LOG MASTER

日誌
管理平台

Billows
竣盟科技

公司介紹

6年前我們團隊因應國際資訊安全與個資法的稽核管理需求，開始提供資安的解決方案和服務。

我們代理與自行開發的產品可依據客戶的需求，建立貼近國內環境的資安稽核監控平台，並滿足國內企業及金融機構的資安法規自動化稽核需求，更利用分析結果啟動資安聯合防禦機制，讓客戶的資訊環境更加安全。

透過產品功能持續不斷的增加，讓工作變得更加智能，並可以輕鬆地將注意力集中在真正的問題上，更希望提供不同的加值服務，讓我們成為企業在資安稽核上最佳的加值夥伴。

LOG MASTER 產品特色

資料收集

1. 設定簡單
2. 資料狀態及系統效能監控
3. 相容其它 SIEM 資料接收程式

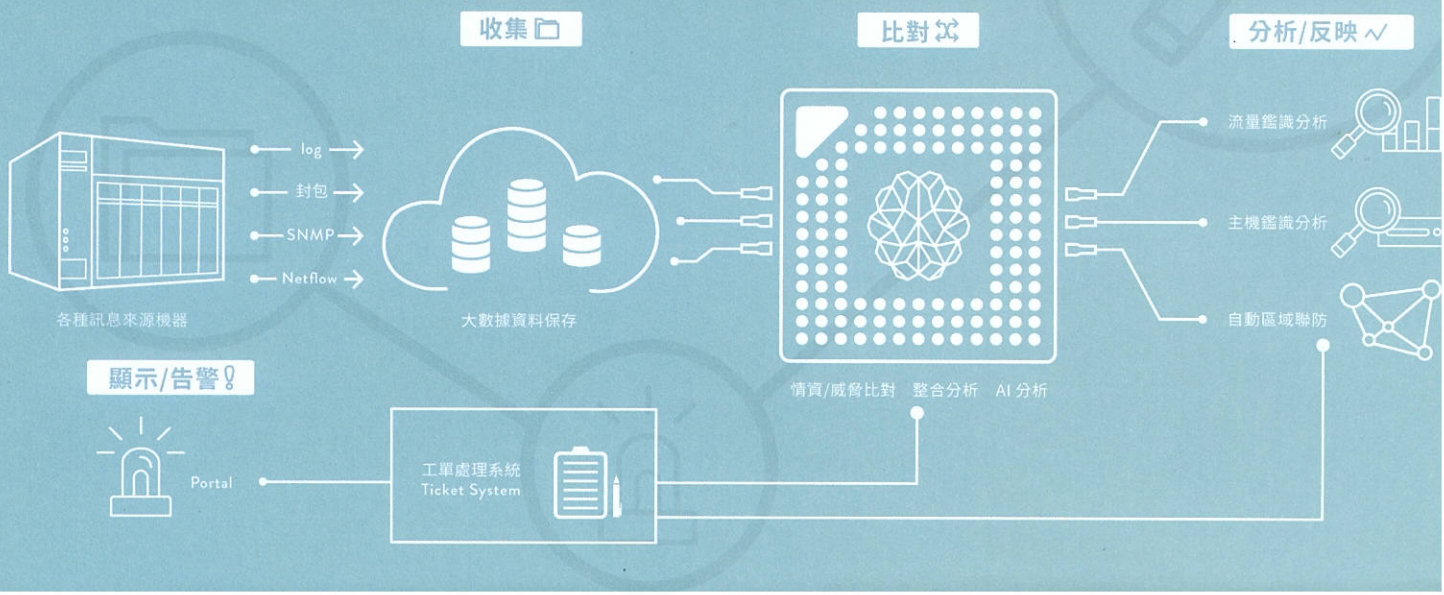
資料保存

1. 正規化/非正規化保存
2. 不可否認性驗證
3. 原始日誌資料保存無上限
4. 資料備援機制

資料加值

1. 情資系統比對
2. 關鍵字告警
3. 稽核報表
4. 動態儀表板
5. AI 行為模式分析

竣盟科技自動化資安稽核解決方案



LOG MASTER 主要功能介紹

設備管理及監控

1. 設備新增
2. 監控設備日誌最後發送時間，若設備停收日誌會發送告警

搜尋

1. 索引-正規化資料庫
2. 原始日誌
3. 日誌下載

智能管理

1. 黑名單 IP 情資管理
2. 資安告警
3. AI 行為模式分析

稽核報表

根據人、事、時、地、物進行資料統計分析

檔案稽核

1. 檔案新增/修改/刪除
2. Storage 特定檔案使 用狀態
3. 使用者存取 Storage 檔案

帳號稽核

1. 使用者帳號新增/刪除/鎖定
2. 使用者密碼變更
3. 使用者群組變更

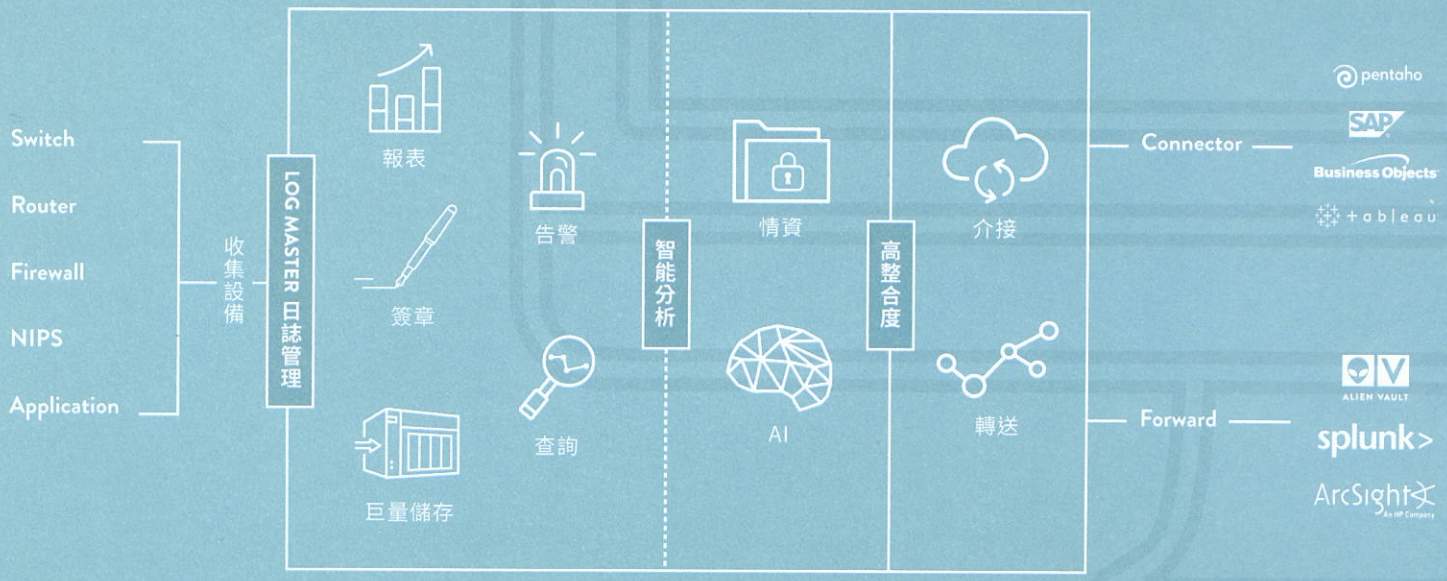
登入行為稽核

1. 管理者登入成功/失敗
2. 使用者登入成功/失敗

資安警示報表

1. 黑名單管理
2. 資安告警
3. 防火牆 Policy 異動

產品架構



Billows
竣盟科技

台北市中山區新生北路二段29之1號12樓

Tel 02-25623952 **Fax** 02-25363763

Line @vri4754n **Mail** gavin@billows.com.tw

www.billows.com.tw