

Ericom Shield - Remote Browser Isolation

網站檔案虛擬隔離淨化解決方案

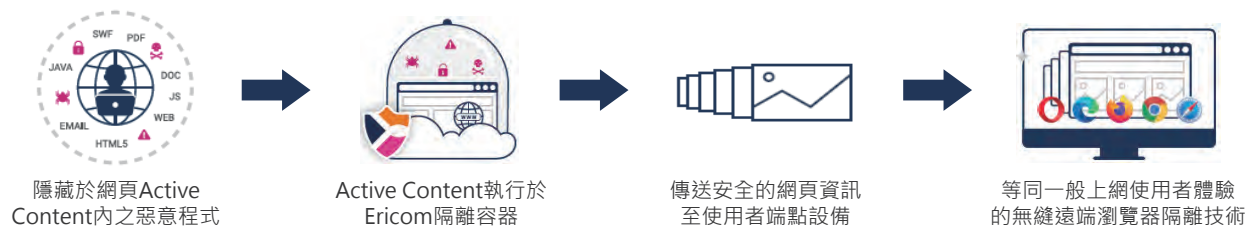


2021年第二季初統計顯示，全球已有逾18億個各類已知與未知的合法或惡意網站，且每天以百萬計的速度增加，而企業組織仍多數藉由NGFW、SWG防火牆或代理伺服器建立已知黑白網站名單，以「偵測」的模式進行防禦，唯此種控管方式已明顯呈現左支右絀，無法因應排山倒海的網站新增速度而阻礙了防禦即時性，更無法針對零時差漏洞遏止各類惡意攻擊，如：偷渡式下載攻擊、Cross Site Scripting (XSS) 跨網站指令碼、Phishing attacks (網路釣魚攻擊) 及Man-in-the-Middle (MITM) attacks中間人攻擊、Malware惡意程式碼等，因此不僅造成大量控管人力浪費，更可能因過度封鎖造成營運受阻，甚至稍有疏漏造成營運風險。

近年屢獲大獎的 Ericom Shield 網站檔案虛擬隔離淨化解決方案以 Remote Browser Isolation (RBI) 技術，從 Protect 的概念與 Airgap Isolation機制有效防範網頁惡意攻擊，落實Zero Trust 終端設備及網站瀏覽安全。Ericom Shield 採用Docker虛擬隔離容器技術將所有使用者上網行為隔離於該容器內，有效防範當使用者連結白名單網站與未知釣魚網站時可能遭受之潛在威脅。Ericom Shield亦具備檔案內容淨化與重組Content Disarm and Reconstruction (CDR)機制，凡於網頁與Webmail下載文件至端點設備之前進行掃描淨化，確保使用者設備免因下載檔案而遭受駭侵或病毒攻擊。

Ericom Shield 無需安裝末端代理程式，可支援各類瀏覽器、作業系統及裝置，其內建自訂隔離政策之功能大幅降低資訊安全管理整體成本與人力，亦具備 Multi-Tenant Architecture 的雲端架構與 3rd Party SWG/NGFW 整合架構，無需汰換既有之各式Web Gateway即可輕鬆快速導入使用，提供建置佈署極大的彈性及多樣化。

Ericom Shield – Remote Browser Isolation (RBI) 落實真正的 Airgap 網站瀏覽零信任政策



產品特色

- 使用者端點設備呈現內容為經由HTML 5串流淨化處理後的延伸圖像，任何外部網站的惡意程式碼僅能在代理虛擬瀏覽器中執行，Ericom Shield 隔離層可將時下駭客組織最常用之網頁或下載攻擊手法阻絕於使用者端點設備外，防範使用者誤陷社交工程、釣魚導致帳號密碼遭竊或遭勒索病毒。
- 每一瀏覽器工作階段或獨立頁籤皆運作於各別獨立容器內，一旦瀏覽器被關閉或逾時，容器隨即銷毀，連同任何惡意程式碼一併消除，可避免跨網站指令碼 (XSS) 攻擊。
- 無需安裝任何元件，全方位支援各式瀏覽器、使用者終端設備及作業系統。網頁內容即時串流傳輸至使用者端點設備，提供即時、互動與原生網站一致的操作體驗。
- 經由網頁、FTP或webmail下載之各式文件到達使用者端點設備之前，預先執行檔案內容淨化與重組(Content Disarm and Re-Construction, CDR)可防範因檔案暗藏惡意程式而遭受攻擊，強化資安防護網。
- 內建NetSTAR網站分類資料庫，提供定期更新之網站分類，於 Ericom Shield 管理介面依需求設定，並依網站分類或使用者群組進行更細膩之上網行為控管。

產品應用

RBI - Zero Trust Web Browsing Strategy

- 彌補「偵測式」防禦方式無法有效遏止零時差攻擊之缺點。
- 避免傳統網站黑白名單控管方式所造成之不便且過度封鎖或疏漏，反而造成企業組織營運受阻或風險。
- 適用雲端服務架構或地端佈署完善企業組織之防護機制。

Email Phishing Protection

- 隔離隱藏於釣魚信件內之未知網站惡意URL。
- 可採用 Read-Only 模式隔離瀏覽器，避免使用者無意間於網站內輸入帳號密碼。

Document-Borne Malware Protection

- 可選擇性開放使用者於瀏覽器之剪貼、Cookies、書籤、列印及檔案上傳下載之功能。預建 CDR 功能，保護端點免於因檔案下載而遭受威脅攻擊。
- 支援多種檔案格式，如Office、PDF、Image、CAD、Archive等，非支援之檔案格式則先予隔離，亦可搭配防毒軟體進行多重掃描。

技術優勢

- 最佳科技融合：以 Linux 系統平台為基礎，結合了 Docker、Kubernetes、Rancher 及 Elastic Search 等最新技術及架構。
- 可整合之CDR軟體包含：Sasa Gate Scanner、Votiro、Check Point Sand Blast Cloud、OPSWAT MetaDefender等。
- 佈署方式彈性靈活，可與既有之 Email gateway 及 Web Security Gateway、Proxy 及 Firewall 搭配並整合，佈署先後順序可依需求彈性調整網路閘道發揮更強大防禦功效。
- 可與 Ericom Shield 整合運作之 3rd Party SWG/NGFW，如：Check Point Gateway、McAfee Web Gateway、Palo Alto Firewall、Cisco Umbrella、Zscaler Cloud、Fortigate Secure Web Gateway (SWG)、Websense ForcePoint Web Security Content Gateway、Symantec Blue Coat 等。

