FORCEPOINT
POWERED BY Raytheon

Datasheet

Forcepoint CASB
網頁雲端服務稽核與防護

網頁應用程式是您企業的門面，請以這樣的方式保護它。

以 FORCEPOINT CASB 保護網頁應用程式

許多組織都有 Apps 用來與他們客戶、合作夥伴及供應商互動，如果組織想保護其企業商譽與盈利的話，確保這些 Apps 的安全是優先要務。

然而，網路犯罪者帶來了巨大風險，因為他們已經非常擅於利用魚叉式網路釣魚或於電話中謊冒等社交工程手法來獲取合法的系統登入帳號密碼。如果他們得到帳號密碼，他們可輕鬆接管使用者的帳戶並提升權限為特權用戶，竊取企業機敏資料並使整個 IT 基礎架構陷入停頓狀態。

當你考慮到法規遵循需求時，事情變得更加複雜，特別是組織需要提供客戶的詳細稽核軌跡，包括登入、更新、下載等。如果組織沒辦法提供這些稽核軌跡，他們的客戶與合作夥伴將無法滿足他們自己的公司管理或法規遵循義務。

監控並防止遭竊帳號密碼的誤用

Forcepoint CASB 使您能夠監控和保護在企業資料中心或 Amazon Web Services (AWS) 和 Microsoft Azure 等公有雲運算環境中，對客戶開放的線上應用程式。Forcepoint CASB 使用完全透通的部署模式來執行活動監控，不影響使用者體驗也不需要對線上應用程式做任何改變。

特色與效益

- 保護防止帳戶被盜用以及被竊帳號密碼的誤用
- 監控並即時偵測異常行為（例如，暴力破解攻擊）
- 阻擋或強制執行以風險衡量的多因素身份驗證以提升安全
- 即時收到可疑活動的警報
- 對所有用戶活動留下日誌以滿足法遵需求

Forcepoint CASB 利用動態用戶和設備指紋識別技術，來自動分析及偵測可能顯示為帳戶被盜用的異常行為，Forcepoint CASB 學習合法用戶行為的正常模式，包括一個人的慣用端點設備和存取位置，並持續監控可疑行為。例如，在 AWS 環境中，如果駭客或惡意內部人員試圖終止伺服器執行個體 (instance) 或刪除資料庫，Forcepoint CASB 可以發出警報、阻止操作或即時要求雙因素身份驗證，使其“證明”他們是他們所聲稱的人。

Forcepoint CASB 提供了多種預設的政策，可以立即偵測和修復與帳戶有關的威脅。

行為細節的偵測	說明
可疑的系統登入次數	x 天內成功登錄的次數超過預定值
竊取 Session ID (Session Hijacking)	在兩個以上不同的用戶設備上偵測到相同的對談 (Session)
從不尋常位置的異常資料使用	由非慣用位置存取非慣用資料所造成的指紋比對不合
不尋常的地理位置	當用戶不在該位置時，由異常地理位置的活動引起的指紋比對不合
可疑的端點	由非習慣所在地理位置使用非慣用端點所引起的指紋比對不合
不尋常的系統存取時間	在不尋常時間的活動引起的指紋比對不合
從不尋常端點裝置的異常資料使用	由非慣用端點存取非慣用資料所引起的指紋不匹配
同時間存取系統	在短時間內由兩個不同位置同時登入系統
從不尋常位置與端點的異常資料使用	由非慣用位置及非慣用端點存取非慣用資料所引起的指紋比對不合

Forcepoint CASB 還可以在您的線上應用程式必須滿足特定的安全與合規性要求時，創建自訂政策。有了自訂政策，您可以選擇您所想要的「誰、什麼、從哪裡、何時及如何」的政策。此外，您可以在政策被觸發時選擇適當的回應。例如，您可以選擇顯示警告或率先阻擋觸發警報的異常行為，直接凍結帳戶或應用雙因素身份驗證來驗證該名人員身份。

保留詳細的稽核軌跡以避免制裁和罰款

追蹤所有用戶活動以滿足合規性要求與保護應用程式本身一樣重要。目前許多行業正在實施 HIPAA、PCI DSS 及其他法規，Forcepoint CASB 即時追蹤組織線上應用程式的用戶和系統管理者活動，確保您保留完整的稽核軌跡，以滿足最嚴格的合規性要求。

下表列出了部分需要詳細記錄用戶活動的法規，包括敏感資料的存取和修改紀錄：

法規	法條	細節
HIPAA (健康保險便利和責任法案)	**164.312(b)**	稽核控制——對含有或使用電子健康資訊的硬體、軟體、記錄與檢查資訊系統活動的程序機制，實施稽核控制
ISO 27002	**9.4.2 (f)**	記錄失敗與成功的系統登入嘗試
PCI DSS (支付卡產業資料安全標準)	**10.7**	保留至少一年的稽核軌跡歷史紀錄；必須立即提供至少三個月的歷史紀錄以進行分析
NIST (美國國家標準技術研究院)	**AU-2(1)(1)**	資訊系統必須能夠依據風險評估、任務或業務需求進行稽核（例如，帳戶登入事件、帳戶管理事件、登入事件、存取物件、政策變更、特權使用、流程追蹤以及系統事件）
FFIEC(美國聯邦金融機構考試委員會)	**Information Security - Appendix A (M)(5)**	確定安全相關事件的日誌是否足以支援資安事件偵測和應變活動，並且應用程式、主機和網路活動的日誌可以隨時關聯。

Forcepoint CASB 可產生一致的正規化存取日誌，使您可以輕鬆滿足內部和外部稽核人員的要求。它同時能統合檢視你所有應用程式，簡化並加速稽核流程。如果您希望將追踪警報和稽核活動納入網路營運中心程序中，Forcepoint CASB 已與領先的 SIEM 解決方案做好整合。最後，Forcepoint CASB 提供了以下預設稽核功能，無需進行客製開發工作。

網頁雲端應用服務防護	
特色	**描述**
活動監控與分析	可依照使用者、群組、位置、設備、應用程式操作、資料物件、時間與部門別進行即時活動監控與分析。
特權使用者監控	即時監控與回報特權使用者與系統管理者，包括資料存取、組態變更、使用者權限修改等。
自動異常偵測	動態用戶和設備指紋識別技術持續監控行為並自動偵測異常行為，包括高風險內部使用者與外部攻擊。
即時威脅防禦	透過設定政策來監控、阻止、允許或要求對應用程式或應用程式內的特定操作進行身份驗證，以阻擋帳戶相關的威脅。
多因素身份驗證	內建多因素身分驗證功能，可以根據端點類型或位置觸發，也可以做為違反政策的回應行動。
動態警示	透過簡訊或電子郵件接收任何違反政策或超過活動設定閥值的即時通知
自訂政策	視覺化政策編輯器可根據用戶、端點、位置、資料物件、操作、時間等的任意組合輕鬆配置精細政策。
網頁雲端應用服務稽核	
特色	**描述**
詳細的活動日誌	獲取資料中心和供客戶使用的應用程式的用戶活動日誌
集中的稽核位置	單一、統一檢視所有應用程式以簡化稽核
企業 SIEM 整合	透過 Adaptors 直接將活動日誌匯入領先的 SIEM 方案如 ArcSight、Splunk 以及 Q1 Labs
企業報表	靈活的報表選項，包括能夠編輯和保存自訂報表的預定報表

與我們聯絡

886-2-8758-2970

fkuo@forcepoint.com

www.forcepoint.com/contact

關於 FORCEPOINT

[DATASHEET_FORCEPOINT_CASB_WEB_AUDIT_PROTECTION_EN]-100057.022217