# How EPAM & Genosity Implemented a Next-Gen Security Solution

## EXECUTIVE SUMMARY

Genosity is a biotechnology company that provides software and laboratory services for clinical and research applications of genomics, so its partners can fully realize the value of precision medicine while improving patient care. Genosity offers a software-as-a-service (SaaS) product, Integrated Genomics Toolkit (IGT), which is a comprehensive solution enabling genomic laboratories to generate and leverage next-generation sequencing (NGS) data for clinical genetic testing as well as meaningful analytics for research collaborations. Genosity and EPAM worked together to ensure that IGT is deployed in Amazon Web Services (AWS) with the right infrastructure to meet the regulatory standards required of healthcare entities dealing with patient data.

## CUSTOMER CHALLENGE

With increasing regulations around data management and the possibility of cyber threats, healthcare institutions constantly face new challenges around the secure retention of large-scale data with Protected Health Information (PHI). As a cloud-based SaaS provider to NGS laboratories, Genosity's products need to comply with a myriad of data security regulations including the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). IGT is an end-to-end platform deployed in AWS under stringent security policies that are constantly monitored by EPAM and Genosity.

## WHY AWS

Genosity's products are built for high-throughput, next-generation sequencing laboratories, that put high demands on infrastructure, compute and storage resources. Key requirements are scalability, confidentiality, privacy, security, availability, process integrity, ability to run complex bioinformatic pipelines, IGT is a fully backed up solution with disaster recovery, and compliance with regulations. Confidence in an infrastructure partner is crucial for Genosity in growing its own business and maintaining its customers' trust. AWS satisfies all the requirements and was identified as the cloud partner of choice.

## WHY THE CUSTOMER CHOSE THE PARTNER

Since 2017, EPAM has partnered with Genosity for the design and development of the IGT product portfolio. For such a complex product line with strict regulatory requirements, any vendor needs to have wide cloud security competencies and capabilities to answer modern security challenges. To that end, EPAM has a Cloud & DevTestSecOps Practice with more than 1,300 engineers, architects and consultants. Security services, provided in conjunction with the EPAM Security Competency Center, is the key offering of the practice.

## PRIMARY AWS SERVICES USED:

IAM, S3, EC2, CloudTrail, ELB, VPC, CMK, RDS

## 3RD-PARTY APPLICATIONS OR SOLUTIONS USED:

Github, Kubernetes (kops), Docker, Prisma Cloud

## RESULTS AND BENEFITS

EPAM provided Genosity an infrastructure meeting HIPAA requirements with security findings remediations. This implementation ensured that Genosity could maintain the regulatory standards required for the security of PHI handled by Genosity and its clients.

Project highlights include:

- Fast turnaround for security assessment
- Ability to perform assessment and provide applicable and actionable recommendations at the late stage of development
- EPAM-developed security best practices

# How EPAM & Genosity Implemented a Next-Gen Security Solution

## PARTNER SOLUTION

The security solution for Genosity included two parts: Ensuring the full alignment of customer security controls with HIPAA requirements and transitioning to a higher security maturity level.

The preparation for HIPAA compliance included manual and automatic security assessments. During the assessments, EPAM engineers used AWS-native, commercial and open-source tools. The assessment scope included access, data integrity, encryption, authentication and audit controls. The assessments resulted in extensive reports with detailed recommendations that were tailored to the customer's infrastructure specifics. Together with the infrastructure team, security engineers conducted remediations and offered the support needed for all changes.

The second part of the project included a thorough analysis of Genosity's cloud and Kubernetes cluster infrastructure. As a baseline, the EPAM-developed security assessment framework was used. The framework is based on the EPAM practice and knowledge from previous security-related projects, best industrial security practice (CIS, NIST), and EPAM's recommendations. As a result of the analysis, EPAM's security team prepared comprehensive security reports with detailed findings and recommendations. According to the set maturity level, the findings were remediated in cloud and cluster.

## ABOUT GENOSITY

Genosity is a biotechnology company focused on providing software and laboratory services to biopharma, biotech companies and health systems.

The core business area is providing and implementing a SaaS technology platform that addresses both somatic and germline clinical applications of genomics and offers data analytics solutions to enable research collaborations at health systems. Genosity is developing resources for precision medicine initiatives through a high-throughput laboratory, which meets strict regulatory standards and provides multiomics services to meet the clinical research needs of its biopharma and biotech partners.

## ABOUT EPAM

As an AWS Advanced Consulting Partner, EPAM works with its global customers to design, migrate, build and support sophisticated cloud applications on AWS with increased flexibility, scalability and reliability. As of 2020, EPAM had over 2,000 AWS engineers, 207 AWS certified professionals and 1,251 AWS business and technical accreditations and has delivered over 300 projects running on AWS.

**CONTACT US AT SALES@EPAM.COM OR LEARN MORE AT WWW.EPAM.COM.**