版本資訊

BlueXP ransomware protection

NetApp
December 20, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/bluexp-ransomware-protection/whats-new.html on December 20, 2024. Always check docs.netapp.com for the latest.

目錄

版本資訊

BlueXP 勒索軟體保護的新功能

瞭解 BlueXP 勒索軟體保護的新功能。

2024 年 16 月 12 日

使用 **Data Infrastructure Insights Storage Workload Security** 偵測異常的使用者行為

在此版本中，您可以使用 Data Infrastructure Insights Storage Workload Security 來偵測儲存工作負載中異常的使用者行為。此功能可協助您識別潛在的安全威脅，並封鎖潛在的惡意使用者，以保護您的資料。

如需詳細資訊、請 "回應偵測到的勒索軟體警示"參閱。

在使用 Data Infrastructure Insights Storage Workload Security 偵測異常使用者行為之前，您必須先使用 BlueXP 勒索軟體保護 * 設定 * 選項來設定選項。

請參閱 "設定 BlueXP 勒索軟體保護設定"。

選取要探索及保護的工作負載

使用此版本，您現在可以執行下列動作：

- 在每個 Connector 中，選取您要探索工作負載的工作環境。如果您想要保護環境中的特定工作負載，而非其他工作負載，您可能會受益於此功能。
- 在工作負載探索期間，您可以針對每個 Connector 自動探索工作負載。此功能可讓您選取要保護的工作負載。
- 探索先前所選工作環境的新建立工作負載。

請參閱 "探索工作負載"。

2024 年 11 月 7 日

啟用資料分類，並掃描個人識別資訊（ **PII** ）

在此版本中，您可以啟用 BlueXP 分類，這是 BlueXP 系列的核心元件，來掃描及分類檔案共用工作負載中的資料。分類資料有助於識別資料是否包含個人或私人資訊、進而增加安全風險。此程序也會影響工作負載的重要性，並協助您確保以適當的保護層級來保護工作負載。

部署 BlueXP 分類的客戶通常可以使用 BlueXP 勒索軟體保護來掃描 PII 資料。BlueXP 分類是 BlueXP 平台的一部分，不需額外付費，可在內部部署或客戶雲端部署。

請參閱 "設定 BlueXP 勒索軟體保護設定"。

若要開始掃描，請在「保護」頁面上，按一下「隱私權曝險」欄位中的 * 識別曝光 * 。

"使用 BlueXP 分類掃描個人識別敏感資料"。

SIEM 與 **Microsoft Sentinel** 整合

您現在可以使用 Microsoft Sentinel 將資料傳送至安全與事件管理系統（ SIEM ），以進行威脅分析與偵測。以前，您可以選擇 AWS Security Hub 或 Splunk Cloud 做為 SIEM 。

"深入瞭解如何設定 BlueXP 勒索軟體保護設定"。

30 天免費試用

在此版本中， BlueXP 勒索軟體保護的新部署現在有 30 天免費試用。以前， BlueXP 勒索軟體保護提供 90 天免費試用期。如果您已經參加 90 天免費試用，該方案將持續 90 天。

在 **Podman** 的檔案層級還原應用程式工作負載

在檔案層級還原應用程式工作負載之前，您現在可以檢視可能受到攻擊影響的檔案清單，並識別您要還原的檔案。以前，如果組織中的 BlueXP Connectors （前身為帳戶）使用 Podman ，則此功能已停用。現在已啟用 Podman 。您可以讓 BlueXP 勒索軟體保護選擇要還原的檔案、上傳 CSV 檔案來列出受警示影響的所有檔案、或手動識別要還原的檔案。

"深入瞭解如何從勒索軟體攻擊中恢復"。

2024 年 9 月 30 日

自訂檔案共用工作負載群組

有了這個版本，您現在可以將檔案共用分組，讓您更容易保護資料資產。此服務可同時保護群組中的所有磁碟區。以前、您需要分別保護每個磁碟區。

"深入瞭解如何在勒索軟體保護策略中將檔案共用工作負載分組"。

2024 年 9 月 2 日

Digital Advisor 的安全風險評估

BlueXP 勒索軟體保護現在可從 NetApp 數位顧問收集與叢集相關的高關鍵安全風險資訊。如果發現任何風險、 BlueXP 勒索軟體保護會在儀表板的 * 建議動作 * 窗格中提供建議：「修正叢集 <name> 上的已知安全性弱點。」在儀表板上的建議中、按一下 * 檢閱與修正 * 、建議檢閱 Digital Advisor 和常見弱點（ CVE ）文章、以解決安全性風險。如果存在多種安全風險、請檢閱 Digital Advisor 中的資訊。

請參閱 "數位顧問文件"。

備份至 **Google Cloud Platform**

透過此版本，您可以將備份目的地設定為 Google Cloud Platform 儲存庫。之前、您只能將備份目的地新增至 NetApp StorageGRID 、 Amazon Web Services 和 Microsoft Azure 。

"深入瞭解如何設定 BlueXP 勒索軟體保護設定"。

支援 **Google Cloud Platform**

這項服務現在支援 Cloud Volumes ONTAP for Google Cloud Platform 以保護儲存設備。此服務先前僅支援 Amazon Web Services 和 Microsoft Azure 的 Cloud Volumes ONTAP 、以及內部部署的 NAS 。

"瞭解 BlueXP 勒索軟體保護及支援的資料來源、備份目的地及工作環境"。

角色型存取控制

您現在可以使用角色型存取控制（ RBAC ）來限制特定活動的存取。BlueXP 勒索軟體保護使用兩種 BlueXP 角色： BlueXP 帳戶管理員和非帳戶管理員（檢視器）。

如需每個角色可執行之動作的詳細資訊，請參閱 "角色型存取控制 Privileges"。

2024 年 8 月 5 日

使用 **Splunk Cloud** 偵測威脅

您可以自動將資料傳送至安全與事件管理系統（ SIEM ）、以進行威脅分析與偵測。在先前的版本中、您只能選擇 AWS Security Hub 做為 SIEM 。在此版本中、您可以選擇 AWS Security Hub 或 Splunk Cloud 做為您的 SIEM 。

"深入瞭解如何設定 BlueXP 勒索軟體保護設定"。

2024 年 7 月 1 日

自帶授權（ **BYOL** ）

在此版本中，您可以使用 BYOL 授權，這是您從 NetApp 銷售代表處取得的 NetApp 授權檔案（ NLF ）

"深入瞭解設定授權"。

在檔案層級還原應用程式工作負載

在檔案層級還原應用程式工作負載之前，您現在可以檢視可能受到攻擊影響的檔案清單，並識別您要還原的檔案。您可以讓 BlueXP 勒索軟體保護選擇要還原的檔案、上傳 CSV 檔案來列出受警示影響的所有檔案、或手動識別要還原的檔案。

在此版本中、如果帳戶中的所有 BlueXP Connector 都未使用 Podman 、則會啟用單一檔案還原功能。否則、該帳戶將停用此功能。

"深入瞭解如何從勒索軟體攻擊中恢復"。

下載受影響檔案的清單

在檔案層級還原應用程式工作負載之前，您現在可以存取「警示」頁面，下載 CSV 檔案中受影響檔案的清單，然後使用「恢復」頁面上傳 CSV 檔案。

"深入瞭解如何在還原應用程式之前下載受影響的檔案"。

刪除保護計畫

有了這次版本，您現在可以刪除勒索軟體保護策略。

"深入瞭解如何保護工作負載及管理勒索軟體保護策略"。

2024 年 6 月 10 日

主儲存設備上的 **Snapshot** 複本鎖定

啟用此選項可鎖定主要儲存設備上的 Snapshot 複本，即使勒索軟體攻擊管理其通往備份儲存目的地的方式，也無法在一段時間內修改或刪除它們。

"深入瞭解如何保護工作負載、並在勒索軟體保護策略中啟用備份鎖定功能"。

支援 **Cloud Volumes ONTAP for Microsoft Azure**

此版本除了支援 Cloud Volumes ONTAP for AWS 和內部部署 ONTAP NAS 之外，還支援 Cloud Volumes ONTAP for Microsoft Azure 做為工作環境。

"Azure中的功能快速入門Cloud Volumes ONTAP"

"瞭解 BlueXP 勒索軟體保護"。

Microsoft Azure 新增為備份目的地

您現在可以將 Microsoft Azure 新增為 AWS 和 NetApp StorageGRID 的備份目的地。

"深入瞭解如何設定保護設定"。

2024 年 5 月 14 日

授權更新

您可以註冊 90 天免費試用。您很快就能向 Amazon Web Services Marketplace 購買隨用隨付訂閱、或是自行攜帶 NetApp 授權。

"深入瞭解設定授權"。

CIFS 傳輸協定

此服務現在支援 AWS 工作環境中使用 NFS 和 CIFS 通訊協定的內部部署 ONTAP 和 Cloud Volumes ONTAP 。舊版僅支援 NFS 傳輸協定。

工作負載詳細資料

此版本現在提供更多有關保護和其他頁面的工作負載資訊，以改善工作負載保護評估。從工作負載詳細資料中、您可以檢閱目前指派的原則、並檢閱設定的備份目的地。

"如需檢視工作負載詳細資料的詳細資訊、請參閱保護頁面"。

應用程式一致且 **VM** 一致的保護與還原

您現在可以使用 NetApp SnapCenter 軟體執行應用程式一致的保護，並使用適用於 VMware vSphere 的 SnapCenter 外掛程式執行 VM 一致的保護，達到靜態且一致的狀態，以避免日後需要恢復時可能發生的資料遺失。如果需要恢復、您可以將應用程式或 VM 還原回任何先前可用的狀態。

"深入瞭解如何保護工作負載"。

勒索軟體保護策略

如果工作負載上不存在 Snapshot 或 Backup 原則，您可以建立勒索軟體保護策略，其中可能包含您在此服務中建立的下列原則：

- Snapshot原則
- 備份原則
- 偵測原則

"深入瞭解如何保護工作負載"。

威脅偵測

現在可使用第三方安全性與事件管理（ SIEM ）系統來啟用威脅偵測。儀表板現在會顯示「啟用威脅偵測」的新建議、您可以在「設定」頁面上設定。

"深入瞭解設定選項的設定"。

消除誤報警示

您現在可以從「警示」索引標籤中排除誤報，或決定立即恢復資料。

"深入瞭解如何回應勒索軟體警示"。

偵測狀態

「保護」頁面上會出現新的偵測狀態，顯示套用至工作負載的勒索軟體偵測狀態。

"深入瞭解如何保護工作負載及檢視保護狀態"。

下載 **CSV** 檔案

您可以從「保護」，「警示」和「恢復」頁面下載 CSV 檔案 * 。

"深入瞭解如何從儀表板和其他頁面下載 CSV 檔案"。

文件連結

檢視文件連結現在已包含在 UI 中。您可以從儀表板垂直 * 動作 * 選項存取此文件  。選取 * 新功能 * 以檢視版本說明中的詳細資料、或 * 文件 * 以檢視 BlueXP 勒索軟體保護文件首頁。

BlueXP 備份與還原

BlueXP 備份與還原服務不再需要在工作環境中啟用。請參閱。 "先決條件"BlueXP 勒索軟體保護服務可透過「設定」選項協助設定備份目的地。請參閱。 "設定"

設定選項

您現在可以在 BlueXP 勒索軟體保護設定中設定備份目的地。

"深入瞭解設定選項的設定"。

2024 年 3 月 5 日

保護原則管理

除了使用預先定義的原則之外，您現在還可以建立原則。 "深入瞭解管理原則"。

二級儲存設備上的不可變性（ **DataLock** ）

您現在可以使用物件存放區中的 NetApp DataLock 技術，在次要儲存區中製作不可變的備份。 "深入瞭解如何建立保護原則"。

自動備份至 **NetApp StorageGRID**

除了使用 AWS 之外，您現在還可以選擇 StorageGRID 做為備份目的地。 "深入瞭解設定備份目的地"。

調查潛在攻擊的其他功能

您現在可以檢視更多鑑識詳細資料，以調查偵測到的潛在攻擊。 "深入瞭解如何回應偵測到的勒索軟體警示"。

恢復程序

恢復程序已增強。現在，您可以針對工作負載，依磁碟區或所有磁碟區來恢復磁碟區。 "深入瞭解如何從勒索軟體攻擊中恢復（在事件被消除之後）"。

"瞭解 BlueXP 勒索軟體保護"。

2023 年 10 月 6 日

BlueXP 勒索軟體保護服務是 SaaS 解決方案、可保護資料、偵測潛在攻擊、以及從勒索軟體攻擊中恢復資料。

對於預覽版本、此服務可保護 Oracle 、 MySQL 、 VM 資料存放區、內部部署 NAS 儲存設備上檔案共用的應用程式型工作負載、以及跨 BlueXP 組織的 Cloud Volumes ONTAP on AWS （使用 NFS 傳輸協定）、並將資料備份至 Amazon Web Services 雲端儲存設備。

BlueXP 勒索軟體保護服務可充分運用多項 NetApp 技術、讓您的資料安全管理員或安全營運工程師能夠達成下列目標：

- 一眼就能檢視所有工作負載的勒索軟體保護。
- 深入瞭解勒索軟體保護建議
- 根據 BlueXP 勒索軟體保護建議、改善保護狀態。
- 指派勒索軟體保護原則來保護您的主要工作負載和高風險資料、防範勒索軟體攻擊。
- 監控工作負載的健全狀況、防範尋找資料異常的勒索軟體攻擊。
- 快速評估勒索軟體事件對工作負載的影響。
- 透過還原資料並確保不會重新感染儲存的資料、以智慧方式從勒索軟體事件中恢復。

"瞭解 BlueXP 勒索軟體保護"。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。