Secure Flow Cytometry Data Analysis with terraFlow

Extract actionable findings with trusted security and compliance.

Security Benefits of terraFlow

terraFlow securely accelerates biological insights and biomarker discovery. By combining advanced automation and analytics with decades of immunology expertise, its cloud native platform delivers fully automated flow cytometry and CyTOF data analysis.

- **Purpose-built for research data**
  terraFlow analyzes standard FCS files and sample population labels — such as time point, dose and treatment group — without requiring any proprietary or patient-identifying information, delivering population-level statistics designed exclusively for early-stage R&D.
- **End-to-end data protection**
  Encryption safeguards data in transit and at rest — across a cloud infrastructure designed for regulatory compliance and research confidentiality requirements — so researchers can focus on discovery without data risk.
- **Complete data ownership**
  Users can delete their own data as needed, and administrators can delete data across the entire organization. terraFlow never mines user data and deletes all data after two years (unless regulations require otherwise). Deleted datasets are immediately removed from all resources.
- **Operational resilience**
  Automated threat detection, continuous monitoring and robust disaster recovery protocols help ensure uninterrupted access to data and workflows, supporting fast, reliable analysis.
- **Precise controls**
  Role-based permissions, least privilege principles and authentication via Amazon Cognito or single sign-on restrict sensitive data and critical operations to approved users only, preserving research integrity. Administrators can add or remove users and delete user datasets as needed.
- **A transparent partnership**
  Detailed security documentation, best practices guides, robust SLAs and access to dedicated advisory services support seamless integration with your organization's security posture.

How terraFlow's Security Works

terraFlow combines industry-leading cloud infrastructure, intelligent automation and rigorous access controls to protect your research at every stage.

Secure Architecture and Infrastructure

- **Hosted on Amazon Web Services with multi-layered security**
  Built-in capabilities including AWS Shield for DDoS protection, Amazon Virtual Private Cloud for network isolation and AWS Identity and Access Management create a secure foundation for sensitive biomedical data.
- **Data encryption enforced in transit & at rest**
  The platform uses TLS 1.3 to secure data transmissions and AES-256 to protect data across all storage types, including Amazon S3 buckets

and Elastic Block Storage Volumes. AWS Key Management Service provides secure, auditable key handling that aligns with industry best practices.

- **Compliance and auditing**
  The control environment is SOC 2 Type 2-certified. Annual third-party audits and penetration tests ensure the continued security, availability and confidentiality of regulated data.

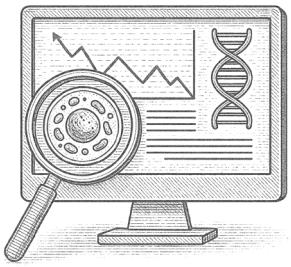
Intelligent Automation

- **Continuous, automated monitoring and protection**
  Multiple technologies work together to stop threats before they affect research work. Amazon Inspector automatically assesses security posture, while AWS Config monitors configuration changes for compliance with security best practices. AWS GuardDuty conducts additional monitoring for malicious or unauthorized activity. And enterprise-grade endpoint protection solutions further detect and neutralize risks.
- **Business continuity and disaster recovery**
  Risk management and incident response protocols combine with comprehensive BC/DR strategies to minimize downtime. Amazon CloudWatch helps terraFlow's incident response team quickly identify and address disruptions. In the event of an incident, data replication across multiple geographic locations within AWS improves availability and accelerates recovery.

Access Management and Change Control

- **Granular policies for maximum control**
  Role-based access controls and IAM policies enforce the principle of least privilege throughout the platform, protecting against unauthorized access.
- **Thorough, secure change management**
  Segregated development and staging environments allow for rigorous testing before promoting changes to production.
- **Secure software development lifecycle**
  The platform's DevSecOps model integrates security at every phase. Mandatory code reviews, static and dynamic code analysis, and automated security testing reduce vulnerabilities and enhance software quality.

terraFlow provides flow cytometry data analysis while meeting the industry's strictest security standards, with a commitment to continuous improvement. Customization options for enterprise users include the ability to deploy on-premises.



Ready to start innovating with confidence? Get in touch with us.

Dan Freeman, CTO
dan@terraflow.app

or schedule a call at
terraflow.app/learnmore