

# Ransomware Protection and Recovery with APEX Backup Services

## Accelerated Ransomware Recovery

August 2022

H19156

## White Paper

### Abstract

This white paper focuses on ransomware protection and recovery with APEX Backup Services.

Dell Technologies

## Copyright

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel, the Intel logo, the Intel Inside logo and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners. Published in the USA August 2022 H19156.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

# Contents

Executive summary.....4

APEX Backup Services – ransomware protection and recovery .....5

APEX Backup Services – ransomware recovery dashboard.....16

Conclusion.....20

References .....21

## Executive summary

### Business challenges

Ransomware is a relentless threat to every enterprise and the attacks are becoming more frequent, advanced, and expensive. Ransomware is a form of malware that encrypts victims' data so threat actors can demand a "ransom" in exchange for a decryption key needed to unlock your data. Even if the ransom is paid, there is no guarantee that the attacker will provide you with the decryption key. In today's diverse and distributed IT environment, restoring your organization's applications and data quickly after a ransomware attack is a significant challenge. Reliable backup and recovery are a crucial line of defense against ransomware.

### Solution

**Dell Technologies APEX Backup Services ransomware recovery** is a fast, reliable data recovery solution that eliminates any reason to even think of paying a ransom. APEX Backup Services is based on a secure and robust cloud architecture that can help you protect your business assets, limit the impact of ransomware, and accelerate recovery. Ransomware cannot modify or delete data protected in APEX Backup Services. APEX Backup Services can ensure that your backup data is safe, help you operationalize security across your backup and primary environments, and accelerate the recovery process so you can get back to normal faster.

### Revisions

Date	Description
August 2022	Initial release

### We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by [email](#).

**Author:** Vinod Kumar Kumaresan

---

**Note:** For links to other documentation for this topic, see [APEX Backup Services](#)

---

## APEX Backup Services – ransomware protection and recovery

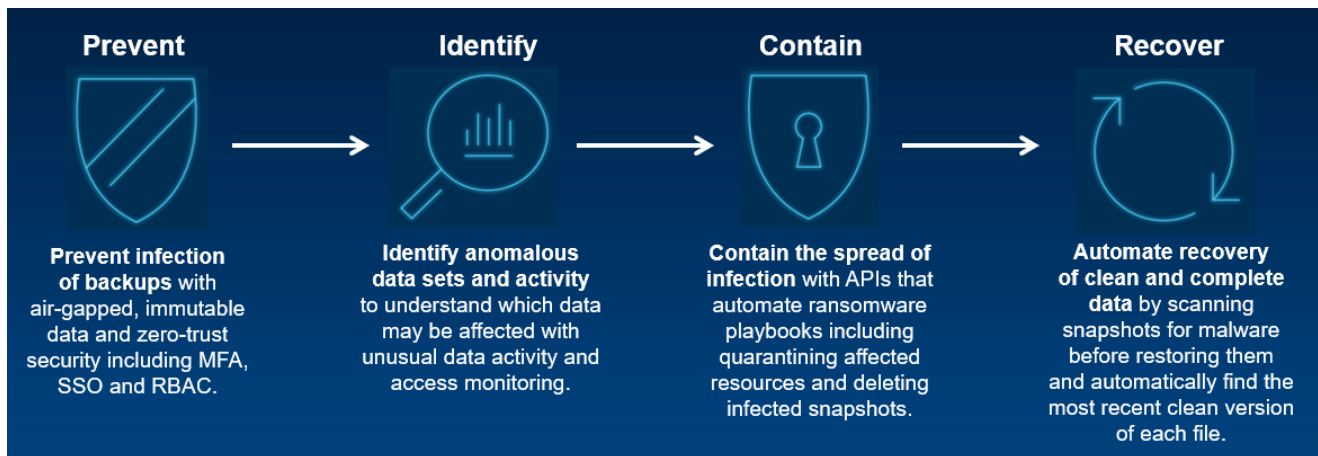
APEX Backup Services empowers security operations and IT teams to protect, detect, respond, and recover faster from external or internal attacks, ransomware, as well as accidental or malicious data deletion.

APEX Backup Services offers immutable protection and backup data is isolated from the customer's network and protected within the APEX Backup Services platform. APEX Backup Services accelerated ransomware recovery module prevents data loss, reduces costs, and accelerates ransomware attack response and recovery.

Today, APEX Backup Services provides accelerated ransomware recovery for endpoints and hybrid workloads (databases, file systems, virtualized environments, and NAS).

### Steps to protect from and limit the impact of ransomware

The secure and robust cloud architecture of APEX Backup Services can help you protect your business assets and limit the impact of ransomware on your organization. APEX Backup Services provides a powerful ransomware recovery service with below capabilities.



**Figure 1. APEX Backup Services – Ransomware recovery and response**

### Protection

The first step in preventing damage from ransomware is ensuring that you have a clean backup copy of your data. Built on highly resilient cloud infrastructure, APEX Backup Services makes it impossible for ransomware to encrypt backup data. Zero trust architecture, including multi-factor authentication, envelope encryption, and separate account access ensures that ransomware cannot use compromised primary environment credentials to tamper with backup data. Finally, excess deletion prevention and soft-delete (recycle bin) features provide a further layer of security to safeguard backups against deletion.

#### Air-gapped backups and object-based storage

Ransomware cannot execute in the APEX Backup Services environment thanks to how its Resiliency Cloud is built.

- The APEX Backup Services platform is not accessible using customer OS/system credentials

- Data is never stored as-is. APEX Backup Services stores data as smaller application-aware blocks before being stored in an object store
- Without access to an operating system, the malware cannot execute on its own. It cannot establish any communication with its command-and-control center for any further triggers or execution code
- The APEX Backup Services cloud environment is not based on Windows and does not depend on the direct-attached storage, Active Directory applications, or Remote Desktop Protocols typically used by ransomware

As an extra layer of security, APEX Backup Services retains deleted snapshots in an inaccessible cache for seven days. It is therefore possible to restore data even if it has been deleted from the backup environment.

### Encryption

Another key to security is encryption for data, both in flight and at rest. APEX Backup Services provides a secure, multi-tenant environment for customer data.

- APEX Backup Services issues unique per tenant AES-256 encryption keys and offers encryption for data in flight and at rest. The use of one unique encryption key per customer along with customer held key encryption keys, creates crypto segmentation between customers, preventing data leakage
- APEX Backup Services stores the data by splitting it into blocks and deduplicating, with unique data blocks stored in AWS S3. Metadata is stored in AWS DynamoDB. AWS EC2 provides the computational layer to enable elastic scalability
- The application layer is separate from the data layer. As a result, anyone having access to the application layer does not get access to the data layer
- Within the data layer, APEX Backup Services encrypts the data using envelope encryption technology, making it impossible for anyone besides the customer to access the data

### Envelope encryption

Our platform uses a digital envelope encryption model, so your data is protected two-fold. First, a unique key is generated, encrypted, and turned into a token, which is then stored. This token can only be accessed by the administrator or end user providing their credentials as the complementary part to decrypt the stored token; and second, the data itself is also encrypted. To access the encrypted data, both parts of the equation need to work together to recreate the key, which only exists in that unique session. Because only the administrator or end user has access to that token, anyone who wants the data would have to go to them to get the first piece of the puzzle. Effectively, no one can access the data without your knowledge.

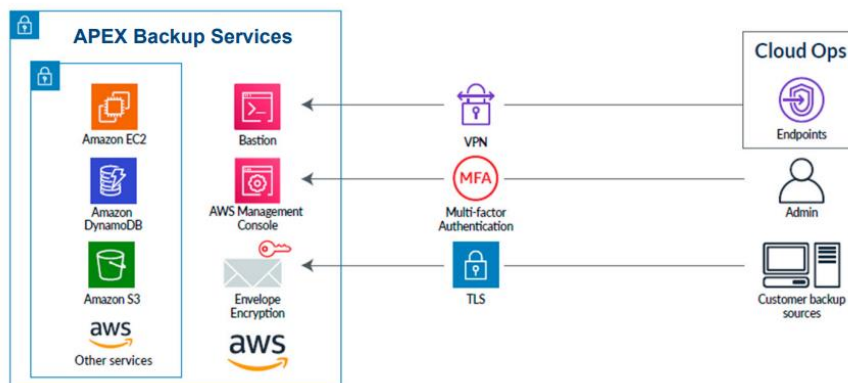
### Access Control

One of the most effective ways to protect data is to limit who can access it. If too many people can access and delete data or reassign administrative roles, threat actors can compromise even low-level credentials, and use them to destroy data or lock other administrators out of the backup environment.

APEX Backup services provides RBAC (Role Based Access Control). It is strongly recommended to ensure that only a small group of administrators can perform destructive actions such as deleting backup data.

- Administrative control settings prevent end users from deleting backup data. You can also require that two administrators approve major deletions.
- APEX Backup Services also allows you to customize admin roles to prevent deletion (screenshot below). As a best practice, designate no more than two people in the organization as admins with the power to delete snapshots.
- Geofencing capabilities ensure that access to the backup environment is for known IP addresses blocking out potential attacks from any bad actors or embargoed countries.
- Dell Technologies employees cannot access customer data or infrastructure directly, in line with our secure by design philosophy. APEX Backup Services has strict logical access controls to prevent access to production backup nodes. No Dell Technologies employees have direct (SSH) access to servers processing backup operations.

It is also important to consider access control for vendor employees. Due to our unique encryption, Dell Technologies never has access to customer data. There is strict control on how developers can access the code that powers APEX Backup Services.



**Figure 2. Access control**

- Access to applications is monitored and controlled using a multi-factor authentication and access control using a combination of Bastion, VPN, MFA, and auto expiring dynamic credentials
- There is no SSH access to production nodes, closing potential security threats from that access point

### Zero Trust Security

Access control is only effective if it is difficult to compromise administrative profiles. To prevent threat actors from gaining access to the backup environment using compromised credentials, you can implement zero trust security protocols.

Zero Trust is a security model based on strict verification processes. This approach treats every access attempt as if it originates from an untrusted source and access is only granted after identity has been verified.

APEX Backup Services was designed around a zero-trust security architecture and offers rich multi-layered defense features including MFA (Multi-Factor Authentication). Built natively on AWS's security framework, APEX Backup Services also inherits the global security, compliance, and data residency controls, thus adhering to the highest standards for privacy and data security.

### Stringent security compliance and certifications for APEX Backup Services

Third-party validation supports the trustworthiness of the security of any SaaS service. APEX Backup Services can claim compliance with the following certifications and frameworks, including (but not limited to):

- SOC 2 type II audited
- HIPAA compliance
- FIPS 140-2 compliant (GovCloud environments)

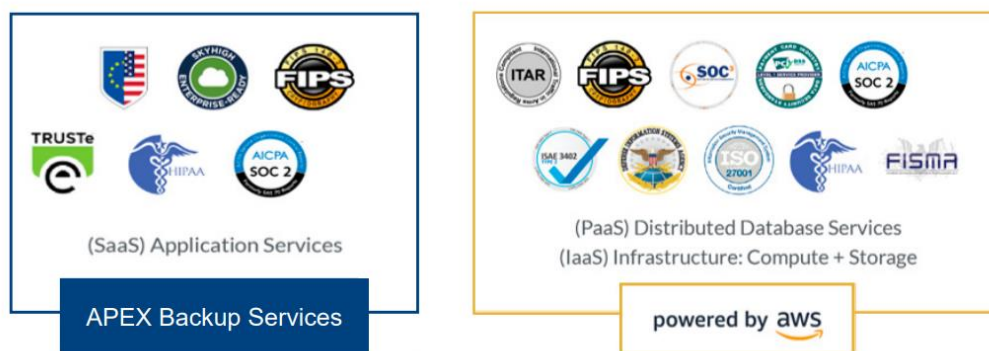


Figure 3. APEX Backup Services - security compliance and certifications

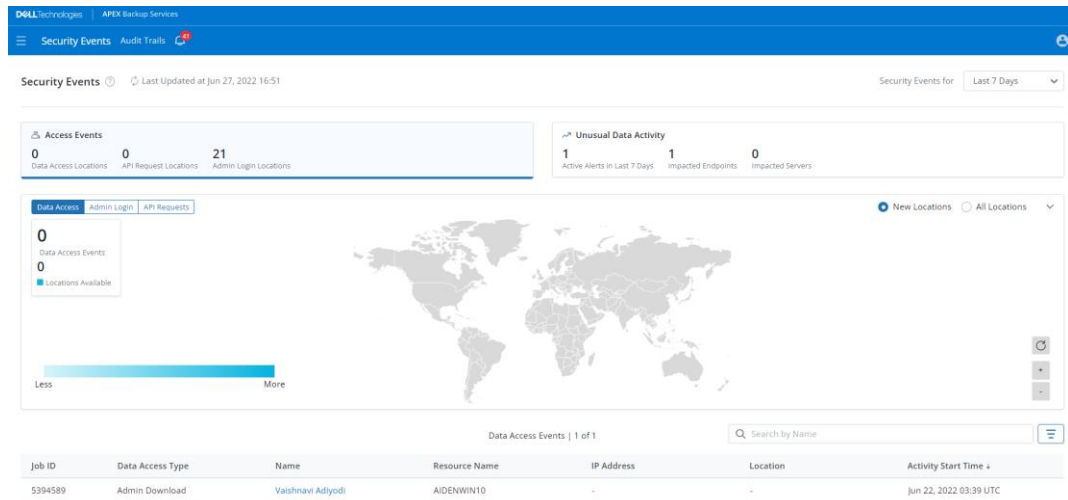
## Detection

Detecting a ransomware attack as soon as possible can help prevent contamination spread. The APEX Backup Services accelerated ransomware recovery module provides access insights and anomaly detection that help you quickly identify possible ransomware attacks. Access insights let you see location, identity, and activity information for all access attempts. Anomaly detection uses proprietary ML algorithms to provide alerts for unusual data activity. The algorithm learns the norms for your specific backup environment, so it does not require any rules setup or tuning. It also uses entropy-based insights to reduce false positives.

### Monitoring security events

APEX Backup Services offers "Security Events", a dashboard that shows you upfront the count of all administrator login events, data access events, API requests, and unusual data activity alerts, and nudges you to take remedial actions if required. This data helps you gain situational awareness about the backed-up data by gathering events from all APEX Backup Services products.





**Figure 4. Ransomware recovery - Security Events**

The security events dashboard displays the following:

- The total count of administrator logins and API requests from new locations
- The restore and download activities performed by administrators and users
- The locations from where administrators have logged into the APEX Backup Services Cloud platform. The locations are displayed on a map for easy visual reference
- The locations from where administrators have made an API request with several important details
- The number of unusual data activity alerts generated
- The number of endpoints and servers that have been quarantined. You can click the count to view the list of quarantined resources

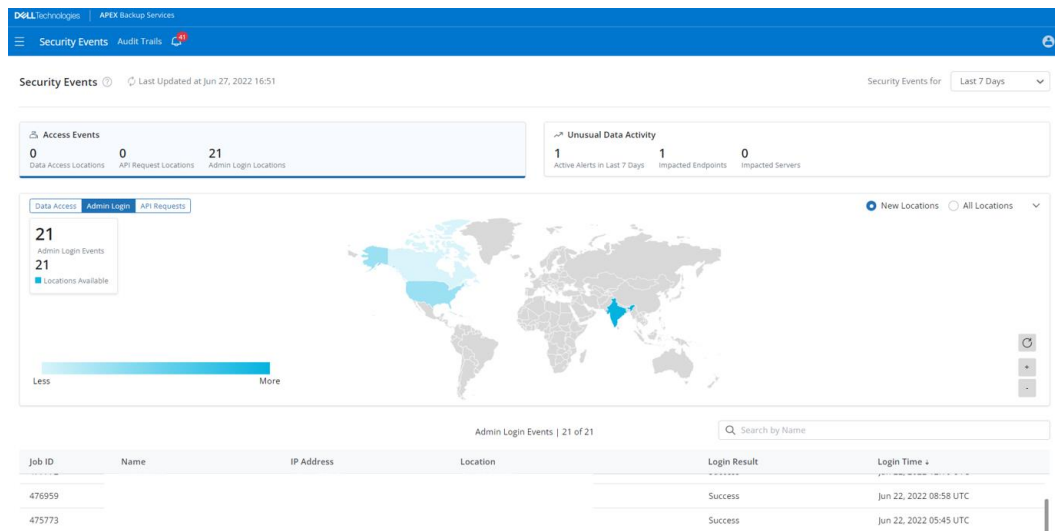
### Anomaly detection

The APEX Backup Services accelerated ransomware recovery module provides access insights and anomaly detection that help you quickly identify possible ransomware attacks. Access insights lets you see location, identity, and activity information for all access attempts.

### Access Insights:

The APEX Backup Services dashboard provides a single pane of glass where you can see all access attempts and activity across all your data sources, including:

- Which users and APIs accessed your backup environment
- Where access attempts originated geographically
- When access attempts were made
- What actions were attempted (recover, delete, and so on)



API integrations can feed this information into SIEM (security information and event management) applications such as Splunk and Arcsight for correlation and accelerated incident response.

### Unusual Data Activity

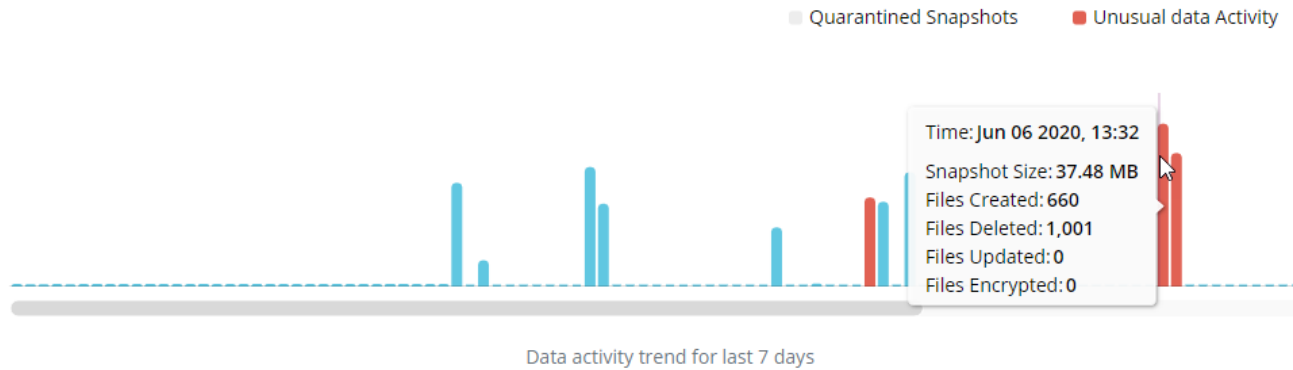
The Unusual Data Activity feature with APEX Backup Services provides continuous monitoring of your backup data. Our proprietary entropy-based algorithm uses machine learning to understand norms for your specific backup environment and provides automated alerts for unusual data activity including bulk deletion and encryption. You can use these insights to quickly identify affected snapshots during recovery. API integrations also enable you to feed these alerts to your SIEM solution, supporting ransomware detection.

Anomaly detection uses proprietary ML algorithms to provide alerts for unusual data activity. The algorithm learns the norms for your specific backup environment, so it does not require any rules setup or tuning. It also uses entropy-based insights to reduce false positives.

Suspicious modification of data on a resource is called Unusual Data Activity (UDA). A user or malicious software can make such changes.

When such a potential threat manipulates the data on a resource, it is suspicious in nature and is unlike how the resource owner works with data on that resource. Since anomalies of this type often indicate issues that require attention, APEX Backup Services flags any such anomalous behavior in a resource and generates an alert.

## Data Activity Trend

**Figure 5. Ransomware recovery - Unusual Data Activity**

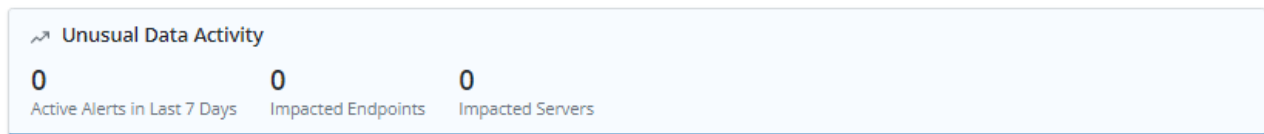
Monitors the data activity trend for a given resource, and after a sufficient sample size, it builds the anomaly baseline.

Following are the prerequisites to start scanning a resource:

- **33 snapshots:** The resource must have a minimum of 33 successfully backed up data snapshots.
- **30 days:** Scanning starts 30 days after the resource was configured for backup.

**Note:** The 30-day count starts from the day the Unusual Data Activity feature was enabled.

Being notified about the resources showing unusual data activity can help you identify a potential threat in your environment such as a ransomware attack or a compromised user.



Click the card to view details of the generated alerts.

6

Active Alerts

14

Total No. of Alerts

2

Total No. of Resources




Quarantine Resource

Download Logs

Total Alerts | 14 of 14

Q

Search by Resource Name

<input type="checkbox"/>	Resource Name	User Name	Affected Snapshot ↓	Alert Type	#Impacted Files ↑↓	Status
<input checked="" type="checkbox"/>	 DEV-13111	John D	May 28 2020, 14:02	Modification	701	Active
<input type="checkbox"/>	 DEV-18965	Ernie C	May 28 2020, 13:58	Deletion	628	Active
<input type="checkbox"/>	 DEV-18965	Ernie C	May 28 2020, 13:57	Creation	506	Active

**Figure 6. Ransomware recovery - UDA alerts**

For any unusual data activity alert, you can do any of the following:

- **Ignore the alert:** If you deem any alert as a false positive, click the resource name and select the false positive alert. Click Ignore to resolve the alert.

- **Quarantine the resource:** Select an alert and click Quarantine Resource to stop the ransomware from spreading further.

Beyond anomaly detection, the federated search aids forensic investigation teams in identifying which other data sources are infected, using a hash and metadata-based search, providing more clarity on the scope of a ransomware attack.

Response

When you have detected an attack, rapid response is vital to ensure a fast recovery. There are many valuable primary environment security tools that can be used for detection and orchestration. The APEX Backup Services accelerated ransomware recovery module offers robust API integrations, that make it easy to fit the solution into your overall security ecosystem. Orchestrating response activities using SIEM and SOAR solutions can dramatically reduce your mean time to respond (MTTR) by automatically completing actions, such as quarantining infected systems or snapshots, based on a predetermined ransomware playbook.

The APEX Backup Services accelerated ransomware recovery enables you to quarantine infected snapshots on the impacted resources, which helps safeguard your system from further infection by barring users or administrators from downloading or restoring data to other resources.

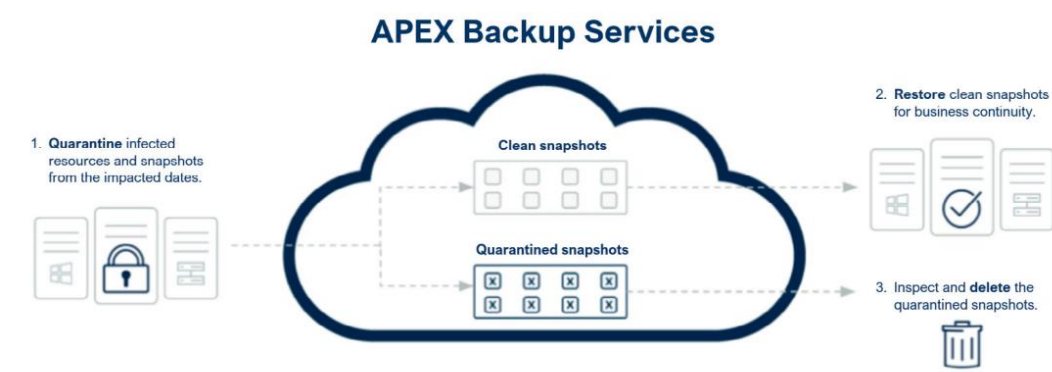


Figure 7. Ransomware recovery - Quarantine

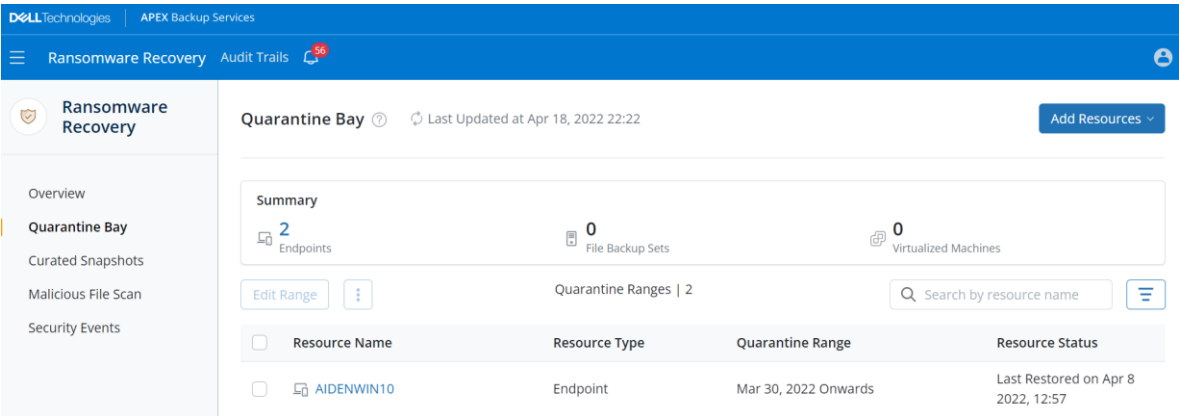


Figure 8. Ransomware recovery – Quarantine Bay dashboard

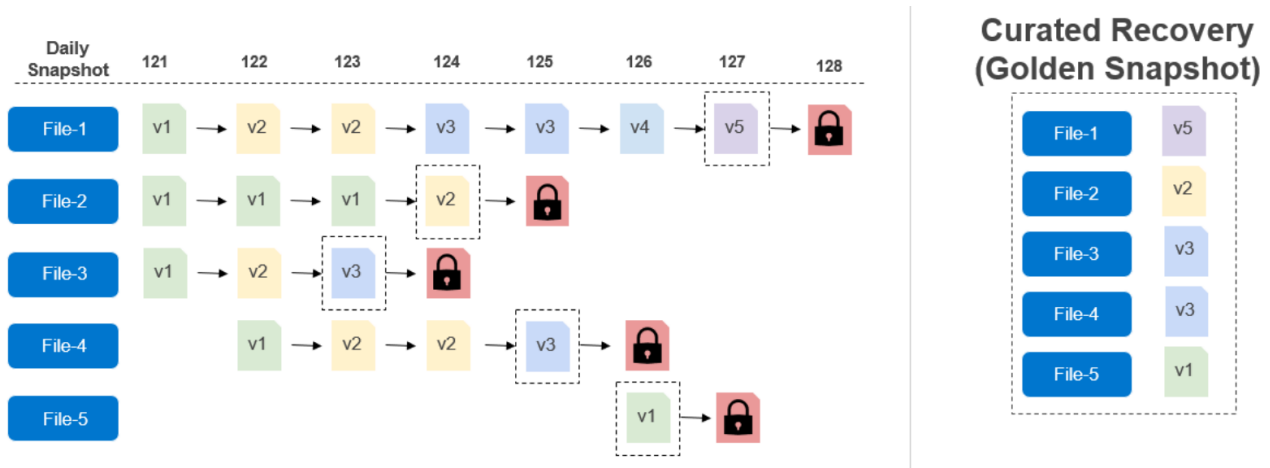
After you quarantine snapshots, access to the quarantined snapshots is blocked for the administrators and the users of that resource. Administrators and users cannot download data or restore data from the quarantined snapshots.

## Accelerated ransomware recovery

The APEX Backup Services cloud platform backs up workloads directly to the cloud, ready for immediate recovery if a ransomware attack occurs. The accelerated ransomware recovery module enables you to recover with confidence by ensuring the hygiene of recovery data. You can scan snapshots for malware and IOCs using built-in antivirus detection or using threat intelligence from your own forensic investigations or threat intel feeds. Scanning snapshots before recovery eliminates reinfection. Accelerated ransomware recovery also solves the problem of data loss due to point-in-time recovery. Now you can automatically identify the most recent clean version of every file within a specified timeframe and consolidate those versions into a single “Golden Snapshot”. Eliminating the manual search and recovery process drastically reduces time to recover and prevents data loss.

### Curated Recovery

APEX Backup Services offers a unique solution to the problem of finding and restoring the most recent unencrypted version of files or data sets after an attack. Until now, IT departments have been forced to restore from a point in time before the initial infection, then manually search for more recent versions of individual files. The Curated Recovery feature automates this process, saving time and ensuring that you have the most recent unencrypted version of all data. The Curated Recovery feature automatically finds the most recent clean version of each file and compiles it into a single curated snapshot.



**Figure 9. Ransomware recovery – Curated Snapshot**

Now you can simply define the time-period of the attack (from initial infection to the present) and let Curated Recovery automatically find the best version of each file.

Create Curated Snapshot for Servers

Resources > Snapshot Details

Snapshot Parameters

Curated Snapshot contains the cleanest and most recent version of the file processed from multiple snapshots within a defined date range.

Date Range ⓘ

Start Date

Select date

End Date

-

Select a date before the suspected intrusion

Retain Snapshot for

15

days

The snapshot will be available for restore during this retention period

Indicators of Compromise

☐ Exclude file extensions

Specify malicious file extensions to exclude from snapshot.

☒ Malicious files will be excluded

Curated Snapshot will be scanned for malware with pre-defined file hashes and antivirus engine.

Previous

Cancel

Finish

Figure 10. Creating curated Snapshot

The solution assembles clean versions into a single “golden snapshot” which you can use for recovery.

Dell Technologies

APEX Backup Services

Ransomware Recovery

Audit Trails

42

Ransomware Recovery

Overview

Quarantine Bay

Curated Snapshots

Malicious File Scan

Curated Snapshots ⓘ

Last Updated at Jun 27, 2022 16:58

Create Curated Snapshot ▾

Snapshot

Jobs 10

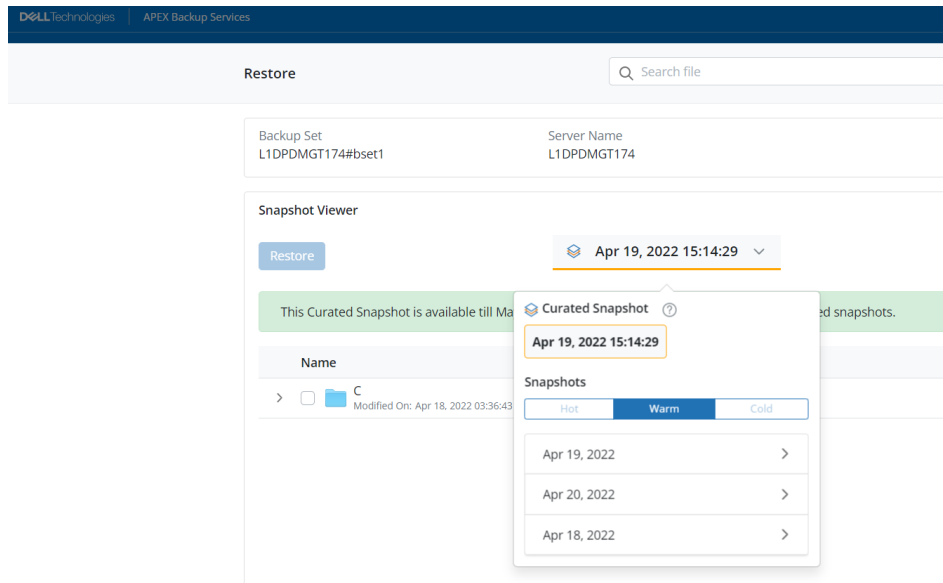
Delete Snapshot

Curated Snapshots | 2 of 2

Search by Resource Name

<input type="checkbox"/> Snapshot ↑↑	Resource Name ↑↑	Snapshot Size ↑↑	Retention till ↑↑	Job ID ↓
<input type="checkbox"/> Jun 15, 2022 17:40	win-01 Backup Set	190.94 MB	Jun 30, 2022 17:40 UTC	10
<input type="checkbox"/> Jun 8, 2022 22:30	Share Backup Set	2 GB	Jul 08, 2022 22:30 UTC	9

Figure 11. Ransomware recovery – Curated Snapshot console



**Figure 12. Performing recovery from hybrid workload console using curated snapshot**

### Malicious File Scan

Reinfection is every IT administrator's worst nightmare. Restoring contaminated data can cost your organization time and money. That is why it is vital to ensure that data is free of malware and IOCs (indicators of compromise) before recovery.

With Malicious File Scan, you can scan the data for viruses and malware during a data restore activity. Moreover, you can enable this feature for end users too so that they too can scan the data before restoring. APEX Backup Services scans the entire data for potential viruses and blocks the malicious and only restores the clean files.

APEX Backup Services uses an industry-leading antivirus engine to search the data for potential viruses and malware. You can also add pre-identified hash values of malicious files to the scan engine. APEX Backup Services will also scan the data for these file hashes so that malicious files can be blocked from restore.

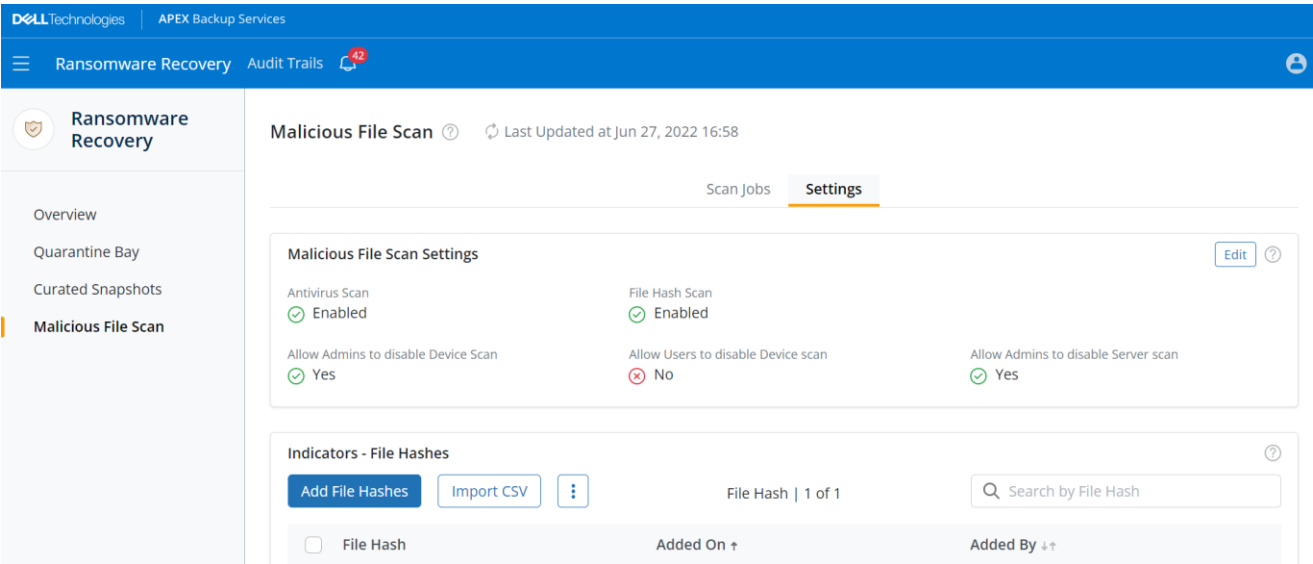


Figure 13. Ransomware recovery – Malicious File Scan

Federated search also allows you to look for compromised data across your entire backup environment. Once infected data has been identified, admins can delete infected snapshots or files, and wipe-clean infected devices, preventing accidental recovery of contaminated data.

## APEX Backup Services – ransomware recovery dashboard

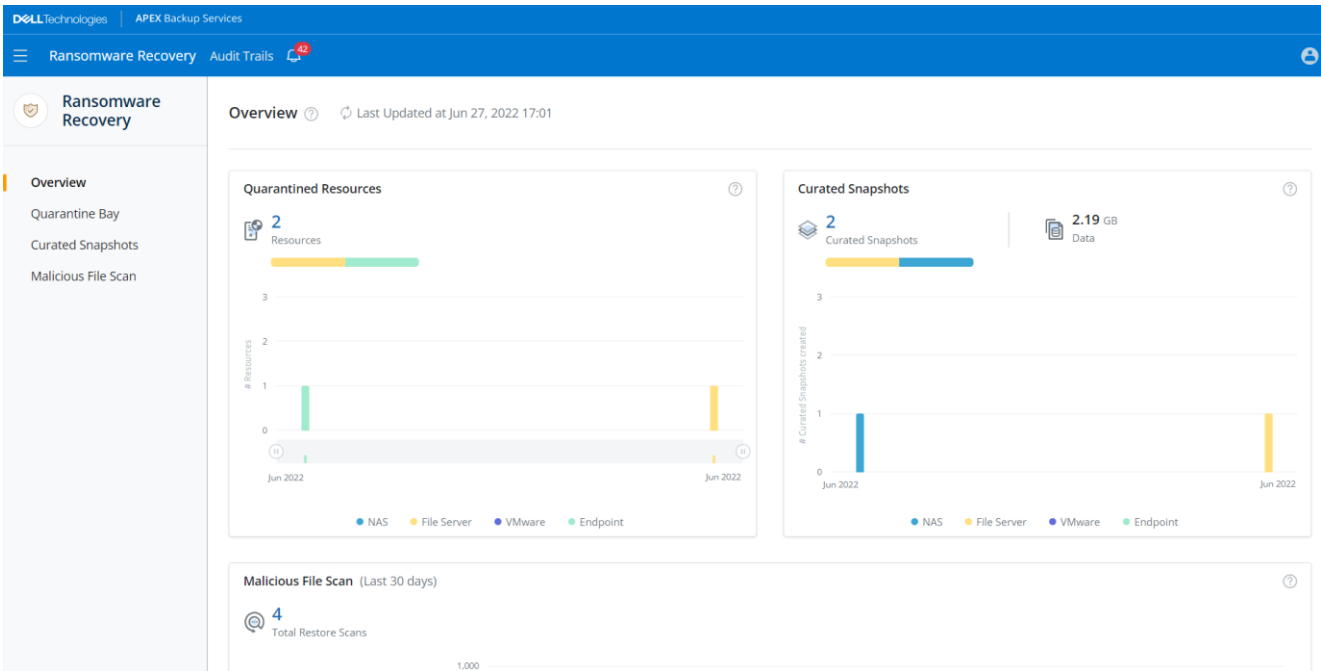
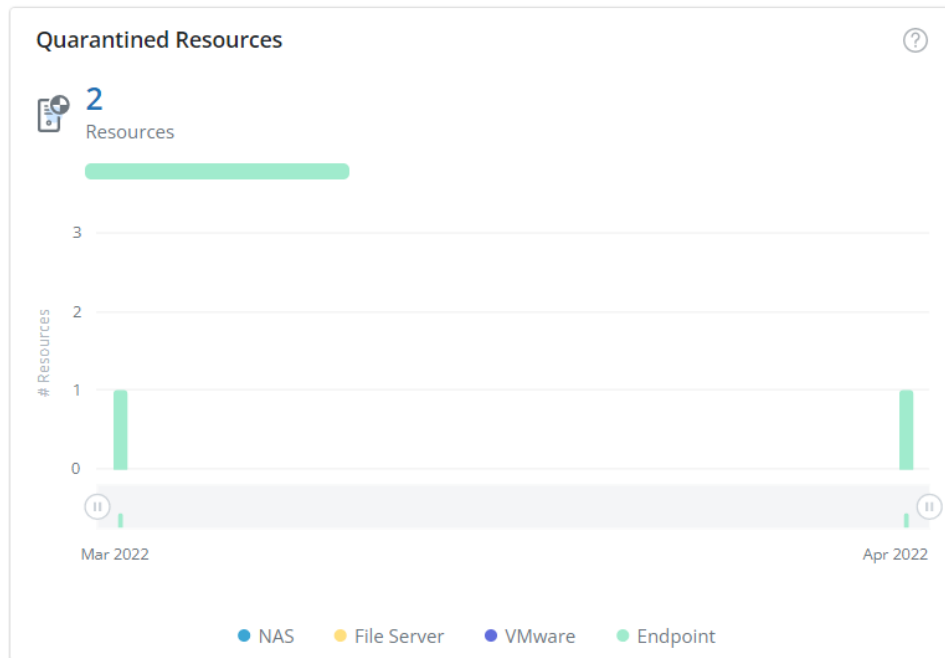


Figure 14. Ransomware recovery dashboard overview



### Quarantined Resources:

Shows the total number of active quarantined resources. The resources can be Endpoints, File Servers, VMware, or NAS devices. You can view the individual count details of active and latest quarantined resources for each resource-Endpoints, File Servers, VMware, or NAS devices using the graphical representation.



**Figure 15. Ransomware recovery dashboard - Quarantined Resources**

### Curated Snapshots:

Shows the total number of active curated snapshots created for your resources. Resources can be endpoints, file servers, or NAS devices. You can view the individual count details of active and latest Curated Snapshots for each resource-endpoints, file servers, or NAS devices using the graphical representation.

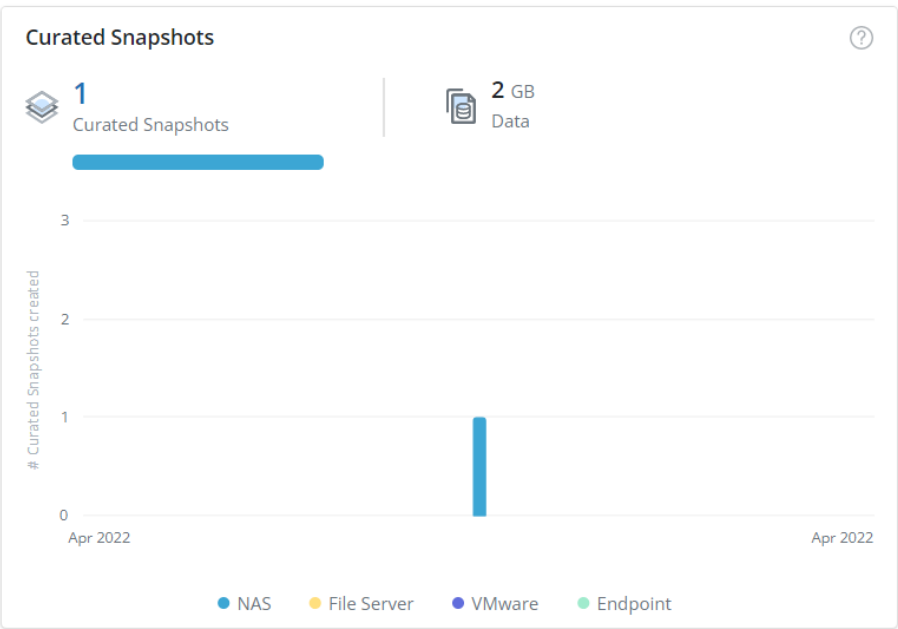


Figure 16. Ransomware recovery dashboard - Curated Snapshots

Malicious File Scan

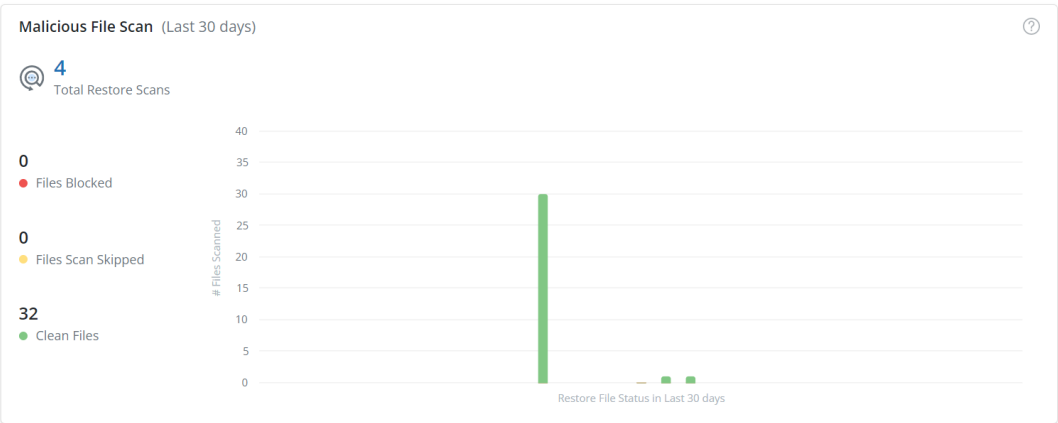


Figure 17. Ransomware recovery dashboard - Malicious File Scan

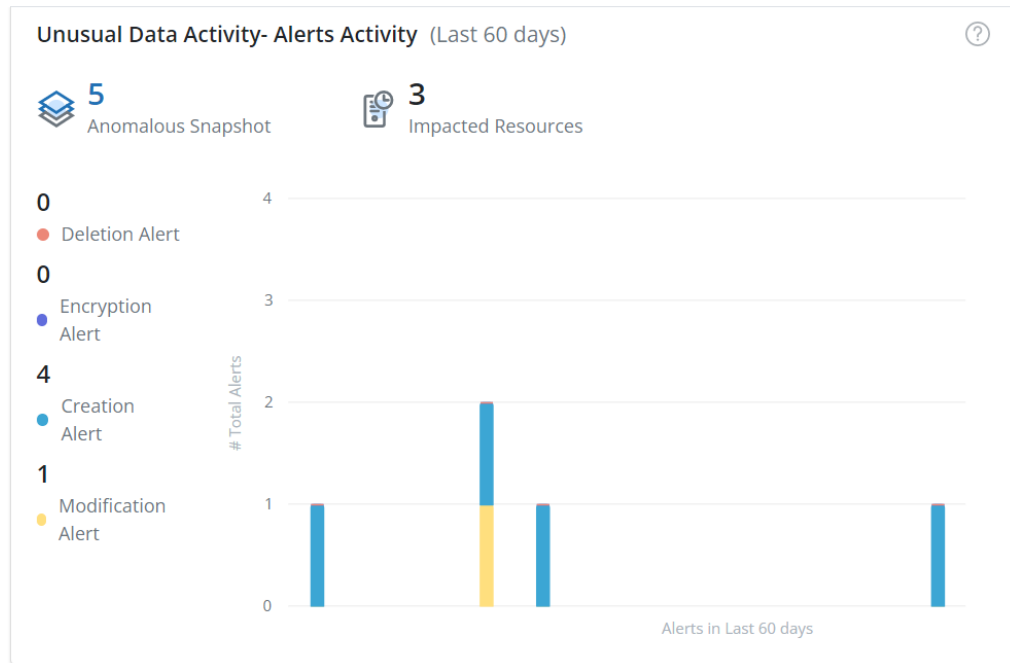
**Total Malicious File Scan** - Total number of malicious file scan jobs run for your resources in the past 30 days. Resources can be endpoints, file servers, or NAS devices.

**Files Blocked** - Total number of malicious files that were blocked out of the total number of files selected for restore for your resources in the past 30 days.

**File Scan Skipped** - Total number of files that were skipped from the scan out of the total number of files selected for restore for your resources in the past 30 days.

**Clean Files** - Total number of files that were found safe out of the total number of files selected for restore for your resources in the past 30 days.

## Unusual Data Activity-Alerts Activity



**Figure 18. Ransomware recovery dashboard - Unusual Data Activity-Alerts Activity**

**Anomalous Snapshot** - Total number of anomalous snapshots for which Unusual Data Activity alerts were generated for your resources.

**Impacted Resources** - Total number of impacted resources on which unusual data activity was identified.

**Deletion Alert** - Total number of alerts generated for deletion of files from the snapshot.

**Encryption Alert** - Total number of alerts generated for encryption of files.

**Creation Alert** - Total number of alerts generated for the creation of too many files.

**Modification Alert** - Total number of alerts generated for the modification or edits of too many files.

Unusual Data Activity-Service Status

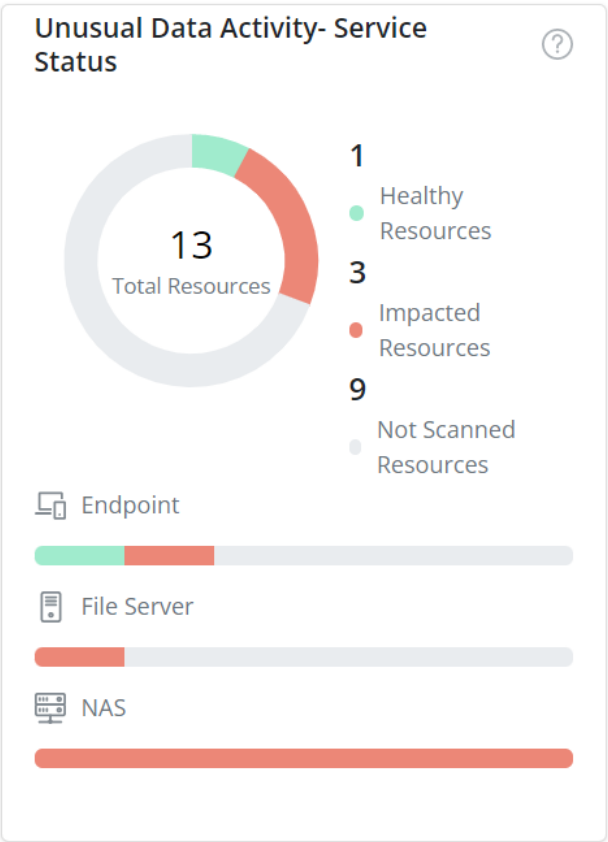


Figure 19. Ransomware recovery dashboard - Unusual Data Activity-Service Status

**Total Resources** - Total number of resources present.

**Healthy Resources** - Total number of resources that were found safe out of the total number of resources for which Unusual Data Activity alerts were generated.

**Impacted Resources** - Total number of resources that were found infected out of the total number of resources for which Unusual Data Activity alerts were generated.

**Not Scanned Resources** - Total number of resources that were not scanned for Unusual Data Activity.

Conclusion

Ransomware attacks are more prevalent today than ever before. You need a sound data protection strategy that addresses business resiliency and continuity concerns. While ransomware attacks may be inevitable, APEX Backup Services can ensure that your backup data is safe, help you operationalize security across your backup and primary environments, and accelerate the recovery process, so you can get back to normal faster.

# References

## Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document:

- [APEX Backup Services: Data protection for the multi-cloud era](#)
- [Solution Overview: Accelerated ransomware recovery with APEX Backup Services](#)
- [White Paper: Five steps to ransomware protection and recovery with APEX Backup Services](#)
- [APEX Backup Services Security Overview](#)
- [APEX: The ransomware survival guide](#)