



Release notes

BlueXP ransomware protection

NetApp
December 20, 2024

Table of Contents

Release notes 1

 What's new in BlueXP ransomware protection 1

Release notes

What's new in BlueXP ransomware protection

Learn what's new in BlueXP ransomware protection.

16 December 2024

Detect anomalous user behavior using Data Infrastructure Insights Storage Workload Security

With this release, you can use Data Infrastructure Insights Storage Workload Security to detect anomalous user behavior in your storage workloads. This feature helps you identify potential security threats and block potentially malicious users to protect your data.

For details, refer to [Respond to a detected ransomware alert](#).

Before you use Data Infrastructure Insights Storage Workload Security to detect anomalous user behavior, you need to configure the option by using the BlueXP ransomware protection **Settings** option.

Refer to [Configure BlueXP ransomware protection settings](#).

Select workloads to discover and protect

With this release, you can now do the following:

- Within each Connector, select the working environments where you want to discover workloads. You might benefit from this feature if you want to protect specific workloads in your environment and not others.
- During workload discovery, you can enable automatic discovery of workloads per Connector. This feature lets you select the workloads that you want to protect.
- Discover newly created workloads for previously selected working environments.

Refer to [Discover workloads](#).

7 November 2024

Enable data classification and scan for personally identifiable information (PII)

With this release, you can enable BlueXP classification, a core component of the BlueXP family, to scan and classify data in your file share workloads. Classifying data helps you identify whether your data includes personal or private information, which can increase security risks. This process also impacts workload importance and helps you ensure that you are protecting workloads with the right level of protection.

Scanning for PII data in BlueXP ransomware protection is generally available to customers who deployed BlueXP classification. BlueXP classification is available as part of the BlueXP platform at no extra charge and can be deployed on-premises or in the customer cloud.

Refer to [Configure BlueXP ransomware protection settings](#).

To initiate scanning, on the Protection page, click **Identify exposure** in the Privacy exposure column.

[Scan for personally identifiable sensitive data with BlueXP classification](#).

SIEM integration with Microsoft Sentinel

You can now send data to your security and event management system (SIEM) for threat analysis and detection using Microsoft Sentinel. Previously, you could select the AWS Security Hub or Splunk Cloud as your SIEM.

[Learn more about configuring BlueXP ransomware protection settings.](#)

Free trial now 30 days

With this release, new deployments of BlueXP ransomware protection now have 30 days for a free trial. Previously, BlueXP ransomware protection provided 90 days as a free trial. If you are already in the 90-day free trial, that offer continues for the 90 days.

Restore application workload at the file level for Podman

Before you restore an application workload at the file level, you can now view a list of files that might have been impacted by an attack and identify those you want to restore. Previously, if the BlueXP Connectors in an organization (previously an account) were using Podman, this feature was disabled. It is now enabled for Podman. You can let BlueXP ransomware protection choose the files to restore, you can upload a CSV file that lists all the files impacted by an alert, or you can manually identify which files you want to restore.

[Learn more about recovering from a ransomware attack.](#)

30 September 2024

Custom grouping of file share workloads

With this release, you can now group file shares into groups to make it easier for you to protect your data estate. The service can protect all volumes in a group at the same time. Previously, you needed to protect each volume separately.

[Learn more about grouping file share workloads in ransomware protection strategies.](#)

2 September 2024

Security risk assessment from Digital Advisor

BlueXP ransomware protection now gathers information about high and critical security risks related to a cluster from NetApp Digital Advisor. If any risk is found, BlueXP ransomware protection provides a recommendation in the Dashboard's **Recommended actions** pane: "Fix a known security vulnerability on the cluster <name>." From the recommendation on the Dashboard, clicking **Review and fix** suggests to review Digital Advisor and a Common Vulnerability & Exposure (CVE) article to resolve the security risk. If there are multiple security risks, review information in Digital Advisor.

Refer to [Digital Advisor documentation](#).

Back up to Google Cloud Platform

With this release, you can set a backup destination to a Google Cloud Platform bucket. Previously, you could add backup destinations only to NetApp StorageGRID, Amazon Web Services, and Microsoft Azure.

[Learn more about configuring BlueXP ransomware protection settings.](#)

Support for Google Cloud Platform

The service now supports Cloud Volumes ONTAP for Google Cloud Platform for storage protection. Previously, the service supported only Cloud Volumes ONTAP for Amazon Web Services and Microsoft Azure along with on-premises NAS.

[Learn about BlueXP ransomware protection and supported data sources, backup destinations, and working environments.](#)

Role-based access control

You can now limit access to specific activities with role-based access control (RBAC). BlueXP ransomware protection uses two roles from BlueXP: BlueXP Account Admin and Non-Account Admin (Viewer).

For details about the actions that each role can perform, see [Role-based access control privileges](#).

5 August 2024

Threat detection with Splunk Cloud

You can automatically send data to your security and event management system (SIEM) for threat analysis and detection. With previous releases, you could select only the AWS Security Hub as your SIEM. With this release, you can select the AWS Security Hub or Splunk Cloud as your SIEM.

[Learn more about configuring BlueXP ransomware protection settings.](#)

1 July 2024

Bring your own license (BYOL)

With this release, you can use a BYOL license, which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep.

[Learn more about setting up licensing.](#)

Restore application workload at the file level

Before you restore an application workload at the file level, you can now view a list of files that might have been impacted by an attack and identify those you want to restore. You can let BlueXP ransomware protection choose the files to restore, you can upload a CSV file that lists all the files impacted by an alert, or you can manually identify which files you want to restore.



With this release, if all BlueXP Connectors in an account are not using Podman, the single file restore feature is enabled. Otherwise, it is disabled for that account.

[Learn more about recovering from a ransomware attack.](#)

Download a list of impacted files

Before restoring an application workload at the file level, you can now access the Alerts page to download a list of impacted files in a CSV file and then use the Recovery page to upload the CSV file.

[Learn more about downloading impacted files before restoring an application.](#)

Delete protection plan

With this release, you can now delete a ransomware protection strategy.

[Learn more about protecting workloads and managing ransomware protection strategies.](#)

10 June 2024

Snapshot copy locking on primary storage

Enable this to lock the Snapshot copies on primary storage so that they cannot be modified or deleted for a certain period of time even if a ransomware attack manages its way to the backup storage destination.

[Learn more about protecting workloads and enabling backup locking in a ransomware protection strategy.](#)

Support for Cloud Volumes ONTAP for Microsoft Azure

This release supports Cloud Volumes ONTAP for Microsoft Azure as a working environment in addition to Cloud Volumes ONTAP for AWS and on-premises ONTAP NAS.

[Quick start for Cloud Volumes ONTAP in Azure](#)

[Learn about BlueXP ransomware protection.](#)

Microsoft Azure added as a backup destination

You can now add Microsoft Azure as a backup destination along with AWS and NetApp StorageGRID.

[Learn more about how to Configure protection settings.](#)

14 May 2024

Licensing updates

You can sign up for a 90-day free trial. Soon you will be able to purchase a pay-as-you-go subscription with Amazon Web Services Marketplace or bring your own NetApp license.

[Learn more about setting up licensing.](#)

CIFS protocol

The service now supports on-premises ONTAP and Cloud Volumes ONTAP in AWS working environments using both NFS and CIFS protocols. The previous release supported only the NFS protocol.

Workload details

This release now provides more details in the workload information from the Protection and other pages for improved workload protection assessment. From the workload details, you can review the currently assigned policy and review the configured backup destinations.

[Learn more about viewing workload details in the Protection pages.](#)

Application-consistent and VM-consistent protection and recovery

You can now perform application-consistent protection with NetApp SnapCenter Software and VM-consistent protection with SnapCenter Plug-in for VMware vSphere, achieving a quiescent and consistent state to avoid potential data loss later if recovery is needed. If recovery is required, you can restore the application or VM back to any of the previously available states.

[Learn more about protecting workloads.](#)

Ransomware protection strategies

If Snapshot or Backup policies do not exist on the workload, you can create a ransomware protection strategy, which can include the following policies that you create in this service:

- Snapshot policy
- Backup policy
- Detection policy

[Learn more about protecting workloads.](#)

Threat detection

Enable threat detection is now available using a third-party security and event management (SIEM) system. The Dashboard now shows a new recommendation to "Enable threat detection" which can be configured on the Settings page.

[Learn more about configuring Settings options.](#)

Dismiss false positive alerts

From the Alerts tab, you can now dismiss false positives or decide to recover your data immediately.

[Learn more about responding to a ransomware alert.](#)

Detection status

New detection statuses appear on the Protection page showing the status of the ransomware detection applied to the workload.

[Learn more about protecting workloads and viewing protection statuses.](#)


Download CSV files

You can download CSV files* from the Protection, Alerts, and Recovery pages.

[Learn more about downloading CSV files from the Dashboard and other pages.](#)

Documentation link

View documentation link is now included in the UI. You can access this documentation from the Dashboard

vertical **Actions**  option. Select **What's new** to view details in the Release Notes or **Documentation** to view the BlueXP ransomware protection documentation Home page.

BlueXP backup and recovery

The BlueXP backup and recovery service no longer needs to be already enabled on the working environment. See [prerequisites](#). The BlueXP ransomware protection service helps configure a backup destination through the Settings option. See [Configure settings](#).

Settings option

You can now set up backup destinations in BlueXP ransomware protection Settings.

[Learn more about configuring Settings options.](#)

5 March 2024

Protection policy management

In addition to using predefined policies, you can now create policies. [Learn more about managing policies.](#)

Immutability on secondary storage (DataLock)

You can now make the backup immutable in secondary storage using NetApp DataLock technology in the object store. [Learn more about creating protection policies.](#)

Automatic backup to NetApp StorageGRID

In addition to using AWS, you can now choose StorageGRID as your backup destination. [Learn more about configuring backup destinations.](#)

Additional features to investigate potential attacks

You can now view more forensic details to investigate the detected potential attack. [Learn more about responding to a detected ransomware alert.](#)

Recovery process

The recovery process was enhanced. Now, you can recover volume by volume or all volumes for a workload. [Learn more about recovering from a ransomware attack \(after incidents have been neutralized\).](#)

[Learn about BlueXP ransomware protection.](#)

6 October 2023

The BlueXP ransomware protection service is a SaaS solution for protecting data, detecting potential attacks, and recovering data from a ransomware attack.

For the preview version, the service protects application-based workloads of Oracle, MySQL, VM datastores, and file shares on on-premises NAS storage as well as Cloud Volumes ONTAP on AWS (using the NFS protocol) across BlueXP organizations individually and backs up data to Amazon Web Services cloud storage.

The BlueXP ransomware protection service provides full use of several NetApp technologies so that your data security administrator or security operations engineer can accomplish the following goals:

- View ransomware protection on all your workloads at a glance.
- Gain insight into ransomware protection recommendations

- Improve protection posture based on BlueXP ransomware protection recommendations.
- Assign ransomware protection policies to protect your top workloads and high-risk data against ransomware attacks.
- Monitor the health of your workloads against ransomware attacks looking for data anomalies.
- Quickly assess the impact of ransomware incidents on your workload.
- Recover from ransomware incidents intelligently by restoring data and ensuring that reinfection from stored data does not occur.

[Learn about BlueXP ransomware protection.](#)

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.