WHITE PAPER

Upwind Runtime CNAPP

以執行時期為核心的雲原生應用防護平台

從告警疲勞到風險聚焦

重新定義雲原生資安的營運模式

SaaSPodium 拓維雲智資安顧問團隊

Authorized Distributor of Upwind

版本 1.0 | 2026 年 4 月

目錄

執行摘要

企業數位轉型與雲原生化已成為不可逆的趨勢。根據 Gartner 研究,到 2027 年,超過 85% 的企業將採用雲優先(Cloud-First)策略,95% 的新數位工作負載將部署於雲原生平台。然而,伴隨而來的資安挑戰,遠比多數組織預期的嚴峻。

傳統的雲端資安工具以靜態掃描為核心,產出數萬筆 CVE 與組態告警,卻無法回答最關鍵的問題——「這些風險中,哪些真的正在被攻擊者利用?」資安團隊淹沒在告警之中,真正的威脅反而被埋沒,整體 MTTR(平均修復時間)不降反升。

Upwind 以 **eBPF 驅動的執行時期可觀測性(Runtime Observability)** 為核心,打造次世代雲原生應用防護平台(CNAPP)。它不只是另一個掃描工具,而是將 CSPM、CWPP、CIEM、KSPM、Vulnerability Management、API Security、Threat Detection 等能力,以 Runtime 為統一視角重新整合,讓資安團隊從「理論上的風險清單」,升級為「真實世界中正在發生的威脅」。

本白皮書將深入剖析:

- 當前雲原生資安架構的結構性問題
- Runtime-Powered CNAPP 如何重新定義雲端資安
- Upwind 的技術架構、核心模組與差異化能力
- 典型企業導入情境、商業價值與 ROI
- 部署流程、整合策略與合作夥伴支援

> *「我們不再需要另一個能產生更多告警的工具。我們需要的是一個能告訴我們『接下來該做什麼』的平台。」— 某金融業 CISO*

一、市場現況:雲原生資安的三大斷層

在深入探討 Upwind 的技術架構之前,必須先理解雲原生資安當前面臨的三個結構性問題。這三個斷層解釋了為什麼即使企業投入大量資源,資安事件仍持續增加。

1.1 告警爆炸 vs. 修復能力有限

一個中型雲端環境(1,000 個容器、100 個雲端帳號)每月產生的資安告警數量可輕易超過 50,000 筆,其中包含:

- 數萬筆 CVE 漏洞(來自容器映像檔、主機作業系統、應用程式依賴)
- 數千筆雲端組態偏差(CSPM 告警)
- 數百筆身分權限過度授權(CIEM 告警)
- 數十筆 Kubernetes 組態風險(KSPM 告警)
- 不定數量的威脅偵測事件

然而,典型的資安團隊每月僅能實際處理數百筆事件。這中間的差距不是靠招募更多人力能解決的,而是需要從根本上改變「風險優先排序」的邏輯。

1.2 工具孤島 vs. 攻擊的跨領域特性

現代攻擊者不會照著企業的工具分類攻擊。一個典型的雲端攻擊路徑可能是:

> *利用公開的 CVE 入侵某個容器 → 透過容器逃逸取得節點存取權 → 濫用節點的 IAM 角色 → 橫向移動至其他雲端服務 → 存取敏感資料。*

這條攻擊路徑涉及:容器漏洞(CWPP)、Kubernetes 組態(KSPM)、雲端身分(CIEM)、雲端服務組態(CSPM)。若企業使用四套不同的工具,資安團隊必須手動拼湊告警才能看見完整攻擊鏈——而這通常在事件發生幾週之後才能完成。

1.3 Shift-Left 的假性成功

過去五年,業界將「Shift-Left」視為雲原生資安的解方——把資安能力前移到開發階段,在程式碼寫完的當下就找出問題。這個方向正確,但執行上普遍失敗。主要原因是:

- **告警太多且缺乏情境** — 開發者在 PR 階段收到數百筆告警,多數不具實際風險,久而久之失去信任。
- **工具責任邊界模糊** — Shift-Left 工具的告警是否要修、由誰修、何時修,往往沒有清楚的流程。
- **缺乏 Runtime 回饋機制** — 開發階段的告警品質,沒有透過執行時期的真實數據來驗證與優化。

真正有效的雲原生資安,必須讓 Shift-Left 與 Runtime 形成閉環——開發階段的決策依據,來自於執行時期的真實風險觀察。這正是 Upwind 的核心設計理念。

二、CNAPP 的演進:從工具整合到 Runtime-Powered

Gartner 於 2021 年首次提出 CNAPP(Cloud-Native Application Protection Platform)概念,主張將分散的雲端資安工具整合為單一平台。然而,市場上的 CNAPP 產品可大致分為三個世代:

世代	核心架構	特徵與侷限
第一代:拼裝式 CNAPP	CSPM + CWPP 簡單整合	透過併購多個獨立產品拼湊而成,各模組資料架構不一致,告警無法真正關聯,Dashboard 只是把多個工具的內容放在同一頁面。
第二代:統一資料模型	以 Agent 或雲端 API 為基礎的統一架構	資料整合改善,但仍以「靜態分析」為主,無法區分「存在的風險」與「正在被利用的風險」,告警疲勞問題未解。
第三代:Runtime-Powered CNAPP	eBPF Runtime Context + 風險關聯引擎	以執行時期的真實行為為核心,結合靜態分析建立完整風險情境,能自動過濾不具可利用性的告警,讓資安團隊聚焦於真正重要的威脅。

2.1 為什麼 Runtime 是下一代 CNAPP 的核心

Runtime-Powered 的核心意義,是用「執行時期的真實行為」作為所有資安決策的基礎。這改變了三件事:

- **從「漏洞存在」到「漏洞是否被載入」** — 一個容器映像檔可能包含 500 個 CVE,但實際被執行時期載入記憶體的套件可能只有 50 個。修復優先順序立刻清晰。
- **從「權限存在」到「權限是否被使用」** — IAM 政策中 80% 的權限可能從未被使用。Runtime 觀察能自動找出應被回收的過度授權。
- **從「可能的攻擊路徑」到「真實的連線行為」** — 靜態分析告訴你「A 服務可能可以連到 B」,Runtime 告訴你「A 服務實際上每分鐘連 B 十次」。

這樣的差異看似細微,但在大規模環境中,能讓告警數量減少 90% 以上,並大幅提升修復決策的準確度。

三、Upwind 平台架構與核心技術

Upwind 的架構設計圍繞著三個核心原則:輕量、即時、關聯。

3.1 eBPF Sensor:無侵入式的執行時期觀察

eBPF(extended Berkeley Packet Filter) 是 Linux 核心中一項革命性的技術,允許在不修改核心、不插入核心模組的前提下,於核心層安全執行自訂程式。Upwind 以 eBPF 為基礎打造 Sensor,在每個工作負載上提供高保真的行為觀察:

- Process 執行事件(fork、exec、syscall 軌跡)
- 檔案系統操作(開啟、讀寫、權限變更)
- 網路連線(來源、目的、埠號、協定、封包特徵)
- 共享記憶體與 IPC 活動
- 容器與 Kubernetes 生命週期事件

相較於傳統 Agent,eBPF 的效能負擔極低(通常 CPU 影響 < 1%),且不需要在應用程式中植入 Sidecar 或修改程式碼,部署對開發與營運團隊幾乎透明。

3.2 Cloud API 整合:覆蓋 Agentless 範圍

並非所有雲端資產都能部署 Agent(例如無伺服器函數、受管資料庫、雲端儲存)。Upwind 透過與 AWS、Azure、GCP、Oracle Cloud 的原生 API 整合,以 Agentless 方式收集:

- 雲端組態與資源清單
- IAM 政策、角色與實際權限使用記錄
- 網路組態(VPC、Security Group、NACL)
- 資料存取記錄(CloudTrail、Azure Activity Log 等)
- 無伺服器與 PaaS 服務的組態與事件

Agent 與 Agentless 兩種資料來源在 Upwind 平台中自動關聯,形成完整的雲端資產與行為視圖。

3.3 Risk Correlation Engine:風險關聯引擎

收集到的所有訊號——漏洞、組態、身分、網路、執行時期——會在 Upwind 的風險關聯引擎中被正規化、關聯,並透過圖資料庫(Graph Database)建構出完整的風險情境。這個引擎能自動回答:

- 這個 CVE 是否在執行時期被載入?
- 這個工作負載是否能從外部網路存取?
- 它持有的身分憑證能存取哪些其他資產?
- 從這個進入點,攻擊者最壞情況可以走到哪裡?
- 對應到 MITRE ATT&CK 框架中的哪些技術?

這些問題的答案,過去需要資安分析師手動串接數個工具才能得到,現在由 Upwind 自動在告警生成的當下提供。

3.4 資料架構:SaaS-Native 雲端平台

Upwind 為 SaaS-Native 架構,客戶無需部署控制平面,所有管理、分析、儀表板、告警皆在

Upwind 的雲端平台提供。這帶來幾個優勢:

- 持續升級而無需客戶介入,新功能與威脅情資即時生效
- 跨多雲、多地區的統一視圖,適合全球化企業
- 具備企業級的資料隔離、SOC 2 Type II 與 ISO 27001 認證
- 支援資料駐留(Data Residency)需求,符合地區合規要求

四、核心能力模組

Upwind 以單一平台、單一 Agent、單一政策模型,提供完整的 CNAPP 能力。以下為各核心模組的功能說明:

模組	核心能力與 Runtime 優勢
CSPM 雲端態勢管理	涵蓋 AWS、Azure、GCP、Oracle Cloud 的組態稽核、合規框架自動檢查(CIS、PCI-DSS、HIPAA、SOC 2、ISO 27001),並結合執行時期資訊驗證組態風險是否真實可被利用。
CWPP 工作負載保護	涵蓋 VM、容器、無伺服器工作負載的漏洞管理、惡意檔案偵測、入侵偵測與行為分析,透過 eBPF 提供執行時期的真實威脅可視性。
CIEM 雲端身分權限管理	盤點所有 IAM 身分、角色、政策,結合實際權限使用記錄自動識別過度授權(Over-Privilege)與閒置權限,提供最小權限建議。
KSPM Kubernetes 態勢管理	涵蓋 Kubernetes 叢集組態稽核、RBAC 分析、Pod Security Standard 檢查、Network Policy 驗證與 Admission Controller 整合。
Vulnerability Management 以 Runtime 為基礎的漏洞管理	掃描容器映像檔、主機、應用程式依賴中的 CVE,並透過 Runtime Context 自動判斷哪些漏洞真正被載入、暴露、可被利用。
API Security API 安全與可視性	自動盤點已知與未知(Shadow / Zombie)API,偵測異常呼叫模式、敏感資料外洩風險,對應 OWASP API Top 10 威脅。
Threat Detection & Response 執行時期威脅偵測與回應	基於 eBPF 的行為分析與 ML 模型,偵測容器逃逸、惡意指令執行、橫向移動、資料外洩等攻擊行為,並提供完整的事件時間軸。
IaC Security 基礎設施即程式碼掃描	在 CI/CD 管線中掃描 Terraform、CloudFormation、Kubernetes YAML、Helm Chart 等 IaC 檔案,並將執行時期觀察到的風險回饋至開發階段。

五、Risk Intelligence:從告警到可行動的風險

Upwind 的核心差異化能力,是將「告警」轉換為「風險」——不只是告訴你「什麼有問題」,而是回答「為什麼重要」與「接下來該怎麼做」。

5.1 五維度風險關聯模型

Upwind 判斷一個風險的真實優先順序,會綜合考量五個維度:

- **漏洞(Vulnerability)** — CVE 嚴重性、是否有已知利用工具、是否為 KEV(已知被利用漏洞)名單
- **組態(Configuration)** — 工作負載與雲端服務的組態是否符合最佳實務
- **身分(Identity)** — 受影響資產持有的憑證、角色與實際存取範圍
- **網路(Network)** — 是否可從網際網路存取、是否與關鍵資產相連
- **執行時期(Runtime)** — 受影響的套件/服務是否實際被載入、連線、執行

只有當多個維度同時指向高風險時,Upwind 才會將其標記為高優先事件,避免基於單一維度的誤判。

5.2 攻擊路徑分析(Attack Path Analysis)

Upwind 以圖資料庫建構雲端環境中所有資產、身分、網路連接的完整關係圖,並以攻擊者的視角模擬可能的攻擊路徑。典型的攻擊路徑分析輸出包含:

- 進入點(Entry Point):暴露於外部的脆弱工作負載
- 中繼點(Pivot Points):可被利用的身分憑證、橫向連接
- 最終目標(Crown Jewels):涉及敏感資料或關鍵服務的資產
- 修復建議(Remediation):切斷該路徑所需的最小修改

這讓資安團隊得以從「修復所有高危漏洞」轉為「切斷最危險的攻擊路徑」——通常修復幾個關鍵節點,就能消除數百筆個別告警所代表的整體風險。

5.3 MITRE ATT&CK 對應

所有 Upwind 偵測到的威脅事件皆對應至 MITRE ATT&CK for Cloud / Containers 框架,協助資安團隊:

- 以標準化語言與管理層、稽核方、董事會溝通風險
- 評估組織對特定 TTP(戰術、技術、程序)的覆蓋率
- 與 SIEM、SOAR、XDR 等平台共享一致的威脅模型
- 持續優化偵測規則,覆蓋新興攻擊技術

六、典型應用場景與導入案例

場景一:整合取代多套 AppSec/雲端資安工具

背景情境:某製造業客戶同時使用 CSPM A 產品、CWPP B 產品、容器掃描 C 產品、獨立的 API Gateway 資安方案,年度授權費用超過 USD 500K,且告警分散於多個儀表板,資安團隊無法建立全面的風險視圖。

導入結果:以 Upwind 取代上述四套工具,授權成本下降 40%,告警數量減少 92%,資安事件平均回應時間從 48 小時縮短為 4 小時。

場景二:滿足金融監理與跨境合規要求

背景情境:某跨國金融機構需同時符合 PCI-DSS、SWIFT CSCF、歐盟 DORA、新加坡 MAS TRM 等多重合規要求,傳統工具需手動產出各框架的對照報告,稽核準備耗時數週。

導入結果: Upwind 內建合規框架映射,支援一鍵產出各法規對應報告,稽核準備時間縮短 80%,並透過持續合規監控及時發現偏差事件。

場景三:Kubernetes 環境的資安治理

背景情境:某電商客戶採用多叢集 Kubernetes 架構(EKS + GKE,共 200+ 個 Node),面臨 Pod 安全標準不一致、RBAC 過於寬鬆、Network Policy 未落實等挑戰。

導入結果:透過 Upwind 的 KSPM 能力統一叢集治理,自動識別高風險的特權容器、過度授權的 ServiceAccount 與缺失的網路隔離,資安態勢評分在三個月內從 62 分提升至 91 分。

場景四:DevSecOps 真正落地

背景情境:某 SaaS 公司曾嘗試導入多種 Shift-Left 工具,但因告警過多,開發團隊普遍忽略。資安與開發團隊關係緊張,專案交期頻繁延誤。

導入結果:透過 Upwind 的 Runtime 回饋機制,開發團隊收到的告警減少 85%,且每筆告警皆附帶執行時期情境與具體修復建議。開發與資安協作評分顯著提升,上線週期未受資安流程拖累。

場景五:事件調查與雲端鑑識

背景情境:某企業發現對外 API 存在異常流量,懷疑遭到入侵。缺乏執行時期可視性,鑑識團隊僅能依靠不完整的 CloudTrail Log,無法還原完整攻擊鏈。

導入結果:導入 Upwind 後,攻擊發生時能自動捕捉完整的 Process、Network、File 事件軌跡,加上攻擊路徑分析圖,MTTR(平均修復時間)由原本 5 天縮短至 8 小時。

七、商業價值與 ROI 分析

Upwind 帶給企業的商業價值可從三個面向量化:營運成本、資安風險、業務敏捷性。

價值面向	傳統架構的現況	導入 Upwind 的效益
工具授權成本	3-5 套分散工具,年度授權費用高,且多數功能重疊	**單一平台取代多套工具,授權成本平均降低 30-50%**
人力成本	資安團隊花 60% 時間處理告警三角(分類、關聯、判斷)	**告警減少 85% 以上,人力可投入威脅狩獵與架構優化**
MTTR	從偵測到修復平均需 3-7 天	**縮短至數小時至一日,依事件類型而定**
稽核準備	多個工具分別產出報告,手動彙整耗時 2-4 週	**一鍵產出合規報告,準備時間縮短 80%**
業務上線速度	資安流程成為開發瓶頸,衝突頻繁	**Shift-Left 與 Runtime 形成閉環,資安不再拖慢交付**
風險可見性	風險呈現為孤立告警,難以向管理層說明整體暴露面	**攻擊路徑圖與風險儀表板,清楚呈現整體資安姿態**

典型企業在導入 Upwind 後的 12 個月內,可達到正向投資回報(Positive ROI)。以一個具備 500 個容器、50 個雲端帳號的中型環境為例,年度總擁有成本(TCO)預估可下降 35-45%,同時顯著降低資安事件造成的業務中斷與品牌損害風險。

八、部署模式與導入流程

8.1 部署架構

Upwind 採用 SaaS 控制平面 + Edge Sensor 的混合架構,客戶僅需負責:

- **Cloud Connector** — 透過 IAM 角色授權連接 AWS、Azure、GCP 等雲端帳號,啟用 Agentless 資料收集(通常 15-30 分鐘完成)
- **eBPF Sensor** — 透過 DaemonSet(Kubernetes)、Helm Chart、Ansible Playbook 或雲端自動化工具部署至工作負載上
- **CI/CD Integration** — 在 GitHub Actions、GitLab CI、Jenkins、Azure DevOps 等管線中嵌入 IaC 與容器映像檔掃描

8.2 標準導入里程碑

階段	時程	主要活動與產出
Phase 1 Discover	第 1-2 週	雲端連接、初步資產盤點、完成 Agentless 資料收集、產出初版雲端資產清單與高風險清單。
Phase 2 Deploy	第 3-4 週	eBPF Sensor 部署至目標工作負載、啟用 Runtime 威脅偵測、CI/CD 整合(IaC 與容器掃描)。
Phase 3 Optimize	第 5-8 週	建立自訂偵測規則、整合告警通知(Slack / Teams / Jira)、與 SIEM / SOAR 串接、團隊培訓。
Phase 4 Operate	第 9 週起	日常維運、事件回應、持續優化、合規報告自動化、與既有資安流程完整融合。

多數客戶在導入後第一週即可獲得初步的風險可視性成果,第一個月內完成核心部署並開始產出價值,第三個月達到完整營運能力。

九、與既有資安架構的整合

Upwind 並非要取代企業所有資安投資,而是以雲原生資安核心的角色,與既有架構協同運作。

9.1 與 SIEM / SOAR / XDR 的整合

Upwind 原生支援主流 SIEM 與 SOAR 平台的資料整合,包含 Splunk、Microsoft Sentinel、Google SecOps、Elastic、CrowdStrike Falcon LogScale、IBM QRadar 等。透過結構化的事件格式(含 MITRE ATT&CK 標記),資安團隊可在既有 SOC 工作流中直接處理 Upwind 產生的告警與事件。

9.2 與 DevOps 工具鏈的整合

- 版本控制:GitHub、GitLab、Bitbucket、Azure Repos
- CI/CD:GitHub Actions、GitLab CI、Jenkins、CircleCI、Azure DevOps
- 容器登錄:Docker Hub、ECR、ACR、GCR、Artifactory、Harbor
- IaC:Terraform、CloudFormation、Pulumi、Helm、Kustomize
- 工單系統:Jira、ServiceNow、Linear、Asana

9.3 與 SaaSPodium 解決方案組合的協同

在 SaaSPodium 的 Cloud-Native Security Pack 中,Upwind 負責執行時期防護層,與其他方案形成端到端資安視角:

- **Corelight NDR** — 當 Upwind 在工作負載層偵測到異常,Corelight 提供對應的網路層證據,協助完整還原攻擊鏈。
- **Cycode SAST & ASPM** — Cycode 負責程式碼與供應鏈階段的風險治理,Upwind 負責執行時期的真實驗證,形成 Shift-Left 與 Shift-Right 的完整閉環。
- **Cribl** — 將 Upwind 產生的高價值遙測資料,以中立、成本最佳化的方式路由至 SIEM、資料湖或威脅情資平台。

十、SaaSPodium 的服務承諾

作為 Upwind 在台灣與亞太區的授權代理商(Authorized Distributor),SaaSPodium 提供的不只是產品授權,而是一整套從評估到長期維運的專業服務:

- **售前諮詢與架構設計** — 依據企業的雲端架構、合規需求與資安成熟度,規劃最適合的 Upwind 導入藍圖。
- **POC 規劃與執行** — 提供標準化 POC Playbook、成功標準定義、與技術團隊共同執行為期 2-4 週的概念驗證。
- **導入服務** — 專業顧問團隊協助 Cloud Connector 設定、Sensor 部署、CI/CD 整合、告警調校與 SIEM 串接。
- **教育訓練** — 為資安團隊、DevOps 團隊、開發團隊提供分層式教育訓練,確保平台效益最大化。
- **長期維運支援** — 提供中文原廠技術支援窗口、定期健檢、新功能導入諮詢與年度架構檢視服務。
- **Managed Service 選項** — 對於資安人力有限的企業,提供由 SaaSPodium 合作 MSSP 夥伴提供的託管式營運服務。

結語

雲原生資安的下一個十年,將由「Runtime-Powered」定義。當企業的雲端架構持續複雜化、攻擊者持續進化、合規要求持續嚴苛,唯有以執行時期真實行為為基礎的資安平台,才能同時滿足可視性、精準度與營運效率三個維度的要求。

Upwind 不是又一個雲端資安工具,而是一個 **重新定義雲原生資安營運模式** 的平台。它讓資安團隊不再是「告警處理者」,而是「風險決策者」;讓資安不再是業務的阻力,而是加速器。

SaaSPodium 以代理商與顧問團隊的雙重身分,協助企業把 Upwind 的技術潛力轉化為實際的商業價值。無論您正在評估第一套 CNAPP、規劃既有工具的整合取代、或希望將 Runtime Security 納入雲原生策略——我們都能為您提供從評估、導入到長期優化的完整支援。

下一步:開啟您的 Runtime CNAPP 之旅

預約技術諮詢 | 申請 POC | 取得完整產品簡報

SaaSPodium 拓維雲智資安顧問團隊

Authorized Distributor of Cribl, Corelight, Cycode and Upwind

Freshworks Premier Partner |