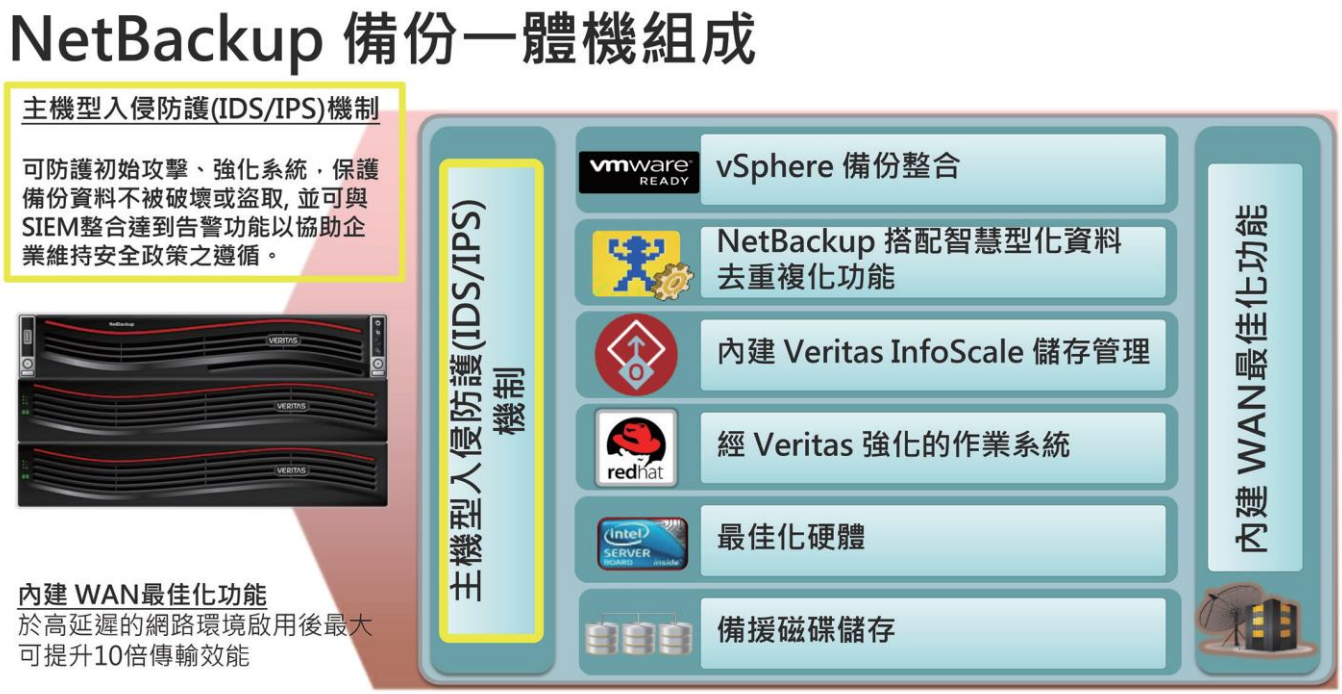
面對勒索軟體 Veritas 解決方案 – VERITAS The truth in information.

在駭客攻擊手法多變、入侵管道多元下，已無法單靠資安設備保護企業資料安全。鑑於勒索軟體潛伏期長，運用 Veritas NetBackup Appliances 打造完善備份機制，並同步使用 Information Studio 提升資料可視性，儘早察覺是否已被勒索軟體入侵，降低機密資料被駭客加密的風險。

免於備份主機及備份資料感染風險 NetBackup Appliances 安全性高

近來台灣勒索病毒事件頻傳，企業已體認到強化備份機制的重要性。只是真正發生爆發勒索病毒入侵事件後，卻也不少公司發生備份主機或備份檔案(Backup image)同步被感染的窘境，這並非將備份檔案(Backup image)離線保存就可以解決的。關鍵在於勒索軟體進入企業內部網路後，會主動透過軟體漏洞進行散播，只要備份主機沒有定時安裝修補程式，就會成為被攻擊對象。

Veritas NetBackup Appliances 內建的主機型 IDS/IPS，具備惡意程式入侵偵測與防護功能外，也會針對產品日常備份行為作系統鎖定工作，所以可避免備份主機及設備被入侵與備份檔案(Backup image)被勒索軟體加密致無法快速開始進行回存。



實現資料可視化 快速掌握被勒索軟體感染的資料位置

Veritas Information Studio，能針對運用 Veritas NBU 所備份的資料，進行多維度的分析，如檔案類型、孤立資料、非業務資料等，協助企業應對法規、安全問題，同時降低減維護壓力，以及降低購置儲存設備的成本支出等。

Information Studio 具備簡單易用的特性，分類引擎部分，針對疑似被勒索軟感染的檔案，內建 ransomware 類型，管理人員只要點選該類型，即可快速找出全球所有主機中，疑似被感染的檔案，以及存放位置等相關資訊，如資料中心、伺服器、檔案路徑等等。

關於 VERITAS TECHNOLOGIES LLC

Veritas Technologies 是全球企業級資料管理領域的領導者。我們的軟體以及解決方案助力企業保護其關鍵業務資料。在數以萬計的企業中，包括 97%的全球財富 100 強，均依靠 Veritas 來進行日常資料備份及冗災恢復，確保資料的安全性與高可用，規避資料損失風險，實現資料合規。在今天的數位化經濟時代，Veritas 所提供的技術解決方案可以幫助企業管理好最重要的數位資產，降低資料管理風險，充分發揮資料價值。欲瞭解更多詳細資訊，請參訪 www.veritas.com。

VERITAS 台灣分公司
台灣華睿泰科技股份有限公司
台北市信義區松智路1號11樓
諮詢服務熱線：+886-2-8729-2188

www.veritas.com