preēmpt

白皮書

透過有條件的存取任何地方Conditional Access Anywhere來保護企業

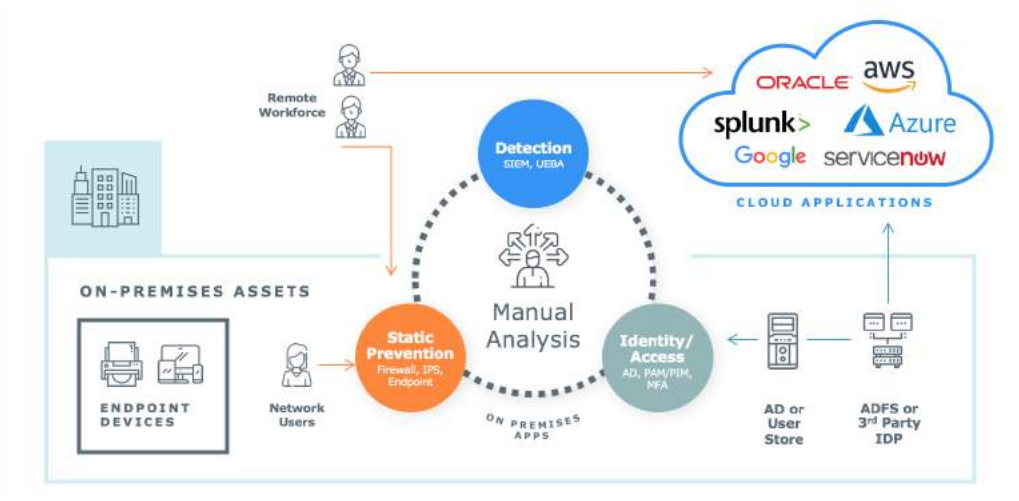
簡介自適應Adaptive與威脅感知的有條件存取Threat-Aware conditional Access，可幫助組織透過了解每個地方的身份來降低風險

目錄

介紹

身份辨識與安全團隊比以往任何時候都需要切實可行的方法來保護其用戶與設備免受網路攻擊、破壞與內部威脅，而又不會破壞他們的業務或使分析人員負擔過重。如今的身份辨識與存取產品缺乏對威脅的洞察力，而安全工具往往會產生許多不確定的警報，需要進行手動調查。同樣的現有的執行方法仍然僅限於簡單的“允許Allow”或“拒絕Allow”反應，這些反應缺乏對行為以及不斷變化的風險環境的理解。

此外隨著組織轉向雲端計算，許多安全團隊已經失去了對其用戶與資產的一致可視性。團隊通常缺乏對雲端中行為的可視性與控制力，或者在最佳情況下，它們依賴於缺少背景的獨立解決方案。



Preempt Platform彌合了這些觀點，使組織能夠提供即時的有條件存取Real-Time Conditional Access與安全控制Security Controls，以防止基於身份、行為與風險的威脅。該解決方案將用戶行為與背景自動反應結合在一起，以偵測威脅，從而重定向危險的用戶行為，並在不中斷業務的情況下主動阻止威脅。該解決方案可以自動了解實體的角色，追蹤一段時間內的行為，並應用靈活的策略，這些策略可以根據情況的變化自動進行調整。靈活的反應選項可以對不斷變化的風險做出漸進反應、自動關閉異常相關的事件、或者在威脅被驗證後立即阻止。

本產品白皮書將深入探討以下領域：

- Preempt Platform的關鍵概念
- 身份辨識與洞察風險 Identity and Risk Insights
- 威脅偵測與分析 Threat Detection and Analytics
- 任何地方有條件存取 Conditional Access Anywhere
- 靈活的部署與過程

Preempt Platform的關鍵概念

Preempt提供了一種新的安全性方法，它將身份辨識、行為與風險整合到統一的安全性背景中。Preempt並沒有保持孤立的安全背景，而是引入了一種新的存取與身份安全方法，它將身份辨識Identity與存取管理Access Management、特權帳號管理Privileged Account Management、行為分析Behavioral Analysis以及網路安全與威脅預防的概念融合為不斷適應改變環境的即時安全方法。

一致的可視性與任何地方有條件存取Consistent Visibility and Conditional Access Anywhere

Preempt 的可視性visibility與策略強制執行Policy Enforcement 可普及到整個企業，包括內部Internal、本地端Premise的行為、用戶與雲端Cloud以及聯合應用程式federated applications中發生的行為。另外策略可以一致地擴展到任何的網路資產，包括工作站、被管理與不被管理管用戶設備，自行定義應用程式、伺服器等。這種一致性使團隊不僅可以追踪整個企業的所有行為，還可以啟用一致的策略，並跟追踪跨越部署在 本地端premise與雲端Cloud資產的事件。

適應性與適當性 Adaptive and Appropriate

取代簡單的“允許Allow”或“拒絕Deny”反應，Preempt可以實現更細微的反應，這些反應可以收集更多資訊並根據所學知識進行調整。這樣可以確保有效用戶不會受到影響。例如如果管理員的設備開始出現異常行為並嘗試存取關鍵伺服器，則Preempt可能會透過第二個身份驗證盤問Identity Challenge。如果管理員未能通過身份驗證盤問，則可能會被 阻斷block連接、透過NAC或其他反應將用戶隔離。如果MFA盤問成功，則政策可以自動解決該事件，以使安全人員不會浪費時間調查低價值事件。

擴展您的安全生態系統

Preempt 可整合包括來自組織中其他解決方案（例如SIEM、防火牆、VPN或SSO產品）的資料的選項。 Preempt可以從其他來源獲取資料（例如信譽饋送Reputation Feeds、MDM解決方案或幾乎任何其他類型的安全產品）。Preempt還可以積極參與其他安全解決方案，例如多因素身份驗證產品以及票證Ticketing或調度系統Orchestration Systems。

身份辨識與洞察風險 Identity and Risk Insights

資料外洩通常從攻擊者在目標環境中發現最初的弱點或漏洞開始，例如員工使用有弱點或已暴露的密碼，或者使用沒有被管理端點unmanaged endpoint的隱影管理員Stealthy Admin，僅舉幾例。為了保護環境，安全團隊對攻擊面（包括所有用戶與帳號）需要具有完全可視性。

查看並驗證所有帳號

安全人員需要了解網路上作業的所有帳號。除了網路的傳統的人為用戶human users外，安全團隊還必須了解許多正在使用的程式服務帳號programmatic service accounts。這些帳號通常具有很高的特權，並且可以成為攻擊者的重要目標。

除了來自Active Directory的資訊外，Preempt還可以直接分析流量。這使Preempt可以對每個實體進行準確的分類，並且還可以識別實體被假冒的時間，例如假冒充服務帳號的人為用戶。此級別的分析還揭露了很多背景，例如能夠將特定的終端與設備特徵與用戶帳號相關聯，例如能夠找到正在使用未被管理設備的管理員。

同樣的該解決方案會自動偵測環境中的多種類型的用戶。該解決方案會根據觀察到的資料自動識別特權用戶與管理員。這種智能包括發現可能具有重要特權但不屬於Active Directory 正式管理員群組official Administrators Group的“隱形管理員stealthy administrators”的功能。該解決方案還可專注於高價值用戶，例如經常成為攻擊者目標的高階主管。可視性同樣可以根據用戶在企業中的職位角色或組織單位與用戶保持一致性。

風險評分Risk Scoring

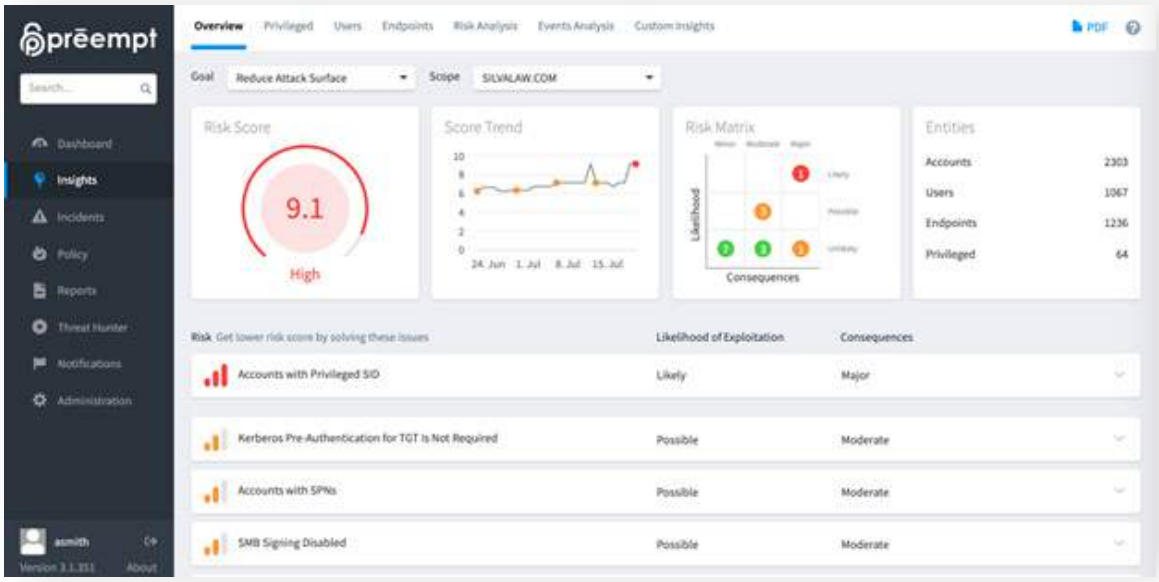
Preempt會將網路中所有實體（用戶、帳號、設備）的所有可觀點和背景納入可行的風險評分中。這可能包括更容易受到攻擊實體，、觀察到的導致危險行為或惡意行為的弱點。該分數表示為介於0到10之間的數字，表示實體的活動或狀態可能導致被惡意攻擊者成功突破，或者內部人員可能流氓。

風險評分會根據環境變化不斷進行評估和更新。風險評分的某些元素會隨著時間的流逝而緩慢衰減，而其他一些則可以快速解決。例如，當用戶從有弱點密碼更改為強固密碼時，用戶的風險分數會立即降低。 此外，重要的用戶或資產可以提高風險得分，例如具有管理權限的帳號，具有執行權限的超級用戶，甚至是具有特定關鍵角色的伺服器。整個Preempt解決方案都使用風險評分來自動化反應，並使員工能夠快速調查事件或識別網路中的問題用戶。透過使用API與其他系統和業務流程平台共享Preempt風險背景，甚至可以在Preempt平台之外使用風險評分。

洞察Insights

發現並搶先解決弱點是強化的網路安全最重要的方法之一。但是弱點可以以多種形式出現-用戶特定的特徵，例如密碼問題、設備設定問題、使用過時與有弱點的通信協定、Active Directory設定以及對面對多種攻擊技術時脆弱性。Preempt Platform的“Insights”洞察頁面專門用於追踪網路的安全狀況，同時更容易查找與監視網路中風險最大的用戶、設備與帳號。

洞察Insights 讓發現許多問題變得容易。例如包括尋找 共用相同的本地管理員憑證的設備、密碼弱的用戶、允許使用RDP或RPC的設備、多個用戶共用的帳號等。這種可視性使組織可以盡可能減少攻擊面，並密切監視可能吸引攻擊者的任何資產。



洞察Insights頁面包含用於查看各種預建的風險檢視圖。工作人員可以立即跳到特權用戶Privileged Users、最終用戶End Users、端點Endpoints以及所有實體的風險評估Risk Assessment的專用檢視圖。或者 員工可以存取與具體使用情況相關的檢視圖，例如檢查Active Directory的整體狀況、網路或特定網段的攻擊面分析。

每個檢視圖都是互動式的，因此很容易深入到更多的資訊。以下列表僅包含Preempt可以自動識別的一些弱點：

- 使用非被管理端點的用戶或管理員
- 陳舊的特權帳號 Stale privileged account
- 與NTLM版本相容的設備
- SMB signing簽章被關閉
- 容易被萬能鑰匙skeleton key攻擊的設備
- 使用相同本地管理員的多台設備
- 僅使用DES 金鑰的帳號
- 永不過期的密碼 Password that never expires
- 隱形管理員 Stealthy administrators
- 使用有弱點的密碼weak password
- 高風險評分
- 使用已經暴露的密碼

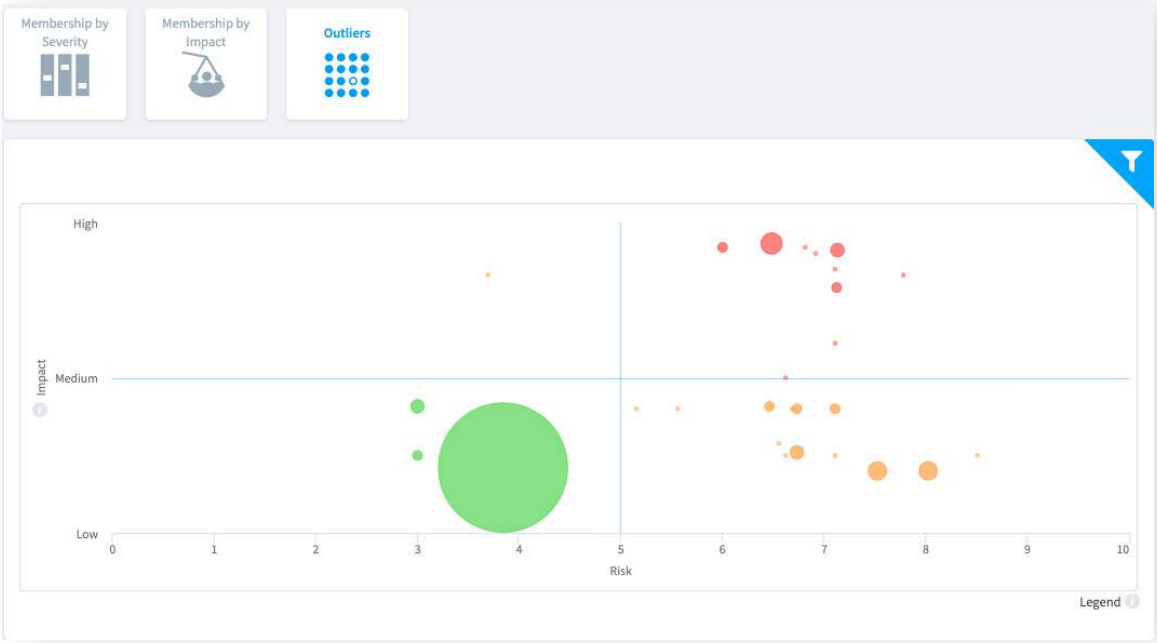
洞察Insights頁面還使工作人員可以輕鬆追蹤隨時間變化的情況。“特權用戶Privileged Users”檢視圖可以輕鬆顯示何時有新建立的管理員帳號，否則可能會有遺漏。同樣的在“端點Endpoints”標籤中，工作人員可以輕鬆地查看在特定時間內是否有更多沒有被管理的端點連進了網路。

洞察Insights頁面會提供每個相關用戶或設備的詳細列表，以供進一步調查。該列表稱為實體列表Entity Table，可深入了解每個實體。該表顯示該實體是人？程式的還是設備？與其組織單位(OU)與風險評分。 然後該表可以基於特定實體提供各種附加的詳細特徵。例如系統可以將特定用戶區分為主管executive、受監視用戶watched user或具有多個設備的用戶。可以進一步將設備標識為App Server或DNS伺服器，或具有易受攻擊的作業系統的設備。員工還可以透過Preempt解決方案追踪基於幾乎任何屬性建立自己的自行定義洞察。

Type Primary	Secondary	Department	Org. Unit	Attributes	Score ↓
Amanda Hutchinson	SILVALAW.COM\AHutchinson	Civil	silvalaw.com/NYC_HQ/Corp_...		8.5
Brian White	SILVALAW.COM\BWhite	Finance	silvalaw.com/NYC_HQ/Corp_...		7.8
Rita Parker	SILVALAW.COM\RParker	HR	silvalaw.com/NYC_HQ/Corp_...		7.2
Carol Carson	SILVALAW.COM\CCarson	Security	silvalaw.com/NYC_HQ/Corp_...		7.1
Paul Taylor	SILVALAW.COM\PTaylor	IT	silvalaw.com/NYC_HQ/Corp_...		7.1
Sharon Jefferson	SILVALAW.COM\SJefferson	M&A	silvalaw.com/NYC_HQ/Corp_...		7.1
Laura Henson	SILVALAW.COM\LHenson	IT	silvalaw.com/NYC_HQ/Corp_...		7.1

風險分析Risk Analysis

“洞察Insights“頁面還為員工提供專門的風險分析檢視圖Risk Analysis view資訊。該資訊可視化與顯示關於對網路的影響的風險評分。例如一個用戶可能具有較高的風險評分，但是如果該用戶在網路上具有相對有限的特權，則影響可能很小。該圖分為四部分，右上角代表具有高風險和高影響力的實體。這再次為員工提供了一種非常有用的方法，可以幫助他們聚焦最需要關注的用戶。



風險分析Risk Analysis頁面還可按照 群組Group與組織單位Organizational Unit細分風險。這使員工可以輕鬆地確定對企業風險影響最大的群體與個人。“異常值Outliers”檢視圖通過顯示單個用戶或實體在影響範圍內的風險來提供更多詳細資訊。 例如用戶可能基於一系列異常或潛在的惡意行為而具有較高的風險評分，並且由於其對高價值資料庫或應用程式的存取而具有較高的影響評分。

報告Reporting

Preempt platform提供了幾乎所有特徵追蹤的內建與可自定義的報告。這可以極大地簡化組織內的資訊共享，同時加速諸如法規遵循報告之類的常規工作的速度。可以根據時間設定報告（每週、每月等），並且可以通過電子郵件發送或以PDF格式下載。

威脅偵測與分析 Threat Detection and Analyticsytics

Preempt sensors感測器可以直接分析往返於身份驗證基礎設施間的流量。這使平台可以直接偵測環境中的各種威脅，並隨著時間的推移不斷追踪所有實體的行為。Preempt會自動學習每個實體的正常行為模式，並識別風險Identifies Risky或異常行為Anomalous Behavior。

增強實體分類 Enhance Entity Classification

除了來自Active Directory的資訊外，Preempt還可以直接分析流量。這使Preempt可以對每個實體進行準確的分類，並且還可以識別實體被假冒的時間，例如假冒充服務帳號的人為用戶。此級別的分析還揭示了很多背景，例如能夠將特定的終端與設備特徵與用戶帳號相關聯，例如能夠找到正在使用未被管理設備的管理員。

異常行為 Anomalous Behavior

Preempt會不斷學習並追蹤環境中每個用戶、設備和帳號的行為，以便識別任何異常行為。異常行為不一定是惡意行為，但它通常可以是環境中某些問題的第一個指標。 例如最終用戶從異常位置或異常時間存取異常資源可能表明該用戶可能已受到攻擊者或惡意軟體的威脅。透過學習各種特徵的正常行為，Preempt可以標記異常、對用戶的風險等級進行評分，將其與同級行為進行比較，然後要求用戶確認身份以確保該行為有效。

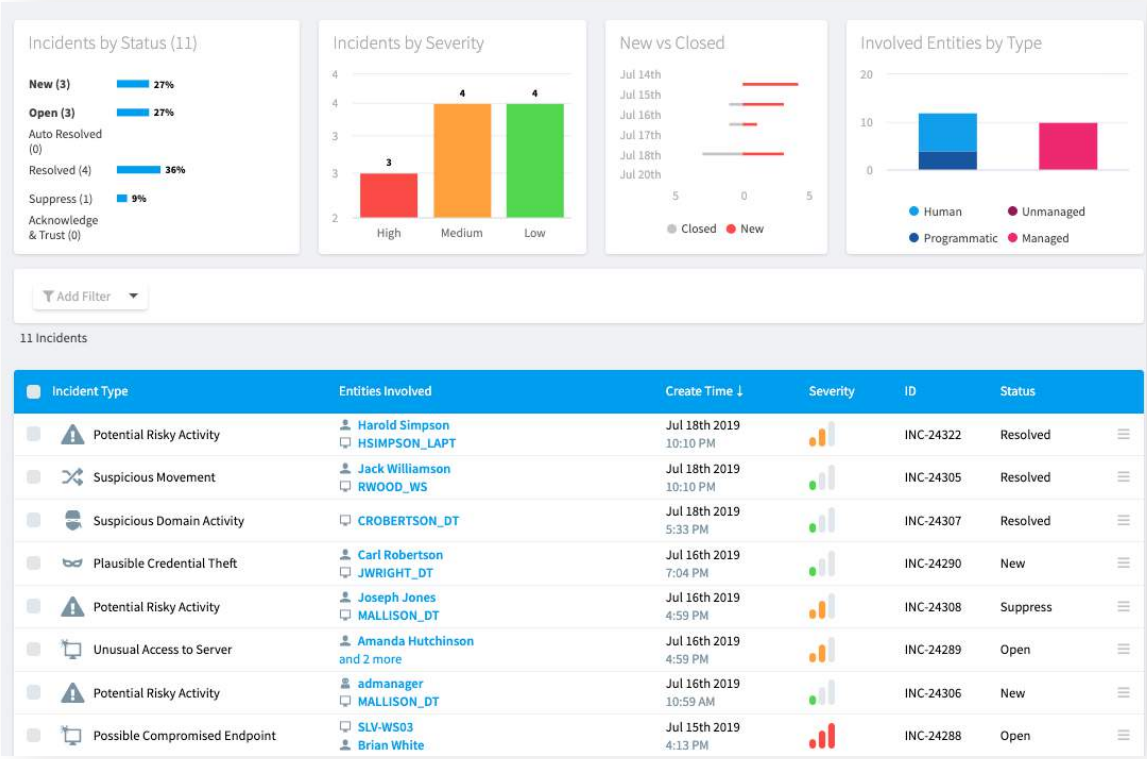
惡意行為Malicious Behavior

Preempt 直接揭露了攻擊者用來在內部橫向移動的惡意行為與擴大入侵的網路技術。這包括如 哈希傳遞(Pass-the-Hash)、金票Golden Ticket攻擊、Active Directory Harvesting等技術，並嘗試通過偽造的特權帳號憑證forged Privileged Account Certificate（PAC）來提升特權。該分析還揭露了使用常見的攻擊工具（例如Mimikatz）或使用不安全的協定（例如NTLM）。 這些偵測特別有價值，因為它們可以顯示更具確定性的攻擊跡象。同樣重要的是要注意，偵測這些行為通常需要直接分析Preempt Platform提供的網路流量，如果只有分析日誌流量就會無法偵測到。

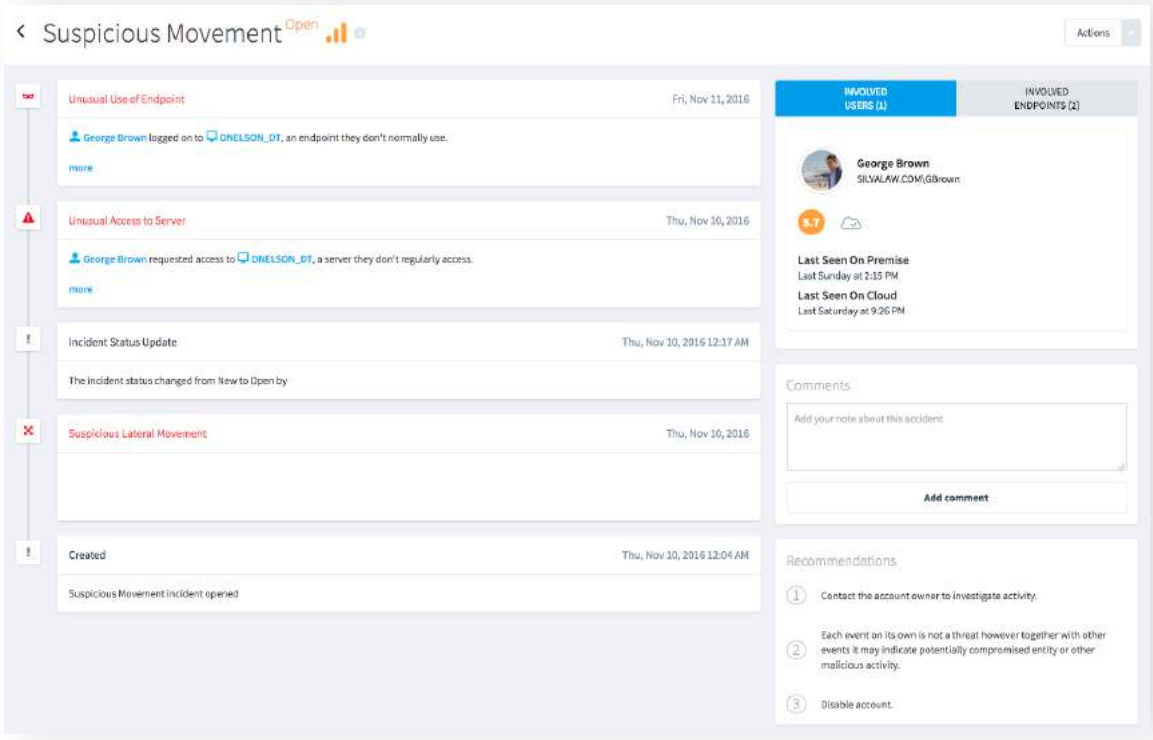
惡意行為Malicious Behavio	異常行為 Anomalous Behavior	實體分類Entity Classification	安全狀態Security Posture
++暴力攻擊 ++帳號掃描 ++哈希傳遞/票證Pass-the-Hash /Ticket ++ AD收集 ++偽造的PAC檔案 ++等等	++存取的資產 ++使用的應用程式或服務 ++時間 ++位置 ++設備 ++等等	++人為或程式Human vsprogrammatic ++工作站或伺服器 ++被管理或未被管理 ++等等	++脆弱的密碼 ++曝光的密碼 ++共用帳號 ++陳舊的特權帳號 ++ NTLM使用 ++等等

事件調查Investigating Incidents

“Incidents事件”頁面讓管理員可以快速存取完成工作所需的資訊。管理員可以自行定義時間範圍，然後根據嚴重性、狀態（新的，打開的，已解決的）與用戶的類型（人為或程式）或設備（被管理或為被管理）進行進一步過濾。工作人員還可以搜索特定類型的事件，或識別涉及特定用戶，帳號或設備的事件。



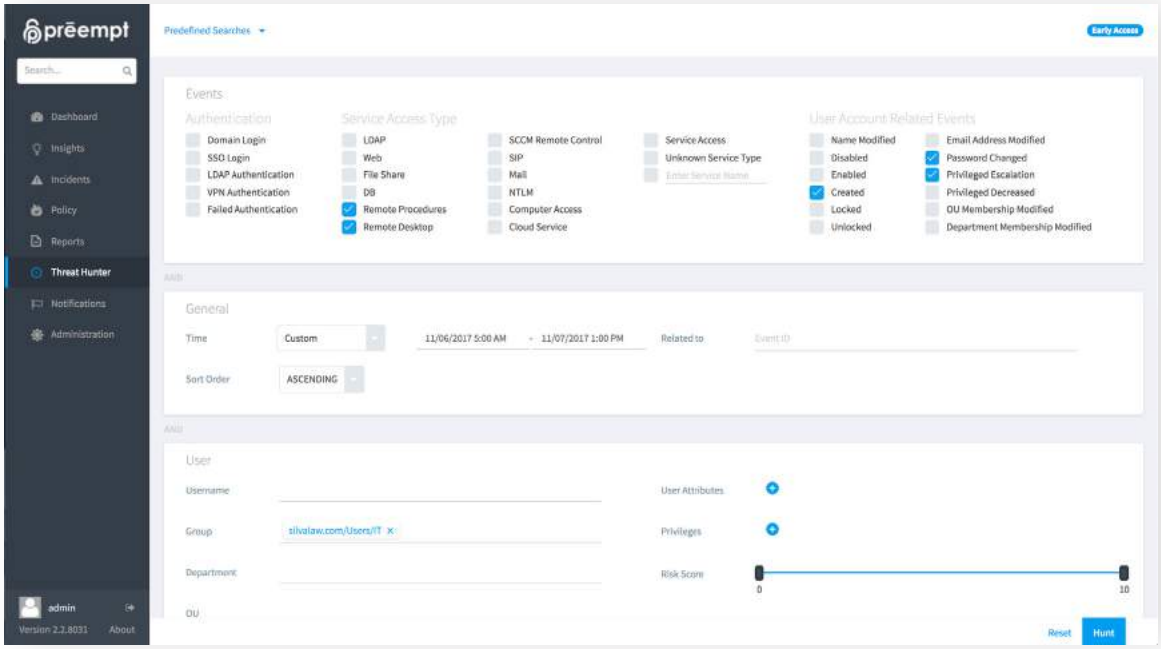
點擊特定事件可提供該事件及其隨時間推移的詳細敘述。例如，在下面顯示的“可疑移動Suspicious Movement”事件中，詳細資訊顯示了事件的建立時間以及觀察到特定用戶的存取和異常伺服器，然後第二天使用異常設備。員工可以點擊以在事件詳細資訊中了解有關特定事件的更多資訊。螢幕的右側還顯示了有關事件中涉及的用戶或設備的詳細資訊，以及其總體風險評分和上次查看時間。該檢視圖還提供了有關後續步驟的建議，並為管理員提供了對事件發表評論的地方。



事件進行調查後，工作人員可以透過將事件標記為 已解決resolved、已撤消dismissed或誤報false positive來進一步管理事件。 儘管Preempt將繼續在後台追踪事件，但已撤消事件將抑制該事件。如果將來發生同一事件，則將再次產生該事件。如果某個事件被標記為誤報，則將獲悉該行為是允許的，並且將來不會產生新的事件。

搜尋威脅Threat Hunter

直覺式的界面使分析人員可以通過Preempt Platform追踪的屬性與網路流量事件的任意組合進行查詢與關聯。分析師可以自由地遵循自己的直覺，並提出開放式問題，這些問題涉及用戶與設備的屬性、存取與身份驗證方法、帳號更改、時間、地理位置等。當分析人員看到有趣的事情時，Threat Hunter可以提供任何相關事件與按時間順序排列的檢視圖，以將搜尋到的詳細資訊置於完整的背景中。



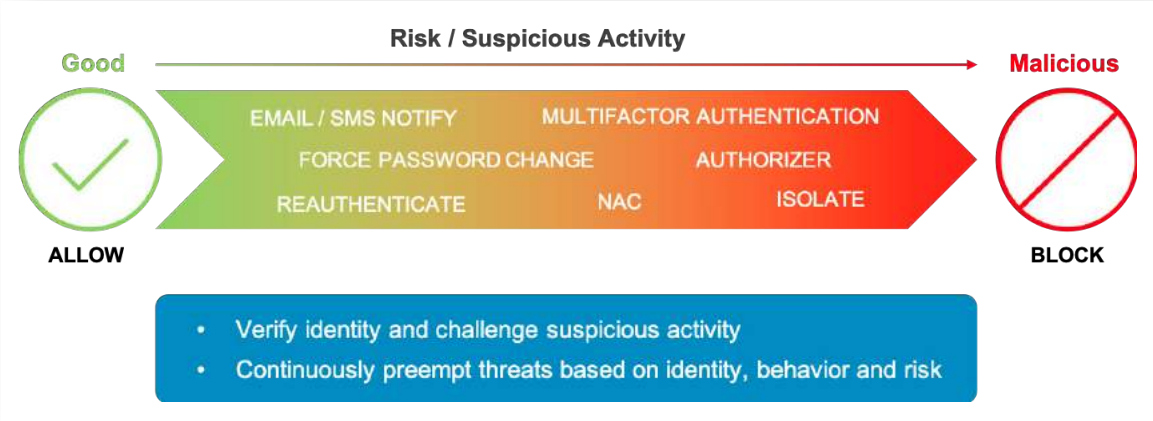
有條件的存取任何地方 Conditional Access Anywhere

偵測威脅Detecting threats顯然是Preempt Platform的關鍵組成元件，但最終的解決方案是將這種智能轉變為適合業務的行動。總體目標是提供自動化的反應，而無需分析師花費時間或影響有效的最終用戶。為了實現這一目標，Preempt利用了高度自適應的策略引擎Adaptable Policy Engine，該引擎可以阻斷block、盤問用戶challenge users、驗證威脅並提供各種即時分級反應。這使組織能夠建立強大的有條件的存取策略，使各種安全背景與即時與業務適當的反應保持一致。

Preempt 策略引擎Policy Engine

Preempt 策略引擎Policy Engine是有條件存取的關鍵。它將觀察到的行為、用戶角色、風險評分、被存取的目標，存取方法以及許多其他因素帶入單一行動導向的背景中。同樣重要的是，政策有能力獲得新的資訊並隨著時間的推移進行調整。當Preempt偵測到異常或危險的用戶行為時，策略引擎可以自動盤問用戶以確認其身份。然後根據反應，策略引擎可以採取進一步的措施，例如透過NAC隔離用戶、阻止存取或通知員工。這種即時、自適應有條件存取的方法可確保行動保持適合情況，而無需分析師的持續關注。

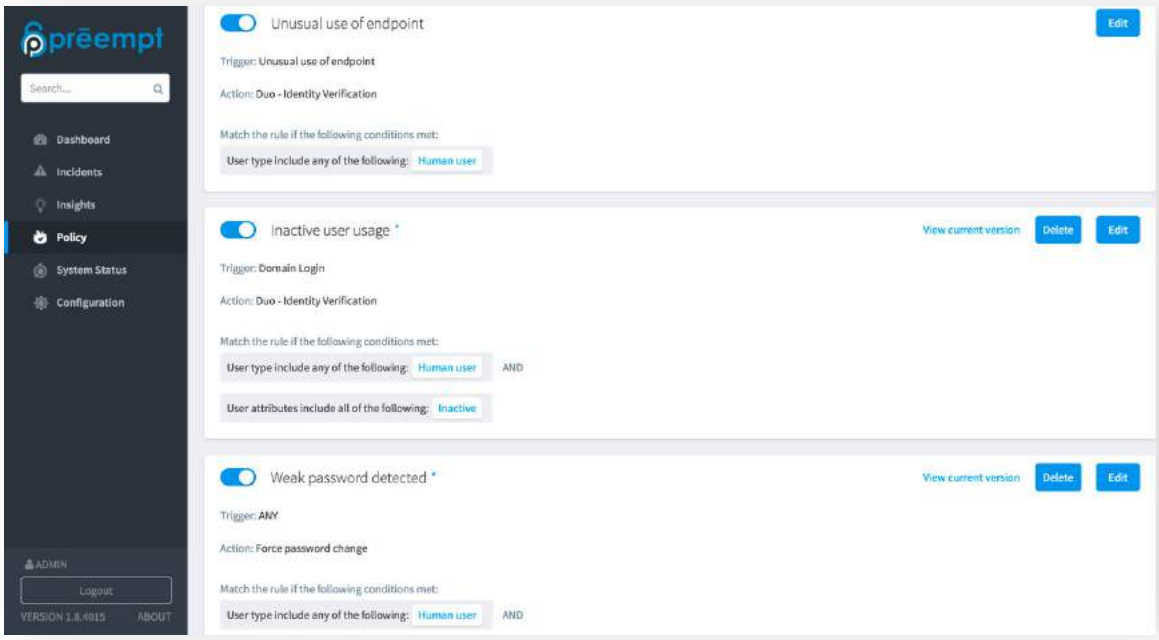
策略引擎接受各種輸入，例如任何偵測規則、用戶自行定義的規則或對實體屬性的更改。反應可以包括阻止用戶、，強制更改密碼或使用多因素身份驗證Multi-Factor Authentication盤問用戶的能力。盤問的結果同樣可以改變用戶的風險評分，也可以推動進一步的反應。 這使策略引擎和組織的反應可以與用戶進行邏輯交互並適應情況。



.

策略引擎如何運作

Preempt策略建立在觸發器trigger、條件conditions與行動actions的組合上。觸發器是策略規則的核心活動，例如端點的異常使用。條件使策略可以針對特定情況或範例。例如針對端點異常使用的策略可以專門清查屬於主管人員的設備的異常行為。行動Actions是指定符合規則時要使用的自動反應或安全控制。



將身份、角色、目標和行為納入策略引擎可確保業務處理在安全威脅的同時持續進行。下表僅提供一些可以使用Preempt建立的有條件存取策略範例。

行動Action	條件Condition	觸發器Trigger	用戶User
需要批准Approver required	任何或特定	從新位置登錄	第三方供應商、顧問
使用第三方NAC進行隔離	任何	風險評分Risk score > 9	任何
將用戶增加到SSO風險群組以限制對雲端應用程式的存取	任何	在本地網路中偵測到哈希傳遞Pass-the-hash	任何
阻斷 Block	工作站	遠端桌面Remote Desktop	管理員Admin
MFA-驗證身份	關鍵伺服器群組	登錄Login	不是來自跳板機的任何用戶
下次登錄時更改密碼	任何	偵測到有弱點密碼	員工

將MFA擴展到任何資源

透過Preempt組織可以將多因素身份驗證MFA擴展到企業中幾乎所有資源。借助Preempt基於網路的方法，團隊可以向自行定義、舊版legacy與本地應用程式增加有條件存取與MFA 控制，而無需對受保護的應用程式進行任何更改。Preempt還可以將MFA控制增加到資產（例如資料庫或工作站），而無需在受保護的設備上安裝代理程式 agent。 此外通過與Active Directory聯合身份驗證服務（ADFS）整合，Preempt可以保護透過Web瀏覽器（如 Office 365）甚至設定為單一登錄（SSO）的應用程式存取的任何聯合服務。

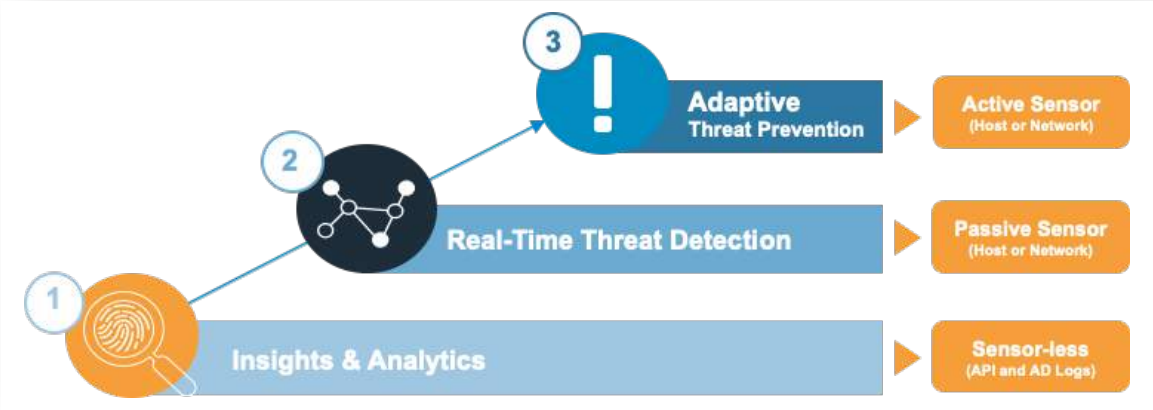
靈活的部署與過程

Preempt Platform在解決方案的部署方式方面為客戶提供了極大的靈活性。在最高等級，可以透過三種不同的方式來部署Preempt Platform：

- **無感測器部署Sensor-less Deployment** -在此種設定中，Preempt透過查詢Active Directory伺服器以獲取與安全相關的重要特徵並通過API整合來自其他企業來源的日誌來收集資訊。此選項提供對用戶帳號的洞察與分析、辨識特權用戶、隱形管理員以及各種與密碼有關的問題。

- **被動式感測器Passive Sensor部署**-此選項利用了被動式Preempt Sensor，可以將其部署在網路中或Active Directory伺服器本身上。這種方法允許Preempt直接分析往返Active Directory基礎設施的流量。這種方法包括無感測器Sensor-less部署的所有洞察，還增加了分析用戶行為與即時偵測威脅活動（例如橫向移動lateral movement、攻擊工具attack tools和危險協定dangerous protocol使用）的能力。

- **主動感測器部署Active Sensor Deployment** -這是最強大的部署選項，包含所有上述功能以及強制執行有條件存取策略enforce conditional access policies（如自適應adaptive MFA、阻止威脅等）的能力。主動感測器可以部署為串聯網路感測器in-line network sensor，也可以直接部署在Active Directory伺服器上。



每次僅需要這些選項之一。這種靈活的架構意味著Preempt可以輕鬆滿足任何環境的需求，同時根據需要保留進行擴展的選項。許多客戶最初將使用主動感測器active sensors 進行部署，以利用Preempt Platform的所有功能，而其他客戶則可以從洞察力與分析開始，這只需要Active Directory憑證即可。

結論

希望本文有助於介紹Preempt Platform的一些關鍵概念。 但是，本文肯定不是該解決方案功能的詳盡列表。 我們鼓勵您通過觀看演示或在您的環境中測試解決方案來繼續學習，在其中我們可以詳細顯示Preempt如何幫助您滿足網路的獨特需求。