cobrasonic™

OSAegis

特權存取管理暨防駭解決方案

Privileged Access Management and
Anti-Hacking Solution

osAegis 特權存取管理暨防駭解決方案

根據知名資安研究機構Verizon的2012資訊安全研究報告指出，企業資訊安全遭遇內外部破壞的事件中，伺服器遭受破壞的比例高達50%，而這些遭受惡意破壞的伺服器更造成了98%的資料外洩筆數。造成資料外洩最高比率是外部間諜與駭客，其次是公司內賊。

由於傳統的防火牆(Firewall)及存取控制(ACL, Access Control List)已不足以防護企業伺服器遭受攻擊，Verizon建議，必須強化伺服器作業系統的必要控制(Essential Controls)及事件監控(Monitor Event Logs)才能有效防護來自內外部的惡意破壞與資料外洩。

osAegis是新世代特權存取管理暨防駭解決方案，其防護範圍涵蓋了存取角色與存取對象之權限管理、網路連線、帳號安全與軌跡管理。osAegis可在不影響作業系統效能下，24小時不間斷地進行稽核、監控與保護。不同於傳統產品只能防禦已知的入侵模式，它可以防禦內部與外部、已知與未知的威脅。osAegis是抵擋駭客入侵、防止資料外洩、與符合稽核法規的最佳利器。

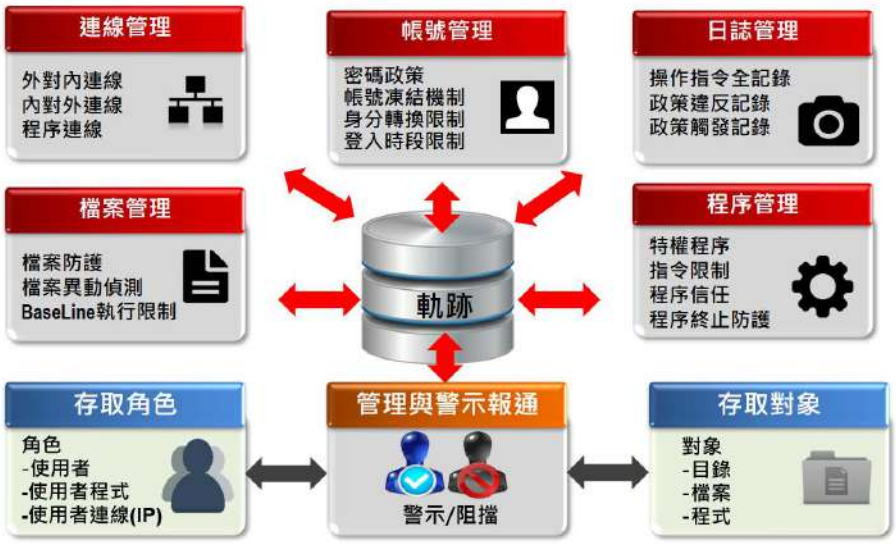

圖1.osAegis功能機制

特權存取管理

特權使用者最令人詬病的就是可以讀取任何敏感資料，可以刪除任何罪證軌跡，企業安裝的視窗錄影監控程式，特權使用者甚至可以輕易的終止躲避稽核。以個資法的角度來看，特權使用者問題在於無法被有效稽核，軌跡資料因可被竄改而無法成為有效證據。特權使用者因為集所有功能於一身，間接地造成共用帳號的問題與稽核的困難。

使用osAegis可達成共用帳號權責分離之效果，並可有效限制特權使用者可執行的指令、檔案存取與保護錄影稽核程式不被終止，甚至特權使用者所有系統操作行為都會被全紀錄。osAegis並可更進一步的將檔案限制成任何人包含特權使用者都無法存取，而只允許程式來存取。畢竟在企業內部會舞弊的是擁有特權的人，而不是程式。

遏止駭客攻擊

駭客入侵系統方法千變萬化，但多以攻擊網站與竊取資料為主。常見攻擊網站的手法，以篡改網頁、修改網站設定檔導引至有害網頁、網頁植入惡意程式碼與植入新後門網頁等手法為主。osAegis透過「檔案權限管理」適當的設定，即使駭客擁有root權限也莫可奈何。

駭客侵入系統竊取資料的步驟可歸納為：植入後門程式方便下次進出、植入背景程式外傳敏感資料、竄改查詢工具避免後門程式曝光、竊取資料備份檔與刪除軌跡躲避偷竊曝光等手法。osAegis除了以「檔案權限管理」做防護外，更可透過「Baseline執行限制」設定禁止執行後門程式，以「連線管理」設定來禁止資料外傳或禁止後門進出。透過osAegis神盾級的保護，有效遏止駭客攻擊與竊取資料。

osAegis主要功能		說明
行程管理	特權行程	透過該設定，可讓行程享有特權不受osAegis的限制。 例如，osAegis將備份檔案設定成任何人都無法讀取，但行程仍然可以新增或刪除備份檔。畢竟我們在解決的是會舞弊的特權使用者行為，對於不會舞弊的行程是不需要加以限制的。
	指令限制	用於限制指令的可執行對象。 通常可用於shutdown指令，避免伺服器遭惡意停機。為了避免少數使用者偷竊root密碼並su成特權使用者，該功能也可以用來限制執行su指令的對象，避免任何人都可以執行su指令達到切換身分的效果。
	行程信任	可限制行程只能被指定的行程呼叫與執行。
	行程終止防護	可指定行程並加以保護，受保護的行程只能被指定對象終止。 通常用於保護監控行程，確保監控行程不被惡意特權使用者或駭客終止，確保24小時無間斷監控與防護。
檔案管理	檔案防護	用於限制檔案的可使用對象，對象可以是使用者或IP來源。 限制的項目包含讀/寫/執行/刪除等。該功能可用將網頁限制成唯讀，僅允許特定人員經由特定IP連線進行維護，避免駭客盜取特權使用者身分置換網頁或將惡意程式植入網頁，造成瀏覽網頁客戶的危害。
	SETUID限制	可一次限制所有被設定為SETUID的程式的可存取對象。 SETUID的程式具有部分特權使用者功能，當程式有漏洞的時候，使用者可藉由漏洞變身為特權使用者。
	檔案異動偵測	用於偵測檔案內容是否被異動，一旦發現檔案內容被異動時，可立即通知管理者。可利用該功能來偵測設定檔的異動。如果系統服務發生問題時，可用於協助釐清責任歸屬。 也可利用該功能來偵測部份工具程式，例如ps、netstat、login等是否發生變動。因為駭客通常會置換工具程式以避免後門程式被發現，使用該功能可確認是否遭到駭客入侵。
	Baseline 執行限制	設定Baseline執行限制在於限定一個時間點後所有的執行檔將無法執行。當駭客入侵後植入後門程式，後門程式會因為超過Baseline的時間點而無法被執行或啓動。可用於阻止駭客偷藏背景程式或後門。
連線管理	程式連線	可設定程式允許連線的連線IP/Port。
	外對內連線	可阻擋外對內連線，防止駭客由外網及內網入侵該伺服器。
	內對外連線	可阻擋內對外連線，防止後門程式向外傳送資料。
帳號管理	密碼組合限制	可用於制定密碼的複雜程度。
	登入失敗限制	當帳號登入失敗N次時，可限制N分鐘內無法再嘗試登入，避免駭客大量測試密碼。
	帳號凍結機制	N天內無登入紀錄的帳號，將自動判定為離職帳號並且停止帳號使用，避免管理者忘記將帳號移除，造成離職員工藉此途徑竊取敏感資料。
	登入時段限制	可設定帳號使用時段，避免使用者在非執行勤務時間使用系統，減少使用者誤用與濫用的機會。
	身分轉換限制	限制可以轉換的身分，避免使用者可以任意轉換成他人的身分。
軌跡	軌跡	設定監控模式下記錄所有軌跡紀錄，並且提供瀏覽欄位選擇。 更提供軌跡紀錄過濾機制，以排除不需要做軌跡紀錄的行程。

* 靜止還沒啓動的狀態稱Program(程式)，啓動後稱 Process(行程)。

支援作業系統

- RedHat Enterprise Linux
- Windows Server
- HP-UX
- AIX
- CentOS
- Solaris

OSAegis

www.cobrasonic.com

庫柏資訊軟體股份有限公司

專業資安代理商

docutek 達友科技

02-26588970

contact@docutek.com.tw