CASE STUDY :PayNearBy

PayNearBy Built up a Highly Secure & Reliable Solution to Keep Their Data Safe & Secure

rapyder
Making CLOUD work for you

Client
PayNearBy

AWS Services
AWS Workspaces, Directory Service, NAT Gateway, VPN, Config, S3, CloudWatch, CloudTrail, IAM

Introduction

Incepted in April 2016, Nearby Technologies is a fintech company offering financial/non-financial services to the underbanked and unbanked segments. Nearby Technologies works on a B2B2C model through its various brands – PayNearby, Insure Nearby, BuyNearby, and a few more. PayNearby empowers retailers at th first mile to offer digital services to local communities, thereby boosting financial inclusion in India. Retailer services focus on Aadhaar based banking services, Domestic Remittances, Bill Payments, Card Payments, and insurance services.

PayNearBy, here after referred to as "Customer".

Business Needs

Customer did the contingency planning for their business along with various operations required for their business & came up with multiple action items internally.

One of the action items was to build a VDI solutions for their internal users so that they should be able to work on their projects in case of any major issue.

Below were the requirements from the customer:

- A highly secure and reliable solution which would keep their data safe & secure from any theft or loss.
- Secure connectivity & access to applications/data deployed in the customer's own data center.
- User authentication using their centralized identity management system in place at customer's own data center to track & manage access smoothly.
- The solution should also serve as a contingency plan for their business continuity, in case their premises are not accessible due to some unavoidable reasons.

Solution Approach

Our AWS Certified Solutions Architects conducted detailed workshop sessions with the customer to understand their existing setup, challenges, and requirements. In the discovery, we also captured the licensing and software requirements for remote users.

Following the solution, the approach was proposed and implemented with best practices and business continuity

principles, and then migrated their production workload to AWS.

- AWS Workspaces were proposed, as it is a highly reliable managed service and would have minimal operational overhead.
- A separate network with a combination of VPC/Subnets was created as per the best practices.
- All the workspaces were launched in private subnet & endpoint accessible through the internet.
- AWS & Customer Data Centre was connected using AWS site to site VPN tunnel for establishing connectivit required between AWS Workspaces & On-Prem Data/applications.
- The workspaces were integrated with ON-Prem Active directory for authentication with the AD connector.
- Workspaces were also hardened according to the requirement of the customer.
- Office & Anti-Virus packages were provided by the customer & included in the image to launch Workspaces.
- Installation packages for other agent-based software required were also included in the image.
- All traffic from the internet has been routed through the site-to-site VPN tunnel to access the internet and applications.
- Restricted policies applied to prevent any data movement between AWS Workspaces & User machine.
- Both web-based and client-based applications were configured as part of this setup.
- AWS CloudTrail will be configured for tracking the API Calls.
- AWS CloudWatch was configured for monitoring various matrices of the setup.

Reaping Rewards

- AWS workspaces solved customers need to have business continuity in place for all the users.
- With this solution, we were able to provide a secure and reliable remote workplace option for the user set separate from the existing setup.
- AWS VPN connectivity between AWS & On-Prem data center helped AWS workspaces communicate with applications & data residing on-prem with low latency.
- Data copy restrictions were applied from AWS Workspaces to user's personal machines to safeguard data from theft & loss.
- Connectivity to On-Prem AD enabled the customer to have common & standard identity management for their users in AWS Workspaces.
- Conducted infra audit after the post-implementation support period to optimize the size of the AWS Infra as per the actual usage.
- Data Backup / Restore drill was also performed to ensure that the automated backups are working & data is restored correctly.