

## Delivering cloud managed services for a global pharmaceutical company during a business transformation enabled by data and app migration

<b>CHALLENGE</b>	To stay ahead of emerging challenges and remain an industry leader, the client needed to undergo a data and app migration while struggling to develop Amazon Web Services (AWS) cyber capabilities.
<b>APPROACH</b>	Informed by client requirements, Deloitte developed a cloud managed service platform for the client provided automated security and controls, risk management frameworks, and continuous visibility and remediation of the cloud environment.
<b>OUTCOME</b>	Deloitte implemented solutions that reduced operational and infrastructure costs for the client while improving the client's ability to send and receive cases under the E2B format to help them adhere to regulations.

Our client, a global pharmaceutical company, was looking to transform their business with a cloud environment enabled by data and app migration. We worked with their executives to identify the regulatory rules, compliance requirements, and cyber risks they were exposed to and developed a solution that would help mitigate those risks.

Our discussions with them identified challenges including:

- The organization's current information technology (IT) staff lacked cloud security risk skillsets
- They had opportunities to save on cost and complexity of printing
- They needed to address their lack of a standard enterprise level architecture that is scalable and follows leading practices

- They could not draw insights from their current data sets due to their outdated toolset

Informed by client requirements, Deloitte developed a cloud managed service platform for the client provided automated security and controls, risk management frameworks, and continuous visibility and remediation of the cloud environment.

We assisted in delivering cloud managed services to them, including:

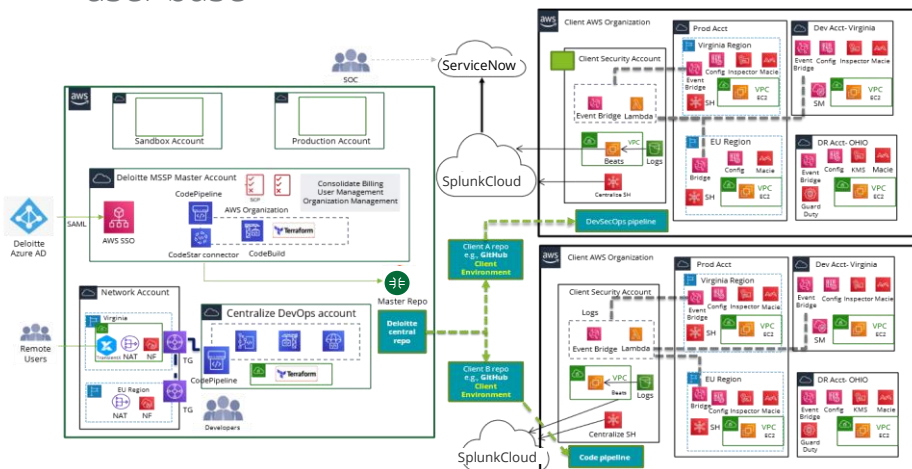
- Developed AWS native security configuration automation that supports infrastructure security for AWS workloads
- Automated secure deployment
- Automated controls resulting in less substantive testing and achieving financial regulatory compliance
- An end-to-end compliance risk management framework
- Visibility into what AWS resources are being added, changed, or removed across the organization
- Continuous monitoring and detecting of potential errors and the associated cyber risks

- Automated process and machine learning that dynamically identifies errors, financial drivers, and trends
- Around-the-clock professionals to review alerts, remediate vulnerabilities, and manage incidents
- Enhancements to their cloud security governance and compliance posture

These managed services helped the client streamline integrations and security of data workloads, uncover actionable insights from the data stored within the data lakes and security events/incidents from cyber tools, reduce their operational and infrastructure costs, and provide the capability to send and receive cases to help adhere to regulations.

## Cloud reference architecture | Cyber cloud managed services

Illustrative architecture for securely deploying AWS to support multiple enterprise applications and user base



## Scope and complexity

The project involved deploying, protecting, and managing:

- AWS EC2 instances
- AWS Firewall Manager
- Lambda
- AWS WAF
- AWS Advance SHIELD
- GuardDuty encryption keys and certificate manager
- AWS Transit Gateway
- Prisma Cloud

Cloud compliance frameworks for privacy and data protection criteria that meet standards and regulations like HIPAA, ISO 27001, SOC2, CCPA, PIPEDA, MITRE ATT&CK, CIS AWS Foundations Benchmark v1.3, CSA CCM, GDPR, HITRUST CSF V9.3, NIST-800, SOC2, ISO27001, and PCI DSS v3.

Industry compliance frameworks: Palo Alto Networks firewall, TrendMicro, Cloudstrike, Okta ASA/SSO, Prisma Compute, Nessus, Hashicorp Key vault, ServiceNow, etc.

Contact us:

**Aaron Brown**

Cyber Cloud Managed Services Leader  
 Partner | Deloitte Risk & Financial Advisory  
 Deloitte & Touche LLP  
[aaronbrown@deloitte.com](mailto:aaronbrown@deloitte.com)

**Fiona Williams**

Advisory AWS Alliance Leader  
 Partner | Deloitte Risk & Financial Advisory  
 Deloitte & Touche LLP  
[fwilliams@deloitte.com](mailto:fwilliams@deloitte.com)

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.