

# Case Study - Asian Banking Customer

## Securing the Perimeter and Applications

This Asian Banking customer provides a comprehensive range of banking, consumer finance, investment, asset management, and other financial products and services to individual consumers, DDoS, cross-site scripting, malicious traffic **DDoS** attack signatures, blacklisted source IP SMEs, and large corporations, through hundreds of branches and over multi-thousand service outlets nationwide.

## Baseline Categories Covered

1. DDoS Mitigation (DDoS-001)
2. Managed WAF (WAF-001, WAF-002, WAF-003)

## Business challenge

The banking giant's goal is to become one of the most innovative financial institutions, by expanding online banking services, offering mobile banking applications, and enhancing customer service through Artificial Intelligence (AI). Being one of the popular bank in this region, a '**Cloud web application and API protection platform (WAAPs)**' is almost mandatory to keep Cyberattacks including **level security layer protection** against known Ransomware, Injection Attacks etc. at bay. Thus, **devising a secure Application Environment & Infrastructure** had been a critical strategic imperative, with the key web applications.

Also, the customer wanted a trusted partner, to help with migration and in devising a hybrid cloud management system, that enables them to migrate and manage their applications seamlessly.

## Transformation

Kyndryl's solution contained a secure AWS landing zone providing Network Infrastructure & Security, Data Protection, Container Security, Intrusion Protection Services, Resiliency & Incident Response framework, and Compliance & Risk Governance.

Aligning with **Layered Defense Architecture principles**, a multi-layered approach was implemented in securing the bank's critical applications - starting with **application & network-databases, Bots and Spammers**, using a cloud-based WAAP engine. It is followed by the **firewall layer**, covering zero- day threat protection, deep packet HTTPS inspection, intrusion prevention system (IPS), and complete application and identity awareness, to the AWS Cloud. Third layer of protection is offered by **Web Application Firewall**, in protecting web-based applications and APIs exposed to the internet.

## Outcome

As a trusted partner, Kyndryl has continued to accelerate the digital transformation journey of this customer.

One of its strategic vision in building a secure and resilient cloud-ready Infrastructure, hosting the critical customer workloads & containers, had been achieved. **Securing the Perimeter and Web Applications had been established, through a layered approach using the DDoS protection, Firewall and WAF technologies, effectively protecting against various Cyberattacks, such Denial of Service, Malicious traffic, Injection Attacks etc.**

Also, Kyndryl has setup a 24x7 Management service support, to ensure the environment is available and secure, as defined by the customer's security policies.

Overall, this has resulted in the customer choosing Kyndryl, as a key long-term partner, in executing their digital transformation strategy



# Case Study : Asian Banking Customer

## Architecture Design

