



Global financial services firm cuts operational risk by 70% with a secure-by-design AWS platform

By embedding security into its Amazon Web Services (AWS) platform, the firm equipped its engineering teams with a safer, faster foundation for cloud innovation.

Client: A large, global financial services (FS) organization

Region: Global

Industry: Banking and capital markets

Client challenge: The company wanted to pursue a cloud-first strategy in a heavily regulated environment, but doing so meant addressing fragmented, manual security processes that were slowing down feature delivery.

Solution: Capgemini partnered with the organization to build a secure-by-design cloud platform, embedding security, compliance, and governance into the foundation. It also enabled native platform capabilities including identity, access management, encryption, and automated policy enforcement.

Benefits:

- 70% reduction in operational risk
- 60% faster remediation and patching
- 45% improvement in engineering productivity
- 20% faster incident investigations
- Improved visibility and auditability through AWS-native telemetry

To accelerate its cloud-first strategy, a global FS organization partnered with Capgemini to implement a secure-by-design cloud platform with embedded security controls and automated governance. The result was a 70% reduction in operational risk, greater operational agility, and the ability to scale securely while supporting ongoing innovation.



gettyimages
Credit: BlackJ

A cloud-first vision for security

A global FS organization runs mission-critical workloads in the public cloud, where meeting stringent security, compliance, and availability requirements is non-negotiable. As part of its ambition to launch a cloud-first strategy, it needed to deliver digital capabilities at greater speed while remaining secure and compliant.

Beyond modernizing its technology environment, the firm set out to transform security from a control function into a strategic business enabler. This vision rested on three objectives: secure use of AWS-native services, high developer velocity with built-in guardrails, and security integrated earlier in the delivery without added operational friction.

However, the organization's existing operating model was becoming a barrier to its cloud ambitions. Fragmented controls, manual processes, and inconsistent governance made it difficult to scale security across a rapidly expanding portfolio of applications and services. This made it slow to deploy new features and difficult to transform the enterprise security strategy into operational controls.

In addition, the company needed to safeguard highly sensitive financial data and manage cryptographic material at scale, including keys, certificates, and secrets. It also needed to enforce zero-trust principles across a distributed microservices architecture – without burdening its engineers with manual oversight.

Recognizing an opportunity to reposition security as an enabler, the company partnered with Capgemini. Together, they set out to develop a secure model that could support continuous delivery without compromising regulatory demands. This meant reimagining and transforming security from a control mechanism to a built-in platform capability that could support faster, more confident innovation at scale.

Designing protection as a platform capability

The transformation was guided by a single principle: embed security into the AWS platform itself rather than layering it on afterwards. This secure-by-design approach meant development teams would be able to inherit strong controls automatically – eliminating security approval delays and operational friction.

To accomplish this, the project team added identity, access, and encryption controls directly into the platform. AWS Identity and Access Management (IAM) provided role-based access, and AWS Key Management Service (KMS) centralized cryptographic control, while data was encrypted at rest and in transit by default. Centralized services – built on proprietary Capgemini tools and enterprise Public Key Infrastructure (PKI) integrations – simplified the management of secrets, certificates, and cryptographic keys across the platform.

To enable secure, cloud-native development, the teams used Kubernetes-based workload isolation and service identity across containerized and microservices architectures. Blue-green deployments supported zero-downtime releases, security controls ran as automated guardrails, and policy-as-code governance enforced compliance by default across all environments. Rather than rebuilding security for each new project, the teams defined platform patterns once and reused them – making sure every initiative starts with a secure foundation.

Throughout the transformation, the company's cloud security leadership worked closely with Capgemini's engineering teams to align strategy and execution. Wherever possible, the partners chose AWS-native services over custom tooling, which kept the platform simple to operate and easy to evolve.

Powering the next phase of innovation

Thanks to this transformation, the FS organization has reduced operational risk by around 70%. Meanwhile, automated, consistent security controls have cut remediation and patching time by 60%. The platform has maintained uninterrupted availability while supporting secure management of hundreds of credentials and certificates.

Engineering teams have already felt the difference in their day-to-day work. Predictable security guardrails have removed the friction that once slowed down releases, improving engineering productivity by 45%. AWS-native telemetry has strengthened auditability and visibility across the platform, and centralized logging with full identity traceability has accelerated incident investigations by 20%. Together, these changes have fortified the platform to operate with lower security incident rates and stronger resilience.

By embedding security into the platform rather than layering it on top, we've been able to scale confidently while enabling our teams to move faster. Security has become a true enabler of innovation, rather than a barrier."

- Client organization business leader

With a secure, AWS-powered foundation in place, the company is poised to expand into additional AWS-hosted platforms and adopt advanced, cloud-native capabilities with greater speed and control. As it keeps working toward the introduction of a fully automated, policy-driven security model, controls are no longer a source of friction: they're a foundation for growth, scale, and innovation.

About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real | www.capgemini.com

