產品簡介

CipherTrust Transparent Encryption Ransomware Protection

勒索軟體防護

cpl.thalesgroup.com

THALES
Building a future we can all trust

自 2020 年以來勒索事件一直不斷攀升。所有資料外洩事件中，有 25%[1]來自勒索軟體。勒索軟體攻擊可以透過阻擋關鍵資料的存取，使業務營運陷入停頓，直到企業支付贖金。預測到2031[2]年，每 2 秒就有一個勒索軟體攻擊企業或個人。

使用次世代防火牆、安全郵件管理/Web 閘道等外部控制的基本安全維護，或是僅專注於縮小漏洞差距，已經不能防止勒索軟體攻擊。 居於 Fortune 500 強的企業，面臨主要的挑戰是，如何在終端設備和伺服器上，不被未經授權的程式或用戶加密攻擊，以保護業務關鍵資料。

解決方案：CipherTrust Transparent Encryption Ransomware Protection

CipherTrust Transparent Encryption Ransomware Protection (CTE-RWP)，提供非侵入式技術來保護文件/檔案目錄免受勒索軟體攻擊。 CTE-RWP 監控每個流經託管業務關鍵資料上的每個異常輸入/輸出（I/O）活動。 它允許管理員在勒索軟體控制您的終端設備/伺服器之前，針對可疑活動發出警報 / 或阻止可疑活動。

主要優勢

- **透明的資料保護。** CTE-RWP 以最少的配置，在無需修改端點/伺服器上的任何應用程式下，持續對每個檔案目錄實施勒索軟體保護。它持續監控由勒索軟體感染的流程，所引起的異常活動，並在檢測到此類活動時發出警報/阻止。
- **易於部署。** 藉助 CTE-RWP 使管理員能夠僅從勒索軟體保護開始，而無需針對每個文件/檔案目錄的基礎上，設置限制性存取控制和加密安全政策，這一功能在 CTE 授權可以使用。
- **強大的勒索軟體檢測功能。** CTE-RWP 使用以機器學習模型來動態檢測可疑文件 I/O 活動。它識別並警告或阻止終端設備 / 伺服器上的勒索軟體。另外用戶可以將已核准的應用程式新增到受信任列表中以繞過監控。

授權

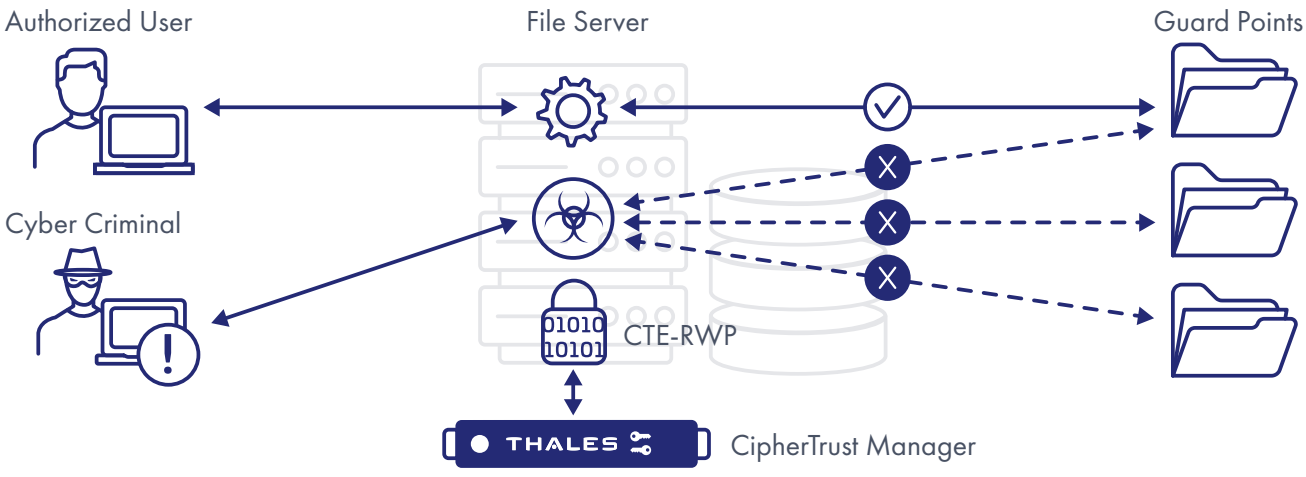
CTE-RWP 可以單獨授權。 它提供細分級別的勒索軟體檢測，用戶不需在每個終端設備 / 伺服器上的文件/檔案夾級別配置詳細的存取控制策略。 結合 CTE 授權，管理員還可以應用更細粒度的存取控制和加密。 CTE-RWP 可以單獨授權，也可以與 CTE 一起授權。

使用CipherTrust Transparent Encryption 提供額外資料保護，防止勒索軟體入侵

客戶可以透過額外 CipherTrust Transparent Encryption (CTE) 授權，對終端設備/伺服器提供最佳化的勒索軟體保護，以獲得 CTE-RWP 未提供的額外優勢。包括：

細緻化存取控制

- 定義（用戶/團隊）誰有權對業務關鍵資料所在的目錄，進行加密/解密/讀/寫
- 圍繞備份流程製定嚴格的存取控制策略，包括加密備份以防止資料洩露
- 對防禦級受信任文件（二進位檔）列表，具有存取和加密/解密受保護文件夾的權限，包括對受信任應用程式進行數位簽名檢查以確保其完整性。



CipherTrust Transparent Encryption - Ransomware Protection (CTE-RWP)

1 https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
2 https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031/#:~:text=Cybersecurity%20Ventures%20predicts%20that%20by,than%20ever%20protecting%20against%20ransomware

靜態資料加密

- 位於公司內部還是雲端的關鍵業務資料進行加密
- 使入侵者無法利用發布的加密資料來威脅獲利，使關鍵資料對入侵者來說喪失價值。
- 對防禦級受信任文件（二進位檔）列表，具有存取和加密/解密受保護文件夾的權限，包括對受信任應用程式進行數位簽章檢查，以確保其完整性。

使用 MFA 進行 CipherTrust Encryption

客戶可以為 CipherTrust Encryption (CTE) 增加多因子身份驗證 (MFA) 功能，在文件夾 / 檔案級別獲得額外的保護層。當系統管理員和特權用戶嘗試存取位於保護點後面的機敏資料時，CTE 的 MFA 會迅速提供系統管理員和特權用戶，除密碼之外還需有額外身份驗證因素。

用於 CTE 的 MFA 可適用於 Windows 平台。它支援包括 Thales 的 SafeNet Trusted Access、Okta 和 Keycloak 在內的多個身份驗證服務供應商。

關於 Thales

不論任何企業在個資保護的技術上都透過Thales保護他們的資料。在資料安全方面，企業面臨著越來越多的決定性時刻。無論是 建置加密策略，移轉到雲端還是滿足合規性要求，在邁向數位化轉型時，您可以依靠 Thales來保護您的有價資料。

關鍵時刻，關鍵技術

聯繫我們 – 有關全球辦公室地點與聯繫資訊，請參訪 cpl.thalesgroup.com/contact-us