SentinelOne

Singularity™ Identity Posture Management

評估、偵測並修復對 Active Directory 的威脅

在以竊取「身分」為主要目標的網路攻擊中，AD 和 Entra ID (舊稱 Azure AD) 已成為最常見的攻擊目標。一旦 AD 或 Entra ID 內的身分被竊取，駭客便能在企業環境中建立立足點，並更進一步探索企業網路、持續潛伏、提升權限，甚至挖掘更多潛在目標並不斷進行橫向移動。

Singularity Identity Posture Management 是 Singularity XDR 平台的其中一項解決方案，用以針對 Active Directory (AD) 和 Entra ID 相關組態進行評估、偵測可能蘊含風險的組態設定即存在的漏洞。 Singularity Identity Posture Management 針對企業可能面對的威脅或攻擊面向提供具體、有建設性的處置建議，以降低企業被滲透風險，並符合最佳實踐 (Best Practice) 以提升企業資產安全。

持續分析身分曝險

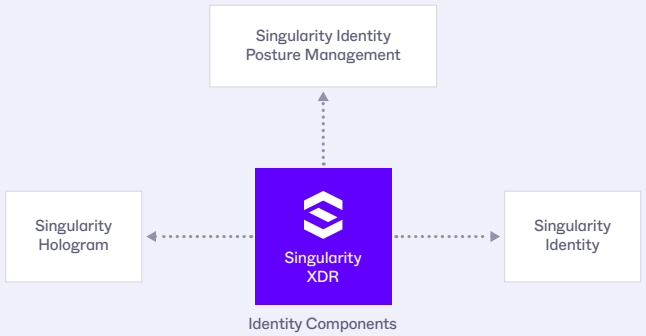
不再採取昂貴且耗費人力的方式，改以全自動從重點網域(Domain)、裝置(Device)及使用者層面 (User-level) 分析 Active Directory 和 Entra ID 曝露風險情形。

減少針對 AD 層面的攻擊

分析並確認組態設定的變更是否符合最佳效益，並取消不必要的特權，快速緩解 AD 層面可能遇到的攻擊。

即時偵測 AD 攻擊指標

主動監控 AD 及 Entra ID 的活動行為，是否具潛在攻擊行為的活動特徵。可依照不同需求進行不間斷控制或一次性偵測。



Singularity Identity Posture Management 部署方便簡單，並針對 Active Directory 和 Entra ID 相關組態設定提供具體且有建設性的處置建議措施，有效降低身分攻擊的可能性。

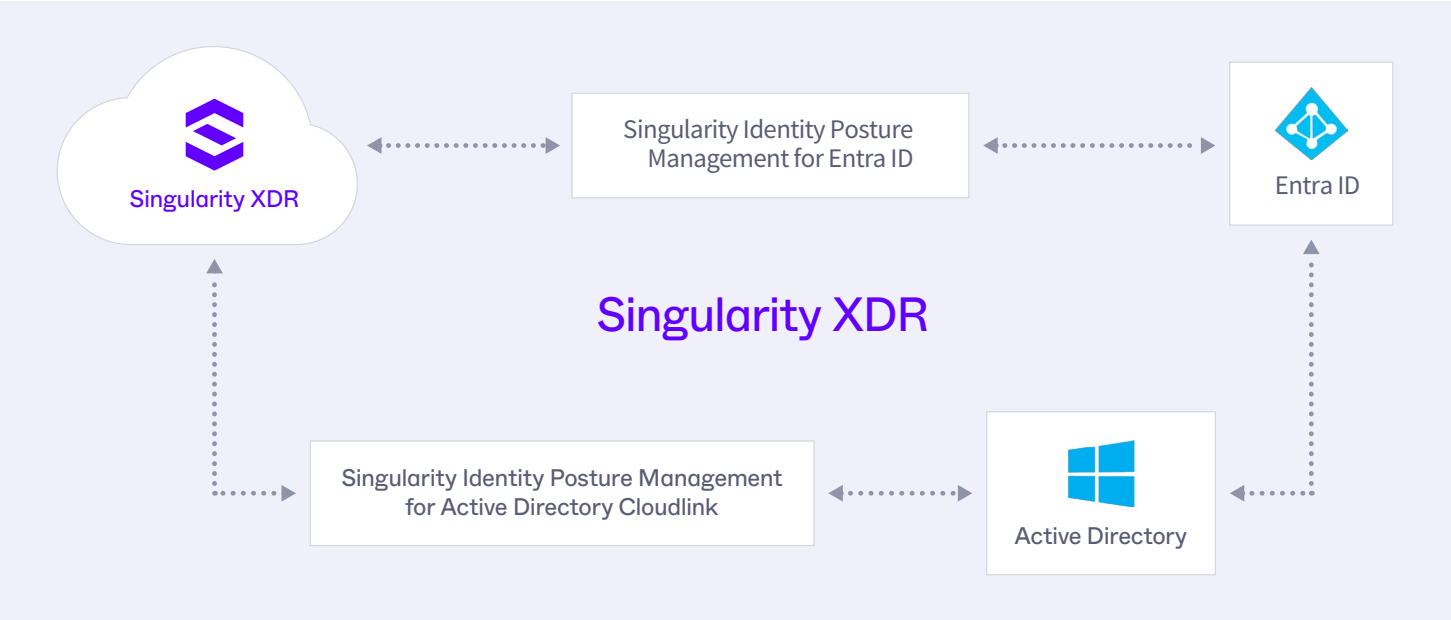
更多資訊請參考 **s1.ai/ranger-ad**

84%

的企業曾遭受帳號竊取相關的攻擊且成功被滲透。 Singularity Identity Posture Management 提供具體的改善建議措施以降低被攻擊的風險。

主要特點和優勢

+ 主動發現身分相關的風險
+ 將 AD 和 Entra ID 目前的組態和最佳實踐進行比較
+ 洞悉 AD 和 Entra ID 錯誤的安全組態設定
+ 揭露網域、裝置和使用者三個面向的曝險
+ 持續針對可疑的 AD 變更進行通知
+ 降低針對身分攻擊可能耗費的平均修復時間 (Mean Time to Recovery, MTTR)
+ 以更具能見度、更彈性的偵測方式，持續或按需求監控 AD中潛在的攻擊活動
+ 提供更細緻的選項降低曝險與回滾原設定



減少 AD 層面攻擊，提升安全性

透過分析企業環境 AD 相關組態並比較其與建議組態的差異，對於企業內的特權帳號提供建議加以限制或取消。Singularity Identity Posture Management 有助於降低可能遭受的攻擊面。依照 Singularity Identity Posture Management 提供的建議措施進行調整，從長遠角度來看，能夠明顯提升企業環境整體的安全性。

數百種即時偵測指標

網域層面	裝置層面	使用者層面
+ 較弱的安全政策	+ 惡意網域控制器	+ 驗證資訊分析
+ 驗證資訊竊取	+ 作業系統問題	+ 特權帳號
+ Kerberos 漏洞	+ AD 漏洞	+ 低活動度的帳號
		+ 共用驗證資訊

快速實現產品價值

+ 彈性部署： On-prem 及 SaaS雲端平台
+ 高支援性： On-prem AD、Entra ID 及多雲架構
+ 提供快速、有效且具體的建議措施並可立即執行
+ 完整防護 On-prem AD、Entra ID 及多雲架構環境
+ 用最少的資源達成最強防護：僅需一台端點且不須額外權限

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

+ 100% Protection. 100% Detection
+ Outstanding Analytic Coverage, 4 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR Level One · VB100 VIRUS · SE Labs Best Innovator Winner 2021 · SE Labs · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

威雲科技 WeiCloudTech
www.weicloud.com.tw