cognizant®

# Securing the cloud

## A strategic approach to AWS security and compliance in the healthcare and life sciences industry

January 27, 2026

## Table of contents

# Securing the cloud

## A Strategic Approach to AWS Security and Compliance in the Healthcare and life sciences Industry

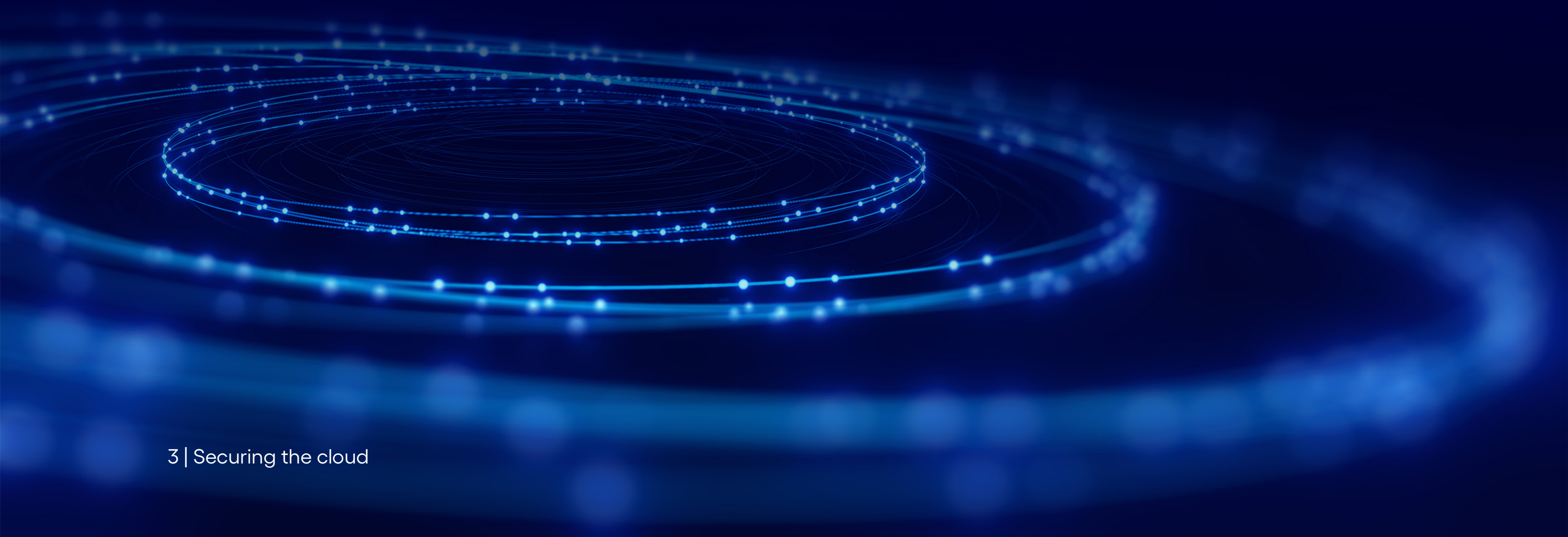
## Executive Summary

The adoption of cloud services, particularly Amazon Web Services (AWS), has accelerated within the healthcare and life sciences (HLS) sector. While the cloud offers unprecedented opportunities for innovation and scalability, it also introduces significant security and compliance challenges. This document addresses the critical need for a robust cloud security framework in an industry where data sensitivity and regulatory adherence are paramount.

The problem being explored here is the increasing complexity of managing and securing a large-scale AWS environment. Many HLS organizations struggle with configuration violations, inconsistent security controls and a lack of centralized visibility, exposing them to compliance risks and operational disruptions. These challenges are often compounded by a misunderstanding of the shared responsibility model and a failure to implement automated, preventative security measures.

Here we describe a case study of a leading HLS company that faced these exact challenges. We will detail the technical solution implemented by Cognizant, which leveraged a suite of native AWS security services to remediate over 9,000 configuration errors and establish a scalable, compliant and automated security operations framework. The solution focused on AWS Config for compliance monitoring, AWS Key Management Service (KMS) for comprehensive encryption and AWS Security Hub for centralized threat visibility, along with Lambda for automated remediation.

By exploring this real-world implementation, we offer a blueprint for HLS organizations to enhance their cloud security posture. We conclude with key lessons learned and actionable advice, providing a strategic guide for navigating the complexities of AWS security and ensuring long-term compliance and operational integrity.



# Introduction

### Purpose:

The purpose of this document is to provide a comprehensive guide for healthcare and life sciences organizations on establishing and maintaining a secure and compliant AWS environment. As the industry increasingly relies on the cloud for critical workloads, the risk of data breaches and regulatory penalties has never been higher. The aim is to demonstrate how a well-architected, automated and AWS-native security strategy can effectively mitigate these risks.

### Scope:

This perspective will cover the common security challenges faced by HLS organizations in the cloud, using a real-world case study to illustrate a successful solution. We will delve into the technical architecture, the rationale behind technology choices, the implementation process and the tangible business outcomes. The scope includes:

- An overview of the key security challenges in a multi-account AWS environment
- A detailed description of a solution leveraging native AWS security tools
- An analysis of the benefits, including compliance improvements and cost savings
- A set of actionable lessons learned to guide your own cloud security journey

# Background

The healthcare and life sciences industry is undergoing a rapid digital transformation, with cloud computing at its core. The need for scalable infrastructure to handle large datasets for research, clinical trials and patient care, coupled with the promise of advanced analytics and machine learning, has made AWS a compelling platform.

However, this migration to the cloud brings a new set of responsibilities. Under the shared responsibility model, while AWS secures the underlying infrastructure, the customer is responsible for securing everything they put in the cloud. This includes data, applications, user access and configurations. Many security incidents arise from misconfigurations at this level, such as publicly exposed S3 buckets, overly permissive identity and access management (IAM) roles or unencrypted data volumes. For HLS organizations, which handle sensitive protected health information (PHI), the stakes are particularly high, with stringent regulatory requirements like HIPAA demanding robust security and auditability.

## Key challenges

A leading HLS company was facing significant hurdles in managing the security and compliance of its expanding AWS footprint. The issues included:

**Configuration violations:** The client had accumulated thousands of configuration violations across various AWS services. These violations posed a direct risk to their compliance posture and operational integrity.

**Lack of automation:** Security processes were largely manual, leading to slow remediation times and an inability to scale security operations in line with their cloud adoption.

**Inconsistent security controls:** There was no consistent enforcement of crucial security measures like data encryption for Amazon EBS volumes and S3 buckets, or proper security group configurations.

**Limited visibility:** The company lacked a centralized view of security threats and compliance status across its multiple AWS accounts, making it difficult to identify and respond to emerging risks effectively.

**Identity and access management risks:** Challenges included managing cross-account roles, ensuring IAM policy compliance and implementing best practices like KMS key rotation.

The impact of these challenges was significant. The organization was exposed to potential data breaches, non-compliance with industry regulations and operational inefficiencies. The lack of a scalable security framework was a major impediment to their long-term cloud strategy.

## Solution

To address the client's complex security requirements, Cognizant designed and implemented a comprehensive, multi-faceted solution centered on native AWS services. This approach was chosen to ensure seamless integration, cost-effectiveness and alignment with AWS best practices.

### Multiple-solution approach and rationale

While third-party cloud security posture management (CSPM) and security information and event management (SIEM) solutions were considered, they were ultimately rejected. The rationale was as follows:

- **Cost and complexity:** Third-party tools often come with significant licensing costs and a steeper learning curve, increasing the total cost of ownership.

- **Integration gaps:** Native AWS services offer unparalleled integration. For instance, AWS Config can trigger Lambda functions for real-time, automated remediation, a capability that is often more complex to achieve with external tools.

The preferred solution, therefore, was an AWS-native architecture that provided a powerful, integrated and cost-efficient security framework.

## Technical solution details

The core components of the solution included:

| Service | Role in the solution |
|---|---|
| AWS Config | Deployed as the backbone for continuous compliance monitoring. It was used to detect configuration violations across services like EBS, S3, RDS and IAM. |
| AWS Lambda | Used to build serverless automation scripts for real-time remediation of identified configuration violations, enforce tagging policies and validate IAM policies. |
| AWS KMS | Implemented to enforce encryption at rest for EBS volumes, S3 buckets and RDS snapshots, ensuring data protection and compliance with key rotation policies. |
| AWS Security Hub | Served as a central hub for security findings, aggregating alerts from AWS Macie, Inspector and GuardDuty to provide a single pane of glass for the InfoSec team. |
| Other AWS Tools | AWS WAF was used for web application protection and Amazon Inspector for vulnerability assessments. Terraform was used for Infrastructure as Code (IaC) to ensure consistent deployment of security controls. |

This integrated solution resolved over **9,000 configuration errors** and established a scalable security operations framework. A total cost of ownership (TCO) analysis, based on the AWS Pricing Calculator, projected significant cost savings by leveraging automation and native controls, thereby reducing the need for manual remediation efforts.

## Implementation and lessons learned

The implementation of this solution provided several key insights and lessons that can serve as a guide for any organization looking to bolster its cloud security. Instead of a rigid step-by-step guide, these lessons learned offer a more strategic view of a successful implementation.

1. **The AWS Shared Responsibility Model is often misunderstood**

   A foundational step is to educate all stakeholders that AWS secures the cloud, but the customer must secure their assets in the cloud.

2. **IAM is the first line of defense**

   Enforce the principle of least privilege, mandate multi-factor authentication (MFA) for privileged users and regularly audit IAM roles and policies.

3. **End-to-end data protection is a requisite**

   Always encrypt data at rest and in transit. Use AWS KMS and enforce strict S3 bucket policies to prevent accidental data exposure.

4. **Logging and continuous monitoring are non-negotiable**

   Enable services like CloudTrail, GuardDuty and AWS Config across all accounts and centralize logs for analysis.

5. **Automate compliance and security checks**

   Use AWS Security Hub and Config rules to enforce security policies automatically. Automation reduces human error and accelerates remediation.

6. **Network segmentation and zero trust are essential**

   Implement virtual private cloud (VPC) segmentation, private subnets and tightly control inbound/outbound traffic with security groups and network access control lists (ACLs).

7. **Prepare for incident response**

   Develop runbooks for responding to security incidents in the cloud and integrate AWS security findings into your security operations center (SOC) workflows.

8. **Design for resilience**

   For critical workloads, a multi-region architecture is crucial to ensure high availability and disaster recovery.

9. **Embed security into DevOps (DevSecOps)**

   Integrate security scanning and validation into your continual innovation/continuous deployment (CI/CD) pipelines to catch issues before they reach production.

10. **Focus on culture and process**

    Security is not just about tools. It requires strong governance, ongoing training and a culture of security awareness and accountability.

## Conclusion

The case study presented here demonstrates that a secure and compliant cloud environment is not only achievable but can also be a driver of operational efficiency. By leveraging the power of native AWS security services, the HLS client was able to transform its security posture, reducing configuration errors from over 9,000 to zero in 14 months and remediating 100% of critical and high-severity violations.

The key takeaway is that a strategic, automated and integrated approach to cloud security is essential. Organizations should move away from manual, reactive processes and embrace a proactive framework built on continuous monitoring, automated remediation and centralized visibility.

## Call to Action

We encourage you to evaluate your own cloud security posture in light of the challenges and solutions discussed here. Assess your use of native security tools, the extent of your automation and the clarity of your security governance. By adopting the principles and practices outlined here, your organization can confidently innovate in the cloud while maintaining the highest standards of security and compliance.

## 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