A mid-size Pan India Bank's Journey to Secure Hybrid Cloud Applications and Crown Jewels with Micro segmentation Use Cases

BANKING

BACKGROUND

Financial institutions, driven by the need for cost savings, automation, and enhanced security, are increasingly embracing agile technologies like hybrid cloud solutions. Amid this digital transformation, security remains a paramount concern. This case study explores how a mid-size Pan India Bank successfully addressed these challenges by implementing a Microsegmentation solution, focusing on Application Ring Fencing.

CHALLENGES

Third-party Access Complexity: The bank heavily relied on third-party applications, partners, and outsourcing vendors, leading to complex access routes. The de-facto use of open-source software libraries in most of the Software these days has further expanded the attack surface, demanding granular access control up to the application library and process level.

Hybrid Environment Complexity: The bank's mix of cloud, container technologies, standalone, and legacy systems created a complex and challenging environment to visualize, audit, and protect. The bank needed a way to monitor and secure lateral network communications effectively.

Ransomware Threats: Ransomware attacks were on the rise, necessitating a rapid response mechanism to contain infections should they occur.

Lack of Data Visibility: The bank lacked comprehensive data, including Software Bill of Materials (SBOM) and communication channel information, which hindered policy definition for Ring Fencing and cloud migration.

SOLUTIONS

The bank engaged QOS to propose the Akamai Microsegmentation (formerly Guardicore) Solution:

Demonstration and Education: QOS demonstrated various use cases of the Akamai Microsegmentation solution, showcasing process-level policy definition and ring-fencing capabilities. This addressed the bank's concerns regarding cloud migration and ring fencing.

References: Akamai provided references from other large banks, including one in the US and a prominent Indian private bank, which successfully implemented the solution and met regulatory requirements.

Expert Consultation: QOS deployed a team of certified GCSE consultants, leveraging in-house accelerators to automate labelling and select authorized communication channels. They achieved Ring Fencing for two critical applications within the first month and 28 applications within three months.

Legacy System Support: The bank's mix of AIX, Solaris, Windows, and Linux servers posed challenges. Akamai's product support and 24x7 Customer TAC assistance helped overcome initial deployment hurdles on legacy systems.

Policy Definitions: QOS used past experience and in-house templates/accelerators to create skeletal policy definitions for Ring Fencing and Zone-wise Microsegmentation, down to the process level.

Sustenance Partner: Post-successful deployment, the bank approached QOS for an annual contract to provide ongoing support and subject matter expertise.

BENEFITS

Regulatory Compliance: The bank achieved compliance with regulatory directives by successfully implementing Ring Fencing for all banking and treasury applications.

Reduced Attack Surface: By enforcing east-west security policies, the bank significantly reduced its attack surface and gained the ability to contain malicious activities, such as malware or ransomware propagation.

Zero Trust Model: The bank now has enhanced visibility into process-level communications and can enforce policies based on a Zero Trust Network Access (ZTNA) model, laying a strong foundation for core applications and underlying compute.

Unified Application Labelling: The bank established a ubiquitous application labelling framework that seamlessly covers on-premise and public cloud applications, ensuring smooth transitions without compromising security.

In conclusion, this case study demonstrates how a mid-size Pan India Bank successfully addressed complex security challenges and achieved regulatory compliance through the implementation of the Akamai Microsegmentation solution supported with a unique set of deployment accelerators by QOS, creating a secure and agile environment for its hybrid cloud applications and crown jewels.

QOS Technology offer intelligent solutions to secure & accelerate businesses. With certified resources, focus on quality and agility in delivery, we combine cyber security and analytics to provide cutting-edge security solutions.

For more information, visit www.qostechnology.in or reach out to us at contact@qostechnology.in

