TLP：CLEAR

零信任成熟度模型

2023 年 4 月 2.0 版
網路安全與基礎設施安全局
網路安全司

修訂記錄

版本號碼隨著文件的修改更新。本文件根據需要進行更新，以反映現代安全實踐和技術。
表 1 列出文件修訂歷史記錄。

表 1，修訂歷史

版本	日期	修訂說明	受影響部分
1.0	2021/8	初始發行	全部
2.0	2023/3	對 RFC 回饋的修訂	全部

一、簡介

網路安全和基礎設施安全局 (CISA) 負責領導國家級別之理解、管理和降低網路安全風險的實作，並支援聯邦行政事務政部門機構發展與實施網路安全計畫和能力。CISA 的零信任成熟度模型 (ZTMM) 提供了一種持續性的現代化作法，以適應快速變化的環境及新技術發展。美國政府頒布之聯邦行政命令「改善國家網路安全」(EO 14028)，要求各聯邦機構制定各自的零信任架構 (ZTA) 實施計劃，而 ZTMM 可作為設計和實施零信任遷移計劃的眾多參考其中之一。雖然 ZTMM 是根據 EO 14028 的要求專門為聯邦機構量身訂製的模型，但所有非官方組織也可考慮採用本方法實作自身機構的零信任架構。

二、背景

近期發生的一些網路資訊安全事件突顯了聯邦政府及大型機構在保護網路安全方面所面臨的重大挑戰：傳統的方法已經不足以保護國家或機構防禦來自網路的威脅。在領導國家理解、管理和減少網路風險的過程中，CISA 必須採用夠清楚地、容易操作、能夠控制已知風險的方法來保護聯邦行政部門。面對新興的網路安全威脅，網路防禦措施需要提高應變速度和靈活性，以便快速地提高駭客攻擊成本，強化自身資訊韌性，並在遭受攻擊時能夠快速恢復到全面營運狀態。

CISA 的網路安全使命是領導國家推動及實現有效的國家網路防禦、強化國家關鍵職能彈性並推動強大的技術生態系統來保護網路空間。CISA 必須在維護聯邦民政暨行政部門機構的網路態勢感知、保護.gov 網域、協助各組織及機構(包括聯邦民政機構、關鍵基礎設施所有者和供應商以及各行業夥伴)管理重大網路安全事件等方面發揮關鍵作用。雖然 CISA 已經具備抵禦已知或可疑網路威脅的能力，但不斷變化的威脅和新興技術帶來了持續的全新挑戰。

EO 14028 代表聯邦政府網路安全現代化的新承諾及重點方向。除了政策要求之外，該行政命令將零信任視為聯邦政府期望的安全模式，並呼籲 FCEB 機構制定相關計劃以實施零信任架構。通常典型的計劃進行方式為評估機構的目前網路安全狀態，然後規劃如何實施零信任。作為聯邦政府的網路安全領導機構，CISA ZTMM 將協助機構制定相應的零信任戰略、持續演進計劃，並提出各種 CISA 服務以支持跨機構的零信任解決方案。

美國白宮辦公室(OMB)備忘錄 M-22-09 (推動美國政府邁向零信任網路安全原則)，表明了聯邦機構需要採取具體行動，按照 ZTMM 提出的零信任支柱制定聯邦推動零信任戰略，並要求各機構於 2024 財政年度結束前實現網路安全目標，以加強 FCEB 網路安全防禦。為了與 M-22-09 保持一致，CISA 對 ZTMM 進行了修訂，各 FCEB 機構在制定和實施零信任策略時，應該同時審閱本文件。

三、什麼是零信任

美國國家標準與技術研究院 (NIST) 特別出版物 (SP) 800-207 提供了零信任的操作型定義：

> **零信任 (Zero Trust) 假定**網路環境並不安全，隨時都有潛伏的破壞者，資訊系統和服務在運作時，為了讓每一個決定存取請求是否放行的不確定性最小化，於是以最小授權原則去執行任務的一系列概念與想法。
>
> **零信任架構 (Zero Trust Architecture)** 是一種企業網路安全的規劃模式，在其中引入了零信任的概念，在實作面則包含邏輯元件關聯性、業務流程規劃與資源存取政策。

SP 800-207 強調零信任的目標是「**防止未經授權對資源和服務的存取，同時使實施存取控制盡可能細緻化**」。國家安全電信諮詢委員會 (NSTAC) 將零信任描述為「一種網路安全策略，其前提是任何使用者或資產都不應被預設隱式信任」。它假定已經發生或即將發生違規行為，因此不應該透過在企業邊境進行的單一驗證來授予使用者存取敏感資訊的權限。相反地，每一個連線、設備、應用程式和交易都必須不斷進行驗證。零信任代表了從位置為中心的模型轉變到以細分、上下游和資料為中心的做法，並為隨著時間變化的使用者、系統、應用程式、資料和資產之間提供細粒度更高的安全控制。因此，運行 ZTA 是一件非常具有挑戰性的工作，這種轉變提供了安全策略的開發、實施、執行和演進所需的可見性。從根本上而言，為了實施零信任，組織可能需要為網路安全理念和企業文化做出一些改變。

零信任之路是個漸進的過程，可能需要數年時間才能實現。

最初，實施零信任所需的技術和服務可能會導致企業的成本增加，但從長遠來看，零信任將使安全投資能夠更審慎地分配給企業最為關鍵的資源和服務，使得安全投資更加明智，而不是一次性的投入所有資訊安全需要的投資。

四、實施零信任的挑戰

與大多數大型企業一樣，聯邦政府實施零信任時都面臨著許多挑戰。老舊系統通常依賴於「預設隱式信任」，它們僅透過少量固定屬性對連線和授權進行安全評估，這與零信任的自適應信任評估之核心原則互相衝突。建置在隱性信任基礎上的現有基礎設施需要投資來改變系統，以便符合零信任原則。隨著技術領域不斷進步，機構亦需要持續討論新的解決方案以及如何最佳化實作以達成零信任目標。

導入零信任需要管理階層、IT 人員、資料及系統擁有者與聯邦政府各組織的參與及共同合作，才能有效設計並實現改善網路安全狀況之目標。聯邦政府網路安全的現代化要求各機構從煙囪式各自獨立的 IT 服務轉變為零信任策略協調和協同合作，在組織預算範圍內採購通用架構和治理政策相關產品，並考量當下或未來逐步採用雲端的技術。

聯邦機構正從不同的起點開始零信任之旅，有些機構可能比其他機構走得更遠或更有能力取得進展，無論起點如何，一旦導入零信任都可以帶來好處，例如，提高生產力、增強用戶體驗、降低 IT 成本、提供更靈活存取策略和強化安全性。

五、零信任成熟度模型

零信任成熟度模型(ZTMM)是從五個不同面向的支柱逐步實施零信任改進的過程。五個支柱包括身份識別 (Identity)、設備 (Devices)、網路(Networks)、應用程式與工作負載 (Applications and Workloads)，以

及資料 (Data)。模型的底層包含橫跨所有支柱的三項能力：可見性與分析、自動化和執行、治理。

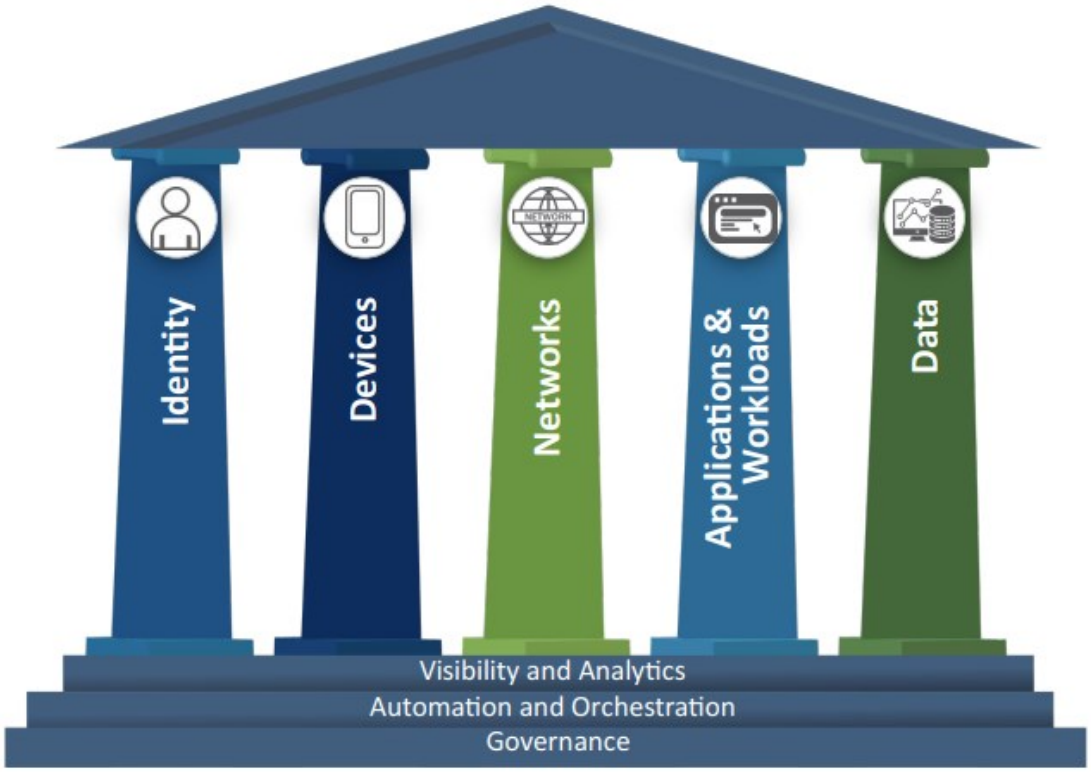

圖 1，零信任成熟度模型支柱

ZTMM 是邁向零信任的眾多途徑之。

各種不同零信任架構的相關出版物都為成熟度模型提供了諸多資訊，本成熟度模型係遵循 NIST SP 800-207 的零信任架構設計與部署的七項基本原則：

1. 所有資料來源和運算服務都被視為資源。
2. 無論與哪一個網路位置的裝置通訊，都必需是安全的。
3. 對企業資源的存取應以連線為基礎去判斷是否授予存取權。
4. 授予資源存取的許可權由動態策略決定。
5. 企業需監控和衡量所有自有與相關資產的完整性和安全狀況。
6. 在決定是否授權存取之前，所有資源的身分鑑別與授權機制，都要依監控結果動態決定，並且嚴格落實。
7. 企業應盡可能地收集有關資產狀態、網路基礎設施和通訊的資訊狀況，並使用這些資訊來增進安全態勢。

隨著各機構逐步實現零信任，相關解決方案將越來越依賴自動化流程和系統，這些系統把各個支柱進一步整合，並動態地執行策略決策。每一個支柱都可以獨立演進發展，甚至可能比其他支柱發展地更快，直到需要進行跨支柱的間協調才暫時停下來。互相協調只能透過彼此相容以及企業範圍的功能和依賴關係來實現，需要定義隨著時間逐步演進所需的分攤成本，而非一開始就一次性全部投入。

根據 NIST 提出的零信任進展步驟，各機構在投資零信任(包括該模型中概述的支柱和功能)之前先評估其當前的機構系統、資源、基礎設施、人員和流程。此評估可以幫助機構確定現有能力，以掌握優先解決的能力缺口。各機構還可以規劃如何透過協調跨支柱的能力，以實現更小細粒度、最小授權的存取控制並降低額外的風險。

零信任成熟度進展依照傳統階段分級為起點，歷經初始、進階和最佳化共四個階段。這種階段性設計有助於促進聯邦零信任的實現，每個後續階段對支柱的保護力、實現細節和技術複雜性都有更高的要求。

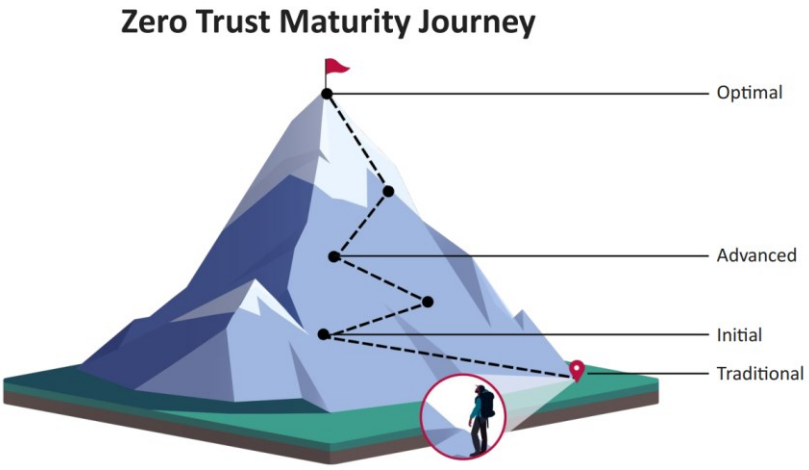

圖 2，零信任成熟度發展旅程

如圖 2 所示，當各支柱和跨支柱的零信任成熟度不斷提高時，各機構將預見到應付出的努力和效益將會顯著增加。在各機構準備展開零信任旅程時，應探索提高支柱成熟度時如何使之與特定的任務需求相匹配，並支援其他支柱的發展。

圖 3 呈現了機構隨著時間的推移從傳統企業向未來狀態發展的預期演變，企業將具備有更多動態更新、自動化流程、整合功能以及最佳階段的其他特徵。這些階段是動態的並且呈現指數增長，由一個成熟度階段到下一階段的進展會隨著時間的推移產生不同範圍的影響。

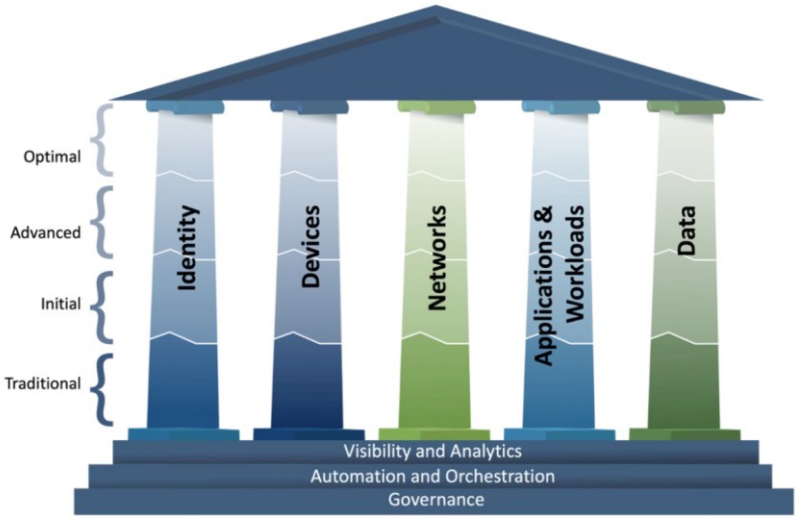

圖 3，零信任成熟度演進

各機構應使用以下的原則來識別、確認個別零信任技術支柱的成熟度階段，以保持成熟度模型標準的一致性：

- **傳統階段**：手動的生命周期管理和屬性分配(安全和日誌記錄)；靜態的安全策略和解決方案；每次只能處理一個支柱，與外部系統的依賴鬆散。僅在建置時遵循最小授權原則，各個支柱形同孤島彼此獨立；手動式的應變和緩解措施；佈署，相依性、日誌和監測只有少量關聯。
- **初始階段**：自動化的屬性配置、生命周期管理、策略決策和執行；具有與外部系統整合的跨支柱解決方案；透過一些方法對權限做響應式調整；建置後實施最小授權原則，讓內部各系統具備可見性。
- **進階階段**：能夠透過跨支柱協調對策略及配置的生命周期和授權分配進行自動化控制。具有集中式的可見性和身份管控，跨支柱的執行策略，能夠執行預定義的緩解措施應變活動，根據風險和安全態勢評估調整最小授權，建立涵蓋機構範圍及外部託管資源的安全意識。
- **最佳階段**：資產和資源能夠通過自動監測觸發器的動態策略提供自我報告，實現完全自動化及時的生命周期和屬性分配。對機構範圍內的資源存取實現動態的最小授權；具有持續監控的跨支柱互通性，具備集中的全面態勢感知可見性。

圖 4 提供了 ZTMM 的高層級概述，包括各支柱和每一個成熟度階段的關鍵功能。

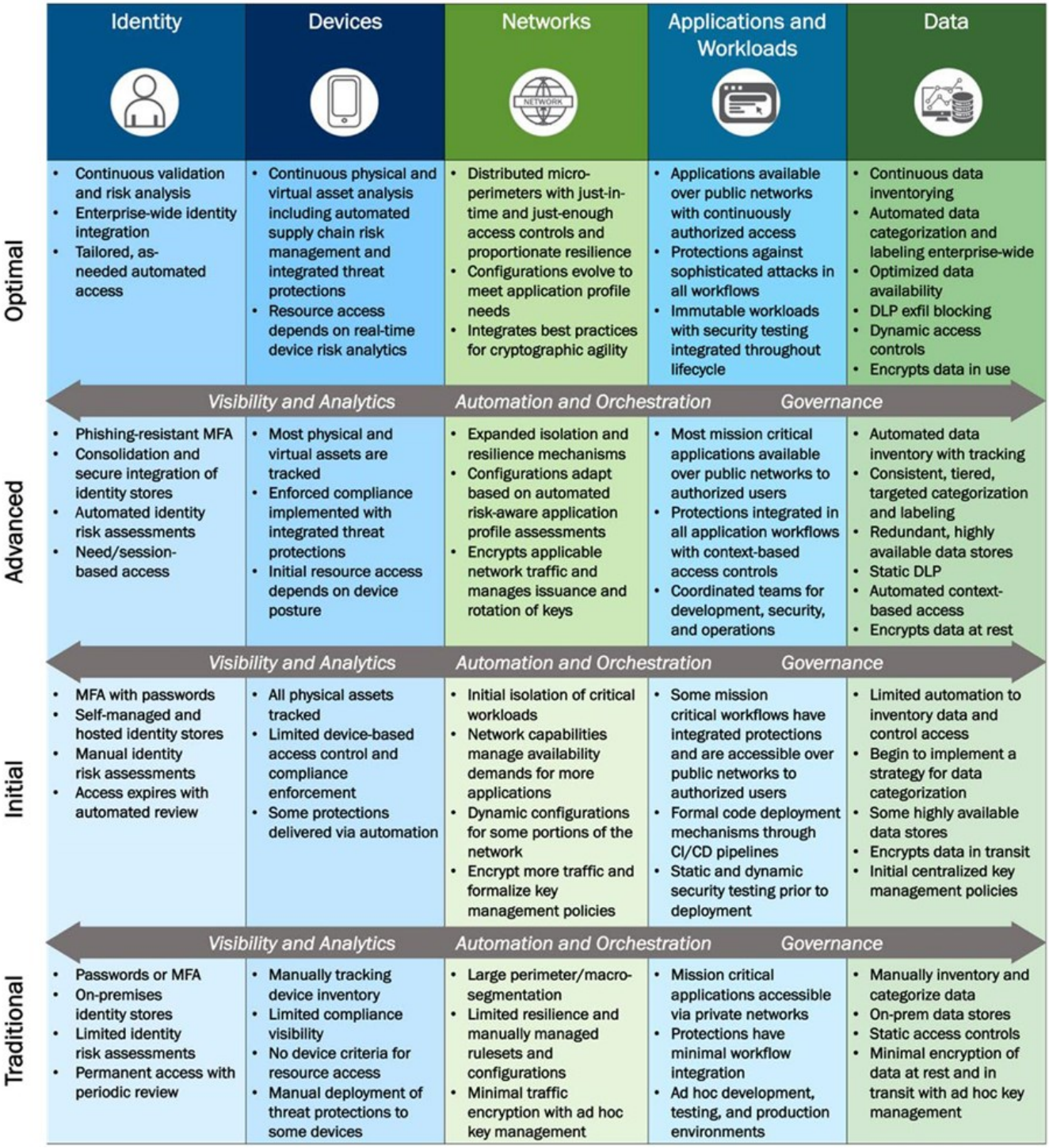

圖 4，各階段零信任成熟度模型

這些成熟度階段以及與各支柱相關的詳細資訊提供機構於評估、規劃和維護實施零信任所需的投資。本文後續各小節將為各支柱提供詳細資訊以協助各機構將五大支柱：身份識別、設備、網路、應用和工作負載以及資料過渡到零信任架構。每一個支柱包括三項支援整合各支柱成為共通模型之細節：可見性與分析、自動化與執行，以及治理能力，這三項跨領域的功能如何支援跨支柱功能互通性描述如下：

- 可見性與分析。可見性是指由機構環境的特徵和事件中產生可觀測的指標。對於網路安全相關的數據進行分析可幫助為政策提供決策依據、促進安全應變活動，建立風險概況，以便於安全事件發生之前主動積極制定安全措施。
- 自動化和執行。零信任充分利自動化工具和工作流程，以支援跨產品和服務安全應變功能，同時維護功能、產品和服務開發過程的監督、安全性和互動。
- 治理能力。支柱內部或跨支柱層面的網路安全策略、程序和流程有一致的定義與相同執行方式，以降低網路安全風險，並符合零信任原則並滿足聯邦政府要求。

雖然零信任成熟度模型涵蓋對聯邦機構網路安全的許多建議，但多少存在一些未涉及的部分，例如，與事件應變相關的活動、日誌記錄、監控、警報、取證、分析、風險接受程度、事後恢復等細節，與機構網路安全態勢管理相關的特性以及最佳實踐都沒有明確地納入成熟度模型中。儘管成熟度模型並無排他性，但它確實也沒有解決與營運相關的挑戰，包括某些類型的物聯網(IoT)設備或已被廣泛採用的新興技術，例如，欺騙平台、可認證的 WAF、行為分析等。另外此模型的解決方案也沒有納入機器學習和人工智慧等方法。成熟的機構應採取各種不同措施以監控和評估其安全性、底層基礎設施和策略的性能和完整性，一旦發現未授權之存取和變化，各機構應該注意不要為攻擊者創造新的可利用機會或被其利用弱化安全的通訊協議。有效確保跨聯邦組織的軟硬體系統完整性的技術，未來也還需要進一步研究和開發。

規劃零信任並實施時，各機構應根據風險、任務、聯邦要求和操作限制等因素做出決策。此模型雖然與聯邦機構的單一管理領域或認證邊界保持一致，但各機構評估零信任的影響因素時，仍然需要考慮與外部合作伙伴、利益相關人和服務提供商的互動和依賴如何影響其零信任架構。另外，機構不應該將此成熟度模型視為一個嚴格強制的要求，而是要將其視為一個能夠幫助機構成功實施零信任並對網路安全態勢進行整體提升的通用指南。

5.1 身分識別

身分識別是指能夠用來唯一辨識使用者或非使用者之實體的屬性或屬性集。

機構應確保使用者和非使用者之實體在正確的時間基於正確的目的以正確的授權存取正確的資源。機構應盡可能將身分認證整合為單一憑證和存取管理的解決方案，並評估用戶和實體身分風險，實行強式身分驗證，以客製化基於上下文操作情境授予權限。機構需視情況整合其身分識別、資料儲存和管理制度，以改善對使用者身分及其相關責任和權限的認知。

表 2 列出了與零信任相關的身分識別功能以及相關於可見性與分析、自動化和執行以及治理的注意事項。

表 2，身分識別支柱

功能	傳統階段	初始階段	高級階段	最佳階段
身份認證	靜態的存取授權，使用密碼或多因素認證(MFA)進行身份認證。	使用 MFA 對身份進行驗證，除了將密碼作為 MFA 中的一種認證方式，並要求驗證多個實體屬性(例如所在之場所或進行之活動)。	使用防釣魚攻擊 MFA 和屬性對所有身份進行身驗證，包括透過 FIDO2 或 PIV 實作無密碼 MFA。	持續使用防釣魚攻擊的 MFA 對身份進行驗證，而不僅僅是在最初授權時進行驗證。
身份儲存	只使用自主管理的本地端身份庫(計劃、佈署和維護皆由組織自行承擔)。	同時使用自主管理的和託管(例如，雲端或其他第三方機構)的身份資料庫，但資料庫之間缺少整合(例如，可支援跨系統單點登錄)。	開始進行安全地合併和整合自主管理與託管的身份庫。	安全地合併和整合自主管理與託管的身份庫。
風險評估	對身份風險進行有限的判斷(例如判斷身份被竊取的可能性)。	使用手動方法和靜態規則來確定身份風險，達成授權之可見性。	使用一些自動化分析和動態規則來確定身份風險，以支援存取決策和回應活動。	持續分析和使用動態規則，即時地確認身份風險，提供持續的保護。
存取管理 (新增)	永久性存取授權，只有定期對特權和非特權帳戶進行審核。	對存取(包括特權存取)進行有限時間授權，並透過自動審核令存取權限過期自動失效。	基於需求和 Session 存取請求(包括特權存取請求)授權，針對不同操作和資源給予不同授權。	使用自動化實現即時授權和恰到好處的存取權限，以滿足操作和存取資源所需之權限需求。
可見性與分析	收集用戶和實體的活動日誌紀錄(特別是特權操作紀錄)，並進行例行性人工分析。	收集用戶和實體活動日誌，進行例行性人工分析和一部分的自動分析，不同類型的日誌僅有少量關聯性。	在某些類型的用戶和實體活動日誌進行自動化分析，並增加日誌收集範圍以縮小可見性的差距。	透過對用戶活動日誌(包括基於行為的分析)進行自動化分析，實現機構範圍的全面可見性和感知安全態勢。

自動化與執行	以人工手動進行用戶和實體身分管理(到職、離職、禁用)，沒有整合性，只有定期進行審查。	人工手動管理特權和外部身份認證，自動管理非特權用戶和自主管理之實體。	人工手動管理特權用戶身份，並自動管理環境中所有整合的身份認證。	依據行為、註冊和佈署需求，在所有環境完全整合所有身份自動管理。
治理	通過靜態機制和人工審核實行身份策略(認證、憑證、存取、生命周期管理等)。	實行少量自動化，主要透過人工手動更新身份策略。	實行自動化定期更新身份策略。	為所有用戶和實體實行針對所有系統執行自動化身份辨識策略，並實現持續的策略動態更新。

5.2 設備

設備是指可以連接到網路的任何資產(包括其硬體、軟體、韌體)，包含伺服器、桌上型電腦、筆記型電腦、印表機、行動電話、物聯網設備、網路設備等

設備包含是機構所擁有的，或者員工、合作夥伴或訪客的 BYOD 財產。機構需保護所有設備的安全，並防止未經授權的設備存取資源。設備管理包括維護所有資產的動態清單(包括其硬體、軟體、韌體等)，以及它們的配置和已知的相關漏洞。

許多設備管理都面臨特定的零信任挑戰，必須根據具體情況進行評估，作為基於風險管理流程的一部分。例如，網路設備、印表機和其他設備可能只能提供有限的身份驗證、可見性和安全性選項。採用 BYOD 策略的機構可能沒有太多選擇來維持此類裝置的可見性和控制。設備的技術不斷變化，隨著機構納入更多設備，他們需要持續管理與這些不斷變化設備的相關風險，在某些情況下，本指南可能無法適用於各機構的特定設備。另外，各機構都會面臨維護設備和服務生命周期結束無法獲得技術支援的挑戰，因為老舊設備通常存在大量未緩解的漏洞、錯誤的配置和未知的風險。然而，儘管存在這些挑戰，各機構仍可在導入零信任的實現中取得設備管理的進步。

私有化運算資源管理和記錄實體資產(設備)，隨著機構將運算遷移到雲端環境，還要考慮如何管理和追蹤機構的雲端虛擬資產。雲端資產包括運算資源(例如，虛擬機器、伺服器或容器)、儲存資源(例如，區塊儲存或檔案儲存)、平台資產(例如，資料庫、Web 伺服器、訊息佇列服務)和網路資源(例如，虛擬網路、VPN、網路閘道、DNS 服務等)以及與其他託管的雲端服務(例如，人工智慧模型)相關的虛擬資源。

表 3 列出了與零信任相關的設備管理功能以及相關於可見性與分析、自動化和執行以及治理的注意事項。

表 3，設備支柱

功能	傳統階段	初始階段	高級階段	最佳階段
政策執行與合規性監控 (新功能)	機構對設備的合規可見性(即檢查設備行為能力)有限，且執行政策或管理的方法很少。	能接收自設備回報的有限特徵(例如，設備上的密鑰、Token、用戶等)。初步建立軟體安裝簽核流程，並能夠把更新和配置推送到設備上。	在最初開始使用設備前對設備進行合規驗證(即管理員可以檢查和驗證設備上的資料)，並對大多數設備和虛擬資產強制執行合規政策。使用自動化方法管理設備和虛擬資產、批准軟體安裝、識別漏洞和安裝修補程式。	在設備和虛擬資產的生命週期中，持續檢查並執行合規性政策。把所有設備包括虛擬資產的軟體安裝、配置和漏洞管理整合到所有機構的環境中。
資產和供應鏈風險管理 (新增)	未能以機構範圍或跨供應商追蹤實體或虛擬資產。採用臨時性採購設備和服務的策略，對機構風險認知非常有限。	追蹤所有實體和虛擬資產，並按照聯邦建議，使用風險框架(例如 NIST SCRM)建立策略和控制基準來管理供應鏈風險。	開始透過自動化開發實體和虛擬資產的完整機構設備之視圖。能夠跨多個供應商採購、追蹤開發週期並提供第三方評估的服務。	擁有全面的、實時或接近實時的跨供應商和服務提供商的資產視圖。在合適情況下，自動化其供應鏈風險管理，建立能容忍供

				應鏈故障的作業流程。
資源存取 (原資料存取)	在存取資源時，未要求對於設備或虛擬資產的可見性。	要求某些設備或虛擬資產回報其特徵，然後利用此訊息審核是否允許資源存取。	初始資源存取時會考慮設備存取經過驗證或虛擬資產的可見性。	資源存取時考慮設備和虛擬資產內的即時風險分析。
設備威脅保護 (新增)	對部分設備手動部署了威脅保護功能。	具有一些自動化流程，用於把威脅保護能力佈署和更新到設備及虛擬資產，並整合了少量的策略執行和合規監控。	將威脅保護能力整合到針對設備和虛擬資產的集中式解決方案，並將其中的大部分功能與策略執行和合規監控整合。	為所有設備和虛擬資產，佈署具有先進功能及集中式威脅保護安全解決方案。採用統一的方法實現設備威脅保護、策略實施和合規監控。
可見性與分析	使用標籤和庫存清單及有限的軟體監控管理，定期執行人工檢查和分析設備資料。	使用數位辨識(例如網路位址、數位標籤)以及設備的手動清單和終端監控來監測設備。 部分設備和虛擬資產能透過自動化分析(例如軟體掃描)以便根據風險執行異常檢測。	實現自動化蒐集設備清單(包括所有標準用戶設備上的終端監控，例如，桌上型電腦、筆記型電腦、手機、平板電腦及虛擬資產)並能夠檢測設備授權異常。	自動化蒐集所有可連接網路的設備和虛擬資產的狀態，並與身份驗證關聯、執行端點監控和異常檢測，為資源存取授權提供資訊。追蹤虛擬資產的建立和銷毀以監測異常。
自動化與執行	以人工進行設備配置和註冊。	使用工具和程式碼自動化處理流程，包括設備和虛擬資產的供應、配置、註冊和銷毀。	實現監控和策略執行機制，能識別、手動斷開或隔離不符合規定(包含，易受攻擊的設備、未經驗證的憑證、未註冊的 MAC 位址)設備和虛擬資產。	全自動化流程實現設備及虛擬資產之供應、註冊、監控、隔離、修復和銷毀。
治理	制定傳統的設備生命周期策略，依賴人工流程來維護(例如更新程式、修補漏洞、掃毒)這些設備。	制定並執行有關新設備採購，傳統設備和虛擬資產的生命周期策略，並定期對設備進行監測和掃描。	為設備和虛擬資產制定生命周期策略，包括設備列舉和責任，並實現了一些自動實施機制。	對所有可連接網路的設備和虛擬資產執行自動化生命周期策略。

備註: 設備生命周期包括採購、配置、追蹤、監控、更新、使用、清理、銷毀以及恢復等多個階段。

5.3 網路

網路是指開放的通訊介質，例如機構內部網路、無線網路和 Internet 等典型通道以及其他例如用於傳輸的行動網路和應用層通道等。

零信任架構令傳統基於邊界的安全控制方法發生改變，機構建立了管理內部和外部流量、隔離主機、強制加密、分段存取活動並增強機構網路的可見性。零信任架構要求在更靠近應用程式、資料和資源的位置實行安全控制，並強化了傳統基於網路的保護措施並提高了防禦深度。由於不同應用的存取權限、優先級、可及性、與依賴服務的連接及連接路徑等方面有不同的要求，這些網路的應用程式都必須以不同的方式處理授權。機構可以透過蒐集應用程式剛要，讓相同的綱要可以視為同一類型進行處理，以簡化管理。

表 4 列出了與零信任相關的網路功能管理以及相關於可見性與分析、自動化和執行以及治理的注意事項。

表 4，網路支柱

功能	傳統階段	初始階段	高級階段	最佳階段
網路分段	使用大邊界的宏觀分段定義網路架構，相同網段內的可及性基本上不受約束。允許依賴提供多重服務的網路互連(例如，VPN)。	佈署隔離關鍵網路的架構，對關鍵工作負載進行隔離，按最小功能(權限)原則限制互通性，並過渡為特定服務互連的網路架構。	透過與特定服務互連的進/出微邊界，將端點和應用程式隔離機制擴大佈署到更多的網路架構。	網路架構由完全分散式的進/出微邊界和基於應用程序的微分段組成，動態實現即時和適度特定服務的連接性。
網路流量管理(新增)	在服務提供過程中，以人工實施靜態網路規則和配置來管理流量，僅具備有限的監控能力(例如應用程式性能監控或異常偵測)，對關鍵業務應用的設定變更透過人工進行審核。	為不同應用程式建立不同流量管理的概要，並開始把應用程式映射到這個概要。將靜態規則擴展應用到所有應用程序，並定期對應用程式概要進行人工審核。	實施動態網路規則配置，以達成資源最佳化，這些規則配置根據自動風險感知和具備風險回應的應用程式概要進行評估和監控，並定期進行調整。	實施持續演化的動態網路規則配置，以滿足應用程式概要的需求。根據關鍵任務、風險等因素確定應用程式優先等級。
流量加密(原加密)	對少量流量執行加密，並依靠手動或臨時流程來管理和保護加密金鑰。	加密所有內部的流量，對外部應用程式的流量盡可能進行加密。制定金鑰管理策略規範，並保護伺服器和服務加密金鑰。	所有應用程式內部和外部流量均進行加密。發行和金鑰及憑證的輪換管理，導入加密敏捷性的實踐。	持續根據需求加密流量，強制實施安全金鑰管理及最小授權原則。廣泛地納入加密敏捷性的最佳實踐。
網路彈性(新增)	根據單一應用程式的可用性需求，依照個案配置網路，只適用於非關鍵任務需求，僅具備有限的彈性。	透過配置網路功能來管理其他應用程式的可用性要求，並擴展非關鍵任務需求及彈性。	配置網路動態管理能力，可符合大部分應用程式的可用性需求和彈性機制。	能感知所有工作負載及可用性需求變化，並整合全面性的需求，提供相對應彈性機制。

可見性與分析	透過以網路邊界為重點的有限監控和分析，開始開發集中式的態勢感知。	採用已知入侵指標(包括網路掃描)的網路監控來發展態勢感知，並把各種環境的不同流量關聯起來，進行分析和威脅檢測。	透過網路異常檢測功能，掌握跨所有環境的態勢感知。關聯多個來源的監測資料進行分析，並結合自動化流程實現強化的威脅探索活動。	機構具備態勢感知和監控能力，同時實現動態的態勢感知與先進的自動畫間測及控制功能。
自動化與執行	使用手動的流程管理網路、環境、配置和資源生命周期。定期整合策略要求和態勢感知的網路和環境。	使用自動化方法管理某些網路、環境、配置和資源生命周期，並確保所有資源都基於策略和監測數據定義其生命周期。	使用自動化變更管理方法(如 CI/CD)管理所有網路、環境、配置和資源生命周期，能夠對感知到的風險進行回應、執行策略和保護措施。	網路和環境由基礎架構即程式碼(IaC)定義，實行自動化變更管理方法，包括自動的初始化與過期失效，以應對不斷變化的需求。
治理	通過以邊界保護為重點的方法實施靜態的網路策略(存取、協議、分段、警告和修復)。	針對所有網路分段和資源制定並實施相對應的策略，並符合機構的策略規則。	自動化執行量身訂做的客製化政策，並將保護從周邊過渡到中心。	實現客製化的本地控制、動態更新，並根據應用程式和使用者工作流程保護外部連線。

5.4 應用程式和工作負載

應用程式和工作負載包括在本機、雲端環境、行動裝置上執行的代理系統、電腦程式和服務。

機構必須管理和保護其佈署的應用程序，並確保具備安全的應用程序交付流程、精細化存取控制和整合的威脅防護，提供增強的應用程式安全態勢感知，並降低應用程序可能遭遇的特定威脅。根據 OMB M-22-09 之規定，各機構應逐漸透過公共網路向授權使用者提供其應用程式。在可能的情況下，各機構應採用基於 DevSecOps 和 CI/CD 流程的最佳實踐，包括使用不可變工作負載。各機構應該探索一些新的選擇，把營運重點由認證邊界和更新 ATO (Authorization to Operate)，逐漸轉向對應用程序自身，使其無論是由內部存取，還是由外部存取都具有相同的安全性。

表 5 列出了與零信任相關的應用程式和工作負載以及相關於可見性與分析、自動化和執行以及治理的注意事項。

表 5，應用程式和工作負載支柱

功能	傳統階段	初始階段	高級階段	最佳階段
應用程式存取 (以前稱為存取授權)	主要基於本機授權和靜態屬性授權應用程式的存取。	機構開始實施授權存取應用程式的能力，當發起請求與授權到期時，參考上下文的資訊(例如身分、設備合規性或其他屬性)決定是否授權。	自動化執行具備擴展上下文資訊和遵守最小授權原則的強制到期條件之應用程式存取策略。	結合即時風險分析和行為或使用模式等因素，決定是否授權請求存取，。
應用程式威脅保護措施 (以前的威脅保護)	威脅防護與應用程式動作流程的整合程度最低，適用於通用的已知威脅之保護。	把威脅保護整合到關鍵業務應用的工作流程中，能針對已知威脅和一些特定的威脅提供保護。	將威脅保護整合到所有應用的工作流程中，保護某些特定於應用程序的針對性威脅。	把高級威脅保護整合到所有應用工作流程中，提供實時可見性和內容感知保護，以應對特定於應用程序的複雜攻擊。
可存取應用 (原可存取性)	關鍵應用僅在私有網路和有監控的安全公共網路連接(例如 VPN)上可用。	為了滿足需要，透過代理連接的方式，提供部分適用的關鍵任務應用程式並授權用戶於開放的公共網路中使用。	根據需要，將大部分適用的關鍵任務應用程式透過開放的公共網路連接提供並授權用戶使用。	根據需要，將所有適用的應用透過開放的公共網路提供並授權用戶和設備使用。
開發和部署工作流 (新增)	使用非正式的開發、測試和生產環境，缺乏健全的程式碼佈署機制。	採用具備符合規範的程式碼部署機制基礎架構來支援開發、測試和佈署到生產環境(包括自動化)。透過 CI/CD 流程和必要的存取控制達成最小授權原則。	由不同團隊完成開發、安全和營運，並取消開發人員程式碼佈署時對生產環境的存取權限。	充分利用不可變工作流程，更改只能透過佈署生效。取消管理員對佈署之生產環境的存取權限，以自動化程式碼佈署流程取代人工佈署。

應用程式安全測試 (原應用安全)	在佈署之前進行應用安全測試，主要通過手動測試方法執行。	應用程式佈署前的安全測試使用靜態和動態測試方法，包括手動的專家分析。	將應用程式安全測試整合到應用程式開發和佈署流程，包括使用周期性的動態測試方法。	在軟體開發生命周期中全面整合應用程式安全測試。已佈署之應用程序持續進行例行性自動化測試。
可見性與分析	對關鍵業務應用程式進行一些性能和安全監控，但整合和分析能力有限。	自動蒐集應用程式訊息(例如狀態、健康度和性能)和安全監控，以改善人工日誌蒐集、整合和分析。	透過啟發式技術，自動化地對大部分應用程式進行資訊蒐集和安全監控，以識別應用程式特有的和機構整體的趨勢，並逐步填補可見性中存在的缺點。	隊所有應用程式執行持續、動態的監控，以保持全面的可見性。
自動化與執行	透過手動方式分配資源，建立靜態的應用程式代管目錄與存取權限，並進行有限度的維護和審查。	定期修改應用程式配置(包括目錄和存取權限)，以滿足相關的安全和性能目標。	自動處理應用程式配置，以應對營運和環境變化。	自動處理應用程式配置，以持續優化安全性和性能
治理	主要依靠手動執行的策略以實現對應用程式存取、開發、佈署、軟體資產管理、安全測試和評估，包括使用之技術、漏洞修補和跟蹤軟體相依性。	根據任務需求(例如，軟體元件清單)以自動化執行策略規範，透過自動化方式實現對應用程式開發、佈署、軟體資產管理及使用技術、修補漏洞和追蹤軟體相依性等方面的管理和監督。	為應用程式實施分級、訂定策略以覆蓋從開發到佈署生命周期的所有階段，並盡可能利用自動化執行策略。	完全自動化的應用程式開發和佈署策略，包括透過 CI/CD 流程動態更新應用程式的程序。

5.5 資料

資料包含所有結構化、非結構化之檔案或曾經保留於系統、儲存裝置、網路、應用程式、資料庫、基礎架構和備份(包括本地和虛擬環境)的原始資料。

根據聯邦要求機構在設備、應用程式和網路上必須妥善保護資料。各機構應該對資料進行盤點、進行分類和標記，保護靜態和傳輸中的資料安全性，並建立機制檢測和阻止資料外洩。各機構應制定和審查資料治理策略，以確保所有資料生命週期的安全管理。

表 6 列出了與資料以及相關於可見性與分析、自動化和執行以及治理的注意事項。

表 6，資料支柱

功能	傳統階段	初始階段	高級階段	最佳階段
資料清單管理	人工識別部分資料(例如，關鍵業務資料)，並為其建立清單。	採用自動化資料清單流程，覆蓋本地端與雲端環境中的大部分資料，並導入防止資料遺失的保護措施。	自動建立資料清單和追蹤異動，涵蓋機構所有適用的資料，並採用靜態屬性和標籤的預防資料洩漏策略。	持續維護所有適用的資料清單，並採用強大的資料防洩漏策略，動態阻止可疑的資料洩露。
資料分類(新功能)	機構採用有限且臨時的資料分類功能。	開始實施具備標記定義的資料分類執行策略。	透過簡單、結構化的格式和定期審查，以一致的、分級的、有針對性的方式動態執行部分資料分類和標記。	採用自動化技術進行分類和標記，以最小細粒度、結構化格式自動對所有資料執行分類和標記。
資料可用性(新增)	主要由本地資料庫提供資料，同時具備一些異地備份機制。	從具有備援、高可用性的雲端資料庫提供資料，並為本地資料建立異地備份。	主要由具有備援、高可用的資料庫中提供資料，並確保可以存取歷史資料。	使用動態方法根據用戶和實體的需求調整最佳化資料可用性，包括歷史資料。
資料存取	透過靜態存取控制管理用戶和實體的資料存取(包含：讀取、寫入、複製、授權他人存取等)權限。	使用最小授權原則，佈署自動化的資料存取控制機制。	在自動化資料存取控制中，採用各種屬性，如身份、設備風險、應用程式、資料類別等，並於適當情況下限制存取時間。	自動執行即時(just-in-time)和恰到好處(just-enough)的資料存取控制，在存取期間持續審查權限。
資料加密	只針對必要的資料進行最低限度的加密，包括資料儲存和傳輸過程中的加密，依靠手動或臨時流程管理加密方法和保護加密密鑰。	對傳輸中的所有資料以及靜態資料加密，並正式制定金鑰管理策略和保護安全加密金鑰。	加密整個機構中所有靜態資料和傳輸中的資料，納入加密敏捷性，並保護加密密鑰(即密碼是會定期輪換的)。	必要時對使用中的資料進行加密，實施最小授權原則以進行安全密鑰管理，並儘可能使用最新的 NIST 標準和密碼敏捷性之應用加密技術。

可見性與分析	對資料位置、存取和使用的可見性非常有限，主要依賴手動流程進行分析。	透過資料清單管理、分類、加密與存取以提高可見性，並結合自動化和相關性分析。	採用自動化和相關性分析，維護更全面的資料可見性，並採用預測分析技術。	能夠全面追蹤資料的生命周期，具備強大的分析能力，包括預測分析，支援全面的資料視圖並持續的進行安全狀況評估。
自動化與執行	透過手動和非正式的流程實施資料的生命周期管理和安全策略(包含：存取、使用、儲存、加密、配置、保護、備份、分類、清除)。	使用了一些自動流程進行資料生命周期管理和安全策略。	以一致的、有分級的、針對性的自動化方式對大部分資料進行生命周期管理和安全策略。	自動化進行所有資料的生命周期管理和安全策略。
治理	手動執行非正式的資料治理策略(包含：保護、分類、存取、清單化、儲存、恢復、清除等)。	定義分級資料治理策略，但仍依賴手動和分段實施。	整合資料生命週期政策，統一提供資料治理的定義。	統一資料生命週期政策。

5.6 跨領域能力

跨領域的可見性與分析、自動化和執行和治理提供五個支柱的進步的機會。各機構提高獨立於支柱本身的每項能力，也可以兼顧提高支柱跨領域能力的成熟度。可見性與分析維持全面的可見性，為政策決策提供資訊並促進回應活動；自動化和執行能夠利用這些可見性來支援穩健和簡化的處理安全事件操作並在事件發生時做出回應；治理使各機構能夠管理和監控其監管、法律、環境、聯邦和營運要求，以支援基於風險的決策，治理能力也確保有合適的人員、流程和技術到位，以達成任務、風險之合規目標。

表 7 列出了每種跨領域功能的各階段成熟度演變。

表 7，跨領域能力

功能	傳統階段	初始階段	高級階段	最佳階段
可見性與分析	手動蒐集有限的日誌紀錄，日誌品質比較差且僅進行了最基本的分析。	自動收集和分析關鍵業務的日誌和事件，並定期評估可見性方面的缺點。	擴大自動化日誌和事件的收集範圍 (包括虛擬環境)，以集中進行跨多個來源的關聯分析分析。	集中日誌和事件的紀錄，動態監控和進行高級分析，全面實現可見性。
自動化與執行	依靠靜態和手動流程執行操作和回應活動，自動化程度有限。	開始自動化執行與回應活動，以支持關鍵任務。	實現自動化執行與回應活動，並利用多個來源的上下文資訊來指導策略決策。	機構自動化協調和回應活動，動態回應不斷變化的需求和環境變化。
治理	以非正式方式實施策略，主要透過手動流程或靜態技術執行策略。	定義並開始實施適用於整個機構範圍的策略，但仍缺乏自動化，需要手動更新。	實施分級和訂製策略，利用自動化技術支援策略執行。存取控制策略的決策是利用了來自多個來源的上下文信息來決定。	實施完全自動化的策略，能透過持續的策略執行和動態更新，實現客製化的本地控制。