10x Genomics Security Overview

Introduction

At 10x Genomics, we empower groundbreaking scientific research to unlock the secrets of biology to improve human health through our tools and technologies.

In this document, we present our proactive approach to information security, covering both our innovative products and our comprehensive organizational practices.

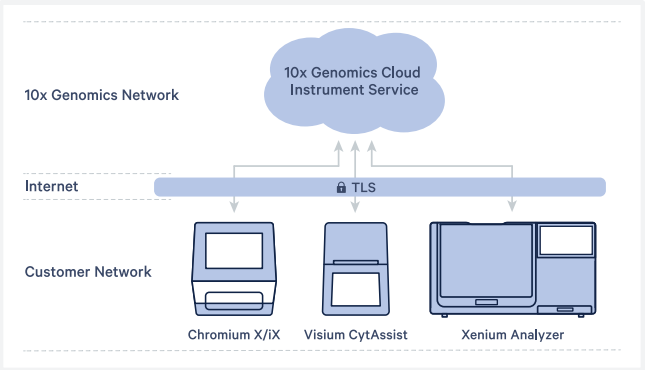
Product Security

The products in scope for this paper are:

- 10x Genomics Cloud Instrument Service platform for monitoring instruments
- Chromium X/iX instrument for single cell analysis
- Visium CytAssist instrument for spatial analysis
- Xenium Analyzer instrument for in situ analysis
- 10x Genomics Cloud Analysis (SaaS) platform for genomic analysis

10x Genomics Cloud Instrument Service

The 10x Genomics Cloud Instrument Service is a central component in the product ecosystem designed to securely monitor the performance of instruments to verify they operate effectively and to empower our support teams to respond quickly to troubleshoot any issues that may occur.



The following summary highlights the multi-tiered security architecture of the 10x Genomics Cloud Instrument Service:

- Leverage the comprehensive and mature cloud security technologies of Amazon Web Services (AWS).
- Prevent unauthorized access to information and equipment through data, system, and physical access management.
- Segregate data within a multi-tenant architecture through application-level access controls.
- De-identify personal data through pseudonymization.
- Encrypt data in transit following industry-standard protocols such as SSL/TLS and 128-bit or higher AES encryption.
- Log access attempts to administration and infrastructure systems.
- Protect against data destruction or loss through offsite backups in separate geographic regions.
- Conduct regular internal and independent assessments, including penetration tests.
- Monitor suspicious activities and deviations from security policies.

The 10x Genomics Cloud Instrument Service's security infrastructure reflects our dedication to safely advancing research while earning your trust in our data protection and privacy measures.

10x Genomics Instruments

The Chromium X/iX, Visium CytAssist, and Xenium Analyzer platforms generate large amounts of data and implement advanced security measures to transmit a subset of this data to 10x Genomics Cloud Instrument Service.

The table and links below describe the security considerations of each instrument.

Security Feature	Chromium X/iX	Visium CytAssist	Xenium Analyzer
Network Connectivity Tech Note	CG000508	CG000653	CG000645
Data collected by the instrument and sent to 10x Genomics	Calibration data, instrument operation logs, mechanical and fluidic system logs, computer system logs	Calibration data, instrument operation logs, optical, mechanical and fluidic system logs, computer system logs	Calibration data, instrument operation logs, mechanical and fluidic system logs, computer system logs
Data not collected	Biological sample data, personal health information	Biological sample data, personal health information Note that 10x Genomics may receive some biological sample data (such as sample images) if the user exports a support bundle for assistance. Such data is used only for support purposes.	Biological sample data, personal health information Analysis and sample data processing is done locally on instrument. Note that 10x Genomics may receive some biological sample data (such as sample images) if the user exports a support bundle for assistance. Such data is used only for support purposes.
Required inbound ports	No open inbound ports required	No open inbound ports required	No open inbound ports required
Data center encryption at rest	Encrypted at rest with AES-256	Encrypted at rest with AES-256	Encrypted at rest with AES-256
Data encryption in transit	Encrypted with TLS	Encrypted with TLS	Encrypted with TLS
Access limitations	(Remote live support not available)	(Remote live support not available)	Live support can be disabled on instrument at any time
Instrument firewall	Blocks all inbound connections	Blocks all inbound connections	Blocks all inbound connections
On instrument restrictions	No installed browser, user account runs with restricted permissions	No installed browser, user account runs with restricted permissions	No installed browser, user account runs with restricted permissions
Operating System	Linux-based OS	Linux-based OS	Linux-based OS
Updates & Patches	Provided by 10x Genomics directly to the instrument	Provided by 10x Genomics directly to the instrument	Provided by 10x Genomics through the Xenium application on the instrument

Table 1. Security considerations by instrument.

10x Genomics Cloud Analysis (SaaS)

The 10x Genomics Cloud Analysis (SaaS) platform offers powerful, scalable analysis solutions designed to accelerate genomic research. It provides users with advanced tools for processing and analyzing large genomic datasets, leveraging our cloud's computational power to deliver fast, reliable results so you can focus on discovery and innovation without the constraints of local compute resources. Importantly, it incorporates the same security measures as the 10x Genomics Cloud Instrument Service. We start analyzing your experimental data only after you subscribe to the service and explicitly agree, thus protecting your data's privacy and placing it under your control.

Enterprise Security

10x Genomics implements a comprehensive suite of industry-standard enterprise security practices, ensuring the protection and resilience of data and systems against evolving cyber risks. The practices detailed in the following sections are fundamental to the company's commitment to being worthy of your trust.

Information Security Program

The 10x Genomics information security program aligns its practices with CIS Critical Security Controls and is maintained by in-house professionals and external managed service providers. A description of each security team is provided below:

Enterprise Security Program

- Monitor and safeguard the overall security of our organizational infrastructure.
- Manage access controls, identity verification, and protect against cyber threats.
- Respond to and mitigate security incidents within the enterprise environment.

Product Security Team

- Build security into our software products throughout the development lifecycle.
- Conduct security assessments, code reviews, and implements secure coding practices.
- Address vulnerabilities and enable products to meet industry security standards.

Cloud Security Team

- Secure our cloud infrastructure and services.
- Implement and manage cloud security controls and configurations.
- Monitor and respond to security incidents within the cloud environment.

Governance, Risk, and Compliance Team

- Establish and enforce our security policies, standards, and procedures.
- Manage risk assessments and monitor compliance with relevant regulations.
- Coordinate with internal teams to align security practices with governance requirements.

Security Awareness and Training

The security training and awareness program equips our workforce with the knowledge and skills necessary to recognize and effectively respond to potential security threats. Through regular, comprehensive training sessions and ongoing awareness campaigns, personnel are not only aware of the latest cybersecurity practices but also understand their role in maintaining the company's security posture.

Authentication and Access Controls

10x Genomics enforces strict access controls to internal systems. Personnel are required to authenticate through a single-sign-on system using multi-factor authentication. Adhering to the principle of least privilege, access requests to systems are documented, reviewed, and approved by the relevant managers and service owners. We routinely review and assess personnel access to infrastructure and revoke access if it is no longer necessary for the performance of specific work tasks.

Infrastructure Security

Our asset management program uses solutions such as Mobile Device Management (MDM) and IT Asset Management (ITAM) to inventory, monitor and control hardware and software components deployed throughout the organization. Assets are categorized based on their function, business sensitivity, and importance to our operations.

We employ comprehensive measures to protect endpoints, servers, and networks through:

- Encryption protocols to safeguard data in transit and at rest.
- Advanced firewalls to control and regulate network traffic and prevent unauthorized access.
- Intrusion detection/prevention systems (IDS/IPS) to scan for and prevent malicious activity.
- Endpoint detection and response (EDR) tools to identify, investigate, and respond to cybersecurity threats.

Security Monitoring

We use a comprehensive suite of tools and processes to detect and counteract malicious, suspicious, or unauthorized activities within our infrastructure, services, and products. Our Security Information and Event Management (SIEM) solution logs and archives instances of administrative access, usage of privileged accounts, changes to configurations, and errors or failures on systems critical to 10x Genomics' operations. Where feasible, we automate log analysis to facilitate prompt identification of potential security concerns to relevant personnel. Access to these audit logs is stringently controlled and limited to authorized staff whose roles necessitate such access.

Vulnerability and Patch Management

The vulnerability and patch management program scans for and identifies vulnerabilities in our systems and applications. We install timely patches and updates to mitigate potential risks and fortify ourselves against the latest security threats. Beyond regular scans and updates, we engage in proactive threat analysis by performing security audits across the organization.

Secure Software Development

At 10x Genomics, building security into our software development lifecycle ensures the integrity and safety of our solutions. Each development stage, from initial design to final deployment, undergoes security testing and validation, including collaborative peer code reviews through our code version control system. We also maintain and regularly communicate guidelines, for example the OWASP Top 10, for secure software development and testing to staff.

Incident Management

10x Genomics has established incident management procedures to effectively minimize downtime, service degradation, and security risks. Security incidents are identified and reported through predefined channels to our security team who then promptly classifies these incidents, assesses their severity, and initiates an appropriate response in alignment with our service-level agreements (SLAs). For incidents potentially impacting privacy, additional analysis and response actions are undertaken with our legal team. We regularly conduct exercises to simulate potential security incidents, preparing our team and refining our procedures to address real-world situations effectively.

Vendor Risk Management

Our third-party risk management program, staffed by subject matter experts from across the company, rigorously reviews specialized vendors to confirm their security posture aligns with our high standards before onboarding their services. The evaluation process includes continuous monitoring and reassessment of vendor security practices to verify alignment with our technical and business requirements.

Data Privacy and Protection

10x Genomics prioritizes data privacy and protection, adhering to policies that classify and manage customers' personal data with integrity and security. Our Privacy Policy spells out the details of our data collection, processing, and retention practices, emphasizing the lawful and safe handling of personal data in compliance with GDPR, CCPA and other privacy laws and regulations. We actively conduct regular reviews of our practices and product offerings to stay in sync with evolving legal and regulatory standards.

Summary

At 10x Genomics, we understand the paramount importance of security for our customers and partners and we embrace the responsibility of safeguarding your data. For any inquiries or concerns regarding our security measures, please feel free to reach out to our support or sales team. We are committed to providing transparency and support on all aspects of our security practices.

Definitions

The term "customer data" is any data, information, or materials submitted by a customer to 10x Genomics Cloud services and including any results, analysis, data, or other information generated by 10x Genomics Cloud in the performance of services on behalf of the customer.

Document Revision Summary

Document Number	CG000753
Title	10x Genomics Security Overview
Revision	Rev A
Revision Date	March 2024

Specific Changes:

N/A

General Changes:

N/A

Contact:
support@10xgenomics.com
10x Genomics
6230 Stoneridge Mall Road
Pleasanton, CA 94588 USA