Cloud security

Secure diagram software

Overview

Over 100,000 customers trust Gliffy with their data. We include both enterprise-class security features with extensive audits of our applications, systems, and networks to ensure your business data is protected. Our clients are assured their information is safe, secure, and their businesses are protected.

Security Features

Data encryption

Gliffy ensures confidentiality with all user connections to our service. This includes:

- Data inflight uses 256-bit encrypted connection to the Gliffy environment via TLS 1.2
- Data at rest encryption to protect the integrity of all data persisted by the application
- Cryptographic keys, protected by a pair of passphrases stored in separate environments

Network protection

Gliffy provides rigorous access controls. These include:

- Network layer (IP) and transport layer (TCP) firewalls
- Virtual Private Cloud (VPC), multiple AZ and Regions
- Access Control LIsts (ACL) protect user data by limiting employee access

Gliffy's network is built using Amazon's secure Virtual Private Cloud (VPC) technology, adding an extra layer of protection against intrusion.

Recovery and backups

All gliffy documents a copied to multiple availability zones on write, reducing the risk associated with data loss from providers that only backup hourly.

Uptime

We monitor our reliability utilizing industry-leading products such as New Relic.

- Since January 2017, Gliffy has maintained an average uptime of 99.8% and Apdex of 0.99
- This ensures the constant availability of our services, 24 hours a day, 7 days a week, 365 days a year

Secure data centers

We partnered with AWS to provide our web and data services because of their stringent security measures, which include compliance with the following certifications and third-party attestations:

- U.S. General Services Administration FISMA-Moderate level operation authorization
- ISO 27001 certification
- SAS70 Type II audits
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)

Password authentication

Gliffy supports sign-on with a unique username and password, or single sign-on with Google/Facebook/Microsoft Live/Yahoo and industry leading Identity Providers.

- User passwords are never transmitted in plain text
- Only salted one-way hashes of passwords are stored by our servers—never the passwords themselves
- Individual user identity is authenticated and re-verified with each transaction, using a unique token created at login

Permission controls

Gliffy follows security best practices by using least privilege access principles to protect your data. Role-Based security can define by an administrator and privileges such as:

- Add/Edit/Delete/Public/Private can be set on any level including:
    - Teams, Members, Groups, Account, Files, Folders and Shapes

- Administrators may also limit functionality within a single organization, system, or by group or user type

Data ownership

Gliffy asserts no ownership over any diagrams and documents created through our services. Users retain:

- Copyright and any other rights
- All intellectual property rights, on created documents and included content

We respect your privacy and will never make your diagrams and documents available publically on a paid plan without your permission.

Constant monitoring

Gliffy performs regular internal security reviews and contracts with third-party penetration experts to test for application vulnerability threats and network vulnerability threats:

- Quarterly tests take place with leading automated tools
- Extensive manual testing also takes place for quality assurance
- Testing covers OWASP top-10 threats and WASC 26 classification sections
- Live systems are constantly monitored