

Security Overview

Updated on 5/24/2024

© 2024 Paximal, Inc.

Overview

Welcome to the Security Overview of Paximal, Inc. (“Paximal”). This document provides a brief overview of our security practices.

Contents

1. Governance **3**
2. Data Protection **3**
3. Data Privacy **3**

1. Governance

Paximal's technical teams establish policies and controls, monitor compliance with those controls, and validate our security and compliance with third-party auditors. Our policies are founded on the following principles:

- **Access Control**: Access is limited to those with a legitimate business need, granted based on the principle of least privilege, and terminated when no longer needed.
- **Defense-in-Depth**: Security controls are implemented and layered according to the principle of defense-in-depth.
- **Consistency**: Security controls are applied consistently across all areas of the enterprise.
- **Continuous Improvement**: The implementation of controls is iterative, constantly maturing across dimensions of improved effectiveness, increased auditability, and decreased friction.
- **Beyond Compliance**: We prioritize security as much as validation of security, going above and beyond standard requirements when necessary.

2. Data Protection

- **Data at Rest**: Datastores containing customer data, including those in the cloud, are encrypted at rest. Data is encrypted before it reaches our database, ensuring it remains inaccessible even in the event of a physical breach or unauthorized logical access.
- **Data in Transit**: We use TLS 1.2 or higher for all data transmitted over potentially insecure networks. Server TLS keys and certificates are managed by AWS and deployed via AWS Load Balancers.
- **Secret Management:** We manage secrets using AWS Secrets Manager. Application secrets are encrypted and stored securely via AWS Secrets Manager, with access to these values strictly limited.

3. Data Privacy

Customer data is a valuable asset that requires meticulous handling and ethical considerations. Paximal is committed to safeguarding the privacy and trust of our customers. We prohibit the use of customers' confidential information, including private usage data (such as unpublished patent applications), for model training purposes without explicit and documented consent from the individuals involved. This consent includes detailed information about the nature of the

training, the specific data elements involved, and the purpose for which the data will be used. We prioritize the security and confidentiality of customer information, ensuring any use for training adheres to legal and regulatory requirements, as well as our commitment to maintaining the highest standards of data ethics.

Vulnerability Scanning: Paximal requires vulnerability scanning at key stages of our secure development lifecycle. These include:

- **Local Development**: Scanning for vulnerabilities on machines during any local development.
- **Dependency Scanning**: Vulnerability scanning of dependencies, also known as software composition analysis.
- **Static Analysis Testing**: Static analysis testing of code during pull requests and on an ongoing basis.
- **External Attack Surface Management**: Continuous running of external attack surface management software to discover new external-facing assets.