威脅防禦平台解決方案
RiskView PLATFORM

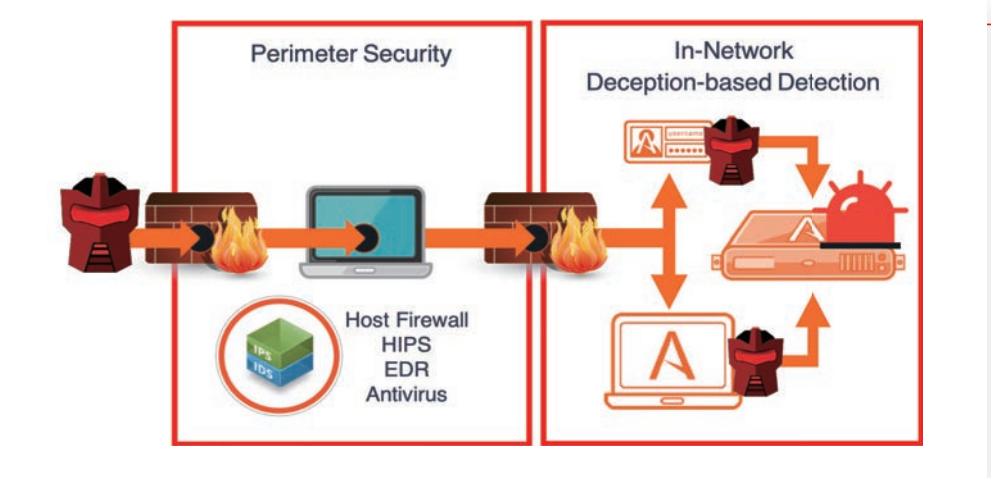
RISKVIEW

序言

隨著網路攻擊者持續尋找滲透外圍防守的方法，網路攻擊事件從不曾減緩。一旦邊界防禦被突破，安全專家需要在攻擊者造成危害之前迅速偵測並加以阻止，因此面臨極大的壓力。除了遵循法規以外，如果企業組織沒有及早通報入侵事件，則一些國家正擬議中的入侵通報法還會對企業處以巨額罰款或入獄刑期。所有產業和不同規模的企業組織都在尋求創新，使其網路安全更完善、填補偵測的縫隙、深入了解對手策略，並遵守入侵追蹤和揭露的規定。現在，企業組織正將其安全策略從被動防禦轉變為主動防禦，不僅是對攻擊的反應，而是在先發制人、早期偵測以及對威脅作出迅速回應等方面尋求平衡的投資。

創新的威脅偵測技術

使用欺敵 (Deception) 方法的威脅偵測技術提供了一個能夠平穩演進到主動式資安防禦態勢的創新。公司可以在端點上放置偵測網，或是在整個網路堆棧 (Network Stack) 中部署誘餌 (Decoy)，藉以在早期對每個威脅載體進行有效偵測。欺敵技術是利用各種高互動性的誘餌、引誘物 (Lure) 和誤導指示 (Misdirection) 來誘使攻擊者暴露自己的身份，並迅速發出告警、辨識試圖躲避安全控管的橫向移動威脅。

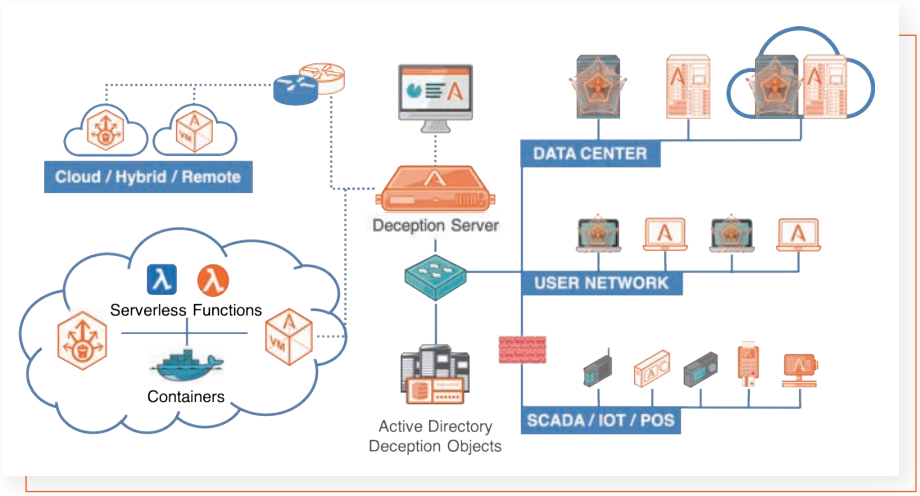


由於欺敵 (Deception)技術能在早期就發現威脅，並發佈可用於事件處理的警訊，因此正迅速成為企業資安首選的解決方案，用以主動發現外部、內部及第三方潛在威脅，並對其做出回應。重視資訊安全的企業組織都在積極採用欺敵技術，以減少員工憑證盜竊、資料洩漏、勒索軟體 (Ransomware)、加密採礦 (Crypto-mining) 及試圖中斷服務或影響公共安全有關的風險。欺敵技術的準確性和易用性是其獲得採用和廣泛部署的重要因素。

2018 年，分析師開始深刻地體認到欺敵技術在偵測進階威脅方面的效率。研究機構 Gartner 更連續三年將欺敵技術推薦為首要的策略性安全技術，並在其新冠病毒指南中推薦利用該技術來減少在家工作等網路使用迅速變遷相關的安全風險。最近亦有各種調查和研究報告也表示欺敵技術能快速有效的阻止攻擊者，為資安控管帶來正面的貢獻。

RiskView 系列解決方案

RiskView® 偵測和回應平台將整個網路化作一個大陷阱，攻擊者要是沒有達到100%完美，就有被發現的風險。該解決方案結合端點引誘物、誤導指示及高互動性的欺敵誘餌，在早期就能發現內部網路威脅，提供高效率且持續性的威脅管理，同時擁有迅速的回應事件的能力。



RiskView 平台被公認是業界最齊全的內網偵測解決方案，可為雲端、網路、端點、應用程式、資料/資料庫及 AD (Active Directory) 提供偵測羅網，並且在偵測來自幾乎所有載體的威脅都非常有效，比如進階持續性威脅 (APT)、憑證盜竊、中間人攻擊 (Man-in-the-Middle)、AD (Active Directory)、勒索軟體、Port Knocking 等等。可在所有類型的網路中進行部署，包括端點、使用者網路、伺服器、資料中心、ROBO、雲端及特殊環境，如物聯網、SCADA、POS、SWIFT、基礎架構及電信等等。

RiskView欺敵平台採主動式防禦網路威脅。該平台包括使用誘餌的 RiskView 欺敵伺服器、用於顯示收集威脅情報的 Informer 顯示板、ThreatOps® 事件回應協調劇本 (Orchestration Playbook) 和端點偵測網 (Endpoint Detection, EDN)；該 EDN 是由 ThreatStrike® 端點模塊、提升攻擊路徑能見度的 ThreatPath® 和用於 AD 防禦的 ADSecure 所組成。ThreatDirect 欺敵系統三層轉發器 (Deception Forwarder) 可支援遠端和分段的網路，管理多個平台的 RiskView 中央管理器 和用於 EDN 部署的端點偵測管理器 (Endpoint Detection Manager) 則拓展了企業欺敵羅網管理的範圍。

- RiskView 欺敵系統還包括 Informer 顯示板和 ThreatOps 事件回應協調劇本 (Incident Response Orchestration Playbooks)，此兩種版本的主要範疇如下：

Edition	VLANs	Engagement VMs	Decoys
RiskView 欺敵系統 (標準版)	受監控的有 32 個 VLAN	6 部 Engagement虛擬機器 (VM)，其中 1 部是 Windows 伺服器 VM	2192 個網路誘餌
RiskView欺敵系統 (企業版)	受監控的有 100 個 VLAN	12 部 Engagement虛擬機器 (VM)，其中 2 部是 Windows 伺服器 VM	2384 個網路誘餌

- 在端點偵測網 (End Point Detection Net, EDN) 套件中用於 Active Directory 防禦的 ADSecure 可單獨購買。在此情況下，需要一個端點偵測管理器來管理所有的端點：

元件	平台支援	定價模型
用於 Active Directory 防禦的 ADSecure	Windows	依每個端點訂購
端點偵測管理器	KVM、VMware、AWS、GCP、Azure	依每個管理器訂購