CASE STUDY – CLOUD SECURITY

# Design and Implementation of Large-Scale Cloud Security Architecture & Security Controls to Protect Consumer Data for a Fortune 500 retailer

## CUSTOMER PROFILE

- Fortune 500 company and a global leader in fashion and consumer essentials.
- Customer across 150 countries and service portfolio of over 30+ international fashion brands.

## INDUSTRY

- Retail

## BUSINESS CHALLENGE

The client had transitioned their marketing, sales and consumer data to the cloud-based Customer Relationship Management platform to drive operational efficiencies in marketing activities, revenue growth, and enable improved customer experiences.

They choose the AWS Cloud Platform to migrate their on-premise data. Though the AWS cloud platform helped them in enabling business growth, it had security issues and challenges such as lack of data visibility, data controls and compliance, inability to monitor data, and increased risk of data theft. These compromises on security could lead to non-availability of platform services, leading to financial and reputational losses.

# SOLUTION RECOMMENDATIONS

Designed a complex, large-scale, multi-layered security architecture and implement security control and data protection for the online data platform.

Real-time cloud monitoring and conduct penetration tests to keep the platform and customer data safe.

Comprehensive cloud defense framework with built-in security from the beginning of the design stage.

Secure SDLC process to enhance the security posture and speed up deployments.

Defense-in-Depth as the core security principle and implement multiple security controls to secure customer data.

Deploy advanced technologies/tools on AWS cloud through virtualized containers to power scalability.

# SOLUTION APPROACH

- Design complex, large-scale, multi-layered security architecture and implement security controls and data protection of online data platforms. These platforms consolidate consolidates transactional and customer data, enabling marketing teams to mine big data and identify prospects for marketing campaigns.

- Real-time monitoring of cloud platform and conduct penetration tests to keep the platform and customer data safe.

- Comprehensive defensive framework with built-in security from the beginning of the design stage.

- Adopt secure SDLC process to enhance the security posture and speed-up deployments.

- Abide by Defense-in-Depth as a core security principle and implement multiple security controls to secure customer data. Advanced technologies & tools were deployed on the cloud through virtualized containers to ensure scalability.

- DevSecOps model for embedding security controls and monitor the deployment cycle.
- Vulnerability Scanners, Continuous Integration and Continuous Deployment, to deliver at speed along with effective vulnerability management.

## SOLUTION HIGHLIGHTS

**BIG DATA SECURITY:** Support the integration of multiple heterogeneous technologies with Hadoop, using Kerberos based authentication and sentry-based authorization. The integration helped to build data integration, data quality, and data governance processes while executing business intelligence and analytics use cases in a secure environment.

**DATA ENCRYPTION:** Ensure sensitive data is encrypted with minimal impact on performance. Data security achieved through Disk encryption, HDFS encryption (Cloudera KMS), AWS KMS, and Cassandra Native encryption.

**PII PRIVACY THROUGH ANONYMIZATION:** Anonymization for data science, analytics and user reports for PII data protection. Anonymizing ensures privacy of end-users is not reversed to the original form and ensuring sensitive data is invisible to unauthorized users, preventing data privacy violations.

**DEFENSE-IN-DEPTH:** Implementation of Kerberos authentication with SSO, RBAC access control, audit controls, non-repudiation, secure backup, and security monitoring (SIEM).

**MULTIPLE DIRECTORY INTEGRATION:** Integrate existing user credentials and multiple active directories to enable single sign-on option for users using heterogeneous applications.

**DATA ISOLATION:** Shield data of directly competing brands/products and third parties through data isolation methods. Data shielding enabled the client to store competing brand data and securely use fishing rules (targeting customers between brands) to grow sales.

**24*7 SECURITY MONITORING:** Implement Security Incident and Event (SIEM) Monitoring for the client's cloud platforms to ensure 24x7 continuous real-time monitoring. Raise alerts and act when unusual or fraudulent activities get detected.

**API SECURITY:** Protect internal and external API's integrated into the platform from attacks. Incorporate API security controls and drive testing activities to avert compromise, manipulation, and tamper of the cloud platform.

# CLIENT BENEFITS

### REGULATORY COMPLIANCE

Mitigate security issues in the cloud platform, ensuring total compliance as per industry standards preventing the risks of hefty fines and losses due to non-compliance.

### CLOUD AGNOSTIC

The security solution's cloud-agnostic approach allowed the client to adopt different cloud platforms across business lines and geographies. Cloud-agnostic security tools deployed for authentication, key management, vulnerability management, API, and containers helped the client in accommodating the migration needs of the future.

### SCALABILITY

Virtual containers used to bundle applications could be scaled based on business needs, VM images using Inspec and registries were also secured by configuring baseline security controls.

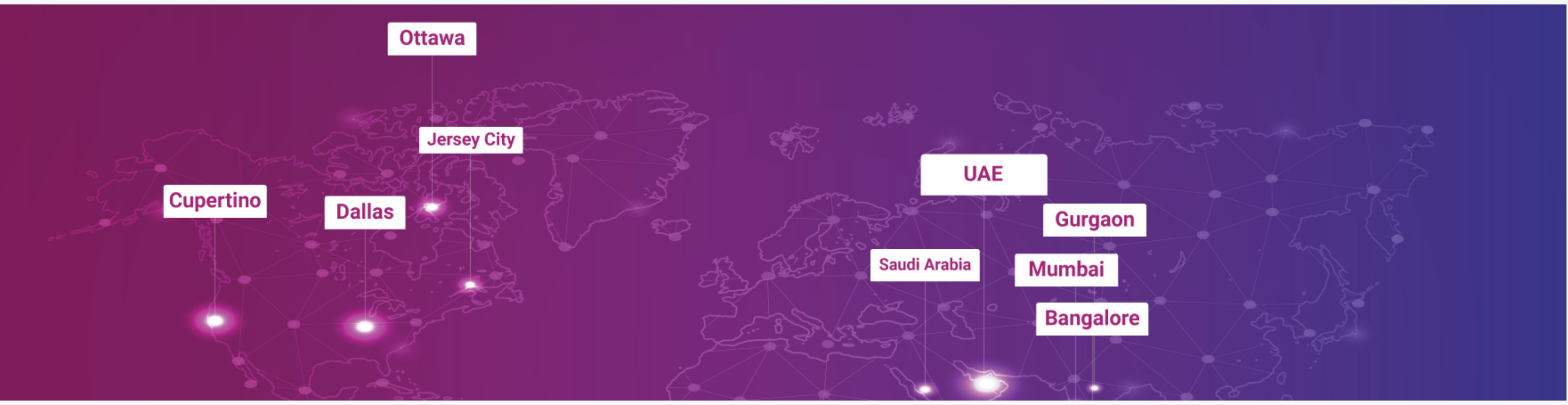
### SPEED AND AUTOMATION

Periodic builds and deployments coupled with automation of manual interventions for speedy onboarding of multiple brands and product lines. Integration of Fortify, Jenkins, JIRA for faster deployment. DevSecOps model implementation for automated security assessments and vulnerability management.

# ABOUT AUJAS

Aujas cybersecurity is an enterprise security service provider for organizations across North America, Asia Pacific, and EMEA regions. Aujas has deep expertise and capabilities in Identity and Access Management, Risk Advisory, Security Verification, Security Engineering & Managed Detection and Response services. By leveraging innovative products and services, Aujas helps businesses build and transform security postures to mitigate risks. The service focus is to strengthen security resilience by minimizing the occurrence of sophisticated attacks and threats while offering 360-degree visibility and protection across enterprise infrastructure.

For more information, do visit us at www.aujas.com or you can also write to us at contact@aujas.com


Ottawa
Jersey City
Cupertino
Dallas
UAE
Gurgaon
Saudi Arabia
Mumbai
Bangalore