性所需的所有要求。 API 管理、閘道器和 WAF 都發揮著關鍵作用，但僅倚靠單一工具可能使 API 遭受攻擊。 Noname API 安全平台與這些技術無縫整合以彌補不足的技術缺口。這些技術的結合有助於為數位化商業應用提供安全可靠的環境，還讓 IT 團隊不僅能夠更好地保護 API 和關鍵資產免於遭收網路攻擊，更還能在組織內建立和維護有效的 API 安全程式。

noname



## 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 | info@nonamesecurity.com | +1 (415) 993-7371