益處

- **以絕佳防護能力降低感染勒索軟體的風險**，在各種威脅試圖生根之前立即加以封鎖。
- **即時保護**系統不受勒索軟體威脅，可讓您專心處理手上業務。
- **全方位的分層式防禦**具備無以倫比的監控能力和反應速度，可讓您輕鬆掌控 DNS 層級、網路及端點環境。
- **動態分割功能**可將勒索軟體隔離至網路一角。
- **領導業界的情資**，由思科 Talos 安全情資與研究集團提供 (Cisco Talos Security Intelligence and Research Group)。

思科勒索軟體防禦

勒索軟體的崛起

勒索軟體是一種惡意軟體或惡意程式碼，可擅自加密個人電腦存放的資訊，像是文件、相片及音樂。若要勒索軟體歸還這些檔案，使用者必須支付一筆費用（或是「贖金」），才可以解鎖並取回這些檔案。

勒索軟體近年崛起速度驚人，現已成為史上獲利最高的惡意程式碼類型，每年敲詐金額即將突破 10 億美元。

勒索軟體經常運用網頁或電子郵件作為進入電腦或網路的管道。在網站上，勒索軟體會透過受到感染的廣告（又名「惡意廣告」）傳遞惡意程式碼並藉此潛入。含有惡意廣告的網站會為正在進行瀏覽的使用者自動下載惡意程式碼，或是引導他們存取入侵程式套件。在電子郵件上，勒索軟體則會使用網路釣魚郵件或垃圾郵件作為敲門磚。使用者只要點擊網路釣魚或垃圾郵件的連結或是開啟隨附附件，勒索軟體便會下載及喚醒其命令與控制伺服器。

勒索軟體也可透過入侵程式套件掌控系統。入侵程式套件是專門打造的惡意軟體套件，可用於辨識用戶端系統上的軟體弱點，並在這些易受攻擊的系統上，上傳及執行惡意程式碼，像是勒索軟體。

不久之後，勒索病毒的鎖定對象將不再僅限於個別使用者，而是整個網路。隨著半自動化的擴散方法與日俱增，勒索軟體編寫者定會伺機入侵網路，並透過橫向移動逐步控制不同網路區域，以盡可能擴大影響範圍及提高可得款項。

提高防護效率，降低勒索軟體帶來的風險

勒索軟體可透過多種方式進入企業系統，若要降低感染勒索軟體的風險，即必須採用以產品組合為主的解決方法，而不是僅依靠單一產品。系統必須能隨時防禦勒索軟體攻擊，在勒索軟體潛入時立即發現並加以隔離，縮小其造成的損壞範圍。

思科®勒索軟體防禦採用思科研發的安全架構，防禦網橫跨網路、DNS 層級、電子郵件及端點，可為企業提供全面保護；由業界領導 Talos 威脅研究團隊提供情資支援，可迅速回應勒索軟體，保護系統不受威脅。

「我們成功掌控網頁攻擊型態的勒索軟體帶來的巨大風險，大大改善使用者的網際網路連線體驗。」

Octapharma

此解決方案包含下列元件：

- **Cisco Umbrella** 可保護公司網路的所有裝置（不論裝置連線狀態），在裝置尚未連接含有勒索軟體的惡意網站之前，便可及早封鎖 DNS 要求。
- **適用於端點的思科進階惡意軟體保護 (AMP)** 可封鎖勒索軟體的檔案，防止這些檔案在端點上開啟。
- **具有思科進階惡意軟體保護技術的思科電子郵件安全服務 (AMP)** 可封鎖垃圾郵件、網路釣魚郵件，以及惡意的電子郵件附件和網址；採用與端點相同的 AMP 技術，但部署位置在電子郵件閘道上。
- **思科 Firepower 新一代防火牆**整合了進階惡意軟體保護技術 (AMP) 和 Threat Grid 沙箱技術，可封鎖已知威脅及命令與控制回呼，同時還可提供未知惡意程式碼和威脅的動態分析。
- **透過思科網路執行的思科 ISE** 可動態分割網路區段，大幅提升伺服器和應用程式存取作業的安全性，使勒索軟體無法順利進行橫向擴散。
- **思科安全服務**可將事件回應情況即時分級，以及簡化 AMP、NGFW 及其他解決方案產品的部署流程。

後續步驟

想要讓公司員工專心處理業務？請與思科銷售代表聯絡，深入瞭解思科勒索軟體防禦的詳細資訊。

C45-737465-00 07/16