Introduction to Dell APEX Backup Services

Data Protection for the Multi-Cloud Era

June 2022

H19143

White Paper

Abstract

This white paper focuses on Dell APEX Backup Services that provide cloud-based data protection for SaaS apps, endpoints, and hybrid workloads.

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.

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

Introduction to APEX Backup Services 5

APEX Backup Services for endpoints 6

APEX Backup Services for SaaS apps 8

APEX Backup Services for hybrid workloads 12

APEX Backup Services cloud platform 13

APEX Backup Service dashboard components: 15

References 28

Executive summary

Challenges

Traditional data protection and backup solutions are no longer meeting the needs of customers. These traditional solutions present many challenges such as building on-premises infrastructure, manual installation and configuration, racking and stacking, managing power and cooling, and planning to prevent physical outages.

Customers choosing cloud deployments for new applications are struggling to find an adequate backup and data protection solution for their SaaS apps, endpoints, and hybrid workloads. Customers need data protection that is cloud-based and can offer the scalability, security, and flexibility they need to meet their business needs.

Solution

With Dell APEX, everything is managed for you **as-a-service** (aaS) with the Dell Technologies innovation you know and trust. Dell APEX Backup Services delivers end-to-end secure protection with backup, disaster recovery, and long-term retention. APEX Backup Services is 100% cloud-based, so there is no infrastructure to manage or administrative tasks to burden your team. It deploys in minutes and provides unlimited, on-demand scaling to ensure growing data volumes are always protected.

Revisions

Date	Description
June 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

Introduction to APEX Backup Services

APEX Backup Services

APEX Backup Services is a cloud-based data protection solution that ensures predictable, controllable costs without increasing complexity. APEX Backup Services delivers all-in-one secure protection with backup, disaster recovery, and long-term retention. The intuitive console provides centralized visibility and management.

APEX Backup Services offers:

- Unified data protection and governance for SaaS apps
- Secure protection of endpoint devices
- Long-term retention for hybrid workloads and automated Disaster Recovery (VMware workloads only)

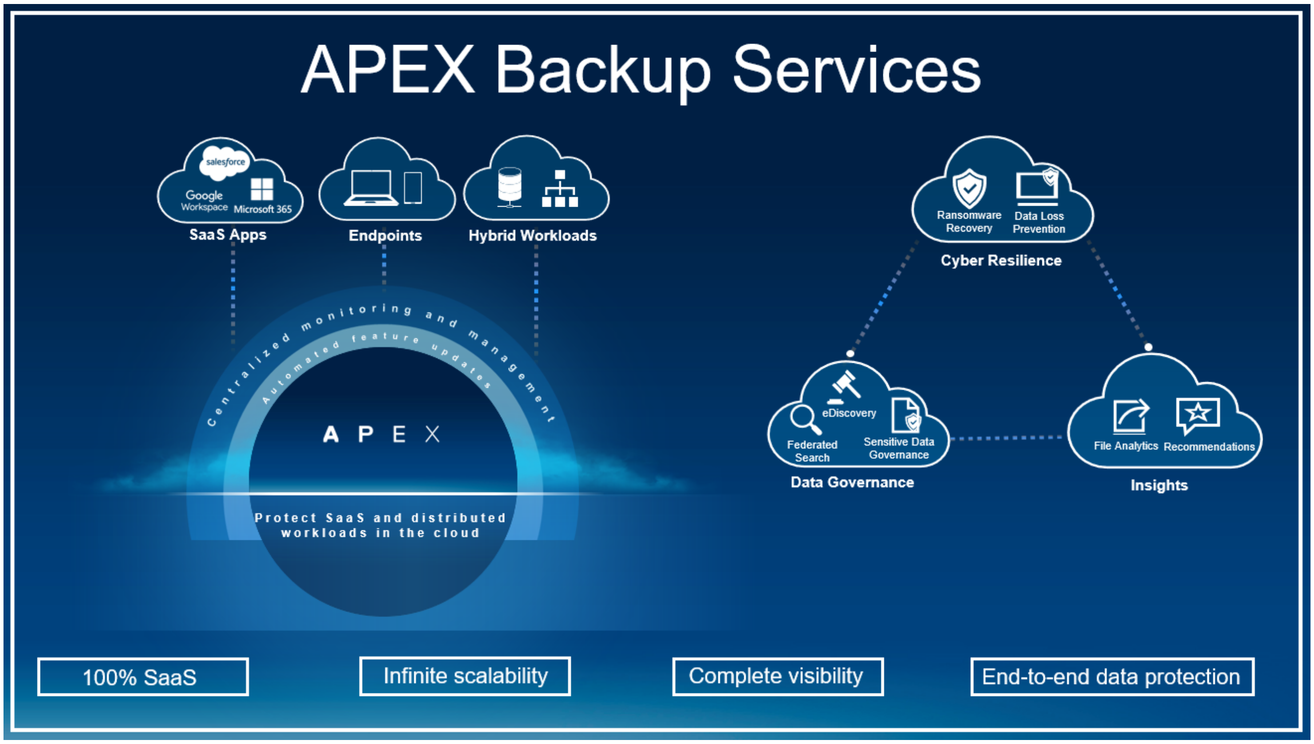


Figure 1. APEX Backup Services

APEX Backup Services uses cloud infrastructure to deliver the resiliency and speed you need to meet business service level agreements (SLAs) with a low total cost of ownership (TCO). Dell Technologies maintains the solution, and the platform is always up to date with the latest features:

- Centralized monitoring and management
- Automated, no-touch feature updates
- Regulatory compliance
- Source-side deduplication

- Encryption, in-flight and at rest
- Cloud-to-cloud backup and restore

APEX Backup Services supports the most stringent and comprehensive privacy and security standards for your backup data. This outcome is possible using a combination of standards supported with the AWS underlying platform and standards that we support directly within the APEX Backup Services cloud platform. To ensure the security and privacy of your data, APEX Backup Services uses an enterprise-grade, digital-envelope-encryption model to encrypt data in-transit (256-bit TLS) and at rest (AES 256-bit).

APEX Backup Services for endpoints

Overview

APEX Backup Services for endpoints provides comprehensive, scalable, and cost-effective cloud-based data protection for desktops, laptops, and mobile devices.

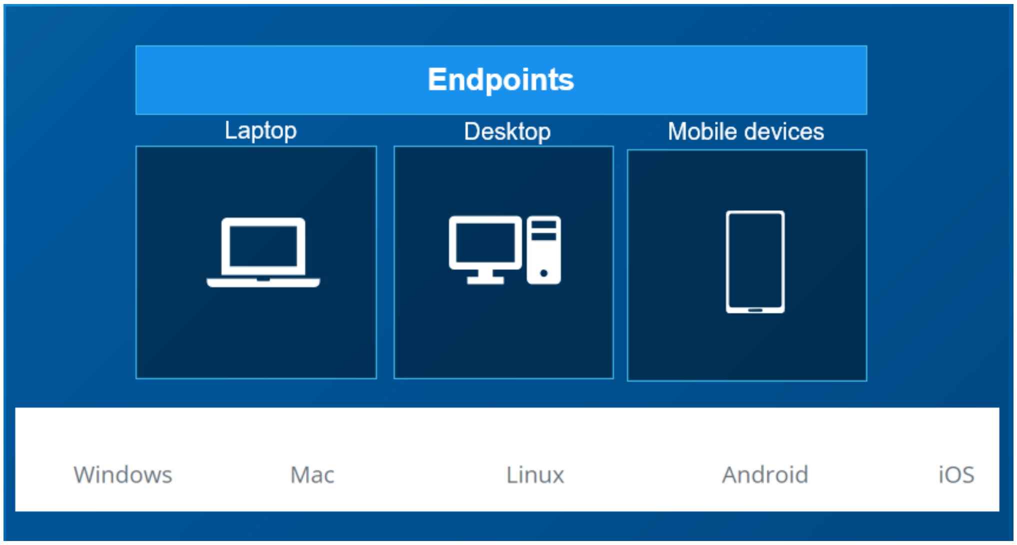


Figure 2. APEX Backup Services for endpoint devices

APEX Backup Services for endpoints protects desktops, laptops, and mobile devices and supports several use cases, including:

- Device and data loss, which is addressed through backup and restore
- Data security, including data loss prevention (DLP) to prevent leaks if there is device loss or theft, and ransomware protection
- Data governance, consisting of eDiscovery and data compliance
- Device life-cycle management including acceleration and streamlining of key IT processes like operating system migration and device refresh

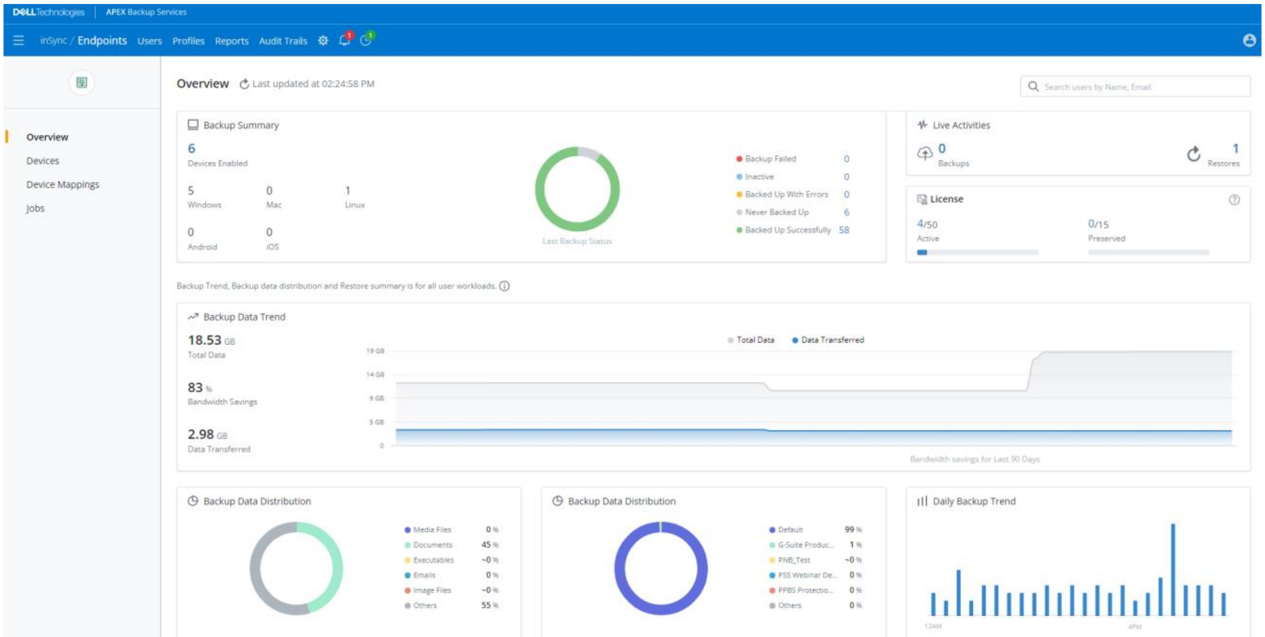
APEX Backup Services for endpoints helps simplify the recovery of data that was residing on a lost or stolen device. It ensures that data is never totally lost with a reliable backup that allows you to quickly recover from all types of data loss. IT administrators can remotely manage cloud backup and restore operations from the centralized cloud portal. Self-service restores are possible using a web interface and from mobile device apps, including iOS and Android. Desktop and laptop support includes Windows, Linux, and macOS.

APEX Backup Services for endpoints provides flexible and granular restore options so that data can be quickly recovered in any loss scenario:

- Loss, theft, or corruption of a device
- An accidental deletion of a file
- Malicious tampering
- Data corruption

Restoration is possible at the file level or through a bulk restore, such as recovery from a ransomware attack.

APEX Backup Services provides a secure, reliable, and fast endpoint-backup solution, so you can always recover end-user data. Integrated backup, eDiscovery, and compliance monitoring simplify endpoint data protection, ensure regulatory compliance, and improve data visibility for the mobile workforce.



Backup Trend, Backup data distribution and Restore summary is for all user workloads.

Figure 3. Endpoints dashboard

APEX Backup Services for SaaS apps

Overview

APEX Backup Services for SaaS apps delivers unified data protection, management, and information governance, including automated compliance and legal hold capabilities. A single dashboard provides complete visibility across Microsoft 365, Google Workspace, and Salesforce.

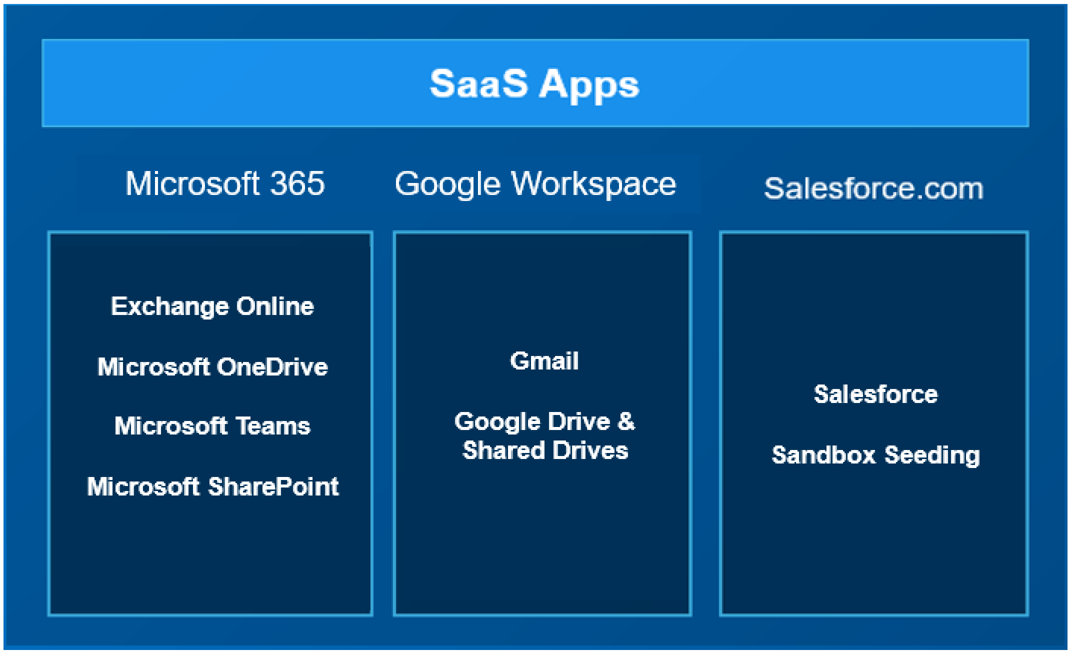
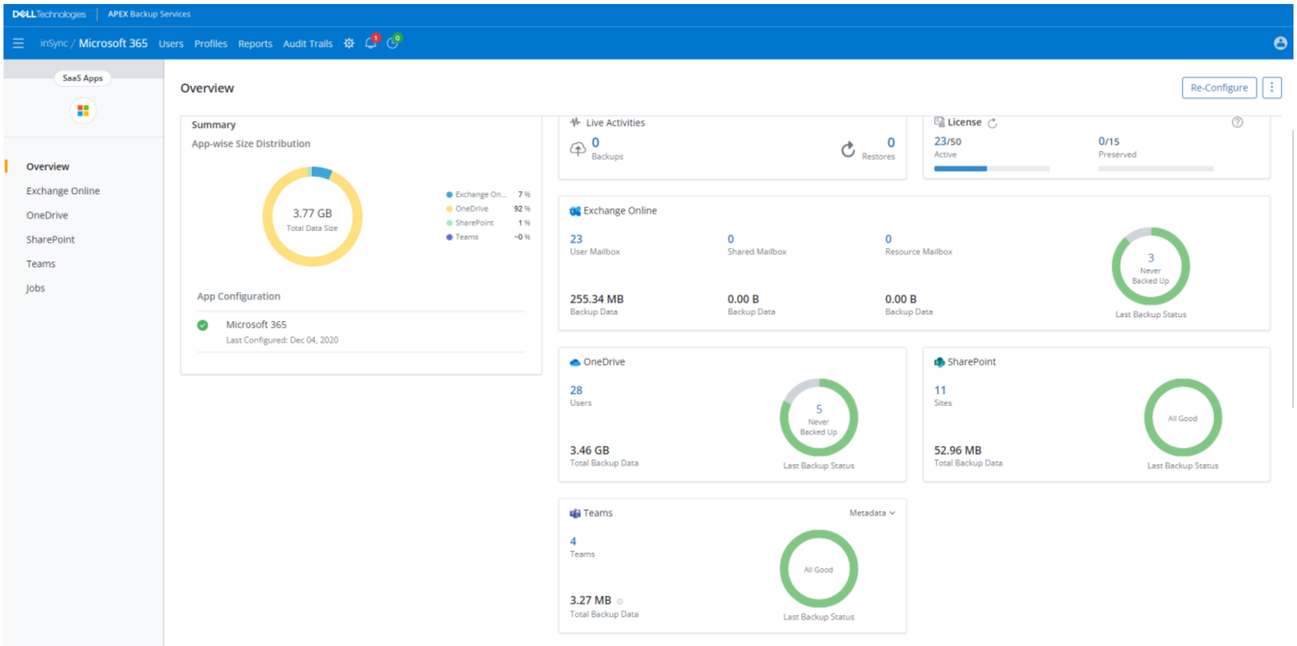


Figure 4. APEX Backup Services for SaaS apps

Data protection for Microsoft 365

APEX Backup Services for SaaS apps provides a scalable and cost-effective cloud-based platform to protect Microsoft 365 data, including Exchange Online, OneDrive for Business, SharePoint, and Teams. It is a single solution for backup, long-term retention, federated search, compliance, and eDiscovery.



Overview

Summary

App-wise Size Distribution

3.77 GB Total Data Size

Exchange On...	7 %
OneDrive	92 %
SharePoint	1 %
Teams	~0 %

App Configuration

Microsoft 365
Last Configured: Dec 04, 2020

Live Activities
0 Backups
0 Restores

License
23/50 Active
0/15 Preserved

Exchange Online
23 User Mailbox
0 Shared Mailbox
0 Resource Mailbox
255.34 MB Backup Data
0.00 B Backup Data
0.00 B Backup Data
3 Never Backed Up
Last Backup Status

OneDrive
28 Users
3.46 GB Total Backup Data
5 Never Backed Up
Last Backup Status

SharePoint
11 Sites
52.96 MB Total Backup Data
All Good
Last Backup Status

Teams
Metadata
4 Teams
3.27 MB Total Backup Data
All Good
Last Backup Status

Figure 5. Microsoft 365 dashboard

Key features

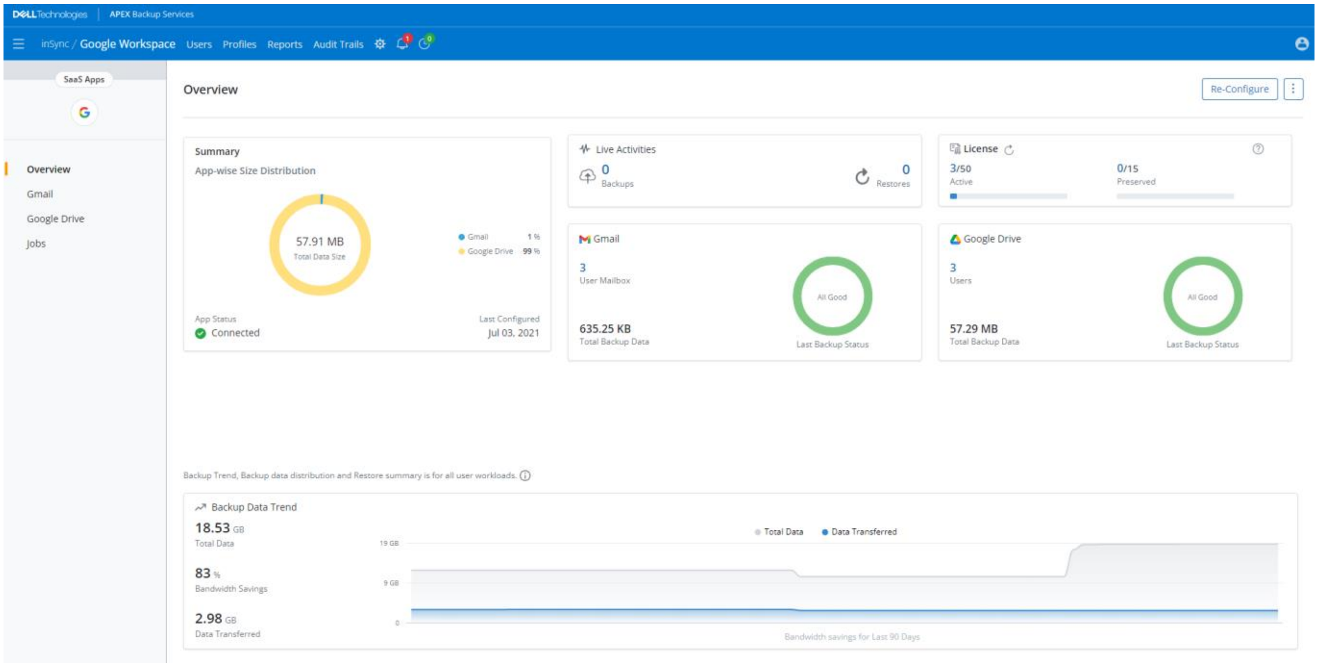
- **Agentless data protection:** Microsoft 365 data is backed up directly from Microsoft Azure to the APEX Backup Services platform on AWS and does not require agents.
- **Complete visibility:** A single dashboard gives you complete visibility across Microsoft applications, providing the insight you need to ensure your data is protected and compliant.
- **Preservation of end-user data:** Data can be retained for inactive and terminated employees, eliminating the need to purchase and maintain additional Microsoft 365 licenses.
- **Self-service restores:** Users are empowered to restore Exchange Online and OneDrive data without IT admin intervention.
- **Federated search:** Search across Microsoft 365 users and endpoints to quickly locate sensitive files or confidential data that should be restricted or requires defensible deletion.
- **Point-in-time recovery:** Recover email messages, OneDrive, and SharePoint files to their original location from any time-based snapshot using a simple intuitive interface.
- **Compliance:** Proactively monitor for potential regulatory violations such as GDPR, HIPPA, and CCPA. Predefined, customizable templates and alerting enable quick remediation of violations.

For more details, see the solution brief [APEX Backup Services for Microsoft 365.](#)

Data protection for Google Workspace

APEX Backup Services protects and governs business-critical data for Google Workspace, including Gmail, Google Drive, and shared drives. The solution provides a consistent backup and recovery experience across these Google Workspace applications including:

- Central IT visibility and control with a single dashboard
- Ability for IT to configure and automate backup policies including retention, backup frequency, and user profiles



Backup Trend, Backup data distribution and Restore summary is for all user workloads.

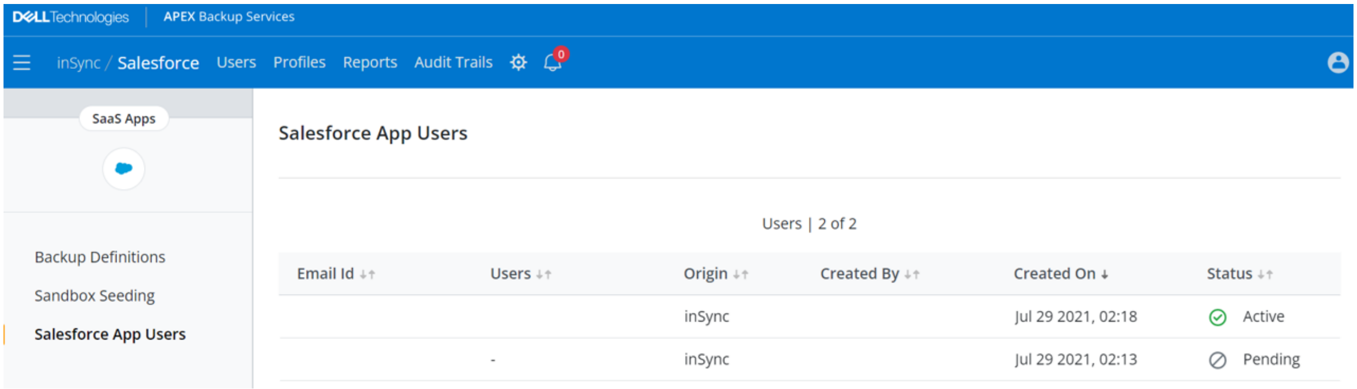
Figure 6. Google Workspace dashboard

There are granular and flexible recovery options for all loss scenarios that can be performed by administrators or through self-service options for the end user. APEX Backup Services also helps you realize more value from your Google Workspace data by helping you to accelerate eDiscovery, monitoring, and remediation compliance.

For more details, see the document [APEX Backup Services for Google Workspace](#).

Data protection for Salesforce

APEX Backup Services also protects business-critical data residing in Salesforce (SFDC) with comprehensive backup that includes, objects, records, metadata, attachments, reports, dashboards, and workflows.



Salesforce App Users

Users | 2 of 2

Email Id	Users	Origin	Created By	Created On	Status
		inSync		Jul 29 2021, 02:18	✓ Active
	-	inSync		Jul 29 2021, 02:13	⊘ Pending

Figure 7. Salesforce dashboard

If there is data loss, you can avoid downtime by accelerating your data restore with:

- Flexible and granular recovery
- Robust recovery which saves re-implementation costs after the data loss

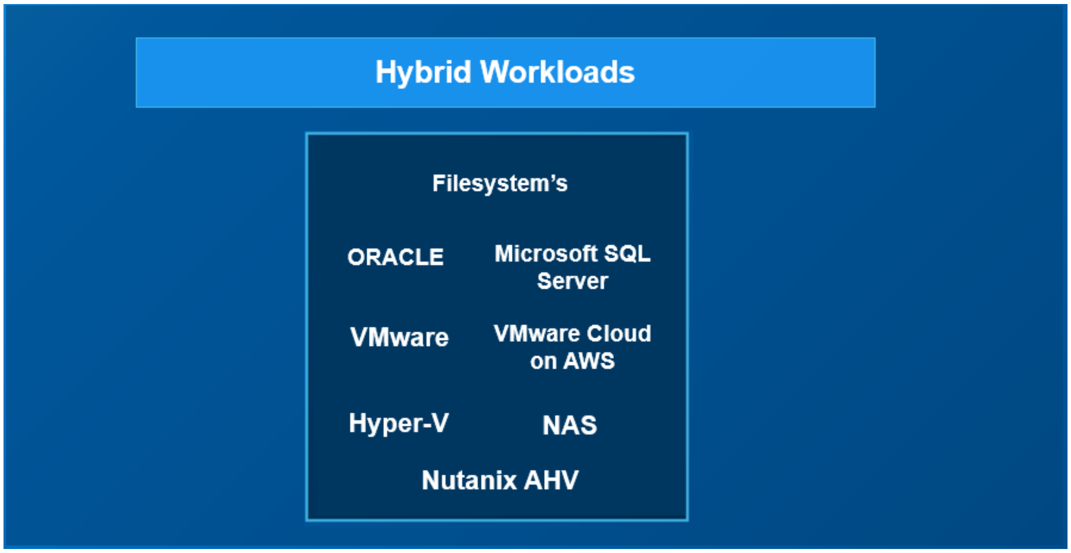
APEX Backup Services for sandbox seeding

Achieve quality test data for your Salesforce sandboxes. For more details about Salesforce sandbox seeding, see the data sheet APEX Backup Services: Salesforce sandbox seeding.

APEX Backup Services for hybrid workloads

Overview

APEX Backup Services for hybrid workloads combines high performance, scalable backup, disaster recovery, and long-term retention to simplify data protection, reduce costs, and improve data visibility for today's complex information environments. Organizations can achieve their most aggressive business SLAs and reduce TCO.


Hybrid Workloads

Filesystem's

ORACLE

Microsoft SQL Server

VMware

VMware Cloud on AWS

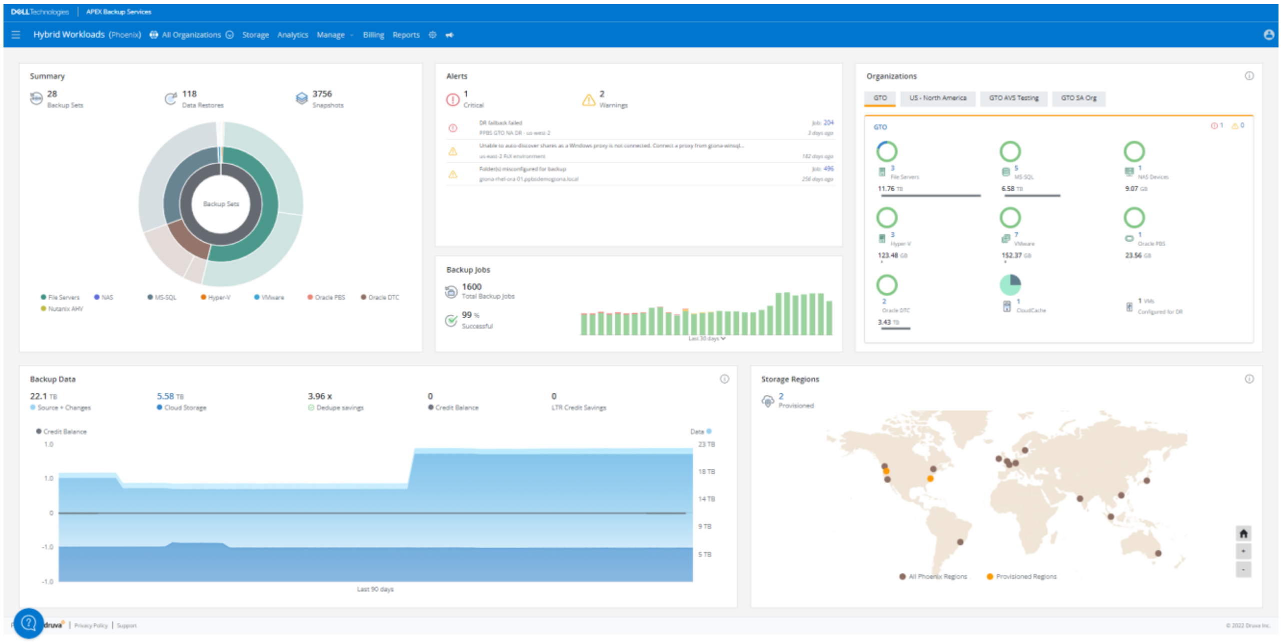
Hyper-V

NAS

Nutanix AHV

Figure 8. APEX Backup Services for hybrid workloads

By using the elasticity and scale-out capabilities provided by the cloud, APEX Backup Services for hybrid workloads enables organizations to centralize the data protection of enterprise workloads including physical file servers, databases, network-attached storage (NAS), and virtual and hybrid environments.



DR failback failed
PPBS GTO NA DR - us-west-2
Job: 204
3 days ago

Unable to auto-discover shares as a Windows proxy is not connected. Connect a proxy from gtona-winsql...
us-east-2 FSX environment
182 days ago

Folder(s) misconfigured for backup
gtona-rhel-ora-01.ppbsdemogtona.local
Job: 496
256 days ago

Figure 9. Hybrid workloads dashboard

From a single console, IT has the flexibility to backup and restore data, failover virtual machines (VMs) for disaster recovery, apply long-term retention to data in the cloud for compliance, and replicate VM workloads across regions and accounts for test-dev purposes.

APEX Backup Services for hybrid workloads delivers against stringent recovery point objectives (RPOs) and recovery time objectives (RTOs) requirements of critical applications while eliminating the complexity and costs associated with on-premises infrastructure. For demanding RPOs and RTOs in the data center, Cloud Cache can be installed on commodity hardware and achieve fast VM restore.

The APEX Backup Services approach to store enterprise data uses both an advanced data-scrambling algorithm and a unique envelope-based encryption model where the data and metadata are decoupled and encrypted. This approach ensures that your data is only accessible by you. This component a critical to help you meet today's stringent global data-privacy regulations. Finally, to enable restoring from ransomware attacks, APEX Backup Services for hybrid workloads provide data isolation and high performance restores to minimize downtime from a breach.

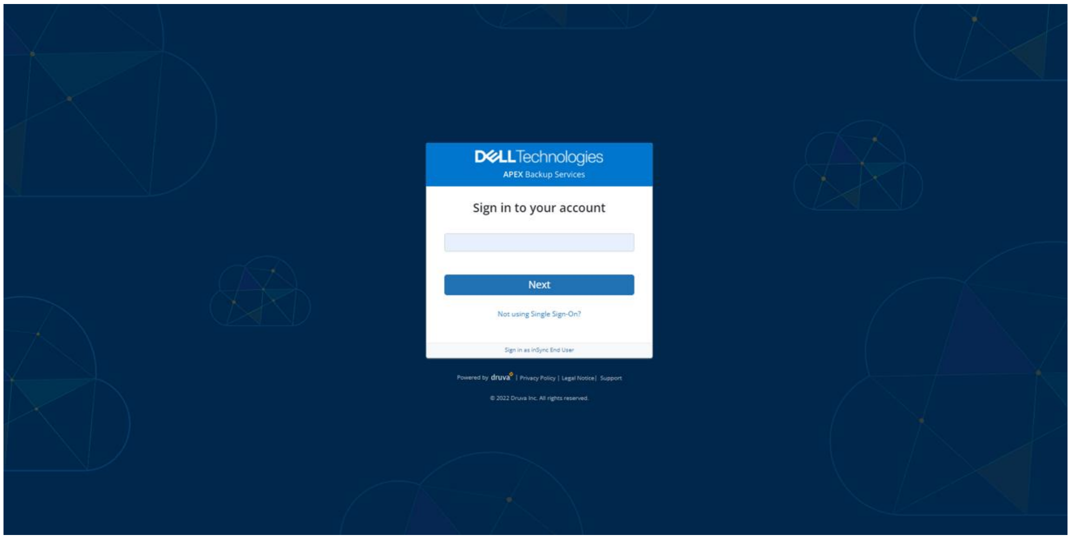
APEX Backup Services cloud platform

APEX Backup Services console

You can perform the following steps to log in to the APEX Backup Service Cloud Platform Console.

1. Open a web browser, enter **https://dell-login.druva.com/** in the address bar, and press Enter.

2. In the email box, enter the **email ID,** and click **Next**.



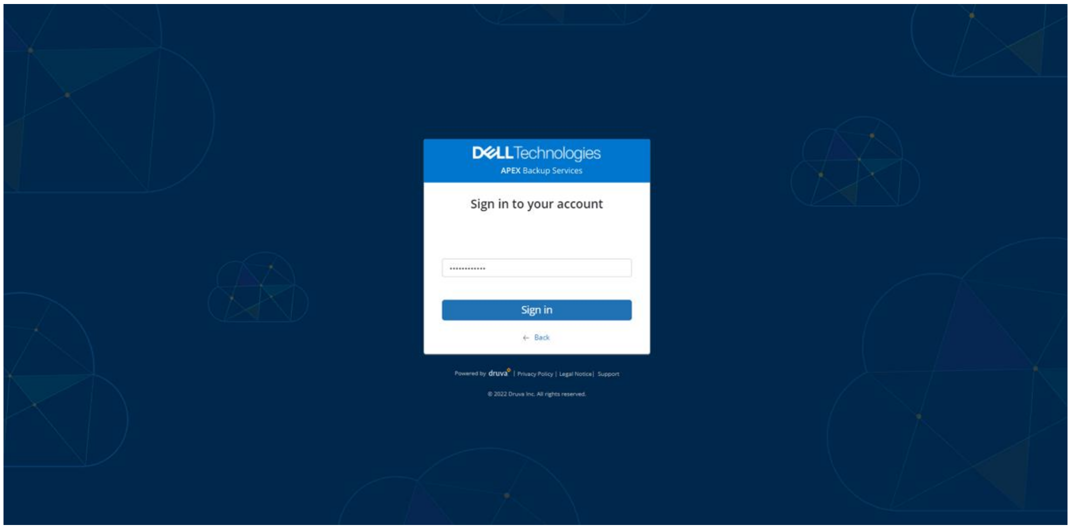
Sign in to your account

© 2022 Druva Inc. All rights reserved.

DELL Technologies
APEX Backup Services
Next
Not using Single Sign-On?
Sign in as inSync End User
Powered by druva | Privacy Policy | Legal Notice| Support

Figure 10. APEX Backup Services console login > registered email address

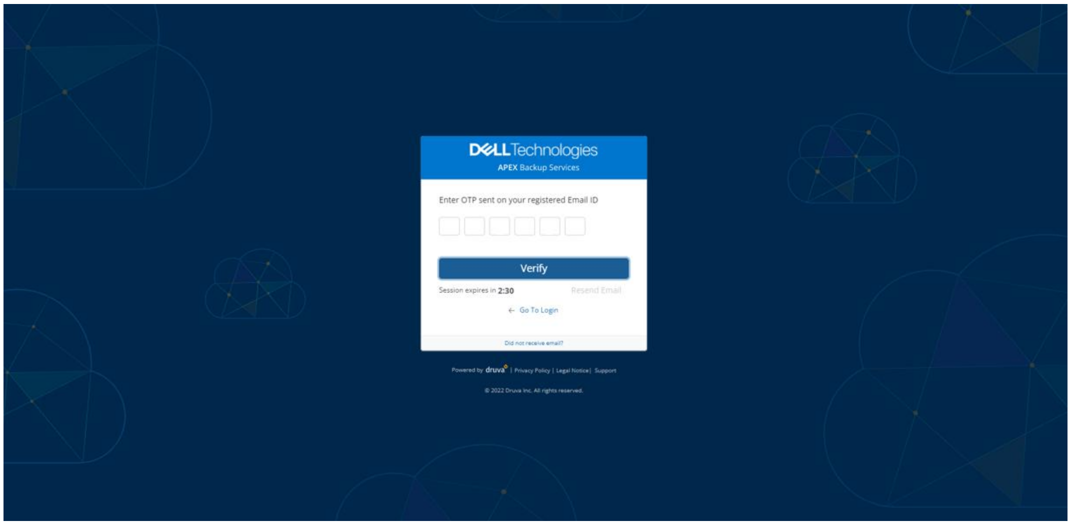
3. Enter the password in the **Password** field, and click **Sign In.**


Sign in to your account

© 2022 Druva Inc. All rights reserved.

Figure 11. APEX Backup Services console login > password

4. Enter the verification one-time password (OTP) that is sent to registered email address and click **Verify**.


Enter OTP sent on your registered Email ID

Session expires in 2:30

© 2022 Druva Inc. All rights reserved.

Figure 12. APEX Backup Services console login > OTP

A centralized dashboard provides insight into the status of backup jobs and the cloud infrastructure performing these backups, including cloud regions in use and the capacity of your cloud storage.

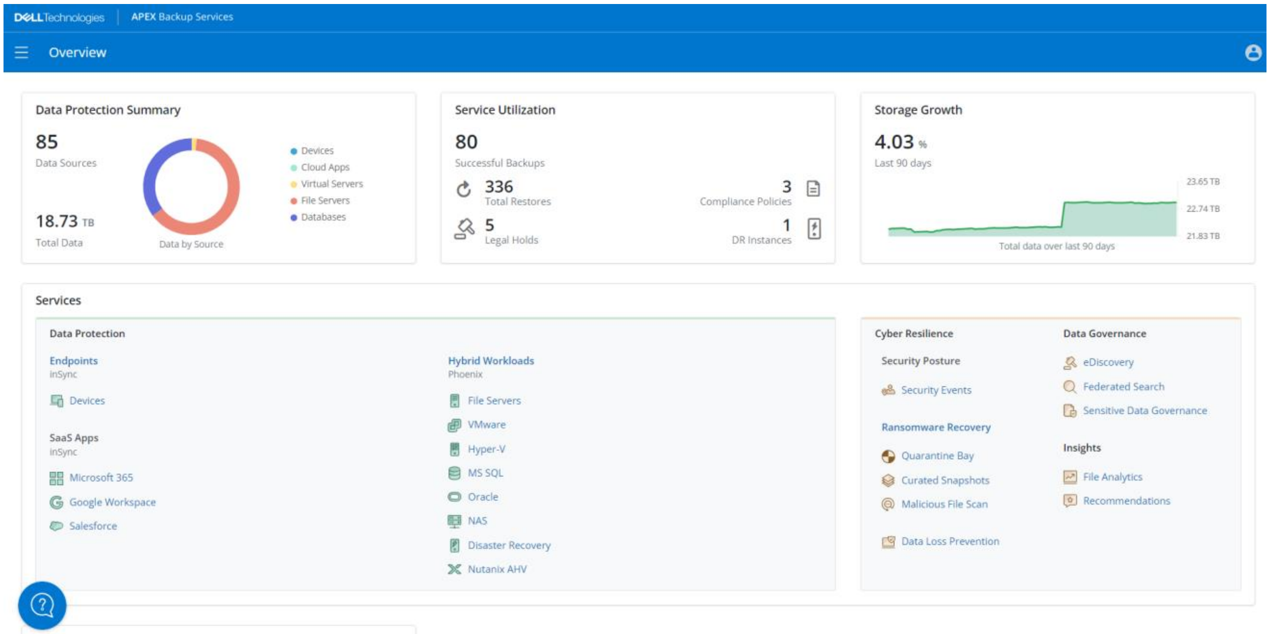


Figure 13. APEX Backup Services cloud platform console

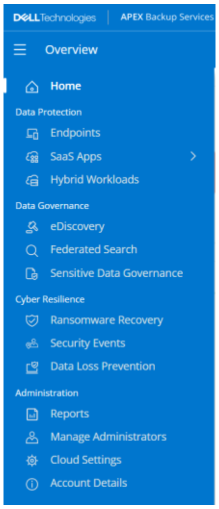
This single console is where you can launch all the features of APEX Backup Services. Whether you are protecting SaaS applications, endpoints, or hybrid workloads (or a combination of the three) you have the visibility and control you need to manage your data protection.

APEX Backup Service dashboard components:

Global navigation panel

On the top-left corner of the page, you can access the **Global Navigation Panel** by clicking the menu icon (three bars).

The Global Navigation Panel provides navigation to the APEX Backup Services products, services, administration, and settings section.



Data Protection Summary

The following describes the information in the Data Protection Summary section:

- **Data Sources:** Shows the total number of sources in your account that APEX Backup services is backing up. Sources can be endpoints such as laptops, or remote servers such as virtual machines.
- **Total Data:** Shows the total amount of data that APEX Backup services has backed up across all the data sources.
- **Data by Source:** Provides a comparative estimate of storage that the data sources consume.

Note: The storage consumed by file servers is equal to the total storage consumed by registered Windows servers, Linux servers, and NAS shares.

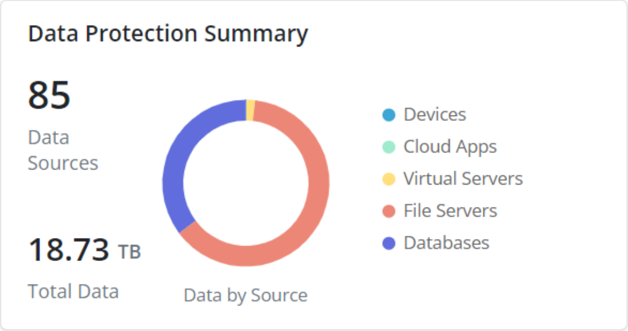


Figure 14. Data Protection Summary

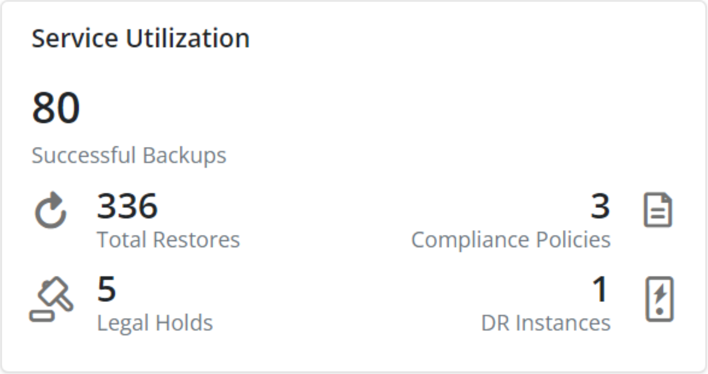
Service Utilization

The following describes the information in the Service Utilization section:

- **Successful Backups**: Shows the total number of successful backups using APEX Backup Services.

  The total number of successful backups is counted as the sum of:

  - Total number of successful backups across all the devices, SaaS apps, and SharePoint sites
  - Total number of successful backups for all the workloads across the organizations
- **Total Restores:** Shows the total number of all successful restore jobs to date.
- **Legal Holds:** Shows the total number of legal holds applied to the snapshots
- **Compliance Policies:** Shows the total number of compliance policies created
- **DR Instances:** Shows the total number of virtual machines replicated in your AWS account.



Service Utilization

80
Successful Backups

336
Total Restores

3
Compliance Policies

5
Legal Holds

1
DR Instances

Figure 15. Service Utilization

Storage Growth

The storage growth section shows how the storage consumption for your account has changed over the last 90 days. When you hover over a particular place in the chart, you can see the storage consumed on a day.

For a new account, the storage growth is zero percent. After the first backup job is complete, the chart shows the growth in comparison to zero bytes consumed on the day of the account creation. The chart is updated over a period of 90 days based on the data backs up from different data sources according to different schedules.

The storage growth chart on the APEX Backup Services cloud platform console displays the total deduplicated data backed up over the last 90 days. It shows the combination of source and changed data backed up in hybrid workloads.

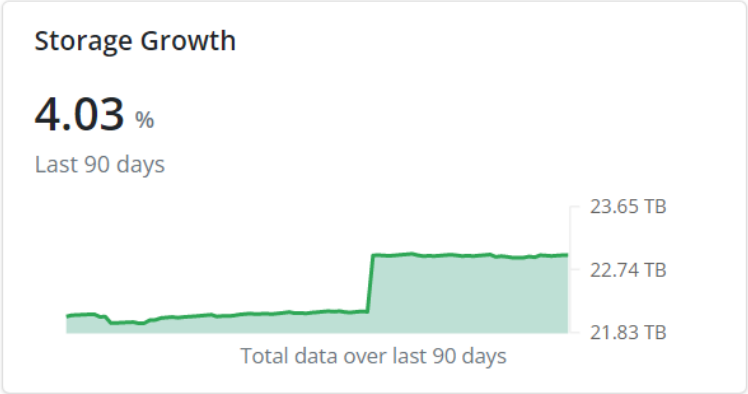
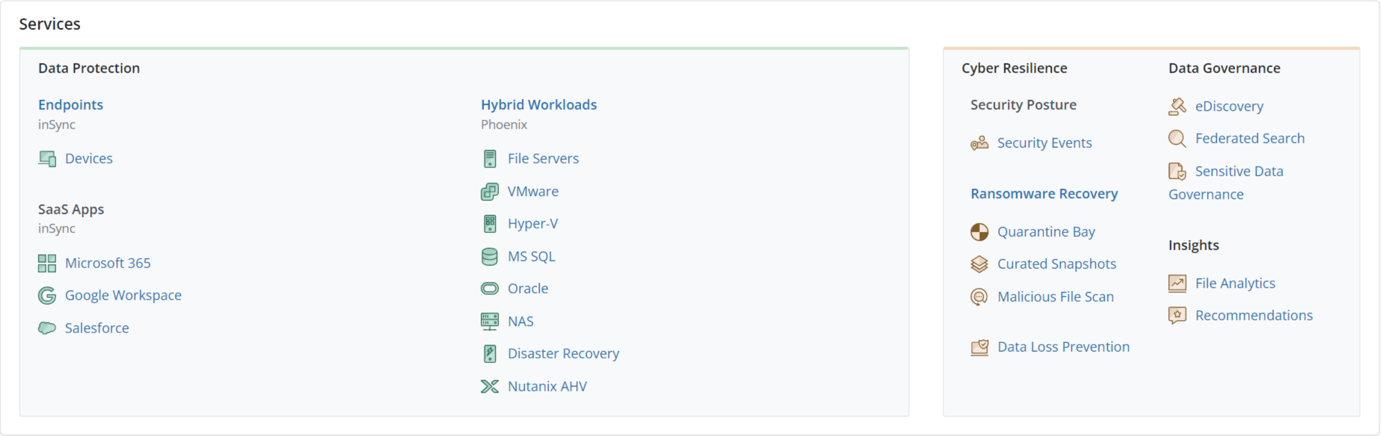


Figure 16. Storage Growth

Overview of services and features

The following figure shows the services and features with APEX Backup Services.



Services

Data Protection

Endpoints
inSync

Devices

SaaS Apps
inSync

Microsoft 365
Google Workspace
Salesforce

Hybrid Workloads
Phoenix

File Servers
VMware
Hyper-V
MS SQL
Oracle
NAS
Disaster Recovery
Nutanix AHV

Cyber Resilience

Security Posture

Security Events

Ransomware Recovery

Quarantine Bay
Curated Snapshots
Malicious File Scan

Data Loss Prevention

Data Governance

eDiscovery
Federated Search
Sensitive Data Governance

Insights

File Analytics
Recommendations

Figure 17. Overview section lists services and features

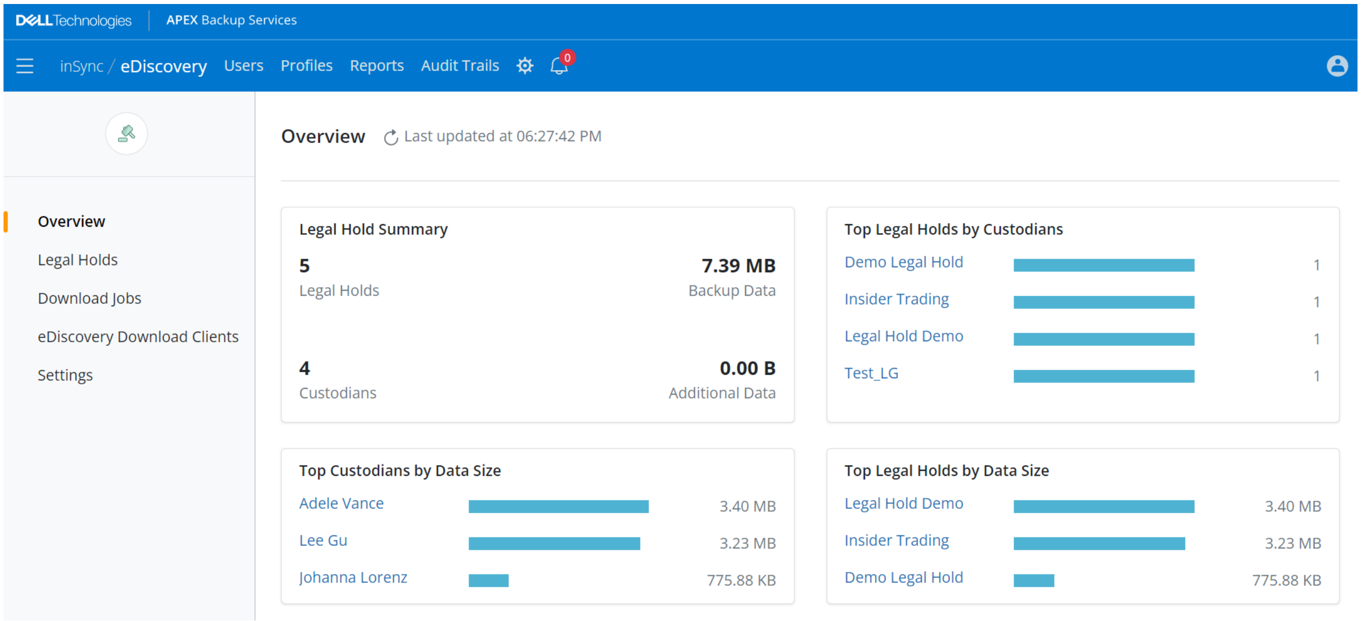
APEX Backup Services are categorized as:

- Data Protection
  - Endpoints
  - SaaS Apps
  - Hybrid Workloads
- Data Governance
  - eDiscovery
  - Federated Search
  - Sensitive Data Governance
- Cyber Resilience
  - Security Posture
  - Ransomware Recovery
- Insights
  - File Analytics
  - Recommendations

Data Governance

Legal Hold (eDiscovery)

With Legal Hold, you can preserve user backup data and avoid data deletion. When you keep a user on Legal Hold, the backup data for that user is excluded from compaction.



Overview Last updated at 06:27:42 PM

Legal Hold Summary

5 Legal Holds	7.39 MB Backup Data
4 Custodians	0.00 B Additional Data

Top Legal Holds by Custodians

Demo Legal Hold	1
Insider Trading	1
Legal Hold Demo	1
Test_LG	1

Top Custodians by Data Size

Adele Vance	3.40 MB
Lee Gu	3.23 MB
Johanna Lorenz	775.88 KB

Top Legal Holds by Data Size

Legal Hold Demo	3.40 MB
Insider Trading	3.23 MB
Demo Legal Hold	775.88 KB

Figure 18. eDiscovery dashboard

APEX Backup Services does not delete the data that the user backs up from any endpoint device. Administrators can analyze user data by using eDiscovery tools.

When you put a user on Legal Hold, the user data from endpoints such as laptops and mobile, and from cloud applications is preserved.

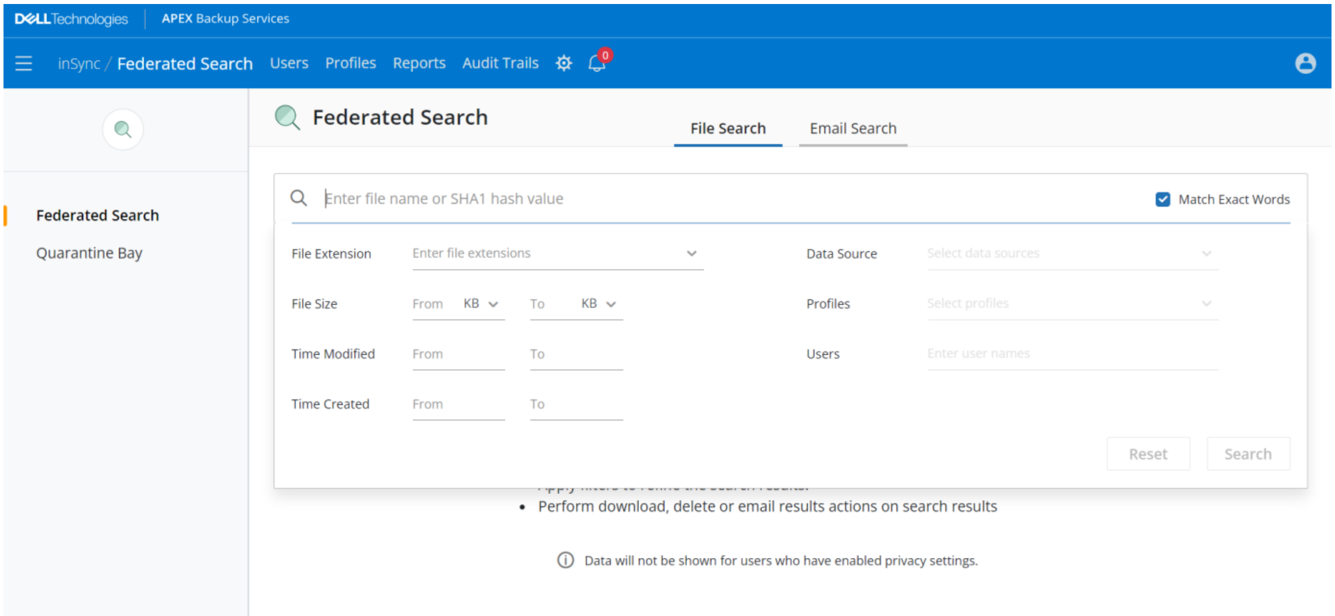
Federated Search for backed up data

APEX Backup Services has a unique capability that allows you to centrally perform a global-federated-metadata search across all users and workloads in the backup, from a single pane of glass. Federated Search extends the keyword-based search with metadata search to enhance investigative capabilities for security, legal, and forensic teams. Federated Search also supports of search of files and email messages using the different parameters available for files and email messages.

Note: Federated Search is only applicable to endpoints and SaaS apps.

Federated search is valuable across multiple use cases including:

- **eDiscovery and forensic investigations**: Locate relevant files to the investigation
- **Security investigations**: Find and delete malicious data in source and backup
- **Compliance**: Find and delete sensitive files in source and backup



☑ Match Exact Words

- Perform download, delete or email results actions on search results

ⓘ Data will not be shown for users who have enabled privacy settings.

Figure 19. Federated Search > File Search

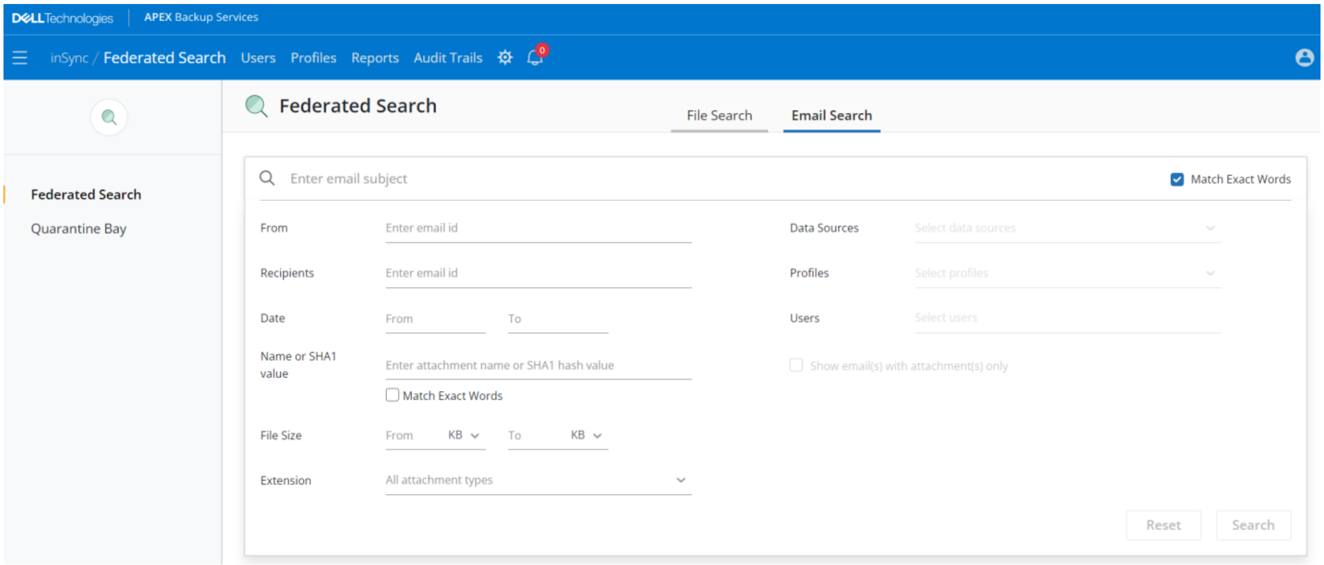
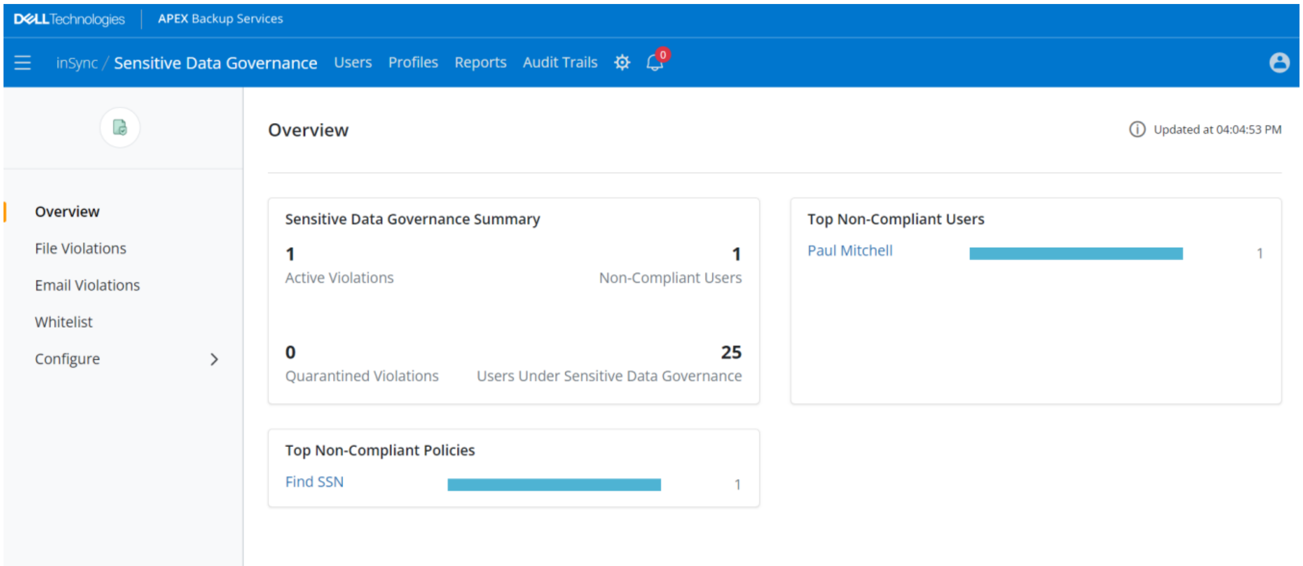


Figure 20. Federated Search > Email Search

Sensitive Data Governance

Sensitive Data Governance provides visibility of compliance breaches associated with end-user data in your organization. Sensitive Data Governance lets you proactively track, monitor, and get notified for data compliance risks in your organization.



Updated at 04:04:53 PM

Sensitive Data Governance Summary

1 Active Violations

1 Non-Compliant Users

0 Quarantined Violations

25 Users Under Sensitive Data Governance

Top Non-Compliant Users

Paul Mitchell	1

Top Non-Compliant Policies

Find SSN	1

Figure 21. Sensitive Data Governance dashboard

The end-user data can be across any of the following data sources:

- Endpoints such as laptops, desktops, iOS, and Android devices
- OneDrive from Microsoft 365 services
- Emails that are backed up from Gmail, MAPI, and Exchange Online
- Google Drive

Sensitive Data Governance reports compliance violations for sensitive data that occurs in the email body, subject, and attachments. APEX Backup Services displays email messages with sensitive data on the Sensitive Data Governance Dashboard and allows administrators to download email messages in the EML file format.

Once enabled, Sensitive Data Governance:

- Enables defining sensitive data and scanning user data for compliance violations or risks of violations
- Allows you to locate end-user data that has violated a compliance policy
- Lets you generate a non-compliance report and view the visual representation to indicate adherence to compliance regulations in your company

Cyber Resilience

Ransomware Recovery

With APEX Backup Services, you have data protection with backup data isolated in a cloud platform and away from the customers' infrastructure, providing immutable protection. Our cloud-native architecture prevents ransomware from encrypting your clean backup copies, and enables you to:

- Provide immutable data protection
- Identify and automate data protection for key business assets
- Isolate backup data from the data center network
- Secure data in flight and at rest

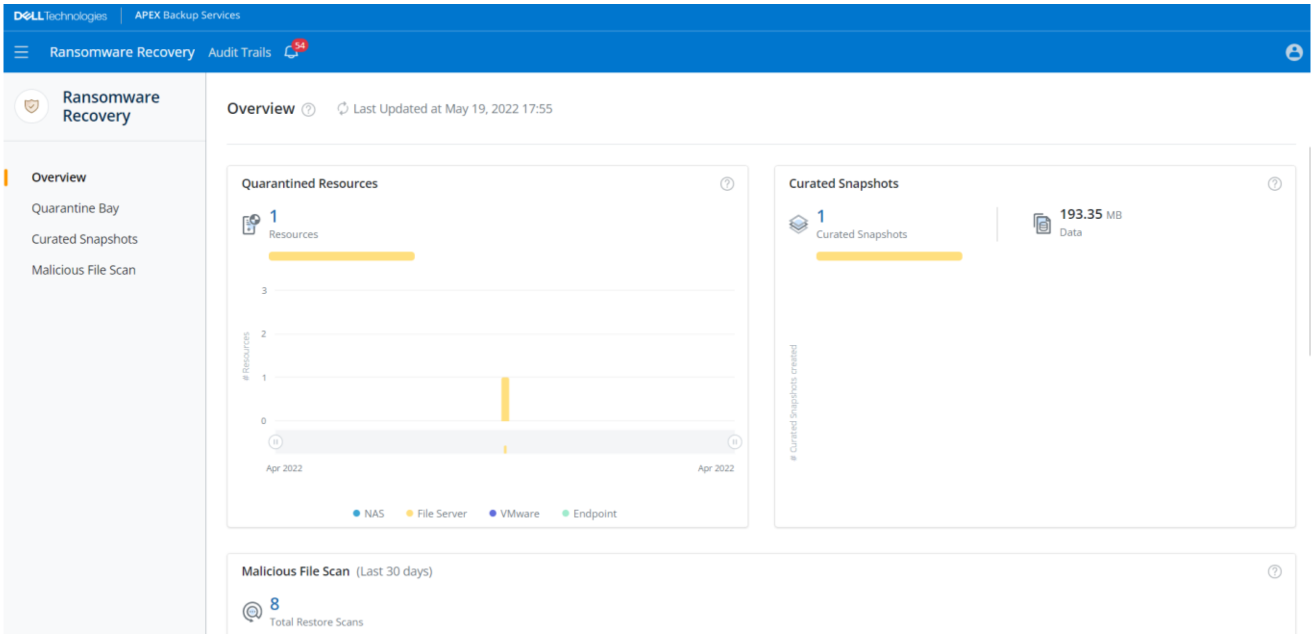
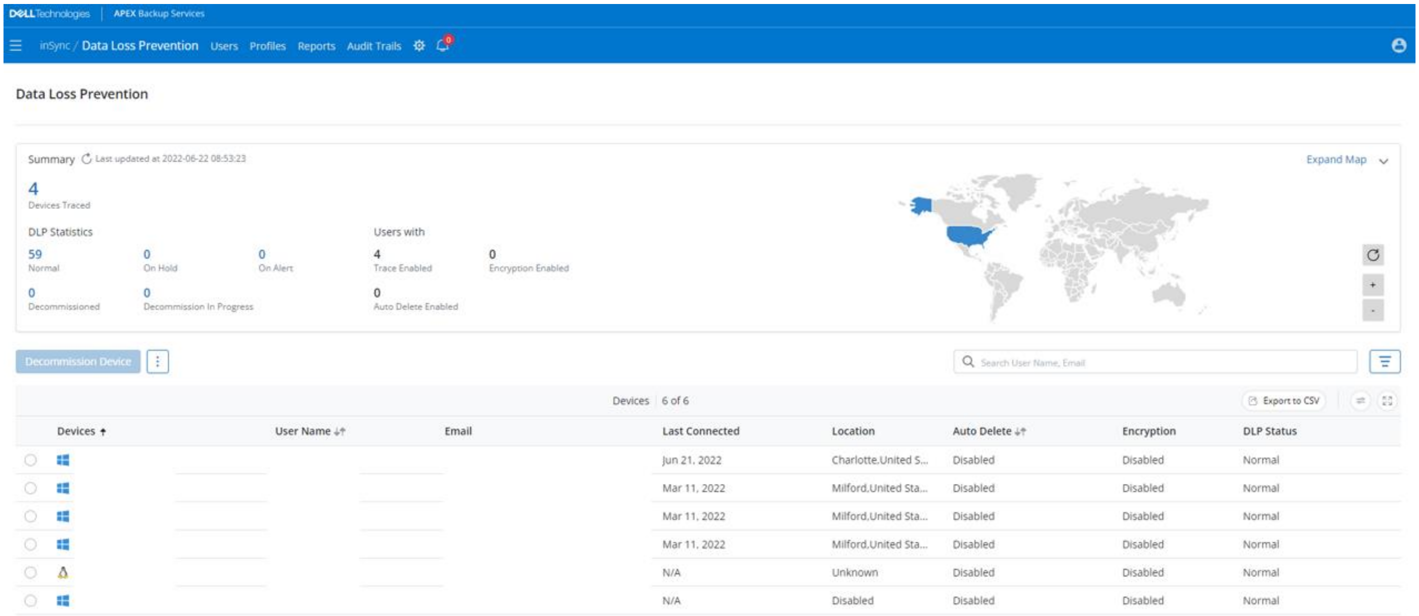


Figure 22. Ransomware Recovery dashboard

Data Loss Prevention

APEX Backup Services offers data loss prevention (DLP) features. These features enable IT administrators to maintain secure control over sensitive data on endpoint devices and respond to potential data loss events quickly if endpoint devices are lost or stolen. DLP is an effective solution that reduces the total economic impact of a lost or stolen laptop or mobile device for enterprises.



Data Loss Prevention

Summary Last updated at 2022-06-22 08:53:23

4 Devices Traced

DLP Statistics

59 Normal

0 On Hold

0 On Alert

0 Decommissioned

0 Decommission In Progress

Users with

4 Trace Enabled

0 Encryption Enabled

0 Auto Delete Enabled

Devices 6 of 6

Devices	User Name	Email	Last Connected	Location	Auto Delete	Encryption	DLP Status
			Jun 21, 2022	Charlotte,United S...	Disabled	Disabled	Normal
			Mar 11, 2022	Milford,United Sta...	Disabled	Disabled	Normal
			Mar 11, 2022	Milford,United Sta...	Disabled	Disabled	Normal
			Mar 11, 2022	Milford,United Sta...	Disabled	Disabled	Normal
			N/A	Unknown	Disabled	Disabled	Normal
			N/A	Disabled	Disabled	Disabled	Normal

Figure 23. Data Loss Prevention dashboard

DLP provides powerful, multi-layered protection of critical data residing in your organization’s devices such as:

- Remote device encryption and sanitization capabilities to prevent data breach
- Geolocation capabilities to aid in device recovery
- Geofencing that can restrict access to data from specific IP addresses or locations

Insights

File Analytics

File Analytics provides you detailed insights which you can turn into a source of discovery to:

- Understand the type of data protected in your organization
- Understand the data growth trend and its impact on your storage consumption
- Visualize, manage, and plan for your storage requirements in the future

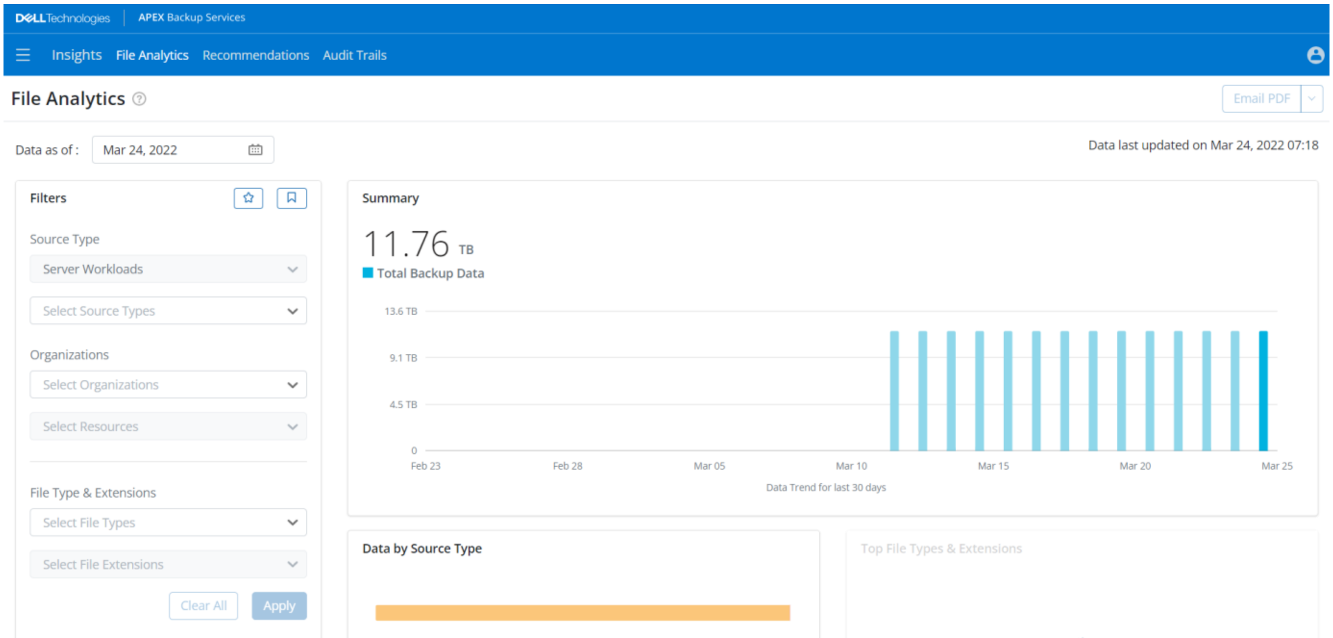
For an organization, the data that is generated can be classified as critical data, essential for running the business, and noncritical data, which may not be required to function a business. While it is essential to protect and preserve the critical data, noncritical data can be deleted or excluded from backup to eliminate the cost of protecting it.

APEX Backup Service dashboard components:

Protecting the right information has the following benefits like:

- Reduces overhead of managing and maintaining the data for operational requirements
- Reduces compliance risks in accordance with the government-imposed data protection acts
- Saves storage cost

File Analytics provides dashboard using which administrators can determine the type of data that is being backed up in the organization, identify whether the data under protection is critical or noncritical, and which datasets are driving up the storage costs.



File Analytics

Data as of : Mar 24, 2022

Data last updated on Mar 24, 2022 07:18

Source Type: Server Workloads

Summary

11.76 TB

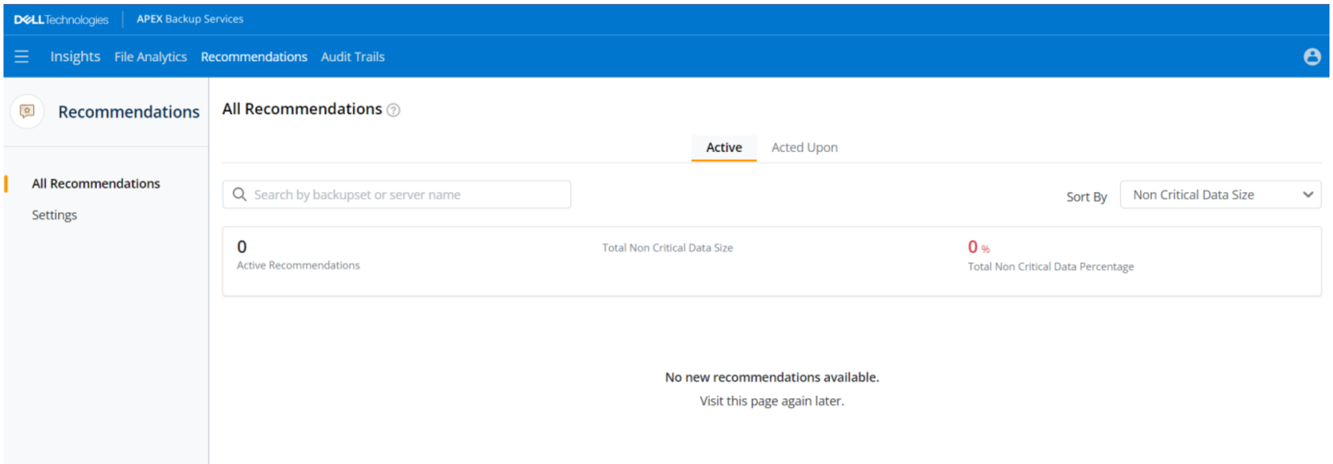
Total Backup Data

Figure 24. File Analytics dashboard

In parallel, you can use **Recommendations**, a smart service that automatically scans the data under protection and identifies the noncritical data and its total size in each of the backup set.

Recommendations

Recommendations is a smart service designed to identify and proactively inform administrators about the backup spends on the noncritical business data under protection and recommend necessary action to exclude it from backup and save costs.



All Recommendations

Search by backupset or server name

Sort By: Non Critical Data Size

0 Active Recommendations

Total Non Critical Data Size

0 % Total Non Critical Data Percentage

No new recommendations available.
Visit this page again later.

Figure 25. Recommendations console

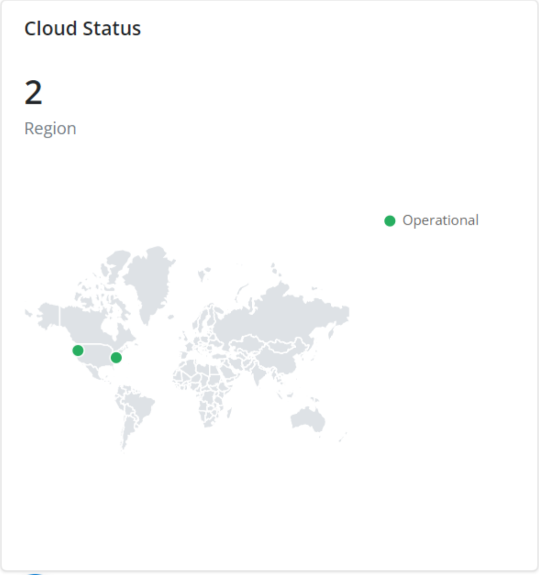
Recommendations sits on top of File Analytics. File Analytics provide administrators detailed insights and enable them to identify whether the data under protection is critical or noncritical. Eliminating noncritical data requires effort. Even if administrators or users decide to eliminate the noncritical data on their own, it can be an overwhelming task to get rid of all the noncritical data.

Recommendations enable faster detection of noncritical files and save costs. They enable administrators to:

- Monitor activity and take real-time actions to stop the noncritical business data from being backed up
- Get unprecedented visibility into the storage and analyze the type of data under protection
- Save the storage costs by improving the content rules and backup policies

Cloud Status

This section shows the region where your snapshots are stored and their health. In the below example, two locations in the account are operational.



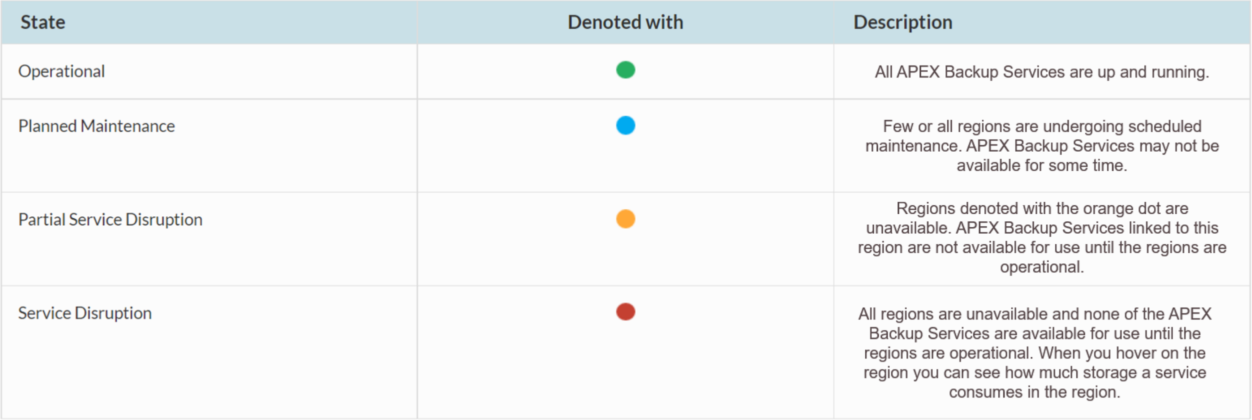
Cloud Status

2

Region

Figure 26. Cloud status > Health

The possible states are shown below:



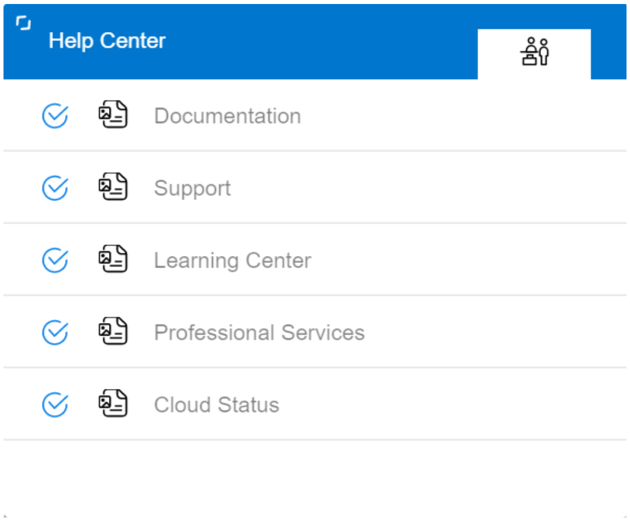
State	Denoted with	Description
Operational	🟢	All APEX Backup Services are up and running.
Planned Maintenance	🔵	Few or all regions are undergoing scheduled maintenance. APEX Backup Services may not be available for some time.
Partial Service Disruption	🟠	Regions denoted with the orange dot are unavailable. APEX Backup Services linked to this region are not available for use until the regions are operational.
Service Disruption	🔴	All regions are unavailable and none of the APEX Backup Services are available for use until the regions are operational. When you hover on the region you can see how much storage a service consumes in the region.

Other services

Besides the services mentioned above, you can use the following services:

Help Center

To access the Help Center, click the Help icon (question mark).



Help Center

- Documentation
- Support
- Learning Center
- Professional Services
- Cloud Status

Figure 27. APEX Backup Services > Help Center

The Help Center provides access to the APEX Backup Services product documentation, support, learning center, professional services, and cloud status.

References

Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- APEX Info Hub
- APEX Backup Services
- APEX Backup Services Data Sheet
- APEX Backup Services for Hybrid Workloads Solution Brief
- APEX Backup Services for Endpoints Solution Brief
- APEX Backup Services for SaaS Apps eBook