DELL Technologies

TD SYNNEX

APEX

APEX Backup Services

A guide to the standard ransomware protection and recovery features in APEX Backup Services

Introduction

The rise of ransomware has become a crisis that has crippled organizations world-wide. New strains of ransomware and other malware threats are on the rise and using more advanced social engineering techniques to facilitate their spread. With more employees transitioning to working remotely, the risks and exposure to ransomware are higher than they have ever been.

Ransomware is a form of malware that encrypts and holds your critical business and customer data hostage, and you are unable to access your data until you pay the demanded "ransom" to obtain the encryption 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, which can permanently shut down your business. With the growing frequency and sophistication of ransomware threats, Security Operations leaders are acutely aware of the consequences of excessive downtime, data loss and business disruption due to ransomware attacks.

In today's diverse and distributed IT environment, restoring the organization's applications and data quickly in the event of a ransomware attack is a significant challenge. In order to give businesses a framework for adopting a strong cyber resiliency strategy, the National Institute of Standards and Technology (NIST) published the Cyber Security Framework, consisting of guidelines and best practices to manage cyber security risk including identification, detection, protection, response and recovery.

Reliable data protection is a crucial line of defense against ransomware. Having secure backup images of critical business data and applications allows companies to roll back in time to recover applications and data before the point of ransomware infection. Organizations should use backup to protect data and applications that are particularly vulnerable to ransomware such as end-user data, NAS, file shares, virtual machines and SaaS applications including Microsoft 365.

There are several data protection solutions in the market to help address backup and recovery. However, on-premises solutions are not immune to ransomware once the data center systems are impacted. Your business needs a solution that provides assurance a clean copy of your data can be restored to a point int time.

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. There are steps you can take to help improve your business resilience to ransomware attacks.

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

Identify and automate data protection for key business assets

In order to recover from ransomware (without paying the ransom), you must have a secure backup copy of your applications and business data. The first step for any data protection strategy is to understand the full scope of the applications and data that needs to be protected. This includes not only the critical servers and applications that power your business, but also the entry points where ransomware can attack (primarily your end users).

When assessing your data protection needs, consider these key areas for protection:

- End user data - One likely source of a ransomware attack comes through social engineering of your end users. Endpoints (laptop, mobiles devices, etc.) need to be protected in order to recover from a ransomware attack.
- Data center applications and data - These systems are the true target of ransomware, and loss of access to these systems can critically impact your business. Protecting the virtual machines, NAS systems and databases are critical to the health of your business.
- SaaS applications - As the use of cloud computing increases, it is critical to ensure that cloud applications (Microsoft 365, Salesforce, Google Workspace, etc.) can be restored quickly in the event that ransomware infects the systems.

Automating the data protection processes of your key assets ensures that you have up to date backups and can facilitate a timely recovery. Configurable backup policies and pre-configured compliance templates assist you with defining the assets to protect with include compliance and retention policies as appropriate to your environment. Flexible recovery options offer the assurance that you can restore your data from a pristine, point-in-time backup. From a single console, IT has the flexibility to perform granular level and bulk restores to the original or an alternate location.

APEX Backup Services offers a unified cloud data protection platform top protect your endpoints, SaaS applications, and hybrid workloads, giving you the flexibility to protect all your key assets.

Isolate backup data from corporate network

One of the challenges of on-premises data protection solutions is that they are exposed to the same ransomware threat as the rest of your data center environment. Any backup environment attached to your network can be infected with ransomware, preventing you from accessing your backup data at a critical time.

Unlike on-premises data protection solutions, APEX Backup Services offers immutable protection. Backup data is isolated from the customer's network and is protected in the APEX Backup Services platform by design.

The APEX Backup Services cloud-native architecture ensures your backup data is not at risk from ransomware and prevents ransomware from encrypting your clean backup copies. Data protected in APEX Backup Services cannot be modified or deleted by ransomware. Your backup data is protected without the need to manage extra processes, software or hardware. These benefits are part of APEX Backup Services foundation and delivered natively.

With distributed data and applications, data management, privacy and security has become a ubiquitous challenge for IT teams. Typically, with an on-premises backup solution, the onus is on the Security Operations or IT administrators to upgrade data protection software and backup appliances, to prevent exposure to security threats. The cost to manage and maintain the on-premises infrastructure and software comes at a price, which could become another challenge given shrinking IT budgets.

APEX Backup Services was designed around a zero-trust security architecture, which is changing the game by enforcing the adoption of newer security best practices to address the security demands on the technology stack. Built natively on AWS's security framework, APEX Backup Services inherits the global security, compliance and data residency controls, thus adhering to the highest standards for privacy and data security.

APEX Backup Services is updated frequently to release the latest features and security updates, transparently in the background. This allows APEX Backup Services to support continuous feature development and automatically apply new security enhancements without IT needing to manage timely upgrades and maintenance.

Secure data in-flight and at rest

- A key attribute of any cloud service is to be able to secure data both in flight and at rest. All data that APEX Backup Services sends to the cloud is protected in flight to AWS using industry standard, Transport Layer Security (TLS 1.2). Data at rest, whether it is stored on-premises with Cloud Cache or in the cloud platform, is protected with AES-256 encryption. APEX Backup Services stores the data by splitting it into blocks and deduplicating, with unique data blocks getting stored into Amazon S3 and metadata in Amazon DynamoDB and uses Amazon EC2 as 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 doesn't get access to the data layer.
- Within the data layer, APEX Backup Services encrypts the data using its proprietary envelope encryption technology, making it impossible for anyone besides the customer to access the data.
- Customers have sole access to their data which is in line with our secure by design philosophy.

The APEX Backup Services cloud-native architecture was designed around a zero-trust architecture model, with access control being an important aspect of that model beyond the secure method by which we store customer data.

- Access to applications is monitored and controlled via 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.
- Administrative control settings prevent end users from deleting backup data.
- APEX Backup Services provides the ability to customize admin roles to prevent snapshots deletion. A best practice would be to designate no more than two people in the organization as APEX Backup Services Admins, and then multiple admins can be created with no rights to delete snapshots

APEX Backup Services stringent security compliance and certifications

While many cloud SaaS vendors simply rely on the certifications that the cloud service providers (CSPs) provide for the infrastructure as their security model, APEX Backup Services provides additional compliance for our cloud services. These certifications are available upon request. In addition to these certifications, APEX Backup Services has ongoing penetration tests conducted for any security vulnerabilities by third parties (Coalfire, Bishop Fox, Cobalt. io) to ensure the highest levels of security compliance.

Conclusion

Ransomware attacks are more prevalent today than ever before. You need a sound data protection strategy that addresses business resiliency and continuity concerns. APEX Backup Services comprehensive cloud data protection and robust security and compliant platform can power Security Operations and IT teams to both protect and recover faster in case of any external or internal attacks including ransomware and accidental or malicious data deletion.

Visit delltechnologies.com/apex-backup to learn more.

DELL Technologies

APEX