要的不止是合規！看 FortiDLP 如何讓數據安全更智能、更全面

Josh Lin 林裕祥 / Fortinet 首席工程師

Title

新版 ISO 27001 真的可以助企業強化防禦？

ISO 27001 : 2013專注在資訊技術，ISO 27001 : 2022 最重要的變化則是加入網宇安全（Cyber Security）與隱私保護，並新增相關條款

1

資訊安全

Information Security

保護重要與敏感資訊及系統，防止未授權存取、竄改、毀損與中斷，確保機密性、完整性與可用性

2

網宇安全

Cyber Security

保護虛擬空間及其設備與資訊，免受勒索病毒、挖礦程式等網路攻擊，確保系統穩定運作

3

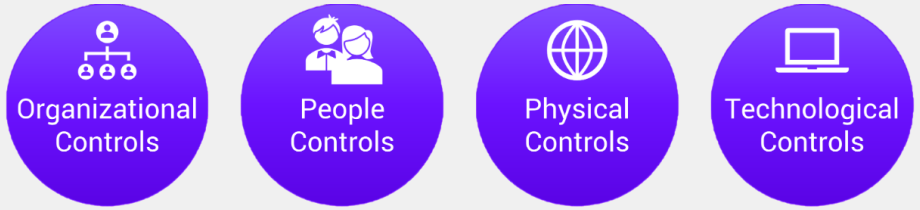
隱私保護

Privacy Protection

兼顧法規與商業應用，以風險導向保護個資與隱私，防範資料外洩

ISO/IEC 27001：2022 架構

15 大執行能力與 4 大領域



治理
人力資源安全
安全配置
系統和網路安全

資訊保護
資料管理
識別與存取管理
應用系統安全

實體安全
威脅和脆弱性管理
供應商關係安全
法律與遵循性

持續性
資訊安全保障
資訊安全事件管理

組織
人員
實體
技術

ISO 27001:2022 vs 2013：不能忽略的核心差異

- 2013 版包含 114 項控制措施 分為14章節
- 2022 版包含 93 項控制措施 分為4個章節

組織 37 個控制措施 | 實體 14 個控制措施
人員 8 個控制措施 | 技術 34 個控制措施

- 沒有刪除任何控制措施 但把許多項目合併在一起，從而減少了總體數量
- 2022 版引入 11 個新控制措施

	Controls	控制措施
[A.5.7]	Threat intelligence	威脅情資
[A.5.23]	Information security for use of cloud services	雲服務資訊安全
[A.5.30]	ICT readiness for business continuity	資通訊技術營運持續整備
[A.7.4]	Physical security monitoring	實體安全監控
[A.8.9]	Configuration management	組態管理
[A.8.10]	Information deletion	資訊刪除
[A.8.11]	Data masking	資訊遮罩
[A.8.12]	Data leakage prevention	資料外洩防護
[A.8.16]	Monitoring activities	監視活動
[A.8.23]	Web filtering	網站過濾
[A.8.28]	Secure coding	安全程式碼撰寫

傳統 DLP 的三重防線的架構與挑戰

提供差異化的覆蓋範圍

網路 DLP

- 網路流量可視性
  針對傳輸中數據及動態數據
- 在網路環境中部署監聽或阻斷模式
- 要先進行加密流量管理

終端 DLP

- 終端活動的能見度：伺服器、電腦裝置、雲端存儲庫、移動設備正在使用、傳輸的數據
- 檔案的寫入、讀取、可移動磁碟的控管
- 終端程序執行監控

雲服務 DLP

- 雲端中資料的可見性：雲端儲存和授權的雲端應用程式使用中的數據、靜態數據

數據風險

保護敏感數據免遭外洩或意外洩露

智慧財產權

- 設計文件
  專案計劃
  專利申請
  程式原始碼
  流程文件
  商業秘密

公司機密

- 財務報表
  員工記錄
  定價文件
  使用者登入

客戶數據

- 一般用戶登入
  信用卡號碼
  社會安全號碼
  醫療數據

保護數據一直是一場艱苦的戰鬥

$4.88M

數據洩露的平均成本

網路複雜性增加

內部人員相關的事件呈上升趨勢

遠端和混合工作力

員工不當行為佔數據披露的大多數

多數組織都有 DLP，然而對 DLP 投資報酬率一點都不滿意。

資料爆炸式持續增長

影子 SaaS 和影子 AI

55% 由於員工疏忽造成的事故百分比 **$7.2M** 修復這些事件的平均年成本

Source: Cost of a Data Breach Report 2024," Ponemon Institute - 2024
Source: "2023 Cost of Insider Risks: Global," Ponemon Institute – October 2023

數據保護的挑戰，企業為何難以跨越？

合規永遠是防護的終點線

策略過多管理繁瑣

過多的策略選項難以確保統一性與一致性，管理成本顯著增加

機敏資料難以界定

機敏資料的定義具有高度主觀性，且各部門的理解不同，導致無法達成統一標準，進而影響資料保護政策的有效性

告警過多無法篩選

經常會產生很多告警，這些告警的嚴重程度和真實的威脅不一樣，讓安全團隊很難分辨哪些問題最需要處理，容易讓人感到疲憊，而忽略了真正的風險

即時風險反應不足

傳統策略無法及時應對新的資料洩漏手段，且需要不斷更新才能保持有效性，這對企業的適應能力提出了高要求

過度干預業務受阻

過於細微的策略干擾正常業務流程，造成員工操作不便或業務效率下降，甚至可能引發對 DLP 系統的反彈

跨部門合作流程繁瑣

需要 IT、法務、合規及業務部門的合作才能準確定義和實施，這使得政策的制定過程變得繁瑣且耗時

情境一：檔案類型變更的風險挑戰

情境說明

員工從 CRM 下載了一份客戶資料清單作為 .csv 文件，並將其副檔名更改為 .png / .pdf。將重新命名的檔案上傳至線上共享儲存空間

傳統 DLP 會怎麼做

依字典檔 / 分類標籤識別資料，根據手動定義的規則觸發動作。上傳行為可能會被偵測到，如果無法讀取正在上傳的資料，將成為一個洩露管道，最終用戶仍能成功上傳

你想要的 DLP 應該怎麼做

資料從下載到端點就會被標記是否為敏感資料，所有操作在端點都會被追蹤，一旦文件被發送出去，會追蹤數據來源。無論上傳的檔案是否可以讀取，它都會比較來源是否標記為敏感資料，如果來源敏感，立即阻止上傳操作

情境二：內部員工突發數據外洩行為

情境說明

某企業的財務部員工平時只會存取內部 ERP 系統中的財務報表，但某天突然大量下載敏感數據，並試圖透過雲端（如 Google Drive）或 WebMail 上傳

傳統 DLP 會怎麼做

依賴靜態規則，定義關鍵字或建立文件指紋，封鎖所有含「財務數據」的檔案傳出，但這樣的策略可能會影響正常業務流程，例如合法的財務報表發送，無論誤擋或漏擋，都只能被動的調整策略

無 AI 分析能力，無法偵測「正常 vs. 異常」行為，容易造成誤判

你想要的 DLP 應該怎麼做

自動學習該員工的日常行為模式，透過 AI 分析使用者歷史行為，建立基準線，如正常存取頻率、檔案大小、傳輸管道等，當偵測到異常時，觸發更嚴格的 DLP 政策

情境三：非授權的機密資料移動

情境說明

員工將機密文件複製到 USB 儲存設備中，並攜帶離開公司，這可能會導致資料洩漏

傳統 DLP 會怎麼做

可能會檢測到數據的傳輸，但往往只能基於預設的靜態規則進行處理，缺乏對 USB 設備的精細控制，難以識別不同設備之間的風險差異，傳統 DLP 系統對 USB 儲存設備的控制也較為薄弱，尤其是在Linux / Mac環境下

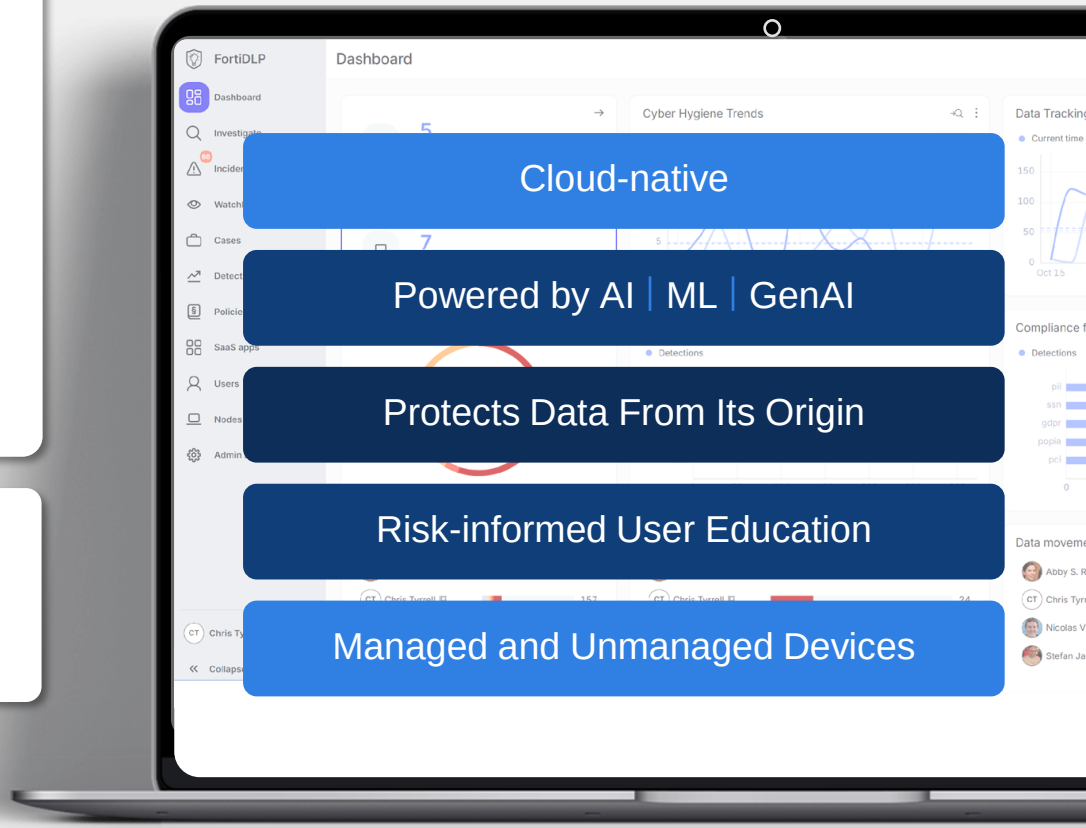
你想要的 DLP 應該怎麼做

能夠識別所有接入設備，包括 USB 儲存設備、外部硬碟、隨身碟等，並對這些設備進行監控，即使在使用 Android ADB 作為傳輸工具，也能提供完整的能見度，在Windows或Linux環境下，功能應該一致

FortiDLP ：AI 驅動的智能防護

新世代端點 DLP 和內部風險管理解決方案，可預測並防止數據竊取

- 對資料流和風險的全面可見性
  即時上下文和內容等級檢查
  跨 SaaS 應用程式的資料保護
  專注於資料訪問時，根據風險對用戶進行宣導



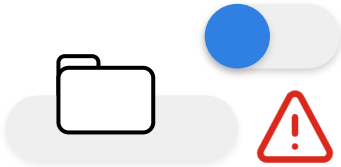
資料外洩防護

內部風險管理

SaaS
數據安全

自動將檢測映射到 MITRE ENGENUITY™ 內部威脅 TTP 知識庫

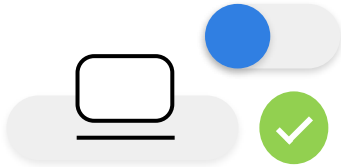
FortiDLP FortiGuard DLP 傻傻分不清



端點資料外洩防護

AI/ML 驅動進化

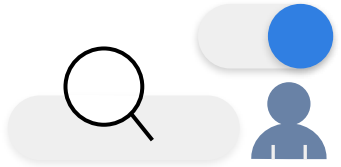
- 檢查上下文 / 內容
- 防止數據被盜
- 確保合規性



內部風險管理

GenAI 驅動進化

- 監控用戶行為
- 識別風險活動
- 減輕風險



SaaS 服務資料安全

數據存取
使用管理限制

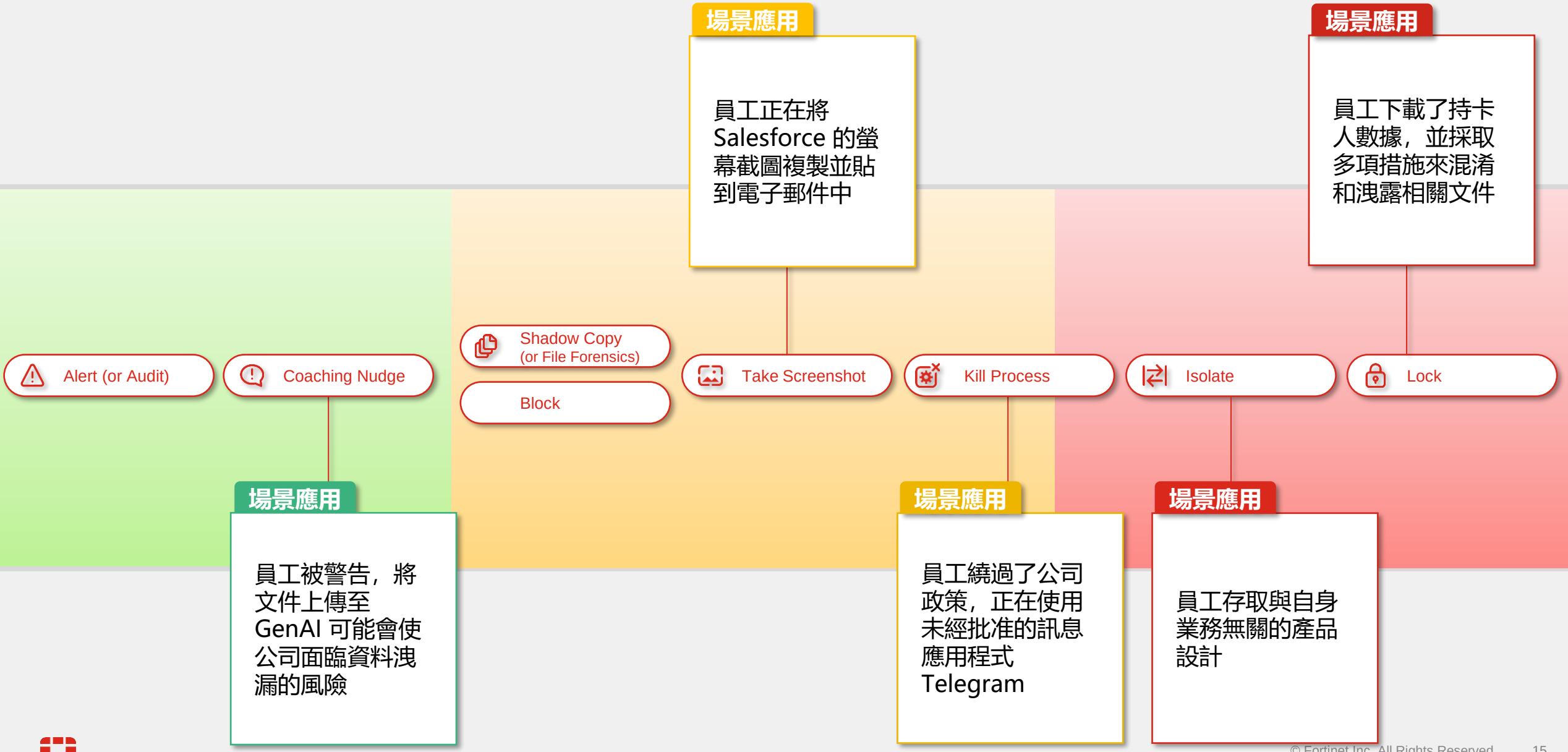
- 對各個 App 進行風險評估
- 追蹤數據流向
- 管控 GenAI 使用

風險導向的用戶教育宣導

- 提示 / 輔導用戶
- 推動責任感

保護數據需要全面且深入的情境能見度

豐富的回應動作



有效防止數據洩漏

新世代數據外洩防護

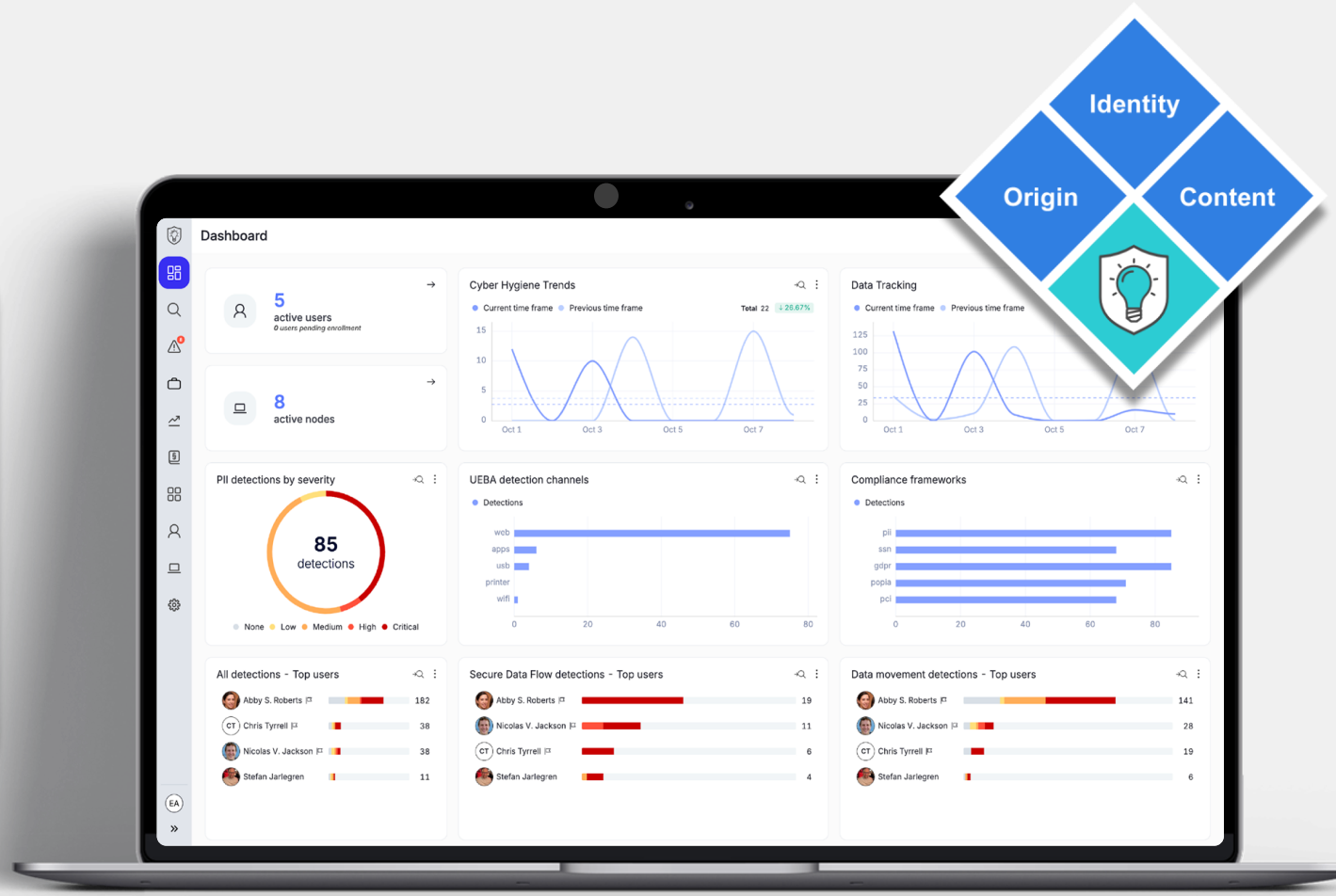
- 雲原生 SaaS 解決方案：幾分鐘內即可啟動

  從第一天起就提供真實的數據保護

  在訪問敏感數據時即時執行上下文和內容分析

  從源頭保護數據

  落實資料外洩防護相關的核心法規遵循要求與控制措施

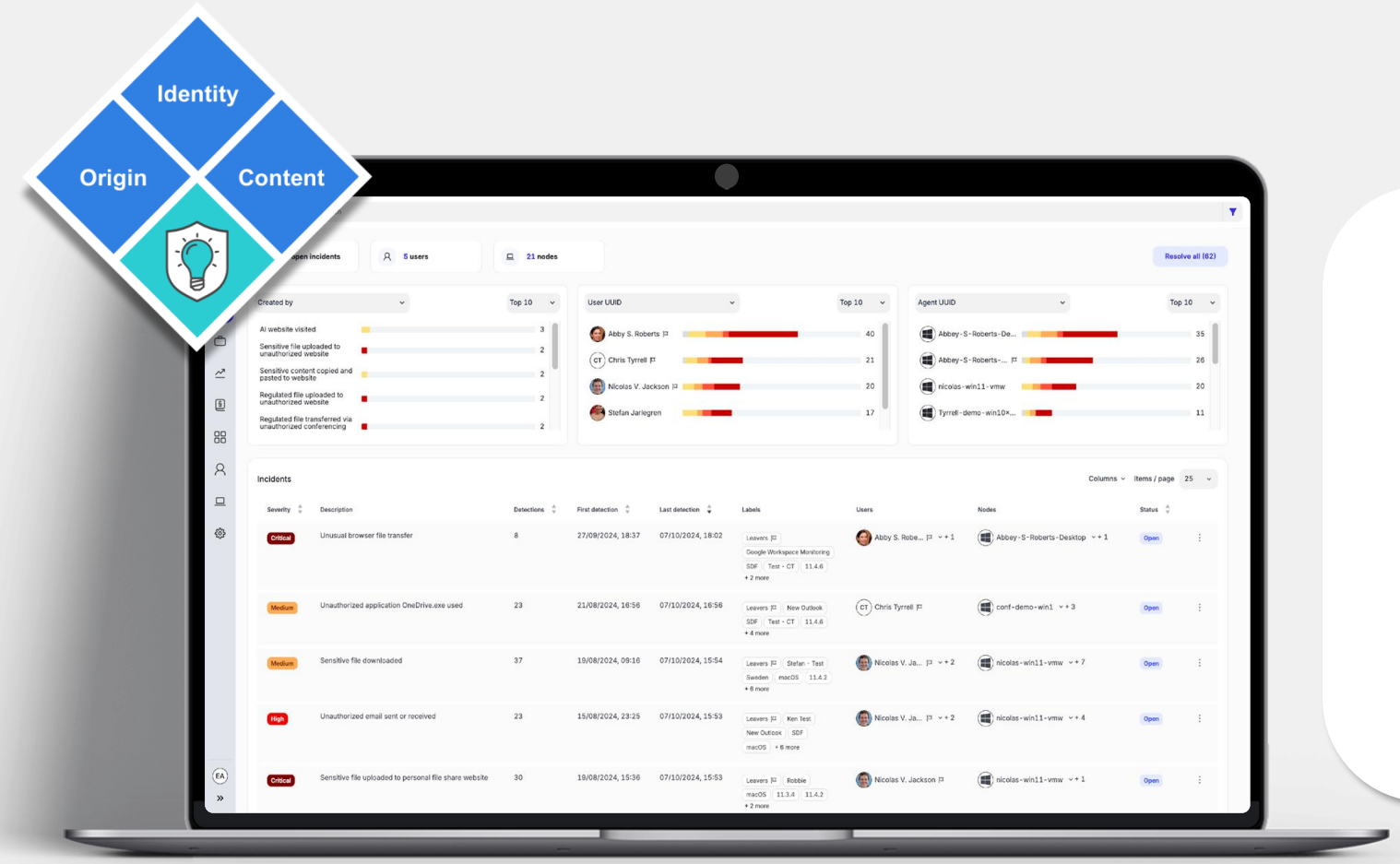


AI 驅動
智能學習

保護數據的
機密性和完整性

任何地方
任何時間

內部風險管理



全面瞭解用戶行為和高風險員工行為

- 增強內部威脅偵測和回應

  深入瞭解使用者如何存取檔案、應用程式和系統

  將高風險內部活動進行情境化分析

  查看並阻止對未經批准的 SaaS 應用程式的存取

  提供匿名化，保護隱私

FortiAI
(人工智能助理)

安全資料傳輸

內部風險
流程檢測

內部風險功能：關鍵焦點

AI 和機器學習在感測器、端點或雲端中的應用

以合理成本實現效益

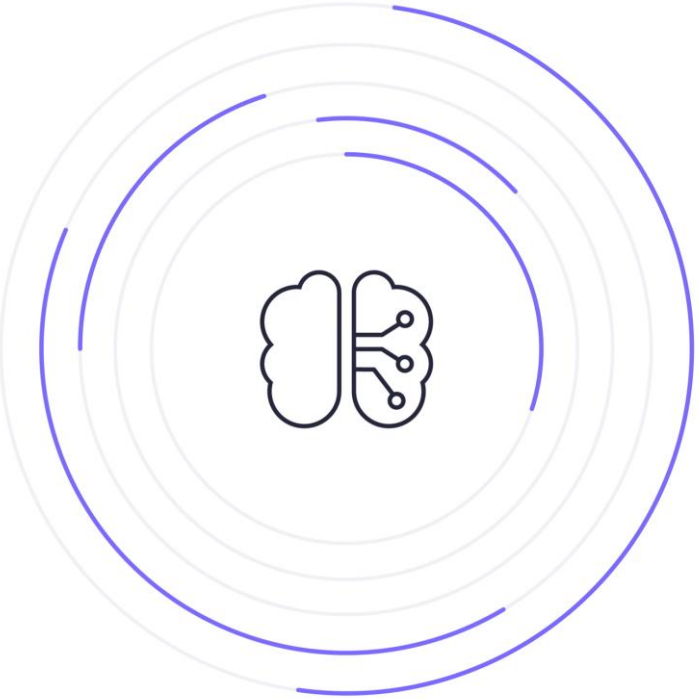
- 分散式代理（agent）技術避免了對大型、高可用性且通常昂貴的雲端基礎設施的需求
  用戶離線仍然保護資料

代理程式上的所有策略決策可確保資料安全和員工隱私

- 在代理程式上執行的所有內容檢查
  最小化對終端用戶體驗的影響；
  代理程式等待雲端基礎設施和資源時不會產生延遲

代理程式依需要即時獲取上下文信息，而不是事先獲取

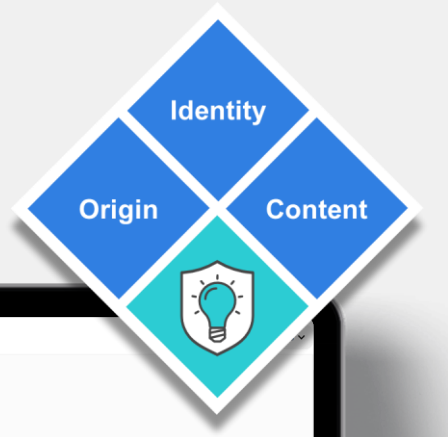
- 代理程式可以根據檔案來源的上下文，決定是否在上傳檔案至檔案共享時進行內容檢查，例如檢查是否包含敏感資訊或是否存在安全風險，並且僅在必要時執行這些檢查
  不需要在每個事件發生時將相關的上下文資料（例如，使用者行為、資料來源等）傳送到雲端，提高效率並減少對雲端資源的依賴



情境、AI、UEBA 模型的結合，
檢測異常的高風險用戶行為

SaaS 數據安全

SaaS 應用程式和 GenAI 風險評估與 DLP 控制



針對 SaaS 應用程式的全面可視化 (包括影子 AI)，無論是未受監控或未經批准的資料

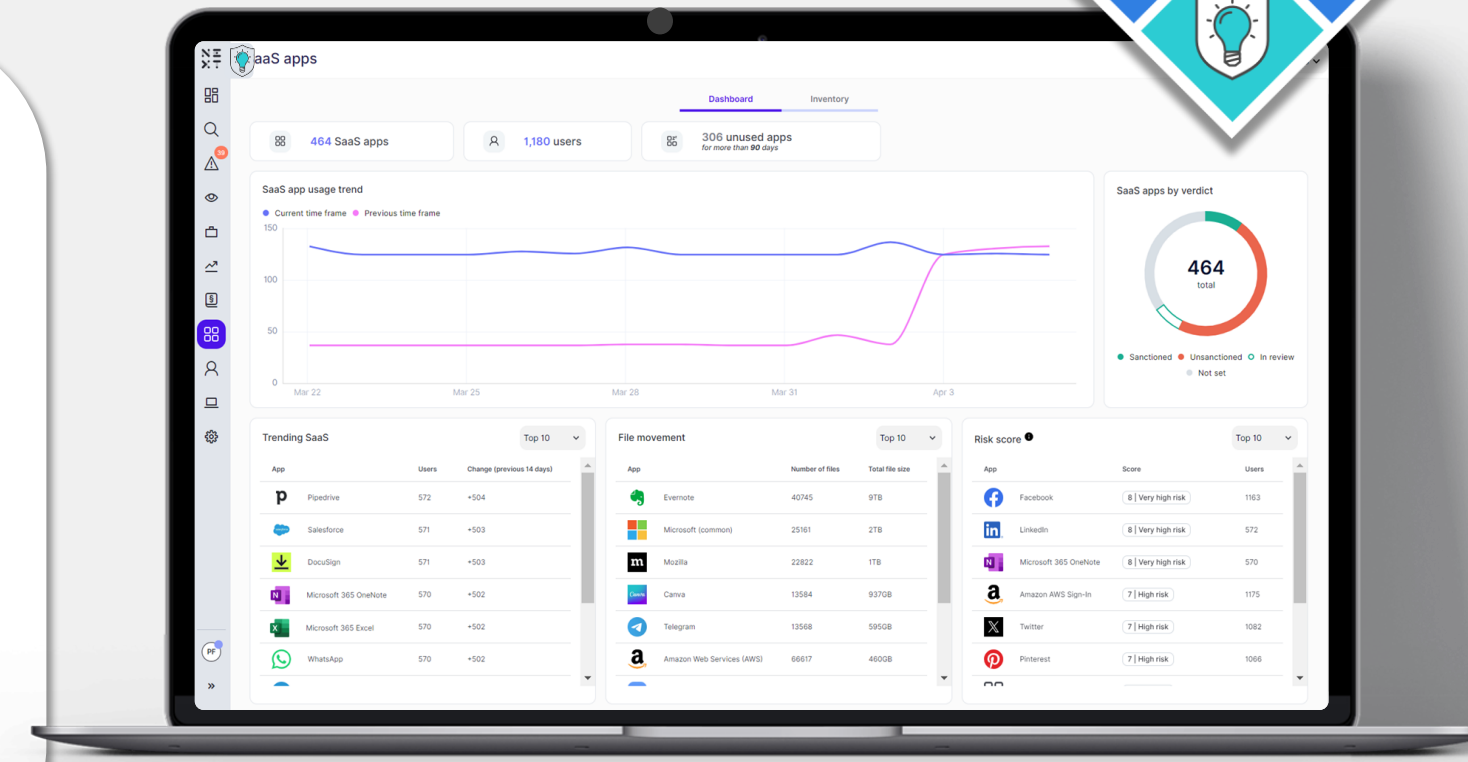
- 跟蹤、分類和風險評估 SaaS 應用服務

  資料進出流動與風險的可視化

  了解整個組織中 GenAI 的使用情況

  揭露未經授權的敏感資料流

  識別未經批准的 SaaS 應用程式使用情況和使用不安全的個人帳戶來存取服務



資料及
身份識別

影子 AI
資料保護

安全資料傳輸

風險導向的使用者教育宣導

產生風險行為時即時宣導或提醒

- 提高員工意識，強化責任追究，確保他們對自己的行為負責
  提醒或引導員工在存取敏感資料時遵循正確的資料處理做法
  根據資料的敏感性（上下文和內容），採取各種不同的政策措施
  無論員工是遠端工作還是離線工作，都會提供適當的引導

基於風險的動作

教育宣導

安全資料傳輸

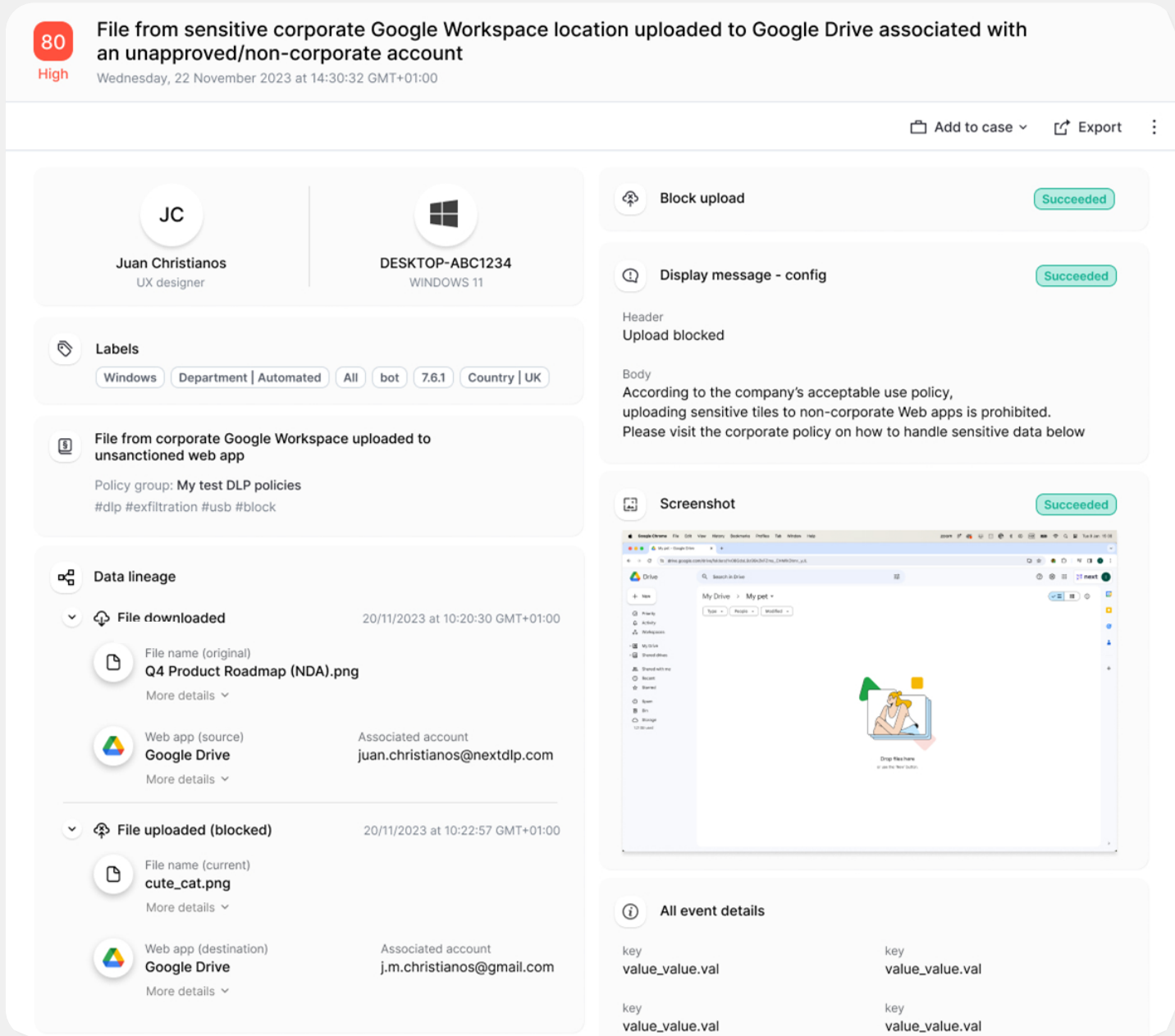
安全資料流：從來源追蹤資料，讓問題更容易發現

有心或無心的意圖

- 離職員工將產品規劃資料外洩到個人雲端硬碟
- 員工試圖透過重新命名檔案來掩蓋痕跡

回應

- Secure Data Flow 可識別從企業 SaaS 應用程式下載的資料，從來源就開始追蹤資料
  代理程式會監控檔案的狀態，包括檔案的建立、修改、更名等操作，所有的操作會被記錄，確保資料安全及合規性
  在檔案傳輸或外洩的過程，檔案會根據資料的來源（如企業雲端硬碟）和目的地（如個人雲端硬碟）進行控制

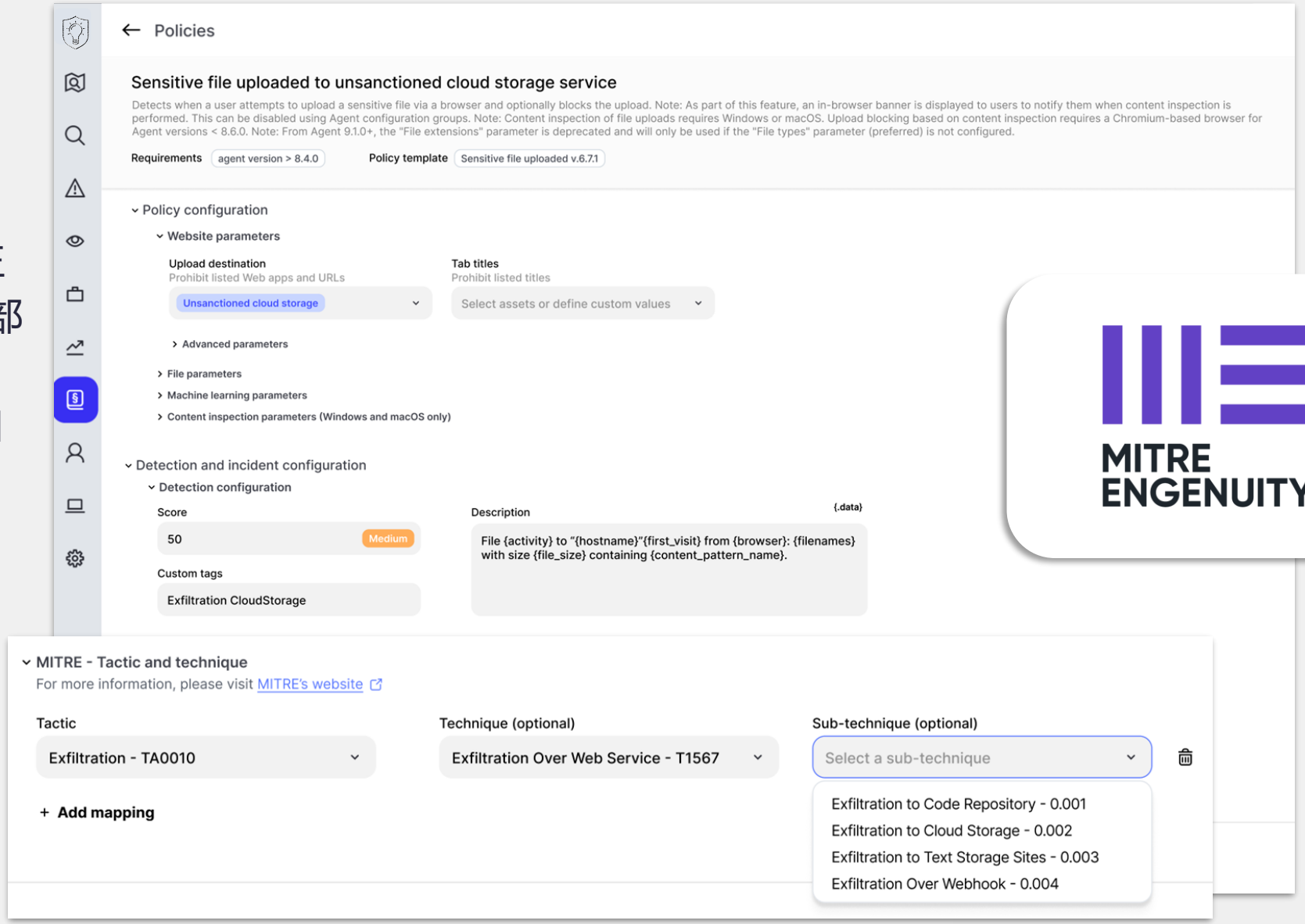


內部風險檢測自動對應 MITRE IT TTPs

加速調查和回應

風險評分

- 安全政策檢測識別高風險活動
  每個策略檢測都會自動對應到正確的 MITRE ENGENUITY™ 內部威脅 TTP 知識庫
  政策管理員可以根據實際需求自訂分配的 TTP



MITRE ENGENUITY™

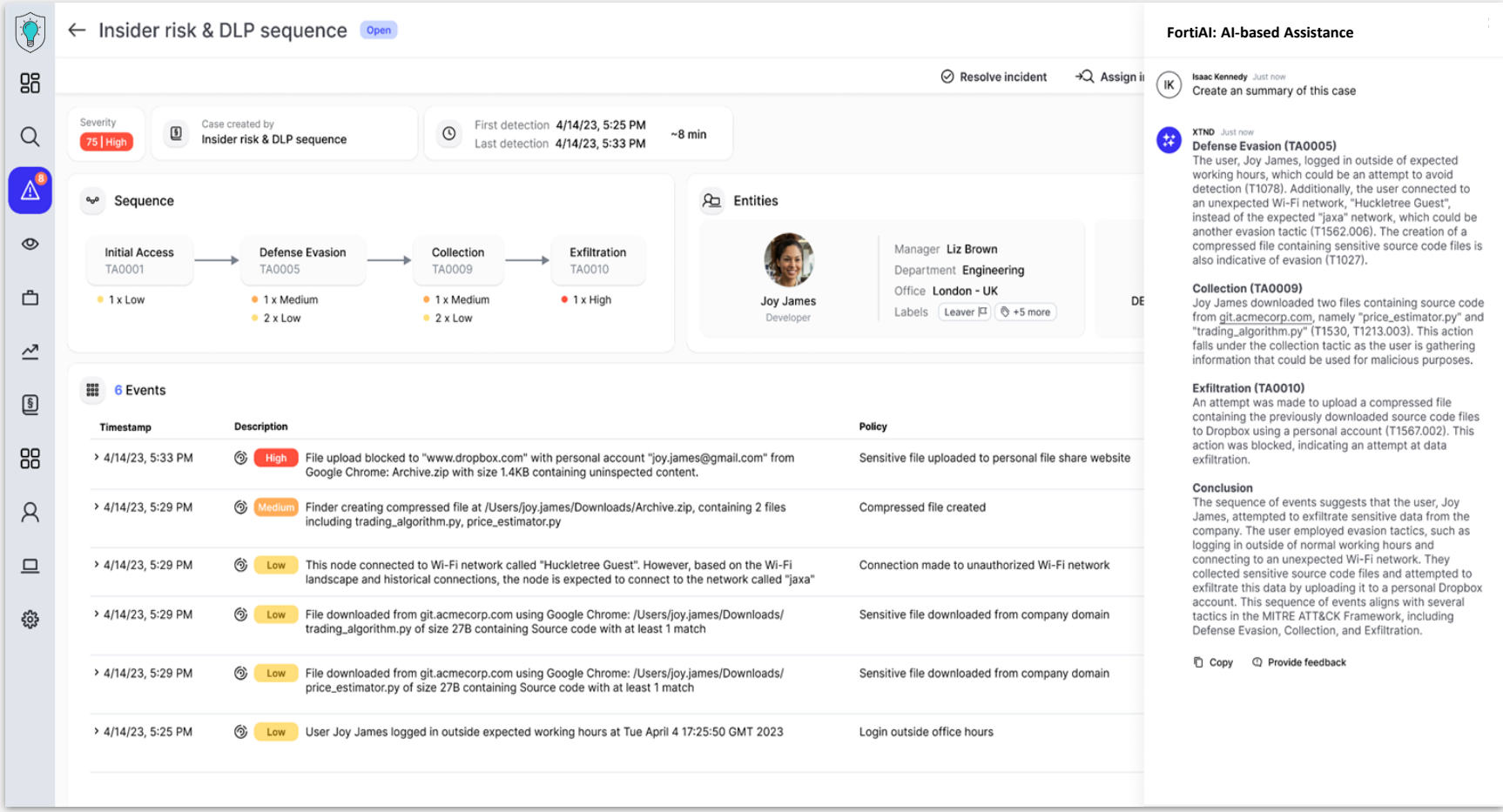
Research Partner

FortiAI（人工智能助理 ）你要的它都知道

智能生成事件報告全方位洞察

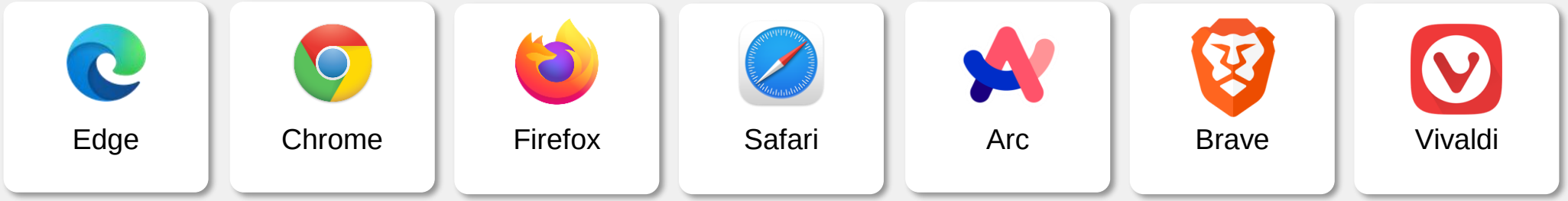
FortiAI 24/7 全天候守護

- 系統管理者啟動 FortiAI (人工智能助理)
- 請求針對內部威脅活動進行總結，並參考 MITRE ENGENUITY™ 內部威脅 TTP 指標
- 基於所提供的事件數據，透過智能演算法或人工智能技術，對資料進行深度分析和邏輯推理，從中找出關鍵並提供詳細摘要



端點插件整合：無縫連接，擴展能見度

OS Support

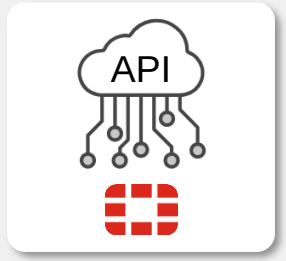


Browser Extensions

Cloud Drive Connectors

Add-ins

跨平台整合：實現完整且全方位的安全防護



Open API

Webhooks

Azure Sentinel

Splunk

Panther

SIEM

Tines

Torq

SOAR

Microsoft Entra ID

Google Cloud Identity

Okta

Identity

Microsoft Entra ID

Google Workspace

LDAP

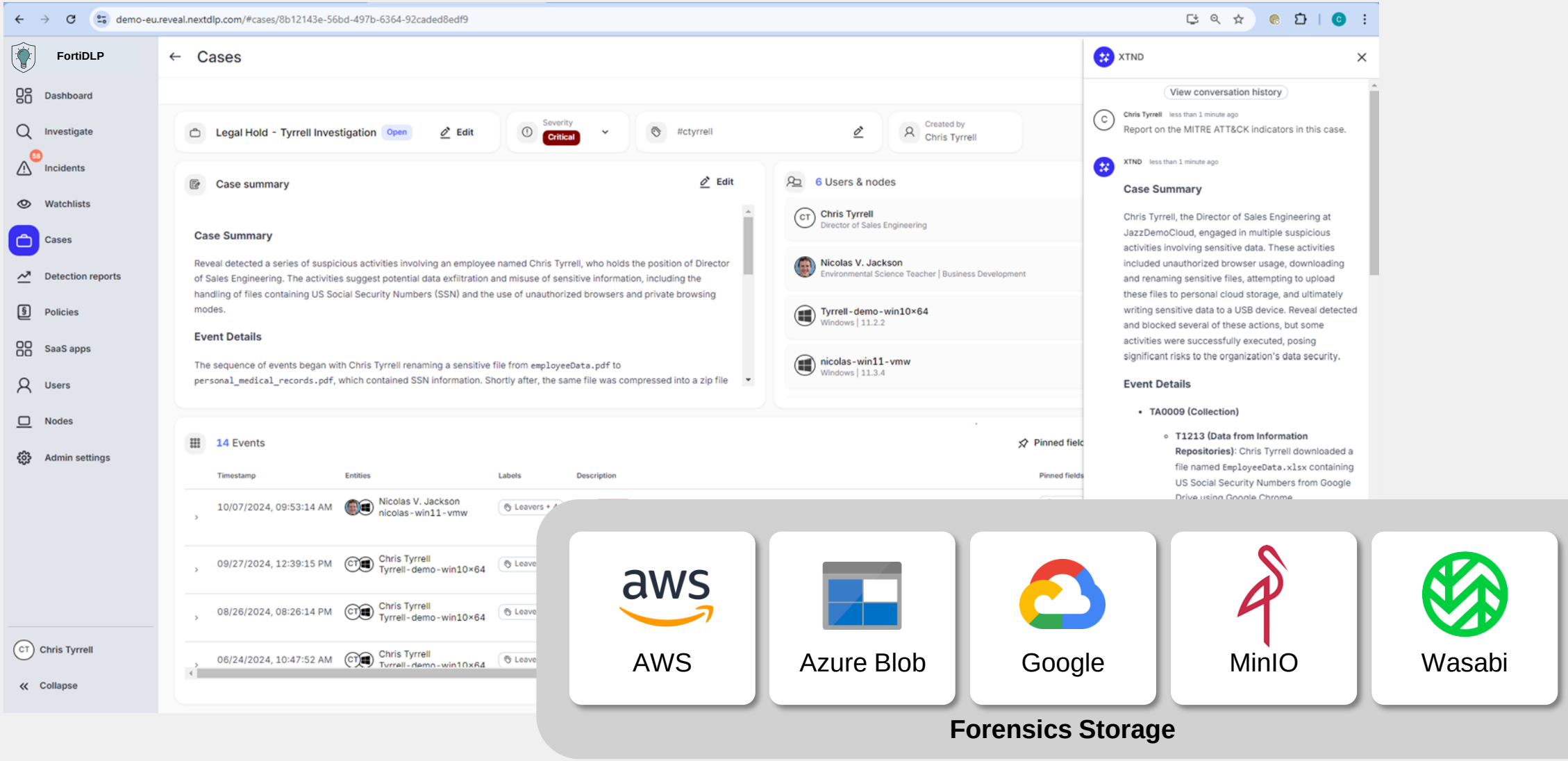
Directories

Microsoft Purview

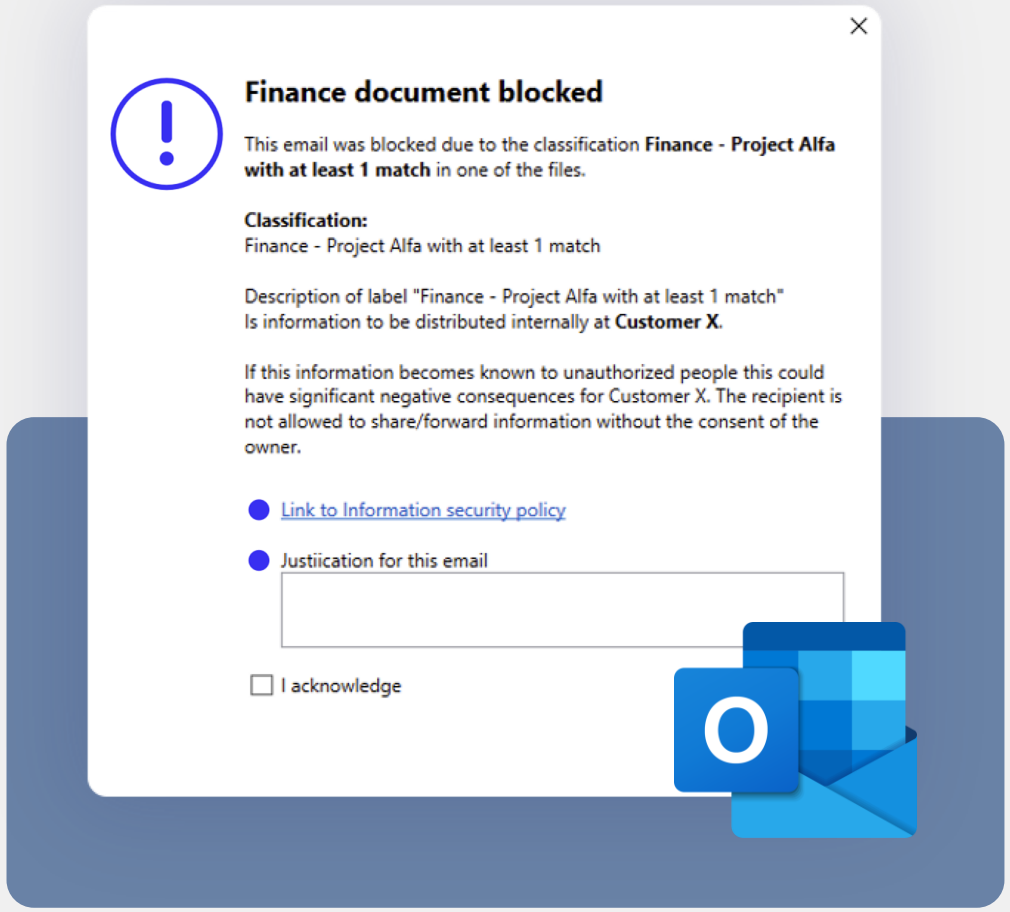
Data Classification

調查與取證：揭開真相的安全工具

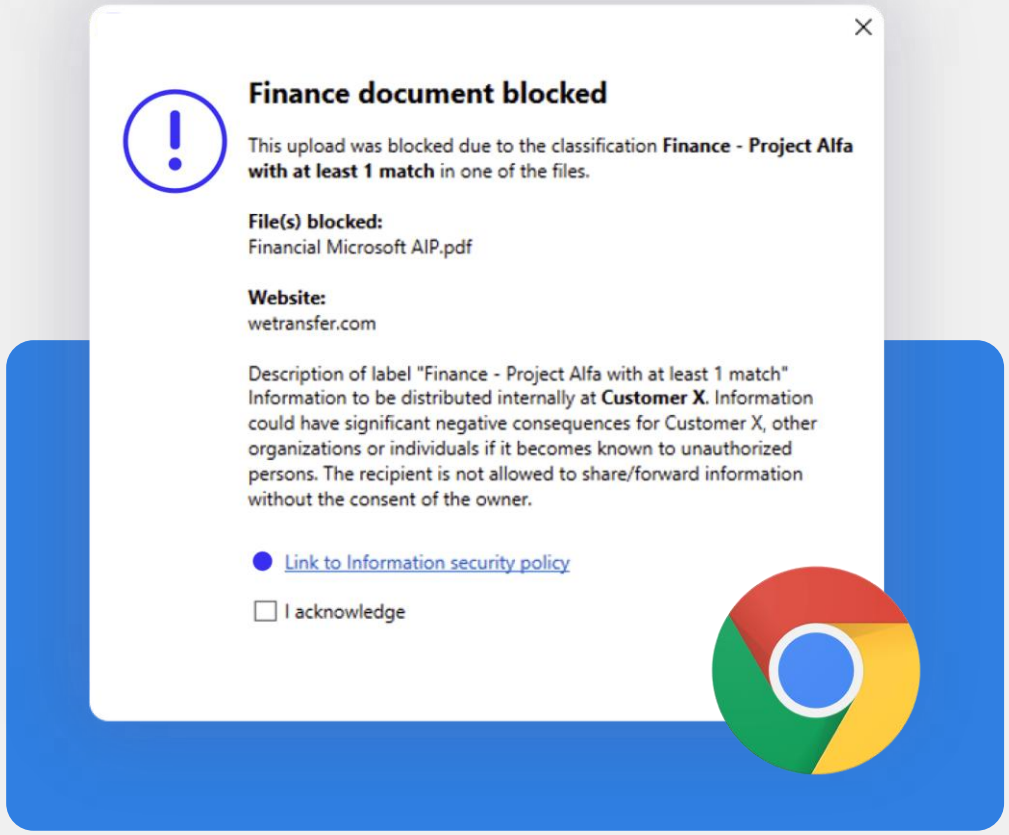
在自己管理或控制的範圍內進行的取證分析



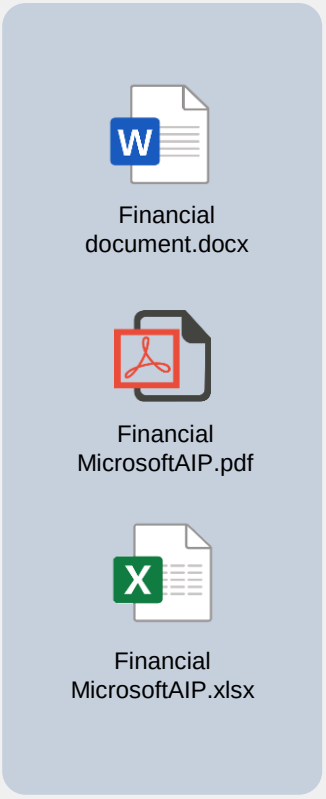
資料傳輸：阻止資料外洩嘗試



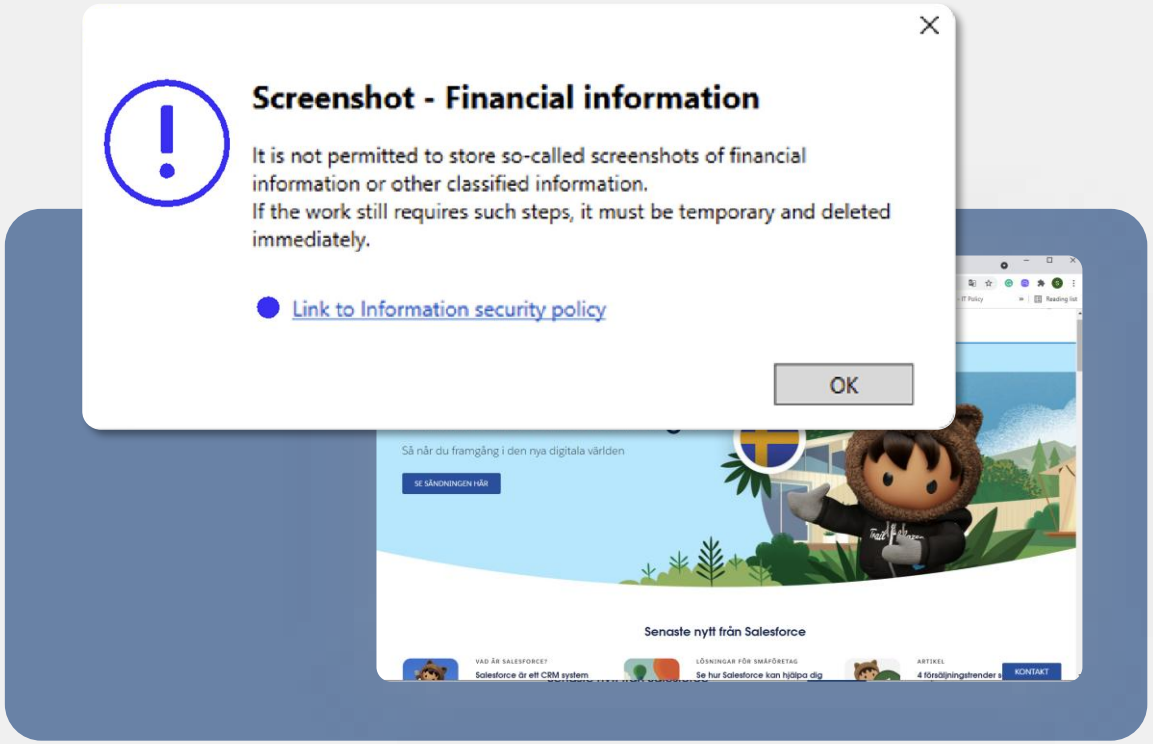
透過 Outlook 傳送



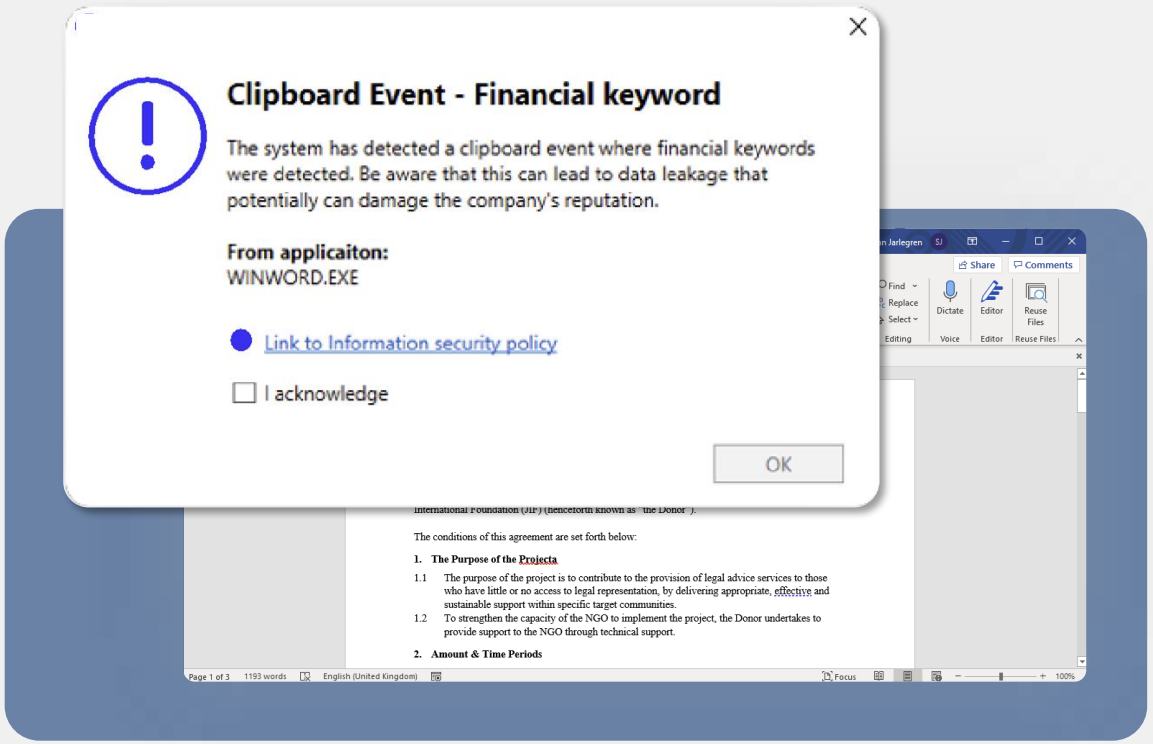
透過 Browser 傳送



宣導：教育員工，減少人為安全風險

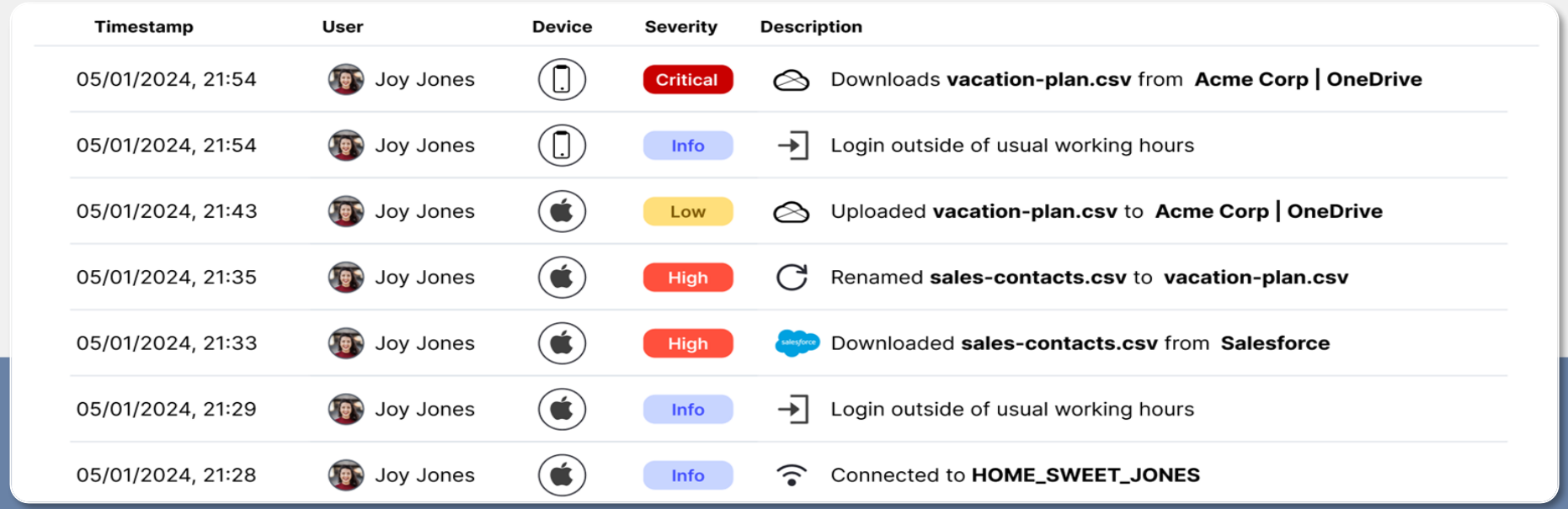


透過螢幕截圖



透過系統剪貼簿

外洩事件：SaaS 應用的可見性與控制



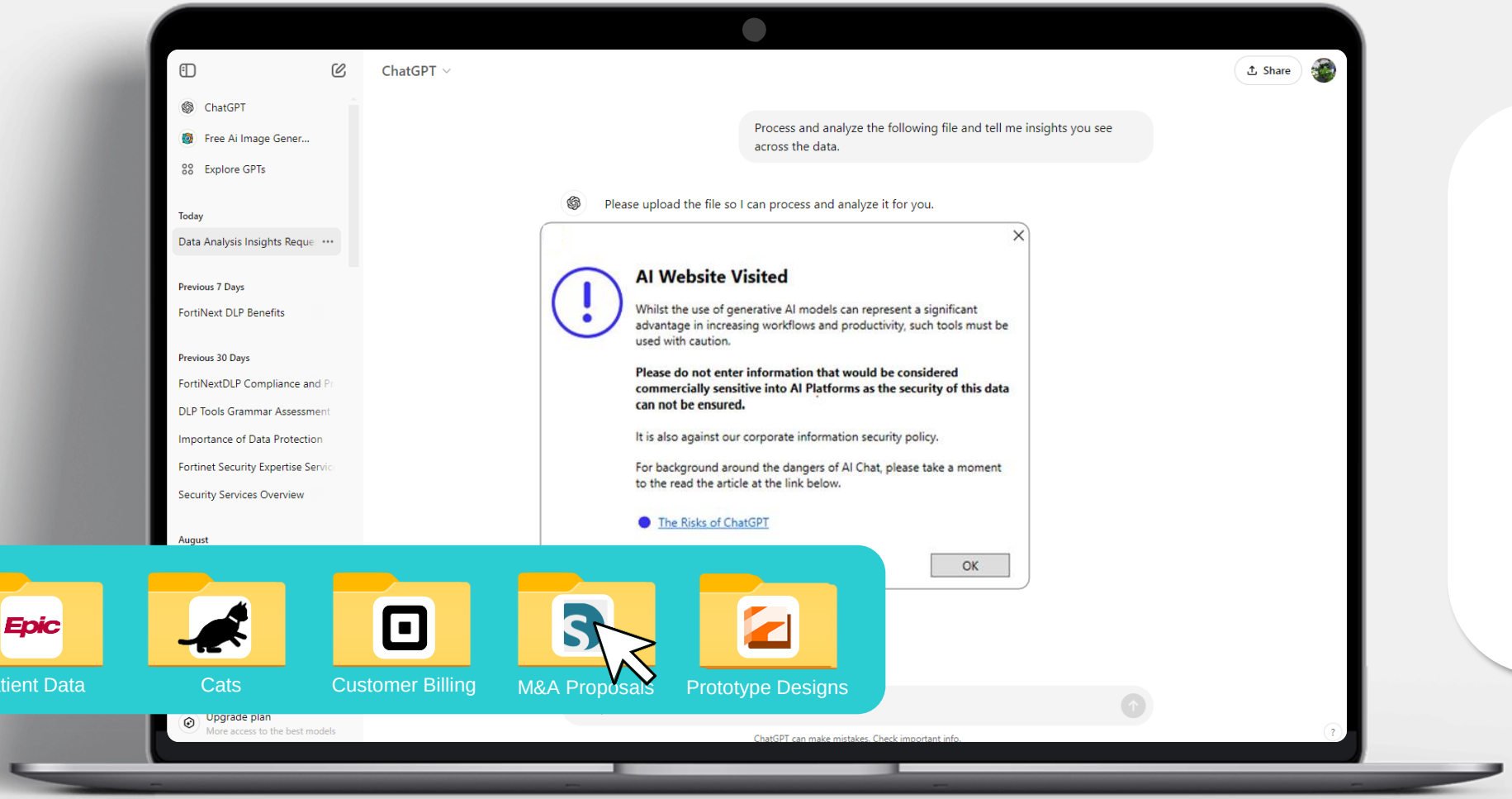
Timestamp	User	Device	Severity	Description
05/01/2024, 21:54	Joy Jones		Critical	Downloads **vacation-plan.csv** from **Acme Corp | OneDrive**
05/01/2024, 21:54	Joy Jones		Info	Login outside of usual working hours
05/01/2024, 21:43	Joy Jones		Low	Uploaded **vacation-plan.csv** to **Acme Corp | OneDrive**
05/01/2024, 21:35	Joy Jones		High	Renamed **sales-contacts.csv** to **vacation-plan.csv**
05/01/2024, 21:33	Joy Jones		High	Downloaded **sales-contacts.csv** from **Salesforce**
05/01/2024, 21:29	Joy Jones		Info	Login outside of usual working hours
05/01/2024, 21:28	Joy Jones		Info	Connected to **HOME_SWEET_JONES**

全面監控 SaaS 和裝置應用程式

高風險活動的防護策略

影子 AI：保護敏感資料在 AI 工具中的分享

當員工使用未經批准的、時下流行 GenAI 工具時，能保護企業資料的同時不影響生產力

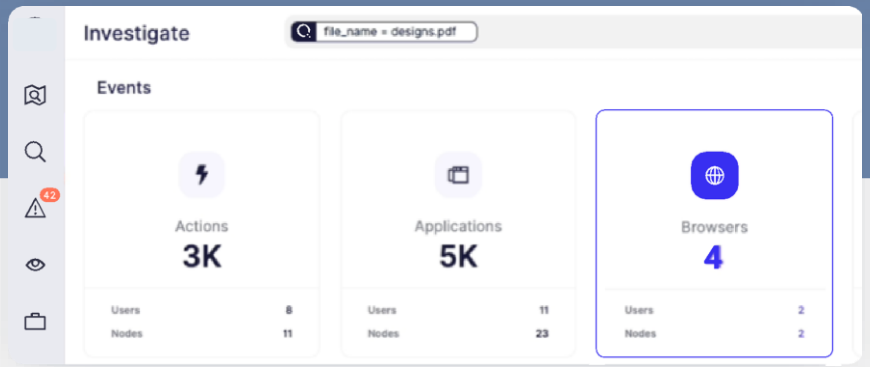


防止員工將敏感數據上傳到 GenAI 和其他 AI 工具

- 當員工/使用者的行為可能暴露敏感資料時，發送警報通知
  宣導員工正確處理資料的責任

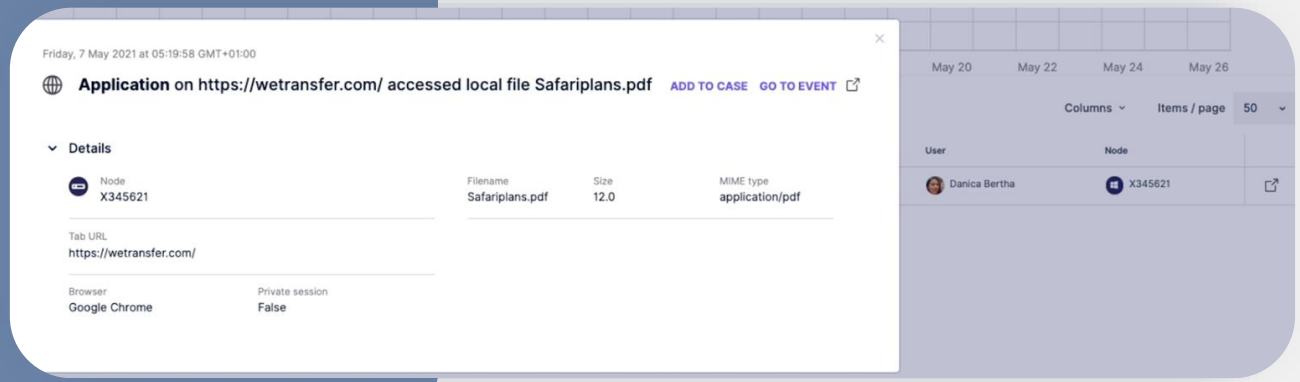
快速有效地調查資料外洩事件

1 強大的檔名搜尋功能，顯示相關的事件流

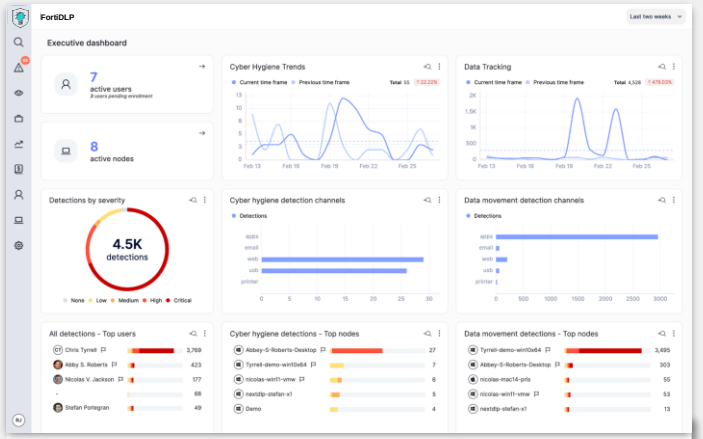


2 觀看瀏覽器事件，查看詳細的背景 / 上下文資訊來縮小搜尋範圍

3 識別到資料外洩事件，詳細過程已被完整記錄下來

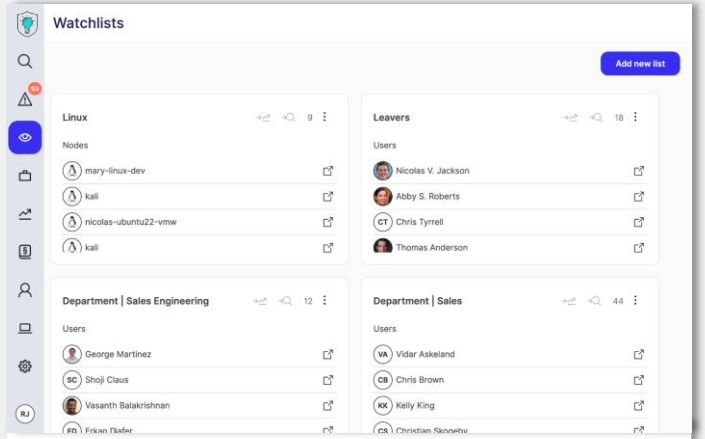


彈性且多樣化的報表



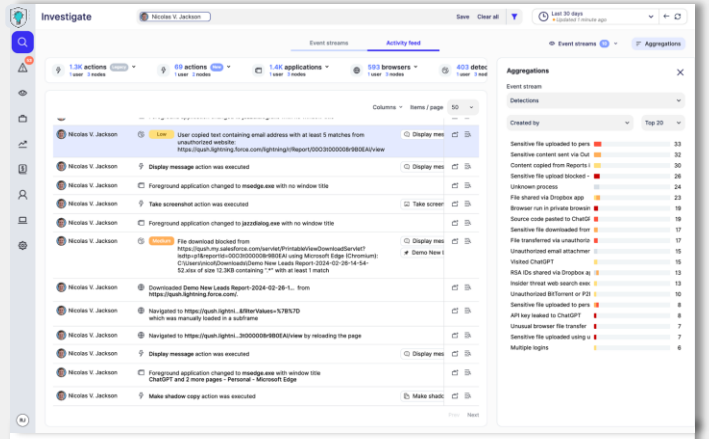
執行報告

設備基本安全措施、實踐和資料移動



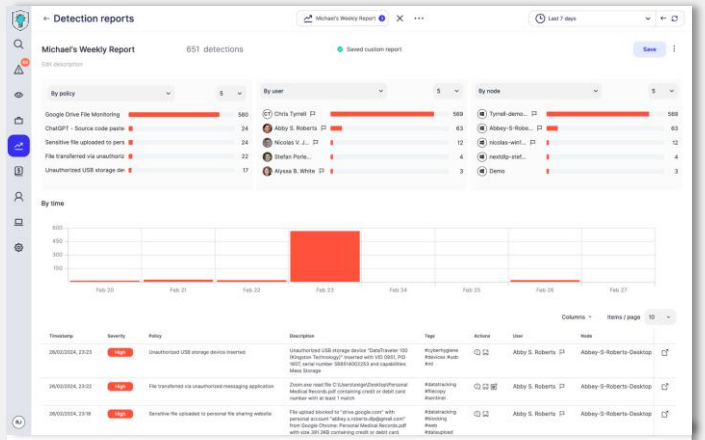
監視清單：離職員工和特權使用者

標註使用者為高內部風險的對象



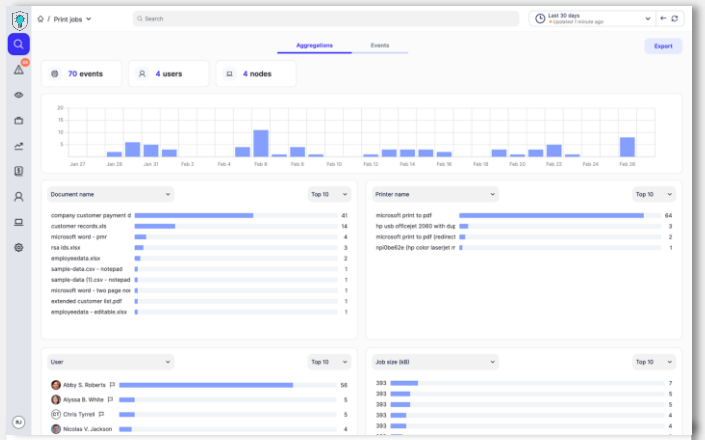
使用者活動紀錄

依時間順序顯示使用者活動



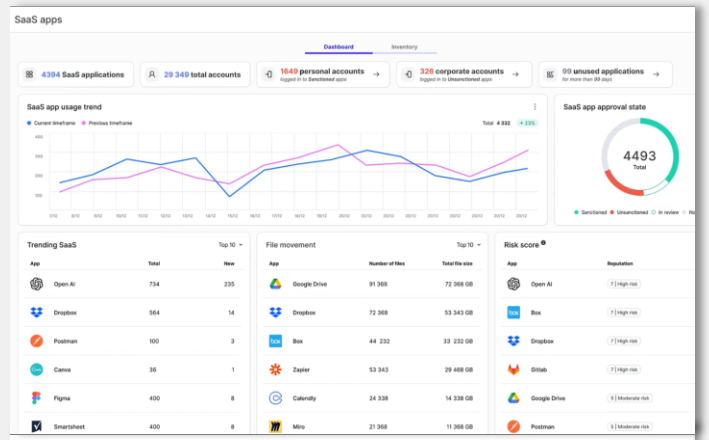
自訂報告

使用進階邏輯生成報告



行為分析

識別異常和高風險活動



SaaS 數據安全儀錶板

發現未經授權的影子 IT

100+ 遍佈全球的客戶

涵蓋多樣化的產業應用與客戶規模

coinbase
RIVIAN
dyson
Versant Health
Investec
KARMA
scansource
DrFirst Unite the Healthiverse
NORGES BANK INVESTMENT MANAGEMENT
tpi COMPOSITES
Enact
CIG Capital Insurance Group
iCapital NETWORK
LRMG
Couchbase
MPS

Channel & MSSP Partnerships

brigantia
ICM CYBER
GUIDEPOINT SECURITY
CyberSecOp

涵蓋從 500 到 500,000 個端點的客戶都選擇 FortiDLP

為何選擇 FortiDLP

FortiDLP 在風險洞察和終端數據外洩預防之間實現了最佳平衡

完整的可視化

收集雲端、系統、用戶、資料和網路等各個層面的數據，以及組織、事件的來源背景

快速實現價值

即時啟用的終端與雲端感測器，無需設定政策，就能對端點和雲端活動進行監控，從第一天起就能獲得保護

跨平台保護

從數據進入 (Ingress) 到流出 (Egress)，對受管理與非受管理的設備上提供動態的數據資料保護

加速事件調查

AI 智能強化內部的威脅活動偵測，透過更高效率的工作流程縮短處理威脅的時間 FortiAI（人工智能助理）提升了安全運營的水平


FORTINET