Aptean GenomeQuest

Focus on Security

aptean

Product Documentation

www.aptean.com

Security is essential to Aptean and GQ Life Sciences. Read about the measures we take to protect your data in our systems and our facilities.

Data Center

Aptean hosts its GenomeQuest service at one of the largest data center facilities in the world – QTS Metro Data Center in Atlanta, Georgia. This facility maintains SOC 1, SOC 2, SOC 2-HIPAA, PCI, ISO 27001, FISMA, and HITRUST compliance certifications. GenomeQuest servers are secured in QTS' carrier grade hardened facility with enhanced levels of protection, providing a fully redundant IP and MPLS fiber-optic backbone to 19 major carrier networks. These carrier backbones were specifically designed for high reliability, high speed, and efficient routing with low latency.

An on-site power substation with four redundant protected feeds from diverse entry points ensures the highest levels of operational availability. The data center utilizes a double, pre-action dry pipe fire suppression system and a state-of-the-art smoke, water, electrical (EPMS) monitoring and alerting system. Redundant hydro feeds are backed up by UPS/battery failover and generators utilizing gravity feed fuel reservoirs. Fuel delivery priority is contracted secondary only to emergency services in the event of an extended outage.

Layered, End-to-End Security Architecture

Aptean safeguards boast a comprehensive, end-to-end defensive architecture that addresses security at every layer, from the application to the servers and the physical wire.

Physical Security

The data center's physical security is comprised of several elements including multi-factor authentication utilizing biometric scanners (fingerprint and retinal) in conjunction with access card mechanisms. CCTV security cameras monitor and record throughout the facility. Access to the data center, its servers, and networking equipment is restricted to the minimum number of Aptean personnel and continually tracked.

Data Backup

In order to ensure the confidentiality, integrity and availability of customer data, GQ Life Sciences performs incremental backups on a daily basis and full backups weekly. We can restore a customer's data daily up to one week prior to a requested restore and weekly for up to three months prior to a requested restore. Backups are replicated automatically to an alternate QTS data center in Dallas/Fort Worth Texas, well beyond any standard disaster containment region.

Disaster Recovery

Aptean utilizes a secondary redundant hosting facility which houses our DR back-up infrastructure. This DR capability provides our customers with a secure and redundant hosting solution essential to an enterprise class platform.

Security features include:

Perimeter Security (Firewalls) and Intrusion Detection

Sound firewall policies are at the root of any secure environment. Restricting both ingress and egress ports to only the required services helps to minimize the overall digital footprint of the environment. Aptean utilizes next generation firewall systems which incorporate Intrusion Detection and Prevention. Additionally, Aptean utilizes enterprise grade artificial intelligence network monitoring to gain insights into wire traffic which would otherwise go unnoticed.

The most current levels of TLS encryption are implemented to ensure our customers' data remains secure from prying eyes. Systems are monitored 24x7x365 to detect any suspicious usage and/or access patterns so that an attack can be detected and mitigated as quickly as possible.

Aptean employs various malicious code protection mechanisms at critical information system entry and exit points to detect, block, and eradicate malicious code. Protection software is updated to include new releases in accordance with Aptean's policies and procedures. Aptean and multiple third-party partners perform regular audits and vulnerability scans of the hosted environments.

Operating System Hardening

Aptean completes systems hardening for all production environments. This ensures the minimum number of services and software are installed on all systems to lower the digital footprint and number of potential avenues of attack. Aptean's security team regularly monitors RSS feeds, subscribes to industry publications, distributions and threat alerts to ensure the highest levels of protection are maintained for our environments. These precautions make it more difficult for intruders to gain a foothold on our systems.

Access Control and Privacy/Confidentiality (Encryption)

The GenomeQuest hosted service is comprised of a layered security approach for all customers. Users are granted access to the system via protected web browser session using TLS 1.2 and 256-bit encryption. Users are required to authenticate to the system at all times. GenomeQuest passwords are stored as SHA256-encrypted salted and hashed strings to make them indecipherable. During transit over the Internet, all data in the GenomeQuest system is protected by TLS 1.2 encryption, which is currently the most secure industry supported cryptographic protocol.

Once authenticated, the user has access only to capabilities, information, or specific data based on their individually defined security profiles. Customers access Aptean's GenomeQuest servers strictly through a web interface. GenomeQuest utilizes a multi resident approach to customer data which stores data on the same disk array but segregates that data in isolated subdirectories associated with the user's profile. Customer data is further insulated by individual accounting groups within the GenomeQuest environment. There is no web-based mechanism to share information among accounting groups.

Directory names are obfuscated through a hashing mechanism, eliminating any identifying information about either the user or organization owning the data. Only GenomeQuest administrators have the ability to decode the hash. Administration access to our systems is limited to the minimum number of Aptean personnel and is continually audited.

Corporate Security Policy/Logging/Auditing

Logging and auditing provide information about use characteristics (including username, time of login and logout, commands, areas accessed, etc.) on each system. GQ Life Sciences monitors this information and stores it for forensic purposes in the event of suspected incidents or breaches and for customer investigation as required.

Aptean's comprehensive corporate security processes and procedures protect systems, employee and customer information, data, and assets. Our Corporate Information Technology Department maintains a SOC 2, Type 1 compliance certification (Type 2 subject to completion of evidence collection).

Security is at the heart of both Aptean and GQ Life Sciences Inc., as part of the larger Aptean family. We understand the level of trust required to allow us to host your data, and we will continue to work hard to earn your confidence in our security measures.

For more information, contact your account manager or email us at **info@aptean.com**.

Aptean Headquarters
4325 Alexander Drive
Suite 100
Alpharetta, GA 30022-3740
+1 (770) 351-9600

info@aptean.com