MOLECULE DATABASE

Your sensitive data is stored securely, and only authorized users have access.

• Our database is a multi-tenant, highly scalable Postgres implementation managed by Amazon Web Services, who:
  • hosts it within their SOC-1, SOC-2 (formerly SAS70), and SOC-3 certified data center,
  • handles physical plant, server, and network access controls, and
  • specializes in keeping it, and the underlying servers, up-to-date with the latest security and feature releases.
• Access to the database is limited to the Molecule engineering and services teams, and is secured by two-factor authentication.
• All data is encrypted at rest in our database.

MOLECULE APPLICATION

Molecule is protected from intrusion, and it shows your data only to you.

• The Molecule application enforces low-level isolation of account information. In addition, it provides role-based access control and data filtering to users within your organization.
• The Molecule application runs a robust set of automated tests on itself daily and for each change made to the software.
• Each new release of Molecule is also hand-tested by our team to ensure that every user sees only what they are authorized to see.
• Authentication in Molecule is enforced by the industry-standard Devise library, and the application itself is built using industry-standard technologies including Ruby on Rails, Ember, and Redis.
• Molecule has automatic user cool-down and lock-out functionality built in. The Molecule team can also lock out a user upon request.
• Molecule retains access logs of every use of our application, and can make them available upon request.
• The Molecule team monitors use of our application to identify and act against any suspicious activity.
• The Molecule team has the ability to shut down or patch the app instantly in response to any unauthorized use.
DATA CENTER

The machines that touch your data are protected from physical and network intrusion.

- The Molecule database, application, and sensitive information live entirely within Amazon’s AWS datacenter. This is a SOC-1, SOC-2 (formerly SAS70), and SOC-3 certified datacenter in Northern Virginia.
- Molecule has defined strict network security rules. Only the portions of the application we specify are available outside the data center.
- Communication within the data center is secured by Amazon's anti-packet sniffing and anti-promiscuous mode technology.
- Connections to the data center are limited to engineering staff, and are secured with two-factor authentication.

INTERNET

Anything that goes over the Internet is encrypted.

- All Internet connections to Molecule are encrypted using 256-bit SSL/TLS encryption.

USER

Molecule uses strong authorization and access controls.

- Authentication in Molecule is enforced by the industry-standard Devise library.
- Access controls are available so that users in your organization can be restricted to seeing only a subset of Molecule data.
- Molecule encourages login hygiene within your organization. The application requires strong passwords, and logs users out after a period of inactivity.

MOLECULE, THE COMPANY

We secure your data even before it’s in the Molecule application. (i.e., while we’re testing your portfolio pre-implementation).

- We store customer data in a single location, accessible only to relevant members of the team.
- Data is downloaded only to encrypted devices and is secured by two-factor authentication.
- Database access, backups, and code are accessible only to the engineering and services teams.
- Passwords for all our tools meet our complexity requirements, and are audited regularly. All passwords are secured by best-practice policies, industry-leading tooling, and multi-factor authentication.
- All Molecule employees (including anyone with access to customer data) are background-checked and under NDA.
- The Molecule application and other stored data are regularly audited for security.
- 24x7 support from the Molecule team ensures that if you ever have a concern we will address it immediately.

COMING SOON

We continuously audit our application and practices for security of our customers’ data. Security enhancements coming soon:

- Multi-factor Authentication - We plan to roll out an option for our customers to require a rotating key for authentication to Molecule. This is something we use internally for many services.
- High Availability - We are migrating our servers to an environment where they can fail over to a different geographic region upon demand.