great expectations

Cloud security

Great Expectations Cloud has comprehensive security controls for your data. That means it fits right in with your existing security protocols and compliance norms.

Preconfigured for security

GX Cloud has security features for authentication, authorization, encryption, and more.

Role-based access management

Configure role-based access rules for admin, editor, and viewer roles to control how users interact with Expectations and Validation Results.

Isolated organizations

GX Cloud logically separates customers' data to ensure that each data quality project is private and secure.

End-to-end encryption

All network traffic is encrypted using **Transport Layer Security** (TLS). Encryption for data at rest is automated using encrypted storage volumes.

Field-level encryption is used for sensitive configuration data.

Compliance

Great Expectations has completed an independent third-party SOC 2 Type II audit. To request a copy of our latest report, email trust@greatexpectations.io.

GX Cloud generates metadata about **Expectations**, Validation Results, and Data Documentation. It's **easy for you to choose** what GX Cloud stores and displays and what it does not—sensitive metadata is never displayed in its UI unless you allow it. Since GX Cloud processes your data in place, it never leaves your infrastructure.

Have questions? Get in touch.

security@greatexpectations.io