WHITEPAPER

Security & Compliance on Polly - Accelerating Drug Discovery Securely

Polly is a biomedical data platform for life sciences R&D that bolsters the ever-growing data management needs of pharmaceutical companies. Being a cloud platform, our users have been able to grasp several advantages of cloud adoption. Some of these include reliability, scalability, mobility, faster development & collaboration. However, storing data on cloud comes with its own concerns. Unlike in-house servers, computational resources and data storage are shared among multiple stakeholders on a cloud setup. Addressing security concerns that arise from this shared system is therefore critical.

At Elucidata, we deal with sensitive biomedical/healthcare data from various research labs and organizations. Concerns around the security of such data are generally much more, mainly because unauthorized access can result in loss of the valuable intellectual property or revealing a competitive study area. Therefore, a key focus has been given to scientific collaboration, ensuring data provenance and privacy while developing the platform. In addition, government compliance requirements, such as HIPAA (U.S Health Insurance Portability and Accountability Act) & SOC 2 are also critical to a secure cloud. This paper outlines how we deal with security, data privacy & compliances on Polly.

Data Privacy & Protection

As soon as the healthcare and life sciences industry began jumping on the digital bandwagon, data privacy and security concerns followed along. The concerns are understandable considering data in these industries carries high stakes. Data breaches can lead to serious outcomes where Intellectual property (IP) of an organization may be revealed. With AWS as our cloud provider of choice, the platform adheres to industry-standard best practices for data protection and security.

1. Virtual Private Cloud

All compute resources are housed within a VPC, providing a secure, isolated segment of the cloud meticulously configured to meet our specific networking requirements.

2. The Principle of Least Privilege

We strictly adhere to this principle across all resources and user access, ensuring minimal access rights are granted, sufficient only for necessary functions, enhancing security and reducing exposure.

3. Data Encryption

Utilizing AES 256 encryption, we secure all data at rest. In transit, data is protected with TLS encryption, safeguarding against interception and ensuring data integrity and confidentiality.

4. Database Security

Our databases are shielded by firewalls, accessible only within the VPC or by system administrators through a secure bastion host, with stringent controls on inbound traffic and SSH access.

5. Private Docker Domain

Docker images in Polly's domain are kept private, accessible solely by system administrators, with a provision for data deletion upon request.

Access Control

In the context of data breaches, companies invest significant effort in mitigating risks associated with system vulnerabilities. In doing so, they usually neglect one of the key risks in data breaches which is unwanted privileged access. It is estimated that over 70% of the enterprise breaches begin with weak and stolen credentials. Keeping that in mind, Polly has been designed by embracing Zero Trust Policy as one of its core security principles. Several safety measures have been put in place even for cases where an attacker might have access to compromised credentials.

1. Multi-factor Authentication

MFA is mandated for all administrators, significantly reducing the risk of unauthorized access through compromised credentials.

2. Access Logs

Polly offers customized access to AWS logs, enabling monitoring and auditing of resource and user activities within the production environment.

3. Encrypted Passwords

User passwords are securely salted and stored within AWS Cognito, ensuring that they remain inaccessible to any internal personnel. Encryption of secrets like STS tokens(temporary authorization tokens) is done at rest.

4. Role-based Access Control

RBAC is employed to meticulously manage access to resources and operations, aligning with the Principle of Least Privilege Access. This system facilitates the creation of teams, assignment of Polly components, and data access levels based on user roles, enhancing security and operational efficiency.

Infrastructure & Application Security

1. Health Monitoring

Polly leverages Prometheus, Sentry, Mixpanel, AWS CloudWatch to monitor it's services, with alerts configured for immediate notification of unexpected events.

2. Protection and Threat Detection -

AWS tools such as WAF, GuardDuty, and Inspector are employed for enhanced web security, threat detection, and vulnerability scanning, with all compute resources securely isolated in a VPC.

3. Security Management and Compliance -

AWS Security Hub and Config provide a unified view of the security posture and continuous compliance checks, ensuring adherence to security standards.

6. Risk Assessment

Elucidata conducts annual third-party VAPT audits, bi-annual vulnerability assessments, and risk assessments to identify and mitigate potential security risks across the organization.

Disaster Management and Recovery

Even though AWS offers an SLA agreement with >99.9999% durability, there will always be uncertainty in the case of a complete region blackout. It is not always due to unforeseen circumstances, but also due to human error, that can result in the accidental deletion of precious data. To ensure we don't lose your critical data, we have the following contingency plan in place.

1. Automated Backups

We perform daily backups for both SQL and NoSQL databases, as well as EFS Filesystems. Utilizing AWS backup services for Dynamo, RDS, EFS, EBS, and S3, located in a separate AWS location. For areas where AWS backup services are not applicable, such as Opensearch, a custom in-house support process is established. This includes 120 days point-in-time restoration, ensuring encrypted at rest data with cross-regional backup capabilities.

2. Versioning of Files

S3 file versioning is enabled to facilitate the recovery of accidentally deleted files upon request, enhancing data protection.

Compliance Standards

SOC 2

Elucidata is compliant with SOC 2 Type 2, focusing on the Security Pillar. SOC 2 is developed by the AICPA to evaluate information systems based on security, availability, processing integrity, confidentiality, and privacy. Audits are conducted annually to attest to the organization's adherence to these principles.

HIPAA

Elucidata supports HIPAA-compliant Standalone Polly Deployment, protecting "Protected Health Information" (PHI). HIPAA encompasses the Privacy Rule, Security Rule, Breach Notification Rule, and Public Safety Rule, setting national standards for patients' rights and the security of PHI.

Final Thoughts

Polly offloads the burden of security and tech, by doing major heavy-lifting with our expertise in technology, so that the organizations can focus on science and efficient drug development. This has been done by following widely acknowledged security standards & principles and getting necessary compliances. Security is something that is as important as speed and user experience of the application and should not be taken for granted. To learn more about Security on Polly, you can reach out to us at security@elucidata.io

