dbAegis

資料庫安全稽核系統

Database Activity Monitoring

dataisec 智安數據科技　合作夥伴：dacutek達友科技

機敏文件外洩事件頻傳
您手上的資料安全嗎？

網路科技的快速發展與便利性，讓人們開始將重要的資料上傳至電腦、網路中，企業的機密資料、一般民眾的個人資訊，變成了有心人士不法牟利的籌碼，根據 IBM 發布的《2022 年企業資料外洩成本報告》顯示，受訪企業說明，單起資料外洩事件讓企業的平均成本增加 435 萬美元。

購買資安產品的最終目的
是為了保護資料庫的機敏資料

市面上充斥著各式各樣、眼花繚亂的資安產品，如 DDoS 防護，防火牆、EDR、入侵偵測防護、資安事件分析系統等。企業購買了各種產品來保護重要資料，但卻治標不治本，因為駭客手法推陳出新、讓人防不勝防。我們應該從問題的根本問起，最重要的資料庫，您保護了嗎？

各國制定法規，逐漸重視資料庫安全

自從美國恩隆案事件發生之後，為了確保資料庫不可因政府調查而竄改、刪除任何紀錄，簽署了沙賓法案 (Sarbanes Oxley Act，SOX)，臺灣政府開始立法保障各家企業，要求企業遵守相關的資安措施，如 ISO 27001、資通安全管理法等。

這些法規會需要業者「自行證明無故意或過失洩漏資料」，所以資料的「使用紀錄、軌跡資料及證據保存」極為重要。dataisec 的 dbAegis 具有完整的資料庫軌跡稽核功能，可獨立稽核，將權責分離，即是 驗明正身的最佳工具。

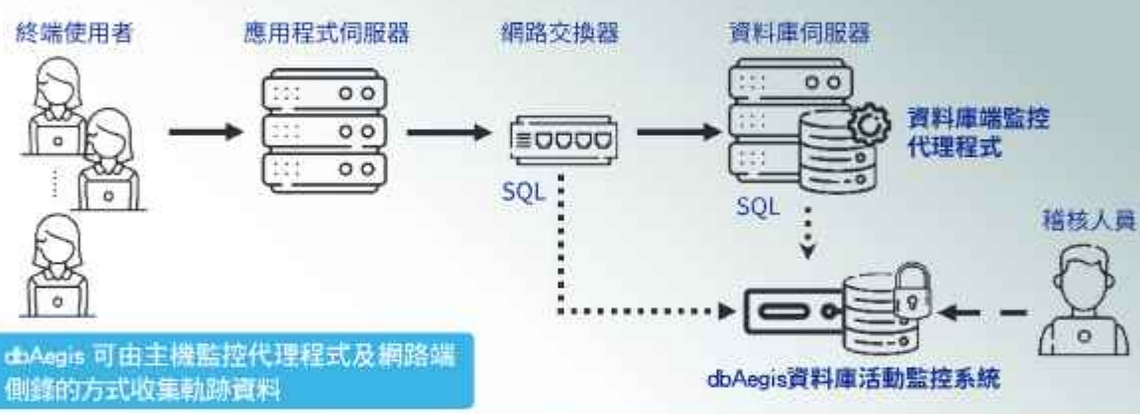
dbAegis 資料庫活動即時監控

dbAegis 是一套由 dataisec 自主研發的資料庫活動監控系統 (Database Activity Monitoring，DAM)，又稱資料庫安全稽核系統，可記錄並稽核所有造訪資料庫的存取軌跡，達到人、事、時、地、物五個面向的追蹤。

人 事 時 地 物

資料庫活動即時監控

dbAegis 可即時並持續監控分析多台異質資料庫活動。針對違反政策的資料庫活動可進行即時警示，並記錄所有軌跡供事後分析。可安裝於獨立硬體設備或虛擬機 (VM)，並支援高可用性(HA)架構，彈性易擴充



不影響資料庫主機的效能，是資料庫稽核產品的首要考量

由於 dbAegis 是安裝於資料庫外的獨立設備或虛擬機中，執行側錄、封包解析功能時，不會影響資料庫主機的效能，即無須設定代理程式 (Agent) 耗用資料庫主機性能的上限，完全避免停用代理程式監控的資安風險。

dbAegis 在操作介面、查詢方式及效能影響等處，比起其他產品，都能更符合市場需求與趨勢。除了具有友善的拖曳式使用者介面外，在設定告警項目時，可以多層次、自定義的方式建立異常事件。另外，在回傳的資訊中，除了輸出即時軌跡紀錄，一目瞭然的 SQL 性能也提供使用者優化調校的指標。誠摯邀請您讓 dbAgeis 保護您手中成千上萬的機敏資料。

支援的作業系統與資料庫

支援 UNIX、LINUX 及 Windows 等作業系統，並可同時監控多種資料庫產品及版本如 Oracle、MS SQL、Informix、DB2、SAP HANA、Sybase、MySQL、MariaDB、PostgreSQL 及 MongoDB 等。

dbAegis 8大特色

1
高度友善的操作介面
僅需用 Web UI 操作，讓非技術背景使用者也可輕鬆駕馭。

2
多層級簽核流程
無限層級簽核功能，完善異常通報流程。

3
直覺的告警設定
輕鬆設定的政策引擎與告警條件，並發送即時通知。

4
隨開即用的法規套件
支援相關法規資訊，協助企業遵守最新政策規範。

5
高效率的查詢系統
站在使用者的角色出發優化，滿足各種客製化的查詢需求。

6
圖形化報表分析
支援各種法規報表（如圓餅圖、長條圖等），提高易讀性。

7
不影響主機效能
不安裝在資料庫上，不影響效能，無須設定效能上限。

8
結合資安監控中心 (SOC)
以CEF格式輸出異常事件及軌跡紀錄，供SIEM/SOC檢視、管理資安事件

加購模組

01 應用程式使用者追蹤模組（APU）

不修改客戶的應用程式，透過 dataisec 獨家技術，不僅能精準取得應用程式使用者對資料庫的存取行為。同時解決動態使用者 IP 的問題。

02 資料庫帳號盤點模組（DAI）

盤點能夠存取資料庫的帳號，利用特定 SQL 語句來查詢並抓取資料庫帳號與資料庫帳號相應的資料存取權限，擷取的資料將回傳給後端接收程式，輸出相應報表，並可結合 dbAegis 判斷幽靈帳號，適時清理帳號以確保資料庫系統安全。

dbAegis 產品家族

產品名稱	功能說明
資料庫本機 SQL 代理程式 (SecuAgent)	監控側錄資料庫本機端的 SQL 存取行為軌跡。
紀錄收集解析器 (SecuEyes)	以 non-inline 建置方式，避免影響資料庫效能，將透過網路存取資料庫的 SQL 封包與通訊協定等資料庫存取行為解析成可讀資訊，並將解析紀錄傳輸至安全稽核控管中心 (SecuCenter) 產出稽核報表。
紀錄鑑識設備 (Log Forensic Server)	提供即時調閱歷史資料做為稽核鑑識使用，並可針對歷史紀錄代入新的稽核政策，讓漏網之魚的歷史事件無所遁形，可將安全稽核控管設備 (SecuCenter) 上的稽核紀錄自動傳送至紀錄鑑識設備，並可搭配外接儲存設備長期保存軌跡資料並提供歷史軌跡資料查詢。

一般問題：info@dataisec.com　銷售問題：sales@dataisec.com　技術支援：support@dataisec.com

dbAegis www.dataisec.com | 智安數據科技股份有限公司
106 台北市大安區光復南路 116 巷 7 號 3 樓（華視大樓）
電話：02-5771-3878　傳真：02-5771-3790