Online Payment Platform

A leading online payment platform secures privileged access by deploying ARCON Privileged Access Management (PAM)

(Name withheld on request for confidentiality purpose)

Key Numbers

no. of privileged accounts

32 (Windows servers 15, UNIX based 11 and Network & Security 6)

no. of devices

Approximately 290

no. of privileged users

About 70 +

client brief

This is a case study of India's leading digital wallet company. With more than 200 million registered users as of today, the online payment company has been transforming payment methods in India with a mission to bring half a billion Indians to the mainstream economy by enabling countrymen to make digital payments and become part of financial inclusion.

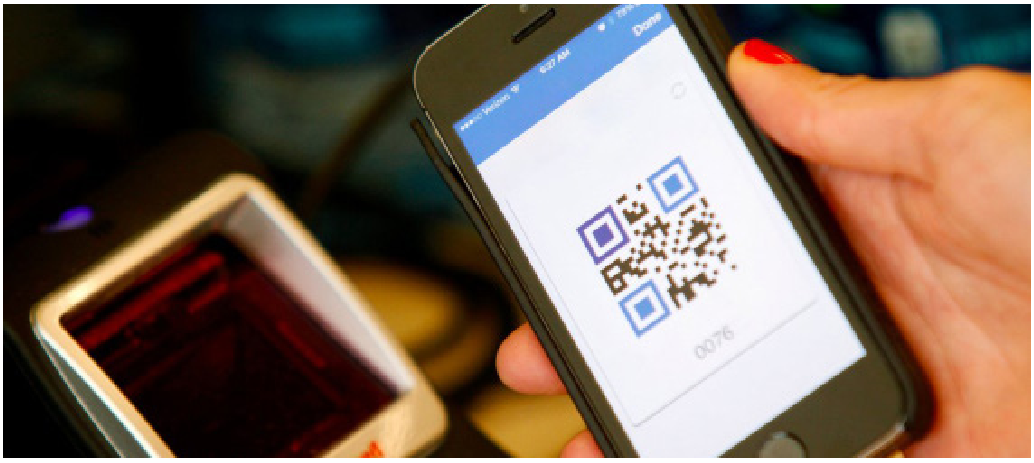
the context

Storing and processing a huge amount of customers' data is a daunting task. With more than 17 million estimated transactions everyday through the client's digital payment platform, slightest of security gaps within the inner realm could compromise IT systems and result in a data breach.

Managing and monitoring privileged access was mission-critical as our client wanted to build a robust security and compliance framework around database servers that were located in two data center environments.

key challenge

- Management of two datacenter environments located in two different cities with devices evenly distributed
- Unmonitored and uncontrolled privileged activities as the operation team used to access servers using Named IDs and Service IDs
- The client had Mac users. It was vital that employees with MacBook were able to access devices through ARCON PAM
- No session monitoring (Absence of video logs)
- No mechanism for password management



the solution

After a thorough IT architecture mapping, ARCON implementation team suggested arole-based generic IDs. Earlier, operation team used Service IDs and Named IDs with high privileges for connecting to devices. After deployment of ARCON PAM, remote access to these highly elevated identities were removed. ARCON PAM enabled the operations team to access devices only through mapped role-based, time-based, and group-based privileged IDs thanks to Granular Access Control feature. The solution also provided password vaulting that ensured compliance with strength and frequency of password change requirements demanded by regulator in a seamless manner.

Additional Value Adds:

- The solution enabled the end users using several operating systems like Windows, Ubuntu, UNIX and MAC to easily access the target devices
- It allowed secure privileged access to an entire network of security devices, windows servers and UNIX systems
- The solution enabled the client to capture comprehensive audit trails and session recordings to ensure that all activities are tracked in a real-time

about ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Identity Management and Continuous Risk Assessment solutions. With its roots strongly entrenched in identifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.