

# RANSOMWARE PROTECTION

**AI-powered built-in cyber defense at storage level**

**David Besson**

Account Technology Specialist

September 19<sup>th</sup>, 2024

# Across several eras in the age of data, NetApp has led in data infrastructure innovation

Increasing amount of data, complexity and cost



Adoption



Acceleration



Complexity



Simplification



2002

## Data Silos & Unification

NetApp becomes the first vendor to **unify file & block workloads, and structured & unstructured data**

## Hybrid Cloud

NetApp creates the first **data fabric strategy** that eliminates silos & provides unified control across any environment

## Hybrid Multiclouds

NetApp becomes the **ONLY** vendor to introduce **cloud ops and data services** as key data infrastructure pillars in addition to being the **only vendor natively embedded in all major clouds**

Today

## Intelligence

NetApp delivers **silos-free infrastructure**, then harnesses **observability and AI** to enable best data management everywhere

# Data storage to meet every need – all powered by ONTAP

For lowest cost,  
secondary use cases

**HYBRID FLASH**

FAS



For best price/  
performance

**CAPACITY FLASH**

AFF C-Series



For best performance  
On Tier1 workloads

**PERFORMANCE FLASH**

AFF A-Series



Unified

Block  
Optimized

ASA C-Series



ASA A-Series



# ONTAP

Comprehensive data management software delivering automation, efficiency, data protection, and security capabilities for file, block, and object



# Unified control across your hybrid multicloud

## NetApp BlueXP



**Unified control**  
of storage and services for  
all your data wherever it lives



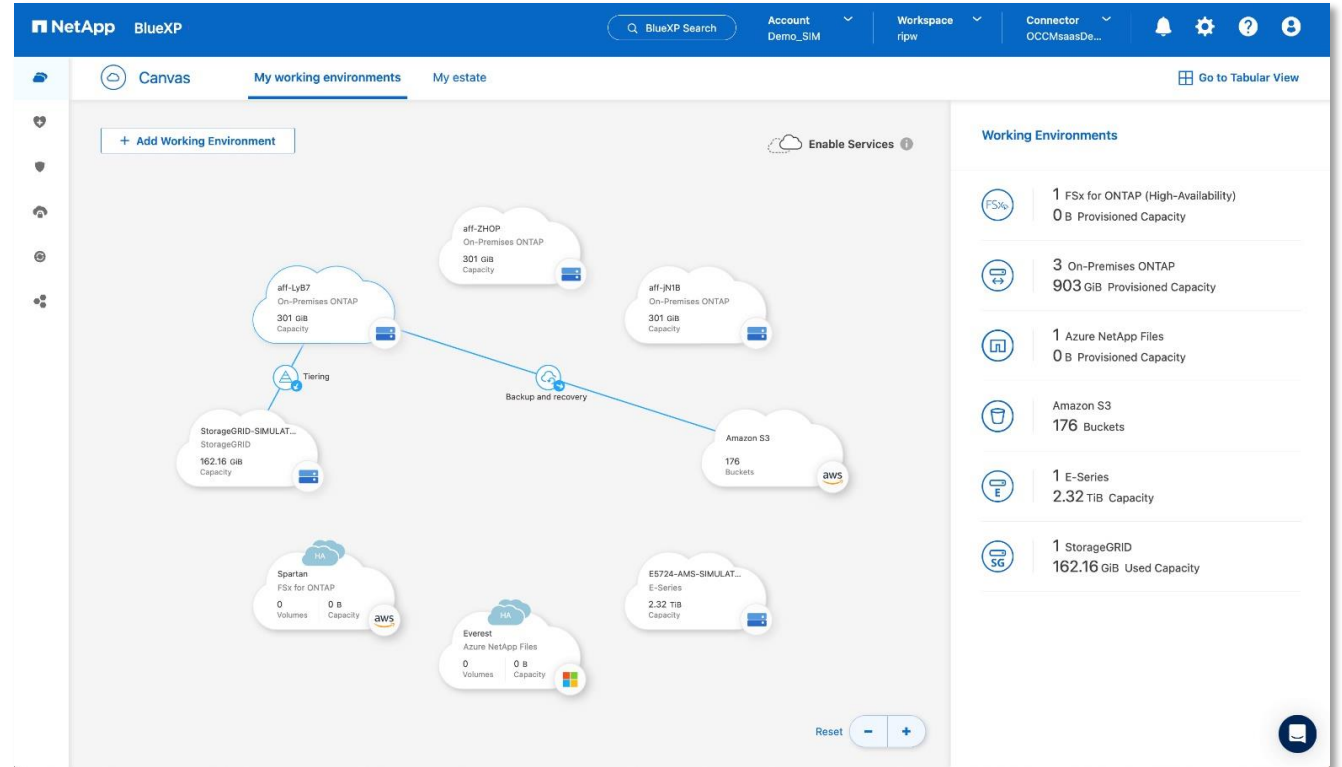
**Powerful AI Ops**  
drives operational simplicity



**Flexible consumption of resources**  
unlocks control, investment protection,  
and ROI



**Integrated services**  
maximize data protection and cyber  
resilience while minimizing costs



**Delivering the speed, simplicity, and security  
required in today's highly complex world**

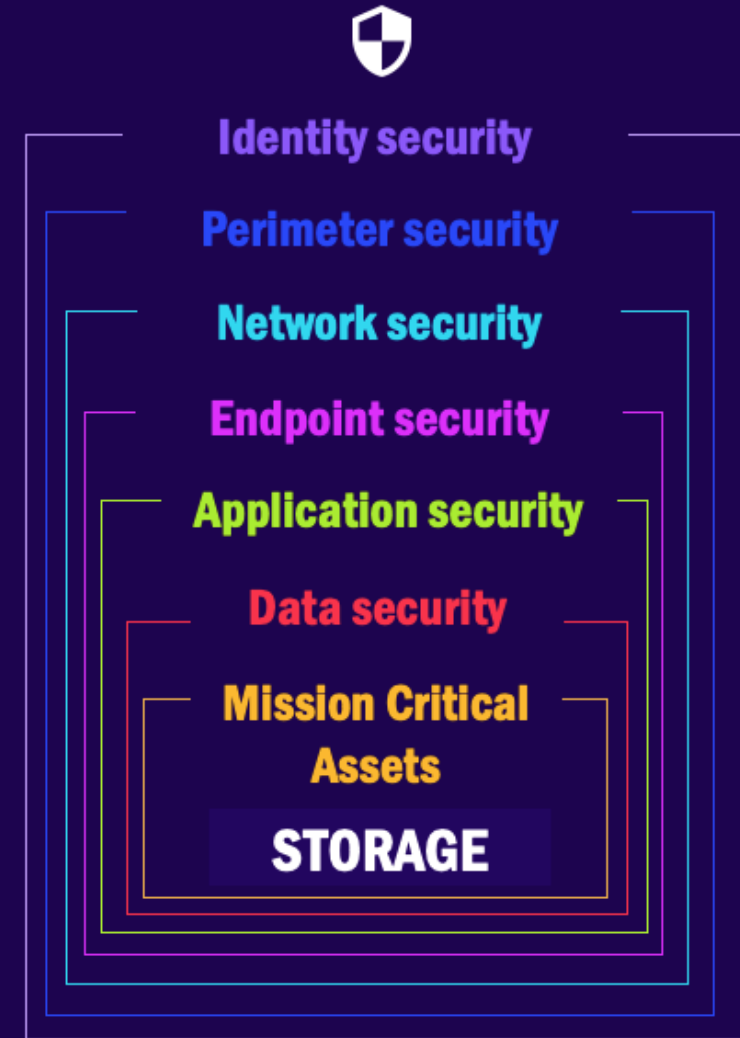
# NetApp Ransomware Protection

- 1 Secure by design**
- 2 Real-time detection & response**
- 3 Single control plane to automate**
- 4 Air-gapped cyber vaulting**
- 5 Recovery guarantee**

# Storage is the last line of defense

## You need to:

- Minimize chance of a successful attack
- Minimize impact of a successful attack
- Protect critical data, know when its under attack, and recover fast
- Isolate critical data backups
- Ensure data recovery



# 72%

In 2024, Ransomware affected 72% of organizations.

Source: [Sophos "The State of Ransomware 2024"](#)

It's not a matter of **if** but  
**when** you will experience  
a cyber-attack.

# Ransomware costs businesses millions annually

**Sophos reports that 92% of companies that pay don't get their data back**

\$1.4M

Average cost to remediate a ransomware attack in 2022

\$3B

Insurance premiums  
92% annual growth<sup>1</sup>

1.7X

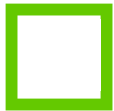
The downtime and recovery time cost to remediate is 1.7 times the ransomware payment<sup>2</sup>

<sup>1</sup> Standard and Poor's report <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-underwriters-premiums-surge-loss-ratios-improve-in-21-70247722>

<sup>2</sup> Sophos report survey data of 5,600 IT manager on "The State Of Ransomware 2022" Average cost was for organizations. <https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnfhqi9bxg8/sophos-state-of-ransomware-2022-wp.pdf>



# HOW PREPARED ARE YOU FOR A RANSOMWARE ATTACK?



**I know, with confidence, that my critical workloads are protected.**



**If a workload was under attack, I'd know immediately, and threats would be automatically contained.**



**If attacked, I am confident I'll recover mission critical workloads within minutes.**

# Effective Ransomware Protection Readiness

**Cyber attacks are more sophisticated**

**Detect with AI-powered detection**

**Backup alone is not sufficient**

**Add defense at the storage layer**

**Operational burden is heavy**

**Use built-in ransomware protection**

# BUILT-IN RANSOMWARE PROTECTION

AI-powered ransomware protection  
embedded in our storage.



NetApp cyber-resilience capabilities can be mapped to the National Institute of Standards and Technology (NIST) cybersecurity framework

## 01 PROTECT

### IDENTIFY

Discover and classify your data, where it is stored, and who has access to it.

### PROTECT

Protect data from inside and outside threats, unplanned outages, accidental data loss, and malware attacks.

Classification

MFA

Policy framework

snapshots

end-to-end encryption

## 02 DETECT

### DETECT

AI-powered detection to monitor and detect anomalies in real time with more than 99% accuracy to thwart cyberattacks and to improve uptime.

### RESPOND

Automatically respond to attacks or failures and minimize damage and downtime.

## 03 RECOVER

### RECOVER

Identify the source of threats and rapidly restore data and applications.



# AI-Powered Ransomware Protection

Next generation ransomware threat detection



- Industry-leading AI-powered ransomware detection for enterprise storage



- Next-gen AI/ML models deliver 100% precision and 99% recall, to detect more sophisticated and evolving cyber threats



- Automatically update model parameters regularly without a required ONTAP update or system reboot



- Seamless upgrade from current generation autonomous ransomware protection



**Precision**

**100%**

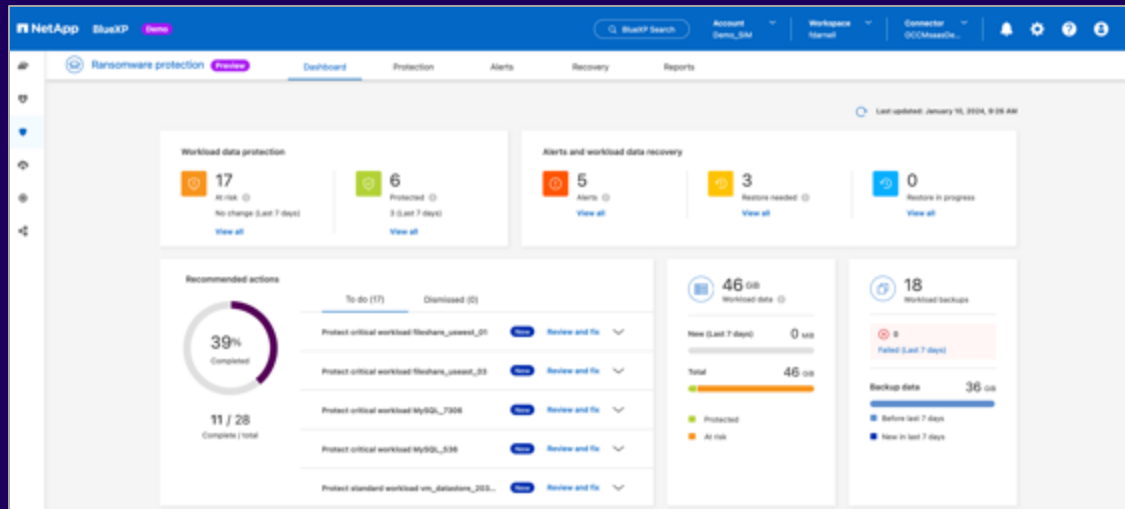
**Recall**

**99%**

TECH PREVIEW AVAILABLE NOW

# NetApp BlueXP ransomware protection

The AI-based intelligence and assistance needed to minimize workload data loss and bounce back quickly



**IDENTIFY:** Automatically identifies workloads (VMs, file shares, DBs) and their data in your NetApp storage, maps data to workload, determines workload importance, and analyzes workload risk.



**PROTECT:** Shows you what to protect. Recommends workload protection policies and applies them with one-click.



**DETECT:** Detects potential attacks on your workload data in near real-time using industry leading AI/ML.



**RESPOND:** Automatically responds in near-real time by taking immutable and indelible Snapshot copies when a potential attack is suspected. Integrates with popular SIEMs.



**RECOVER:** Rapidly restores workloads, with application consistency, through simplified orchestrated recovery.



**GOVERN:** Implements your ransomware protection strategy and policies, and monitors outcomes.



**NetApp**

**The most secure storage  
on the planet**

# The only enterprise storage validated for top-secret data



Commercial Solutions for  
Classified (CSfC)  
Components List



FIPS 140-2



Department of Defense  
Information Network  
Approved Products List  
(DoDIN APL)



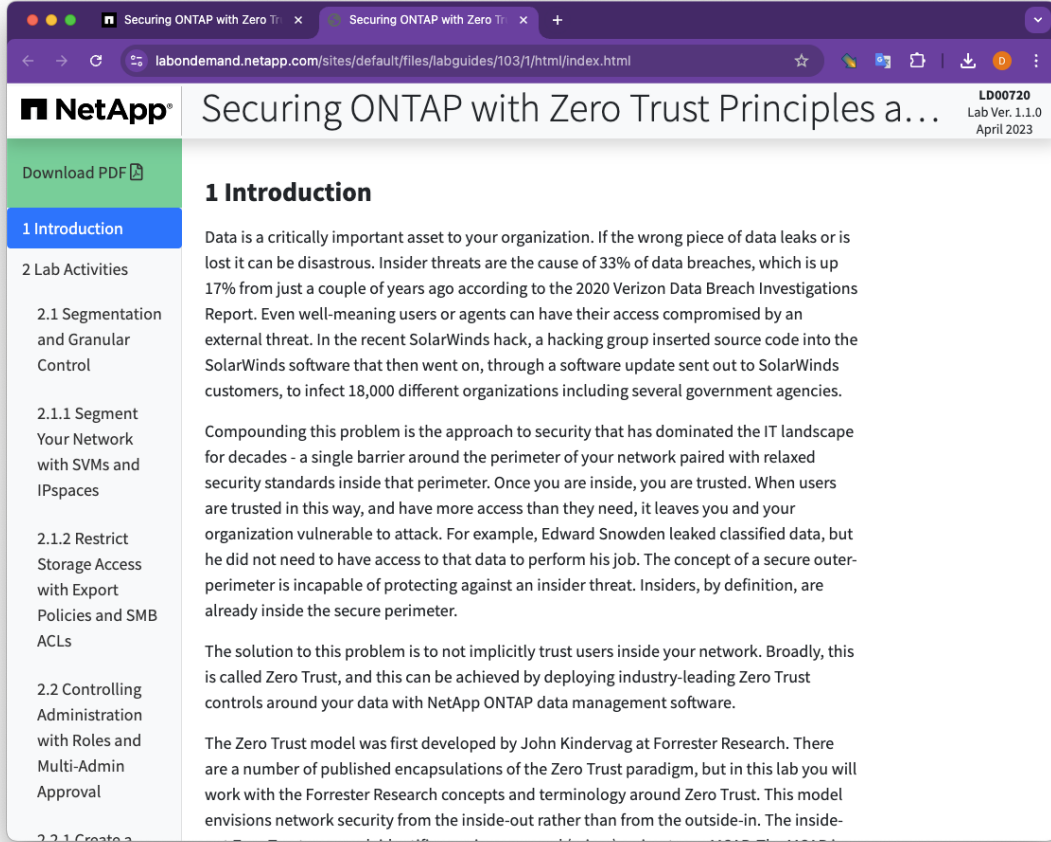
Common Criteria



# Where to go more information

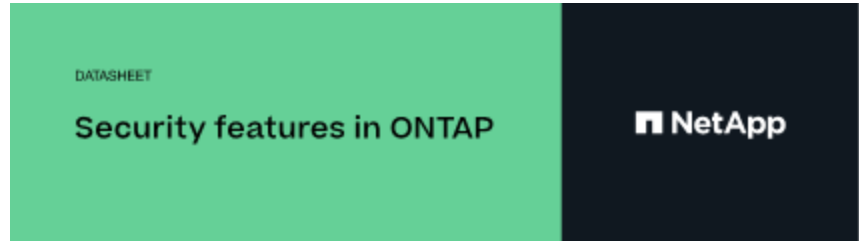
## Security hardening & Ontap features

<https://labondemand.netapp.com/lab/securing-ontap-zero-trust>



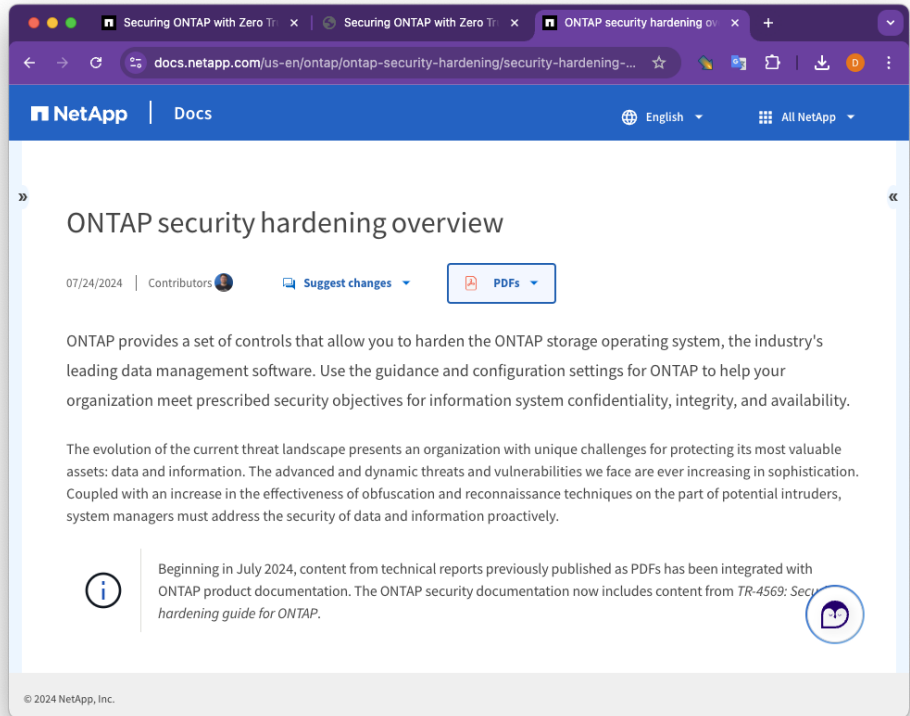
Hands-on labs for customers

Complete hardening guide for Ontap



Security features explained

<https://www.netapp.com/pdf.html?item=/media/8128-ds-3846.pdf>



<https://docs.netapp.com/us-en/ontap/ontap-security-hardening/security-hardening-overview.html>

# MERCI DE VOTRE ATTENTION !

**Sondage de satisfaction**  
Merci de votre feedback



**Scannez-moi**

# THANK YOU



Learn more at:  
<https://www.netapp.com/cyber-resilience/ransomware-protection/>

# BACKUP SLIDES

# Landing page – Start by discovering your workloads with a 90-day free trial

**NetApp BlueXP Demo** | BlueXP Search | Account: Demo\_SIM | Workspace: JosephAbouk... | Connector: OCCMsaasDe... | Settings | Help | Profile

## Ransomware protection

### Outsmart ransomware

BlueXP ransomware protection orchestrates a comprehensive AI-driven defense for workload data on NetApp NAS storage with ONTAP 9.11.1 or later, on-premises or Cloud Volumes ONTAP in AWS or Azure (FlexGroup, iSCSI, and data protection volumes are not supported).

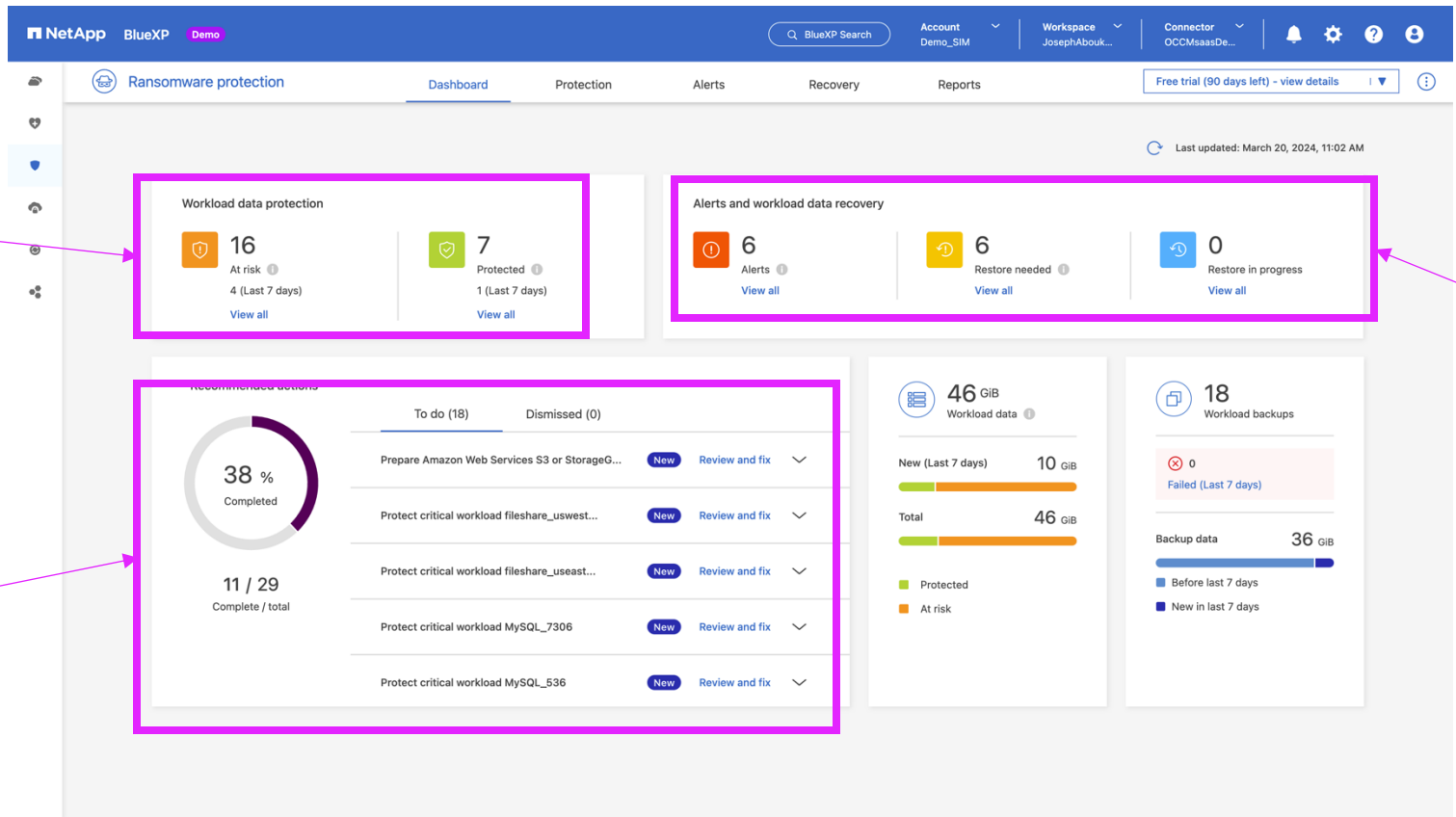
Start your 90-day free trial today to get full access to BlueXP ransomware protection.

[Start by discovering workloads](#)

- Identify and protect**  
Automatically identifies workloads at risk, recommends fixes, and protects with one-click
- Detect and respond**  
Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point
- Recover**  
Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

# Dashboard – Posture assessment and recommendations

Workload protection posture assessment summary



Potential attack alerts and activities

Recommendations to improve protection posture

# Protection tab – Workload protection and configuration

The screenshot displays the NetApp BlueXP Ransomware protection interface. At the top, there's a navigation bar with 'Ransomware protection', 'Dashboard', 'Protection', 'Alerts', 'Recovery', and 'Reports'. Below this, a summary section shows: 16 At risk (4 Last 7 days), 32 GiB Data at risk, 7 Protected (1 Last 7 days), and 14 GiB Data protected. A 'Free trial (90 days left) - view details' button is also present.

The main section is titled 'Workloads (23)' and contains a table with the following columns: Workload, Type, Connector, Importance, Protection status, Detection status, Detection policy, Snapshot and back..., and Backup destination. The table lists various workloads such as 'Vm\_datastore\_useast...', 'Oracle\_8821', 'Oracle\_2115', 'Mysql\_9294', 'Mysql\_8009', 'Fileshare\_uswest\_02...', 'Oracle\_9819', 'Vm\_datastore\_203\_267...', 'Vm\_datastore\_uswest...', and 'Vm\_datastore\_uswest...'. Each row includes a 'Protection status' (e.g., Protected, At risk) and a 'Detection status' (e.g., Active, Learning, Learning mode). Action buttons like 'Edit protection' and 'Protect' are visible for each workload.

Intelligently identify workloads and assign importance

Discover existing protection posture

Improve protection posture

# Protection tab – Workload protection

NetApp BlueXP Demo

Protect "Oracle\_2115"

Protect

Select a detection policy to apply to the workload Oracle\_2115.

| Detection policies (2)   1 selected                    |                   |                                  |
|--|-------------------|----------------------------------|
| Name   | Primary detection | Block suspicious file extensions |
| rps-policy-ai  | Yes               | Yes                              |
| <input checked="" type="checkbox"/> rps-policy-primary | Yes               | No                               |

Policies managed by SnapCenter

These policies managed by SnapCenter will not be modified by applying a detection policy to this workload.

- ss-policy-daily1 Snapshot policy
- ss-policy-weekly1 Snapshot policy
- ss-policy-weekly2 Snapshot policy
- ss-policy-monthly1 Snapshot policy

Cancel Protect

Apply detection policy to workload already protected by SnapCenter



# Protection tab – Workload protection and configuration

The screenshot displays the NetApp BlueXP Protection tab. At the top, there are navigation tabs for Ransomware protection, Dashboard, Protection, Alerts, Recovery, and Reports. A summary card shows 15 items at risk (4 in the last 7 days) and 30 GiB of data at risk. Another card shows 8 items protected (1 in the last 7 days) and 16 GiB of data protected. Below this is a table of 23 workloads with columns for Workload, Type, Connector, Importance, Protection status, Detection status, Detection policy, Snapshot and back..., and Backup destination. A notification at the bottom states 'Successfully initiated workload protection, Oracle\_2115.' A purple box highlights the 'Protected' status for Oracle\_2115, and a purple callout box labeled 'Protection policy applied' points to the 'rps-policy-primary' policy for this workload.

| Workload                | Type          | Connector                | Importance | Protection status | Detection status | Detection policy   | Snapshot and back...      | Backup destination    |
|-------------------------|---------------|--------------------------|------------|-------------------|------------------|--------------------|---------------------------|-----------------------|
| Vm_datastore_useast...  | VM file share | aws-connector-us-east... | Critical   | Protected         | Active           | rps-policy-all     | BlueXP ransomware prot... | netapp-backup-vsajgd1 |
| Vm_datastore_uswest...  | VM file share | aws-connector-us-west... | Critical   | Protected         | Learning         | rps-policy-all     | BlueXP ransomware prot... | netapp-backup-vsajgd1 |
| Vm_datastore_uswest...  | VM file share | aws-connector-us-west... | Standard   | At risk           | None             | None               | None                      | netapp-backup-vsajgd2 |
| Vm_datastore_uswest...  | VM file share | aws-connector-us-west... | Standard   | At risk           | None             | None               | None                      | netapp-backup-vsajgd1 |
| Vm_datastore_useast...  | VM file share | aws-connector-us-east... | Standard   | At risk           | None             | None               | None                      | netapp-backup-vsajgd1 |
| Vm_datastore_201_334... | VM file share | onprem-connector-acco... | Standard   | At risk           | None             | None               | None                      | netapp-backup-vsajgd2 |
| Oracle_9821             | Oracle        | aws-connector-us-east... | Critical   | Protected         | Active           | rps-policy-all     | BlueXP ransomware prot... | netapp-backup-vsajgd1 |
| Oracle_9819             | Oracle        | aws-connector-us-east... | Important  | Protected         | Learning mode    | rps-policy-all     | SnapCenter                | netapp-backup-vsajgd2 |
| Oracle_2115             | Oracle        | aws-connector-us-east... | Critical   | Protected         | Learning mode    | rps-policy-primary | SnapCenter                | netapp-backup-vsajgd1 |
| Mysql_9294              | MySQL         | aws-connector-us-east... | Critical   | At risk           | None             | None               | BlueXP backup and reco... | netapp-backup-vsajgd3 |
| Mysql_8009              | MySQL         | aws-connector-us-east... | Critical   | At risk           | None             | None               | BlueXP backup and reco... | netapp-backup-vsajgd1 |

Protection policy applied

# Alerts – View potential attacks

Alert details including number of incidents, impacted data, and timeframe

The screenshot displays the NetApp BlueXP Alerts page. At the top, there is a navigation bar with the NetApp logo, 'BlueXP Demo', a search bar, and user information. Below the navigation bar, the 'Alerts' tab is selected. The main content area shows a summary of alerts: 6 Alerts and 12 GiB Impacted data. To the right, there is a section for 'Automated responses' showing 9 Snapshot copies. Below this, a table lists 6 alerts. The second row of the table is highlighted with a purple box, and a purple arrow points from the text box on the left to this row.

| Alert ID  | Workload                | Location                            | Type         | Status | Connector                                     | Incidents | Impacted data | First detected |
|-----------|-------------------------|-------------------------------------|--------------|--------|---|-----------|---------------|----------------|
| Alert9314 | Fileshare_uswest_02_... | svm_cvoawswest01rpsdemosandbox02aws | File share   | Active | aws-connector-us-west-1-account-LXtf4Xh-e...  | 1         | 2 GiB         | 8 days ago     |
| Alert8727 | Oracle_8821             | 10.0.1.193                          | Oracle       | Active | aws-connector-us-east-1-account-LXtf4Xh-10... | 2         | 2 GiB         | 8 days ago     |
| Alert9823 | Oracle_9819             | 10.0.1.193                          | Oracle       | Active | aws-connector-us-east-1-account-LXtf4Xh-10... | 1         | 2 GiB         | 8 days ago     |
| Alert3932 | Mysql_9294              | 10.0.1.10                           | MySQL        | Active | aws-connector-us-east-1-account-LXtf4Xh-10... | 2         | 2 GiB         | 8 days ago     |
| Alert7918 | Vm_datastore_202_735... | 10.195.52.126                       | VM datastore | Active | onprem-connector-account-LXtf4Xh              | 1         | 2 GiB         | 8 days ago     |
| Alert5319 | Vm_datastore_uswest_... | 10.0.1.215                          | VM datastore | Active | aws-connector-us-west-1-account-LXtf4Xh-e...  | 1         | 2 GiB         | 8 days ago     |

# Alerts – View all incidents of a potential attacks

The screenshot displays the NetApp BlueXP interface for Ransomware protection. The top navigation bar includes the NetApp logo, 'BlueXP Demo', a search bar, and account/workspace information. The main header shows 'Ransomware protection' with tabs for Dashboard, Protection, Alerts, Recovery, and Reports. A 'Free trial (90 days left) - view details' button is visible on the right.

The alert details for 'alert8727' are shown below the navigation. It includes workload information: 'Workload: Oracle\_8821 | Location: 10.0.1.193 | Type: Oracle | Connector: aws-connector-us-eas...'. A 'Mark restore needed' button is present. Summary statistics are displayed in a grid:

- 2 Potential attacks
- 8 days ago First detected
- 2 GiB Impacted data
- 286 Impacted files

Below the summary is a table of incidents (2 total). The table has columns for Incident ID, Volume, SVM, Working environ..., Type, Status, First detected, Evidence, and Automated respo... Two incidents are listed:

| Incident ID | Volume              | SVM                    | Working environ...    | Type             | Status | First detected | Evidence                 | Automated respo... |
|-------------|---------------------|------------------------|-----------------------|------------------|--------|----------------|--------------------------|--------------------|
| Inc4922     | oracle_useast_data2 | svm_cvoawseast01rps... | cvoawseast01rpsdem... | Potential attack | New    | 8 days ago     | 4 new extensions dete... | 1 Snapshot copy    |
| Inc3163     | oracle_useast_log2  | svm_cvoawseast01rps... | cvoawseast01rpsdem... | Potential attack | New    | 8 days ago     | 6 new extensions dete... | 1 Snapshot copy    |

Two volumes for this workload had potential attacks

What was detected and the automated response taken to protect data from further damage

# Alerts – Investigate a potential attack incident

The screenshot displays the NetApp BlueXP Alerts interface. The top navigation bar includes the NetApp logo, 'BlueXP Demo', a search bar, and user account information. The main navigation tabs are 'Ransomware protection', 'Dashboard', 'Protection', 'Alerts', 'Recovery', and 'Reports'. The current view is 'Alerts', showing a specific alert for 'inc4922'. The alert details include: 'New Status' (indicated by a bell icon), 'Potential attack Type' (indicated by a red warning icon), and '8 days ago First detected'. Below this, there are three main sections: 'Incoming data', 'File activity', and 'Impacted files (105)'. The 'Incoming data' section shows 'Entropy of incoming data' with 'Detected' at 2173 KIB / min and 'Expected' at 21732 KIB / min. The 'File activity' section shows 'Creation rate' with 'Detected' at 10 files / min and 'Expected' at 66 files / min, and 'Renaming rate' with 'Detected' at 300 files / min and 'Expected' at 10 files / min. The 'Impacted files (105)' section shows a list of impacted files, including file paths and extensions like .pck, .xyz, .lck, and .omg.

| Section                  | Detected        | Expected        |
|--------------------------|-----------------|-----------------|
| Entropy of incoming data | 2173 KIB / min  | 21732 KIB / min |
| Creation rate            | 10 files / min  | 66 files / min  |
| Renaming rate            | 300 files / min | 10 files / min  |


| New file extensions (4) | Suspect file extensions (4) |
|-------------------------|-----------------------------|
| .pck                    | .lck                        |
| .xyz                    | .omg                        |
| .lck                    | .pck                        |
| .omg                    | .xyz                        |

| Impacted files (105)                        |
|---|
| /Top_Dir_1/Sub_Dir_11/test_file_11964.1.pck |
| /Top_Dir_1/Sub_Dir_11/test_file_11964.1.xyz |
| /Top_Dir_1/Sub_Dir_11/test_file_27869.2.lck |
| /Top_Dir_1/Sub_Dir_11/test_file_27869.2.omg |


Details of a potential attack incident to help identify what happened and what files were potentially impacted

# SIEM integration

Streamlines threat detection and analysis across an organization's tools

 Integrate with a SIEM / XDR

---

 Disconnected



Automatically send data to a security information and event management (SIEM) or extended detection and response (XDR) server for threat analysis and detection.

[Connect](#)





























- Sends logs from BlueXP to SIEM
- Shows incidents detected by SIEM (coming soon)
- Automated response and alerts on SIEM-detected incidents (coming soon)

alert001

Workload: patient-app | Location: host.name.com | Type: Oracle | Connector: connect1 [Mark restore needed](#)

 2 Potential attacks |  14 mins ago First detected | 10 TiB Impacted data | 1,092 Impacted files

Incidents (6) [Search](#) [Download](#) [Edit status](#)

| <input type="checkbox"/> | Incident ID | Type   | Status  | Evidence   | Automated responses  | First detected  | Detected by |   |
|--------------------------|-------------|--|---|--|--|---|-------------|---|
| <input type="checkbox"/> | inc001      |  Potential attack |  New         | 2 new extensions created<br>File creation increased by 40% |  Snapshot copies: 6 |  2 hours ago | SIEM/XDR    |  |
| <input type="checkbox"/> | inc002      |  Potential attack |  In progress | 3 new extensions created<br>Entropy increased by 20%       |  Snapshot copies: 5 |  1 day ago   | BlueXP      |  |
| <input type="checkbox"/> | inc003      |  Warning          |  Resolved    | File deletion increased by 30%                             |  Snapshot copies: 1 |  5 hours ago | BlueXP      |  |
| <input type="checkbox"/> | inc004      |  Warning          |  Resolved    | File creation increased by 30%                             |  Snapshot copies: 4 |  4 days ago  | SIEM/XDR    |  |
| <input type="checkbox"/> | inc005      |  Warning          |  Dismissed   | File creation increased by 30%                             | n/a  |  18 mins ago | BlueXP      |  |
| <input type="checkbox"/> | inc006      |  Warning          |  Dismissed   | File creation increased by 30%                             | n/a  |  14 mins ago | BlueXP      |  |



More coming soon

# Alerts – Manage incidents

The screenshot shows the NetApp BlueXP Alerts interface. At the top, there is a navigation bar with 'NetApp BlueXP Demo', a search bar, and account/workspace information. Below this is a breadcrumb trail: 'Ransomware protection > Alerts > alert8727'. The main content area displays details for 'alert8727', including workload, location, type, and connector. A summary card shows 2 potential attacks, first detected 8 days ago, with 2 GiB of impacted data and 286 impacted files. Below this is a table of incidents with 2 items selected. An 'Edit status' button is highlighted with a red box and a red arrow pointing to it.

| Incident ID | Volume              | SVM                    | Working environ...    | Type             | Status | First detected | Evidence                 | Automated respo... |
|-------------|---------------------|------------------------|-----------------------|------------------|--------|----------------|--------------------------|--------------------|
| inc4922     | oracle_useast_data2 | svm_cvoawseast01rps... | cvoawseast01rpsdem... | Potential attack | New    | 8 days ago     | 4 new extensions dete... | 1 Snapshot copy    |
| inc3163     | oracle_useast_log2  | svm_cvoawseast01rps... | cvoawseast01rpsdem... | Potential attack | New    | 8 days ago     | 6 new extensions dete... | 1 Snapshot copy    |

Change status from "New" to "Resolved" or "Dismissed"

# Recovery – View status and restore

The screenshot shows the NetApp BlueXP Recovery interface. At the top, there are navigation tabs for Dashboard, Protection, Alerts, Recovery, and Reports. The Recovery tab is active. Below the navigation, there are three summary cards: '4 Restore needed' (8 GiB Data), '0 In progress' (0 MiB Data), and '1 Restored' (2 GiB Data). Below these cards is a table titled 'Workloads (5)'. The table has columns for Workload, Location, Type, Connector, Managed by, Recovery status, Progress, Importance, Total data, and Action. A red box highlights the 'Importance' and 'Total data' columns, and the 'Restore' buttons in the 'Action' column for the first four rows. A callout box points to these buttons with the text 'Restore workloads in your preferred order: Priority, Type ...'.

| Workload                | Location      | Type         | Connector                   | Managed by                  | Recovery status | Progress | Importance | Total data | Action  |
|-------------------------|---------------|--------------|-----------------------------|-----------------------------|-----------------|----------|------------|------------|---------|
| Mysql_9294              | 10.0.1.10     | MySQL        | aws-connector-us-east-1-... | BlueXP backup and recove... | Restore needed  | n/a      | Critical   | 2 GiB      | Restore |
| Oracle_9819             | 10.0.1.10     | Oracle       | aws-connector-us-east-1-... | SnapCenter                  | Restore needed  | n/a      | Critical   | 2 GiB      | Restore |
| Oracle_8821             | 10.0.1.193    | Oracle       | aws-connector-us-east-1-... | BlueXP ransomware prote...  | Restore needed  | n/a      | Critical   | 2 GiB      | Restore |
| Vm_datastore_202_735... | 10.195.52.126 | VM datastore | onprem-connector-accou...   | SnapCenter for VMware       | Restore needed  | n/a      | Standard   | 2 GiB      | Restore |
| Vm_datastore_uswest...  | 10.0.1.215    | VM datastore | aws-connector-us-west-1-... | None                        | Restored        | 100%     | Critical   | 2 GiB      | Restore |

Restore workloads in your preferred order: Priority, Type ...