DRP Nuabee solution security architecture

Security architecture · https://nuabee.com/documents/security-architecture-drp-solution-nuabee/

Introduction

Nuabee offers a complete backup and Disaster Recovery Plan (DRP) solution, designed to guarantee the confidentiality, integrity and availability of backups throughout their lifecycle. Here's a detailed look at the Nuabee solution's secure architecture, highlighting the various stages of data protection, from initial backup encryption to encryption key management.

Backups encrypted at source

Data security at Nuabee begins with the creation of backups. All data is encrypted at source, i.e. before it leaves the customer's infrastructure. It is the customer's responsibility to define the backup encryption key and store it in a secure location.

This initial encryption process uses advanced encryption algorithms (AES) to ensure that data is protected against unauthorized access from the outset. By encrypting data at source, Nuabee provides a robust first line of defense against compromise attempts.

Secure transport of backups to the cloud

Once encrypted, backups are securely transported to the cloud. Nuabee uses secure transmission protocols to protect data in transit. These protocols include technologies such as SSL/TLS, which ensure that data cannot be intercepted or altered during transfer to cloud environments.

This secure transport is crucial to maintaining data integrity and confidentiality during transit.

Secure cloud storage

Encrypted backups are stored in an isolated, highly secure Cloud environment.

Specifically, they are stored in dedicated S3 buckets, an object storage service renowned for its flexibility and security. S3 object storage provides advanced features to ensure data durability,

availability and protection.

Nuabee implements rigorous configurations for S3 storage to ensure that data is protected by robust security measures, such as data-at-rest encryption and granular access controls. Designed for high durability, S3 uses a data redundancy architecture to ensure continuous availability. In addition, S3 buckets enable fine-grained access and permissions management, offering precise control over who is authorized to view or modify stored data.

In addition to these measures, Nuabee has set up a secure internal process for managing critical modifications to data stored in these buckets. This process is activated following specific customer requests, and involves rigorous checks to ensure that only authorized people can make changes to the storage. Critical modifications, such as restoring or deleting data, are strictly controlled and audited to guarantee data security and integrity.

Immutability of backups in S3

Nuabee offers the option of storing backups in S3 buckets with immutability functionality. Data immutability ensures that backups cannot be modified or deleted during a specified period. This feature is activated using the Object Lock option, which adds an extra layer of security by making data unalterable for a defined period.

Secure encryption key management

The encryption keys used to encrypt backups at source are managed with the highest level of security. They are stored in a digital safe, encrypted and totally inaccessible to humans. This safe is designed to protect the keys from unauthorized access, ensuring that only automated industry procedures, known as "indus", can use them.

This indus is the only one with access to the encryption keys, and only for specific processes such as data restoration during DRP or DRP testing. This approach ensures that even if the system is compromised, the encryption keys remain protected and the data secure.

Identity and Access Management (IAM) in DRP environments

In Nuabee's Disaster Recovery Plan (DRP) environments, Identity and Access Management (IAM) is essential to guarantee the security of critical data. Nuabee applies granular access controls, ensuring that only authorized users can access and manipulate the necessary resources. Multi-

factor authentication (MFA) to Cloud environments reinforces this security by adding an extra layer of verification.

Access is rigorously monitored and logged, with activity logs regularly audited to detect any anomalies. In addition, strict processes are in place to manage temporary access in the event of emergency intervention, ensuring that every operation is carried out safely and in accordance with security policies.

More details

Cloud-native security solutions OTC

To further protect data and resources, Nuabee integrates cloud-native security solutions such as Cloud Trace Service (CTS) and CloudEye.

> **Cloud Trace Service (CTS)** provides detailed monitoring of activities in the cloud environment, logging events for complete visibility of actions performed and resources accessed. This enables suspicious or non-compliant behavior to be detected and analyzed, providing a rapid response to potential incidents.
>
> **CloudEye**, meanwhile, is a real-time monitoring and alerting solution that monitors the status and performance of cloud resources. It provides proactive alerts on anomalies and potential threats, enabling effective management of incidents before they affect operations. By combining these security tools, Nuabee provides enhanced protection against internal and external threats, while offering complete visibility and rapid response to security incidents in cloud environments.

In addition, Nuabee uses **Security Groups** and **Access Control Lists (ACLs)** to control network traffic and secure cloud instances. Security Groups act as virtual firewalls, defining ingress and egress rules for instances, while ACLs offer more granular control over network traffic at subnet level.

VPC (Virtual Private Cloud) isolation is also a key component, enabling the network to be segmented to isolate different applications and data, minimizing the risk of lateral compromise in the event of a security breach.

Conclusion

The secure architecture of the Nuabee solution offers end-to-end protection for customer data, from initial encryption to key management. By encrypting data at source, ensuring secure transport to the cloud, and offering immutability options, Nuabee effectively protects it against internal and external threats.

Rigorous management of encryption keys, with limited access to indus for restore operations, ensures that data security is maintained at every stage. Thanks to these measures, Nuabee provides a backup and disaster recovery solution that meets the security and reliability requirements of the market.