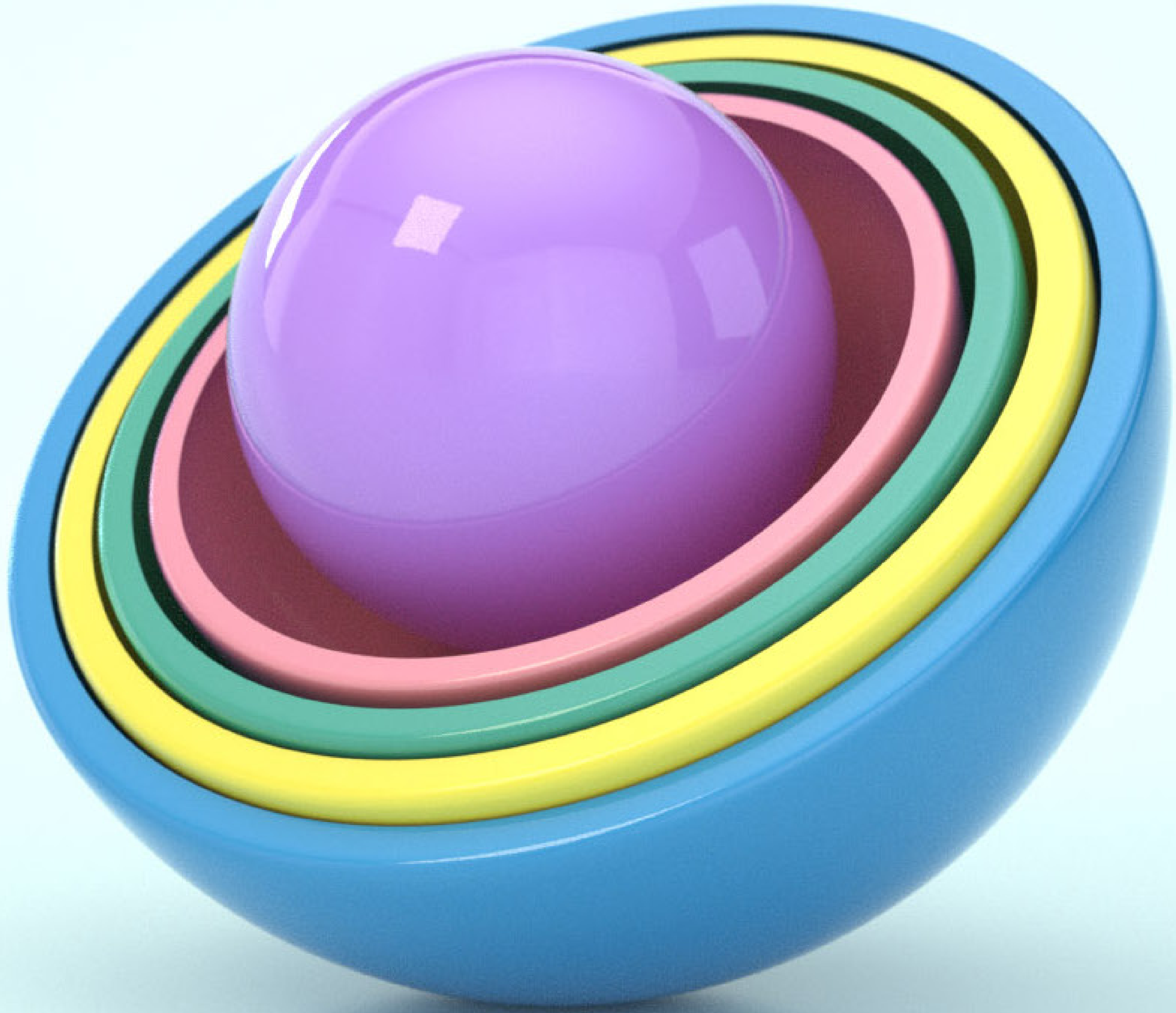
NetApp

What Is the Data-Centric Approach to Ransomware Protection?



A complete guide to the principles and tools

↓

Executive Summary

Ransomware continues to be the most serious threat to enterprises, and organizations are realizing that the traditional ransomware protection method of securing the network and relying on backups just doesn't cut it anymore. More often than not, successful ransomware attacks still take place after networks are secured.

So what's to be done? A truly comprehensive security posture needs to protect not only the network, but also the asset. The ransomware ultimately wants to target—your data. This is what is known as a data-centric approach to ransomware protection.

This guidebook will give you a full review of ransomware threats and what you can do to create a data-centric protective stance using NetApp Ransomware Protection.

PART 1

Ransomware on the Rise

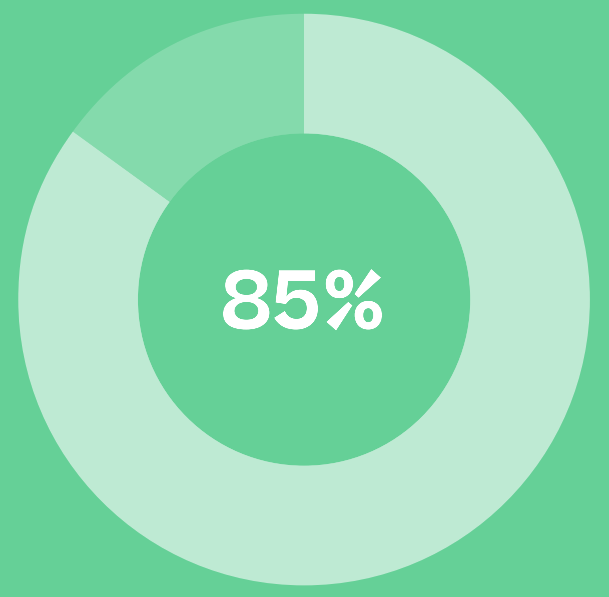
Cyberthreats are Keeping Executives Awake at Night

Ransomware is a form of malicious code that locks users out of their data. Once the data is locked, the attacker demands a ransom to unlock the data.

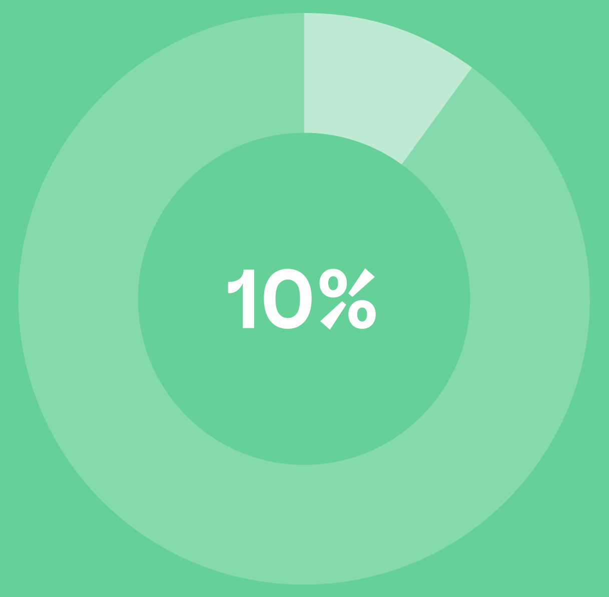
According to the Allianz Risk Barometer of 2022, cyberthreats now rank as the top business risk for enterprises, with ransomware being the most concerning cyberthreat to a business.

5,258 Breaches

29,207 Incidents



of breaches involved
a **human element**



of breaches involved **ransomware**,
doubling last year's frequency

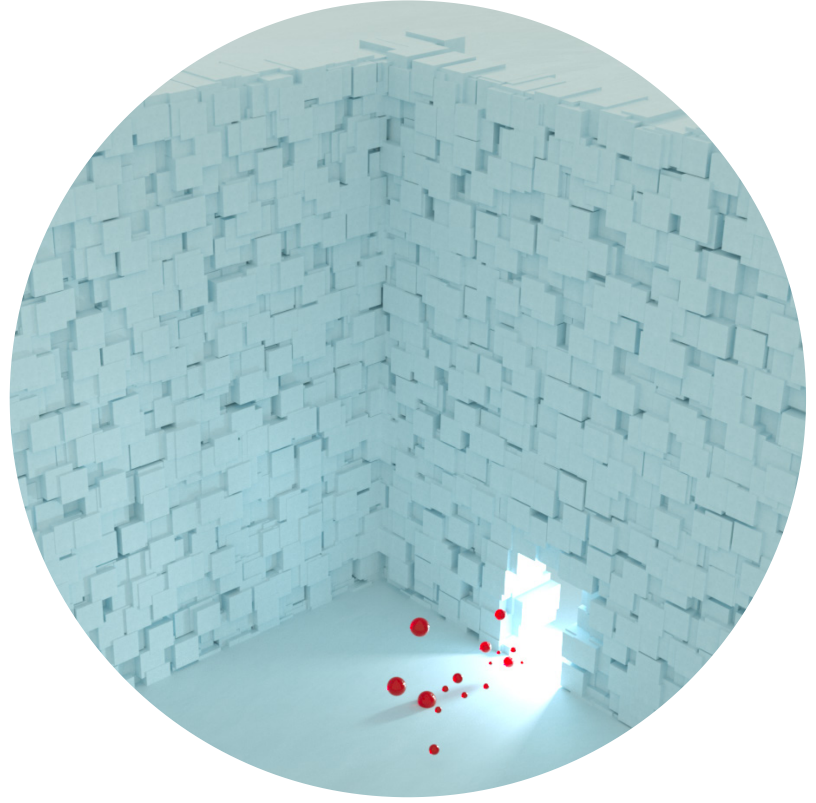
Source: 2021 Data Breach Investigations Report

Learn more

PART 2

Why Common Protection Methods Don’t Work

There are two main ways that enterprises have sought to protect themselves against ransomware attacks, allowing them to recover locked data:

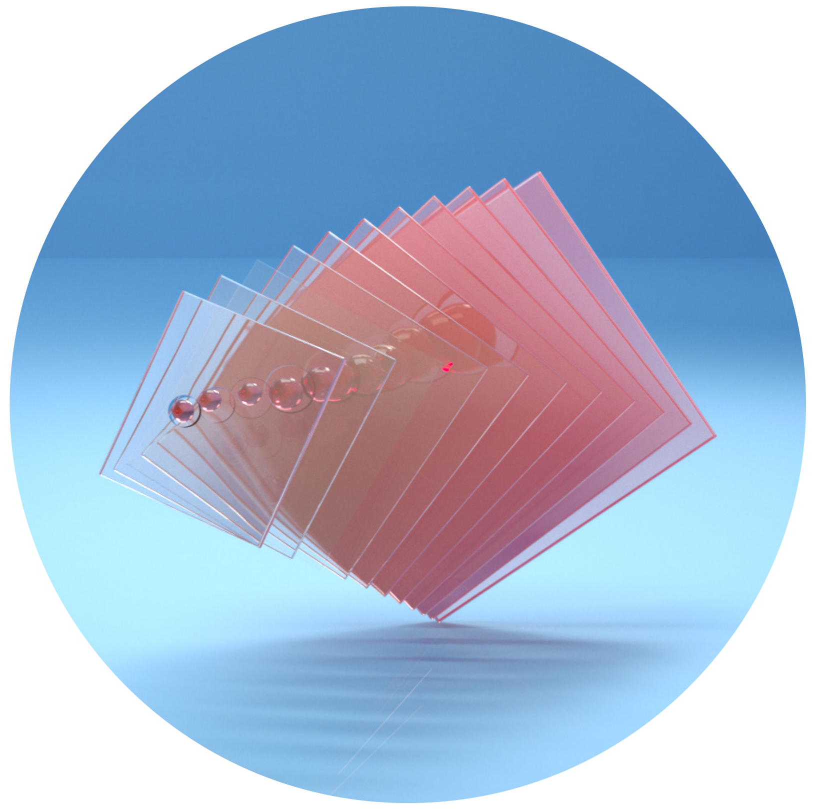


Perimeter Protection

Dedicated attackers are always probing at defenses and looking for ways in. There is no guarantee that protecting the network will ensure ransomware infections won’t take place.

What is it?
Building a good defensive wall is an idea as old as the foundations of civilization itself and the basis of perimeter protection: Tighten access to your network to ensure no infections can enter.

Why is it not enough?
Any wall can be breached. Ransomware perimeter protection is constantly challenged by a large range of ever-changing malware injection techniques and doesn’t work against threats that may already be inside the system, lying in wait to deploy malicious code.



Backup Solutions

With no awareness of the actions going on in your system, backup data is as vulnerable to infection as the rest of your data.

What are they?
Backups are the last line of defense in ransomware attack situations. If data becomes inaccessible after a ransomware attack, an up-to-date backup copy can allow systems to be restored.

Why are they not enough?
Backups are not aware of attacks, and so are vulnerable to them. The latest strains of ransomware recognize it is crucial to find and lock backups alongside the primary dataset. And so an attack might wait until the backup is effectively neutralized, ensuring that the victim has no other option than to pay up.

Learn more

PART 3

Protecting What's Most Important—Your Data

The attacker wants your data, not your network

While all cyber attacks can be damaging, **ransomware attacks disrupt an organization's most valuable asset: their data.** Centralized file storage solutions are a particularly attractive target for ransomware actors.

The network is not the target of a ransomware attack, it's merely a barrier to get around. The goal is to seize the data, so the best security stance to combat ransomware should be at the data level.

Who is responsible for protecting data?

Ultimately, the security of your company is a responsibility that every member of the organization shares, but **when it comes to protecting data, it's integral to the IT role.**

This responsibility goes far beyond the traditional data protection tasks of backing up and restoring data. While that responsibility is key to maintaining business continuity should an attack take place, there is a lot that IT teams can do to stop ransomware attacks before they ever happen. Since control over data is the end goal of any ransomware attack, IT infrastructure & operations (I&O) expertise in handling the data layer on a regular basis puts their team in a greater position to protect that data. IT can go beyond routine activities and **play a proactive role in advanced data protection solutions that reduce the risks of ransomware attacks.**

These actions are all part of **taking a data-centric approach** to ransomware protection.

Learn more

PART 4

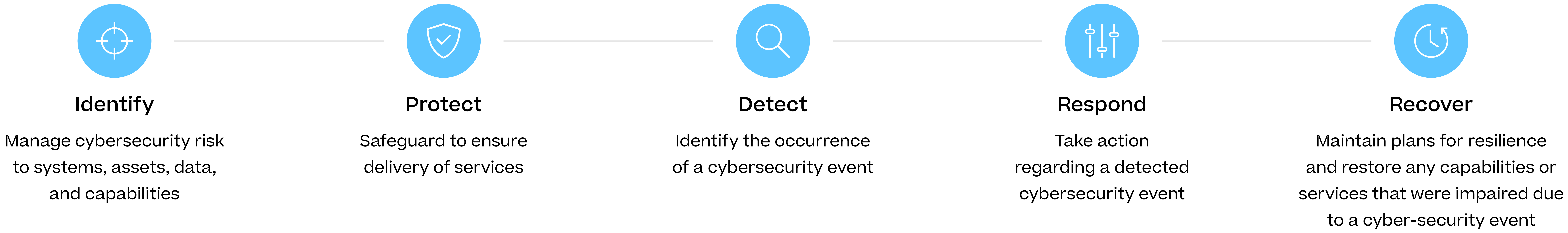
The Data-Centric Approach to Ransomware Protection

In a data-centric context, cyber resilience is centered around the state of the data itself, with the overall system's wellbeing built from the data outward.

The goals for cyber resilience aren't specific to ransomware. Exploring and applying them in a data-centric context sets the required capabilities apart from the traditional security mechanisms and enables us to significantly increase the security posture of the organization.

A core part of understanding a data-centric security posture is to consider how cyber resilient systems are built.

As defined by the National Institute for Standards and Technology (NIST) in "Ransomware Risk Management: A Cybersecurity Framework Profile", cyber-resilient systems include five functions in their framework:



Identify

Manage cybersecurity risk to systems, assets, data, and capabilities

Protect

Safeguard to ensure delivery of services

Detect

Identify the occurrence of a cybersecurity event

Respond

Take action regarding a detected cybersecurity event

Recover

Maintain plans for resilience and restore any capabilities or services that were impaired due to a cyber-security event

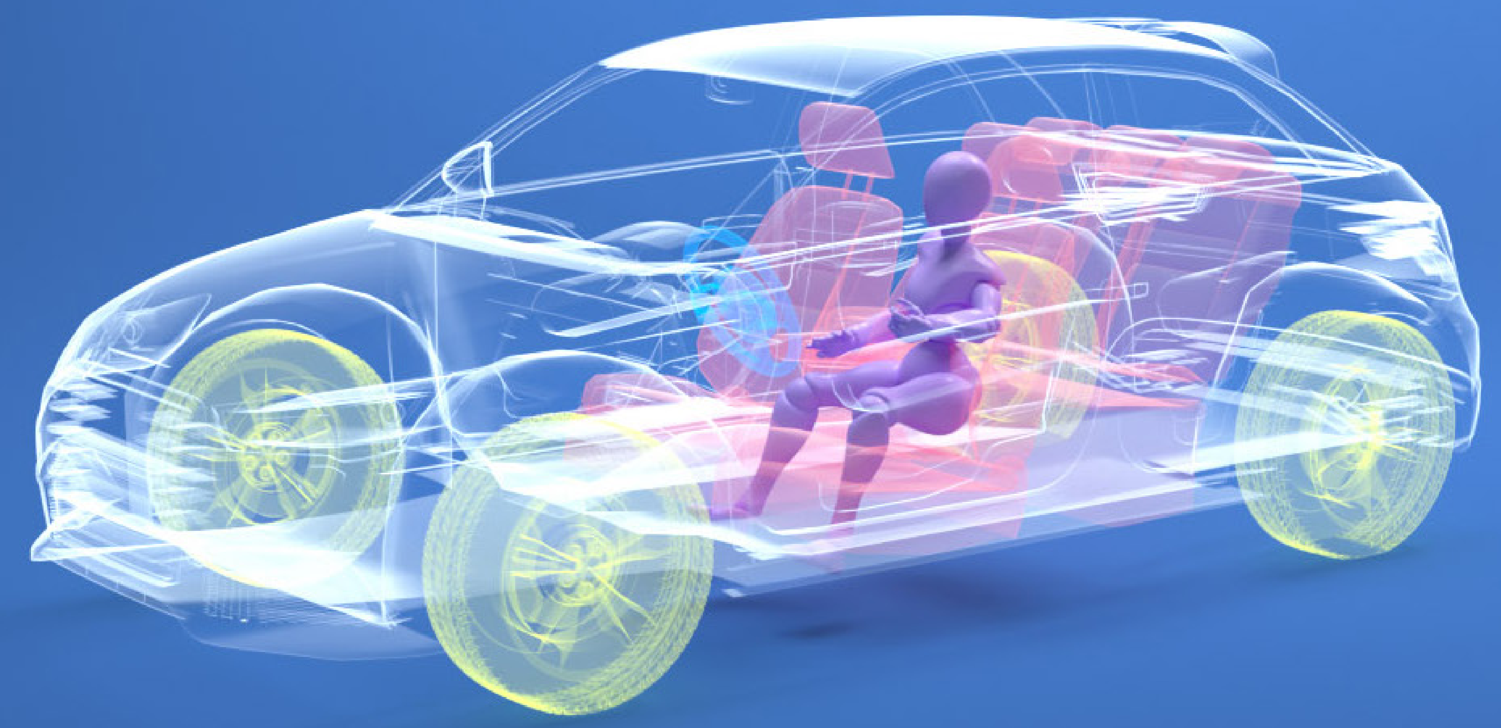
Learn more

Consider how cars are designed.

The airbags, seat belts, crush zones, car seat attach points, rollover strength, and side impact protection— **the most important safety features of a car — are all designed with one thing in mind: to keep the people inside the car safe.**

Some features, like proximity sensors, are there to make sure those features never need to be utilized, but no one gets into a car relying just on those sensors. People are the main focus of the most important safety features because people are more important than making sure the exterior, the engine, or the wheels survive an impact.

Data-centric cyber resilience is designed the same way—with your data as the number one priority.



Learn more

What does it mean to take a data-centric approach to ransomware protection?

Approach begins with data at the center, it starts from the innermost levels of data protection and then moves outward from level to the next.

These levels are:

Data content

Understanding what data you have and how it should be protected is key in ransomware defense.

Metadata

Your data attributes define who can access your data and what they can do with it.

Data usage

Continuously analyzing the behavior of how users and systems use your data allows you to detect when something is not right.

Data storage

Data storage capabilities allow you to respond and recover when ransomware is detected to ensure business continuity.

Automatic recommendations

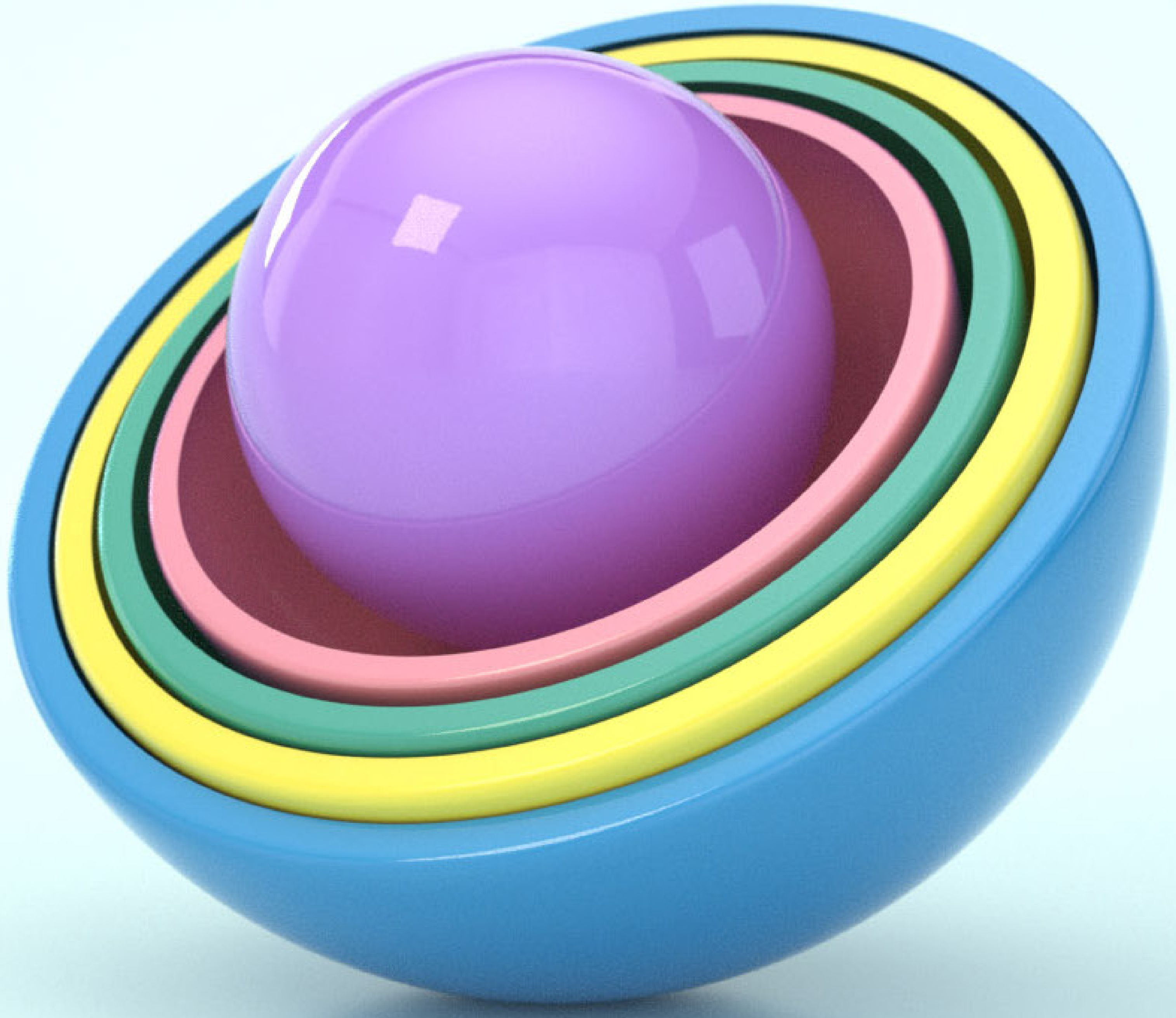
Understanding and adopting industry cyber resiliency best practices across the board provides a holistic approach to your protection strategy.

Perimeter security

Typical mechanisms such as firewalls and anti-virus software are examples of external-level security that should be implemented on top of data-centric layers.

Learn more

NetApp's Data-Centric Ransomware Protection

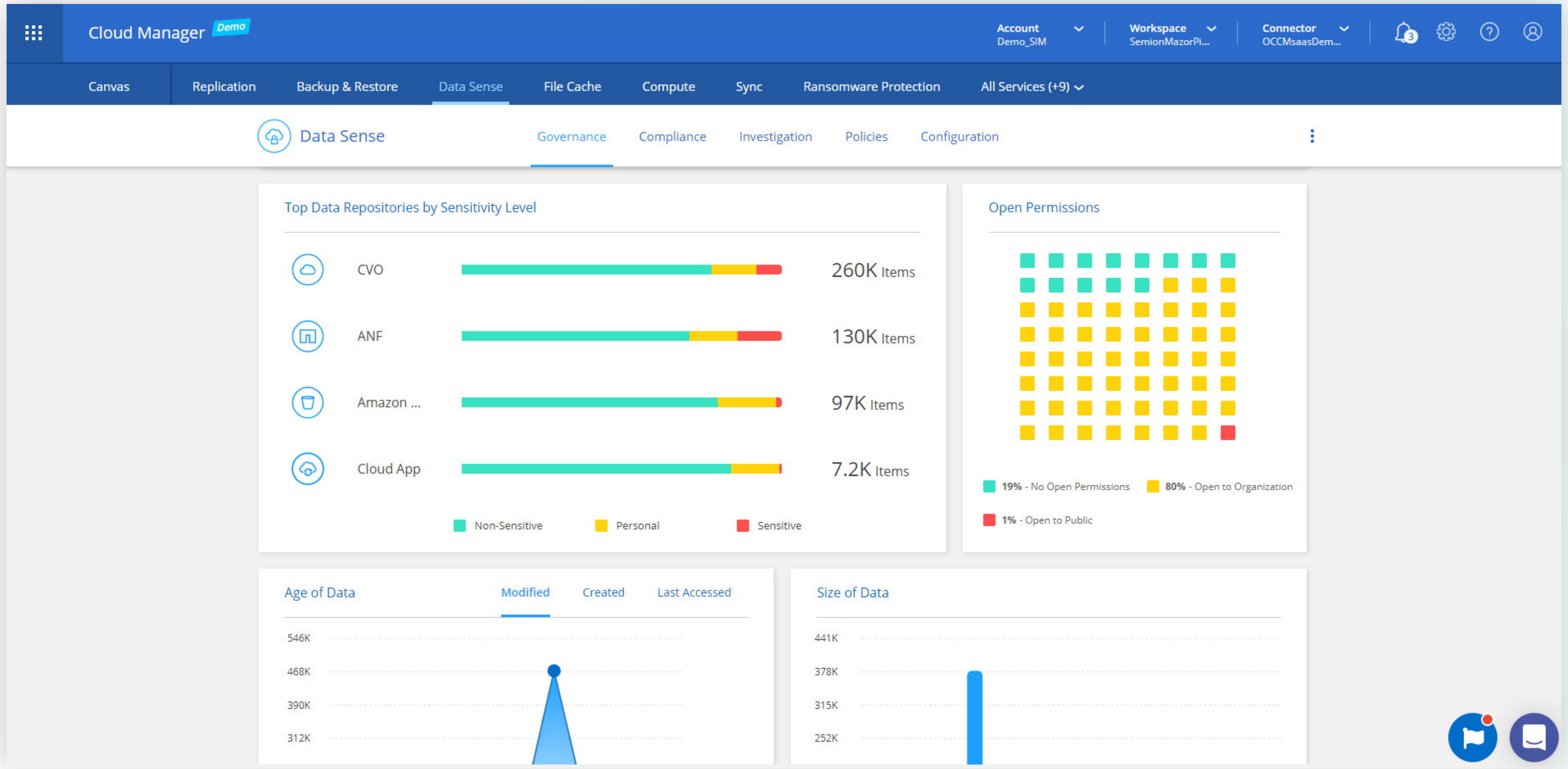


Let's explore NetApp's capabilities to implement comprehensive data-centric ransomware protection at each level

Data content

Data classification

Use **Data Sense**’s governance capabilities to better understand what information is stored in your data estate. Locate the most sensitive information using AI-driven analysis engines that categorize and classify your data. With this information, you can continuously make the right adjustments to properly secure your data and mitigate the risks involved with ransomware.



Easy data classification with Data Sense

Learn more

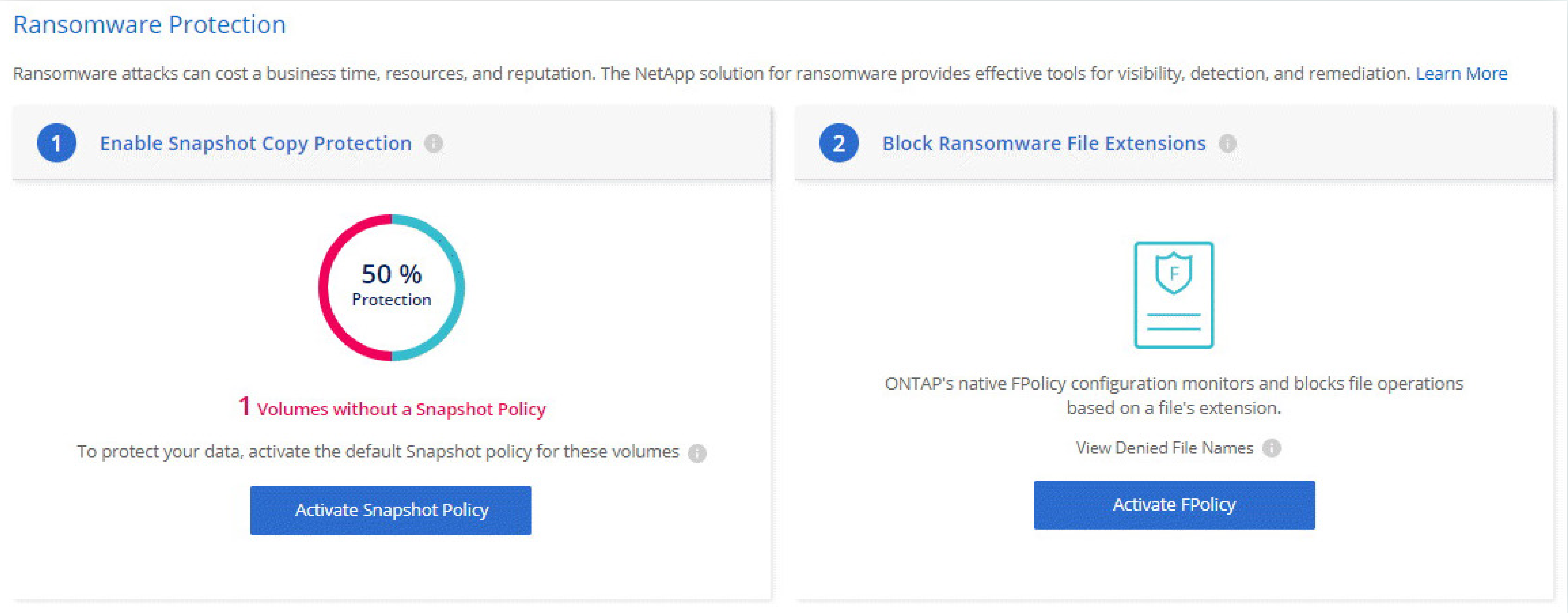
Metadata

Analyze file access permissions

Part of our governance capabilities includes constant insights into your first level of defense: file and folder level permissions. With **“Data Sense”** permissions analysis, enhanced filtering capabilities, and auditing, you can tighten your security and ensure the right people get access to the right data, at the right level.

Malicious file blocking

Based on access permissions set across your data estate, data gets created only where it’s allowed, and that includes files encrypted by ransomware during an attack. With **ONTAP**’s file access notification framework (**FPolicy**), you can block file creation and other operations based on known ransomware file extensions. This policy can be implemented even if an attacking user or computer instance has write permissions to folders.



Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. Learn More

1 Enable Snapshot Copy Protection

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

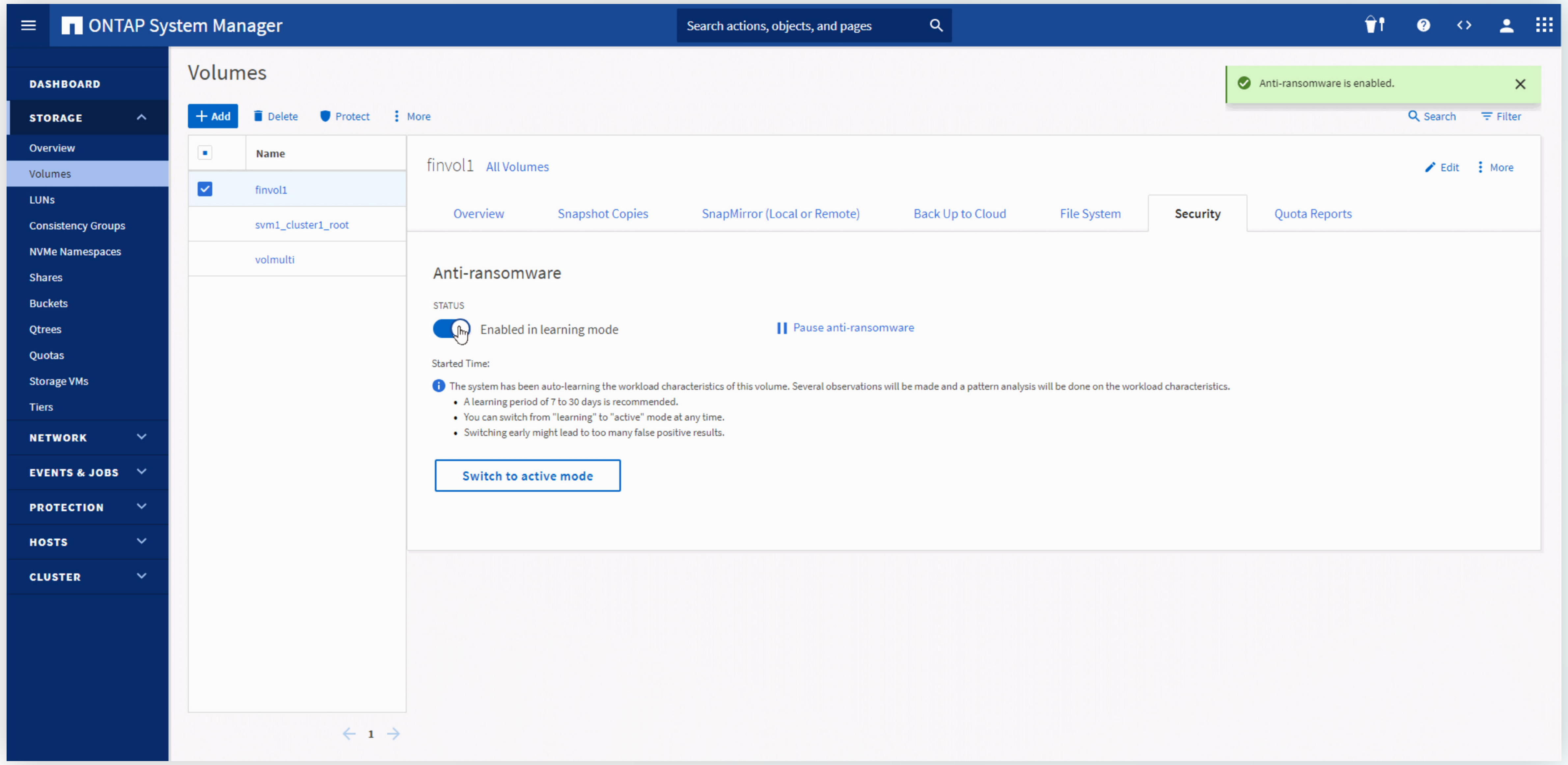
ONTAP’s malicious file blocking with **FPolicy**

Learn more

Data usage

Storage anomaly detection

Using machine learning capabilities, **ONTAP** is able to identify, prevent, or limit sophisticated ransomware attacks by continuously analyzing workloads (available from **ONTAP 9.10.1**). This anti-ransomware feature uses workload analysis in NAS (NFS and SMB) environments to proactively detect and warn about abnormal activity that could point to a ransomware attack. When the system detects an attack, anti-ransomware creates a new **Snapshot** copy in addition to the ongoing protection from scheduled snapshots.



Anti-ransomware is enabled.

Anti-ransomware

STATUS

Enabled in learning mode

Started Time:

The system has been auto-learning the workload characteristics of this volume. Several observations will be made and a pattern analysis will be done on the workload characteristics.

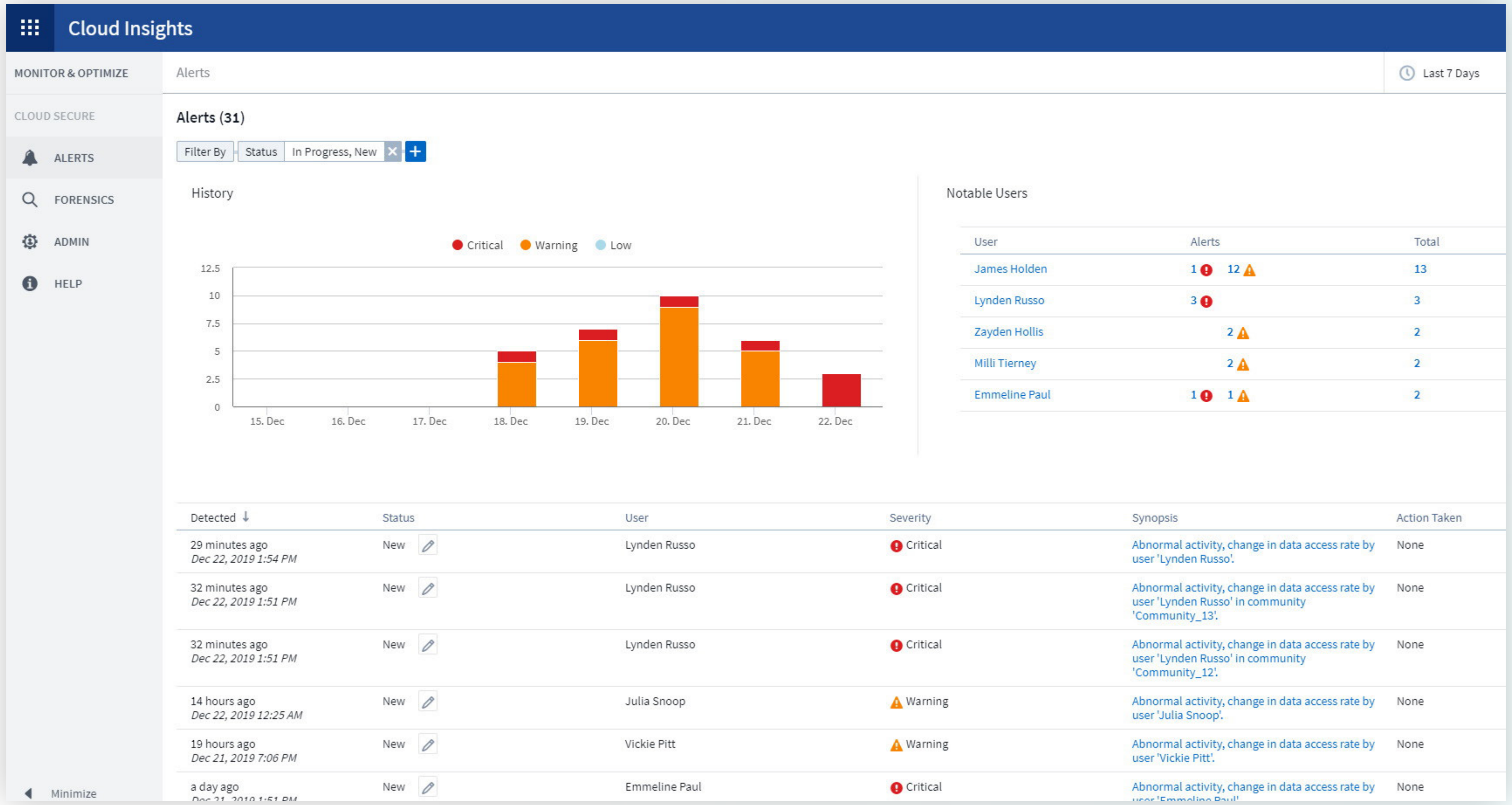
- A learning period of 7 to 30 days is recommended.
- You can switch from "learning" to "active" mode at any time.
- Switching early might lead to too many false positive results.

ONTAP's autonomous anti-ransomware feature

Learn more

User anomaly detection

Ongoing **user behavior analytics (UBA)** is required to identify, prevent, or limit sophisticated ransomware attacks. **NetApp's UBA** capability tracks the behavior of individual users and communities to identify typical data access patterns. It then reports when behavior differs from the normal observed pattern. In such cases, **UBA** can proactively respond by denying access to files and folders where suspicious activity is taking place and take further actions to protect your data using **Cloud Secure** and **FPolicy** external mode.



Alerts (31)

Notable Users

User	Alerts	Total
James Holden	1 ❗ 12 ⚠	13
Lynden Russo	3 ❗	3
Zayden Hollis	2 ⚠	2
Milli Tierney	2 ⚠	2
Emmeline Paul	1 ❗ 1 ⚠	2

Detected ↓	Status	User	Severity	Synopsis	Action Taken
29 minutes ago *Dec 22, 2019 1:54 PM*	New	Lynden Russo	❗ Critical	Abnormal activity, change in data access rate by user 'Lynden Russo'.	None
32 minutes ago *Dec 22, 2019 1:51 PM*	New	Lynden Russo	❗ Critical	Abnormal activity, change in data access rate by user 'Lynden Russo' in community 'Community_13'.	None
32 minutes ago *Dec 22, 2019 1:51 PM*	New	Lynden Russo	❗ Critical	Abnormal activity, change in data access rate by user 'Lynden Russo' in community 'Community_12'.	None
14 hours ago *Dec 22, 2019 12:25 AM*	New	Julia Snoop	⚠ Warning	Abnormal activity, change in data access rate by user 'Julia Snoop'.	None
19 hours ago *Dec 21, 2019 7:06 PM*	New	Vickie Pitt	⚠ Warning	Abnormal activity, change in data access rate by user 'Vickie Pitt'.	None
a day ago *Dec 21, 2019 1:51 PM*	New	Emmeline Paul	❗ Critical	Abnormal activity, change in data access rate by user 'Emmeline Paul'.	None

User anomaly detection in **Cloud Secure**

Learn more

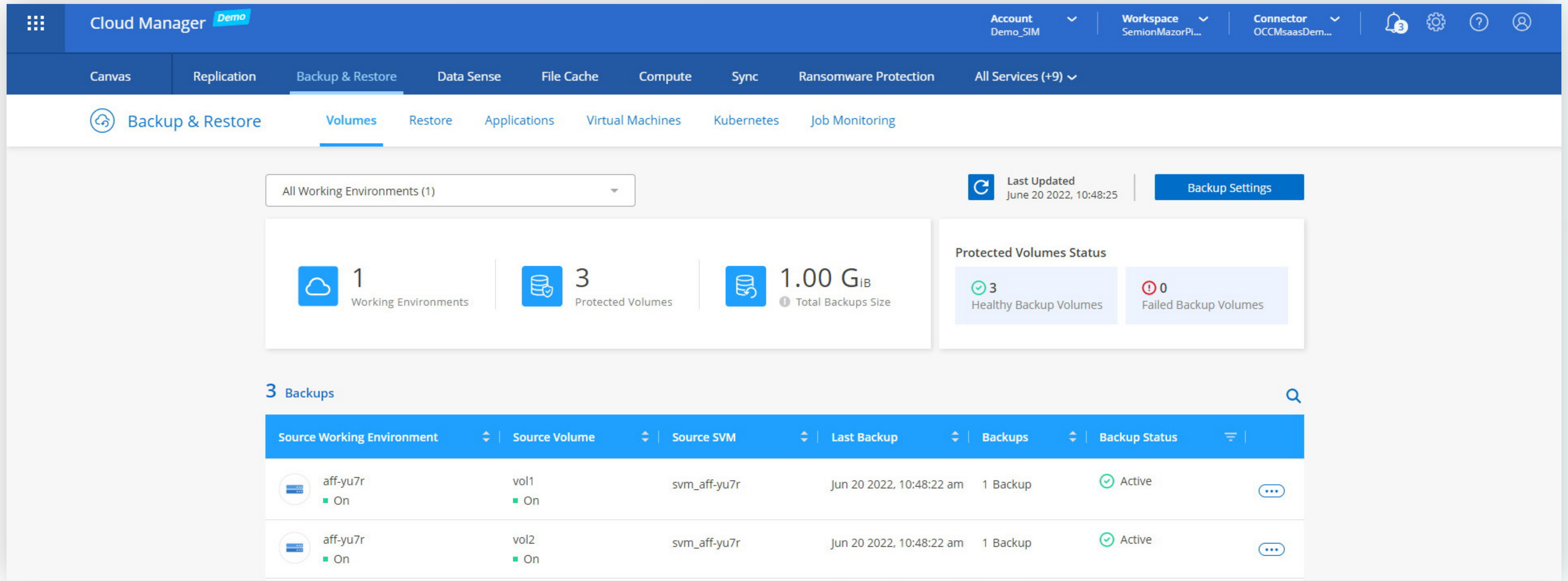
Data storage

Immutable data copies

Data stored in **ONTAP** systems is protected by **Snapshot**, which is a point-in-time, read-only image of your data that shows exactly what your data looked like the moment the snapshot was taken. Since **Snapshot** images are read-only, captured data can't be encrypted and locked by ransomware. With the **FlexClone** and **SnapRestore** features, you are able to restore an entire volume or individual files from a snapshot in the event of a ransomware attack, significantly faster than with any other possible recovery method.

Secure backup

Immutable backups, such as those provided by **NetApp Cloud Backup**, help bring your business back online without having to pay heavy ransoms in the event of an attack. With immutable backups, you can honor customer SLAs and recovery point objectives. **Cloud Backup**'s incremental forever backups on the block level provide faster restores that are more cost-efficient than any other backup solution on the market.



Last Updated
June 20 2022, 10:48:25

1 Working Environments

3 Protected Volumes

1.00 GiB Total Backups Size

Protected Volumes Status

3 Healthy Backup Volumes

0 Failed Backup Volumes

3 Backups

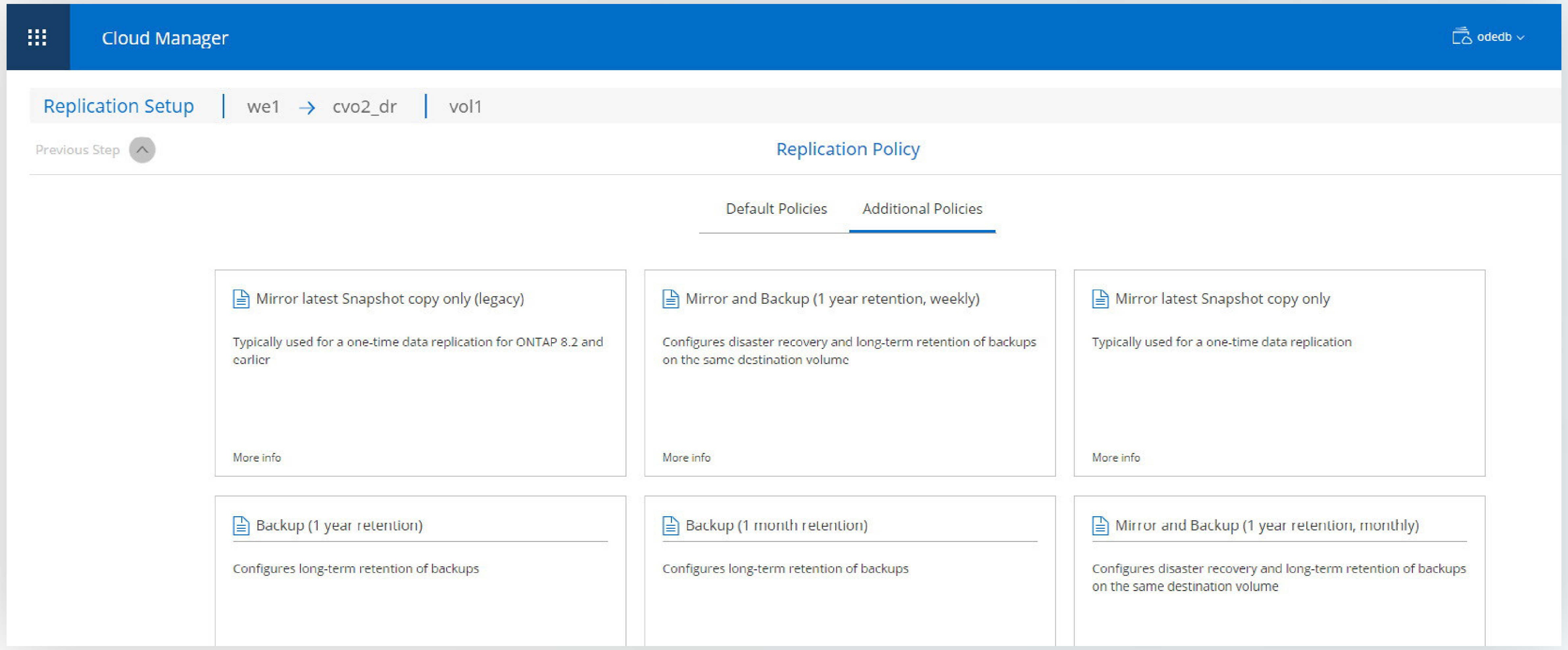
Source Working Environment	Source Volume	Source SVM	Last Backup	Backups	Backup Status
aff-yu7r On	vol1 On	svm_aff-yu7r	Jun 20 2022, 10:48:22 am	1 Backup	Active
aff-yu7r On	vol2 On	svm_aff-yu7r	Jun 20 2022, 10:48:22 am	1 Backup	Active

Secure backup with **NetApp's Cloud Backup**

Learn more

Efficient replication

To add another layer to your data protection strategy, data can be easily and efficiently replicated to a different geographic location. These data recovery sites can be created with **Cloud Volumes ONTAP** or **Amazon FsX** for **NetApp ONTAP**. Since NetApp's data replication engine replicates your immutable snapshots, your secondary copy is protected and can also be used to recover from attacks. Entire snapshots or individual files can be replicated back to the original location or, in a worst-case scenario, you can failover to your data recovery site and work on a ransomware-free copy of your data.



Mirror latest Snapshot copy only (legacy)
Typically used for a one-time data replication for ONTAP 8.2 and earlier

Mirror and Backup (1 year retention, weekly)
Configures disaster recovery and long-term retention of backups on the same destination volume

Mirror latest Snapshot copy only
Typically used for a one-time data replication

Backup (1 year retention)
Configures long-term retention of backups

Backup (1 month retention)
Configures long-term retention of backups

Mirror and Backup (1 year retention, monthly)
Configures disaster recovery and long-term retention of backups on the same destination volume

Efficient replication engine

Learn more

Air gap copies

Air-gapped backups prevent malicious activities from accessing your additional copy of the data. By creating a **WORM** (Write Once Read Many) volume, **SnapLock** prevents your production data and snapshots from being tampered with, resulting in a **logical air gap** of your data that is quickly accessible, safe from deletion, and immutable.

Active Directory monitoring

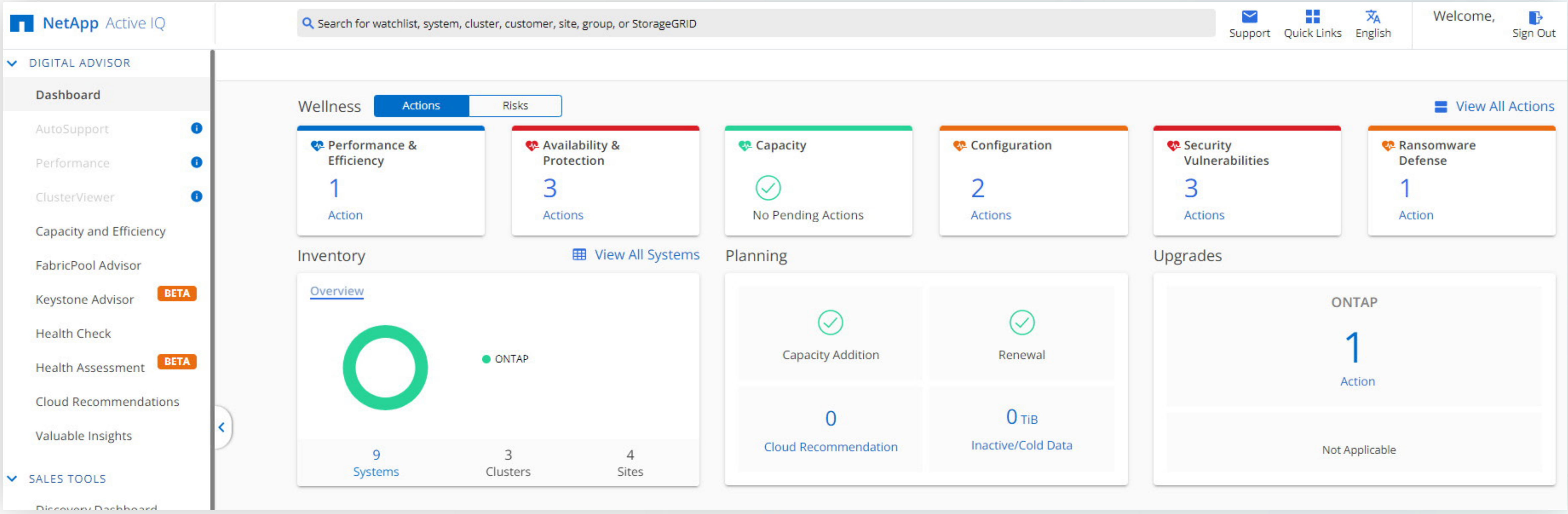
Your Active Directory retains a lot of information and is responsible for many functionalities of your domain assets including resource allocation, authentication, authorization, and more. Therefore, it's a "holy grail" for infiltrators who use it to gain access, escalate privileges, and collect information on your network. It's important to constantly monitor your Active Directory with tools like Data Sense to find anomalous activities or unnecessary privilege allocations and remove possible security gaps that exist.

Learn more

Automatic recommendations

Alerting and recommendations

NetApp provides built-in tools to help detect ransomware in early stages. For **ONTAP** in particular, these tools include **Active IQ Unified Manager** and **Active IQ Digital Advisor**. These tools alert about abnormal Snapshot copy and volume growth rates, and loss in storage efficiency, which may indicate an ongoing ransomware attack. They also alert when there are snapshot creation failures and unconfigured security capabilities, such as **FPolicy**.



Active IQ Unified Manager’s recommendations

Learn more

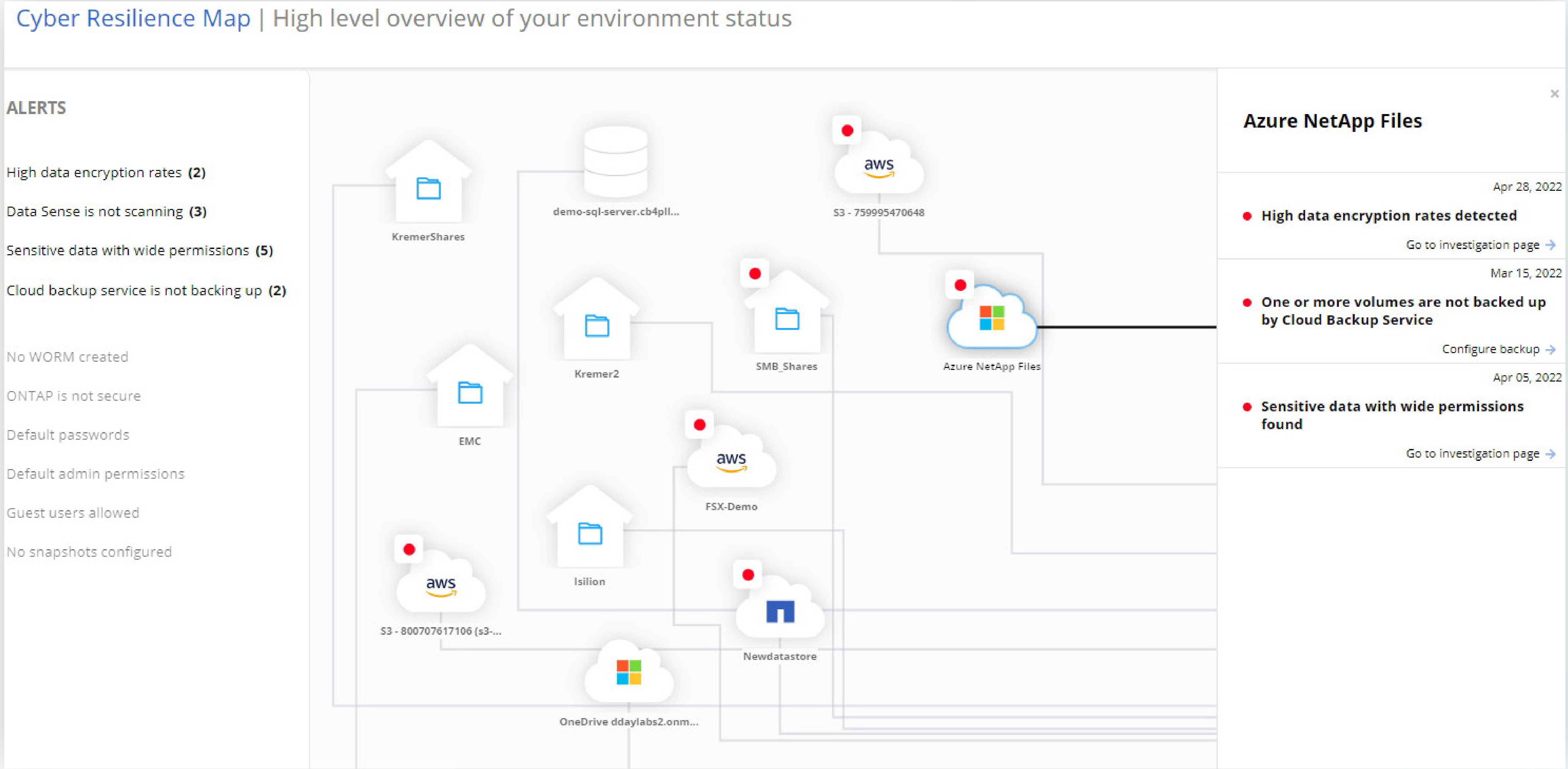
Single pane of glass

NetApp also offers a dedicated **Ransomware Protection Dashboard** in **Cloud Manager** that allows you to respond to threats in real time.

This dashboard provides your IT teams with **insights into the cyber resiliency posture** of their entire on-prem and cloud data estate. The dashboard also offers a single interface to multiple ransomware protection tools.

The dashboard additionally scores your system's cyber resiliency and readiness with built-in best practice recommendations. This allows you to identify problem areas without the overhead of searching for them on your own.

IT teams can use these advanced defense mechanisms to ensure your most critical data is protected and to strengthen cyber resilience.



Cyber Resilience Map | High level overview of your environment status

ALERTS

High data encryption rates **(2)**

Data Sense is not scanning **(3)**

Sensitive data with wide permissions **(5)**

Cloud backup service is not backing up **(2)**

No WORM created

ONTAP is not secure

Default passwords

Default admin permissions

Guest users allowed

No snapshots configured

Azure NetApp Files

Apr 28, 2022

- **High data encryption rates detected**

Go to investigation page →

Mar 15, 2022

- **One or more volumes are not backed up by Cloud Backup Service**

Configure backup →

Apr 05, 2022

- **Sensitive data with wide permissions found**

Go to investigation page →

Cloud Manager's Ransomware Protection Dashboard

Learn more

NetApp

Get Cyber Resilient with NetApp Ransomware Protection

At NetApp, we've been providing industry-leading data management solutions for decades. That's why we understand data protection better than anyone and are perfectly positioned to offer the most comprehensive suite of tools to protect your data.

Netapp Ransomware Protection is a comprehensive set of data-centric capabilities, allowing you to protect your data estate with a zero trust approach from the inside out. It enables you to map and classify your data, detect abnormal user activity, manage access, and avoid costly downtime with rapid backup and restore. IT teams can use these advanced defense mechanisms to strengthen your cyber resiliency and make sure your most critical data stays protected.

Learn more about Ransomware Protection

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

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

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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NA-000-0322