關於 NetApp 勒索軟體保護

ONTAP 9

NetApp
August 31, 2024

目錄

關於 NetApp 勒索軟體保護

勒索軟體和 NetApp 的保護產品組合

勒索軟體仍是 2024 年組織造成營運中斷的最重大威脅之一。根據 "Sophos State of 勒索軟體 2024"、勒索軟體攻擊影響了 72% 的受訪對象。勒索軟體攻擊已進化成更精密且目標明確、威脅行動者運用人工智慧等先進技術、將其影響和利潤最大化。

組織必須從周邊、網路、身分識別、應用程式、以及資料位於儲存層級的位置、查看整個安全狀態、並保護這些層級的安全。在現今的威脅環境中、在儲存層採用以資料為中心的網路保護方法是至關重要的。雖然沒有任何單一解決方案能阻擋所有攻擊、但使用包括合作夥伴關係和第三方在內的解決方案組合、可提供分層防禦。

NetApp 產品組合提供各種有效的工具來進行可見度、偵測和補救、協助您及早發現勒索軟體、防止散播、並在必要時快速恢復、以避免代價高昂的停機時間。傳統的分層防禦解決方案依然盛行、第三方和合作夥伴的可見度與偵測解決方案也同樣如此。有效的補救措施仍是回應任何威脅的關鍵部分。運用不可變的 NetApp Snapshot 技術和 SnapLock 邏輯空空缺解決方案的獨特產業方法、是一項產業差異化優勢、也是勒索軟體補救功能的最佳實務做法。

自 2024 年 7 月起、技術報告 _TR-4572 中的內容： NetApp 勒索軟體保護 _ （先前以 PDF 格式發佈）已與 ONTAP 產品文件的其餘部分整合。

資料是主要目標

網路犯罪者越來越直接鎖定資料、以辨識其價值。雖然周邊、網路和應用程式的安全性都很重要、但卻可以略過這些安全性。儲存層著重於保護資料來源、提供關鍵的最後防線。存取正式作業資料、加密或使其無法存取、是勒索軟體攻擊的目標。為了達到目標、攻擊者必須已經破解組織目前部署的現有防禦措施、從周邊環境到應用程式安全性。

[從周邊到資料安全的安全層]

可惜、許多組織並未充分利用資料層的安全功能。這就是 NetApp 勒索軟體保護產品組合的其中一項、可在最後一道防線上保護您的安全。

勒索軟體的實際成本

贖金本身並不是對企業造成最大的金錢影響。雖然這筆款項並不微不足道、但與遭受勒索軟體事件的停機成本相比、這筆款項卻很微不足道。

贖金付款只是處理勒索軟體事件時的一項回收成本要素。根據該 "2024 Sophos State of 勒索軟體"報告、 2024 年企業組織申報的勒索軟體攻擊平均回收成本為 2.73 萬美元、比 2023 年報告的 1.82 萬美元增加將近 100 萬美元。對於高度依賴 IT 可用度的組織、例如電子商務、股票交易和醫療保健、成本可能高出 10 倍以上。

網路保險成本也持續攀升、因為受到保險公司勒索軟體攻擊的可能性非常大。

資料層的勒索軟體保護

NetApp 瞭解您的安全態勢、從邊界到儲存層的資料所在、都是在整個組織中的廣泛且深入的。您的安全堆疊十分複雜、應該能在技術堆疊的每個層級提供安全性。

資料層的即時保護更為重要、而且有獨特的需求。為了有效運作、此層的解決方案必須提供以下關鍵屬性：

- * 設計上的安全性 * 可將成功攻擊的機率降至最低
- * 即時偵測與回應 * 、將成功攻擊的影響降到最低
- * 空中綁定 WORM 保護 * 可隔離關鍵資料備份
- * 單一控制飛機 * 提供全面的勒索軟體防禦

NetApp 可以提供所有這些功能、甚至更多功能。

[NetApp 勒索軟體保護產品組合、包含所述的關鍵屬性]

NetApp 的勒索軟體保護產品組合

NetApp "內建勒索軟體保護"為您的關鍵資料提供即時、強大、多面向的防禦功能。先進的 AI 驅動偵測演算法是其核心、可持續監控資料模式、以 99% 的準確度迅速識別可能的勒索軟體威脅。快速回應攻擊可讓我們的儲存設備快速建立資料快照、並保護複本的安全、確保快速恢復。

為了進一步強化資料、 NetApp 的"網路拖運"功能會將資料隔離在邏輯空氣間隙中。透過保護關鍵資料、我們可確保快速的業務持續運作。

NetApp "BlueXP 勒索軟體保護"可透過單一控制面板、以智慧方式協調及執行以工作負載為中心的端點對端點勒索軟體防禦、讓您只需按一下滑鼠、就能識別並保護關鍵工作負載資料、準確且自動地偵測並回應、以限制潛在攻擊的影響、並在幾分鐘內恢復工作負載、保護寶貴的工作負載資料、並將代價降至最低。

身為內建的原生 ONTAP 解決方案、"多重管理驗證（ MAV ）"可保護未經授權存取您的資料、並具備一組強大的功能、可確保刪除磁碟區、建立其他管理使用者或刪除快照複本等作業、只有在至少有第二位指定管理員核准之後才能執行。如此可防止遭到入侵、惡意或缺乏經驗的系統管理員進行不必要的變更或刪除資料。在刪除快照複本之前、您可以視需要設定任意數量的指定管理員核准者。

NetApp ONTAP 解決了 "多因素驗證（ MFA ）"在系統管理器中基於 Web 和 SSH CLI 驗證的要求。

NetApp 的勒索軟體保護功能可在不斷演變的威脅環境中、讓您高枕無憂。其全方位方法不僅能抵禦目前的勒索軟體變種、也能因應新興威脅、為您的資料基礎架構提供長期安全性。

瞭解其他保護選項

- "Active IQ 勒索軟體保護"
- "Cloud Insights 儲存工作負載安全（ CISWS ）"
- "FPolicy"
- "SnapLock 和防竄改快照複本"

勒索軟體恢復保證

NetApp 保證在發生勒索軟體攻擊時還原 Snapshot 資料。我們保證：如果我們無法協助您還原快照資料、我們會做對的。新購買的 AFF A 系列、 AFF C 系列、 ASA 和 FAS 系統均提供保證。

深入瞭解

- "恢復保證服務說明"

- "勒索軟體恢復保證部落格"。

相關資訊

- NetApp 支援網站資源頁面 http://mysupport.netapp.com/ontap/resources
- NetApp 產品安全性 https://security.netapp.com/resources/

SnapLock 和防竄改快照複本可保護勒索軟體

SnapLock 是 NetApp Snap Ar武庫 中的重要武器之一、它在防範勒索軟體威脅方面已獲證實相當有效。SnapLock 可防止未經授權的資料刪除、提供額外的安全層級、確保即使發生惡意攻擊、關鍵資料仍能保持完整且可存取。

符合法規SnapLock

SnapLock Compliance （ SLC ）為您的資料提供不可磨滅的保護。即使系統管理員嘗試重新初始化陣列、 SLC 也會禁止刪除資料。與其他競爭產品不同、 SnapLock Compliance 不易透過這些產品的支援團隊而遭受社會工程駭客攻擊。受 SnapLock Compliance Volume 保護的資料可在資料到達到期日之前恢復。

若要啟用 SnapLock 、"ONTAP One"則需要授權。

深入瞭解

- "SnapLock 文件"

可防竄改的Snapshot複本

防竄改 Snapshot （ TPS ）複本提供了一種方便且快速的方法、可保護資料免受惡意行為的侵害。與 SnapLock Compliance 不同的是、 TPS 通常用於主要系統、使用者可以在確定的時間內保護資料、並將資料留在本機以進行快速恢復、或不需要將資料從主要系統複寫。TPS 使用 SnapLock 技術、即使 ONTAP 管理員使用相同的 SnapLock 保留到期期間、也無法刪除主快照複本。即使磁碟區未啟用 SnapLock 、也無法刪除快照複本、不過快照與 SnapLock Compliance 磁碟區的性質並不相同。

若要製作防竄改的 Snapshot 複本"ONTAP One"、必須取得授權。

深入瞭解

- "鎖定快照複本以防止勒索軟體攻擊"。

FPolicy 檔案封鎖

FPolicy 可防止不想要的檔案儲存在企業級儲存設備上。FPolicy 也可讓您封鎖已知的勒索軟體副檔名。使用者仍擁有主資料夾的完整存取權限、但 FPolicy 不允許使用者儲存管理員標記為封鎖的檔案。無論這些檔案是 MP3 檔案或已知的勒索軟體副檔名、都沒問題。

使用 FPolicy 原生模式封鎖惡意檔案

NetApp FPolicy 原生模式（名稱的進化、檔案原則）是檔案副檔名封鎖架構、可讓您封鎖不想要的檔案副檔名、使其無法進入您的環境。這是 ONTAP 十多年來的一部分、在協助您防範勒索軟體方面非常有用。這款 Zero Trust 引擎非常實用、因為除了存取控制清單（ ACL ）權限之外、您還能獲得額外的安全措施。

在 ONTAP 系統管理員和 BlueXP 中、有超過 3000 個副檔名的清單可供參考。

> 某些擴充功能在您的環境中可能是合法的、而封鎖這些擴充功能可能會導致非預期的問題。在設定原生 FPolicy 之前、請先建立適合您環境的清單。

所有 ONTAP 授權均包含 FPolicy 原生模式。

深入瞭解

- "部落格：對抗勒索軟體：第三部分： ONTAP FPolicy 、另一個強大的原生（又稱為免費）工具"

使用 **FPolicy** 外部模式啟用使用者和實體行為分析（ **UEBA** ）

FPolicy 外部模式是檔案活動通知和控制架構、可提供檔案和使用者活動的可見度。外部解決方案可使用這些通知來執行 AI 型分析、以偵測惡意行為。

也可以將 FPolicy 外部模式設定為等待 FPolicy 伺服器核准、再允許特定活動通過。這樣的多個原則可在叢集上進行設定、提供您極大的彈性。

> 如果設定為提供核准、 FPolicy 伺服器必須回應 FPolicy 要求；否則、儲存系統效能可能會受到負面影響。

FPolicy 外部模式包含在"所有 ONTAP 授權"中。

深入瞭解

- "部落格：對抗勒索軟體：第四部分：使用 FPolicy 外部模式的 UBA 和 ONTAP 。"

Cloud Insights 儲存工作負載安全（ CISWS ）

儲存工作負載安全性（ SWS ）是 NetApp Cloud Insights 的一項功能、可大幅提升 ONTAP 環境的安全狀態、可恢復性和責任歸屬。SWS 採用以使用者為中心的方法、追蹤環境中每位已驗證使用者的所有檔案活動。它使用進階分析功能、為每位使用者建立正常和季節性的存取模式。這些模式可用來快速識別可疑行為、而無需勒索軟體簽章。

當 SWS 偵測到可能的勒索軟體、資料刪除或竊取攻擊時、它可以採取自動行動、例如：

- 拍攝受影響磁碟區的快照。
- 封鎖疑似惡意活動的使用者帳戶和 IP 位址。
- 傳送警示給管理員。

由於 SWS 可以採取自動化行動來快速阻止內部威脅、並追蹤每個檔案活動、因此從勒索軟體事件中恢復的過程更簡單、更快。內建進階稽核和鑑識工具、使用者可以立即查看哪些磁碟區和檔案受到攻擊、攻擊來自哪個使用者帳戶、以及執行了哪些惡意動作。自動快照可減輕損害並加速檔案還原。

[Cloud Insights 儲存工作負載安全攻擊的結果]

ONTAP 的自主勒索軟體保護（ ARP ）所發出的警示也會顯示在 SWS 中、為同時使用 ARP 和 SWS 的客戶提供單一介面、以防止勒索軟體攻擊。

深入瞭解

- "NetApp Cloud Insights"

NetApp ONTAP 內建的內建 AI 型偵測與回應功能

隨著勒索軟體威脅越來越複雜、您的防禦機制也越來越複雜。NetApp 的自動勒索軟體保護（ ARP ）是由 AI 提供、內建於 ONTAP 的智慧型異常偵測功能。開啟此功能、為您的網路恢復能力增添另一層防禦。

ARP 和 ARP/AI 可透過 ONTAP 內建管理介面、系統管理員進行設定、並以每個磁碟區為基礎啟用。

自主勒索軟體保護（Arp）

自主勒索軟體保護（ ARP ）是自 9.10.1 起的另一個原生內建 ONTAP 解決方案、從 NAS 儲存磁碟區工作負載檔案活動和資料 Entropy 來自動偵測潛在的勒索軟體。ARP 為系統管理員提供即時偵測、洞見和資料還原點、提供前所未有的隨裝即用勒索軟體偵測功能。

對於支援 ARP 的 ONTAP 9 ・ 15.1 版和更早版本、 ARP 會以學習模式開始學習一般工作負載資料活動。對於大多數環境而言、這可能需要七天的時間。學習模式完成後、 ARP 會自動切換至使用中模式、並開始尋找可能是勒索軟體的異常工作負載活動。

如果偵測到異常活動、就會立即擷取自動快照複本、以最少受感染的資料、盡可能提供最接近攻擊時間的還原點。同時、系統會產生自動警示（可設定）、讓系統管理員能夠查看異常的檔案活動、以便判斷該活動是否確實是惡意活動、並採取適當的行動。

如果活動是預期的工作負載、管理員可以輕鬆地將其標示為誤判。ARP 會將這項變更視為正常的工作負載活動、不再將其標示為潛在的未來攻擊。

若要啟用 ARP 、"ONTAP One"需要授權。

深入瞭解

- "自主勒索軟體保護"

自主勒索軟體保護 /AI （ ARP/AI ）

ARP/AI 在 ONTAP 9 15.1 中推出技術預覽、將 NAS 儲存系統的隨裝即時偵測功能帶入更高層級。全新 AI 驅動的偵測技術已針對超過一百萬個檔案和各種已知的勒索軟體攻擊進行訓練。除了 ARP 中使用的訊號之外、 ARP/AI 也會偵測標頭加密。AI 電源和額外訊號可讓 ARP/AI 提供超過 99% 的偵測準確度。SE Labs 已驗證這項功能、這是一項可給予 ARP/AI 最高 AAA 評等的測試實驗室。

由於模型持續在雲端進行訓練、因此 ARP/AI 不需要學習模式。它會在開啟時作用。持續訓練也意味著 ARP/AI 一律會在發生新的勒索軟體攻擊類型時加以驗證。ARP/AI 也隨附自動更新功能、可為所有客戶提供新參數、讓勒索軟體偵測功能保持在最新狀態。ARP 的所有其他偵測、洞見和資料恢復點功能、都會保留給 ARP/AI 。

若要啟用 ARP/AI 、"ONTAP One"需要授權。

深入瞭解

- "部落格： NetApp 的 AI 即時勒索軟體偵測解決方案達到 AAA 評等"

利用網路拖運技術提供空中綁帶式 **WORM** 保護

NetApp 的網路資料保險箱方法是專為邏輯上無線網路資料保險箱所打造的參考架構。這種方法利用安全強化和法規遵循技術（例如 SnapLock ）來實現不可改變和難以磨滅的快照。

使用 **SnapLock Compliance** 進行網路鏈接、並在邏輯上造成空氣落差

攻擊者越來越傾向於破壞備份複本、在某些情況下甚至加密這些複本。因此網路安全產業中有許多人建議將氣隙備份作為整體網路恢復策略的一部分。

問題在於傳統的空缺（磁帶和離線媒體）可能會大幅增加還原時間、進而增加停機時間和整體相關成本。即使採用更現代化的方法來解決空缺問題、也可能是問題所在。例如、如果備份資料保險箱暫時開啟以接收新的備份複本、然後中斷與主要資料的網路連線、再次「無線搭接」、攻擊者就可以利用暫時的開啟。在連線上線期間、攻擊者可能會攻擊以破壞或破壞資料。這類組態通常也會增加不必要的複雜度。邏輯氣隙是傳統或現代氣隙的絕佳替代品、因為它有相同的安全保護原則、同時保持備份在線上。有了 NetApp 、您就能解決磁帶或磁碟氣在邏輯氣帶上的複雜性、這可以透過不可變的快照複本和 NetApp SnapLock Compliance 來達成。

[與 NetApp 網路資料保險箱的邏輯空空缺]

NetApp 在 10 多年前推出 SnapLock 功能、以因應資料法規遵循的要求、例如健康保險可攜性與責任法案（ HIPAA ）、沙賓法案（ arbanes-Oxlei ）及其他法規資料規則。您也可以將主要快照複本儲存至 SnapLock 磁碟區、以便將複本提交至 WORM 、避免刪除。有兩個 SnapLock 授權版本： SnapLock Compliance 和 SnapLock Enterprise 。為了保護勒索軟體、 NetApp 建議您使用 SnapLock Compliance 、因為您可以設定特定的保留期間、在此期間、即使是 ONTAP 管理員或 NetApp 支援人員、快照複本也會被鎖定且無法刪除。

深入瞭解

- "部落格： NetApp 的網路資料保險箱解決方案提供分層勒索軟體保護"

防竄改快照複本

雖然利用 SnapLock Compliance 作為邏輯間距、可提供終極保護、防止攻擊者刪除備份複本、但您必須使用 SnapVault 將快照複本移至啟用 SnapLock 的次要磁碟區。因此、許多客戶都會在整個網路的次要儲存設備上部署此組態。相較於在主要儲存設備上還原主要 Volume Snapshot 複本、這可能會導致更長的還原時間。

從 ONTAP 9 · 12.1 開始、防竄改快照複本可在主要儲存設備和主要磁碟區上、提供近乎 SnapLock Compliance 層級的快照複本保護。不需要使用 SnapVault 將快照複本儲存至次要 SnapLoced Volume 。防竄改的快照複本使用 SnapLock 技術、即使是由完整的 ONTAP 管理員使用相同的 SnapLock 保留期限、也能防止主快照複本遭到刪除。如此可加快還原時間、並能使用防竄改、受保護的快照複本來備份 FlexClone Volume 、這是傳統 SnapLock Compliance 資料保險箱 Snapshot 複本所無法做到的事。

SnapLock Compliance 與防竄改快照複本之間的主要差異在於、如果 SnapLock Compliance 磁碟區存在尚未達到到期日的拱形 Snapshot 複本、則 SnapLock Compliance 不允許初始化及清除 ONTAP 陣列。若要使 Snapshot 複本防竄改、必須取得 SnapLock Compliance 授權。

深入瞭解

- "鎖定快照複本以防止勒索軟體攻擊"

Active IQ 勒索軟體保護

NetApp Active IQ 是一位數位顧問、透過可據以行動的情報、簡化 NetApp 儲存設備的主動式照護與最佳化、以實現最佳的資料管理。由我們高度多樣化安裝基礎的遙測資料所驅動、它使用先進的 AI 和 ML 技術來發掘降低風險的機會、並改善儲存環境的效能和效率。

不僅能 "NetApp Active IQ" "消除安全漏洞"提供協助、還能提供專為保護免受勒索軟體攻擊而提供的深入見解與指引。專屬的健康卡片會顯示所需的行動和所解決的風險、因此您可以確保系統符合這些最佳實務建議。

[NetApp Active IQ 儀表板上的健康監控器]

在勒索軟體「國防健康」頁面上追蹤的風險和行動包括下列（以及更多）：

- Volume Snapshot 複本數低、降低了勒索軟體的潛在保護。
- FPolicy 未針對所有針對 NAS 傳輸協定設定的儲存虛擬機器（ SVM ）啟用。

若要查看 Active IQ 勒索軟體保護的實際運作情形、請參閱"NetApp Active IQ"。

BlueXP 勒索軟體保護提供全方位的恢復能力

請務必儘早進行勒索軟體偵測、以防止擴散並避免代價高昂的停機。然而、有效的勒索軟體偵測策略應涵蓋單一層以上的保護。NetApp 的勒索軟體保護採用全方位的方法、包括即時的隨裝功能、使用 BlueXP 延伸至資料服務、以及用於網路拖運的隔離式分層解決方案。

BlueXP 勒索軟體保護

BlueXP 是單一控制面板、可智慧地協調以工作負載為中心的完整勒索軟體防禦。BlueXP 勒索軟體保護功能結合了 ONTAP 強大的網路恢復功能、例如 ARP 、 FPolicy 和防竄改快照、以及 BlueXP 資料服務、例如 BlueXP 備份與還原。此外、它也會新增自動化工作流程的建議和指引、透過單一 UI 提供端點對端點的防禦。它會在工作負載層級運作、以確保執行業務的應用程式受到保護、並在發生攻擊時儘快恢復。

[BlueXP 勒索軟體保護是一項以 AI 為基礎的情報與協助、可將工作負載資料遺失和快速恢復降至最低。此影像顯示 BlueXP UI 。]

客戶效益：

- 輔助勒索軟體準備工作可減少營運成本並提高效率
- 以 AI / ML 為動力的異常狀況偵測功能可提供更高的準確度、並更快地因應風險
- 引導式應用程式一致的還原可讓您更輕鬆地在幾分鐘內恢復工作負載

"BlueXP 勒索軟體保護"讓這些 NIST 功能更容易達成：

- 自動 * 探索 * 並優先處理 NetApp 儲存設備中的資料 * 、重點放在最重要的應用程式型工作負載 * 上。
- * 一鍵保護 * 、可執行工作負載最高的資料備份、不可變更、安全組態、惡意檔案封鎖及不同的安全網域。
- * 使用 * 次世代 AI 型異常偵測、 * 盡可能 * 快速 * 精確偵測 * 勒索軟體。 *
- 自動化回應與工作流程、並與頂尖 * SIEM 與 XDR 解決方案整合。 *

- 使用簡化的 * 協調式恢復 * 來快速恢復資料、以加速應用程式正常運作時間。
- 實施勒索軟體保護 * 策略 * 和 * 政策 * 、以及 * 監控成果 * 。