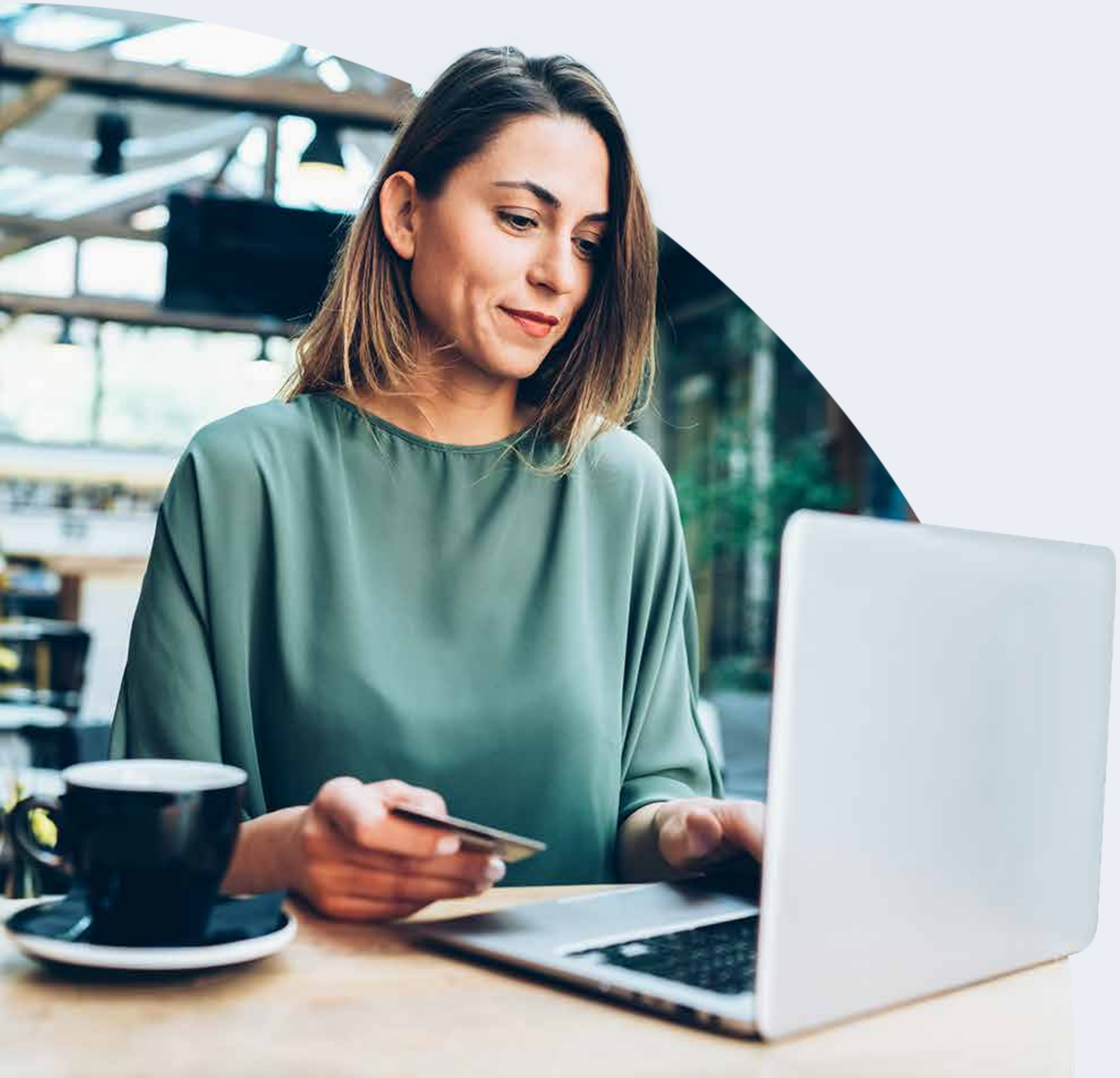
zensar



Secured Banking Over Cloud through Cloud Secure Framework

Case study

Client

The client is one of the fastest-growing banks in the United States. The existing client infrastructure consisted of many obsolete mainframe servers (200+) and applications in four different data centers across various locations in the US. In addition to this, the client also had about 25% of the applications in Azure cloud regions. The client's focus was to reduce the reliance on data centers for its remote users to connect cloud applications and achieve cost optimization through cloud transition of its obsolete servers.

Challenges

- Decentralized security solutions with no overall visibility
- Obsolete mainframe servers vulnerable to the evolving threat landscape, with little to no support
- Consolidation of DC and Greenhouse project to migrate and secure obsolete mainframe servers from the data center to Azure cloud
- High rate of false positive incidents and alerts posing a significant challenge due to lack of well-trained staff to manage the existing solutions
- Lack of proper security automation solutions leading to high mean time to detect (MTTD) and mean time to repair (MTTR)

Solutions

We helped the client save cost through cloud migration security services and achieve adherence to all major security compliances.

Initially, we carried out an eight-week assessment study to understand the existing mainframe server dependencies. We created a plan on how to facilitate the migration process to Azure cloud by consolidating the data from on-premises and cloud servers.

We carried out the following activities in a nine-month implementation and transformation phase:

- We served as the intelligent migration advisor to migrate obsolete servers to Azure cloud
- Cloud secure framework was implemented to provide holistic visibility and security around cloud posture and risks
- Single-pass architecture was deployed to improve security for remote users to access cloud applications through secure access service edge-based (SASE) solution. The benefits of the SASE solution were secure web gateway, data loss prevention, next-gen firewall, and intrusion detection and prevention system
- Cloud security controls were designed and implemented at different layers from perimeter to workload

- Security controls with security orchestration, automation, and response (SOAR) and total security management (TSM) integration were automated
- After completing the transformation phase, we created a six-week transition plan to business as usual to ensure that smooth onboarding was in place. We developed custom alert rule books and a playbook library along with 24/7 monitoring support to facilitate this.

Further, we planned the following steps to optimize the security solution:

- Continuous fine-tuning of the alert rule library to reduce the false positives
- Continuous automation of workflows and runbooks to reduce L1 efforts

Business Impact:

- 34% overall security costs reduced with cloud secure framework
- 60% productivity improvement through automation
- Reduced false positive reporting by 90%
- 100% obsolete servers migrated to Azure
- Achieved SOX, PCI compliance and adherence

zensar

An RPG Company

At Zensar, we're 'experience-led everything.' We are committed to conceptualizing, designing, engineering, marketing, and managing digital solutions and experiences for over 145 leading enterprises. Using our 3Es of experience, engineering, and engagement, we harness the power of technology, creativity, and insight to deliver impact.

Part of the $4.8 billion RPG Group, we are headquartered in Pune, India. Our 10,000+ employees work across 30+ locations worldwide, including Milpitas, Seattle, Princeton, Cape Town, London, Zurich, Singapore, and Mexico City.

For more information, please contact: **info@zensar.com | www.zensar.com**