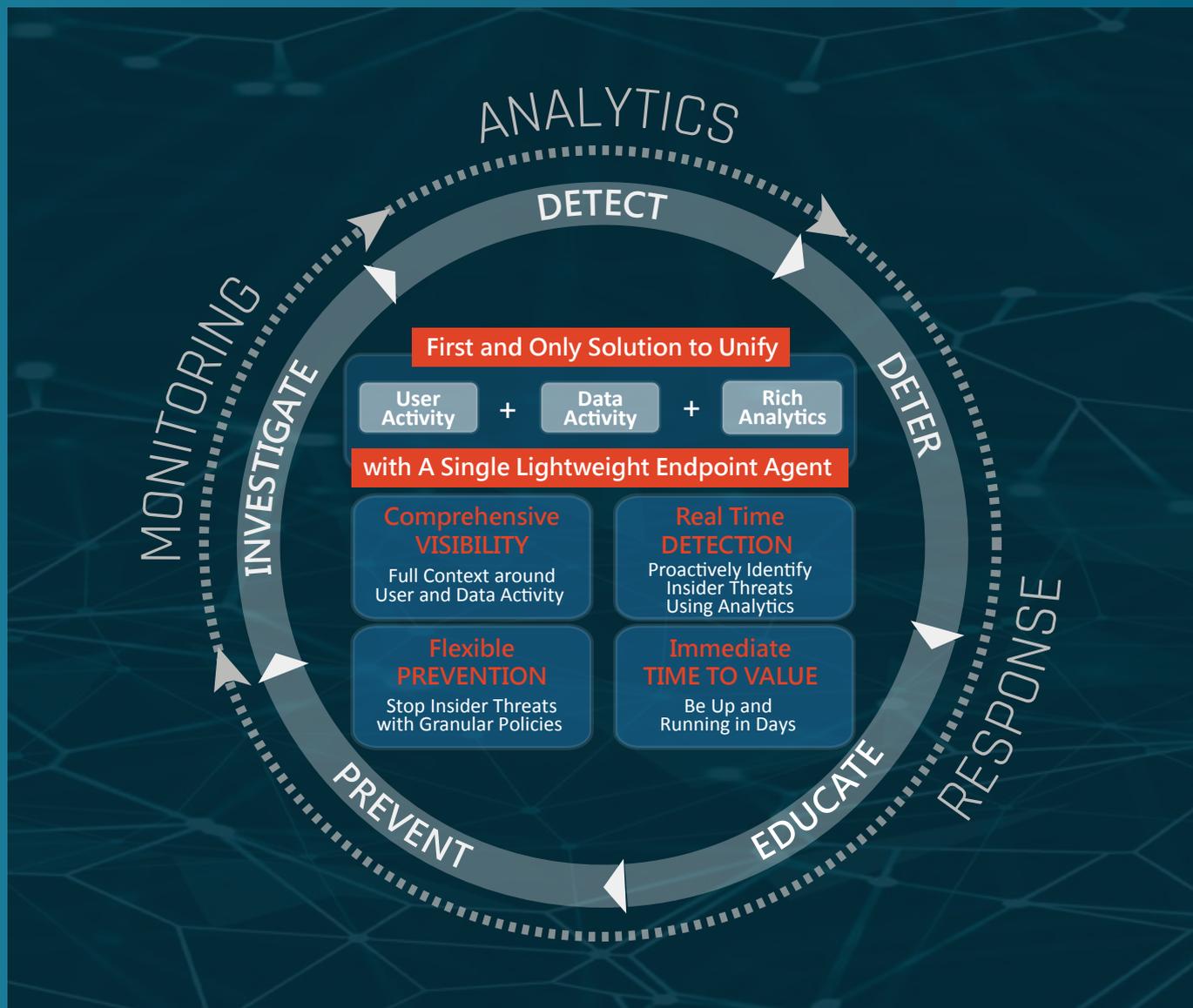


Identify and Eliminate Insider Threats

智慧型視覺化內部威脅暨資料外洩防護解決方案



Your biggest asset is
also your biggest riskSM

ObserveIT 資安新攻略：提前偵測防禦時間軸

著名研調機構 Phonemon 於 2018 年第二季針對全球歐美亞洲金融、服務、科技、製造、醫療、電信、公共事業等共159家代表性企業組織717位資安資訊人員進行調查所發表之「Insider Threat Statistics: The Cost of Insider Threats」報告指出，受調查企業於過去一年內發生逾3千起內部威脅事件，所造成之每一事件損失平均額達876萬美元之鉅。分析結果顯示，內部威脅事件源頭為員工或約僱人員輕忽所造成者約佔64%，每起事件平均損失約28萬美元；內部惡意使用行為所造成者約佔23%，平均損失約65萬美元；其餘13%為使用者身份遭駭客竊取，平均損失約61萬美元。調查結果亦指出，內部威脅事件平均處理天數長達72天，僅有不到16%的事件處理天數在30天以內，而處理時間愈短，事件損失金額愈低。與以往相較，內部威脅事件之數量及損失金額均呈現逐年向上攀升現象。

「人」是內部威脅的原生點，使用者所引發的資安威脅最具殺傷力亦最難偵測與防禦。使用行為分析無法單藉圖像辨識技術或系統日誌精確還原事件全貌，必須藉由具備廣度、深度且細膩的 Metadata，加上時間序列提升可視性及可追蹤性，達到精準辨識並提前偵測內部威脅，進而在事件發生前消弭於無形。ObserveIT針對使用行為進行偵測、阻絕、分析與告警，原解析視覺化加密軌跡精確還原事件過程以利提前辨識行為意圖，完整的「事前偵測阻絕」、「事中蒐證回應」與「事後稽核舉證」內部威脅管理，大幅縮短MTTD與MTTR，強化資安防護。

ObserveIT v7.7 - 後DLP時代內部威脅偵測與防禦

資訊資產保護與資料外洩阻絕需求正急速攀升，成為內部威脅管理重要的一環，從Data、應用程式、各類系統的權限控管、檔案存取進出歷程追蹤與數位證據保存，威脅可視性的涵蓋面更須積極延伸至檔案一致性、網路連結、系統執行序、系統日誌等分析與監控能力。Gartner評估DLP產業的方式已改變，因DLP解決方案無法獨自擔當資料外洩防禦，亦無法應付巨量多元化資料細節分類，導致DLP解決方案被迫縮小應用範圍且產業呈現衰退。

ObserveIT專事各類使用行為之偵測分析，藉由操作行為實際畫面記錄及詳盡Log輔助，協助管理者將防禦時間軸提前，及早洞悉與阻絕各類威脅使用行為與資料外洩的可能性。ObserveIT自v7推出更積極納入DLP-like的資料外洩防禦功能，強化檔案歷程追蹤機制，主動偵測內部檔案異常使用行為，如：異常時段登入、可卸載式儲存裝置、大量檔案複製、雲端上傳/下載及檔案追蹤、Webmail瀏覽、異常列印、使用特殊功能鍵、URL及檔案上傳下載管理政策等。

Detect 偵測

- 內建逾300種國內外常見之內部威脅偵測告警規則。
- 內建29種內部威脅分類可依使用者群組分別設定，如：資料外洩、提權、滲透、未經授權之管理行為、應用程式之資料竊取、肆意或蓄意資料搜尋等，亦可依內規自行定義。

Deter 阻絕

- 針對使用者違反內部資安政策之行為發出告警。
- 告知使用者其違規行為已被側錄並將進行稽核。
- 經證實即時警告使用者可有效減少80%的違規行為。

Educate 教育

- 以即時資安訊息宣導對使用者進行資安教育。
- 經證實宣導教育可有效降低50%資安事件之發生。

Prevent 預防

- 內部資安政策貫徹執行與檢視。
- 立竿見影之數據資產保護與損害控管。
- 最佳偵測與管控流程：資安政策宣導、中斷操作、阻絕關閉及強制登出，實施資安分段防護。

Investigate 調查

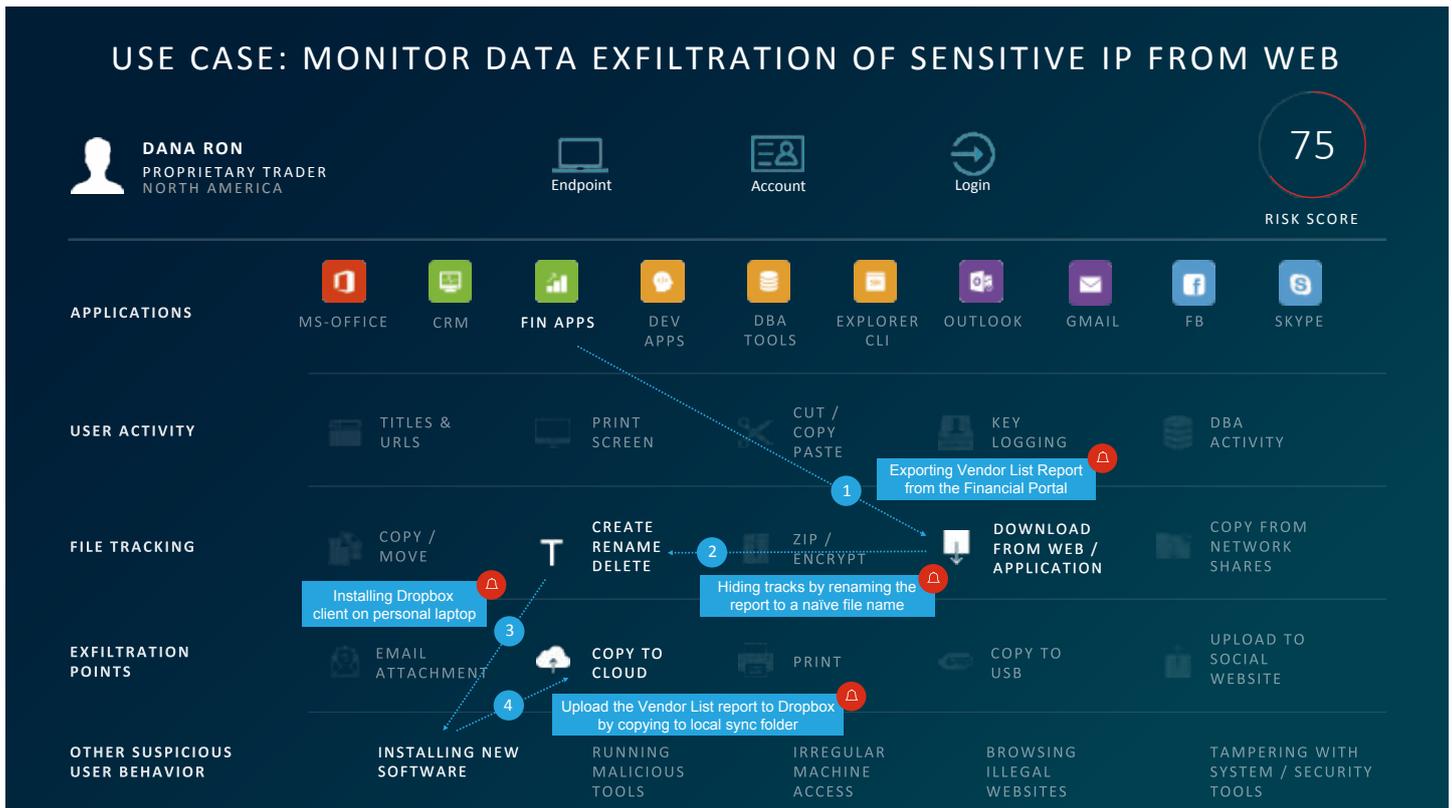
- 精確追溯違規事件發生點，大幅縮短回應與調查時間。
- 即時辨識與過濾內部威脅行為與意圖。
- 進行視覺化軌跡蒐證，具不可竄改之證據能力。



ObserveIT 功能特色

1. Web-Based風險儀表板即時提供管理者整體內部威脅可視性與關聯性軌跡，明確顯示各類使用者、各部門單位、各類觸警風險行為累計/新增之指數與趨勢，並可自訂或套用內建逾300種告警規則/逾29種分類，可進行風險指數重置。
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。
3. FAM (File Activity Monitoring) 檔案活動監控功能，提供詳細的檔案日誌與使用歷程，凡檔案複製、移動、重新命名、刪除、上傳或下載等，皆可立即告警與追蹤視覺化檔案軌跡，以利加速數據資料外洩事件之調查。
4. 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。
5. 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。
6. 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。
7. 針對連結之USB儲存設備、SD Card、iPhone、Android行動裝置進行裝置序號、廠牌名稱、型號名稱等辨識，可依裝置序號建立黑白名單。當系統偵測到以快捷鍵複製或拖拉複製檔案至黑名單USB儲存設備時，將主動告警並紀錄資料外洩完整過程。
8. 可針對列印工作進行監控、偵測與記錄本機/網路印表機的列印工作細節，顯示使用者、主機名稱、印表機名稱/品牌、列印檔案名稱、列印頁數與大量列印等資訊。
9. 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，針對例如釣魚、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。
10. 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。
11. 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ObserveIT播放器進行回播，確保資料無法竄改同時提升證據能力。
12. 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之Watchdog機制將自動重啟並發送即時警示email通知管理者。
13. 支援Windows、Mac、Linux、Unix/HP-UX、Solaris等作業平台，並可增設Windows/Linux管理者身份或共用帳號之第二道認證，及Windows身份盜竊偵測與警示功能。
14. 支援VMware View/RDSH、Citrix XenApp/XenDesktop、Ericom Connect、Windows Remote Desktop、Team Viewer、PCanywhere、VNC、Telnet、SSH、Netop、Dameware、Putty、WinSCP、SFTP等遠端連線操作側錄。
15. ObserveIT之Metadata/告警事件提供Database API、Restful API、CSV/CEF log供外部SIEM如：LogRhythm、IBM、Splunk、RSA、ArcSight等進行Real-time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，落實申請核准記錄、軌跡資料、存取證據、監控記錄之保存。

ObserveIT內部威脅偵測分析應用範例 - 資料外洩歷程軌跡



內建逾300種告警規則/逾29種內部威脅分類，進行偵測、阻絕、告警、側錄，可匯出風險使用行為分析報表

內部威脅偵測分析範例情境	ObserveIT - 偵測、阻絕、告警及視覺化調查
異常時段登入系統	<ul style="list-style-type: none"> › 非正常時段遠端或本機登入行為 › 非正常遠端來源 IP 之登入行為
瀏覽內部機敏資訊平台或外部高風險網站	<ul style="list-style-type: none"> › 內部機敏資訊平台及高風險外部網站 URL 瀏覽行為 (可匯入自訂黑白名單，或整合內建之惡意網站分類資料庫)
未經授權複製機敏資料至外接儲存裝置或上傳至外部雲端硬碟	<ul style="list-style-type: none"> › 使用 FTP 應用程式、指令或 FTP 網址之行為 › 檔案拖拉 / 快捷鍵複製至外接儲存裝置或雲端硬碟等行為
寄送機敏資料至外部信箱或與競業進行聯繫	<ul style="list-style-type: none"> › 連結雲端硬碟、Dropbox 等 URL、Email 收件者帳號、主旨關鍵字、Email 夾檔點選動作及大量複製檔案等觸警行為
未經授權之安裝/解除程式、帳號建立、異常執行序等	<ul style="list-style-type: none"> › 非白名單之應用程式與執行序之使用行為 › 執行 Setup、Installer 等應用程式之行為 › 使用管理工具建立帳號之行為
存取機敏資料夾或共享磁區、編輯文件與圖片	<ul style="list-style-type: none"> › 非授權帳號存取特定資料夾、或開啟/複製特定文件、內文與圖片之行為
應用程式、機敏資料夾、內/外部網站之機敏字串搜尋	<ul style="list-style-type: none"> › 應用程式、機敏資料夾、網站URL等搜尋機敏字串之行為 (In-App) › 鍵盤輸入敏感性字串之行為 (Keylogger)
使用LINE、Skype或Messenger等社交應用程式	<ul style="list-style-type: none"> › 登入應用程式行為 › 傳送與複製特定檔案、內文等觸警行為 › 鍵盤輸入敏感性字串之行為 (Keylogger)



檔案歷程搜尋追蹤



使用者行為分析統計



鉅細靡遺的視覺化調查證據



全球87個國家近2,000家國際知名企業客戶青睞
持續獲得國際資安大獎肯定



Insider Threat Solution



Data Exfiltration Prevention Solution



Best Product Insider Threat Detection



End-Point Security Management

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，符合使用紀錄、軌跡資料及證據保存之規範標準。
- 提供完整的AES加密視覺化紀錄，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 Agent 支援版本

Windows : <ul style="list-style-type: none"> 32/64-bit Windows 7/8/8.1/10 Windows Server 2008/2008 R2 64-bit Only Windows Server 2012/2012 R2/2016 	Linux : <ul style="list-style-type: none"> RHEL/CentOS 5.10-5.11 & 7.0-7.6 x86_64 6.7-6.9 & 7.0-7.4 x86_64/ppc64 Oracle Linux 5.10-5.11, 6.7-6.9, 7.0-7.4 Ubuntu 12.04, 14.04, 16.04, 18.04 (LTS) i386/x86_64 SLES SuSE 11, SP2-3, 12 i386/x86_64 Debian 7, 8 & 9 (32/64-bit) Amazon Linux AMI 2015.03, 2017.09 	Mac OS : <ul style="list-style-type: none"> Sierra 10.12 High Sierra 10.13 Mojave 10.14 	Solaris : <ul style="list-style-type: none"> X86/x64 or Sparc 10 update7-update11 11 update1-update3
ObserveIT Application Server & Web Console	ObserveIT Database		
Windows : <ul style="list-style-type: none"> 64bit Windows Server 2012/2012R2/2016 IIS 8.0 with ASP.NET .NET Framework v4.5 	Windows : <ul style="list-style-type: none"> 64bit Windows Server 2012/2012R2/2016 MS SQL Server 2012/2014/2016/2017 with latest Service Pack 	<p>HTTP traffic (by default - TCP 4884) or HTTPS traffic (TCP 443)</p> <p>SQL traffic (by default - TCP 1433)</p> <ul style="list-style-type: none"> ObserveIT Agent .NET Framework ObserveIT Application Server .NET Framework ObserveIT Database Server MS SQL Server ObserveIT Web Management Console .NET Framework 	