DELL Technologies

APEX

SOLUTION OVERVIEW

APEX Backup Services Security Overview

Why end-to-end security is crucial when choosing a cloud-based platform

Introduction

Your organization is tasked with ensuring data security, regardless of how or where backup solutions are deployed. Whether extending your existing data center or leveraging SaaS applications as part of a cloud-first strategy, data security is paramount. This is true regardless of whether your backup deployment is on-premises, in the cloud, or a hybrid model. Choosing the power of the cloud doesn't result in lessened security. At rest or in flight, your data is protected by the security and data governance tools APEX Backup Services provides. APEX Backup Services is built on AWS and offered as-a-Service, with inherently strong security. AWS provides a mature, cloud-based infrastructure, and its platform is globally ubiquitous. Security at an infrastructure level remains constantly on-duty, allowing organizations to access cloud data whenever, wherever. By freeing themselves from the burden of unnecessary hardware, capacity planning, and software management, customers can drive down costs.

Protect data from loss or compromise, anywhere

The amount of data stored in and used from the cloud is rapidly expanding. At the same time, end users are increasingly accessing that data from mobile devices. Smartphones and tablets, in conjunction with the cost savings and elasticity of the cloud, are stretching traditional security perimeters to the point that they almost dissolve. This dissolving of the traditional security perimeter makes it mandatory for data to be secure and recoverable no matter where it lives.

The cloud-native architecture and data loss prevention (DLP) capabilities of APEX Backup Services take this security paradigm into account. Organizations are empowering to protect data with:

- Flexible backup and recovery solutions that protect data from loss or compromise
- 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

Protecting data in flight and at rest

A key attribute of any cloud service is securing data both in-flight and at-rest. To protect data in-flight, APEX Backup Services uses industry-standard Transport Layer Security (TLS) for all data transmitted to the platform. Once the data arrives in the cloud platform, it's immediately encrypted using a customer-unique AES 256-bit encryption key. This encryption key is also completely controlled by that customer; each customer has their own unique key to access their backup data. This provides logical separation from the APEX Backup Services control plane and prevents data leakage in the cloud for data at-rest.

The customer encryption key is a session-only based key algorithm modeled on digital envelope encryption. This results in the customer key is never stored unencrypted, transferred, or accessible from outside a user's active cloud-side session. Thus, the need for expensive and complex key management solutions is eliminated.

An additional layer: Deduplication for data at rest

Deduplication technology provides another layer of security. Deduplication, or dedupe, refers to files being separated into individual blocks. Only unique blocks are sent to APEX Backup Services globally, across all devices. This means that entire files don't have to be repeatedly stored and replaced when changes are made, just some of the building blocks.

These unique blocks are stored in an object-based storage repository without any identifying metadata, while block reference data and associated source file metadata are stored in a separate object-based NoSQL database. This approach completely obfuscates the underlying data. Reconstitution of data is only possible through authenticated customer credentials, which are required to instantiate the session-based key mechanism.

The result of this encryption of unique blocks is that the data is sharded, scrambled, and stored within the environment in a manner that makes it impossible for anyone to decrypt and reassemble the information without authenticated customer credentials.

Shared security for the cloud

Building SaaS applications on top of cloud-based infrastructure requires shared security responsibilities. APEX Backup Services protects data across the entire stack, from infrastructure to application. The Cloud Service Provider (CSP) provides security for the infrastructure and platform layers, while the software delivers additional security functionality, safeguarding the information residing within the application being hosted.

Data resiliency and storage efficiency

APEX Backup Services uses Amazon S3. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. Amazon S3 also regularly verifies the integrity of data stored using checksums. If Amazon S3 detects data corruption, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Moreover, periodic integrity checks are performed on the APEX Backup Services cloud platform to ensure restorability of customers data. This involves simulating a full restore of data. If any of the files are not restorable, subsequent backup ensures that the files are fully backed up again. A checksum of each block is also stored and periodically integrity checked to avoid bit rotting.

Single sign-on simplifies access

When the number of applications increases, so does complexity. The addition of SaaS-based applications generates challenges like managing authentication and user access, and effective scaling across a variety of device types and browsers. Organizations have embraced cloud-based, single sign-on (SSO) solutions to handle Identity and Access Management (IAM) holistically.

To seamlessly integrate with this strategy, APEX Backup Services supports the use of cloud based SSO solutions such as Okta, Ping Identity, and Microsoft ADFS for both administrators and end users. Organizations can also leverage more traditional directory services implementations such as Microsoft Active Directory or LDAP for user authentication, if necessary.

Manageability and traceability keep data audit-ready

Traceability of security events on any device is a standard requirement in any regulated environment. APEX Backup Services supports the use of audit logging of security events for both users and administrators.
Audit logging for SaaS applications is done in real time, on an event-driven basis, with time and date stamping. The audit logs can be stored on the system based on customer requirements. They can also be downloaded for additional analysis in CSV or HTML format.

RBAC affords granular privilege control

To prevent privileged users from making unauthorized changes to resources within their own instance of APEX Backup Services, role-based access control (RBAC) has been implemented. This capability allows organizations to limit privileged user access to a predefined set of roles and data assets, making it possible to create ethical walls to enforce privacy. RBAC also enables the implementation of a delegated administration structure to meet customers' organizational, compliance, and security requirements.

Conclusion

As the use of cloud-based SaaS applications continues to grow, so will the need for proper security and information governance capabilities that give organizations total visibility of their information, no matter where it resides. The good news is we have the tools and the knowledge to deliver security in the virtual environment, improving the state of virtual security over time.

DELL Technologies

APEX