Altinity's Commitment to Security

Security is critical to our customers, and we take everything about the subject very seriously. This page summarizes the policies and investments we undertake related to security, as well as our commitments to customers and the broader community of ClickHouse users.

Security policies are improved regularly and we will update this page as major changes occur. If you have additional questions please contact us at info@altinity.com.

Reporting a Security Problem

If you would like to communicate a security issue to us, please send email immediately to security@altinity.com. We ask that any reports adhere to our Responsible Disclosure Policy.

Security Compliance Standards

Altinity is currently undergoing audit for SOC 2 Type 1, a stringent standard that assesses the quality, scope, and maturity of the security controls that are in place at the company carrying the certification. We expect to complete certification in Q1 2021. We plan to continue immediately to SOC 2 Type 2 certification.

Altinity is committed to meeting additional compliance standards needed by customers. Please contact us to discuss your requirements.

General Policies

Personnel Training and Protection

Security starts with people. Altinity has implemented the following procedures to ensure protection of user data.

- Altinity has written policies for all aspects of security management from acceptable use to vulnerability management.
- Employees receive training in security policies as well as standard security measures to prevent hacking of accounts through Phishing, social engineering, and the like.
- Employee laptops run auditing software that reports compliance with required policies such as disk encryption.
- Employees are regularly briefed on policies to ensure protection of customer data.

Access Controls

Altinity implements strict authentication and authorization protocols for access to all services.

- Employee authentication to services is controlled through industry-standard single sign-on for major services, email, and cloud systems.
- SSO access is supplemented with two factor authentication.
- Access to cloud environments is granted through temporary credentials. We do not use stored passwords or access keys.
- Altinity employees use a password manager that avoids written passwords.
- Employee accounts are deactivated efficiently upon departure from Altinity.

Altinity.Cloud Policies

Altinity.Cloud offers a managed service for Clickhouse. The following industry standard policies protect the data of customers on the service.

- Access to production Altinity.Cloud resources is restricted to members of the core engineering team responsible for operation of the site.
- Connections to all service public endpoints are protected by TLS encryption with valid X509 certificates.
- Customer data at rest including database storage and backups are protected by encryption. Customers may choose the level of protection required.
- Tenant environments are fully isolated from each other and use separate compute, storage, and networking resources.
- The management plane encrypts sensitive metadata within the application.
- All cloud systems have intrusion detection and monitoring software installed.
- All production and staging environments are under strict configuration control with automated creation of tenant environments as well as software deployment.
- New releases of the Altinity.Cloud service undergo extensive QA including tests for security prior to deployment.

Cloud service security is complex. Please contact us for further details if your business requires a deeper understanding of protection mechanisms.

ClickHouse Software and Services

ClickHouse Server and Ecosystem Projects

Altinity is a major committer to ClickHouse. We focus on enterprise features including security, where we actively seek out opportunities to enhance ClickHouse security.

- Altinity implemented and tested log cleaning regex expressions, which prevent leaks of sensitive data into system logs.
- Altinity implemented and tested AES encryption functions for column data. We are actively involved in general verification of encryption capabilities in the ClickHouse server.

- Altinity implemented the entire functional test suite of Role-Based Access Control (RBAC) which runs to thousands of test cases.
- Altinity implemented and tested LDAP-based authentication and user management.
- We regularly post and present on security-related topics.

Please contact us for more information on engineering projects related to ClickHouse security.

ClickHouse Support and Training

Altinity regularly advises customers on security-related topics. We also follow practices designed to protect customer data.

- Support engineers provide answers as well as best practices for security configuration of ClickHouse.
- Altinity Proof-of-Concept services include advice on design of security, privacy-compliant analytic applications.
- Altinity engineers do not directly touch or change customer on-prem systems unless explicitly authorized under terms of a Statement of Work.
- Altinity engineers do not store sensitive customer data in support case management systems.

More Information

Security is a never-ending topic. If you have additional questions, please contact us at info@altinity.com.