WHITE PAPER

Cribl

Security Data Pipeline Platform

新世代安全資料管線平台

讓 SIEM 擺脫授權費失控,
把資料的控制權還給企業

以資料路由、精煉、重塑能力,降低 Splunk 與新世代 SIEM 授權費 40-70%

SaaSPodium 拓維雲智資安顧問團隊
Authorized Distributor of Cribl
版本 1.0 | 2026 年 4 月

目錄

執行摘要

企業的資安與營運資料正以每年 28-35% 的速度增長,遠超過 SIEM 與 Observability 平台的消化能力。對多數企業而言,最直接的衝擊不是技術層面,而是財務層面——Splunk、Microsoft Sentinel、Google SecOps(Chronicle)、CrowdStrike Next-Gen SIEM、Datadog、Elastic 等平台,皆採用「按資料量計價」的授權模式,導致企業每年的授權費失控成長。

某亞太金融業客戶 2022 年 Splunk 年費為 USD 1.2M,到 2024 年已飆升至 USD 3.5M——短短兩年成長 **192%**,而真正對資安團隊有價值的資料比例估計不到 35%。剩下 65% 的授權費,基本上是用來儲存「可能永遠不會被查詢、只為了合規留存」的重複與低價值資料。

Cribl 以 **「Security Data Pipeline Platform(SDPP)」** 的架構,在資料來源(Endpoint、網路設備、雲端、應用程式)與目的地(SIEM、Data Lake、Observability、儲存)之間建立一個 **中立、廠商無關的資料管線層**,讓企業第一次真正掌握自己的資料流向與成本結構。

透過 Cribl,企業可以:

- **路由(Route)** — 依資料類型、價值、合規需求,將資料分別送往不同目的地,高價值資料送 SIEM、低價值資料送低成本儲存。
- **精煉(Reduce)** — 去除重複欄位、壓縮冗餘欄位、剔除無用日誌,平均可將送入 SIEM 的資料量減少 30-50%。
- **重塑(Reshape)** — 將原始日誌轉換為結構化格式、欄位標準化、遮罩敏感資料(PII)、聚合(Aggregate)為事件指標。
- **回放(Replay)** — 將保留在低成本儲存的歷史資料,在需要時重新回放進 SIEM 分析,避免為了合規付出高額 SIEM 費用。
- **豐富(Enrich)** — 透過 Threat Intel、GeoIP、CMDB 等外部資料源,在進入 SIEM 前完成資料豐富化,提升偵測準確度。

實際導入案例顯示,Cribl 可協助企業將 Splunk 年度授權費降低 **40-70%**,將 Microsoft Sentinel 的 Ingestion 成本降低 **35-60%**,並在 6-9 個月內達到正向 ROI。更重要的是,Cribl 讓企業未來不再被單一 SIEM 廠商鎖定,可以自由遷移、混合部署、或分階段替換。

> *「我們沒有換掉 Splunk,但透過 Cribl,我們的 Splunk 費用減少了 62%,同時還擴大了資料覆蓋範圍。」— 某全球 500 大企業 CISO*

一、企業資料爆炸與 SIEM 授權費失控

要理解 Cribl 為什麼能為企業節省大量 SIEM 授權費,首先需要理解當前企業資安資料架構所面臨的結構性問題。

1.1 資料量的爆炸性成長

根據 IDC 研究,企業每年產生的機器資料量(日誌、遙測、事件、網路流量)以 28-35% 的複合成長率增加。推動這個成長的主要因素包括:

- **雲端遷移** — 混合多雲架構使得每個應用都產生來自多個層級(基礎設施、平台、應用)的日誌。
- **微服務與容器化** — 單體應用拆解為數百個微服務,每個容器都產生日誌與遙測資料,容器生命週期短、事件頻繁。
- **SaaS 爆炸式增長** — 企業平均使用 100+ 個 SaaS 應用,每個應用的 Audit Log 都需納入資安監控。
- **Endpoint 遙測** — EDR/XDR 產品產生大量 Endpoint 行為資料,單台電腦每天可產生數 GB 的遙測。
- **合規要求** — GDPR、PCI-DSS、HIPAA、金融監理等要求日誌保存 7 年以上,長期儲存成本龐大。

1.2 傳統「All-In-SIEM」架構的三大問題

過去十年的主流架構是「所有資料都送 SIEM」——Splunk、ArcSight、QRadar 承擔了資料收集、儲存、分析、告警的全部責任。但隨著資料量爆炸,這個架構暴露出嚴重缺陷:

問題一:授權費呈指數成長

Splunk 以「Ingestion GB/Day」計價,每增加 100 GB/Day 的資料量,年費就增加 USD 50K-120K(依版本與合約條件)。當企業的資料量從 500 GB/Day 成長到 2 TB/Day,Splunk 年費從 USD 800K 飆升至 USD 3M+ 並非罕見。

問題二:低價值資料排擠高價值分析

SIEM 的計算與儲存容量是有限的。當 70% 的容量被合規日誌、系統心跳、DEBUG 級訊息佔用時,真正需要即時告警的威脅資料(EDR 偵測、網路異常、身份異常)反而被壓縮空間、延遲索引。

問題三:資料被單一廠商鎖定

一旦資料進入 Splunk 內部的 Indexer,就以其專有格式儲存,遷移成本極高。企業想要測試新的 SIEM(如 Microsoft Sentinel、Google SecOps、Crowdstrike NG-SIEM),需要耗費巨大工程投入重新建立資料收集管線。

1.3 新世代 SIEM 雖便宜,但計價模型仍是陷阱

許多企業為了降低 Splunk 成本,轉向 Microsoft Sentinel、Google SecOps、CrowdStrike Next-Gen SIEM 等「新世代 SIEM」。這些平台確實在單位資料成本上較 Splunk 便宜,但:

- Microsoft Sentinel 以 GB 計價,同時綁定 Log Analytics Workspace 費用與保留期費用,隨著資料量成長,費用增幅仍可觀。
- Google SecOps(Chronicle)雖然按員工數計價、資料量無上限,但前提是資料必須符合 UDM 格式,大量資料轉換工作需自行負擔。

- CrowdStrike Next-Gen SIEM 綁定 CrowdStrike 生態,資料主權仍落在單一廠商手中。
- 所有新世代 SIEM 都面臨同一個問題:若將所有資料直接送入,授權成長曲線仍會複製 Splunk 的老路。

關鍵洞察: 無論選擇哪一家 SIEM,企業都需要一個 **廠商中立的資料管線層**,在資料進入任何 SIEM 之前,先篩選、精煉、路由、豐富。這正是 Cribl SDPP 的定位。

二、什麼是 Security Data Pipeline Platform(SDPP)

Security Data Pipeline Platform(SDPP,資安資料管線平台)是 Gartner 在 2023 年正式提出的新興類別,用來描述 **位於資料來源與目的地之間、負責處理與路由安全相關資料的獨立平台**。Cribl 是 SDPP 類別的開創者與市場領導者,也是目前唯一完全 **獨立、廠商中立** 的 SDPP 解決方案。

2.1 SDPP 的五個核心能力

核心能力	英文名稱	說明
收集	**Collect**	支援 300+ 種資料來源:Syslog、HTTP、Kafka、S3、Azure Event Hub、Splunk HEC、Cloud SaaS API、Agent 等。
路由	**Route**	依資料類型、內容、標籤,智慧分配至不同目的地。高價值 → SIEM;長期保存 → Data Lake;即時分析 → Observability。
精煉	**Reduce**	去除重複欄位、剔除無用日誌、壓縮冗餘內容,平均可減少 30-50% 資料量而不影響偵測能力。
重塑	**Reshape**	格式標準化(CEF、OCSF、ECS)、欄位改名、PII 遮罩、Schema 強制、聚合(Aggregate)。
回放	**Replay**	將儲存於低成本位置的歷史資料,在需要時(如合規查詢、事件調查)重新回放進 SIEM。

2.2 SDPP 與傳統 Log Management / ETL 的差異

許多人第一次聽到 SDPP 時,會認為這只是「重新包裝的 Log Management 或 ETL」。事實上,SDPP 是為現代資安資料工作流設計的新類別,與傳統工具有根本性差異:

比較面向	Cribl SDPP	傳統 Log Management	ETL 工具
定位	**資料管線,不儲存資料**	資料儲存 + 分析	資料搬運工具
目標資料	**資安與營運日誌、遙測**	日誌檔案	結構化業務資料
資料流	**Streaming 即時處理**	批次收集、存入索引	批次搬運
處理能力	**路由/精煉/重塑/回放/豐富**	僅收集與檢索	抽取/轉換/載入
多目的地	**可同時送多個 SIEM/Lake**	單一儲存庫	單一目標資料庫
廠商中立	**完全獨立**	綁定廠商生態	資料平台廠商綁定

比較面向	Cribl SDPP	傳統 Log Management	ETL 工具
授權費優化	核心價值主張	無此能力	無此能力

2.3 為什麼 Cribl 是唯一獨立的 SDPP

市場上有幾個看似類似 Cribl 的產品,但多數屬於 SIEM 或可觀測性廠商的「護城河產品」,目的在於鞏固自家生態:

- **CrowdStrike Onum** — CrowdStrike 於 2025 年收購 Onum,最終必然深度整合入 Falcon LogScale 與 NG-SIEM,促使客戶資料往 CrowdStrike 平台集中。
- **Palo Alto Chronosphere** — Palo Alto 於 2025 年收購 Chronosphere,將與 Cortex XSIAM、Prisma Cloud 整合,資料主權仍在 Palo Alto。
- **Google Bindplane** — Google 收購後,主力服務 Google SecOps 與 GCP Observability,對其他目的地支援度有限。
- **Tenzir、NXLog、Axoflow、Abstract Security、DataBahn** — 均為近年新進廠商,功能成熟度、生態完整度、台灣在地支援皆不及 Cribl。

Cribl 由 Splunk 前核心工程師創立於 2018 年,完全獨立、廠商中立,其商業模式就是為客戶 **優化 SIEM 成本、打破資料廠商鎖定**,而非為任何 SIEM 或可觀測性廠商服務。這是 Cribl 獨一無二的戰略定位。

三、Cribl 平台架構總覽

Cribl 並非單一產品,而是一個以資料管線為核心的平台套件,包含四個主要產品:

3.1 Cribl 產品組合

產品	定位	核心能力
Cribl Stream	**資料管線核心**	路由、精煉、重塑、回放、豐富。支援 300+ 資料來源與目的地,提供視覺化 Pipeline 編輯器。
Cribl Edge	**輕量 Agent**	部署於 Endpoint、伺服器、容器,取代 Splunk UF、Fluentd、Logstash 等 Agent,可遠端管理、動態配置。
Cribl Search	**聯邦式查詢**	無需搬移資料,直接查詢位於 S3、Azure Blob、GCS、Splunk、Elastic、Loki 等位置的資料。
Cribl Lake	**低成本長期儲存**	基於物件儲存的資料湖,開放格式(Parquet),供 Cribl Search 與第三方工具查詢,合規保存成本極低。

3.2 部署架構

Cribl 提供三種部署模式,滿足不同企業的架構需求:

Cribl.Cloud(SaaS)

Cribl 託管的全代管服務,企業無需管理基礎設施,Cribl 負責版本升級、擴展、備援。適合希望以最低維運成本快速上線的企業。

Self-Hosted(自建)

部署於企業自有 VM、Kubernetes 或地端伺服器,完整掌控資料流與架構。適合金融、政府、國防等對資料主權嚴格要求的客戶。

Hybrid(混合)

管理平面(Leader)在 Cribl.Cloud,資料處理 Worker Node 部署於企業環境,兼顧管理便利與資料主權。

3.3 企業級合規與安全

- SOC 2 Type II、ISO 27001、HIPAA、PCI-DSS、FedRAMP Moderate 合規認證
- 資料駐留選項:US、EU、APAC 區域
- RBAC 角色權限控制、SSO(SAML、OIDC)、稽核日誌
- 資料處理過程中可執行 PII 遮罩、Hashing、Tokenization
- 支援 Kafka、AWS Kinesis、Azure Event Hub 等主流串流技術

四、Cribl Stream:資料處理引擎

Cribl Stream 是整個 Cribl 平台的核心,也是實現 SIEM 授權費優化的關鍵引擎。

4.1 Pipeline 視覺化編輯

Cribl Stream 提供圖形化的 Pipeline 編輯器,工程師透過拖拉式介面設計資料流。每個 Pipeline 由一連串 Function 組成,常用 Function 包括:

- **Eval** — 欄位運算、新增、刪除、重新命名
- **Drop** — 依條件刪除不需要的事件
- **Regex Extract** — 從原始日誌擷取結構化欄位
- **Parser** — 解析 JSON、Key-Value、CEF、Syslog、XML 等格式
- **Lookup** — 以外部資料表豐富欄位(如 GeoIP、CMDB、Threat Intel)
- **Mask** — 遮罩 PII、機敏資料(卡號、身分證、密碼)
- **Aggregation** — 將多筆事件聚合為指標(如每分鐘失敗登入次數)
- **Sampling** — 對高頻低價值資料進行取樣

4.2 Routes:多目的地智慧分流

Cribl Stream 的 Route 機制讓同一筆資料可同時送往多個目的地,並對每個目的地應用不同的 Pipeline:

- 高價值告警事件 → Splunk / Sentinel(完整欄位、即時索引)
- 所有原始資料 → Cribl Lake / S3(低成本長期保存,供合規)
- 關鍵指標 → Datadog / Prometheus(時序監控)
- 可疑行為 → SOAR(即時處置)
- DEBUG 日誌 → 直接 Drop(不儲存,不計費)

這個能力是 SIEM 授權費優化的核心——企業不再被迫「所有資料都付 SIEM 高價」,而是依資料價值動態分流。

4.3 Packs:預建最佳實務範本

Cribl 提供 Packs(資料處理範本),涵蓋常見資料來源的最佳實務配置,包括:

- Windows Event Logs 精煉 Pack(去除重複欄位、聚合心跳事件)
- Palo Alto Firewall 精煉 Pack
- CrowdStrike Falcon 事件分類 Pack
- Cisco ASA / FTD 精煉 Pack
- Microsoft 365 Audit 精煉 Pack
- AWS CloudTrail 精煉 Pack

企業可直接採用 Pack,或以 Pack 為基礎再客製化,大幅縮短 Pipeline 建置時間。

五、Cribl 如何大幅降低 Splunk 授權費

Splunk 作為全球 SIEM 龍頭,其計價模型與技術架構對多數企業造成巨大成本壓力。本章節深入解析 Cribl 如何在不影響資安偵測能力的前提下,將 Splunk 授權費降低 40-70%。

5.1 理解 Splunk 的計價模型

Splunk 的主要計價模型有三種:

Ingestion-Based(依資料量)

依每日納入的資料量(GB/Day)計價,也是最傳統、最普遍的模型。當資料量成長,費用線性成長。企業資料每增加 100 GB/Day,年費增加 USD 50K-120K。

Workload Pricing(依計算量)

依查詢、分析的計算資源計價,不限制納入資料量。看似更公平,但實際上對資料分析頻繁的企業反而更貴,且計算量難以預測,預算編列困難。

Splunk Cloud Services / SVC

混合 Ingestion 與 Workload 的新模型,但 SVC 單位換算複雜,多數企業表示授權費反而上漲。

無論採用哪種模型,一個殘酷事實是: Splunk 的架構決定了「資料量越大、費用越高」這個基本公式不會改變。因此,要降低 Splunk 費用,根本方法就是 **減少進入 Splunk 的資料量,同時保留分析所需的關鍵資訊**。這正是 Cribl 的核心價值。

5.2 Cribl 降低 Splunk 費用的七個具體機制

機制一:去除重複欄位(Field De-duplication)

許多原始日誌包含大量重複、冗餘的欄位。例如 Windows Event Log 4624(登入事件)的原始格式中,同一個欄位可能以多種方式重複出現(如 SubjectUserName、TargetUserName、Account Name 等可能指向同一使用者)。Cribl 可保留最有價值的欄位,移除重複內容,將單筆事件大小減少 20-40%。

機制二:剔除低價值日誌(Low-Value Event Drop)

許多系統產生的日誌對資安偵測並無實際價值,如心跳訊號、Health Check、DEBUG 級訊息、成功的重複事件。Cribl 可依規則完全 Drop 這些事件,避免佔用 Splunk 容量。實務上,這類資料常佔總資料量的 15-30%。

機制三:欄位裁剪(Field Pruning)

原始日誌常包含數十個欄位,但實際用於告警規則或查詢的通常只有 5-15 個。Cribl 可只保留需要的欄位,將事件大小減少 30-60%。

機制四:聚合高頻事件(Event Aggregation)

部分事件以極高頻率發生(如網路流量、效能指標、Firewall Allow 規則),但實際分析時只需統計數字。Cribl 可將這些事件聚合為每分鐘指標(例如「某 IP 在 5 分鐘內失敗登入 47 次」),將 1000 筆原始事件壓縮為 1 筆統計事件。

機制五:資料分層儲存(Tiered Storage)

並非所有資料都需要 Splunk 的即時索引與快速查詢能力。Cribl 可將資料依價值與頻繁度分層:

- 高價值 + 高查詢頻率 → Splunk(即時告警)

- 中價值 + 中頻查詢 → Cribl Lake / S3(Cribl Search 查詢)
- 合規保存 + 低頻查詢 → S3 Glacier / Azure Archive(僅保存)

此分層策略可將 Splunk 資料量減少 50% 以上,同時保持完整的合規保存能力。

機制六:取樣與智慧過濾(Smart Sampling)

對於某些高容量但重複性高的資料(如 Web Access Log、CDN Log),可透過 Smart Sampling 只保留異常、錯誤、慢請求等關鍵事件,正常 200 回應取樣 1/100。這可將資料量減少 80-90%,且完整保留問題事件。

機制七:格式優化(Format Optimization)

部分原始日誌格式(如 XML、Verbose JSON)包含大量結構標籤,實際資訊密度低。Cribl 可將其轉換為更精簡的 Key-Value 或 JSON 格式,減少 30-50% 體積。

5.3 實際案例:某亞太金融業 Splunk 成本優化

面向	導入 Cribl 前	導入 Cribl 後
每日進入 Splunk 資料量	2.4 TB/Day	**820 GB/Day(-66%)**
Splunk 年度授權費	USD 2.8M	**USD 1.05M(-62%)**
長期儲存資料量	僅 Splunk 90 天	**Cribl Lake 保存 7 年**
合規保存成本	含於 Splunk 費用	**USD 180K/年(S3)**
Cribl 授權費	—	**USD 280K/年**
整體年度成本	USD 2.8M	**USD 1.51M(-46%)**
偵測能力	基準	**無退步,部分規則因資料品質提升而更準確**
ROI 達成時間	—	**導入後 7 個月**

> *「Cribl 讓我們三年內累積節省了超過 USD 4M 的 Splunk 授權費,並且讓我們有能力擴大資安資料覆蓋範圍,而不是因為預算壓力而裁減資料。」— 該客戶 CISO*

六、Cribl 對新世代 SIEM 的授權優化機制

近年來,許多企業為了擺脫 Splunk 的高成本,轉向新世代 SIEM——Microsoft Sentinel、Google SecOps、CrowdStrike Next-Gen SIEM、Elastic Security、Exabeam。雖然這些平台在單位資料成本上較 Splunk 便宜,但計價陷阱依然存在。Cribl 對這些平台同樣能提供顯著的成本優化。

6.1 Microsoft Sentinel

計價模型: 依 Log Analytics Workspace 的 Ingestion GB 計價,另加資料保留期費用。Sentinel Analytics 依分析規則啟用數量計價。

Cribl 優化機制:

- Commitment Tier 優化:Sentinel 提供「100GB/Day 起」的 Commitment Tier 折扣。Cribl 可精準控制 Ingestion 量,讓客戶穩定維持在理想折扣區間。
- Basic Logs 分流:Sentinel 近期推出 Basic Logs 分層(單位成本約為 Analytics Logs 的 1/5)。Cribl 可依資料用途自動分流,大量低價值資料送 Basic Logs,只有告警規則需要的資料送 Analytics Logs。
- Archive 整合:極低頻查詢的資料送至 Azure Blob / Data Explorer(ADX),Cribl Search 可跨源查詢。
- 典型節省:Sentinel Ingestion 費用可降低 35-60%。

6.2 Google SecOps(Chronicle)

計價模型: 依企業員工數計價,資料量無上限。看似無需優化,但前提是資料必須符合 Google UDM(Unified Data Model)格式。資料轉換與 Parser 維護成本往往被低估。

Cribl 優化機制:

- UDM 轉換:Cribl 可將各類原始日誌(Windows、Firewall、Cloud)轉換為 UDM 格式,取代自行撰寫 Parser 的工程負擔。
- 分流至 BigQuery:並非所有資料都需進入 Chronicle,低頻查詢資料可直接送 BigQuery 降低成本。
- Parser 標準化:企業可避免被 Google Parser Pack 綁定,保持資料格式的靈活性。
- 典型節省:資料工程成本減少 40-60%,避免未來不必要的員工授權升級。

6.3 CrowdStrike Next-Gen SIEM(Falcon LogScale)

計價模型: 依資料納入量計價(以 GB/Day 為單位),價格通常較 Splunk 低 40-50%,但隨著資料量成長仍有上升壓力。

Cribl 優化機制:

- 一般資料路由:CrowdStrike Falcon EDR 原生資料直接進 NG-SIEM,第三方資料(Firewall、Cloud、SaaS)由 Cribl 先精煉再送入。
- 避免 CrowdStrike 鎖定:CrowdStrike 推廣 Onum(2025 年收購)作為資料管線,但此舉會深化 CrowdStrike 生態鎖定。以 Cribl 作為獨立 SDPP,保留多 SIEM 選項。
- 典型節省:NG-SIEM Ingestion 費用減少 30-50%。

6.4 Elastic Security

計價模型: 依 Resource Unit(RU)計價,包含 CPU、Memory、Storage。企業自建 Elastic 成本可控但維運複雜;Elastic Cloud 則按使用量計價。

Cribl 優化機制:

- 冷/熱資料分層:高頻查詢資料進 Hot Tier,低頻資料送 Frozen Tier(S3),Cribl 負責智慧分流。
- 索引減量:Elastic 的索引(Index)直接影響儲存與查詢成本,Cribl 先精煉再送入可減少索引膨脹。
- 典型節省:Elastic 基礎設施成本降低 30-50%。

6.5 Exabeam New-Scale SIEM

計價模型: 依資料量與使用者數量計價,強調 UEBA 能力,但基礎資料處理仍需外部管線。

Cribl 優化機制:

- Cribl 作為 Exabeam 前置處理層,減少資料量並豐富身份關聯欄位,提升 UEBA 準確度。
- 典型節省:整體資料進入量減少 30-50%。

6.6 關鍵結論:SIEM 無論哪家,Cribl 都能優化

不同 SIEM 的計價細節各異,但共通邏輯都是:「資料量越大、費用越高」。Cribl 的價值在於:

- **減量** — 精煉送入 SIEM 的資料量,降低計費基礎
- **分流** — 依資料價值分配至不同層級(熱/冷/封存),最小化高單價儲存
- **解耦** — 讓資料不再被單一 SIEM 綁架,保留未來遷移或混合部署的彈性
- **提質** — 資料進入 SIEM 前完成豐富化與標準化,提升偵測準確度,減少誤報調查時間

七、Cribl Search 與 Cribl Edge

7.1 Cribl Search:聯邦式查詢,不再搬移資料

傳統資料分析架構假設所有資料必須集中到單一平台(如 Splunk 的 Indexer、Elastic 的 Cluster),才能進行查詢分析。但這種「先搬移、再查詢」的模式,是高額儲存成本的根源。

Cribl Search 改變了這個模式,提供 **「查詢就地資料,不搬移」** 的聯邦式查詢能力。

Cribl Search 支援的查詢來源:

- Cribl Lake(開放 Parquet 格式)
- AWS S3、Azure Blob、GCS 物件儲存
- Splunk(跨 Index 查詢)
- Elastic / Opensearch
- Grafana Loki
- Snowflake、BigQuery、Databricks

查詢結果可同時呈現來自不同來源的資料,並可直接輸出至 Cribl Stream 進行回放(Replay)到 SIEM。典型應用場景:

- **事件調查(Investigation)** — 查詢保留於 S3 的 2 年前資料,無需將其重新載回 Splunk
- **合規稽核** — 依稽核人員需求直接查詢 Cribl Lake,不影響 SIEM 運行
- **資料探索** — 評估新資料源的價值,決定是否納入 SIEM

7.2 Cribl Edge:輕量 Agent,取代 Splunk UF

Cribl Edge 是部署於 Endpoint、伺服器、容器的輕量資料收集 Agent,設計目標是取代現有多樣化的 Agent 組合:

- Splunk Universal Forwarder(UF)
- Fluentd / Fluent Bit
- Logstash
- NXLog / Rsyslog
- Filebeat / Metricbeat

Cribl Edge 的核心優勢:

- **中央管理** — 數萬台 Edge Agent 可由中央 Leader 統一管理、監控、升級
- **動態配置** — 遠端即時更新 Pipeline,無需重新部署 Agent
- **Edge 精煉** — 在資料離開 Endpoint 前即進行精煉,減少網路頻寬與後端處理負擔
- **資源消耗低** — CPU 與 Memory 佔用顯著低於 Splunk UF

企業導入 Cribl Edge 可同時減少授權費(取代多個商業 Agent)與維運成本(單一管理平面)。

八、Cribl Lake:長期儲存與低成本查詢

Cribl Lake 是建構於開放物件儲存(S3、Azure Blob、GCS)之上的資料湖服務,以 Apache Parquet 格式儲存,提供三個核心價值:

8.1 極低的保存成本

物件儲存的成本約為 Splunk 的 1/50、Sentinel 的 1/30。對於合規要求 7 年保存的企業,這個成本差異是決定性的:

- Splunk 保存 1 TB 資料 7 年:約 USD 420K-840K
- Cribl Lake 保存 1 TB 資料 7 年:約 USD 8K-15K(S3 Standard-IA)
- 成本差距:50-100 倍

8.2 開放格式,避免鎖定

Cribl Lake 採用開放的 Parquet 格式,可被 Cribl Search、AWS Athena、Snowflake、Databricks、Trino 等工具直接查詢。企業對資料的控制權完全掌握在自己手中。

8.3 Replay 回放能力

當企業需要分析歷史資料時(如事件調查、合規稽核、新增告警規則的歷史驗證),可透過 Cribl Stream 的 Replay 功能將 Lake 中的資料重新送入 SIEM,彈性極高。這讓企業不再為了「可能偶爾需要分析」的資料,付出每日 24 小時的 SIEM 索引費用。

九、Cribl 完整 Use Case 分析

9.1 SIEM 授權費優化

最常見也最具直接 ROI 的應用場景。透過前述七大機制,將 Splunk / Sentinel / LogScale 年度授權費降低 40-70%。典型中大型企業每年可節省 USD 500K 至 USD 5M。

9.2 SIEM 遷移與混合部署

企業從 Splunk 遷移至 Sentinel、或評估 CrowdStrike NG-SIEM 時,Cribl 可同時將資料送至兩個 SIEM,讓企業在不中斷既有告警的情況下平行驗證新平台,遷移風險大幅降低。

9.3 合規長期保存

金融、醫療、政府等產業需保存日誌 7-10 年。透過 Cribl Lake + Cribl Search,合規保存成本僅為傳統 SIEM 保存的 2-5%。

9.4 多雲資料整合

企業跨 AWS、Azure、GCP 的日誌需統一納入資安監控。Cribl 提供 300+ 原生整合,無需為每個雲撰寫自訂 Parser。

9.5 資料治理與敏感資料保護

在資料進入 SIEM 前完成 PII 遮罩、敏感欄位 Tokenization,符合 GDPR、PIPL、資保法等法規要求。避免敏感資料因進入 SIEM 後難以追蹤與刪除的問題。

9.6 Observability 資料管線

除了資安資料,Cribl 同樣可用於 Datadog、New Relic、Dynatrace 等 Observability 平台的資料優化,降低 APM 與日誌監控成本。

9.7 AI / ML 資料準備

企業訓練資安 ML 模型需要高品質的結構化資料。Cribl 可將原始日誌轉換為標準化格式(OCSF、ECS),直接輸入 ML Pipeline。

十、導入流程與最佳實務

SaaSPodium 提供標準化的四階段 Cribl 導入方法論,典型導入週期 8-12 週:

階段	時程	主要活動
Phase 1 Assess	第 1-2 週	現況資料盤點、SIEM 成本分析、資料價值評估、節省潛力試算、優先順序規劃。
Phase 2 Deploy	第 3-4 週	Cribl 平台部署(Cloud / Self-Hosted / Hybrid)、Worker Node 擴展、與既有資料來源/目的地建立連線。
Phase 3 Optimize	第 5-10 週	依優先順序建立 Pipeline、Pack 部署、精煉規則驗證、A/B 測試偵測能力、效能調校。
Phase 4 Scale	第 11-12 週及之後	全量切換、監控 Cribl 本身效能、持續優化新資料源、定期檢視成本節省效益。

10.1 導入最佳實務

- **從最大資料源切入** — 優先處理佔比最高的 3-5 個資料源(如 Windows Event Log、Firewall、EDR、Cloud),通常可達成 70% 以上的節省。
- **保留偵測能力驗證期** — 精煉後的資料送 SIEM 時,同時保留原始資料至 Cribl Lake,至少運作 30 天以驗證告警規則不受影響。
- **善用 Packs** — 先採用 Cribl 官方 Packs 快速取得基礎效益,再依企業需求客製化。
- **持續監控與迭代** — 資料組成會持續變化,每季重新檢視 Pipeline 效益,發掘新的優化空間。

十一、TCO 與 ROI 量化分析

以下為典型中大型企業(Splunk 年度授權 USD 2M,每日資料量 1.5 TB)導入 Cribl 後的三年 TCO 分析:

年度	原始 Splunk 費用	優化後 Splunk	Cribl + 儲存	年度節省
Year 1	USD 2.0M	USD 0.8M	USD 0.35M	**USD 0.85M**
Year 2	USD 2.6M	USD 1.0M	USD 0.4M	**USD 1.2M**
Year 3	USD 3.4M	USD 1.3M	USD 0.45M	**USD 1.65M**
三年累計	**USD 8.0M**	**USD 3.1M**	**USD 1.2M**	**USD 3.7M**

註:原始 Splunk 費用假設以每年 30% 成長率計算(符合資料量年增趨勢);優化後 Splunk 為減少 60% Ingestion 後的預估費用;Cribl + 儲存包含 Cribl 授權與 S3 Glacier 長期保存成本。

三年累積節省: USD 3.7M(約 NT$ 120M)

除了直接授權費節省外,Cribl 還帶來以下隱性效益:

- 資安資料覆蓋範圍擴大 2-3 倍(原本因成本考量捨棄的資料源現可納入)
- SOC 分析師因資料品質提升,MTTR(平均回應時間)縮短 25-40%
- 廠商議價能力提升:不再被 SIEM 廠商鎖定,續約時具談判籌碼
- 資料遷移能力:未來評估新 SIEM 時無縫切換

十二、SaaSPodium 的服務承諾

作為 Cribl 在台灣與亞太區的授權代理商,SaaSPodium 提供完整的 Cribl 解決方案服務:

- **免費 Data Assessment** — 協助企業盤點現有 SIEM 資料結構,量化潛在節省金額,作為決策依據。
- **Cribl 授權諮詢** — 依資料量、部署模式、產品組合,提供最佳 Cribl 授權方案。
- **標準化 POC 服務** — 提供 30 天的 POC,以實際資料驗證節省效益,零風險評估。
- **導入顧問服務** — Cribl Level 2 認證顧問團隊協助完成部署、Pipeline 設計、資料來源整合、效能調校。
- **中文教育訓練** — 針對管理者、Pipeline 工程師、SOC 分析師的分層式培訓,建立企業內部 Cribl 能力。
- **長期維運支援** — 提供中文技術支援、季度健檢、新資料源整合諮詢、年度成本檢視。
- **SIEM 遷移顧問** — 協助企業評估從 Splunk 遷移至 Sentinel、Google SecOps、CrowdStrike NG-SIEM 的路徑與風險。
- **與 Corelight、Cycode、Upwind 整合方案** — SaaSPodium 的 Cloud-Native Security Pack 中,Cribl 作為資料管線基礎層,與 Corelight NDR、Upwind Runtime CNAPP、Cycode ASPM 形成完整的現代化資安資料架構。

結語

SIEM 是企業資安架構的核心,但不應該成為企業財務的無底洞。當前主流 SIEM 的計價模型,將企業置於「資料越多、費用越高」的結構性困境。越是積極擴大資安監控覆蓋,越陷入授權費的通膨壓力。

Cribl 以 Security Data Pipeline Platform 的架構,為企業提供了根本解方:

- 讓每一筆資料送到正確的地方,而不是全部擠進 SIEM
- 讓資料的價值決定儲存成本,而不是資料量決定儲存成本
- 讓企業重新掌握資料主權,不再被單一 SIEM 廠商鎖定
- 讓資安團隊聚焦於威脅分析,而非追逐資料與預算

SaaSPodium 作為 Cribl 授權代理商,擁有六位 Cribl Level 2 認證專業團隊,協助企業從評估、POC、導入到長期優化,打造現代化的資安資料架構。我們不只是銷售 Cribl,更是您資安資料戰略的長期夥伴。

下一步:評估您的 SIEM 節省潛力

免費 Data Assessment | 30 天 POC

SaaSPodium 拓維雲智資安顧問團隊

Authorized Distributor of Cribl, Device42, Corelight, Cycode and Upwind | Freshworks Premier Partner