Modzy Security Overview

Defense in Depth

Even though AI is an emerging technology, AI security threats and attacks are already sophisticated. That's why Modzy has developed the only comprehensive security offering for AI, built to counter even the most advanced attacks all the way down to the model level.

- **Modern Zero-trust security architecture**
- **API Keys and Role-Based Access Control limit permissions to specific actions in the Modzy API**
- **End-to-end encryption and mutual TLS authentication**
- **Complies with security standards, including those from NIST, FISMA, STIGs, and FedRAMP**
- **Comprehensive auditing of all API actions**

Run on your own infrastructure to meet your own security and compliance requirements.

Modzy is built to comply with a wide range of security standards for software products, including the most stringent ones set forth by FISMA and FedRAMP, as well as AI-specific standards set by NIST. With adversarial defense and the ability to detect data poisoning before your models run inference, Modzy gives you the peace of mind to securely deploy AI at enterprise scale.

Infrastructure Security

Run on your own infrastructure to meet your own security and compliance requirements. Alternatively, get started quickly in the Cloud with our pre-made AWS CloudFormation Templates built to comply with the most stringent standards and accreditations (e.g., FISMA, FedRAMP, NIST, etc.).

Application Security

Encryption In Transit

All traffic coming into Modzy is encrypted using TLS 1.2 or higher. Each customer is able to use their own domain and a TLS certificate issued by the Certificate Authority of their own choosing.

internal traffic will be encrypted by a full mutual-TLS encrypted service mesh so that no over-the-wire traffic will be sent in plaintext. Additionally, the service mesh restricts internal traffic between services to only that traffic that is required for the Modzy application to function. This ensures that even if your perimeter infrastructure security is breached that no unauthorized backdoor access can occur within the Modzy application.

Encryption At Rest

Modzy encourages the use of encrypted volumes, object stores, and databases. Our QuickStart AWS CloudFormation Templates set up encryption at rest by default for all data storage locations.

Sensitive data submitted to Modzy will be just-in-time encrypted before storage and can only be decrypted by the service(s) that require(s) the ability to read it. This ensures that even if your encrypted storage has unauthorized access that your data will remain safe.

Role-Based Access Control

- All privileged access to Modzy user interfaces and APIs is governed by role-based access control
- Single-Sign On (SSO) for User Interface Access
- User-interactive access uses your existing SAML 2.0-based SSO identity provider

API Key Security

Programmatic access to the Modzy API uses a Modzy-issued API Key. All Modzy-issued API Keys are assigned to a person for auditing and accountability. Modzy-issued API Keys are only viewable in their full plaintext form exactly once when they are created. After the key has been issued, half the key is permanently one-way encrypted to prevent any future access to the full unencrypted key. The unencrypted portion of the key is used to identify which key was used to perform every action against the Modzy API.

modzy™

Model Security

Adversarial Defense

Certain models are trained using Modzy's proprietary training solution to defend against adversarial attacks. Further, Modzy's novel adversarial input detector can parse data for potential adversarial attacks and filter out adversarial inputs before they get to the model.

Model Immutability and Version Control

All models in Modzy are immutable and assigned a version number. Versions of a model cannot be changed, allowing full reproducibility of results.

Software Security

Static Code Analysis

All Modzy source code undergoes automated static code analysis as a part of our Software Development Lifecycle (SDLC) process.

Container Security

All Modzy software is delivered via OCI-compliant containers that are verified to be free of Critical and High CVEs.

Software Security

All Modzy API calls generate audit logs so that a complete trail of every action, the time the action took place, and the credentials used to perform the action are logged. Access to the audit logs is controlled by a special "Auditor" role which can be assigned separately from any other access or role.

Modzy.com