IMPERVA

Imperva CounterBreach
資料庫AI智能防護

DATASHEET

保護企業資料，免於內部威脅

對企業而言，最大的資安威脅其實是內部人員。出於工作需求，員工、外包廠商、顧問和供應商必須具備存取企業資料庫和共享檔案內機敏資料的權限。

然而，當內部人員濫用這些存取權限，或是內部人員被外部駭客利用時，就可能造成企業資料外洩。要能準確辨別並遏制內部威脅，需要對使用者行為深入分析，包括使用者存取的資料和存取的方式。

Imperva CounterBreach

Imperva CounterBreach 能保護儲存在資料庫和共享檔案中的企業資料，避免被惡意、粗心大意和帳號被盜用的使用者竊取或濫用。透過動態學習使用者正常存取資料的模式，CounterBreach 能偵測不當或濫用的存取活動，並主動向 IT 團隊進行危險行為告警。

員工需要存取資訊資產才能執行工作，但惡意或出於無知而濫用權限的存取是難以發現且具高風險的。

GARTNER, BEST PRACTICES FOR MANAGING ‘INSIDER’ SECURITY THREATS, ANDREW WALLS, 17 JUNE, 2014

資訊安全策略需要從 bottom-up、以設備和網路為核心的策略轉成 top-down 、以資訊為核心的策略，並聚焦在資訊本身。

GARTNER, PREVENTION IS FUTILE IN 2020: PROTECT INFORMATION VIA PERVASIVE MONITORING AND COLLECTIVE INTELLIGENCE, NEIL MACDONALD, 27 JANUARY, 2016

找出不當的使用者存取行為

CounterBreach 能偵測不當的資料存取行為與相關使用者，藉此發現潛在的資料外洩事件。

CounterBreach 資料庫AI智能防護

CounterBreach 透過機器學習及動態群體分析，自動找出異常的資料存取事件。這個過程可建立一般使用者存取資料庫和共享檔案的完整行為模式基準，進而檢測並設定異常活動的告警優先順序。
結合對使用者的專業分析和存取資料的方式，為企業提供找出資料外洩事件所需的資訊和準確性。透過 CounterBreach，資安團隊可以快速辨別惡意和正常的資料存取事件，並能立即依不同的風險行為採取有效的行動。

CounterBreach 主要特點

偵測關鍵資料的誤用

行為分析偵測到的事件將顯示在 CounterBreach 易於操作的儀表板上。CounterBreach 彙整最具風險的使用者、用戶端主機(Client host)和伺服器，以便IT人員能針對最嚴重的資料存取事件進行優先排序，並讓資安人員可以深入了解各個事件並查看相關細節資訊。

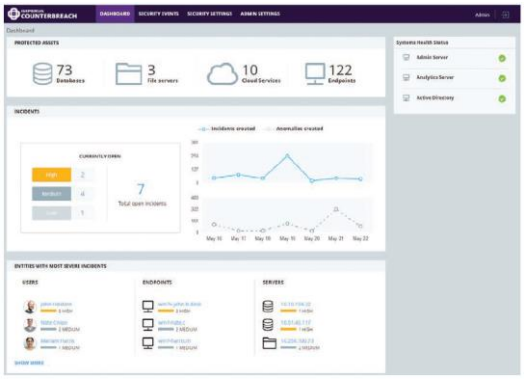
加快事件應變速度

資安團隊可以依嚴重程度、特定使用者、伺服器或用戶端主機作為過濾條件，有效調查不當的資料存取行為，藉此深入了解特定事件，查看相關使用者和被存取資料的細節資訊。而 SOC 人員可以接著關閉被授權或不能立即修復的事件或白名單行為。

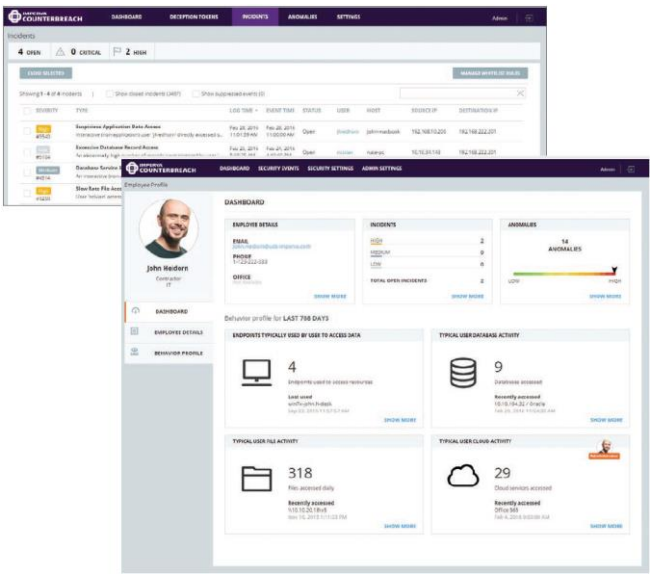
簡化調查流程

資安團隊可以透過使用者儀表板分析特定使用者的資料存取行為，並以同一介面查看事件內容，藉此獲得整個組織內的使用者資料存取全貌。

同時資安團隊也可深入調查特定使用者的相關事件和異常行為，並與該使用者所處群體內的一般使用者行為基準進行對等比較。



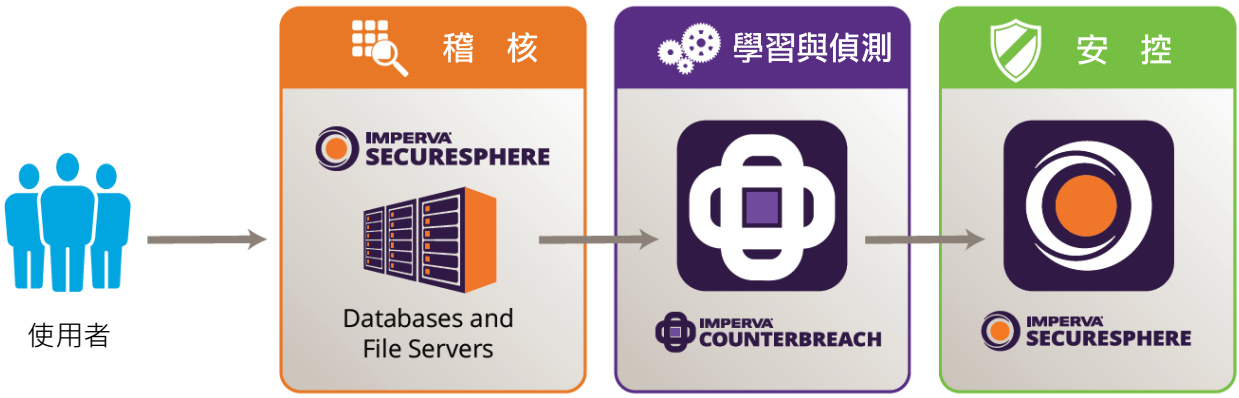
- CounterBreach 儀表板匯集了所有企業資料內的威脅指標



- CounterBreach 事件分析介面將所有異常存取事件依嚴重性排序
- CounterBreach 使用者分析介面提供存取企業資料的使用者一覽表，並標示具風險的使用者行為

用 Imperva 防止資料外洩

要偵測、遏制資料外洩，企業組織需要知道”誰“正在存取企業資料，並了解這些存取行為是否合法，以及在非法行為發生時能立即反應。CounterBreach 結合 Imperva SecureSphere，讓企業能快速找出資料庫與檔案伺服器內機敏資料的重大異常存取行為。



稽核

Imperva 資料保護解決方案能直接控管所有使用者對內部資料的存取。SecureSphere 提供對使用者存取資料庫和檔案伺服器的全觀視野，讓 IT 人員可以掌握曾存取機敏資料的人、事、時、地、物。

學習與偵測

CounterBreach 結合 Imperva 在資料稽核與保護的專業，以先進的機器學習找出不當的使用者資料存取行為。以 SecureSphere 所提供的詳盡資訊為基礎，CounterBreach 建立一般使用者存取的行為模式基準，進而偵測出不同於基準模式的不當行為。CounterBreach 能主動標示這些不當行為，以便相關人員能立即進行調查。

安控

透過 CounterBreach，資安團隊能在潛在資料外洩演變成重大事件之前就進行管控。 一旦偵測到不當的異常行為，企業就能快速隔離具風險的使用者，主動遏制、控管資料外洩情形。

Imperva CounterBreach Cyber Security

Imperva CounterBreach 能保護儲存在資料庫和共享檔案中的企業資料，避免被惡意、粗心大意和帳號被盜用的使用者竊取或遺失。透過動態學習使用者正常存取資料的模式，Counter-Breach 能偵測不當或濫用的存取活動，並主動向 IT 團隊進行危險行為告警。

IMPERVA COUNTERBREACH

系統需求

CounterBreach 必備條件

CounterBreach 需要結合下列 Imperva 稽核與安控產品之一：SecureSphere 資料庫稽核(DAM)、資料庫安控防火牆(DBF)、檔案防火牆(FFW)。

CounterBreach 虛擬版本

CounterBreach易於部署為虛擬設備，且不會影響既有的 SecureSphere 運作。每個硬體主機（host）及 虛擬系統（guest）所需的最小系統要求如下表所示。

	硬體主機(Host)		虛擬系統(Guest)				
	Hypervisor	Processor	CPU	記憶體	儲存空間	作業系統	檔案系統
CounterBreach 管理主機[1]	Dual-core server Intel VTx or AMD-V	VMWare ESX/ESXi 4.x/5.x/6.x	2	4 GB	50 GB		
CounterBreach 分析系統			4	16 GB	1 TB		

[1] 管理主機 (Admin Server) 用於行為分析 (Behavior Analytics)，Imperva 將在上述規格環境下，以軟體方式安裝在預先設定好的虛擬設備上。

支援平台

CounterBreach 資料庫AI智能防護	
Database Platforms	Oracle, Microsoft SQL Server, DB2 for LUW, Sybase ASE
File Systems	CIFS file storage systems, NAS devices
File Operating Systems	Microsoft Windows Server
SIEM Integration	Splunk, ArcSight
Supported Syslog Formats	CEF, LEEF, Raw