

Thales 端點到端點加密解決方案： 保護政府資料



內容

3	保護政府數據
3	為什麼需要加密
3	保護與預防
4	受到20多個國家/地區政府的信任
4	堅決的盡最大程度保護資料
4	政府客戶
5	選擇正確的加密解決方案
6	端點到端點加密解決方案
6	Thales CNSeries硬件加密器
6	Thales CV系列虛擬加密器
6	Suredrop加密文件共享
7	為什麼 Thales 加密器是獨一無二的？
7	優異的性能
7	高保證
8	獨立網路加密
8	多功能與簡易性
9	低成本高效能
9	關於 Thales

保護政府資料



中央與地方政府機關擁有大量的敏感資料，網路安全成為大眾注目與關注的焦點。

不論是公民個人資料或國家機密的保護，都需要採取整體的防護思維，一種可以全面預防和保護靜態和動態資料的解決方案。

直到現在，我們仍關注在結合物理和虛擬技術的預防技術。但是，過去十多年的教訓經驗告訴我們，資料外洩是不可避免的。

近年來，資料意外遺失的事件有所減少，但仍佔所有資料外洩或被竊取的三分之一。資料外洩的罪魁禍首是惡意的外部未經授權存取或“駭客”。在2019年發生的資料外洩事件中，有52%是駭客攻擊，其中28%涉及惡意軟體，其餘32-33%涉及社交工程技術—俗稱的網絡釣魚。

為什麼需要加密？

隨著虛擬化、資料中心和雲端計算技術的蓬勃發展，我們愈來愈倚賴在任何地方和任何時間，透過高速/高可用性的資料網路進行訊息的傳輸。

駭客攻擊、產業間諜活動甚至是網路恐怖主義形式的網絡犯罪不斷攀升。面對普遍存在的資料安全威脅，保持靜態資料和傳輸資料的完整性、安全性，對企業至關重要。

我們無法保證資料在公司內部就是絕對安全的。所有企業都依賴使用公共網路以存取和共享系統與資訊，現今企業大多數設立多個辦公室，有些距離很近，有些則相隔數千公里。

光纖電纜每天用於在私有和公有網路之間傳輸PB級的大量資料。儘管它被認為是最快、最可靠的傳輸方式，但是隨著駭客技術變得更加複雜，攻擊成本更低且更容易獲得，光纖網路也變得越來越脆弱，威脅著數據的安全性。

保護與預防

許多企業普遍存在一個誤解，認為只要有強大的防火牆就可以阻止未經授權的網路存取。不幸的是並非如此。

儘管防火牆可以檢測並降低各種滲透或阻斷服務式攻擊，但它無法防止防火牆內部或外部的物理攻擊。

加密是唯一可以確保資料在透過網路傳輸時的安全措施。此外，您的加密解決方案應該獨立於任何特定的網路架構之外，並獲得全球安全標準的認證。

受到20多個國家/地區政府的信任

Thales認證的高安全性加密模組是專業的硬體產品；致力於保護透過高速資料網路傳輸的機敏性政府訊息，而不會影響網路性能。

Thales 硬體加密模組已獲得FIPS通用標準和北大西洋公約組織等多個獨立測試機構的認證，政府部門和國防各機構均安心採用。

認證程序涵蓋權威認證機構，在自我實驗室內進行多年的嚴格測試。沒有認證的產品，就無法安裝在政府資料網路上。

除了這些認證，政府和國防部還針對Thales加密設備執行了內部的概念驗證和基準測試。任何測試下，Thales加密器都表現優異。

更重要的是，為政府和國防部門提供如雲端計算或資料中心儲存等服務的服務供應商，可以使用Thales優質保證的加密產品來滿足其政府客戶的認證要求。

獲得多重認證的Thales加密器，是保護世界上眾多高機敏性資料的重要承諾之一，也成為全球政府與國防部門的加密設備首選。

除了長期保護的資料的完整性和安全性之外，Thales加密器還為政府提供以下的保護：

- 封包竊聽
- 資料外洩及重新導向
- 輸入惡意資料
- 知識產權損失
- 侵犯隱私或身份盜用
- 失去信任或聲譽
- 財務損失或罰款
- 違反合規義務
- 盡量避免人為疏失和技術錯誤

堅決的盡最大程度保護資料

Thales加密器可提供最高的安全性，而不會影響網路效能。

相較於其他“低端”類似方案，Thales加密器不會增加網路負擔，也不會使網路鏈接暴露給不必要的漏洞。

20多個國家/地區的政府在各廣泛應用領域中使用Thales加密器，來保護機敏性資料，其中包括：

- 雲端計算
- 大數據資料收集與分析
- 資料中心備份和災難復原
- CCTV網路

政府客戶

Thales加密器保護範圍擴及政府和國防組織的網路傳輸資料。

Thales加密設備適用於需要NATO或FIPS通用標準認證的企業或機構，包括：

- 政府機關 – 執法單位、服務機構、監管機構等
- 國防軍事
- 跨政府機關和部門資料共享
- 提供給政府網路服務的電信服務供應商
- 政府日益廣泛的雲端計算和資料中心服務
- 各辦公室之間和辦公室內部的資料網路

選擇正確的加密解決方案

各種網路加密解決方案之間缺乏兼容性，當希望同時擁有保護核心IT基礎架構和虛擬化WAN(區域網路)的公司，必須更加謹慎地考量技術適用性。

選擇加密解決方案服務供應商時，必須考慮所有潛在的應用程式用途。更要記住，並非所有加密解決方案的設計都是一樣的。

根據市場領導地位的資料安全和加密分析師建議：如果您想要一個強大可靠的網路加密解決方案，並且可以長期保護您的資料（甚至超出資料的使用壽命），建議您選擇“質量高保證”解決方案。

所謂的“混合”加密設備（例如具有嵌入式加密功能的網路路由器/交換機）或使用MACSec或類似標準（不適用於WAN和MAN安全性）僅提供“低端”級別的資料保護。

相較之下，Thales CN系列網路加密解決方案已獲得全球領先的獨立測試機構的認證，適用於政府和國防的應用。它是專屬為保證網路所需的資料安全性而設計。

Thales網路加密器的高安全憑證，包括以下四個基本的高保障特點：

- 專用於網路資料加密的防篡改硬體
- 最先進的加密密鑰管理，提供高安全性的客戶端金鑰儲存功能
- 端點到端點的身份驗證加密管理
- 基於標準的加密演算法

提供即時的資料應用服務，延遲是一個大問題。將網路加密接口控制器添加到現有交換機似乎是一個可行的選擇，但與第二層專用設備相比，它將導致更高的延遲和更低的處理效能。

在某些情況下使用網路接口控制器時，意味著在整個網路路由中都需要使用同一個服務供應商，並且在每一個“傳輸路徑”處，都必須重新對資料進行解密和加密。

這種情況帶來了安全風險和重大的金鑰管理問題。而專用設備可以讓資料在整個網路路徑中保持加密狀態，與交換機供應商無關。

使用網路接口控制器時，加密設備的壽命將取決於主機網絡設備，並且在更換交換機時，還必須更換加密設備。

大多數現代基礎架構都由各網路層（通常是第2、3和4層）組成。因此，企業應盡可能選擇可以支援各層加密技術的解決方案供應商。

Thales的CV系列虛擬設備提供並行的多層加密，並支援DPDK，提供高達5Gbps性能。

Thales的虛擬設備支援所有網路拓撲架構，從P2P到Hub&Spoke到fully meshed networks，就如同使用CN系列硬體加密設備。

端點到端點加密解決方案

Thales CN系列硬體加密器

CN系列網絡加密器為核心IT和通訊網路基礎架構，提供業經認證的高保障資料保護。

所有CN系列加密器共享一個通用的加密平台，並且100%兼容且可互操作。

CN系列硬體加密器用於保護任何傳輸速度機敏資料的安全，從典型的10 Mbps到頻寬高達100 Gbps。



CN4000

它是一種小型（桌面）加密設備，用於支援10Mbps、100Mbps和1Gbps頻寬速度，如CCTV等該領域的安全性。



CN6000

適用於關鍵業務應用的機架式高速加密器 – 提供1 Gbps至10 Gbps的頻寬速度。



CN9000

具有超高頻寬、機架式加密器 – 提供高達100 Gbps的速度支援大資料傳輸。

Thales CV系列虛擬加密器

CV1000虛擬加密器為大型、虛擬化的廣域網提供強而有效的資料加密。

CV系列虛擬加密器可擴展到數千個端點，是受信任的Thales加密平台的軟體應用程式。搭配DPDK的加速技術，Thales 虛擬加密機制，可達到5 Gbps經濟高效的傳輸效能。

作為在任何x86硬體上執行的虛擬化網路功能（VNF），在FIPS兼容技術下，CV系列虛擬加密器可與Thales CN系列硬體加密器無縫協作。

Suredrop加密文件共享

SureDrop提供了普及的沙盒式應用程式的便捷文件共享，不但強化了端點到端點加密安全性，更完全掌握資料位置。

它同時提供本地端內部部署的解決方案及服務供應商的彈性託管解決方案，客戶可以依據需求靈活性的選擇運用。

SureDrop協助客戶包括政府機關和服務供應商，消除他們與不受到保護的外部用戶共享文件時的風險憂慮。

SureDrop提供了共享安全文件的新途徑。當大型公司和政府機構經常透過網路共享敏感和機密資訊時，SureDrop提供的服務可以滿足它們對高安全保障的需求。

此外，SureDrop還提供企業常用的目錄管理服務(Active Directory)的用戶身份驗證安全優勢。

為什麼Thales加密器是獨一無二的？



優異的效能

高速

在業界，Thales以高優異加密器的最佳性能表現傲視群倫

在10 Mbps、100 Mbps、1 Gbps、10 Gbps或100 Gbps速度的性能測試中，Thales加密器的性能優於競爭對手。

Thales加密器擁有極出色的加密速度，在資料負荷和延遲幾乎為零，非常適合在最嚴苛的網路環境中使用。

超低延遲

Thales高速加密器在全雙工模式下以99.99%的全線速度運行，而不會丟失封包。

延遲不受資料封包大小的影響（在10 Gbps時每單位小於2微秒），因此可以保持最佳吞吐量，並且幾乎沒有資源負荷。

重要的是，通過使用Field Programmable Gate Array（FPGA）技術，提供穩定可靠的性能。

零影響

Thales加密器的零影響不僅限於網路頻寬和延遲，它擴展到網路運營和管理。

它們也簡易適用於用戶網路。您不需要更改其他設備或重新配置網路。因此，Thales加密器成為網絡工程師的最愛。



高品質保證

深度認證

Thales CN系列加密器是同類產品中唯一經過多重認證的產品，因此受到全球政府和國防單位的信任。

多年來的嚴格測試使政府和企業客戶充滿信心。Thales CN系列加密器已通過FIPS、Common Criteria和NATO認證。

二十年來，Thales研發部門一直致力於獲得深入認證。客戶則依賴測試機構對產品進行全面且持續評估的優勢。

最佳加密金鑰管理

所有Thales產品均採用最先進的加密密鑰管理技術。客戶的加密密鑰在本地端僅由該客戶自行持有並存取，並受到高安全的存放和加密保護。

解決方案完整性

Thales加密器可提供最大的解決方案完整性；不像“低保證”解決方案，例如基於路由器的網路資料加密或所謂的“混合”加密器。

Thales 高保障加密解決方案配備專用的防篡改硬體，並提供基於標準（AES256）加密演算法的無縫、端點到端點的身份驗證加密。

獨立網路加密

許多企業利用多種資料網路層協議（第2層，第3層和第4層）來幫助交付業務應用程式和通訊服務。基於客戶需求，Thales開發內置網路獨立加密技術 (Network Independent Encryption)。

這項先進、獨立於網路層的高級加密技術，可實現基於目標策略的同時多層加密需求。

更重要的是，當受保護的資料遍布各個網路層時，例如從第2層乙太網到第3層IP網路目的地，客戶仍然可以得到高安全性及強大的端點到端點加密保護。



多功能與簡易性



加密-敏捷性

所有Thales加密器均具備“Crypto-agility”（加密敏捷性）概念，基於自定義加密和FPGA的靈活性所提供的100% 相容性和互操作性。選定的Thales加密器還支援量子密鑰分配（量子密碼）Quantum Key Distribution, QKD(Quantum Cryptography)和量子隨機數生成 (Quantum Random Number Generation,QRNG)，以確保長期資料安全。

支援所有協議

Thales CN系列加密器提供了最廣泛的功能。它們能夠以10Mbps至100 Gbps的速度運行，專為第2層營運服務供應商乙太網WAN和MAN網路而設計，並支援所有第2層(乙太網、光纖通道； SONET / SDH和LINK)協議。

支援所有拓撲

Thales CN加密器以點對點（P2P）、點對多點（P2MP）和全網狀網路拓撲運行。特別是，Thales CN9000是業界唯一支持多點到多點（MP2MP）拓撲結構的100 Gbps加密器。

自定義加密

除基於標準的AES256和128位演算法外，Thales CN加密器還支援使用客戶自定義演算法（BYOC / BYOE）。

簡易使用

便利性、簡易和網路透明性是Thales產品設計的基本要素。Thales加密器可確保易於執行、操作和管理。所有Thales加密器均具備自動零接觸密鑰管理功能。它還支援自動網路探索和連接功能。

互通性

同時支援第2層網路協議的Thales加密器可以彼此無縫地運作。所有Thales CN型號都向下相容。

本地或集中管理

可通過直觀的Thales CM7管理軟體在本地或遠程執行配置。並且經由設備簽署和分發X.509憑證以集中策略進行管理。



低成本、高效率

相容性

所有Thales CN加密器均以最高速運行，實現最高的網路性能，並提供簡單而輕鬆的管理，一次設置即可完成。

從企業投資案例中我們可以看出，就長遠觀察，購買低價低端的解決方案將會付出高昂的代價。

選擇低成本、低保證的解決方案，既無法滿足最嚴苛的業務實例和TCO要求，更無法獲得任何益處。

成本效益

Thales加密器結合了節省網絡頻寬、簡化管理和高可靠性等特性，使其成為降低總體擁有成本的理想選擇。

堅固耐用、互操作性、向下相容性，最小的安裝(minimal installation)和維護成本以及解決方案的靈活性，都有助於快速獲得投資回報。

其他成本優勢包括低功耗，最小的機架空間使用，以及機架空間/電源綜合利用率。

可靠性

正常運行高達99.999%的可用性，並符合國際安全和環保標準要求。Thales所有電信級機架加密器都可以熱插拔，例如風扇、電源。因此，進一步提高了網路傳輸資料加密操作的可用性。

與混合加密器和其他低端解決方案不同，Thales加密器不會中斷網絡正常運作時間。

靈活性

Thales加密器採用FPGA技術，實現最大的操作靈活性。除了滿足客戶不同的特定需求，更提供優化的高速資料加密解決方案。

這種靈活性可隨著客戶需求的轉變立即提供升級支援，保護您在產品技術上的投資，保障企業不中斷運作。

關於Thales

重視個人機密隱私的公司，將 Thales 解決方案作為保護資料安全的首選。在資料安全方面，企業面臨越來越多的關鍵時刻。無論是建構加密策略、轉移到雲端還是滿足合規性要求，您都可以依賴 Thales實現數位化轉型。

決定性技術，決定性時刻。



聯繫我們

有關所有辦公地點和聯繫資訊，請參訪

cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <

