SENTRY

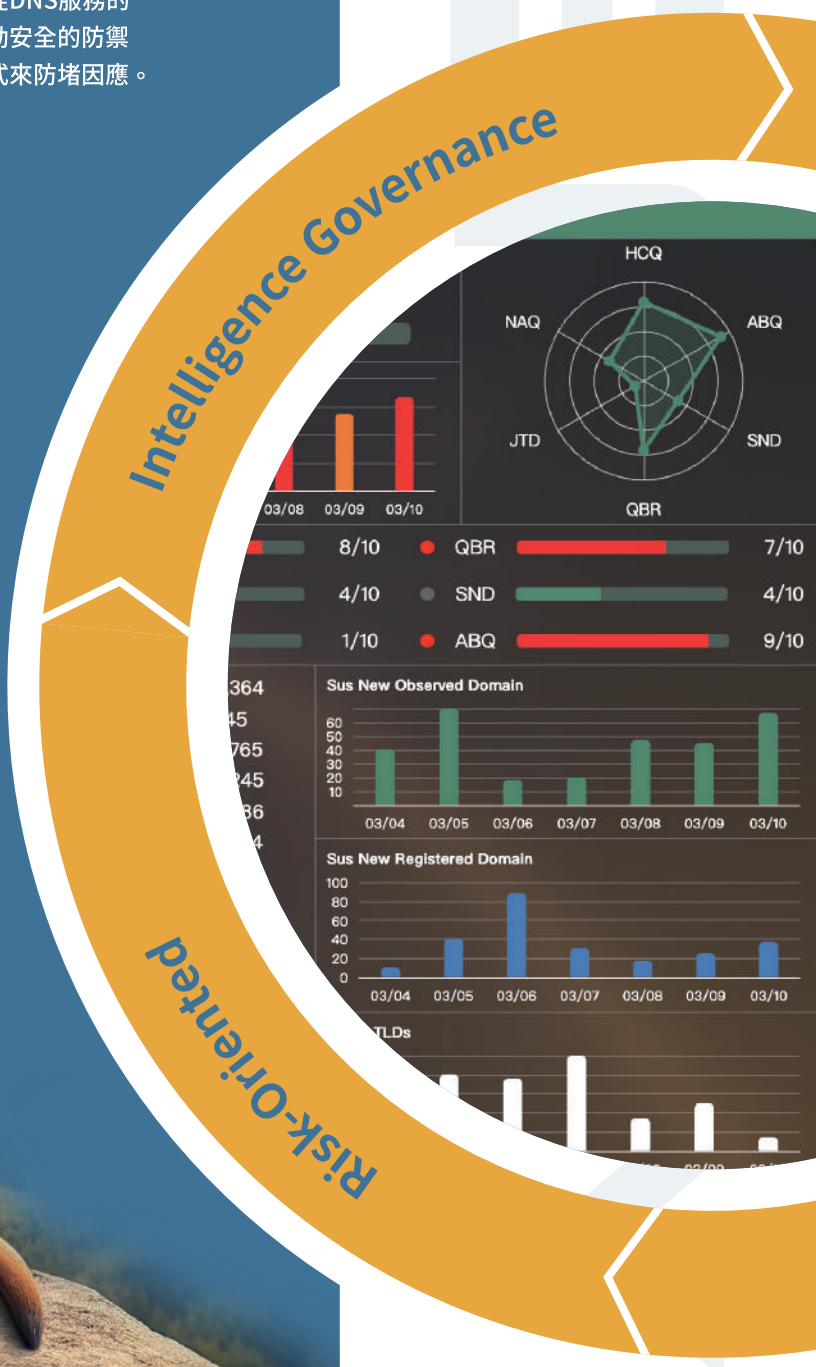
防禦未知資安威脅最佳前哨

在主流的安全閘道產品中所配置的安全特徵機制，實際上是面對過去已知攻擊手法以進行防禦，但現在和未來滿是充斥著AI變異的新攻擊手法，沒有曾經的參考數據，所以對於這些未知的資安威脅，有什麼方式能在其尚未轉化成特徵前就可以預警，甚至採取防禦作為呢?

DNS服務是企業組織運作線上數位服務所必要基礎元件，正因如此，從DNS服務的內容中可輕易透視企業內的機敏數據，而防火牆正是缺乏對於DNS活動安全的防禦能力，以致經常被駭客所利用作為資安破口，組織需要以DNS對應方式來防堵因應。

我們的SENTRY®系列軟體產品即是應用在”保護性域名服務(Protective Domain Name Service)” 領域的資安解決方案。

「合規導向」轉換「風險導向」。



 | www.urmazi.com | 16F, No. 80, Sec. 1, Zhongxiao W. Rd., Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.) | SE-DS-5050901

SENTRY® 產品承擔企業組織存取內/外網服務域名查詢解析的主控權，搭配業界首創的 ScoutEye 關聯威脅分析模組，這是專為資安團隊快速回應高風險連線所開發的進階分析工具。

ScoutEye 支持以多種風險指標就端點連線行為進行關聯性資訊分類、風險評分以及威脅內容採證等功能 ， 讓DNS活動內容清晰可視與接觸資安威脅風險如放大攻擊 、 隧道攻擊 、 殭屍網路、機敏數據竊取外洩 、公有雲 服務態勢的可預防作為大幅提升，避免因人工檢視龐大資訊時可能面臨的判斷失誤及長處理時效，對於中大型網路環境這將是最佳資安戰略工具。

在資安防禦機制 ， URMAZI 團隊中的情資分析專家為 SENTRY® 內置了 DNS 專屬威脅情資庫 ， 提供包含釣魚、探測、勒索、DGA、C2、惡意軟體等超過60種以上分類情資內容 。其連動DNS防火牆攔阻和誘捕獵搜技術，以及高靈活性的自動安全回應機制，使得具資安侵害力的連線活動在端點發出請求時即被阻斷也被明確定位 ， 系統亦支持保留 DNS連線軌跡數據及事件內容，並得以融合於 EDR / SIEM 等分析平台以擴大相關資安內容的判讀利用。

SENTRY®系列產品 能為企業組織發揮諸多的應用優勢：

- 不須異動網路架構最便捷的資安防禦方案。
- 在未形成攻擊特徵前的洞察與回應能力。
- 主控端點連線行為與威脅風險評等。
- DNS關聯數據輔助資安事件鑑識採證資訊。
- ISO-27001/27002 資安法規的合規標準。
- 提早發現機敏數據外洩跡象與來源。
- 預防及降低內網橫向攻擊行為。

URMAZI 是專注在保護性域名資安防禦應用的技術研發團隊，成立旨在為企業組織打造DNS層級的強大資安防禦生態系統，並建構能自主管理企業專屬資安威脅情報的核心資源，以及對未知風險形成威脅前即能施行相關回應作為；DNS既是所有產業網路運作的必要服務，更是企業組織端點資安防禦作為的首要關鍵位置，

URMAZI SENTRY® -
推動『風險導向、情資治理』具體作為，DNS是您永遠的資安哨兵。

SENTRY®產品功能一覽：

功能 / 型號	50	200	300	500	2000	3000
Performance(RPS)	50	200	300	500	2000	3000
DNS Firewall Feature	V	V	V	V	V	V
DNS Recursive Feature	V	V	V	V	V	V
DNS Server Feature	X	V	V	V	V	V
Inbound Multihoming/Domain	X	Opt.	Opt.	V/2	V/2	V/2
DNS Threat Intelligence	V	V	V	V	V	V
ScoutEye Feature Module	X	Opt.	V	V	V	V
Internal Reports	V	V	V	V	V	V

*. 本公司保有對上述功/效能進行修改權利而不另通知。

 | www.urmazi.com | 16F, No. 80, Sec. 1, Zhongxiao W. Rd., Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.) | SE-DS-5050901