observe IT
a division of Proofpoint

People-Centric Insider Threat Management

智慧型視覺化內部威脅暨資料外洩防護解決方案

People-Centric means

Understanding Context

Solving Business Challenges

Respecting Privacy

台灣區授權代理 | 漢領國際有限公司

內部威脅連年持續攀升中！

著名的研調機構 PONEMON 於 2020 第一季所發表最新研究調查報告指出，相較於前一年，2019 年全球內部威脅 Insider Threat 事故成長率高達 47%，所造成的資安事故損失成本，每起事故約 1,145 萬美元，上升了 31%，事故的平均處理時間為 77 天。調查中有 60% 的企業每月約發生 2 起資安事故，再分析資安事故損失成本，則以事故調查費用成長率最明顯，成長率高達 86%。調查結果顯示，事故處理時間愈長，所造成的損失愈高，當處理時間拉長到 90 天時，平均損失金額達 1,371 萬美元。

內部威脅意指凡被授權接觸組織內部資料、應用程式與系統之使用者，因蓄意或輕忽的使用行為所導致的資安風險或損失。蓄意行為包含了惡意破壞、間諜行為、竊取智慧財產、詐欺等，而輕忽行為則涵蓋了人為疏失、判斷錯誤、帳號被盜用，或遭釣魚郵件、惡意程式攻擊等。「人」是內部威脅發生的根因，換言之，針對被授權人員與其使用行為加強資安防禦，方為正本清源之策。

2020 持續推出 ObserveIT ITM v7.9 及 v7.10 版強調 Contextual Intelligence、Threat Signals、即時回應、整合、注重隱私等應用能力

全球最佳內部威脅管理解決方案 ObserveIT ITM 自問世以來即聚焦以「人」、「流程」、「技術」為中心的資安防禦策略，已經協助全球 1200 家以上的標竿企業迅速防範使用者行為所導致的資安事件與商業損失。就功能面，ObserveIT ITM 鎖定細膩與精確的 User Activity、Metadata 與 Analytics 作為持續研發藍圖，而應用面，則以內部威脅為核心主軸不斷深化與擴展。

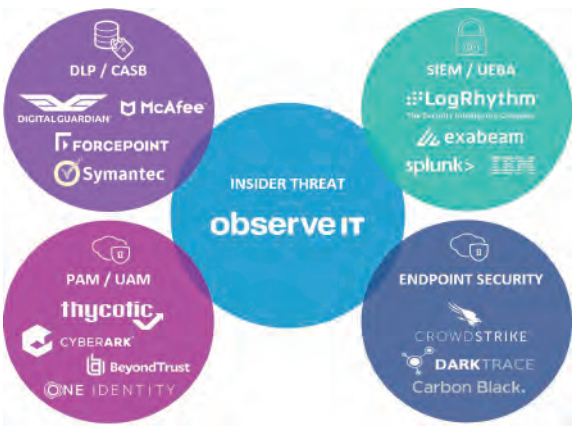
ObserveIT ITM 自 v7.0 版即持續精進其 FAM (File Activity Monitoring) 資料外洩防禦應用範圍，強化檔案日誌歷程追蹤軌跡，主動偵測內部檔案與異常使用行為。2020 推出 v7.9 及 v7.10 版，經由 1200 實證客戶及 NIST、CERT、OSIT 與 NITTF 業界專家累積建立了多達 350 條以上內部威脅專用之告警規則與情境，隨選即用亦可自訂。

ObserveIT ITM 亦強調隱私及去個資識別化，符合國際個資隱私之規範遵循，可自訂管理者瀏覽項目之權限，避免管理或稽核人員獲取權限以外之個資。

快速整合各系統日誌、告警事件與使用者之關聯性

近年來 ObserveIT ITM 被賦予更高層級的資安使命，積極強化「偵測」與「回應」能力，著重於 Contextual Intelligence 與 Threat Signals 主動預警能力的發展，更以提升洞悉使用者行為風險、Know the Whole Story、提前防禦時間軸為指標，提供各類威脅使用行為與資料外洩之關聯性，以利採取最及時的回應。

以往多重來源的系統日誌、常態性大量告警以及無法還原具體行為歷程軌跡等，乃延宕事件調查、辨識與回應速度之主因，ObserveIT ITM Contextual Intelligent 以人為中心的完整軌跡與快速關聯能力，可具體還原告警前後的人事時地物，進而補足其他資安系統資訊與軌跡之不足，並將以往被動的資安防禦於彈指之間立即轉化為主動。



ObserveIT ITM 功能特色與技術優勢

1. Web-Based風險儀表板提供管理者整體內部威脅可視性與關聯性，明確顯示各類使用者、部門單位、觸警風險行為累計/新增之指數與趨勢，並可自訂或套用，以進行風險評級。
2. 提供使用者行為歷程進階統計分析，包括遠端連線來源、常用登入帳號/端點/裝置/應用程式/網站等分析與使用時間、平均活動或超時工作統計等，適合居家異地辦公之應用。
3. FAM (File Activity Monitoring) 提供檔案日誌歷程追蹤軌跡，主動偵測內部檔案異常使用行為如：大量檔案複製、雲端上傳/下載追蹤、Webmail瀏覽、異常列印、檔名變更、檔案刪除等，皆可立即告警與追蹤視覺化軌跡。
4. 偵測 email 郵件寄送主旨、收 / 寄件人及密件副本欄位、附檔檔名、檔案數量與檔案大小等功能，以及提供附檔完整歷程追蹤。
5. 具備URL安全過濾機制，內建逾數十種分類及逾數百億筆 Indexed URLs情資資料庫並可每日更新，針對釣魚、高危險性、未被授權網站等之瀏覽行為進行偵測、告警或中斷。
6. 可設定「匿名模式」，將風險儀表板及 Web Console 所顯示之使用者資訊加以匿名，確保使用者隱私與個資之保護。
7. Windows環境可進行應用程式進階控管，針對未授權或異常應用程式使用行為進行偵測，具備強制關閉未授權之應用程式或強制登出等預防機制。
8. 針對Linux環境可阻絕未經授權指令、指令參數或蛙跳行為，可偵測與側錄Linux/Unix使用者執行之命令與輸入指令後的Output字串，包括Script中內含之指令與系統命令產生的底層指令，及所有終端螢幕之輸出畫面。
9. Key-Logger功能完整記錄Windows/Mac鍵盤輸入及組合鍵，如：PrtScr、Alt-PrtScr、Ctrl-V、Cmd-Shift-3、Cmd-V等，亦可設定偵測告警。
10. 可偵測 USB 儲存設備、SD Card 、iPhone、Android 行動裝置之序號、廠牌名稱、型號名稱、編號等辨識，並建立黑白名單。當偵測到以快捷鍵複製或拖拉檔案至黑名單儲存設備時，將告警並紀錄資料外洩完整過程。
11. 活動歷程回播 (Activity Replay) 可設定告警觸發前後之側錄方式與時間長短，有效降低側錄軌跡資料儲存所需的磁碟空間，且軌跡之工作階段增加了端點當地時間戳記，以利全球化企業組織管理。
12. 側錄資料皆具備AES加密保護與浮水印，並具備雙重密碼保護機制亦可整合數位簽章，並須依管理權限以播放器進行回播，確保資料無法竄改同時提升證據能力。
13. Agent符合FIPS國際標準。具備離線側錄功能，網路斷線時Agent仍持續側錄，待連線恢復自動回傳檔案至資料庫。凡蓄意更改、刪除Agent檔案或終止Agent運作時，Agent Watchdog機制自動重啟並發送即時警示email通知管理者。
14. Agent支援Windows、Mac、Linux、Unix/HP-UX、Solaris等平台，Windows/Linux管理者身份或共用帳號可增設第二道認證並可與AD整合，及Windows身份盜竊偵測與警示功能。
15. 支援 VMwareView / RDSH、Citrix XenApp / XenDesktop、Ericom Connect、Windows Remote Desktop、Team Viewer、PCanywhere、VNC、Telnet、SSH、Netop、Dameware、PuTTY、WinSCP、SFTP遠端連線操作側錄。
16. Metadata / 告警事件提供 Database API、Restful API、CSV / CEF log 供外部 SIEM 進行即時收容及分析。亦提供 Webservice 整合 Ticketing 系統，如 OITicket 工單申請覆核流程系統，以進行工單申請、核准及權限開通與視覺化覆核。

observe IT
a division of Proofpoint

內建29種分類高達350+種告警規則與情境，以利高風險使用行為與內部威脅之偵測與分析

1. 特權人員：擁有IT系統管理權限或服務帳號之使用者。
2. 第三方人員：服務廠商、委外人員、產業供應鏈或上下游夥伴。
3. 專業從業人員：研究調查、系統開發、稽查人員等。
4. 離職員工。

DATA EXFILTRATION

- Exfiltration to USB/ Removable Media
- Exfiltration to Cloud Storage like DropBox
- Exfiltration via Large Print Jobs
- Exfiltration via Webmail Clients
- Exfiltration via Copy/Paste

PRIVILEGE MISUSE

- Modifying / Deleting Rows in a Database
- Accessing Source Code during Irregular Hours
- Connecting by Impersonating Privileged / Disabled User
- Running Unauthorized Software on Server
- Accessing Sensitive Data of Previous Employer

ACCIDENTAL INSIDERS

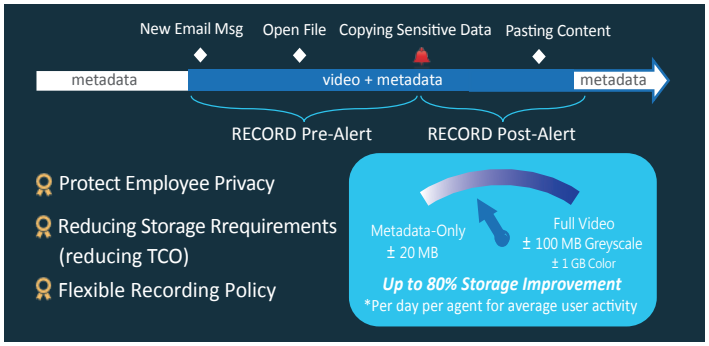
- Storing Passwords in Clear Text
- Downloading from Insecure Websites
- Using Unapproved Removable Media
- Using Unapproved Websites
- Accidental Misconfigu-ration of Cloud Infrastructure

SECURITY CONTROL BYPASS

- Tampering with Security Controls
- Accessing Websites Associated with Criminal Organizations
- Downloading Unapproved Software
- Utilizing VPN or Proxy Tools
- Using Steganography Software

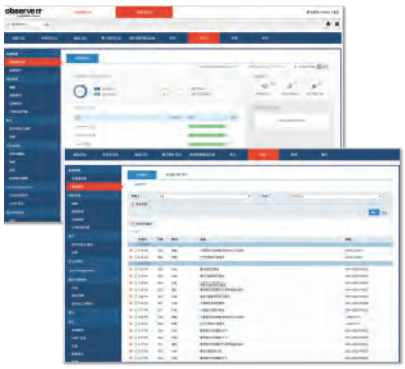
資料外洩之應用 - 偵測、告警、阻絕、側錄，可匯出風險使用行為分析報表

上傳檔案至外部雲端平台及應用程式	雲端空間 – Dropbox、Box、Google Drive、iCloud。 Office365、OWA、Gmail、Webmail 等。
於內部機敏資訊平台上傳/下載檔案	內/外部Portal，如：醫療網、網路銀行、企業SharePoint、Salesforce、CRM 等。
可卸除式儲存裝置使用監控	偵測可卸除式儲存裝置廠牌、型號、序號及標籤。 偵測下載至可卸除式儲存裝置檔案之軌跡與來源。 建立可卸除式儲存裝置黑白名單及告警規則。
Email 資料外洩防禦及監控	寄/收件者郵件地址、主旨、夾檔之可視性。 網域名稱、檔案大小之黑名白單監控政策。 郵件夾檔上傳來源及下載後歷程追蹤。
檔案列印、複製/貼上	非上班時段大量列印、複製/貼上。 未授權檔案列印、複製/貼上、滑鼠右鍵貼上 ...。
Key-Logging告警/偵測/控管	鍵盤特殊功能鍵、組合鍵 - PrtScr, [Alt-PrtScr], [Cmd-Shift-3] , CTRL-V, CMD-V。
複製/貼上機敏文字	複製/貼上疑似信用卡號碼。 複製/貼上機敏檔案內文字。
存取未授權資料夾及檔案	存取未授權資料夾。 存取未授權UNC路徑。
執行惡意/駭客工具	使用惡意工具之即時告警：Nessus、Netsparker、Maltego等。
執行圖像隱碼術工具	使用隱碼術工具之即時告警：xiao_steg、camouflage 等。
於Linux/Unix系統執行檔案傳送指令	偵測Linux傳送指令，如：tftp、scp、rsync、GET。
使用P2P工具	偵測P2P 工具使用。



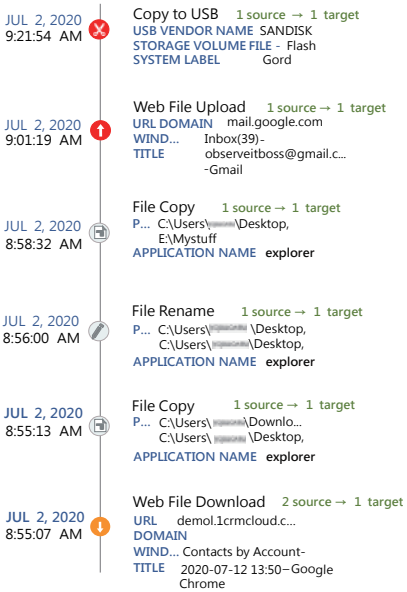
Activity Replay：可設定告警觸發前後之側錄方式與時間長短，如：觸發前後側錄方式為 Metadata + Video，一般時間則只側錄 Metadata; 亦可設定觸發前後側錄的時間長度，有效降低所需之磁碟空間。

Web-Based 管理介面支援中英日韓德等多國語言，具備https加密連線



細膩且完整的檔案活動時間軸，協助管理人員精確掌握檔案存取動態

File Activity Details



榮獲全球逾100國1,200家國際標竿企業客戶青睞 持續獲得國際資安大獎肯定

Insider Threat Solution Gold Award

Insider Threat Detection Best Product

Insider Threat Solution

Black Unicorn Awards

法規遵循與軌跡稽核

- 符合「個人資料保護法」、「金融機構辦理電腦系統資訊安全評估辦法」、「電子支付機構資訊系統標準及安全控管作業基準辦法」 等各項法規之遵循。
- 符合PCI、SOX、HIPAA、NERC、FFIEC、FISMA、FERPA ISO27001等國際法規遵循性，以及SWIFT國際組織CSP規範。
- 視覺化記錄內外部/遠端連線之使用者操作行為，同時提供詳盡的 Log 記錄，符合使用記錄、軌跡資料及證據保存之規範標準。
- 提供完整的AES加密視覺化記錄，提升證據能力及證據價值。

OITicket 工單申請覆核流程系統（額外模組）

提供Web-Based線上核准稽核4A機制，可與 Windows AD 整合以利快速建置上線使用，並以AD內建組織層級自訂核准流程，點選“側錄畫面”欄位可立即回播操作行為之加密視覺化記錄。

Authorization - 特權帳號工單申請核准及權限開通

- 統一內外部申請程序，可依資安政策與權限加以規範工單核准流程。
- 申請人可自訂作業期間、作業時段、伺服器、工作項目，並填寫工作描述，系統自動Email通知主管核准後，特權帳號之工單申請人方可登入伺服器執行核准之作業。
- 可依核准內容限制登入伺服器之作業期間及作業時段。
- 可防制蛙跳至後端其他未授權作業之主機。

Authentication - 工單流程記錄

- 集中保存申請記錄。
- 工單申請人依工單所核准之作業期間/作業時段內進行登入，未經核准之帳號或時段則不得登入。申請人工作完成後可自行回播並確認執行之內容，亦可列印執行結果之畫面。

Auditing - 視覺化線上稽核

- 稽核與相關主管可隨時檢視申請人執行內容畫面，並對工單記錄予以覆核。
- 各層級主管針對「待覆核」之工單，可於檢視歷程或回播後，標示為「勾選為已覆核」，若認為作業內容未完成或不符合申請，主管亦可將工單變更為「失效」。

Alert - 即時警示通知

- 可依執行應用程式、視窗標題、登入帳號、用戶端、時段等規則發送即時Email警示予管理者。

ObserveIT ITM Agent 支援版本

Windows :

- 32/64-bit Windows 8.1/10
- 64-bit Windows Server 2012/2012 R2/2016/2019

Linux :

- RHEL/CentOS 6.7-6.9; 7.0-7.6 x86_64/ppc64, 7.0-7.6 x86_64, 7.2-7.6, 8.0
- Oracle Linux 6.7-6.9, i386/ x86_64,7.0-7.4 x86_64, 8
- Ubuntu 14.04, 16.04, 18.04 (LTS), i386/x86_64
- SLES SUSE 11, SP2-3, 12 i386/x86_64
- Debain 8 & 9 (32/64-bit)
- Amazon Linux 2

Mac OS :

- MacOS High Sierra 10.13
- Mojave 10.14
- Catalina 10.15

IBM :

- AIX 7.1/7.2 (32/64 bit)

HP :

- UX 11.31 (Itanium 64 architecture)

Solaris :

- X86/x64 or Sparc; 10 update7-11; 11 update1-3

Virtual Desktop :

- VMware View
- Citrix XenApp/XenDesktop 5.x, 6.x, 7.x (支援最高版本7.15)

Application Server & Web Console

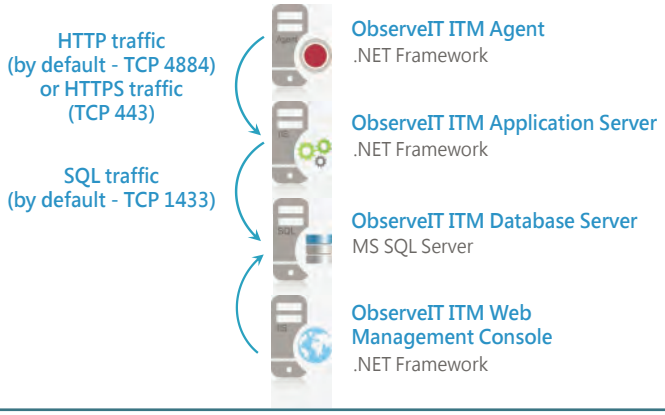
Windows :

- 64bit Windows Server 2012/2012R2/2016/2019
- IIS 8.0 with ASP.NET 4.5/4.6
- .NET Framework v4.5/4.6

ObserveIT ITM Database

Windows :

- 64bit Windows Server 2012/2012R2/2016/2019
- MS SQL Server 2012/ 2014/2016/2017/2019 with latest Service Pack



observe IT
a division of Proofpoint
授 權 台 灣 區 代 理

漢領國際有限公司
JASLEAD

10682 台北市大安區敦化南路二段77號8樓之2
電話：+886-2-2709-6983
傳真：+886-2-2707-6983
www.jas-solution.com sales@jas-solution.com