MOLECULE SOFTWARE
1333 WEST LOOP SOUTH, SUITE 950
HOUSTON, TX 77027
+1 (832) 464-4037 | info@molecule.io | molecule.io

SECURITY + COMPLIANCE.

2024

MOLECULE

INTRODUCTION

Molecule is the leading Enterprise SaaS platform for Energy and Commodities Trading Risk Management (E/CTRM), helping companies track and model their position, valuations and risk metrics across hundreds of commodities and tens of thousands of products.

Molecule brings automation, integrations, cutting edge innovations and consumer-grade quality to provide a better, modern experience.

Our priority is to make Molecule one of the most reliable and secure E/CTRMs ever built. We designed and built our product with security at its core, and we operate our company to exceed the highest security standards in the industry.

This document is a high-level overview of Molecule's security measures in various categories.

APPLICATION SECURITY

SDLC

Molecule maintains Software Development Life Cycle (SDLC) policies that govern the design and implementation of any application and infrastructure changes.

We have quality assurance (QA) and code review processes to maintain standards for product quality, security, and user experience.

PATCHING

Our entire codebase is version-controlled in GitLab. The main branches are protected, and any change to the codebase is subject to comprehensive CI tests, code reviews, QA cycles, and approvals before it can be shipped. Any changes made to the application codebase are tracked and the history is maintained in GitLab.

Our patch management policy ensures that operating systems, software, frameworks, and libraries used in Molecule's infrastructure are reviewed to identify required updates on a regular basis. Whenever a vulnerability in a product/service used by Molecule or a high or critical vulnerability is publicly reported, prompt actions are taken to mitigate any potential risks for our customers.

SECRETS MANAGEMENT

Application secrets are managed through AWS EKS backed by Hashicorp Vault. Access is restricted to only a handful of engineers and is provided on a need-to-know basis.

All tokens, passwords, certificates, and other sensitive data are securely stored in an encrypted form. Access and usage of these secrets are regularly audited and monitored.

BEST IN CLASS TOOLING

Molecule is built on industry-standard technologies including Ruby on Rails, Python, and PostgreSQL.

Authentication in Molecule is enforced using industry-leading libraries and providers, including Auth0.

ACCOUNT SECURITY

LOGIN + SIGNUP

Molecule uses Auth0 to support web authentication. Customers can opt to manage user access through Single sign-on (SSO) authentication using an external identity provider or via user-configured passwords.

For fallback purposes, Molecule also supports authentication using Magic Links which are secured by JWT.

Sign-in methods are configurable with two-factor authentication.

PASSWORD + SESSION POLICIES

All user login passwords are managed by an external identity provider called Okta, through their industry-leading Auth0 service. More information about Okta's security policies can be found here.

Sessions on Molecule have a finite duration.

Molecule has automatic user cool-down and lock-out functionality built in. The Molecule team can also lock out a user upon request.

The application requires strong passwords.

CUSTOMER/ACCOUNT PERMISSIONS

All Molecule data is tagged with account ID so that users can only access data that belongs to their account.

Every new release is tested by our team to ensure every user only sees what they are authorized to see.

USER PERMISSIONS

An account administrator can grant permissions to govern the actions users can perform in the system and the screens and types of data that users can see.

API PERMISSIONS

API access requires a username and token. The token is one-way encrypted, stored by Molecule, and easy to revoke.

AUDIT TRAILS

Molecule retains access logs of every use of our application and can make them available upon request.

INFRASTRUCTURE SECURITY

PHYSICAL AWS SECURITY

Molecule uses Amazon Web Services (AWS) as its cloud hosting provider. AWS handles the physical security of the facilities in which the services operate, in addition to the security of the host operating system and virtualization layer.

Amazon's physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication at least twice to access data center floors. More information can be found on the AWS Compliance center here.

NETWORK SECURITY

Molecule has defined strict network security rules. Only the portions of the application we specify are available outside Molecule's internal network.

Communication within the data center is secured by Amazon's anti-packet sniffing and anti-promiscuous-mode technology.

STAGING ENVIRONMENT

Molecule has multiple staging environments that are isolated from our production environment. Any change made to the infrastructure/application is first deployed and tested in the staging environment before rolling it out to production.

PRODUCTION ACCESS

To access our production environment, engineers are required to use AWS client VPN which establishes a secure connection between the AWS network and endpoint device. More information can be found here.

Access to the AWS Console is restricted to necessary personnel. SAML and 2-factor authentication are required to log into the AWS console.

DATA SECURITY

MULTI-TENANT ARCHITECTURE

Molecule is built as a pure multi-tenant SaaS application. At the data layer, all customer accounts are logically isolated with data access limited to the account's users.

TESTING ON EVERY RELEASE

Automated testing ensures that account security is maintained as features are added and changed.

Molecule employs a modern array of testing techniques including linting, static code scans, peer review, manual testing, 90%+ coverage ratio for automated tests, and post-release security testing.

The app also runs a robust set of checks on itself daily.

BACKUPS

Data is periodically backed up in near real-time. Nightly backups are also taken, of all databases. The last seven nightly backups are always available, and backups are tested weekly for consistency. Off-site backups are taken bi-weekly.

ENCRYPTION AT REST

All customer data is stored within AWS and encrypted at rest, providing an added layer of security. Protecting data at rest reduces the risk of unauthorized access, with encryption and access controls.

Click here to learn more.

ENCRYPTION IN TRANSIT

All customer data is encrypted in transit using the Transport Layer Security (TLS) protocol. Insecure protocols, such as HTTP, are either redirected to HTTPS or blocked using AWS security groups.

Click here to learn more.

RELIABILITY

99.9% UPTIME

Ever since its inception, Molecule has consistently met or exceeded 99.9% uptime, while ensuring access to projects and tasks for customers without any interruptions. 99.98%+ uptime annually is routine.

BCP + DR PROCESS

Molecule runs a BCP (Business Continuity Process) drill and DR (Disaster Recovery) simulation at least annually. An internal audit is conducted to ensure both BCP and DR are seamless in case of any unforeseen circumstances.

MULTI-AZ DEPLOYMENTS

Our application is deployed across multiple availability zones (AZ) in AWS. This ensures that our application can still recover even in case of unforeseen incidents affecting an entire AZ.

MONITORING

Molecule has monitors in place to alert our team immediately in case of service degradations to any of Molecule’s features. When a component underperforms, our engineers receive an alert within seconds. A dedicated ops team keeps a tab on these alarms.

NO DOWNTIME DEPLOYMENTS

New software rollout at Molecule occurs through a ‘rolling deployment’ strategy. This ensures customers receive new changes without disruption.

ENDPOINT SECURITY

ALL COMPUTERS ARE ENCRYPTED + MANAGED BY MDM

A Mobile Device Management (MDM) solution automatically installs all security components and allows Molecule to remotely wipe devices if they are compromised. The MDM system also enforces regular security patching from Apple and Windows.

Employees who have access to our production infrastructure and data are required to have anti-malware installed in their systems. We review monthly and address any shortcomings via centralized MDM and anti-malware control panels.

PENETRATION TESTING

Automated penetration testing and vulnerability scans are run weekly, and white hat penetration testing is conducted at least annually by a third party. Updates and fixes are incorporated based on their recommendations. Molecule has consistently received the highest possible score on our penetration tests. But there's always more we can do, so we welcome issue reports and suggestions for improvement.

COMPLIANCE

DATA PRIVACY

Molecule is committed to protecting the privacy of your data. Please see our full data privacy policy here.

INDEPENDENTLY AUDITED FOR SOC 1 TYPE 2 + SOC 2 TYPE 2

Molecule meets the standards of AICPA SOC 1 Type II and SOC 2 Type II, and is audited annually to ensure compliance at the highest possible level. Our policies and system controls are audited for both effectiveness and design. Click here to learn more.

LOCAL COMPLIANCE

Molecule offers our solutions in compliance with privacy standards such as GDPR, California and other leading jurisdictions. Specific local compliance information is available on request.

CONCLUSION

If you have any specific concerns that are not addressed in this document, feel free to reach out to us at support@molecule.io.

At Molecule, we are committed to continuously improving our security practices. This means the information in this document is subject to change.