Katalon Security & Trust

Executive Summary

A Commitment to Protecting Your Data and Accelerating Innovation

November 7, 2025 | Version 1.0

At Katalon, trust is the foundation of our partnership with customers. In an era of rapid digital transformation and artificial intelligence, we understand that a robust security and privacy posture is not just a feature—it is a prerequisite. This document provides a transparent, high-level overview of the programs, controls, and principles that protect your data when you use the Katalon Platform.

Our mission is to provide you with the verifiable proof and clear documentation you need to conduct due diligence efficiently, allowing your teams to adopt innovative solutions like TrueTest with confidence and speed.

Key Pillars of Trust

1. Enterprise-Grade Security

Our security program is built on industry best practices to protect your data at every layer, from our infrastructure to our application code.

- **Secure by Design:** Security is integrated into every phase of our Software Development Lifecycle (SDLC), including mandatory threat modeling, static and dynamic code analysis, peer reviews, and vulnerability scanning before any deployment.
- **Resilient Infrastructure:** The Katalon Platform is hosted on Amazon Web Services (AWS), leveraging its world-class physical security, operational excellence, and highly available architecture. All data is stored in the AWS us-east-1 region (USA).
- **Data Encryption:** All customer data is encrypted in transit using **TLS 1.2+** and at rest using industry-standard **AES-256 encryption**. Sensitive database records are further protected with SHA256 hashing.
- **Vendor Risk Management:** We maintain a robust vendor management program, including formal security and privacy reviews of all sub-processors, to ensure a secure supply chain. This program is audited as part of our SOC 2

certification.

2. Verifiable Compliance

We engage independent, third-party auditors to validate the effectiveness of our security controls, providing you with objective proof of our commitment.

- **SOC 2 Type II:** Our SOC 2 Type II report, which covers the Security, Availability, and Confidentiality trust services criteria, is available upon request.
- **ISO/IEC 27001:2022 and ISO/IEC 27017:2015:** We are certified against the global standards for Information Security Management Systems (ISMS) and for cloud-specific information security controls.
- **Global Privacy Standards:** We adhere to global privacy regulations, including GDPR, and are a participating member of the **EU-U.S. Data Privacy Framework (DPF)** for trusted international data transfers.

3. Responsible AI & Data Privacy

We have established a clear framework for our native-AI product, TrueTest, and other features utilizing artificial intelligence, to ensure your data is handled responsibly and transparently.

- **Our Core Commitment: Zero Data Retention.** Customer data is **never** used to train or improve third-party AI models. We maintain contractual zero-retention and no-log agreements with all our AI service providers.
- **Complete Customer Control:** AI features are optional. Your administrators have full, granular control to enable or disable all AI services. For enhanced data sovereignty, TrueTest supports a **"Bring Your Own Key"** model, allowing you to integrate with your own private instance of Microsoft Azure OpenAI.
- **Proactive Data Filtering by Design:** The TrueTest agent is designed with privacy at its core. It automatically detects and filters common sensitive data types (e.g., PII, credit card numbers, passwords) at the source, *before* any data is sent for processing. Customers can also manually define specific UI elements to exclude from capture.

TrueTest AI Data Flow Architecture

This high-level diagram illustrates our multi-layered approach to protecting your data. Customer-specific data from your Application Under Test (AUT) is filtered and anonymized before any processing by third-party AI models.

Your Environment	→	Katalon Platform (Our Secure AWS Environment)	→	Third-Party AI Service
Data: User Prompts, Application Under Test (AUT) Data.		**Action:** TrueTest agent automatically filters sensitive data at the source. Our platform receives user prompts & anonymized AUT structure (DOM), removing any remaining user-entered values.		**Action:** Processes the anonymized prompt to generate test steps. **No data is stored, logged, or retained.**
Your sensitive data, including PII, passwords, and credit card numbers, is filtered at the source via regex and user rules.		*Data is anonymized and secured before processing.*		*Contractual Zero Data Retention is enforced.*

For a complete view of our policies, certifications, and AI Architecture, please visit the full Katalon Trust Center.