報告摘要：TLS 1.3在企業中的普及狀況

不斷成長的加密應用擴展成為新標準

企業管理協會® (EMA™) 研究
撰文：Paula Musich
2019年1月

贊助公司：

ixia
A Keysight Business

EMA™
IT 和資料管理
研究 | 產業分析顧問

目錄

前言

TLS 1.3規範在其1.2前版成為IETF標準10年後，於2018年8月發表。新標準降低延遲，提高端點到端點通訊的隱私性，但這也讓企業付出了代價。這是因為它將現有的靜態RSA金鑰交換替換為Diffie Helman Ephemeral (DHE) 完美前向加密(PFS)交換，此要求監控解決方案可以存取每個對話的臨時金鑰，而不是每個伺服器的靜態金鑰。儘管在TLS 1.2中存在完美前向加密，但它是可選擇的； 而在TLS 1.3規範中則為必要。這讓各企業更難被動地監控流量，以檢查惡意軟體、資料洩露和惡意活動，以及排查網路可用性或校能問題。串接即時攔截仍然是可能的，但是它增加延遲，以至於在大多數網路中變得不可行。同時，TLS 1.3規範要求對憑證本身進行加密，使得企業更難收集關鍵中繼資料。考慮到分析產品能夠存取相關工作階段金鑰，具可對經解密的連外網路流量進行分析，但在所有企業中，特別是在中小型企業中，使用比即時串接解密更為有限。

考慮到這些變化以及為了繼續監控和排除網路故障進行調整的必要性，企業資料中心聯盟等產業組織參與TLS 1.3規範開發的後期階段，試圖在保留現有管理作法的同時，減少延遲並提高隱私效益。儘管沒有成功，但該聯盟繼續尋找補丁或變通辦法。同時各企業正開始普遍採用TLS 1.3規範。本研究分為兩個部分闡述：

1. IT從業人員對於TLS 1.3規範、其採用計畫、處理可視性的方法、預期成本等問題的關注。
2. 企業內部網路整體加密、作法、關注點和發展趨勢。

首要安全問題：應用安全和資料中心的可視性

對於因為可視性下降而導致的四個潛在問題按1級到4級進行排名，其中1級代表最關切的問題，4級代表最不重要的問題，57%的受訪者表示，無法監控應用程式的安全性是他們最關心的問題。

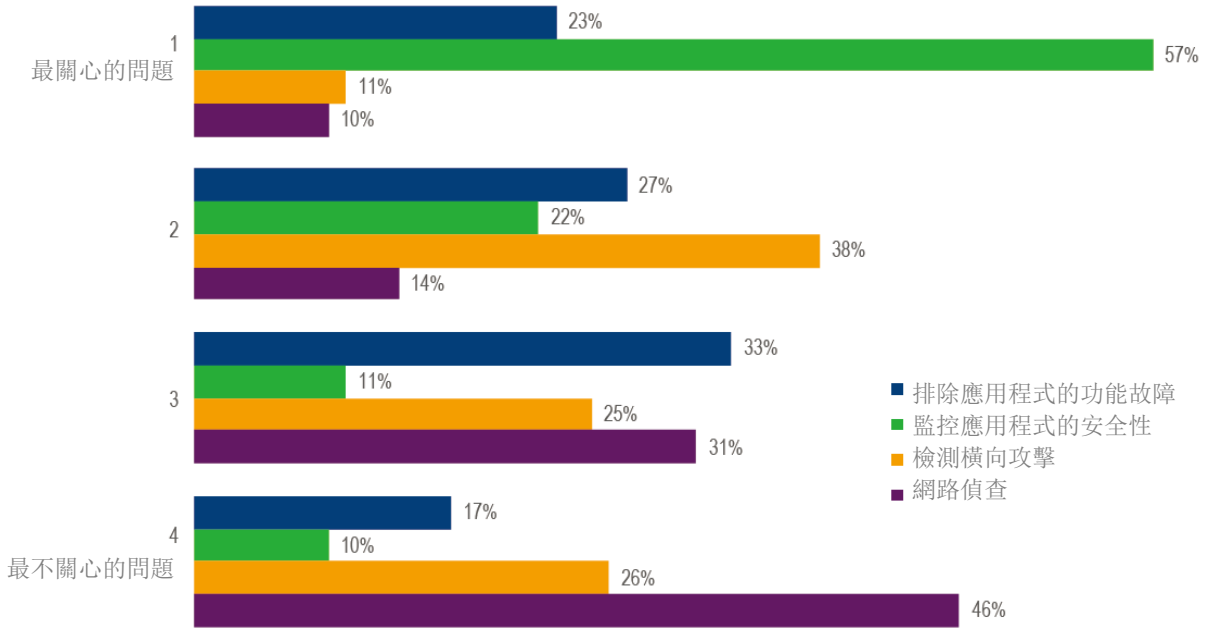

圖1：缺乏對應用安全性的可視性是最大的問題

正如房地產一樣，這一切考量都與位置有關。當綜合考慮具體位置和失去的可視性時，毫不意外，喪失對資料中心的可視性成為最大的關切點，緊隨其後的則是企業網路缺乏可視性。當要求受訪者按1-8個級別對最擔心失去可視性的八個不同資料地點進行排序時，其中1表示最擔心，8表示最不擔心，27%的受訪者表示他們最擔心資料中心失去可視性，而24%的受訪者最擔心失去對核心網路的可視性。令人驚訝的是，隨著雲端服務的迅速採用，受訪者似乎最不關心在私有雲和公有雲上失去對橫向流量的可視性。

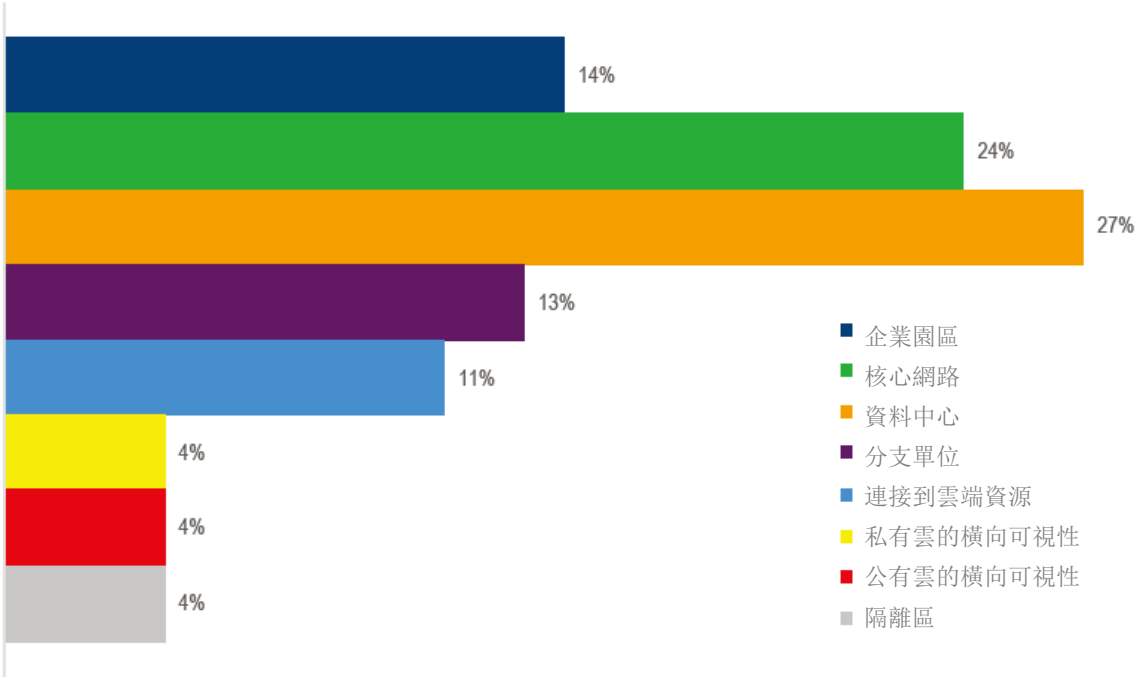

圖2：根據資料所處位置對失去可視性的擔憂

實施TLS 1.3的營運問題

在企業內部實施TLS 1.3規範引發多個營運問題，不僅涉及IT運營和安全，還包括內部網路應用程式和網路服務開發。隨著各大網路服務器和瀏覽器供應商紛紛採用此規範，促使著企業也開始了啟用計畫中，受訪者們均對開發網路應用需要更多的成本和時間表示擔憂。事實上，當被問及各大網路服務器和瀏覽器供應商採用了TLS 1.3規範，影響網路應用和服務開發的三個主要問題時， 21%的受訪者表示最關心開發生命週期的時間和成本是否會因此而增加；另外21%的受訪者表示他們最關心開發培訓時間和成本增加；又有21%的受訪者表示，更多的運營生命週期時間和成本是他們關心的三大問題之一。

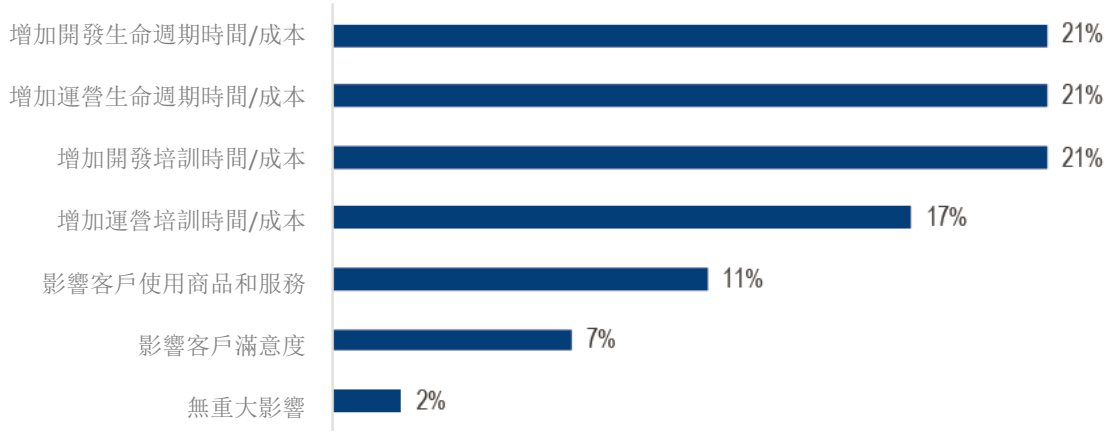

圖3：網路服務器供應商採用TLS 1.3規範帶來的三大內部網路應用開發問題

在促進TLS 1.3規範的實施過程中，受訪者表示，他們並不期待在安全架構和改變TLS 1.3標準方面的工作會一帆風順。95%的受訪者表示，為了適應TLS 1.3及其完美前向加密(PFS)的強制要求，這些安全架構必須經過調整。然而，他們對於這種改變的程度方面存在著分歧。一半的受訪者認為只需做輕微的改動，而45%的受訪者則認為需要進行明顯的更改。值得注意的是，在超大型企業中，大多數受訪者（62%）認為所需的更改會很小。

TLS 1.3將日益普及

然而，這些擔憂並沒有讓各企業機構停止在其內部繼續施行TLS 1.3規範。73%的受訪者要麼已經開始為網內連接啟用TLS 1.3，要麼計畫在未來六個月內為這些網內連接啟用TLS 1.3。與此同時，74%的受訪者已經開始為內部連接啟用TLS 1.3，或者計畫在未來六個月內為內部流量啟用TLS 1.3。只有2%的受訪者表示，他們的組織不打算啟用TLS 1.3。這令人感到驚訝，但也有客觀原因。該規範於2018年8月才發佈，僅比此調查早幾個月。同時，一般來說，當面臨重大變化時，IT組織（尤其是大型IT商店）往往更緩慢、更謹慎地適應這些變化。或許IP V6採用期較長就是最好的例子。受訪者提出了相反的觀點，表明超大型企業往往率先採用該規範。59%的超大型企業聲稱，已經為網內連接開始啟用TLS 1.3，55%的超大型企業指出已在為內部連接啟用TLS 1.3；而緊隨其後已經為網內流量和內部流量啟用該規範的企業分別占比40%和45%。同樣值得注意的是，40%的受訪者正在為內部流量實施TLS 1.3，41%的受訪者預計將在6個月內為網內連接啟用TLS1.3。

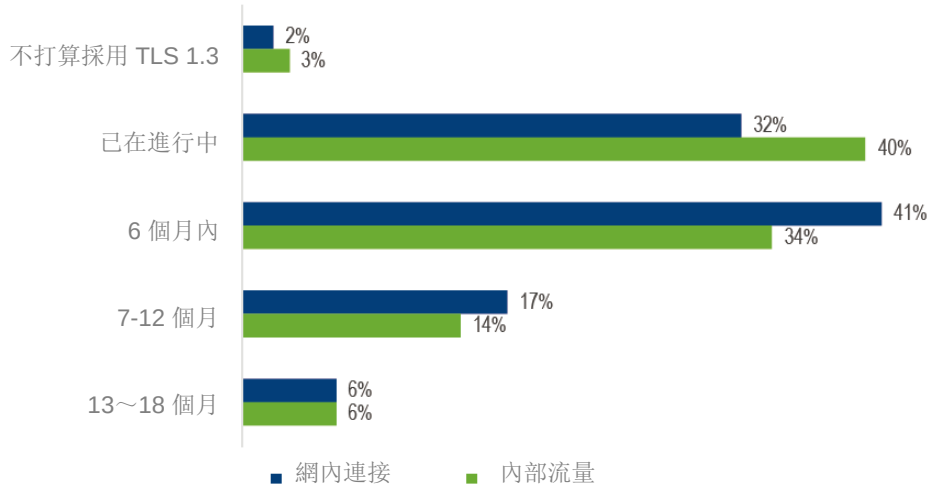

圖4：針對網內和內部連接啟動TLS 1.3的時間表

快速採用背後的驅動因素

新的TLS 1.3規範之所以能夠如此快地被採用，或許是因為包括蘋果（Apple）、CloudFlare、谷歌（Google）和微軟（Microsoft）在內的主要網路服務、網路服務器和瀏覽器供應商提前採用了TLS 1.3。當被問到這種提前採用對受訪者的TLS1.3啟用計畫有何影響時，他們（絕大多數）表示，這迫使他們加快其計畫實施。63%的受訪者表示，他們感到被迫加快實施計畫，只有33%的受訪者表示沒有影響。值得注意的是，儘管大多數中小企業和超大型企業表示，由於瀏覽器供應商提前採用該規範，他們被迫加快啟用計畫，但是超大型企業小組的受訪者認為啟用TLS 1.3的壓力很小（52%），並且他們中有許多人表示根本沒有影響。然而，由於該小組一直處於採用曲線之中，意味著越來越多的超大型企業一直計畫採用該規範。同時似乎即使認為自己對TLS 1.3瞭若指掌，並且積極升級其現有系統以便與雲端服務和網路服務保持相容者，也可能沒有如其想像的瞭解情況。儘管TLS 1.3影響安全性、網路和應用程式效能監控等方面，但對日常使用和網路作業的影響應該微乎其微。因此，對工作的最大需求不是來自於影響業務，而是來自對流量可視性的維護能力，以便進行安全和作業故障排除。

圖5：主要瀏覽器供應商提前採用對企業TLS 1.3啟用計畫的影響

針對內部流量採用更先進的加密標準可能還有其他業務驅動因素。例如，企業已經認識到其網路受到破壞，並且認為新傳輸加密標準能進一步保護更敏感和更有價值的資料。考量受訪者在啟用TLS 1.3時獲得的好處，此一解釋在研究結果中得到了證實。每個受訪者都有一份列表，上面列明啟用TLS 1.3的七個潛在動機，然後受訪者根據每個動機與其組織的相關性，從非常重要到完全不重要，對每個動機進行五分評等。所有受訪者都認為最重要的優勢是提高了資料安全性（73%），改善了端點到端點安全的隱私性（67%）。在受訪者看來，在更短的連線溝通時間內減少延遲僅次於TLS 1.3的安全優勢，只有44%的受訪者表示這是一個非常重要的採用驅動因素。

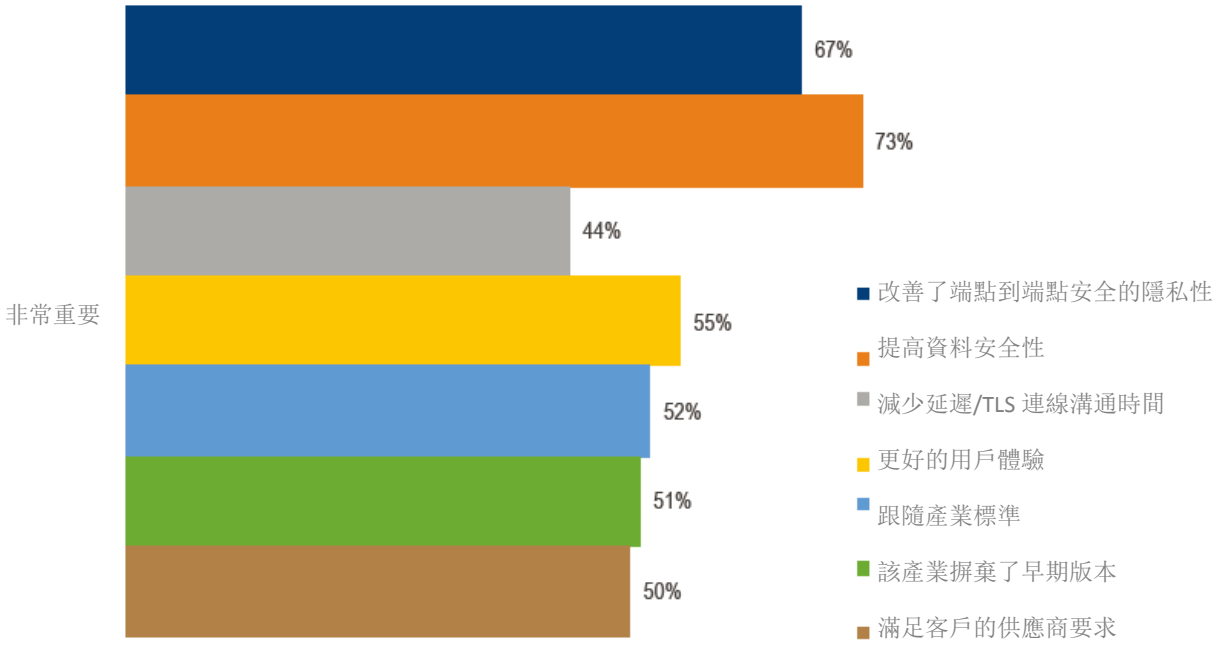

圖6：啟用TLS 1.3的主要動機

近30%的大型企業仍然認為，架構變更需要100多萬美元的投資。當然，對於IT預算每年超過1億美元的企業來說，不過是九牛一毛。從年度IT預算的角度來看，報告表示IT預算為5千萬~1億美元的54%受訪者預估安全架構變更的成本將介於25.1萬~50萬美元之間。報告表示年度IT預算為1千萬~2.5千萬美元的51%受訪者預估調整組織安全架構的成本將介於10.1萬美元~25萬美元之間。另一方面，雖然中小企業受訪者的樣本數很小，但代表中小企業的受訪者中沒有一人預計成本低於5萬美元。

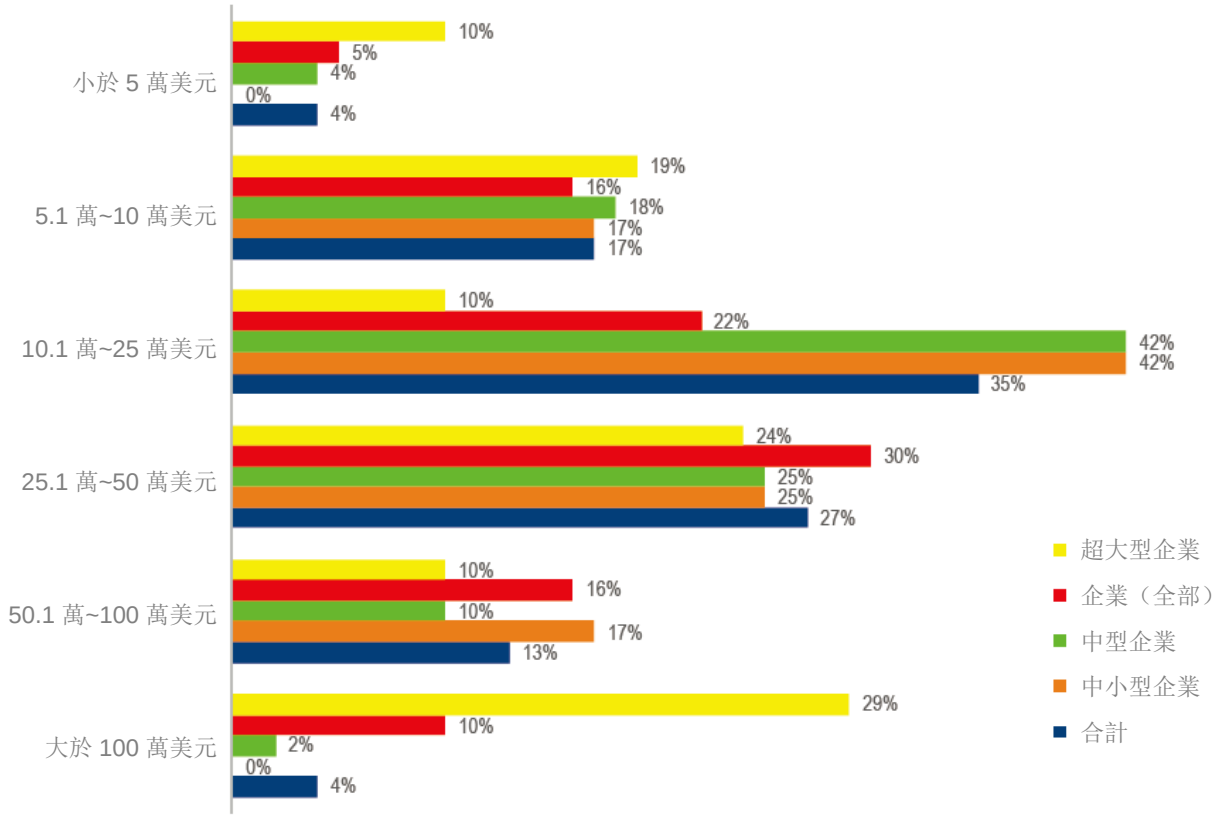

圖7：按公司規模將安全架構調整為TLS 1.3的預估成本

啟用TLS 1.3的策略

當處理由TLS 1.3引起的可視性問題時，受訪者似乎在反復考慮幾種策略。整體來說，60%的受訪者希望盡可能延長在TLS早期版本上沿用現有防火牆，而中型企業的大多數受訪者表示這也是他們的首要策略。大型或超大型企業的受訪者對於首選方案出現了分歧，即盡可能延長在TLS早期版本上維護現有防火牆，還是在現有的串接安全設備上啟用解密和再加密，同時希望不會增加太多的延遲、複雜性或安全性漏洞。TLS 1.3 PFS的強制要求讓大型企業中的IT安全和營運作業人員進退兩難。前一種選擇意味著推動啟用TLS 1.3的計畫與盡可能長期在TLS早期版本上維護現有防火牆之間存在明顯的脫節，而後一種選擇類似於孤注一擲——代表著某種程度的絕望或樂觀。此外，半數受訪者報告表示將尋找透過現有安全控制進行解密和檢查而不會造成重大功能損失的串接替代方案，這也是中型企業的第二個明確選擇。只有代表中小企業的受訪者表示，他們的首選方案是用代理防火牆替換目前全狀態檢測防火牆，69%的受訪者表示會採用此選項。儘管如此，應注意中小企業受訪者的樣本數很小。

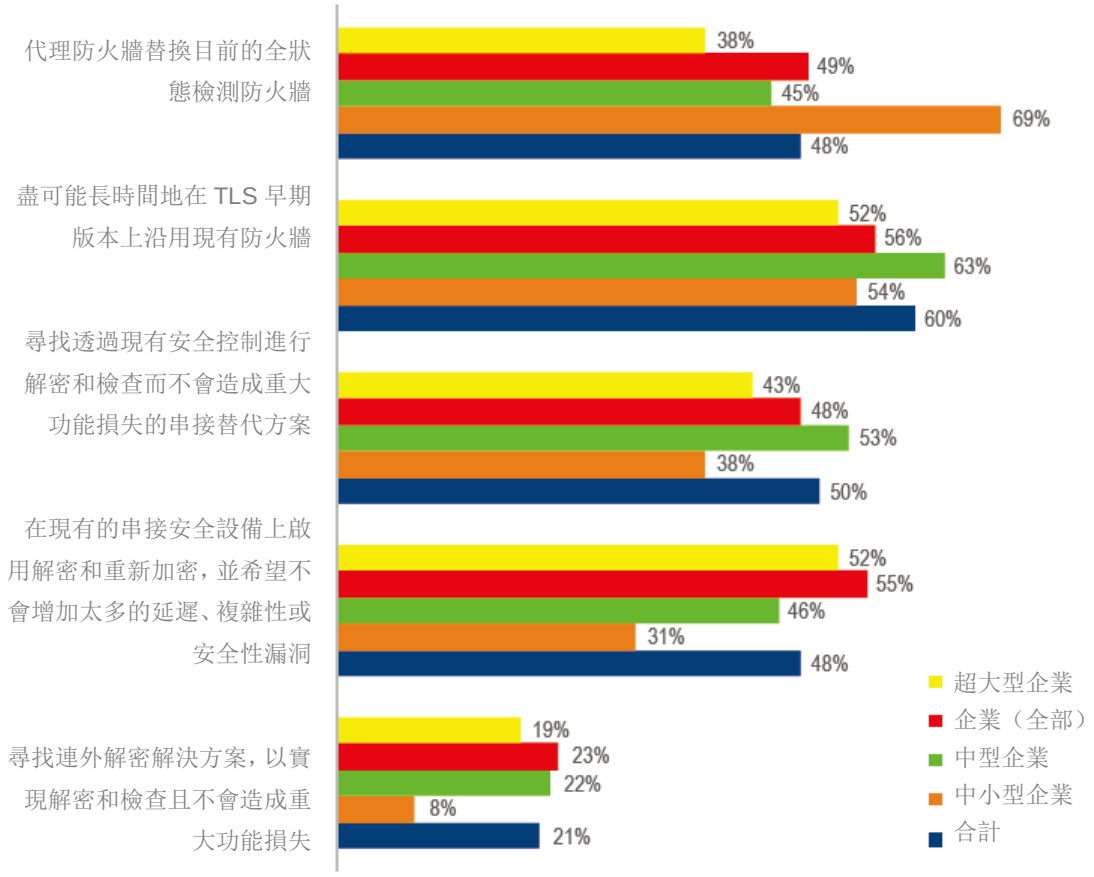

圖8：解決TLS 1.3可視性問題的考慮選項

從哪裡開始？

當企業處理與啟用TLS 1.3相關的架構問題時，他們不太可能同時在所有應用和網路流量中全權授權啟用TLS1.3。企業可以採用多種方法在整個企業網路中啟用TLS 1.3。調查顯示，不同規模的組織可能採取不同的方法。例如，超過半數代表大型企業的受訪者表示，他們打算先為關鍵流量啟用TLS 1.3，然後方便時為其他流量啟用。相反地，46%代表中小企業的受訪者表示，其所有組織打算同時為所有流量啟用TLS 1.3。對於中型企業而言，首選方案似乎是只為關鍵流量啟用TLS 1.3，40%的受訪者認為這是他們的首選方案。這些差異顯示網路複雜程度不同、安全營運複雜性以及可用人力對於各類組織是否打算啟用TLS 1.3都發揮作用。令人疑惑的是儘管美國和歐洲隱私法規制定趨於嚴格，但對許多受訪者來說，合規性並不是考慮因素。整體只有7%的受訪者表示，其組織只會在符合合規性要求的情況下啟用TLS 1.3。

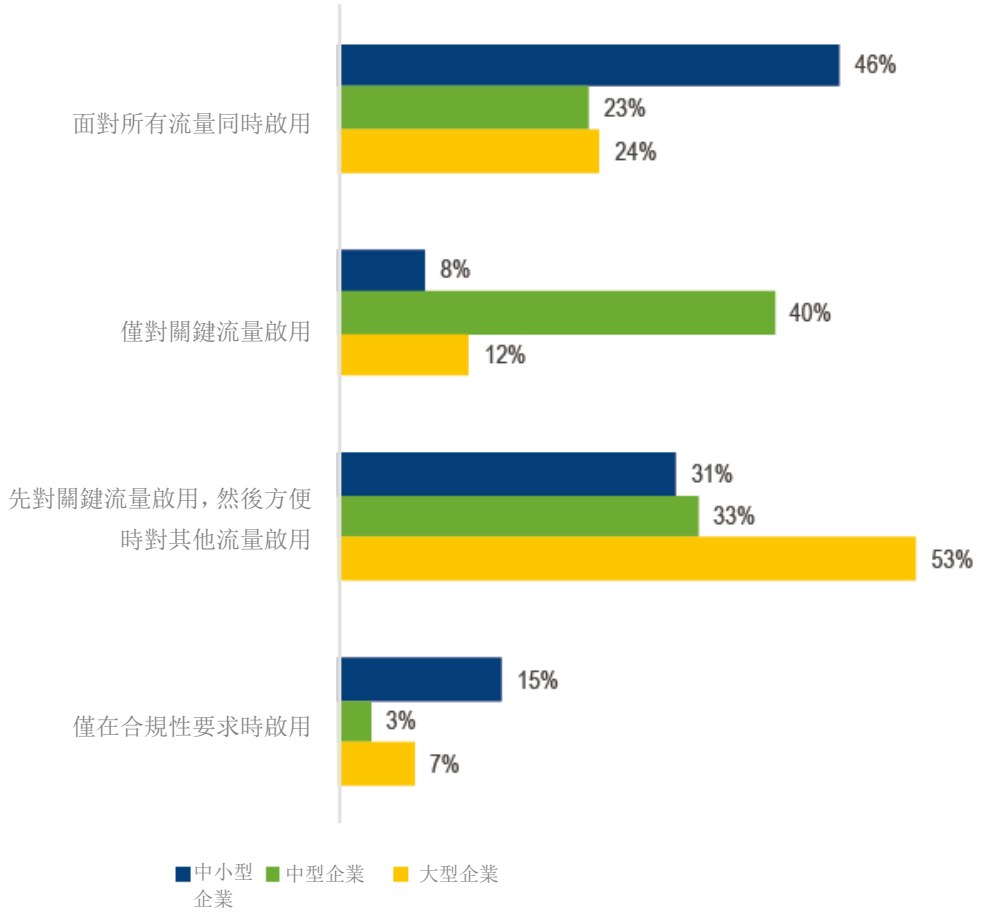

圖9：不同規模的組織打算如何實現TLS 1.3啟用

解密政策和作法

IT部門一般擁有多種解密網路流量的方法，以排查功能和可用性問題，以及監控惡意軟體和潛在惡意行為。這些方法通常分為兩類：串接或中間人解密和再加密，以及被動或連外解密和再加密。串接選項通常會損失效能，因此在企業網路中較少。使用被動或連外部署在大型企業中相對常見，尤其是那些受合規性強制要求管理的企業。EMA詢問了該受訪者們使用五種常用方法中的哪一種，以及其是否進行解密。在這五種方法中，各類別的各規模組織均先選擇網路代理進行解密，其次是使用串接安全設備，然而中小型企業和超大型企業都會首先選擇串接安全設備。不太受歡迎的選項包括使用連外安全設備、串接負載等化器和串接專用解密設備進行解密。奇怪的是12%的超大型企業受訪者表示，其所在組織一般不會解密企業中的任何流量——這在各種規模的組織中占比最高。

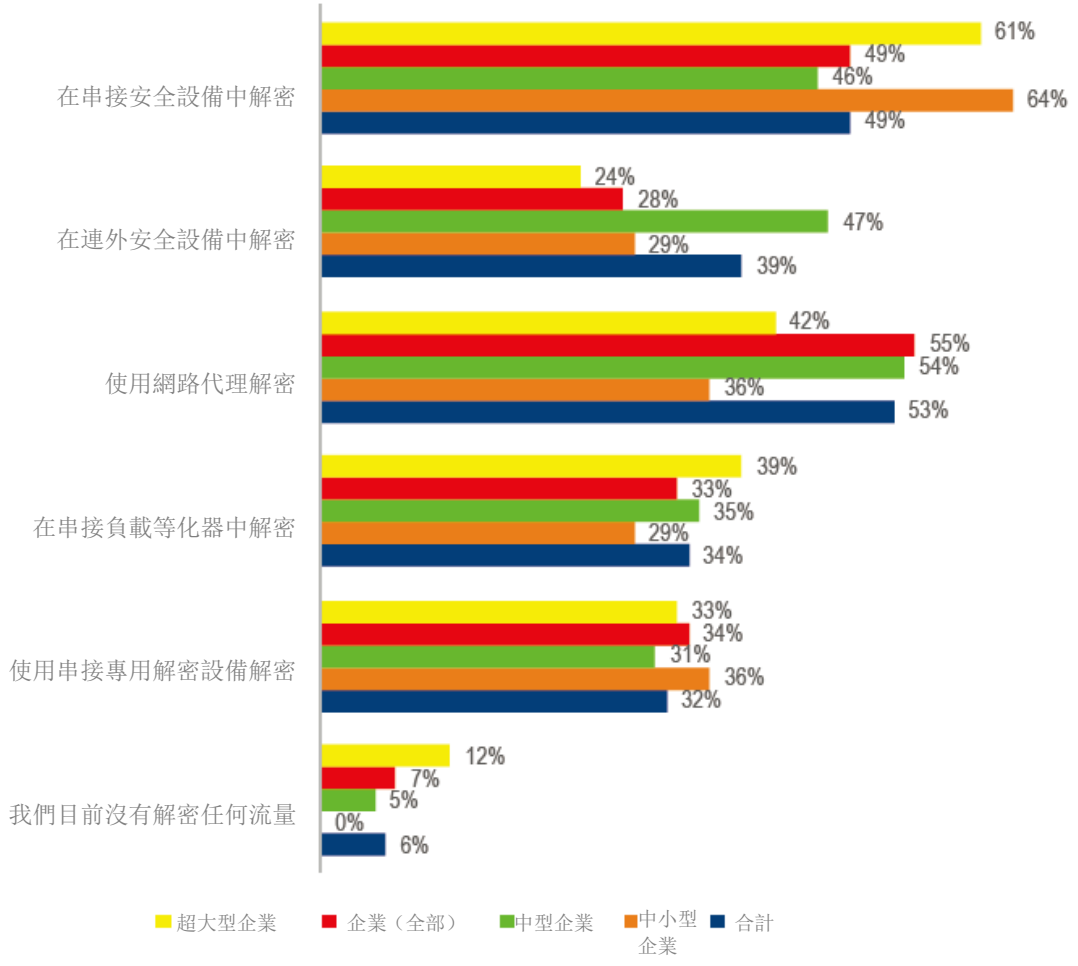

圖10：目前採用的解密方法

結論

加密在各種規模的企業網路中應用非常普遍，而且成長迅速。它不只限於資料中心，而且正迅速擴展到多個地點和應用程式。儘管人們對加密檔中隱藏的惡意活動或惡意軟體的檢測能力存在疑慮，但這些似乎並沒有減緩網路加密的發展。

同時安全從業人員似乎已準備好接受最新的TLS 1.3標準，儘管其對於現有安全架構的影響以及對網路問題排查帶來的營運限制仍令人擔憂。安全從業人員清楚地意識到新標準將需更改現有的安全架構，並預計要投入額外資金來啟用TLS 1.3。

當他們準備啟用TLS 1.3時，本次調查的受訪者們在實施計畫中提出警告。受訪者們提出的一些新標準實施方法似乎更異想天開，而不是精心規劃的部署。一些受訪者所在的組織可能會發現必須務實，提出啟用TLS 1.3的B計畫，同時不會失去可視性、導致難以承受的效能瓶頸以及大大增加的營運開銷。

無論是因為各大網路服務器和瀏覽器供應商已經先行啟用TLS 1.3，而別無選擇只能啟用TLS 1.3，還是因為本產業已設立了新標準，必須跟上產業的發展步伐——這一點尚不明確。顯而易見的是，安全從業人員認為新標準為各自的組織提供更大的隱私和端點到端點資料安全，而漫長等待期已經結束。

總公司：

1995 North 57th Court, Suite 120 Boulder, CO 80301

電話：+1 303.543.9500

傳真：+1 303.543.7687

www.enterprisemanagement.com

3802-Keysight.012919