Modernizing cloud security operations in financial services

02-03-2026

Table of contents

Modernizing cloud security operations in financial services

Executive Summary

Financial services firms operate under intense regulatory scrutiny while facing increasingly sophisticated cyber threats. As cloud adoption accelerates, leaders must ensure continuous monitoring, rapid incident response and centralized control across growing AWS environments without slowing innovation. This document details how a large American financial services company partnered with Cognizant to establish a 24/7 cloud security operating model on Amazon Web Services (AWS), creating a blueprint for the industry.

The core business challenge stemmed from the complexity of maintaining consistent security controls as the firm's AWS footprint expanded. The security team required real-time visibility into threats, a rapid and coordinated response capability and centralized orchestration for policies and audit evidence. They needed an always-on operating model capable of handling security incidents at any time.

The program integrated AWS-native and best-in-class marketplace controls to deliver full-stack protection. The solution spans threat detection, vulnerability management, identity and access, application security and automated response, all delivered as a managed service. This strategic approach addressed the immediate security gaps and established a scalable framework for future growth.

The results were transformative, leading to a 40% faster security incident response time and establishing 24/7 monitoring for business-critical environments. The program enabled risk-aligned remediation, improved continuous integration/continuous deployment (CI/CD) security integration and streamlined audit support through standardized configuration hardening and information technology infrastructure library (ITIL) aligned service delivery. This demonstrates a clear path for financial institutions to achieve a robust, efficient and compliant cloud security posture.

Introduction

Purpose:

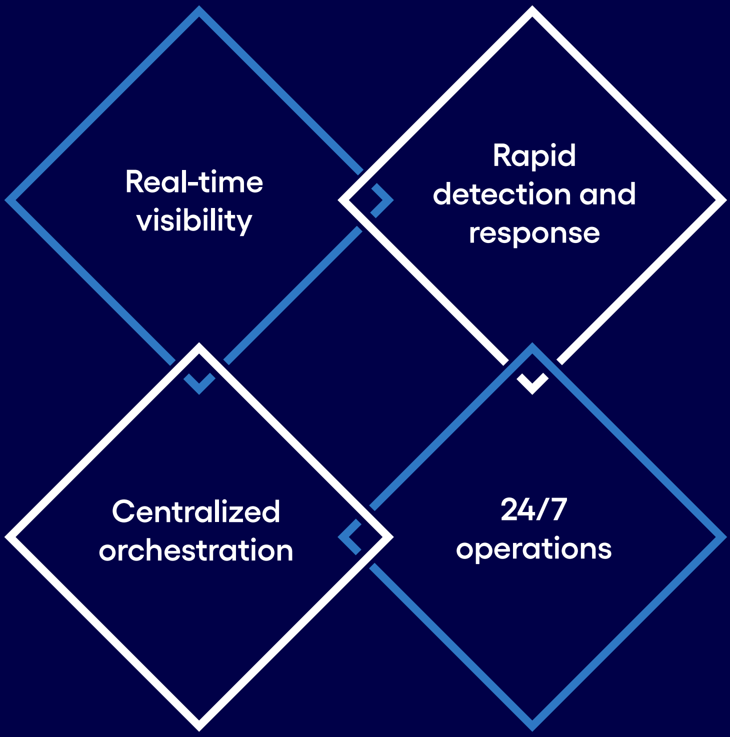
This document provides a strategic blueprint for financial services organizations aiming to build a modern, resilient and audit-ready cloud security operations model. It addresses the critical need for a framework that can scale with cloud adoption while defending against an evolving threat landscape.

Scope:

We will explore the business challenges, program objectives and technical architecture of a successful 24/7 cloud security program. This includes a detailed look at the operating model, the technology stack, measurable outcomes and key lessons learned from a real-world implementation at a large American financial services company.

The business challenge:

As the financial services company expanded its AWS footprint, it increased the complexity of maintaining consistent controls across dozens of accounts, workloads and environments. The security teams faced several critical needs:



A lack of a unified view into threats and misconfigurations across the entire cloud estate.

The need for swift detection and response capabilities that span the cloud, applications, endpoints and networks.

Difficulty in managing policies, aggregating logs and gathering evidence for frequent and rigorous audits.

The requirement for an always-on security operations model capable of handling incidents around the clock.

The solution

Cognizant deployed an AWS-native, automation-first security architecture augmented by leading marketplace solutions, delivered as an ITIL-aligned managed service. The solution was built on several core technology pillars to provide defense-in-depth.

Security domain	Core technology and purpose
Threat and posture management	AWS Security Hub, GuardDuty and Inspector were used to centralize findings and continuously monitor for threats and misconfigurations.
Vulnerability and app security	Qualys was integrated for comprehensive vulnerability management, while static application security testing (SAST) and dynamic application security testing (DAST) tools were embedded in the CI/CD pipeline to shift security left.
Web and network protection	Barracuda Web Application Firewall (WAF), intrusion detection systems (IDS) and intrusion prevention system (IPS) and a software-defined perimeter (SDP) were deployed to protect the network edge and enforce zero-trust access.
Endpoint security	CrowdStrike Endpoint Detection and Response (EDR) provided advanced threat detection and response for cloud workloads and endpoints.
Identity and access	Okta was used for enterprise federation with multi-factor authentication (MFA), AWS Cognito for application authentication and AWS Directory Service for AD integration.
Analytics and response	IBM QRadar on Cloud (QRoC) served as the central security event and incident management (SIEM) for log correlation, advanced analytics and incident response orchestration.

This hybrid model allowed the organization to leverage the deep integration of AWS-native tools while filling specific security gaps with best-of-breed third-party solutions, creating a holistic and robust defense framework.

Implementation

The program was rolled out in phases to ensure a smooth transition and continuous improvement.

Phase 1
Foundations
(0–8 weeks)

- Establish governance, logging baselines and centralized findings in AWS Security Hub
- Deploy GuardDuty and Inspector and integrate logs with the SIEM (QRoC)
- Define initial incident response runbooks and service level agreements (SLA)
- Roll out endpoint protection (CrowdStrike) and enforce MFA with Okta federation

Phase 2
Scale and automate
(2–4 months)

- Deploy and tune WAF/ IDS/IPS policies and implement the SDP for zero-trust access
- Establish a full vulnerability management lifecycle with Qualys
- Integrate SAST/DAST security gates into the CI/CD pipeline
- Automate compliance evidence collection and develop KPI dashboards

Phase 3
Foundations
(0–8 weeks)

- Conduct threat-informed defense exercises and tabletop incident response drills
- Perform cost optimization and rightsizing of security infrastructure
- Refine the managed service and expand controls to new business lines

Outcomes and business value

The program delivered significant and measurable improvements to the company's security posture and operational efficiency.

Security outcomes

- 40% improvement in incident response time and mean time to repair / resolution (MTTR) through centralized analytics and automated runbooks
- 24/7 monitoring and protection for business-critical applications and sensitive data
- Risk-based remediation that prioritizes the most critical threats first
- Hardened configurations and standardized policy enforcement across the environment

Operational and compliance benefits

- ITIL-aligned service delivery for disciplined change governance
- Streamlined regulatory audit support with automated reporting and evidence gathering
- Reduced operational toil for the security team through automation

Lessons learned

1 Shared responsibility is not shared accountability

AWS secures the cloud infrastructure, but security personnel must protect identities, data and configurations within it.

2 Identity is the perimeter

Enforce least privilege, rotate credentials frequently and mandate MFA for all privileged access.

3 Encrypt by default

All data, both at rest and in transit, must be encrypted. Prevent public S3 bucket exposure at all costs.

4 Log everything that matters

Centralize logs from CloudTrail, Virtual Private Cloud (VPC) Flow Logs and AWS Config into a SIEM for retention and analysis.

5 Automate compliance

Use tools like AWS Security Hub, Config rules and policy-as-code to enforce standards and eliminate human error.

6 Adopt zero-trust networking

Implement VPC segmentation, private subnets and restrictive egress policies. Use WAF, Shield and IDS/IPS for layered defense.

7 Prepare to respond

Develop and practice incident response runbooks that are integrated with SOC workflows.

8 Engineer for resilience

Utilize multi-availability zone (AZ) and multi-region strategies to ensure high availability and disaster recovery for regulated workloads.

9 Shift security left with DevSecOps

Embed security scanning (SAST/DAST, container scanning) and policy gates directly into CI/CD pipelines.

10 Foster a security culture

Security is more than tools; it requires strong governance, continuous training and organization-wide accountability.

Conclusion

This program demonstrates that financial institutions can successfully move beyond disparate point solutions to an integrated, AWS-native security operating model that is always on, automation-driven and audit-ready. By combining the power of native AWS services with proven marketplace tools and a disciplined managed service, organizations can achieve faster detection and response, stronger data protection and measurable improvements in cost, risk and compliance. This approach provides a clear and effective roadmap for securing cloud environments in a highly regulated industry.

Author

Spencer Pepe, Associate, Projects, AWS BG

Spencer Pepe is a cloud architect and frontend developer with a strong track record of building, optimizing and maintaining enterprise applications. He has led cloud migration initiatives that enhanced testing efficiency, reduced infrastructure costs and improved overall scalability. Spencer focuses on leveraging modern cloud technologies to drive performance optimization and support business growth.

He brings deep experience across cloud transformation, application modernization and frontend engineering, helping organizations streamline operations and accelerate innovation.

Email: Spencer.Pepe@cognizant.com

LinkedIn: linkedin.com/in/spencer-pepe-789614b6/

cognizant®

Cognizant (Nasdaq-100: CTSH) engineers modern businesses. We help our clients modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. Together, we're improving everyday life. See how at www.cognizant.com or follow us **@Cognizant.**

World Headquarters
300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233

European Headquarters
280 Bishopsgate
London
EC2M 4AG
England
Tel: +44 (01) 020 7297 7600

India Corporate Office
Siruseri-Software Technology Park of India (STPI)
SDB Block—Ground Floor North Wing
Plot No H4, SIPCOT IT Park
Chengalpattu District
Chennai 603103, Tamil Nadu
Tel: 1800 208 6999

APAC Headquarters
1 Fusionopolis Link,
Level 5 NEXUS@One-North,
North Tower Singapore 138542
Phone: + 65 6812 4000