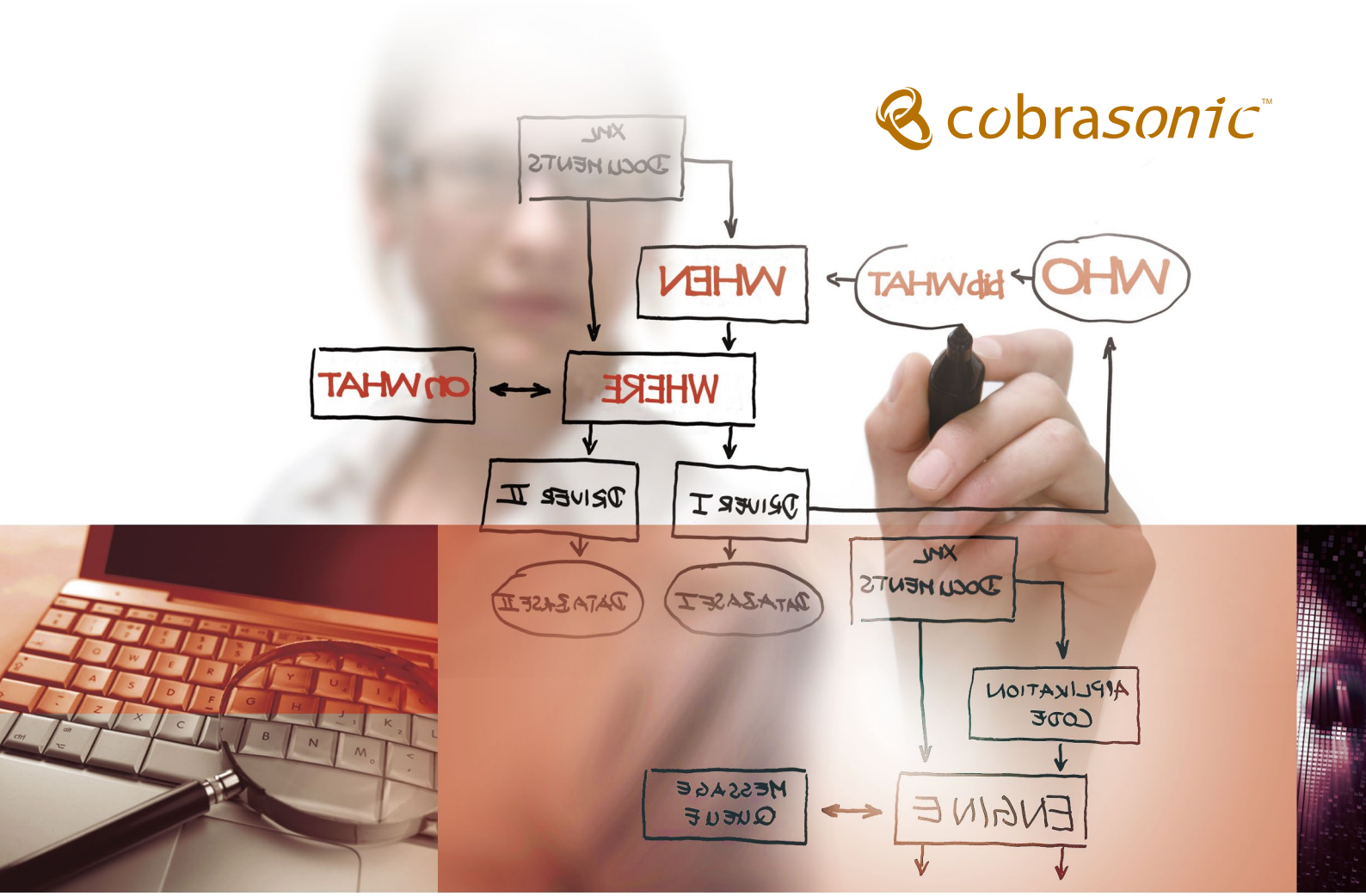
cobrasonic™



dbAegis

資料庫活動監控系統

Database Activity Monitoring System

dbAegis 資料庫活動監控系統

根據2010年Verizon Business資料外洩調查報告，92%資料外洩來自於資料庫系統。IDC的分析指出，數位資料每年以兩倍的速度持續成長，敏感資料也隨著資料的成長而增加。庫柏dbAegis是一套獨立運作的資料庫活動監控系統(Database Activity Monitoring，DAM)，可記錄並稽核所有造訪資料庫的存取軌跡，並可在不修改應用程式的前提下追蹤終端使用者的真實身分，達到人、事、時、地、物五個面向的追蹤。dbAegis是企業預防資料庫個資外洩與遵循法規的最佳選擇。

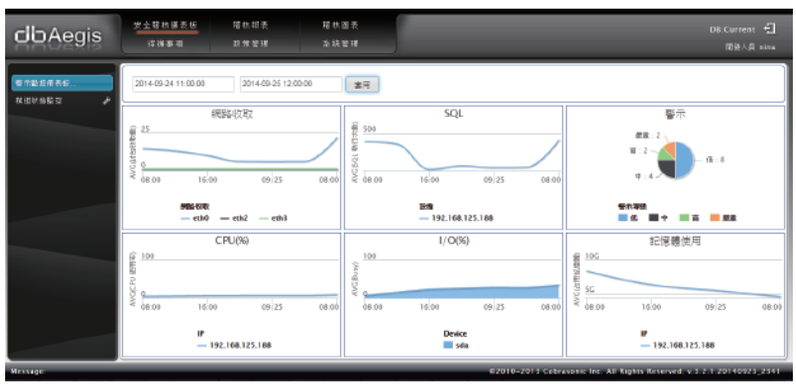


圖1.dbAegis圖形化分析協助稽核人員全面了解資料庫活動

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或阻擋，並可記錄所有軌跡供事後查詢分析。

辨識終端使用者與責任追究

在目前市面上的DAM產品十之八九有一個難以突破的瓶頸，就是無法辨識終端使用者。一般DAM產品記錄的是應用伺服器對資料庫伺服器的SQL指令，及其資料庫使用者，然而現今的應用系統架構，N-Tier的終端使用者大多使用共用資料庫連線或共同帳號與資料庫伺服器溝通，換言之無法辨識SQL指令所對應到的真正終端使用者。要解決這項瓶頸，大多數的DAM產品都必須修改應用程式才能解決，但對現今的企業來說，修改應用程式不僅工程浩大且有其風險，企業多半不會採行。

dbAegis採取獨家專利技術，無論應用系統架構是集中式、主從式、或N-Tier，無需改變任何既有環境，包含不修改應用程式、不加裝軟體於應用系統與終端使用者環境，即可辨識終端應用系統使用者的真實身分及其存取資料庫的行為。dbAegis記錄終端使用者與應用伺服器的HTTP/HTTPS存取軌跡，利用特別的演算法，比對應用伺服器與資料庫伺服器的存取軌跡，找出每個SQL活動是哪個終端使用者所為，達到追究責任的目的。

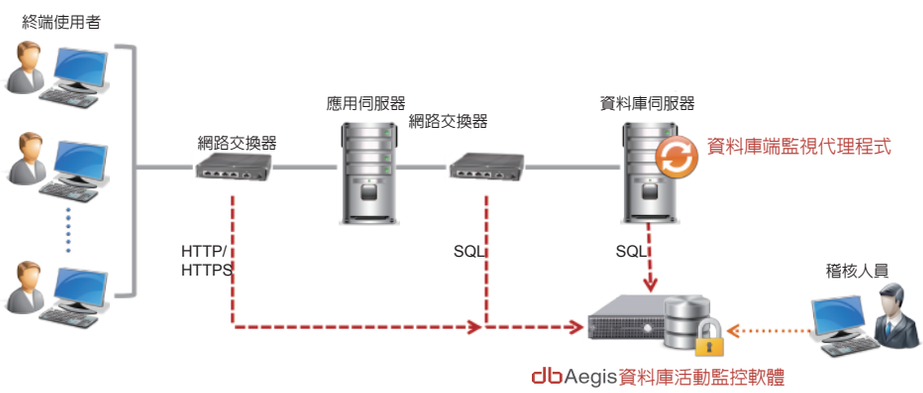


圖2.dbAegis可由主機端監控代理程式及網路端側錄的方式收集軌跡資料

dbAegis

產品特色

- 彈性可擴充架構，安裝容易。
- 即時監控，即時事件警示。
- 獨立稽核，權責分離。
- 真實使用者追蹤。
- 完整軌跡紀錄，用於事後追蹤。
- 實施數位簽章，確保稽核資料的不可否認性。
- 支援各類法規報表 。
- 操作簡單易懂。
- 多重訊息管道，可結合安控管理中心(SOC)。
- 圖形化報表分析。

支援作業系統與資料庫

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Informix、Oracle、DB2、Sybase、MS SQL、MySQL、MariaDB及PostgreSQL等。

軌跡監控模式

無論是網路端或者本機端的資料庫存取皆可透過dbAegis監控存取軌跡。提供以下兩種監控模式：

- 網路監聽模式(Sniffer Mode)側錄網路存取資料庫行為。
- 代理程式(Agent)記錄收集資料庫本機端之存取行為。

系統管理

- 提供網頁式(WEB-Based GUI)管理介面，支援語言包括繁體中文、簡體中文及英文。
- 提供管理帳號密碼安全強度設定。
- 提供系統使用軌跡紀錄。
- 提供異常事件線上稽核簽核流程，可彈性自訂簽核層級及待辦事項。
- 支援帳號角色分權管理，能依人員權責劃分，提供不同權限。
- 提供報表敏感資料遮罩功能。
- 提供多重訊息傳送管道，事件通知可透過簡訊(SMS)、Email、SNMP、Syslog或客製化程式傳送。
- 結合LDAP認證系統。

軌跡紀錄與報表

- 完整記錄使用者所有資料庫活動與產生報表，如DML、DDL、DCL等，可完整記錄資料庫SQL述句。
- 支援資料庫登入失敗活動等異常行為紀錄。
- 支援 5 W(人、事、時、地、物)軌跡紀錄，包含Web使用者、資料庫使用者，時間(Web登入時間、資料庫登入時間、SQL執行時間、SQL完成時間)，SQL述句，參數值，回傳值，回傳筆數，錯誤碼，來源與目的(IP/Port)、終端機資訊等。
- 可過濾敏感表格之存取活動，且可限定記錄特定表格的SQL回傳值與筆數限制，並可以中、英文字串搜尋回傳值內容。
- 支援HTTP/HTTPS通訊協定，具備Web行為網路側錄解析功能，可記錄存取網頁、網頁傳送方式、Web參數值、Web使用者名稱、執行時間。
- 稽核報表提供統計功能。

異常告警與通報機制

- 可依需求針對5W(人、事、時、地、物)設定異常事件、建立警示報表並發出告警通知。
- 提供E-Mail 及SMS(簡訊)兩種異常告警機制，並支援SNMP及Syslog。
- 提供黑白名單群組設定，可針對資料庫使用者、Web使用者、資料庫客戶端IP、Web客戶端IP設定黑、白名單方便稽核政策定義。
- 支援下列警示通報，包含登入失敗、非上班時段存取資料庫、危險指令、高危險群(黑名單)使用者及撈取大量資料通報。

備份與還原

- 支援備份加密。
- 具備資料加密壓縮功能，可藉由FTP及SFTP方式，採用電子簽章演算法將資料備份至外部儲存設備，並可指定日期或日期區間，還原備份資料至系統。
- 提供自動與手動還原指定日期方式還原歷史備份檔案作為歷史軌跡紀錄查詢之用。

法規政策制定

包含ISO27001、新巴賽爾協定(Basel II)、個人資料保護法、沙賓法案(SOX)、醫療業的聯邦健康保險法案(HIPPA)、金融業的金融服務現代法(GLBA)、支付卡產業資料安全標準(PCI-DSS)等。

稽核統計圖表與安全稽核儀表板(Dashboard)

- 提供趨勢圖、長條圖及圓餅圖等圖形化報表分析功能。
- 提供安全儀表板功能、以圖形化表示整體稽核收錄與資安狀況，包含網路收取封包量、收錄SQL數量、警示事件統計、稽核主機CPU、I/O、記憶體等使用情形。
- 可以圖形化顯示稽核紀錄，以挖掘資安異常事件發生的詳細資訊，透過縮小範圍查詢，逐步drill down到觸發異常事件發生的該筆紀錄資訊。
- 可以顯示Top N統計圖形，可選擇針對應用系統、資料庫類型、DB伺服器IP、DB伺服器連接埠、DB客戶端IP、DB客戶端連接埠、DB伺服器、資料庫、DB使用者、OS使用者、SQL執行程式、SQL分類、資料影響筆數、SQL歷時等顯示統計圖形，並以可設定統計圖的資料起始、結束時間區間。

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。
資料庫異動稽核軟體 (CDA Agent)	可支援紀錄被竄改，滅失等異動資料稽核功能(Update Before & After)，當資料庫資料被異動時，可記錄異動前與異動後的資料並呈現於報表中。
程序軌跡記錄軟體 (Process Agent)	安裝於被監控伺服器上，擷取程序相關資訊傳送至SecuCenter，可記錄資料庫主機本機作業系統層級的使用者行為,及應用程式存取資料庫的軌跡。
紀錄收集解析器軟體 (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/HTTP/HTTPS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。
安全稽核控管軟體 (SecuCenter)	將SecuEyes與各式Agent所傳送的稽核軌跡資料經過規則判定並發出警示與提供報表分析，安全稽核控管設備收錄來自Web/AP/DB存取軌跡紀錄，除了可以自動辨識前端登錄使用者功能外，也可以串聯使用者後端資料庫存取紀錄。
紀錄鑑識軟體 (Log Forensic Server)	提供即時調閱歷史資料做為稽核鑑識使用，並可針對歷史紀錄給予新的稽核政策，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。

dbAegis

www.cobrasonic.com

台北總公司

庫柏資訊軟體股份有限公司

10694 台北市大安區忠孝東路四段322號3樓之1

電話：+886-2-8771-3878

傳真：+886-2-8771-3790

北京

庫柏軟件有限公司北京分公司

北京市朝陽區建國路93號（萬達廣場）

4號樓3201室 郵編100022

電話：+86-10-5820-5668

傳真：+86-10-5820-5662

南京

庫柏軟件有限公司南京分公司

南京市長江路109號（長江路九號大廈）

A3幢819室 郵編210005

電話：+86-25-8451-0602

傳真：+86-25-6867-0458

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