Qdrant Security Policy

We understand how critical data protection is, and we take the security of Qdrant code, software, and cloud platform very seriously. If you believe you have found a security vulnerability in Qdrant, we encourage you to let us know immediately. We will investigate all legitimate reports and do our best to fix the problem fast.

Need to report a vulnerability?

We would like to keep Qdrant safe and secure for everyone. Please report any issues or vulnerabilities to security@qdrant.com instead of posting a public issue on GitHub. If you have discovered a security vulnerability, we would greatly appreciate your help in disclosing it to us responsibly. Publicly disclosing a vulnerability can put the entire Qdrant community at risk.

When submitting a security vulnerability, please include the Qdrant version and details on how the vulnerability can be exploited. We will work with you to assess and understand the scope of the issue and fully address any concerns. Any emails are immediately sent to our engineering staff to ensure that issues are addressed rapidly. Any security emails are treated with the highest priority, as the safety and security of our service are our primary concerns.

Physical security

Qdrant Cloud services are hosted on Google Cloud Computing and Amazon Web Services, and Azure. The data centers are staffed 24x7x365 by security guards, and access is authorized strictly on a least privileged basis.

The cloud hosting providers are certified with the ISO 9001:2008, ISO 27001:2013, ISO 27017:2015, and ISO 27018:2014 security standards - global standards that outline the requirements for information security management systems. This requires that the hosting provider must systematically evaluate its information security risks, taking into account the impact of company threats and vulnerabilities; must design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks; and adopt an overarching management process to ensure that the information security controls meet the information security needs on an ongoing basis. In addition, all hosting providers are certified at PCI DSS Level 1, which means that the application is run on the PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud.

Perimeter security

Access to perimeter devices, servers, and network hardware is permitted only from defined IP addresses over secure private and public key authentication mechanisms with encryption. Access to all servers is secured using automatically-rotating private and public key pairs. All data is encrypted when in transit, preventing man-in-the-middle attacks and data snatching.

All servers are tested for vulnerability and intrusion detection quarterly. The servers and services hosted on them are certified as complying with the PCI Data Security Standard established by the PCI Security Standards Council, which is an open global forum for the development, enhancement, storage, dissemination, and implementation of security standards for account data protection. The certification confirms that the services adhere to the PCI DSS Level 4 requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.

Network security

The system is designed with scalability and redundancy in mind. Web load balancers and database servers are distributed globally across geographically dispersed data centers in different operating regions.

Each database server has its own firewall configuration based on its role within the Qdrant Cloud platform, and only the necessary ports are opened on each server. All outbound connections pass through the stateless access control rules, whilst inbound connections from the internet must pass through a secure, highly-available load balancer layer, and the stateless access control firewall rules before then being routed to each server.

Software security

We take the security of the Qdrant code very seriously. The database is built using the Rust language - a static multi-paradigm, memory-efficient, low-level programming language focused on speed, security, and performance. The intention is to build Qdrant with as few moving parts as possible, thereby keeping the attack vector as low as possible.

Email security

Qdrant supports TLS encryption on all inbound and outbound emails. Qdrant uses Gmail to provide email and communication services. For an explanation of how email encryption works, take a look at this overview from Google.

Data residency

On Qdrant Cloud, the location of data can be specified. Locations may include London, Ireland, Belgium, Germany, Switzerland, North America, South America, Australia, Canada, Tokyo, or Singapore. Data will not be moved or replicated outside of a specified location.

Data in transit

All data is encrypted when it is being transmitted between client devices and Qdrant Cloud. SSL/TLS certificates shield data using 256-byte signatures and either 2048-bit or 4096-bit keys. All connections to Content Delivery Network (CDN) servers and the database layer are secured using TLSv1.3. All TLS/SSL keys for client-to-server communication are changed annually.

Data at rest

When at rest, all files are encrypted at multiple different levels. Auth tokens are stored using pbkdf2, bcrypt, scrypt, or argon2 hashing algorithms.

Data backup

All data is historically stored at the database level, allowing for access and querying of data and changes made at any time. Full-snapshot backups of the Qdrant Cloud platform (both current and historical) are performed nightly, and backup data is stored offsite in an encrypted format using the 256-bit Advanced Encryption Standard (AES-256).

Authentication

All services access is authenticated using JSON Web Tokens (JWT) digitally signed using the HMAC SHA512 or RSA SHA512 hashing algorithms. All highly-sensitive data, such as passwords, are stored using a one-way encryption technique.

Security incidents

Security incidents and downtime incidents are reported to an online status page as soon as incident information is available.

Contact us

Have a question, concern, or comment about Qdrant security? Please contact Qdrant Support. security@qdrant.com