THE PREEMPT PLATFORM

透過有條件的存取Conditional Access保護企業並防止威脅

如果您難以識別組織中的所有用戶與帳號，以及了解他們正在做什麼和存取的內容，那麼主動降低風險與預防威脅將非常困難。Preempt Platform採用現代方法進行身份驗證與保護身份，並幫助您重新回到駕駛員的位置，這樣您就可以降低風險，並在威脅影響您的業務之前自動防止威脅。

優點

- 隨時了解身份
- 即時偵測威脅
- 透過有條件的存取Conditional Access防止威脅

防止威脅的新方法

Preempt Platform可快速清查網路中的所有用戶，並提供持續的洞察風險risk insights與行為分析behavioral analytics，以便在威脅影響您的業務之前更好地偵測與反應威脅。Preempt Platform獨特的自適應功能adaptive capabilities允許您使用基於身份、行為與風險程度正確執行或通知自動化威脅反應。這可確保提供適當級別的安全性，以阻止威脅或允許合法用戶繼續工作。

無論是在本地端on-premises還是在雲端cloud，Preempt都可隨著組織的發展與變化適應您的需求。您可以在短短兩小時開始使用Preempt Platform的優點，並獲得即時和持續的好處。

洞察身份 Identity Insights

清查您網路中的所有用戶 - 業務、特權、服務 - 並通過查看 脆弱密碼 Weak Password、隱形的管理員 Stealthy admins、陳舊帳號 Stale accounts以及更多來減少您的攻擊面

分析與偵測威脅 Analytics and Treat Detection

持續的洞察與分析使您能夠偵測威脅並降低風險

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

基於身份、行為與風險策略執行適應性 Adaptive與規範性的 Prescriptive自動化反應

preempt

THE PREEMPT PLATFORM

Platform 組成

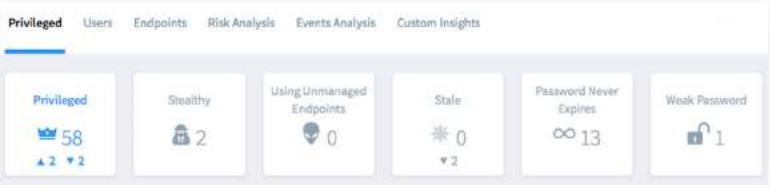
洞察身份與風險
Identity and Risk Insights

組織通常對於誰存取多個安全解決方案與平台的內容、時間、地點和方式有著錯綜複雜或不完整的觀點。Preempt 通過自動發現並持續監控所有用戶、權限、帳號和存取來解決此問題，無論是在本地端on premise還是在雲端cloud。

通過一個易於使用的管理控制台，Identity and Risk Insights提供持續的健康與風險評估 - 揭露 密碼問題、特權存取、隱形的管理員、Active Directory（AD）設定問題等，以便您可以更好地控制所有帳號（一般用戶、特權、服務等）同時允許您的安全團隊輕鬆主動地降低風險和攻擊面，使您更容易通過下一次稽核。

透過統一的可視性降低風險

- 持續清查所有用戶：特權、服務帳號、一般用戶、陳舊帳號
- 制定統一的用戶存取設定檔user access profiles 並識別可疑行為
- 在攻擊者發動之前降低風險並發現問題



分析與偵測威脅
Analytics and Threat Detection

Preempt的用戶與實體行為分析User and Entity Behavior Analytics了解網路上每個用戶與設備的行為，包括特權用戶與服務帳號，並為每個用戶與設備制定風險評分risk scoring。該系統根據各種因素對用戶與機器進行分類與度量，包括來自雲服務、SSO，VPN、監督與無監督學習以及即時身份驗證流量的活動。

分析揭露有風險的用戶行為、惡意的內部人員、攻擊者、被入侵帳號或設備、橫向移動 lateral movement、嘗試升級權限escalate privileges以及攻擊內部基礎設施。

基於憑證的攻擊仍然是組織受到入侵的首要方式。Preempt以不同方式處理偵測到的威脅。 通過將關注身份、行為和風險的分析與即時流量（passive/sniffer模式或inline）相結合，您可以在攻擊偵測中獲得更高的真實度。

獨特的是，通過Preempt Platform，您可以防止由於濫用網路工具（例如PsExec、PowerShell）和使用駭客工具（例如Mimikatz、Bloodhound等）而導致的橫向移動 lateral movement 與未經授權的網域存取。 Preempt還能夠深入檢查身份驗證協定（NTLM、Kerberos、LDAP等），以幫助控制不安全的協定使用並降低安全威脅的風險，包括憑證轉發credential forwarding和密碼破解憑證以及偵測如Kerberoasting、Pass-the-Hash Golden Ticket等攻擊。

即時偵測與調查對憑證的威脅

- 即時偵測可疑或危險行為
- 確定辨識攻擊與使用惡意攻擊工具
- 加強調查與搜尋威脅 threat hunting
- 確定通過有條件的存取Conditional Access對風險區域更好的地控制

透過有條件的存取 Conditional Access 預防威脅

當您的團隊因為資安事件不堪重負時，就無法對每個威脅做出反應。現在當偵測到可疑行為時，Platform的有條件存取Conditional Access功能可以介入，以幫助主動反應威脅，而不會讓分析師參與或干擾有效用戶。

Preempt可以逐步與用戶交互以驗證威脅並執行策略。細緻的操作允許您將反應級別與風險相匹配，並可根據不斷變化的背景context自動進行調整。

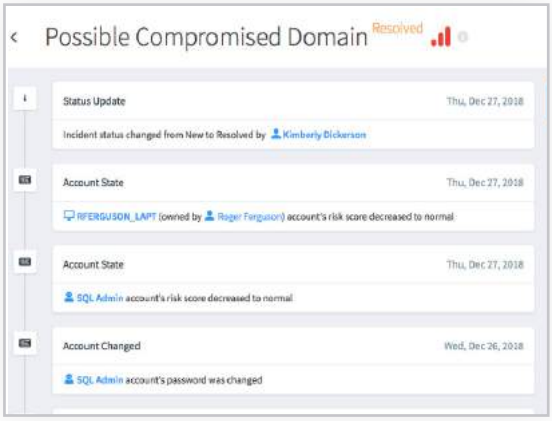
基於策略的反應（例如 阻止Block、多因子認證MFA、隔離Isolation、減少特權Isolation、報警alert、允許allow等）根據身份、行為與風險不斷進行調整。例如：在授予存取權限之前，可以根據風險行為將MFA多因子認證要求推播給用戶。

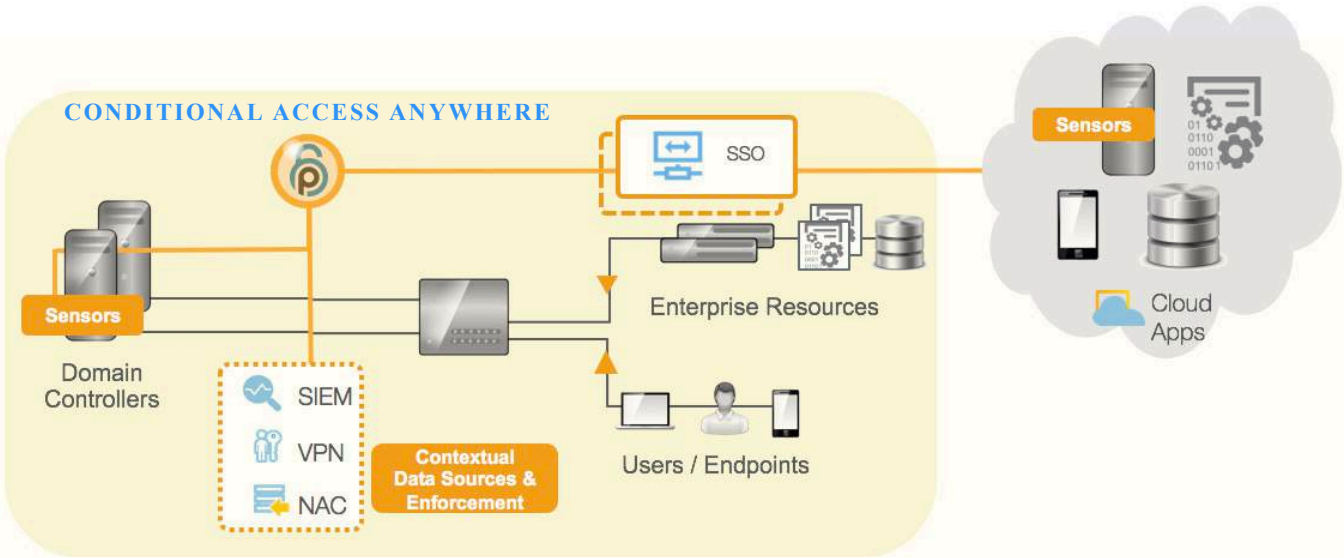
自適應多因子認證Adaptive MFA可根據您的需求與政策提供最佳靈活性：

– 通過增加基於策略的強制執行來立即保護內部資源
- 在使用任何網路資源前輕鬆增加多因子認證MFA，無需修改應用程式或增加端點代理程式agents
- 確定並強制執行誰能夠存取哪些資源以及在何種背景（例如角色role、設備device、位置location等）例如：限制承包商對敏感伺服器的存取、服務帳號的互動式登錄等

在威脅影響前先發製人

- 即時阻止威脅
- 通過自動反應發揮最高效率
- 為本地端或雲端應用APP增加有條件的存取Conditional Access
- 在沒有開發且沒有端點代理程式情況下將多因子認證MFA 增加到任何資源





Contextual Data Sources:

背景資料來源：網路流量/日誌/第三方整合

Enforcement Options:

選購強制執行：自適應多因子認證Adaptive MFA /減少特權/隔離、阻止等更多

客戶如何使用Preempt Platform

自適應多因子認證Adaptive MFA

+基於身份、行為與風險的有條件的存取Conditional Access
+工作站登錄身份驗證
+高價值伺服器與應用程式存取
+基於政策的存取權限
+將多因子認證MFA增加到任何程式存取
+ 雲端Cloud、本地On Premises、混合雲Hybrid

特權帳號安全 Privileged Account Security

+特權帳號清查/使用
+特權用戶的風險評估
+防止特權升級 privilege escalation、橫向移動 lateral movement
+特權存取濫用
+隱形（影子）管理員的存在
+基於政策的控制

“我們研究了其他四種解決方案，沒有其他產品能讓我們能夠即時阻止與反應威脅。”

大型保險協會的首席資訊官

偵測內部威脅 與憑證竊取 Detect Insider Threats + Credential Compromise

+被入侵的帳號/設備Compromised accounts/devices
+橫向移動Lateral movement
+基礎設施攻擊，如Golden Ticket或Kerberoasting
+異常或危險行為
+受限制的資料存取
+勒索軟體/惡意軟體 ransomware/malware的傳播

Active Directory 安全

+工作站登錄身份驗證
+高價值伺服器與應用程式存取
+基於政策的存取權限
+將多因子認證MFA增加到任何應用程式

每一步的價值	Preempt Platform		
	Identity and Risk Insights 洞察身份與風險	Analytics and Threat Detection 分析與威脅偵測	有條件的存取 Conditional Access
用戶與帳號存取可視性	✓	✓	✓
清查特權帳號	✓	✓	✓
清查隱藏的管理員與陳舊帳號	✓	✓	✓
密碼強弱的可視性	✓	✓	✓
法規遵循報告	✓	✓	✓
風險用戶行為與異常偵測		✓	✓
攻擊工具與誤用的通信協定		✓	✓
橫向移動與搜尋威脅		✓	✓
適應性反應與策略執行			✓
保護雲端應用程式的聯合存取			✓
保護任何應用程式的存取控制			✓
即時防止威脅			✓

preempt

www.preempt.com info@preempt.com

Preempt提供了一種現代化的身份驗證方法，並通過市場的第一個解決方案提供 身份辨識、有條件的存取Conditional Access，以便根據身份、行為與風險持續偵測並防止威脅。Preempt的專利技術使企業能夠優化身份保護，並在影響業務之前即時阻止攻擊者和內部威脅。

詳細 產品資訊請洽 商丞科技股份有限公司 02-29148001