產品型錄

ONTAP 安全功能

確保「資料」這個世上最重要的資源安全無虞

NetApp® ONTAP® 資料管理軟體持續演進發展，其中安全性是此解決方案不可或缺的要素。最新版本的 ONTAP 包含許多新的安全功能，對貴組織具有重要價值，可協助保護組織的混合雲資料、防範勒索軟體攻擊，並嚴格遵循業界最佳實務做法。這些新功能也支援貴組織朝向零信任 (Zero Trust) 模式的方向發展。

如欲深入瞭解有關 ONTAP 解決方案的強化功能，請參閱《TR-4569：NetApp ONTAP 安全強化指南》（英文）。

挑戰

今日的企業正面臨數位化轉型的沉重壓力：企業需要有效管理整個混合雲中日漸分散、動態及多元的資料。威脅情境每天都變得更為精密複雜，使 IT 環境的危險性日漸升高。身為資料與資訊的系統管理員和營運者，您會期望 IT 團隊以安全方式，在整個資料生命週期內妥善管理及維護資料。

解決方案

NetApp ONTAP 軟體扮演核心角色，協助保護資料安全及遵循法規要求。本產品型錄及《TR-4569：NetApp ONTAP 安全強化指南》（英文）提供一些基本資訊，協助您為「資料」這個最重要的資源建立獲業界證實的安全態勢。

主要效益

強化資料機密性、完整性及可用度

ONTAP 混合雲安全技術可保護貴組織最重要的資源：資料。

強化貴組織的安全態勢

利用可保障基礎架構安全的可見度及安全功能，為貴組織的混合雲奠定安全基礎。

運用 NetApp 及業界最佳實務做法來因應安全需求及提供勒索軟體防護

藉助 NetApp 專家及產業知識，建立通過審查的安全足跡。

因應監管及法規遵循需求

利用既有的安全最佳實務做法，輕鬆遵循及支援業界規範與安全法規要求。

ONTAP 安全功能

軟體或功能	效用	影響
自動勒索軟體防護	自動勒索軟體防護為內建功能，透過機器學習來主動偵測及對抗攻擊。	如果偵測到異常情況，ONTAP 會自動製作 Snapshot 複本，並向系統管理員提出警示。
NetApp Snapshot™ 快照複本	ONTAP Snapshot 是高效的時間點唯讀資料複本，Snapshot 可確切呈現資料在建立 Snapshot 時的樣貌，不論是幾小時、幾天、幾週、幾個月、甚至幾年前建立的都沒問題。	由於 Snapshot 複本是唯讀的，因此不會受到勒索軟體影響，如果需要從勒索軟體攻擊中恢復，只要使用攻擊前建立的 Snapshot 就能輕鬆還原。
NetApp SnapLock® 技術	NetApp SnapLock 可實現真正無法消除的邏輯實體隔離備份，利用 NetApp SnapVault® 保護 Snapshot 快照複本。	SnapLock 可消除風險，避免 Snapshot 複本因人為錯誤遭系統管理員刪除、遭不滿的員工刪除，或是遭不良份子運用竊取的認證資料加以刪除。
Snapshot 快照複本鎖定	Snapshot 快照複本鎖定功能使用 SnapLock 技術，手動或自動將 Snapshot 快照設為在一段指定期間內不可刪除。	Snapshot 可能因人為錯誤遭系統管理員刪除、遭不滿的員工刪除，或是遭不良份子運用竊取的認證資料加以刪除。
NetApp FPolicy 技術	FPolicy 是 ONTAP 的一個基礎架構元件，允許合作夥伴應用程式監控及設定檔案存取權限。檔案政策是以檔案類型為基礎。FPolicy 可決定儲存系統如何處理來自個別用戶端系統的要求，例如建立、開啟、重新命名及刪除等操作。 附註：ONTAP 利用篩選控制及能對抗短暫網路停機的恢復能力，來強化 FPolicy 檔案存取通知架構。	存取控制是相當關鍵的安全建構，因此可見度以及回應檔案存取與檔案操作的能力，對於維護安全態勢至關重要。為了提供檔案的可見度及存取控制，ONTAP 解決方案使用 FPolicy 功能。包含 NetApp Cloud Insights / Cloud Secure 在內的外部 FPolicy 伺服器，會利用使用者行為分析來識別惡意軟體及勒索軟體，以減輕資料外洩範圍擴大的效應。
NetApp Volume Encryption (NVE)	NVE 是軟體型加密機制，可讓您利用每個 Volume 獨一無二的金鑰，在任何類型的磁碟上加密資料。	靜態資料加密仍是業界焦點，NVE 能夠滿足這項重點需求，同時也可在整個混合雲範圍內，維持強大的安全態勢。
NVE 安全清除	本功能透過一項指令，即可用密碼編譯的方式，銷毀刪除 NVE Volume 上的檔案，其方法是將良好的檔案搬至別處，然後刪除當初用來加密受感染檔案的金鑰。	您可在系統仍處於使用中狀態時，於線上修正資料外洩問題。本功能也提供頂尖的「刪除權」(right-to-erasure) 功能，以因應歐盟資料保護規範 (GDPR) 要求。
NetApp Aggregate Encryption (NAE)	NAE 是軟體型加密機制，可讓您針對橫跨數個已加密 Volume 的每個共享 Aggregate，使用獨一無二的金鑰來加密任何類型磁碟上的資料。	和 NVE 一樣，NAE 也能加密靜態資料。NAE 具備 Aggregate 重複資料刪除功能，又因為 Volume 在 Aggregate 之間共用金鑰，因此可提供更出色的儲存效率。

ONTAP 安全功能

軟體或功能	效用	影響
預設的靜態資料 (DAR) 加密	如果定義了外部金鑰管理程式或內建金鑰管理程式，就會啟用預設的 DAR 進行加密，可以是使用 NVE 或 NAE 軟體型加密機制。如果 NSE 磁碟機不是叢集組態的一部分，就會採用 DAR 加密，依預設將不使用軟體型加密。	預設的 DAR 加密能在整個混合雲範圍內，簡化並維護強大的安全態勢。
NetApp Storage Encryption (NSE)	NSE 是 NetApp 實作的全磁碟加密 (FDE) 機制，使用 FIPS-140-2 第 2 級自我加密磁碟機。此外 NSE 可提供不中斷營運的加密實作，支援全套 NetApp 儲存效率技術。	靜態資料加密仍是業界焦點，NSE 提供 FDE 以滿足這項重點需求。NetApp Data Fabric 可以端點對端點，維持強大的安全態勢。
SMB 加密使用 Intel AES New Instructions (AES-NI) 加速	Intel AES-NI 受支援的處理器系列可強化 AES 演算法，以加速資料加密。	加速安全功能可提升效率，高效使用資源則是提供成功安全解決方案的關鍵所在。
NetApp 密碼編譯安全模組	本模組可執行已通過 FIPS 140-2 驗證的密碼編譯，適用於特定安全通訊端層 (SSL) 型管理服務。自 ONTAP 9.11.1 及 TLS 1.3 支援開始，可進行 FIPS 140-2 驗證。	專用安全模組可提升資源效率。此外，FIPS 140 是密碼編譯產品及解決方案公認的產業標準。
NetApp CryptoMod	本模組可執行已通過 FIPS 140-2 驗證的密碼編譯，適用於 NVE、NAE 及內建金鑰管理程式 (OKM)。	FIPS 140-2 是密碼編譯產品及解決方案公認的產業標準。
SHA-2 (SHA-512) 支援	為了強化密碼安全性，ONTAP 支援 SHA-2 密碼雜湊功能，並預設使用 SHA-512 雜湊來新建或變更密碼。	SHA-2 已成為雜湊功能的產業標準，因為其安全態勢遠比經常遭到入侵的 SHA-1 標準更為出色。
安全日誌轉送（透過傳輸層安全性 [TLS] 轉送系統記錄）	日誌轉送功能可讓系統管理員配置目標或目的地系統，以便接收系統記錄與稽核資訊。由於系統記錄與稽核資訊均為安全保密性質，因此 ONTAP 會利用 TCP 加密參數，透過 TLS 安全地傳送資訊。	就支援及可用度觀點而言，日誌與稽核資訊對企業非常重要。此外日誌（系統記錄）、稽核報告及輸出資訊，一般而言在本質上都相當敏感。為了維護您的安全控制及安全態勢，您必須安全地管理日誌及稽核資料。
TLS 1.1 及 TLS 1.2	ONTAP 使用 TLS 1.1 及 TLS 1.2 提供安全通訊與管理功能。	NetApp 不建議使用 TLS 1.0，因為其中具有重大漏洞，不符合 PCI-DSS 等法規遵循標準。NetApp 基於強度及完整性等因素，建議使用 TLS 1.1 及 TLS 1.2。
線上認證狀態傳輸協定 (OCSP)	啟用 OCSP 時，使用 TLS 通訊（例如 LDAP 或 TLS）的 ONTAP 應用程式可擷取數位認證狀態。應用程式會收到經過簽署的回應，藉此掌握所要求的認證是處於良好、已撤銷或不明狀態。	OCSP 有助於判斷數位認證的目前狀態，而無需使用認證撤銷清單 (CRL)。
內建金鑰管理程式 (OKM)	ONTAP 的 OKM 為獨立加密解決方案，適用於靜態資料。OKM 可搭配 NVE 一起加密資料以提供軟體型加密機制，也可使用任何類型的磁碟。OKM 另可搭配 NSE，使用自我加密磁碟機來執行 FDE。	OKM 針對 NSE 及 NVE 提供金鑰管理功能。此外在 ONTAP 中使用此項加密技術，可確保靜態資料安全，提供重要的資料安全解決方案。
OKM 安全開機	本選項可在解除磁碟機鎖定時，以及在節點重新開機後解密 Volume 時，要求提供通關密碼。	NSE 及 NVE 如果使用 OKM，即可享有安全重新開機，在整個儲存陣列遭竊時提供保護，而非只保護磁碟機而已。這項功能也利於安全地實體運輸整個叢集，並讓設備安全返回。

ONTAP 安全功能

軟體或功能	效用	影響
外部金鑰管理	外部金鑰管理是在儲存環境中以協力廠商系統進行處理，該協力廠商系統能夠安全地管理儲存系統中用於加密功能的驗證金鑰與加密金鑰，例如 NSE、NVE 或 NAE。儲存系統使用 SSL 連線聯繫外部金鑰管理伺服器，然後透過金鑰管理互通性協定 (KMIP) 儲存及擷取驗證金鑰或 Volume 資料加密金鑰。	外部金鑰管理可讓您將貴組織的金鑰管理功能集中在一起，並確保金鑰不會儲存在資產附近，這種方法可降低遭到入侵的可能性。
安全的多租戶共享	安全多租戶共享是指在共享的實體儲存環境中使用安全的虛擬化分割區，以便讓多個不同租戶可以共用一個實體環境。在 ONTAP 之中，這些分割區稱為儲存虛擬機器 (SVM)。	安全多租戶共享功能可讓 ONTAP 做為共享平台，透過 SVM 在平台內部安全地隔離所有租戶。
多租戶外部金鑰管理	多租戶外部金鑰管理可讓個別租戶或儲存虛擬機器 (SVM)，透過適合 NVE 的 KMIP 來自行維護金鑰。	多租戶外部金鑰管理可讓您依據部門或租戶，將貴組織的金鑰管理功能集中在一起，並確保金鑰不會儲存在資產附近，這種方法可降低遭到入侵的可能性。
叢集式外部金鑰管理工具	將 NetApp KMIP 金鑰伺服器合作夥伴提供的各項功能叢集化，以支援外部 KMIP 伺服器備援機制。在 ONTAP 9.11.1 之前，最多可定義四個外部 KMIP 伺服器，ONTAP 將會寫入金鑰至各個伺服器以提供備援。	叢集式外部金鑰管理工具獲得 ONTAP 客戶廣泛採用，ONTAP 支援可讓這些客戶順利運用此項功能。
強化檔案系統稽核	ONTAP 在整體解決方案報告中，增加了稽核事件及詳細資料的數量。建立事件後即會記錄下列關鍵詳細資料： 檔案 資料夾 共用存取 已建立、修改或刪除的檔案 成功的檔案讀取存取 嘗試讀取欄位或寫入檔案失敗 資料夾權限變更	在現今備受威脅的環境中，NAS 檔案系統的地位日漸重要，因此前述稽核功能所提供的可見度仍是重要關鍵，而 ONTAP 中增加的稽核功能，可提供比之前更豐富的 CIFS 稽核詳細資料。
CIFS SMB 簽署及密封	SMB 簽署可協助保護 Data Fabric 安全性，在儲存系統與用戶端之間保護流量，避免遭受重播攻擊或中間人攻擊，也可確認 SMB 訊息使用有效的簽署。此外 ONTAP 可支援 SMB 加密，也就是所謂的密封。	檔案系統及架構的一項共同威脅因子就位在 SMB 傳輸協定之中，簽署及密封能夠真正驗證流量，並維護個別共用區的資料傳輸安全。
Kerberos 5 及 krb5p 支援	ONTAP 支援對 Kerberos 進行 128 位元及 256 位元的 AES 加密。隱私權服務包含驗證接收的資料完整性、使用者身分驗證，以及在傳輸前進行資料加密。	Krb5p 驗證利用 Checksum 加密用戶端與伺服器之間的所有流量，可保護資料不被竄改及窺探。
輕量型目錄存取通訊協定 (LDAP) SMB 簽署及密封	ONTAP 支援簽署及密封，以保護對 LDAP 伺服器查詢的工作階段安全性。	簽署是利用秘密金鑰技術來確認 LDAP 有效負載資料的完整性。密封可加密 LDAP 有效負載資料，避免以純文字格式傳輸敏感資訊。
安全殼層 (SSH) 中的 Ed25519 及 NIST 曲線（更新演算法及雜湊型方法驗證碼 [HMAC]）	ONTAP 提供更新的 SSH 密碼及金鑰交換機制，包括 AES、3DES、SHA-256 及 SHA-512。	隨著威脅情境持續演進發展，傳輸協定演算法、密碼及金鑰交換機制的強度，都對傳輸協定和產品功能的完整性至關重要。

ONTAP 安全功能

軟體或功能	效用	影響
能夠設定 SSH 登入嘗試失敗次數上限	ONTAP 可利用安全 SSH 修改指令，新增參數以驗證重試次數上限，藉此限制嘗試登入次數。每個 SSH 連線的預設上限為六次，不過 NetApp 建議使用三次做為安全最佳實務做法。	本功能可協助對抗暴力攻擊法。
多要素驗證 (MFA)	MFA 用於 NetApp ONTAP System Manager 及 NetApp Active IQ® Unified Manager，透過安全判定標示語言 (Security Assertion Markup Language，SAML) 及外部身分識別供應商來存取管理網路。ONTAP 透過本機的雙要素驗證方法來啟用管理命令列存取，以使用者 ID / 密碼及公共金鑰做為雙要素。您可將公共金鑰做為雙要素的其中一項，搭配 nsswitch 進行 SSH 命令列管理存取。若是使用 Yubikey 硬體授權裝置或其他 FIDO2 相容裝置進行 SSH 驗證，則也可以使用 FIDO2。	大部分系統的管理存取認證帳戶強度不足，很容易遭受入侵，有了 MFA 功能，就不可能透過簡易的密碼型帳戶取得管理存取權限。
NetApp SnapLock 技術搭配 NSE 及 NVE	ONTAP 支援 SnapLock 功能搭配 NSE 及 NVE 一起使用，可用於單寫多讀 (WORM) 資料的管理及儲存。	SnapLock 技術可建立特殊用途 Volume，將檔案儲存及指定為不可消除也不可寫入的狀態。SnapLock 可無限期保留此狀態，也可以指定保留期限，同時能維持 NSE 及 NVE 解決方案的安全態勢（加密）。
升級映像驗證	ONTAP 升級時會驗證映像是否為正版 ONTAP。	此項驗證會偵測升級過程中是否使用毀損或偽造的映像。
統一可延伸韌體介面 (UEFI) 安全開機	每次系統開機時都會進行映像驗證。	已簽署的 ONTAP 映像是由開機載入器驗證，可在每次開機時防止偽造映像。
叢集對等端點加密	叢集對等端點加密使用 TLS 1.2，在叢集對等端點及使用叢集對等端點複寫資料的基礎 ONTAP 功能（NetApp SnapMirror®、SnapVault®、FlexCache®）之間，加密透過實體線路傳輸的所有資料。	會複寫資料的 ONTAP 功能皆可使用這項傳輸中資料加密功能，此外，使用靜態資料加密 (NVE/NSE) 的客戶，可在使用叢集對等端點加密機制的 ONTAP 叢集之間，使用端點對端點加密功能。
網際網路傳輸協定安全性 (IPsec) 加密	網際網路傳輸協定安全性 (IPsec) 提供傳輸中資料加密功能，適用於所有 IP 流量，包括 NFS、iSCSI 及 SMB/CIFS 傳輸協定。	IPsec 可確保資料在傳輸過程中持續維持安全及加密狀態。其利用預防性措施來保護用戶端與 ONTAP 之間的網路流量，對抗重複攻擊和中間人 (MITM) 攻擊。
角色型存取控制 (RBAC)	ONTAP 角色型存取控制可讓系統管理員限制使用者的管理存取權，讓使用者只能存取授與其定義角色的層級。有了這項功能，系統管理員可依照使用者獲指派的角色來管理使用者。	存取控制是基礎要素，有助於建立安全態勢。角色型存取控制等功能，可協助企業組織決定哪些人擁有資料存取權，以及其存取範圍。這項功能可防止漏洞及入侵，包括資料外洩及權限提升等問題。
多管理員驗證 (MAV)	MAV 可防止單一叢集管理員在未經一位以上管理員核准的情況下，便執行「Volume Snapshot 快照刪除」或「Volume 刪除」等各項敏感指令。	MAV 可阻止惡意或遭入侵的管理員破壞寶貴資料，這是強化 ONTAP 資料導向零信任環境的必要功能。
防毒連接器（掃毒）	掃毒作業是在執行防毒連接器及防毒軟體的 Vscan 伺服器上執行，一般而言，執行 ONTAP 的系統是設定在遭到用戶端修改或存取時掃描檔案。	由於威脅及攻擊範圍持續成長，因此針對被存取或修改的檔案進行即時掃毒，有助於保護組織檔案的完整性。

ONTAP 安全功能

登入及當日訊息 (MOTD) 橫幅	登入橫幅會在進行身分驗證之前輸出顯示。組織及系統管理員可以透過這類橫幅，即時與系統使用者溝通。	登入橫幅可讓組織向操作者、系統管理員甚至不法分子，顯示條款與條件來指出可接受的系統使用方式，也可以使用這些橫幅來指出哪些人有權存取該系統。
磁碟資料抹除	磁碟資料抹除可讓您從磁碟或一組磁碟中徹底移除資料，讓資料永遠無法恢復。	安全傳輸協定通常會要求您讓資料無法從磁碟恢復，此項磁碟資料抹除功能就具有這樣的能力。

NetApp 台灣
台北市 110 信義區松仁路 97 號 8 樓之 2 電話 : 886 2 8729 5000 傳真 : 886 2 8729 5050

+1 877 263 8277