CLOUDFLARE

執行指南

一致風險狀態：

CISO 的降低風險和複雜性指南

目錄

超越風險管理：一致風險狀態

作為 CISO，您負責網路安全和風險管理。但您並非始終「擁有」為企業帶來風險的所有技術和數位資產，例如：

- 您的員工和第三方使用的網際網路連線的應用程式、裝置、雲端和網路
- 由員工和客戶建立、儲存和共用的資料
- 由開發人員構建和使用的程式碼和 API

隨著時間的推移，組織積累了很多單點解決方案，試圖將保護擴展到日益分散的 IT 環境中。但這些工具往往孤立運作，互通性有限，因此無法構建一個全面的風險檢視，而它們產生的資料可能會讓安全人員不堪重負。總之，管理這種碎片化環境需要太多的手動工作、時間和專業知識，才能有效確定風險的優先順序。

這種複雜性會導致危險。例如，依據 TechTarget 的企業戰略集團進行的一項調查，**四分之三 (76%) 的組織曾因面向網際網路的資產未知、未受管理或管理不善而遭受網路攻擊。**

在當今的分散式環境中提升網路安全狀態需要變革。隨著攻擊面的擴大，組織應探索更統一、更整合的風險狀態管理方法，以便：

- **緩解**風險——更高效、更輕鬆
- **最佳化**現有工具和風險訊號的作用
- 更快**適應**不斷演變的風險
- **自動執行**更多的安全工作流程

《一致風險狀態：CISO 的降低風險和複雜性指南》將介紹考慮風險管理的優勢、使用案例以及三階段架構（如下）。繼續閱讀以瞭解更多資訊。

3 階段架構

評估風險——涵蓋整個 IT 環境

…在工具之間交換風險指標，以獲得更全面的瞭解

…實施風險控制並保護企業

什麼是一致風險狀態管理？

多個組成要素 — 一個整體目標

從較高層次上看，風險管理需要三項關鍵工作：

1. 使用動態的第一方風險評分模型，評估整個 IT 環境中的風險
2. 交換風險指標意味著在不同工具之間共用資料，從而構建更全面的風險檢視
3. 以自動化、一致的方式，基於所瞭解的情況實施控制

統一風險狀態透過在盡可能少的安全系統（理想情況下是使用一個平台）中完成這些步驟，簡化了這一過程。透過這種方式，將動態的第一方風險評分、在安全工具之間共用背景資訊的整合以及自動化的安全措施結合在一起，讓組織能夠更專注地評估風險、確定風險優先順序以及緩解風險。

如果您能在整個攻擊面上擴展更多的可見度和控制，這種方法就會變得更強大，包括保護人員、應用程式、資料和網路。

此外，透過將這些風險管理工作融合到一個平台中，您還可以減少對單點解決方案的依賴，在現有的 IT 生態系統內利用風險訊號執行更多操作，並在所有位置套用保護措施。

統一風險狀態管理可協助您因應各種媒介中不斷演變的內外部風險，包括：

使用者風險

- 網路釣魚
- 勒索軟體
- 遠端存取
- 行動裝置/BYOD
- 第三方/供應鏈
- ...以及更多

資料風險

- 資料遺失/暴露
- 資料竊取/外洩
- 侵犯隱私
- 違反合規性
- 資料竄改
- ...以及更多

應用程式風險

- 阻斷服務
- Zero-day 漏洞利用
- SQL 資料隱碼攻擊
- Cross-site scripting
- 帳戶盜用
- 影子 IT（包括影子 API）
- ...以及更多

一致風險狀態管理的優勢

將以上評估、交換和實施階段統一起來，有助於組織更輕鬆、更高效地管理整個攻擊面上的風險狀態。

優點	樣本指標
減少 SecOps 工作量 減少手動原則建立，提高事件回應敏捷性	• 增加自動化工作流程數量 • 減少構建原則所需點擊次數 • 減少平均偵測時間 (MTTD) • 減少平均回應時間 (MTTR)
降低網路風險 在整個攻擊面上實現自動化和動態風險狀態實施	• 減少嚴重事件數量 • 增加自動封鎖的威脅數量

安全技術及其在統一風險狀態中的作用

安全服務邊緣 (SSE) 平台讓組織可以確保存取安全、抵禦威脅，並為 Web、SaaS 和私人應用程式環境中的資料提供保護。這種廣泛的範圍為 SSE 平台提供了對 IT 環境中使用者活動的獨特可見度，從而豐富用於即時識別危險和可疑行為的模型。此外，雲端交付的 SSE 網路安全方法還有助於在整個組織內集中構建和實施原則。

如果說 SSE 主要用於保護組織的內部 IT 基礎架構，則 Web 應用程式與 API 安全 **(WAAP)** 是用於保護面向公眾的攻擊面。這意味著抵禦廣泛的風險，包括漏洞利用、機器人、未經授權的存取、詐騙、濫用和阻斷服務。

將 SSE 和 WAAP 功能融合於單一平台，可幫助組織將風險管理擴展到人員、應用程式和資料這些關鍵領域。

其他廣為人知的技術對 SSE 和 WAAP 安全平台進行了補充：

- **安全性資訊與事件管理 (SIEM) 以及延伸偵測和回應 (XDR)** 平台彙總了環境中的記錄和風險資訊，以實現監控、分析和報告。很多企業依賴這些工具來調查和回應事件以及支援合規性。
- 企業往往還依賴於端點安全來保護裝置，以及身分識別與存取管理工具來驗證使用者。這些工具作為額外的安全層，提供了有關裝置和使用者活動的大量情報，然後可在安全平台之間共用。

單獨來看，上述任何一項技術對攻擊面上可見度和控制的擴展程度都有一定的限制。然而，**利用整個安全生態系統的功能和情報是實現更有效的風險狀態管理的基礎。**

第 1 步：評估風險

使用 SSE 簡化對使用者的風險評分

使用者與實體行為分析 (UEBA) 模型在幫助組織因應不斷演變的風險中發揮著重要作用。UEBA 模型通常使用機器學習，來偵測使用者、裝置和其他實體中的異常或危險活動，然後提醒安全團隊採取行動。這大大減少了手動分析工作，幫助安全團隊跟上威脅的步調。

然而，在實踐中，部署 UEBA 模型可能仍然是低效的。例如，這些模型通常在 SIEM 和 XDR 工具中使用，但這些工具需要進行微調和自訂以避免不準確，這在大規模使用時，即使對於資源充足的 SOC 而言也是不可持續的。

相反，將風險評分直接嵌入 SSE 平台有助於在 Web、SaaS 和私人應用程式中實現一致的記錄和規則。這就避免了僅在 SIEM/XDR 內使用 UEBA 模型的複雜性。SSE 平台可在網路安全環境中的偵測危險行為與實施原則（例如，封鎖流量）之間快速「形成迴圈」。

使用者風險評分範例

使用者風險評分是 UEBA 的一個組成部分，可檢查使用者活動中的可疑和不安全動作。動作越危險，產生的分數就越高，表示遭受入侵、內部人員威脅或其他風險的可能性越大。使用者風險評分在 SSE 平台內很常見，這些平台具有對網路活動的直接可見性。

例如，出現以下情況時，會即時將使用者評為高風險：

- **不可能的旅行：**指使用者在不合理的短時間內從兩個不同的位置登入（例如，一名員工從紐約市登入，幾分鐘後，又從雪梨登入）
- **資料丟失預防 (DLP) 違規：**指以違反公司政策或法規的方式移動、共用或存取敏感或機密資訊（例如，開發人員試圖將專有原始程式碼上傳到第三方 AI 聊天機器人）
- **重複使用危險裝置：**指裝置被視為不安全或違反公司政策（例如，缺少最新的 OS 更新；存在未修補的漏洞）

將使用者和應用程式中的風險評估聚集起來

SSE 平台成為越來越熱門的現代基礎，用來透過 UEBA 模型偵測使用者層級的風險。但隨著當今對 IT 整合的關注，組織正在尋找方法來進一步擴展風險評估，以涵蓋針對面向公眾的應用程式、網站和 API 的威脅。

將 SSE 以及 Web 應用程式和 API 安全功能融合到一個平台上，為企業提供對使用者和應用程式（這二者在一般組織的攻擊面中佔很大的比例）的可見度、控制和共用情報。

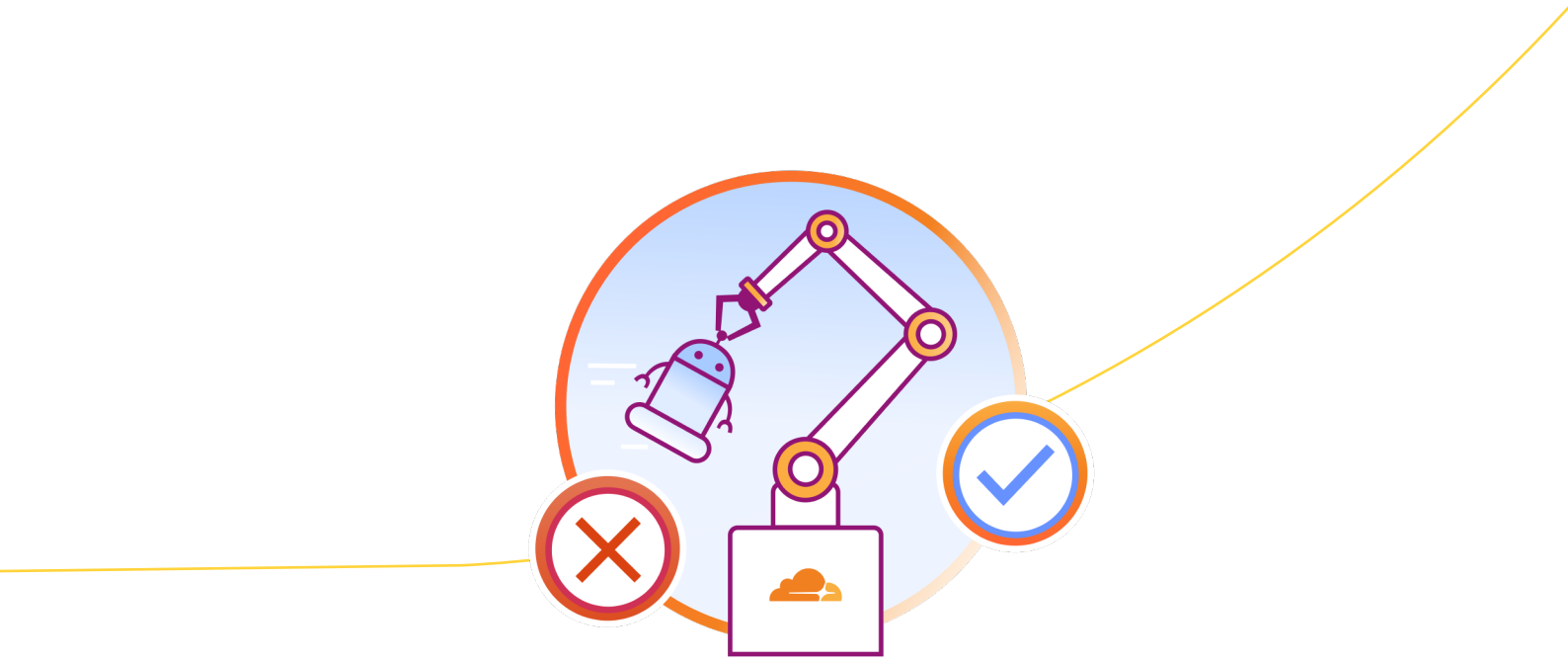
應用程式風險的模型範例

例如，為了保護應用程式，Cloudflare 的平台使用由機器學習 (ML) 提供支援的風險模型偵測並緩解惡意負載和機器人，包括：

- 我們的 **WAF Attack Score**，它對請求是否包含 zero-day 漏洞或常見的 OWASP 十大風險（例如，SQL 資料隱碼攻擊、Cross-site scripting 或遠端程式碼執行負載）進行評分
- 我們的**機器人分數**，它對請求來自機器人的可能性進行評分
- 我們的**惡意指令碼分類器**，它會檢查瀏覽器指令碼對網站訪客的危險

其他 ML 模型可幫助安全團隊探索新的 API 端點和結構描述，而無需客戶提前輸入任何內容。

對整個應用程式基礎架構的可見度有助於在儀表板中主動發現風險，例如，公開的 RDP 伺服器、未代理的 DNS 記錄、沒有 TLD 加密的網域等。



第 2 步：交換風險指標

更輕鬆、更高效地利用現有工具

想像一下，您的安全團隊成功識別（並阻止）了一起針對承包商「Bob Fisher」的網路釣魚嘗試。看到使用者成為一起網路釣魚活動的目標就足以將該使用者標記為危險，這與我們剛剛概述的第一步是一致的。增加該使用者的風險分數可能會轉化為增加對系統存取的限制。

然而，這是一起孤立的事件嗎？同樣的對手是否會繼續以不同的方式攻擊 Bob 或其他員工？他的裝置是否遭到了入侵？

CISO 需要的是全貌，而不僅僅是一組記錄，才能繼續保持並提升組織的網路安全狀態。

為了有效且高效地應對威脅，CISO 需要透過更廣泛的工具生態系統，實現自動化的風險指標雙向交換，這些工具包括：

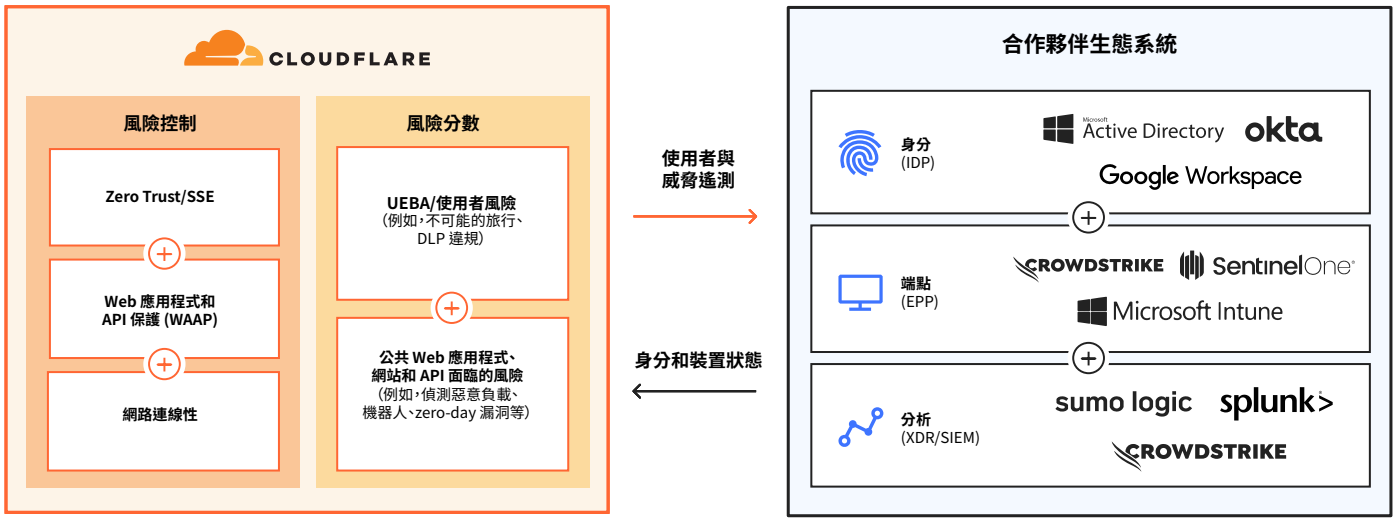
- **身分識別提供者 (IdP)**，可儲存並管理使用者的數位身分
- **端點保護 (EPP)**，可保護連線至您的網路的裝置
- **安全性資訊與事件管理 (SIEM)**，可收集、分析和管理記錄和事件資料，以尋找安全事件的跡象
- **延伸偵測和回應 (XDR)**，可簡化安全資料分析擷取，並幫助您實施進一步預防和補救

因此，在這起涉及「Bob」的事件中，一致風險狀態管理透過自動與現有安全工具交換資訊，減輕了 SecOps 團隊的負擔：

1. Cloudflare 提供的遙測（包括有關已封鎖活動的記錄，甚至個別使用者風險分數）會在您的安全生態系統中共用，包括與可繼續執行更深入的並行自動化掃描的 SIEM 和 XDR 工具共用。
2. 這些安全工具會將動態風險情報回報給 Cloudflare，例如，IdP 和 EPP 合作夥伴可以反過來與 Cloudflare 分享其使用者和裝置風險分數，後者將此類資訊內建為狀態檢查以限制存取。

Cloudflare 與這些 EPP、IdP、XDR 和 SIEM 工具的單次整合為 CISO 提供了更多的可見度，並在多個領域自動執行安全協調流程，這樣，您的 SecOps 團隊就可以**利用現有工具取得更多成果**。

Cloudflare 的第一方風險評估以及與一流合作夥伴的風險交換



第 3 步：實施

在不斷擴大的攻擊面上實現自動化風險控制

透過前兩步，CISO 可在環境中構建一個動態、全面的風險檢視。

但最後一步是最重要的：基於在第 1 步和第 2 步中所瞭解的情況實施控制和保護。透過一個統一平台將三個步驟結合在一起，有助於在所有位置和環境中一致地套用原則，以便安全性根據您的需求而發展。

以下三個使用案例說明了如何透過 Cloudflare 將一致風險狀態管理的優勢變為現實。

使用案例 1：透過裝置狀態檢查採用 Zero Trust

Cloudflare 與 EPP 和 SIEM 工具合作來實施 Zero Trust 控制，以應對整個工作團隊中的風險。

例如，考慮這樣一種情況：威脅惡意行為者透過多種通道（包括 Web 和電子郵件）針對某個使用者發起攻擊。Cloudflare 將：

- **提供第一道防線**——封鎖對危險網站和網路釣魚電子郵件的瀏覽
- **從 EPP 工具中擷取裝置狀態**，該工具掃描並確定該使用者的裝置已感染
- **限制該使用者存取**應用程式——基於 EPP 的裝置狀態
- **與 SIEM/XDR 共用記錄資料**以便進一步分析，這可能會帶來更多的補救措施，如隔離裝置

使用案例 2：保護應用程式、API 和網站，甚至可以免遭 zero-day 威脅

安全團隊很難應對使用 zero-day 漏洞、機器人、惡意第三方用戶端指令碼、資料隱碼以及其他漏洞利用的不間斷攻擊。

為了保護應用程式、API 和網站，Cloudflare 提供以下幫助：

- **自動封鎖**惡意負載、機器人，甚至 zero-day 漏洞，利用 ML 支援的風險模型識別攻擊變體以及危險或異常流量。
- **將可見度集中**於儀表板和分析中，以便查看潛在的設定錯誤、資料外洩風險以及影響基礎架構的漏洞。

藉助 Cloudflare，組織在面向公眾的應用程式前方部署的安全措施（如 WAF、DDoS 緩解和機器人管理）同樣也可用於保護內部基礎架構，如自託管的 Jira 和 Confluence 伺服器。

使用案例 3：保護敏感性資料

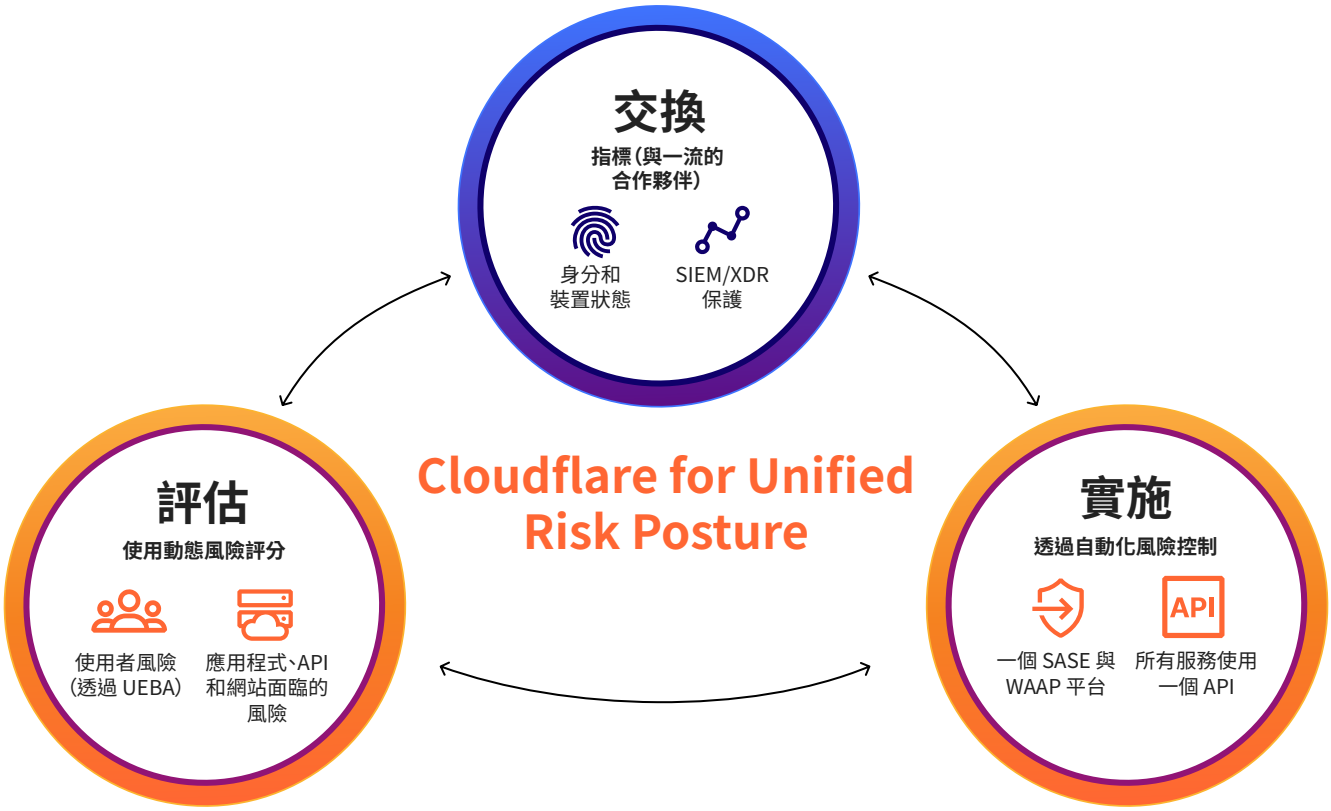
由於大數據、IoT 裝置的數量十分龐大，再加上目前 AI 和 LLM 的流行，對資料在雲端環境中的共用情況保持可見度和安全控制比以往任何時候都要困難。

利用 Cloudflare，可輕鬆識別處理敏感性資料的高風險使用者，並相應地限制存取。

例如，如果一名開發人員試圖將專有原始程式碼上傳到公用 GitHub 存放庫，Cloudflare 就會：

- **實施資料控制**來封鎖該上傳，並防止程式碼離開您的企業租用戶
- **提高使用者的風險分數**（透過 UEBA），讓安全人員針對這次可疑活動進行進一步調查
- **限制存取**直到調查完成——完全隔離或封鎖對業務應用程式的存取

為什麼選擇 Cloudflare for Unified Risk Posture



簡便性 | 透過一個平台實現一致風險狀態

Cloudflare 透過整合安全產品並簡化在人員、應用程式和網路中管理風險的方式，減少營運支出。

Cloudflare 透過將 SSE 和 WAAP 風險評分以及控制融合到一個平台和全球網路上，幫助您消除多種重疊工具，這些工具會帶來冗餘、盲點和隱藏成本。

- 減少原則構建和實施所花費的時間和精力
- 藉助服務之間的無限互通性，以自己的步調擴展保護措施
- 利用我們支援自訂和自動化的單一 API，協調所有服務
- 透過 Zero Trust 最佳做法，最大限度縮小並保護攻擊面

「Cloudflare 幫助我們更輕鬆、更有效地緩解風險，並簡化了我們在整個組織中實現 Zero Trust 的方式。」

indeed

為什麼選擇 Cloudflare for Unified Risk Posture

靈活性 | 與一流合作夥伴的單次整合

Cloudflare 可與您已在使用的工具交換風險資料。與其他廠商不同，僅建立一次整合即可在 Cloudflare 的整個平台上利用那些功能，因此，您可以專注於風險管理，而不是設定。

端點保護提供者 (EPP)：當使用者登入由 Cloudflare 保護的應用程式時，我們可以驗證裝置是否受 EPP 保護，EPP 可以檢查裝置是否已感染惡意程式碼或存在任何其他作用中安全威脅。在某些情況下，Cloudflare 會從 EPP 合作夥伴擷取風險分數，來進一步驗證裝置是否被視為風險過高而無法存取內部應用程式或網路功能。這種即時的資訊交換可以自動關閉威脅。

身分識別提供者 (IdP)：與此同時，身分識別提供者會驗證存取網路的員工是否是他們所聲稱的身分。Cloudflare 與領先的 IdP 合作，來遏止詐騙性存取嘗試，包括不可能的旅行事件。

SIEM/XDR 提供者：我們的協同合作也擴展到了 SIEM 和 XDR 合作夥伴，他們將來自 Cloudflare 的資料全部擷取至集中式儀表板中。這樣，安全分析師便能夠迅速偵測並應對安全威脅。一些 XDR（包括由 AI/ML 提供支援的那些 XDR）透過高保真度警示來提示分析師，使其做出果斷回應，在威脅升級之前將其消除。

擴展 | 透過一個全球網路提供實施和威脅情報

每一項安全服務都可供客戶在 320 多個網路位置中的每一處執行（截至 2024 年第一季）。單遍檢查和原則實施始終快速、一致且具有復原能力。

此外，我們用於識別風險的採用 AI/ML 技術的模型由來自我們全球網路的獨特資料提供支援，包括：

- 作為將近 20% 的 Web 使用的反向代理可獲得的可見度
- 每天約 3 萬億個 DNS 查詢
- 每 2 週爬取超過 80 億個網頁
- 平均每天封鎖 2090 億次網路威脅

「有了單一的 Cloudflare 解決方案來幫助我們管理全球營運的複雜性，我們的生活變得輕鬆多了。Cloudflare 一路相隨，始終為我們提供支援。」

Delivery Hero

瞭解更多

Cloudflare for Unified Risk Posture 是一套新的網路安全風險管理功能，可以幫助企業在不斷擴大的攻擊面中實現自動化和動態的風險狀態實施。

進一步瞭解 Cloudflare 的統一方法

+ 886 8 0185 7030 | enterprise@cloudflare.com | cloudflare.com/zh-tw

REV:BDES-5826.2024MAY15