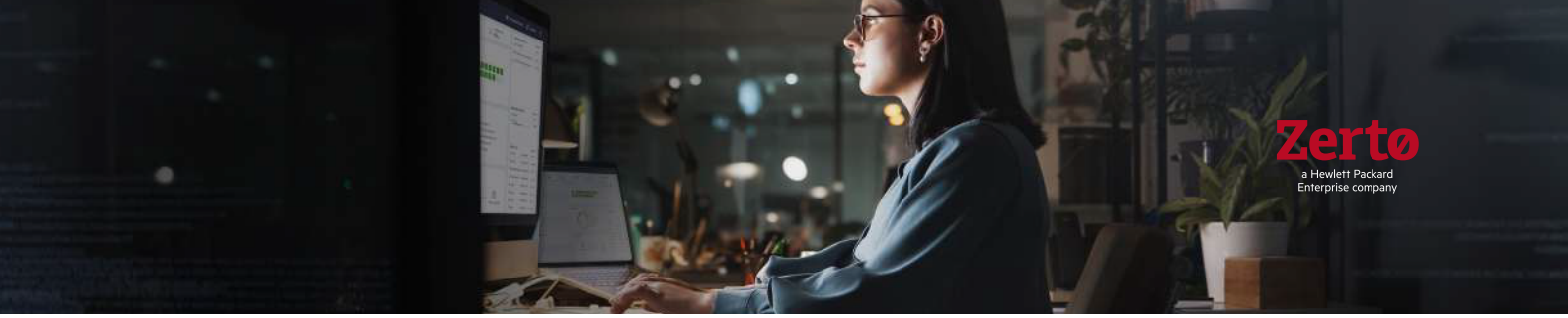

勒索軟體即時偵測

現在多數企業深知，為打擊勒索軟體，須部署多層次主動與被動式安全解決方案堆疊，又稱為縱深防禦。不過，若要在安全鏈的每一關卡盡可能提升保護，該選擇哪些解決方案？該如何整合這些解決方案呢？

即使資安防護工具偵測及阻擋攻擊的表現優異，勒索軟體仍可能突破重重防護，成功入侵。如此情境下，復原解決方案將為關鍵．然而，我們如何得知該復原哪些資料？如何得知哪些復原點資料仍完整、未加密，哪些復原點已被入侵？

定期偵測面臨的挑戰

不幸的是，現在資安領域日新月異，用來判斷復原點安全的傳統方法已經跟不上了。現行解決方案通常會掃描備份，備份資料（可能是前晚儲存的版本）與最新資料往往有著數小時落差，而惡意軟體掃描程序又須多耗費數小時。更糟的是，企業可能受限於供應商隨附的安全掃描工具（外加於產品之上或由第三方授權），還需負擔附加成本。

轉向即時偵測

慧與科技旗下公司Zerto以創新科技推出即時加密偵測。Zerto的純軟體解決方案應用演算法智慧，在發現加密異常（表示可能有勒索軟體發動攻擊）數秒內發出警示。若遭受攻擊，企業不再需要耗費數小時或數天才能確認是否需復原資料，可大幅減少資料遺失和業務中斷時間，更毋需支付贖金。

> Zerto 10 在資安威脅與日俱增的環境扮演重要角色，可有效進行資料保護與災害復原。即時勒索軟體偵測讓我們更有能力辨識並緩解勒索軟體攻擊。這讓我們更有信心能主動因應勒索軟體帶來的風險，並達成既定業務目標。
>
> - Steve Smith
> Unverferth Manufacturing 網路管理員

重要特色

Zerto 10 的專屬加密分析工具，與業界其他資料保護與復原選項大不相同：

- **即時防護，而非定期防護：**在線式、串流式偵測，持續監測所有流入企業數位環境的資料。幾乎立刻發出警示，IT或資安團隊可在攻擊當下採取行動，而不是資安犯罪事件發生後數小時或數天才有所作為。

- **不影響生產線運作：**輕量化元件（體積小、負荷低）與獨特架構使企業生產環境工作負載和效能不受影響。同樣元件亦負責資料復原所需的不間斷複製作業，強大的即時偵測技術不須部署額外資源。

- **API優先的方法：**與同業過於普遍的黑箱方法不同，Zerto利用以Swagger為基礎的的開源REST API，在企業既有資安或可視性堆疊整合加密分析。將即時偵測與所有相關警示串流至客戶自選SIEM或SOAR，包括利用Prometheus、Grafana等開源軟體的強大視覺化資料；可於 GitHub 參閱免費範例。

- **無附加成本：**Zerto的即時加密偵測功能為開箱即用，不須額外付費或訂閱，不須加購、安裝、設定或管理軟體。資安威脅過於迫切，加密偵測應為資料復原和確保勒索軟體韌性的核心，不應被付費牆所阻擋。

重要企業成效

減少資料遺失與業務中斷時間：利用及早警示系統，拒付贖金、快速復原資料，盡可能降低勒索軟體的整體影響。

將風險與成本降至最低：不須為了確保資安而採購高價資料保護解決方案，更可避免支付贖金、品牌與商譽損害、生產力損失等成本。

發揮最高營運效率：可在數秒內偵測惡意加密並在數分鐘內復原，統合資安與基礎架構團隊的工作內容。

縮短實現價值的時間：不須部署新的基礎架構、新增成本或部署多個獨立解決方案，可立即偵測異常，補強既有安全堆疊。

隨著企業持續聚焦於韌性和營運不間斷，Zerto 10的即時勒索軟體偵測能力更顯重要，不僅有效維護資安，更把資料遺失與服務中斷的風險降至最低。我們的研究顯示，勒索軟體入侵並非不知『是否』發生的事件，而是不知『何時』發生。藉由聚焦於快速偵測與復原，Zerto為企業提供重要的必備能力，協助組織辨識勒索軟體威脅，緩解其影響並從中修復。

- Christophe Bertrand
Enterprise Strategy Group (ESG)
業務總監

了解如何利用Zerto即時加密偵測、結合即時資料保護，提升因應勒索軟體的韌性。

了解更多

關於Zerto

Zerto為慧與科技旗下公司，藉由簡化本地與雲端應用的保護、復原與遷移，協助客戶維持業務不間斷。無論是私有、公有或混合式部署，Zerto可消除資訊科技現代化與使用雲端的風險和複雜性。Zerto的純軟體解決方案，操作簡易，以大規模的不間斷資料保護，提升因應勒索軟體的韌性、災害復原能力及多雲端的可動性。Zerto已贏得全球逾9,500位顧客的信任，驅動Amazon、Google、IBM、Microsoft、Oracle，及超過350位代管服務供應商旗下產品。

www.zerto.com