NetApp 與 Zero Trust

ONTAP Technical Reports

NetApp

January 23, 2026

目錄

NetApp 與 Zero Trust

NetApp 與 Zero Trust

零信任傳統上是一種以網路為中心的方法、用於建構微核心和周邊（ MCAP ）、以控制區段閘道的方式來保護資料、服務、應用程式或資產。NetApp ONTAP 採用以資料為中心的 Zero Trust 方法、將儲存管理系統變成區段閘道、以保護及監控客戶資料的存取。特別是、 FPolicy Zero Trust 引擎和 FPolicy 合作夥伴生態系統成為控制中心、可深入瞭解正常和異常的資料存取模式、並識別內部威脅。

自 2024 年 7 月起，技術報告 _TR-4829 的內容： NetApp 與 Zero Trust ：啟用以資料為中心的 Zero Trust 模式 _ ，此模式先前以 PDF 格式發佈，可在 docs.netapp.com 取得。

資料是貴組織最重要的資產。根據 2022 年的資料外洩、內部威脅是 18% 資料外洩的原因 "Verizon 資料外洩調查報告"。組織可以利用 NetApp ONTAP 資料管理軟體、針對資料部署領先業界的 Zero Trust 控管措施、提高警覺性。

什麼是 **Zero Trust** ？

Zero Trust 模式是由 John Kindervag 在 Forrester Research 首次開發。它從內到外都能實現網路安全性、而非從外到外。 「內到外零信任」方法可識別微核心和周邊（ MCAP ）。MCAP 是資料、服務、應用程式和資產的內部定義、可透過一套完整的控制功能加以保護。安全外部邊界的概念已經過時。受信任且允許透過周邊環境成功驗證的實體、可能會使組織容易遭受攻擊。根據定義、內部人員已經在安全的邊界內。員工、承包商和合作夥伴都是內部人員、他們必須能夠在組織基礎架構中執行職務時、以適當的控管方式運作。

零信任被視為一項技術、可在 2019 年 9 月向 DoD 提供承諾 "FY19-23 DoD 數位現代化策略"。它將 Zero Trust 定義為「一種網路安全策略、可在整個架構內嵌安全性、以阻止資料外洩。這種以資料為中心的安全模式消除了受信任或不受信任的網路、裝置、角色或程序的概念、並移轉到多屬性型信任層級、以在最低權限存取概念下啟用驗證和授權原則。實作零信任需要重新思考我們如何使用現有基礎架構，以更簡單，更有效率的方式設計安全性，同時實現不受阻礙的作業。」

2020 年 8 月、 NIST 發佈 "Special Pub 800-207 Zero Trust Architecture" （ ZTA ）。ZTA 著重於保護資源、而非網路區段、因為網路位置不再被視為資源安全狀態的主要元件。資源是資料和運算。ZTA 策略適用於企業網路架構設計師。ZTA 引進了一些來自 Forrester 原創概念的新術語。稱為原則決策點（ PDP ）和原則執行點（ PEP ）的保護機制、類似於 Forrester 分割閘道。ZTA 推出四種部署模式：

- 裝置代理程式或閘道型部署
- 以飛地為基礎的部署（有點類似於 Forrester MCAP ）
- 資源入口網站型部署
- 裝置應用程式沙箱

就本文件而言、我們使用 Forrester Research 的概念和術語、而非 NIST ZTA 。

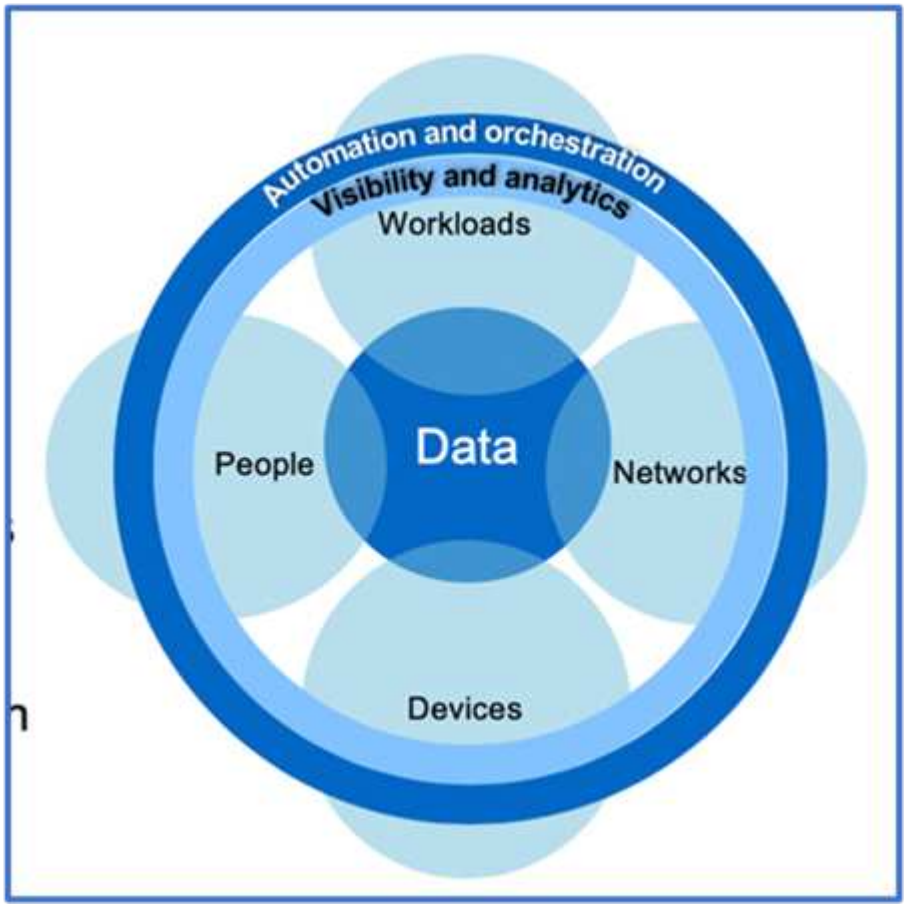
安全資源

有關報告漏洞和事件、 NetApp 安全響應和客戶機密性的信息，請參閱 "NetApp 安全入口網站"。

使用 ONTAP 架構以資料為中心的零信任方法

Zero Trust 網路是以資料為中心的方法所定義、其中的安全控管措施應盡可能接近資料。ONTAP 的功能搭配 NetApp FPolicy 合作夥伴生態系統、可為以資料為中心的零信任模式提供必要的控制。

ONTAP 是 NetApp 提供的安全性豐富的資料管理軟體、而 FPolicy Zero Trust Engine 則是領先業界的 ONTAP 功能、可提供精細的檔案型事件通知介面。NetApp FPolicy 合作夥伴可以使用此介面、在 ONTAP 中提供更多資料存取的照明。



建構 Zero Trust 資料導向的 MCAP

若要架構以資料為中心的 Zero Trust MCAP 、請遵循下列步驟：

1. 識別所有組織資料的位置。
2. 將資料分類。
3. 安全地處理不再需要的資料。
4. 瞭解哪些角色應該能夠存取資料分類。
5. 應用最低權限原則來強制執行存取控制。
6. 使用多因素驗證來進行管理存取和資料存取。
7. 對靜止資料和正在傳輸的資料使用加密。

8. 監控並記錄所有存取。
9. 警示可疑的存取或行為。

識別所有組織資料的位置

ONTAP 的 FPolicy 功能搭配 FPolicy 合作夥伴的 NetApp 聯盟合作夥伴生態系統、可讓您識別貴組織資料的存在位置、以及哪些人可以存取。這是透過使用者行為分析來完成、可識別資料存取模式是否有效。「監控」和「記錄所有存取」中會討論使用者行為分析的更多詳細資料。如果您不瞭解資料的位置和存取權、使用者行為分析可以提供基準、以根據經驗觀察來建立分類和原則。

將資料分類

在零信任模型的術語中，資料分類涉及有毒資料的識別。有毒資料是不適合在組織外部暴露的敏感資料。洩漏有毒資料可能會違反法規合規性並損害組織的聲譽。在監管合規方面，有毒數據包括持卡人數據 "支付卡產業資料安全標準（PCI-DSS）"，歐盟的個人數據 "一般資料保護規範（ GDPR ）"或醫療保健數據 "健康保險可攜性與責任法案（ HIPAA ）"。您可以使用NetApp "NetApp Data Classification" （以前稱為 Cloud Data Sense），一款人工智慧驅動的工具包，可自動掃描、分析和分類您的資料。

安全地處理不再需要的資料

將組織的資料分類之後、您可能會發現有些資料不再需要或與組織的功能相關。保留不必要的資料是一項責任、應刪除此類資料。如需加密清除資料的進階機制、請參閱「靜止資料加密」中的安全清除說明。

瞭解哪些角色應該擁有資料分類的存取權、並運用最低權限原則來強制執行存取控制

對應對敏感資料的存取權、並套用最低權限原則、意味著只有組織中的人員才能存取執行工作所需的資料。此過程涉及基於角色的訪問控制 ("RBAC")，適用於數據訪問和管理訪問。

有了 ONTAP 、儲存虛擬機器（ SVM ）可用來區隔 ONTAP 叢集內租戶的組織資料存取。RBAC 可套用至資料存取、以及對 SVM 的管理存取。您也可以在叢集管理層級套用 RBAC 。

除了 RBAC 之外、您也可以使用 ONTAP "多重管理驗證" （ MAV ）來要求一或多個系統管理員核准或等命令 `volume delete` `volume snapshot delete`。啟用MAV之後、修改或停用MAV需要MAV管理員核准。

另一種保護快照的方法是使用 ONTAP "Snapshot 鎖定"。Snapshot 鎖定是一種 SnapLock 功能，可在磁碟區快照原則上以手動或自動方式呈現快照，並保留一段時間。Snapshot 鎖定也稱為防竄改快照鎖定。快照鎖定的目的是防止惡意或不受信任的系統管理員刪除主要和次要 ONTAP 系統上的快照。可在主要系統上快速恢復鎖定的快照，以還原遭勒索軟體毀損的磁碟區。

使用多因素驗證來進行管理存取和資料存取

除了叢集管理 RBAC 之外、 "多因素驗證（ MFA ）" 也可部署以進行 ONTAP Web 管理存取和安全 Shell （ SSH ）命令列存取。美國公共部門組織或必須遵守 PCI-DSS 的組織、都必須使用 MFA 來進行管理存取。MFA 讓攻擊者無法僅使用使用者名稱和密碼來危害帳戶。MFA 需要兩個以上的驗證因素。雙因素驗證的範例是使用者擁有的東西、例如私密金鑰、以及使用者知道的東西、例如密碼。安全聲明標記語言（ SAML） 2.0 可讓管理網路存取 ONTAP 系統管理員或 ActiveIQ Unified Manager 。SSH 命令列存取使用連結的雙因素驗證搭配公開金鑰和密碼。

您可以使用 ONTAP 中的身分識別與存取管理功能、透過 API 控制使用者和機器存取：

- 使用者：

- * 驗證與授權。 *透過適用於 SMB 和 NFS 的 NAS 傳輸協定功能。
- * 稽核 *存取與事件的系統記錄。CIFS 通訊協定的詳細稽核記錄、以測試驗證和授權原則。精細精細的 FPolicy 稽核檔案層級的詳細 NAS 存取。

- 裝置：
  - * 驗證。 *用於 API 存取的憑證型驗證。
  - * 授權。 *預設或自訂角色型存取控制（ RBAC ）。
  - * 稽核 *系統記錄所採取的所有行動。

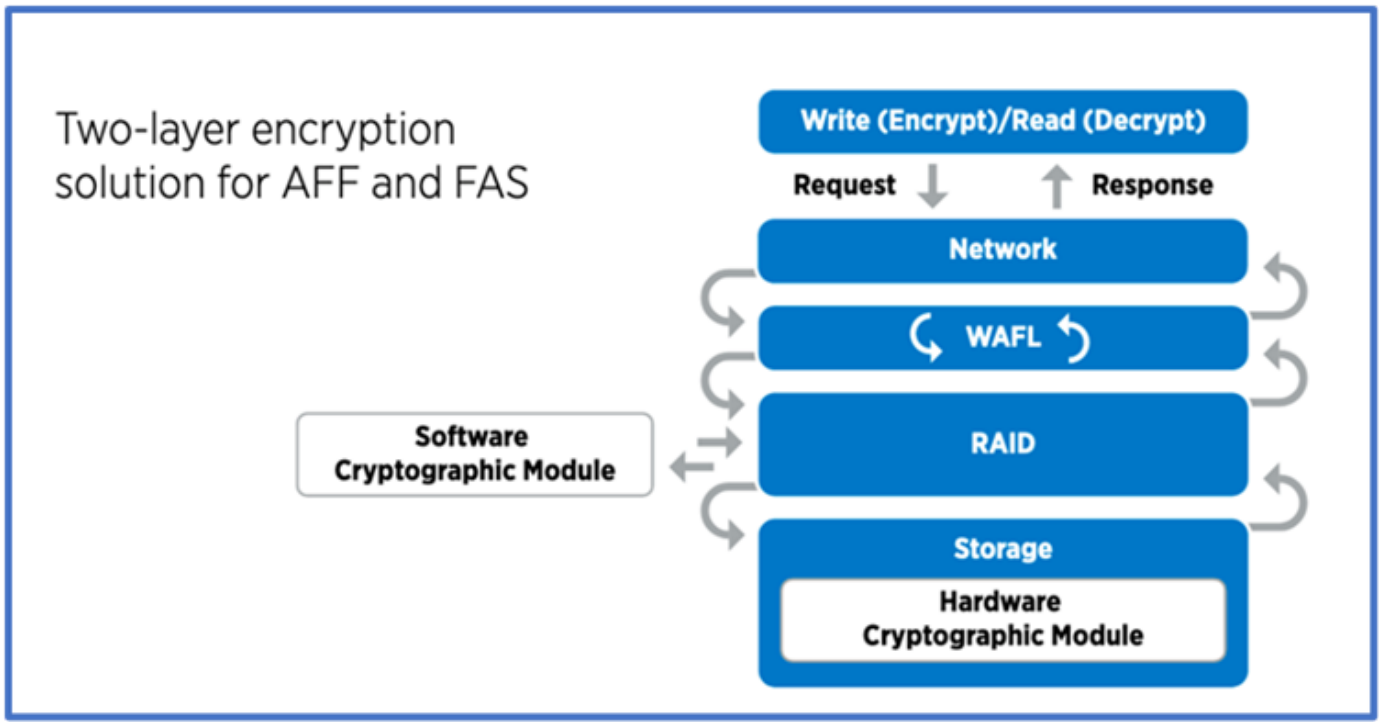
對靜止資料和正在傳輸的資料使用加密

靜態資料加密

每天都有新的要求、可在組織重新調整磁碟機用途、退回故障磁碟機、或透過銷售或交易方式升級到較大磁碟機時、降低儲存系統風險和基礎架構漏洞。 身為資料的管理員和操作者、儲存工程師必須在資料的整個生命週期內、安全地管理及維護資料。 "NetApp 儲存加密（ NSE ） ；#44 ； NetApp Volume 加密（ NVE ） ；#44 ；以及 NetApp Aggregate 加密" 協助您隨時加密所有資料、無論資料是否有毒、而且不會影響日常作業。 "NSE" 是 ONTAP 硬體 "靜態資料" 解決方案、使用 FIPS 140-2 第 2 級驗證的自我加密磁碟機。 "NVE 和 NAE" 是使用的 ONTAP 軟體 "靜態資料" 解決方案 "FIPS 140-2 第 1 級驗證 NetApp 密碼編譯模組"。有了 NVE 和 NAE 、硬碟或固態硬碟都可用於靜態資料加密。此外、 NSE 磁碟機也可用於提供原生的分層加密解決方案、提供加密備援和額外的安全性。如果有一層被破壞、則第二層仍會保護資料安全。這些功能讓 ONTAP 成為 "Quantum 就緒加密"的理想選擇。

NVE 也提供一項稱為的功能 "安全清除" 、可在將敏感檔案寫入非機密磁碟區時、以密碼方式移除資料外洩的有毒資料。

可將 "內建金鑰管理程式（OKM）"內建於 ONTAP 的金鑰管理員或協力廠商搭配 NSE 和 NVE 使用、以安全地儲存金鑰 "已核准" "外部金鑰管理員" 資料。



如上圖所示、可結合硬體和軟體型加密。這項功能可讓您 "將 ONTAP 驗證為 NSA 的商業解決方案、以供分類

方案使用" 儲存重要機密資料。

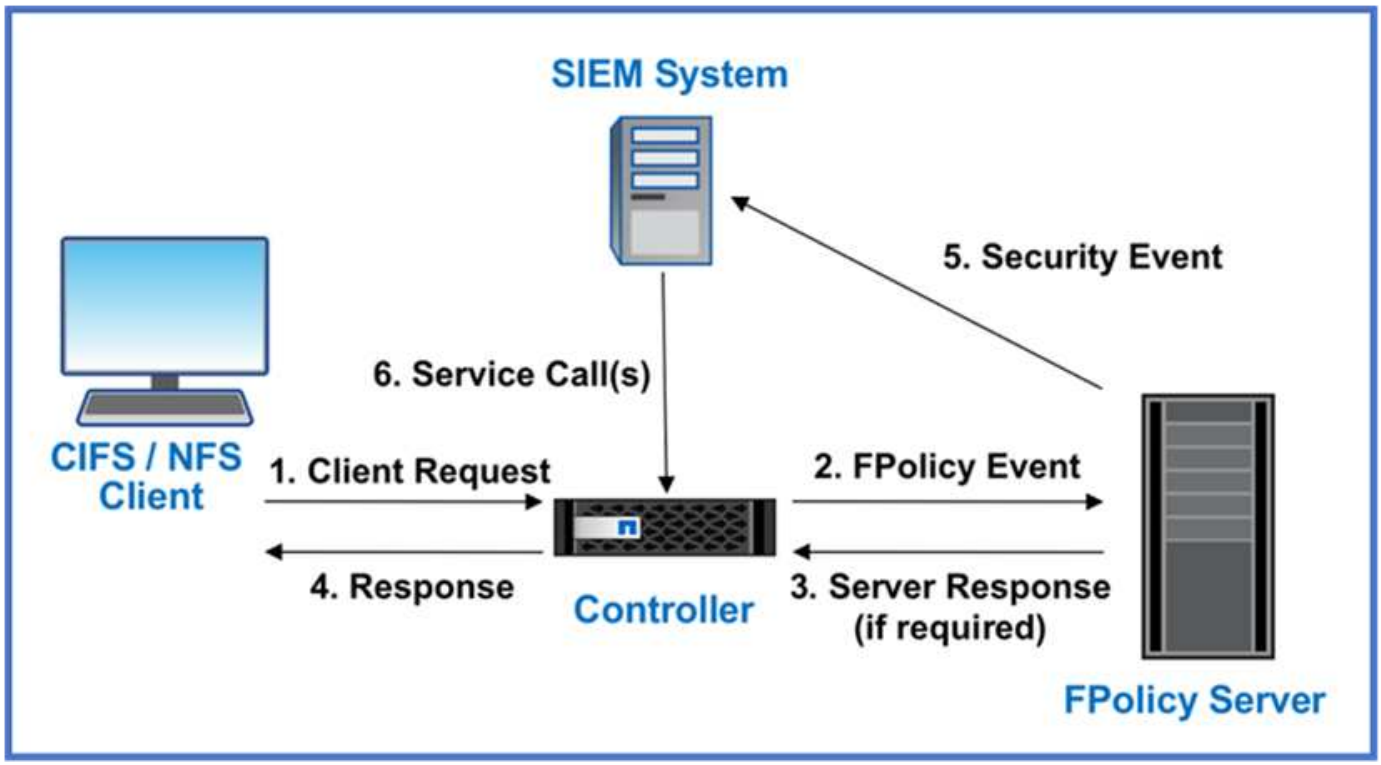
資料傳輸中加密

ONTAP 資料傳輸加密功能可保護使用者資料存取和控制面板存取。使用者資料存取可透過 SMB 3.0 加密來加密 Microsoft CIFS 共用存取、或透過 krb5P for NFS Kerberos 5 來加密。使用 CIFS 、 NFS 和 iSCSI 也可以加密使用者資料存取 "IPsec" 。控制平面存取是以傳輸層安全性（ TLS ）加密。ONTAP 提供"FIPS"控制平面存取的法規遵循模式，可啟用 FIPS 核准的演算法，並停用未經 FIPS 核准的演算法。資料複寫是使用加密 "叢集對等加密"的。這可為 ONTAP SnapVault 和 SnapMirror 技術提供加密。

監控並記錄所有存取

建立 RBAC 原則之後、您必須部署主動監控、稽核及警示。NetApp ONTAP 的 FPolicy Zero Trust Engine 搭配提供資料導向的 Zero "NetApp FPolicy 合作夥伴生態系統"Trust 模式所需的控制功能。NetApp ONTAP 是安全性豐富的資料管理軟體、 "FPolicy" 是領先業界的 ONTAP 功能、可提供精細的檔案型事件通知介面。NetApp FPolicy 合作夥伴可以使用此介面、在 ONTAP 中提供更多資料存取的照明。ONTAP 的 FPolicy 功能搭配 FPolicy 合作夥伴的 NetApp 聯盟合作夥伴生態系統、可讓您識別組織資料的存在位置、以及哪些人可以存取。這是透過使用者行為分析來完成、可識別資料存取模式是否有效。使用者行為分析可用於警示異常或可疑的資料存取、而這種存取方式不符合正常模式、並在必要時採取行動拒絕存取。

FPolicy 合作夥伴正從使用者行為分析轉向機器學習（ ML ）和人工智慧（ AI ）、以提高事件的逼真度、減少誤報（如果有）。所有事件都應記錄到 Syslog 伺服器或安全資訊與事件管理（ SIEM ）系統、而此系統也可以採用 ML 和 AI 。



NetApp 的 "DII 儲存工作負載安全"利用雲端和本地ONTAP儲存系統上的 FPolicy 介面和使用者行為分析，為您提供惡意使用者行為的即時警報。儲存工作負載安全性透過先進的機器學習和異常檢測保護組織資料不被惡意或受感染的使用者濫用。儲存工作負載安全性可以識別勒索軟體攻擊或其他惡意行為，呼叫快照並隔離惡意使用者。儲存工作負載安全性還具有取證功能，可以詳細查看使用者和實體活動。儲存工作負載安全性是NetAppData Infrastructure Insights的一部分。

除了儲存工作負載安全性之外、 ONTAP 還具備內建的勒索軟體偵測功能、稱為 "自主勒索軟體保護" （ ARP

）。ARP 會使用機器學習來判斷異常檔案活動是否表示勒索軟體攻擊正在進行中，並叫用快照並向系統管理員發出警示。儲存工作負載安全性與 ONTAP 整合、可接收 ARP 事件、並提供額外的分析和自動回應層。

如需有關本程序中所述命令"ONTAP 命令參照"的詳細資訊，請參閱。

ONTAP 外部的 NetApp 安全性自動化與協調控制

自動化功能可讓您以最少的人力協助來執行程序或程序。自動化功能可讓組織將 Zero Trust 部署規模擴充至遠超出手動程序的範圍、以抵禦同樣自動化的誤報活動。

Ansible 是開放原始碼軟體資源配置、組態管理及應用程式部署工具。它可以在許多類似 Unix 的系統上執行、而且可以同時設定類似 Unix 的系統和 Microsoft Windows 。其中包含自己的宣告語言、可用來描述系統組態。Ansible 由 Michael DeHaan 撰寫、並於 2015 年由 Red Hat 收購。Ansible 是無代理程式、可透過 SSH 或 Windows 遠端管理（允許遠端執行 PowerShell ）進行遠端連線以執行工作。NetApp 開發的不只是、還 "150 個適用於 ONTAP 軟體的 Ansible 模組"能進一步整合 Ansible 自動化架構。適用於 NetApp 的 Ansible 模組提供一組指示、說明如何定義所需的狀態、並將其轉送至目標 NetApp 環境。模組的設計可支援設定授權、建立集合體和儲存虛擬機器、建立磁碟區、以及還原快照等工作。Ansible 角色 "發表於 GitHub" 專屬於 NetApp DoD 統一化功能（ UC ）部署指南。

使用者可以利用可用模組庫輕鬆開發 Ansible 教戰手冊，並根據自己的應用程式和業務需求自訂這些手冊，以自動化日常工作。在撰寫教戰手冊之後、您可以執行該手冊來執行指定的工作、這樣可以節省時間並提高生產力。NetApp 已建立並共用範例教戰手冊、可直接使用或根據您的需求自訂。

Data Infrastructure Insights是一種基礎設施監控工具，可讓您了解完整的基礎架構。透過Data Infrastructure Insights，您可以監控、排除故障並最佳化所有資源，包括公有雲實例和私有資料中心。Data Infrastructure Insights可以將平均解決時間縮短 90%，並防止 80% 的雲端問題影響最終用戶。它還可以平均降低 33% 的雲端基礎設施成本，並透過使用可操作的情報來保護您的資料來減少您受到內部威脅的風險。Data Infrastructure Insights的儲存工作負載安全功能支援透過 AI 和 ML 進行使用者行為分析，以便在因內部威脅而出現異常使用者行為時發出警報。對於ONTAP，儲存工作負載安全使用零信任 FPolicy 引擎。

Zero Trust 與混合雲部署

NetApp是混合雲的資料權威。NetApp提供了多種選項，可透過 Amazon Web Services (AWS)、Microsoft Azure、Google Cloud 和其他領先的雲端供應商將內部部署資料管理系統擴展到混合雲。NetApp混合雲端解決方案支援與本機ONTAP系統和ONTAP Select軟體定義儲存相同的零信任安全控制。

您可以使用適用於 AWS（FSxN）、Google Cloud（GCNV）和適用於 Microsoft Azure 的Azure NetApp Files 的企業級雲端原生檔案服務，輕鬆擴展公有雲的容量，而不受典型的資本支出限制。這些雲端資料服務非常適合分析和 DevOps 等資料密集型工作負載，它將NetApp的彈性按需儲存即服務與ONTAP資料管理結合在一起，形成一個完全託管的產品。

ONTAP借助NetApp SnapMirror資料複製軟體，支援在本機ONTAP系統與 AWS、Google Cloud 或 Azure 儲存環境之間移動資料。