



A-LIGN

Tricentis USA Corp.

Type 2 SOC 3

2023



SOC 3 FOR SERVICE ORGANIZATIONS REPORT

July 1, 2022 to June 30, 2023

Table of Contents

SECTION 1 ASSERTION OF TRICENTIS USA CORP. MANAGEMENT	1
SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT.....	3
SECTION 3 TRICENTIS USA CORP.'S DESCRIPTION OF ITS QTEST, TESTIM, VISIONAI, TRICENTIS TEST AUTOMATION, TTA FOR SFDC, TTM FOR JIRA SERVICES SYSTEM THROUGHOUT THE PERIOD JULY 1, 2022 TO JUNE 30, 2023	7
OVERVIEW OF OPERATIONS	8
Company Background.....	8
Description of Services Provided	8
Principal Service Commitments and System Requirements	40
Components of the System	42
Boundaries of the System	45
Changes to the System Since the Last Review.....	45
Incidents Since the Last Review	45
Criteria Not Applicable to the System.....	45
Subservice Organizations	45
COMPLEMENTARY USER ENTITY CONTROLS.....	48

SECTION 1

ASSERTION OF TRICENTIS USA CORP. MANAGEMENT

ASSERTION OF TRICENTIS USA CORP. MANAGEMENT

September 11, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within Tricentis USA Corp.'s ('Tricentis' or 'the Company') qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services System throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Tricentis' service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "Tricentis USA Corp.'s Description of Its qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services System throughout the period July 1, 2022 to June 30, 2023" and identifies the aspects of the system covered by our assertion.

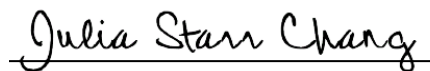
We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Tricentis' service commitments and system requirements were achieved based on the trust services criteria. Tricentis' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Tricentis USA Corp.'s Description of Its qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services System throughout the period July 1, 2022 to June 30, 2023".

Tricentis uses Amazon Web Services ('AWS' or 'subservice organization') and Microsoft Azure ('Azure' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Tricentis, to achieve Tricentis' service commitments and system requirements based on the applicable trust services criteria. The description presents Tricentis' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Tricentis' controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Tricentis' service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Tricentis' controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that Tricentis' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Tricentis' controls operated effectively throughout that period.



Julia Starr Chang
Director, Governance, Risk and
Compliance
Tricentis USA Corp.

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT



INDEPENDENT SERVICE AUDITOR'S REPORT

To Tricentis USA Corp.:

Scope

We have examined Tricentis USA Corp.'s ('Tricentis' or 'the Company') accompanying assertion titled "Assertion of Tricentis USA Corp. Management" (assertion) that the controls within Tricentis' qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services System were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Tricentis' service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

Tricentis uses AWS and Azure to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Tricentis, to achieve Tricentis' service commitments and system requirements based on the applicable trust services criteria. The description presents Tricentis' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Tricentis' controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Tricentis, to achieve Tricentis' service commitments and system requirements based on the applicable trust services criteria. The description presents Tricentis' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Tricentis' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Tricentis is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Tricentis' service commitments and system requirements were achieved. Tricentis has also provided the accompanying assertion (Tricentis assertion) about the effectiveness of controls within the system. When preparing its assertion, Tricentis is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Tricentis' qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services System were suitably designed and operating effectively throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Tricentis' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Tricentis' controls operated effectively throughout that period.

The SOC logo for Service Organizations on Tricentis' website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Tricentis, user entities of Tricentis' qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services during some or all of the period July 1, 2022 to June 30, 2023, business partners of Tricentis subject to risks arising from interactions with the qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
September 11, 2023

SECTION 3

**TRICENTIS USA CORP.'S DESCRIPTION OF ITS QTEST, TESTIM, VISIONAI,
TRICENTIS TEST AUTOMATION, TTA FOR SFDC, TTM FOR JIRA SERVICES
SYSTEM THROUGHOUT THE PERIOD
JULY 1, 2022 TO JUNE 30, 2023**

OVERVIEW OF OPERATIONS

Company Background

Tricentis was founded in 2007 and is a provider of Automated Testing Solutions helping organizations attract, acquire and grow customers at scale. Tricentis Automated Testing Solutions are built on a patented Intelligent Testing Automation Platform integrating machine learning, autonomous action chains, and deep learning capabilities identify test case gaps, optimization, which in turn delivers unparalleled test automated capabilities and drives consistent software quality. Tricentis has more than 1,600 customers, including many of the largest brands in the world.

Description of Services Provided

qTest - Description of Services Provided

qTest Manager

Tricentis' qTest manager is an agile test management solution that is designed to help QA teams plan, manage, and execute all testing activities in a software development lifecycle. qTest Manager provides the following functionality:

- Plan Tests: Organize and plan test strategies across projects, releases, and sprints
- Manage Requirements: Requirements and associated defects are directly linked to test cases and associated defects giving full traceability within a project
- Manage Test Cases: Import, create, manage and organize tests (i.e., manual, automated, performance, exploratory) - even multiple versions of a test case to be executed - across releases, environments, data parameters, configurations, and custom data aligned to the application under test
- Execute Tests: Manage test cycles, create and execute test runs, and filter results in real-time by status, test type, or defect
- Generate Reports: Real-time out-of-the-box or customizable reports with advanced query capabilities
- Track Defects: Create custom queries to locate defects and export results into Excel

By adding qTest integrations to the Issue Tracking software, qTest provides a mechanism to manage requirements and defects in the customers' ALM (Application Lifecycle Management) of choice, providing more visibility to the development organization around testing status. Some of the integrations include Jira software, VersionOne, and CA Agile Central.

qTest Explorer

Tricentis' qTest Explorer is designed specifically for agile testers to provide the tester with a rich documentation tool that simplifies scripted and unscripted testing by intelligently capturing each mouse click, field change, page change, and more. qTest Explorer provides the following functionality:

- Record: Intelligent capture technology tracks interactions from the testing session
- Edit: Allows annotated, deletion, and editable recorded sessions from a single interface
- Share: Share detailed defects with other team members quickly and easily
- Generate: Generate test cases from recorded sessions
- Automate: Create web-based automated test scripts from recorded actions
- Manage: Plan and organize session-based testing in a central session manager
- Submit: Submit defects directly to Issue Tracking software and other supported defect trackers

qTest Insights

Tricentis' qTest Insights is a way to view real-time results and progress from agile testing. Different than traditional static reporting, qTest Insights provides a dynamic high-level visualization of test results, allowing quick identification and troubleshooting of issues. qTest Insights provides the following functionality:

- **Analysis:** Visually see results of the testing process with actual data from the test execution and associate defects and notes within a test
- **Integrate:** Insights connects into qTest Manager to report test progress and to other integrated tools in the software development pipeline
- **Manage:** Visually manage the testing process by seeing who tested what and quickly identifying untested areas of an application
- **Executive Reporting:** Insights allows users to create multiple dashboards from different projects or teams and to share this information with internal and external stakeholders for enterprise reporting
- **Customize:** In addition to the pre-built report templates, qTest Insights gives users the ability to custom build various test metrics reports, pie charts, bar graphs, scatter plots, and data tables

qTest Launch

Tricentis' qTest Launch is test automation and machine management at scale through a single interface. qTest Launch allows enterprises to centrally manage test automation scripts and test machines to increase test automation efficiency. qTest Launch provides the following functionality:

- **Centralize Test Automation:** Unify execution of automated tests to increase efficiency
- **Integrate Across Frameworks and Tools:** Manage all test automation across a wide variety of frameworks and tools
- **Increase Test Automation Coverage:** Tie automated test results directly to business requirements through an integration with Issue Tracking software

qTest Scenario

Tricentis' qTest Scenario (Enterprise Edition) is an Issue Tracking software add-on for enterprise teams practicing Behavior-Driven Development (BDD). When integrated with the qTest platform, qTest Scenario (Enterprise Edition) enables a test-first approach by facilitating test scenario creation and helping to ensure feature traceability. qTest Scenario allows BDD practitioners to perform the following:

- **Improve BDD Collaboration:** qTest Scenario allows testers, developers, and product owners to create, update, edit, and link feature files directly on the Issue Tracking software
- **Issue Tracking Software Traceability to Features:** Test run results are passed directly to the Issue Tracking software for instant test coverage reporting so that stakeholders in the Issue Tracking software know the progress of feature development
- **Store Tests as Code:** qTest Scenario directly stores all feature files into private Git repositories, such as GitHub and Bitbucket, to standardize feature files and scenario steps as code

qTest Pulse

qTest Pulse is a workflow engine for products in the qTest Platform and is currently optimized to integrate BDD workflows for qTest Scenario. It works behind the scenes to integrate Issue Tracking software with Jenkins, Slack, and many different plugins to increase productivity within the development process. qTest Pulse provides the following functionality:

- **Automate:** Leverage custom workflows and real-time integrations to automate handoffs between Continuous Integration (CI), Application Lifecycle Management (ALM), tests, and other development tools
- **Customize:** Create custom Pulse rules through a combination of 'Events' (webhooks) and 'Actions' (program code)

qTest - System Requirements

Tricentis designs its processes and procedures related to the qTest product to meet the compliance and security objectives that apply to the qTest testing services. Those objectives are based on the service commitments that Tricentis makes to user entities, the laws and regulations that govern the provisioning of qTest services, and the financial, operational, and compliance requirements that Tricentis has established for the services. The qTest testing services of Tricentis are subject to the security and privacy requirements state privacy security laws (Ex: GDPR, Australia Privacy Act, US States Privacy Laws, PIPEDA) and regulations in the jurisdictions in which Tricentis operates.

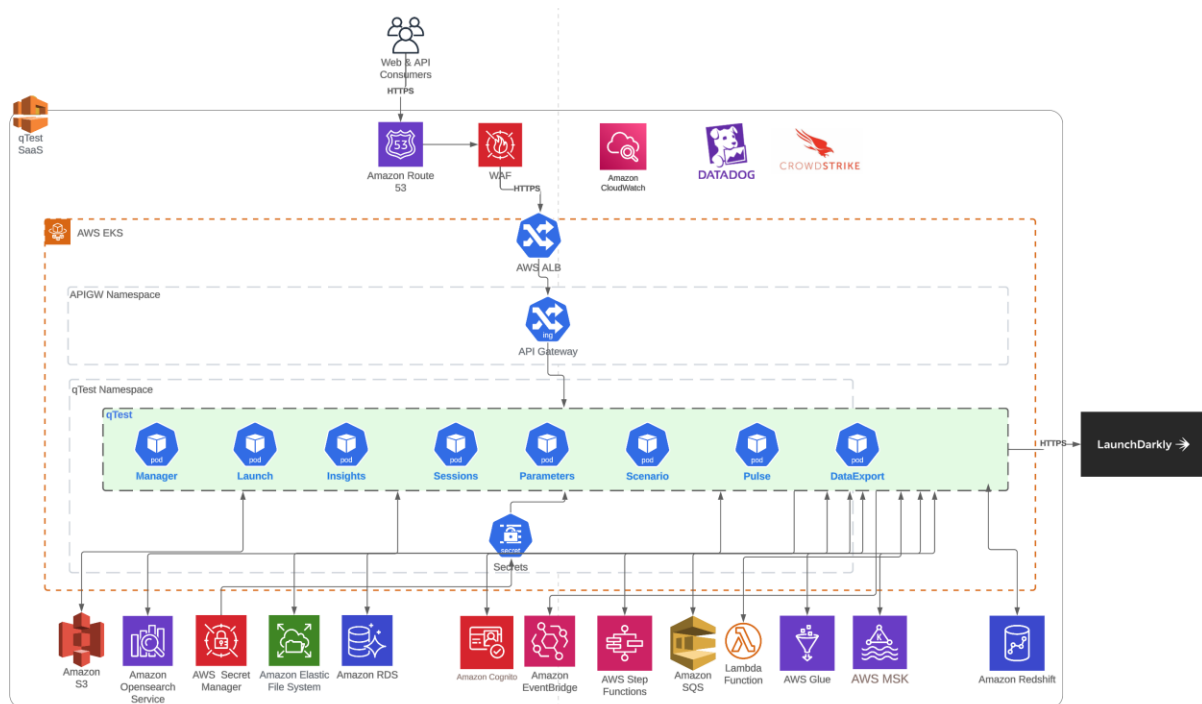
Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the security principles within the fundamental designs of the qTest services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Encryption technologies are used to protect customer data both at rest and in transit.

Tricentis establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Tricentis' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the qTest services.

qTest - Components of the System

qTest HLAD



Infrastructure

Primary infrastructure used to provide Tricentis' qTest manager includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Amazon Service Simple Storage Services (S3)	AWS	Storage service for backups and auxiliary data
AWS Elastic Compute Cloud (EC2)	AWS	A web service that provides resizable compute capacity in the cloud utilizing NGINX, an advanced application load balancing, Transport Layer Security (TLS) termination, and monitoring
AWS Relational Database Service (RDS)	AWS	Allows a user to set up, operate, and scale a relational database in the cloud while managing database administration tasks
AWS Elastic Load Balancer (ELB)	AWS	Elastic Load Balancing that distributes incoming application traffic across multiple targets; Amazon Service EC2 instances, containers, and IP addresses
AWS Application Load Balancer (ALB)	AWS	Application Load Balancer that provides ingress traffic routing and load-balancing (Ingress Controller) to containerized workloads
AWS Route 53	AWS	Route end users to Internet applications by translating web address names (www) into the numeric IP addresses to connect to Amazon Service EC2 instances, Elastic Load Balancing load balancers, or Amazon Service S3 buckets
AWS CloudTrail	AWS	Log, continuously monitor, and retain account activity related to actions across AWS infrastructure. CloudTrail logs event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services
AWS GuardDuty	AWS	Threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts, workloads, and data stored in Amazon Service S3
AWS EKS Fargate	AWS	Fully managed Kubernetes service and integrated with services such as Amazon Service CloudWatch, Auto Scaling Groups, AWS Identity and Access Management (IAM), and Amazon Service Virtual Private Cloud (VPC), to enable monitoring, scaling, and load-balancing the services
Amazon Service Simple Storage Service (Amazon Service S3)	AWS	Object storage service that provides scalability, data availability, security, and performance for attachments received in Testing Services communications
Amazon Service File Integrity Monitoring (FIM) (AWS CloudTrail)	AWS	AWS service that helps you enable governance, compliance, and operational and risk auditing of your account. Actions taken by a user, role, or a service are recorded as events in <i>SERVICE</i> . Events monitored will include actions taken in the Management Console, Command Line Interface, and SDKs and APIs

Primary Infrastructure		
Hardware	Type	Purpose
AWS Elastic Beanstalk	AWS	Manage EC2 images and deploys applications to applicable servers (used for satellite apps)
AWS Redshift	AWS	Managed Columnar Database for storing data for reporting purposes
AWS MSK	AWS	Managed Kafka to handle message queuing and delivery
AWS Lambda	AWS	Managed serverless compute to handle transformations of data for reporting
Debezium	AWS	Debezium is used for change data capture from the database to support ETL

Software Integrations and Subprocessors

Primary software integrations and other SaaS services used to provide Tricentis' SaaS includes the following:

Primary Software Integrations	
Software	Purpose
Amazon Corretto	OpenJDK
Angular	Web Framework
AngularJS	Web Framework
Ansible	On-Premise deployment Testing
AquaSec	Docker image scanning
ArgoCD	GitOps for Kubernetes applications
Artifactory (JFrog)	Build and Delivery Dependencies Management for qTest On-Premise
Atlassian	SDLC (JIRA); SDK; Product internal Wiki (Confluence)
AWS*	Infrastructure/Log containing e-mail, username, IP address
Caliburn.Micro	Custom WPF (XAML) Application Framework
checkov.io	Helm configuration scanning
CircleCI	CI/CD, VCS
CrowdStrike	Intrusion detection system (IPS) monitoring and alerting
DataDog*	Log Management; APM management, diagnostics, and alerting
dbeaver	Database Access Tool
Docker	Container Image Delivery for qTest On-Premise
Dojo	Web Framework
Elasticsearch	Free text search engine
ExpressJS	Web Application Framework
external-secrets.io	Cloud-native secret integration (AWS Secret Manager)

Primary Software Integrations	
Software	Purpose
Gainsight - CS*	Customer success relationship management
GitHub	CI/CD, VCS
GitLab	CI/CD, VCS
Gradle	Java build tool On-Premise installer
Helm	Package management application for Kubernetes applications
IntelliJ	IDE
Intercom*	Customer notifications
Jenkins	CI/CD
JMeter	Performance Test
Knex	RDBMS Management
Liquibase	RDBMS Management
Logi Info	Reporting Engine
MahApps.Metro	Custom UI controls for WPF Application
MailChimp*	SMTP for qTest OnDemand
Maven	Java build tool
Microsoft	Internal and External documentation on products for customers; E-mail integrated exchange to ServiceNow
MS 365 Exchange*	Corporate E-mail Tool
Nginx	Reverse Proxy Server
PagerDuty	Services health alters and incident management
pgAdmin 4	Database Access Tool
PingDom	OnDemand Production monitoring
PM2	NodeJS Management for Production
Postgres	RDBMS
Postman	API Test
Protractor	Automate Test
Qlik	Reporting Engine
Recurly*	Customer Billing / Licenses
Salesforce	Tricentis use - nothing user / privacy specific for qTest here except Client ID
ServiceNow*	Support application for Tricentis supported SAP Partner Products
Skilljar*	Tricentis application training for SAP Partner Products
Slack	Integration to PagerDuty and general engineering support escalation

Primary Software Integrations	
Software	Purpose
Sonar	Static Code Analysis
Spring	Java Framework
Stakato Reloader	Dynamic Configuration for Containers
Swagger	API Documentation
Tomcat	Web App Server
Tricentis Flood	Performance Test
Ubuntu	Base OS Docker images
Virtual Box	Virtualization on Developer PC
Visual Studio Code	IDE
Weave Net	On-premise Delivery for Docker Networking
WhiteSource	Static Code Analysis

**Indicates Subprocessors*

Data

Data required:

- Full qTest project when using qTest SaaS platform for runtime
- qTest License, and current usage of the License
- Git access in case of the connection between qTest Web and a customer GIT repository
- Kubernetes/OpenShift access in case of Dynamic Infrastructure usage
- Configuration settings related to the usage of qTest SaaS platform: preferred language, charts
- User profile (first name, last name, e-mail, API tokens) and authentication data

Collected Data

The data stored by qTest SaaS platform are:

- Test results, including:
 - Overview information (summary and key indicators)
 - Statistics for the customer test data
 - Customer entered API, CMDB, Integrated application, or other test configuration information within test data
 - Error messaging

Data processed and stored using the qTest application, the data sent and stored on the qTest Cloud Platform are related to the customer managed testing.

This information contains:

- E-mail addresses
- Logs
- Customer-managed free text

Using the qTest application data sent and stored in the platform are integrated Defect/Requirements Applications:

- Defects
- Test Status
- Requirements / Stories

Tricentis Test Management for JIRA - Description of Services Provided

Tricentis Test Management for Jira (aka TTM4J) is a collaboration-driven test management tool. It lets you create, execute, and analyze test activities all in one place: your Jira projects. This allows you to seamlessly integrate product testing into your release planning routine.

Tricentis Test Management for Jira is a collaboration-driven test management tool. It lets you create, execute, and analyze test activities in your product development cycle - directly from your Jira projects. This facilitates deep collaboration among your business and QA teams. Plus, Tricentis Test Management for Jira is easy to use - any user can create effective tests with dynamic objectives.

Design Your Tests

Designing tests plays an important role in the development cycle. Only well-designed tests let you verify whether your application is ready for release or whether you still need some adjustments. By providing a set of easy-to-use tools, Tricentis Test Management for Jira makes it simpler for developers and testers to design their tests.

The first step in your testing journey with Tricentis Test Management for Jira is to create test cases and requirements that mirror your testing activities.

In Tricentis Test Management for Jira, you design your tests with two specific issue types in Jira:

- **Test cases**, which define a particular low-level objective in your application. Test cases contain one or more test steps, which are the actions you need to take to test a feature or specification.
- **Requirements**, which define a particular high-level objective in your application. This can be, for instance, a major specification. To track the progress of your specifications, you link requirements to test cases. You may need several test cases to meet a given requirement.

Below is an illustration of a Test Case with a linked requirement and multiple test steps:

The screenshot displays a Jira issue page for a test case. At the top, the breadcrumb navigation shows 'Projects / My Sample WebApp / SAMPLE-1'. Below this is a 'Log in with email and password' section with buttons for 'Attach', 'Create subtask', 'Link issue', 'Test Case Panel', and a menu icon. The 'Description' field contains the text: 'Test if a user can log in with an email and password. User credentials are validated individually.' Below the description is a 'Linked issues' section showing a requirement 'SAMPLE-10 Enable three login methods' with a status of 'SELECTED FOR DEVELOPMENT'. The 'Test Case Panel' section includes buttons for 'Expand view', 'Create test run', and 'Add'. Below this is a table with four test steps, each with a step number, a description, an expected result, and an attachments column.

Step description	Expected result	Attachments
1 Enter a valid email.	Email is validated.	...
2 Enter a valid password for a valid email.	Password is validated.	...
3 Enter an invalid email.	Validation fails with "Email could not be found".	...
4 Enter an invalid password for a valid email.	Validation fails with "Incorrect password".	...

Hint: when editing the last step, press TAB to add a new step.

New step

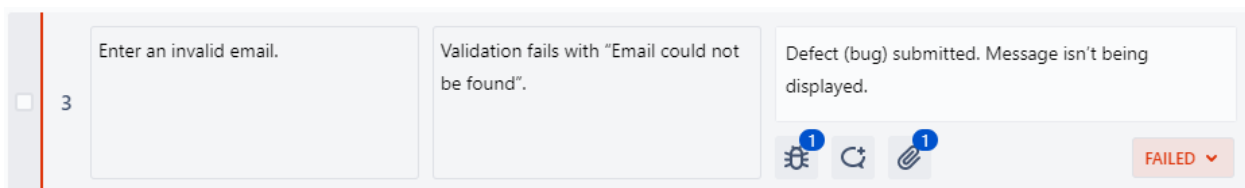
Execute Your Tests

Once you have your test cases, you can prepare and trigger their execution. This tells you whether your application behaves as expected and is ready for release.

The second step in your testing journey is to assemble test cycles and execute your test runs. For each test case, you create an associated test run to document the test results. During the documentation process with Tricentis Test Management for Jira, you can attach relevant resources such as screen captures, comments, or files.

Working with a test run is a vital part of the product development cycle. It is important for testers to add as many details and resources as possible so that stakeholders, developers, and QA teams can easily assess and track the testing progress.

Below is an illustration of test results during the execution of a test run:

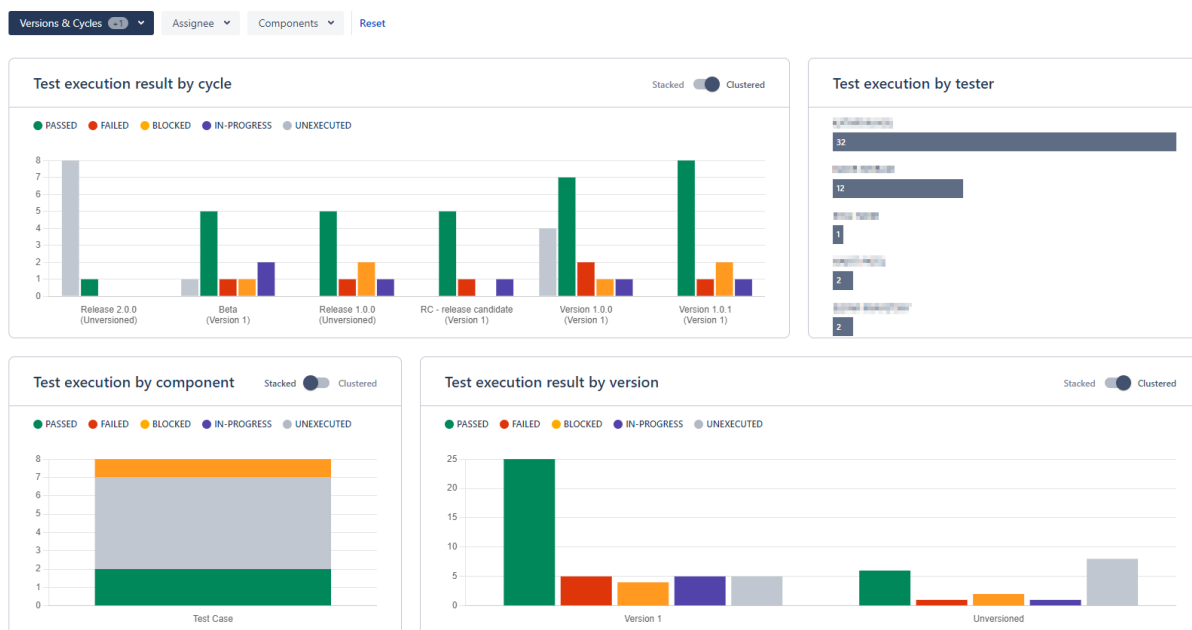


If you encounter a problem during execution, create defects (bugs) to make the rest of the team aware of the issue you discovered. This helps you track any unwanted behavior. All test runs contain specialized tabs where you can keep track of defects, attachments, and associated comments.

Analyze Test Results

It is important that you understand the overall progress of your development cycle and can distribute feedback. So, the third step in your testing journey is to assess your test results and provide the necessary feedback. Tricentis Test Management for Jira allows you to interpret and analyze your test results in many ways.

Test metrics



Integration to Other Tricentis Testing Applications

In Tricentis Test Management for Jira, you can choose to manage your tests via the graphical user interface or through the API. The API gives you the tools you need to create, edit, and delete test cases and test runs, as well as manage folders and attachments.

You can use the API to perform the following tasks in your workspace:

- Manage your **Test Cases** and **Folders**. This includes the ability to find a particular test case, add a new test case, update an existing test case, or delete an obsolete test case.
- Track any **Test Cases** that are automated by your tool of choice.
- Work with **Attachments**.
- Manage your **Test Runs**. This includes the ability to find a particular test run, add a new test run, or delete an obsolete test run.

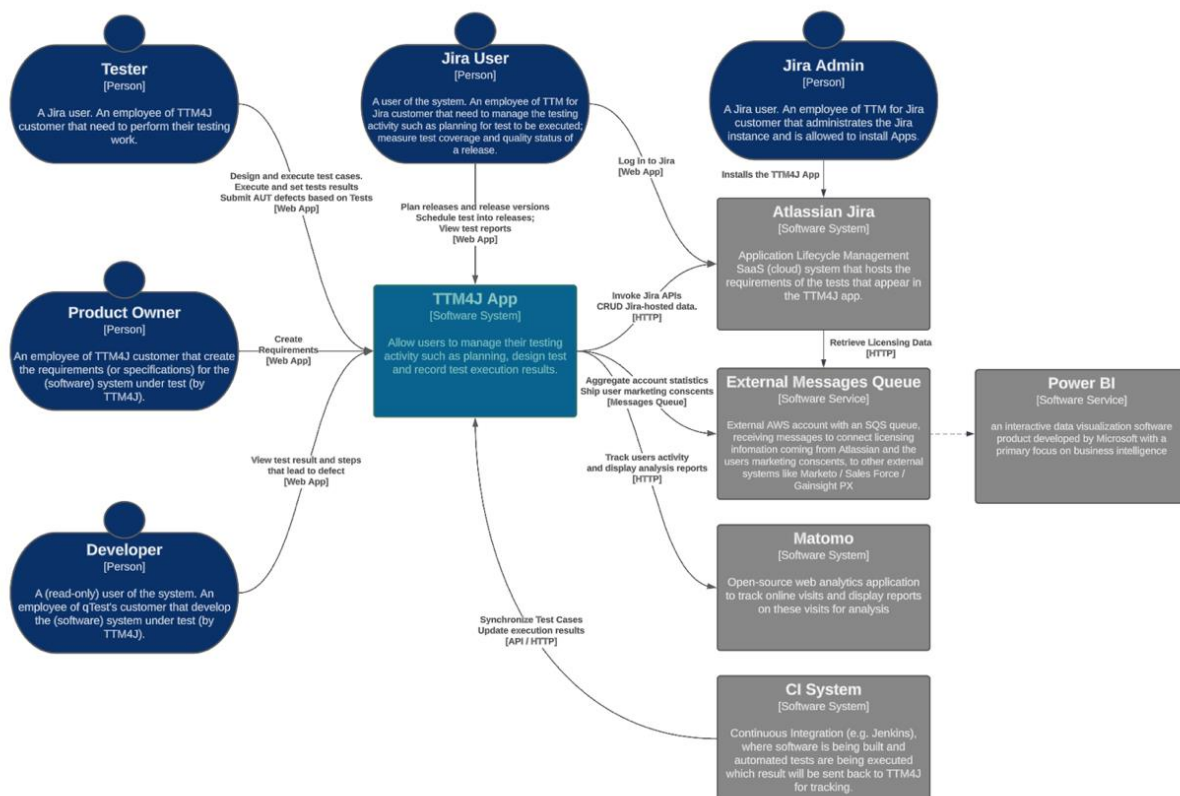
Principal Service Commitments and System Requirements

Tricentis Test Management for Jira is a cloud-based, software-as-a service application, so no onsite installations or upgrades are required. It is distributed in a form of a Jira add-on via the Atlassian marketplace.

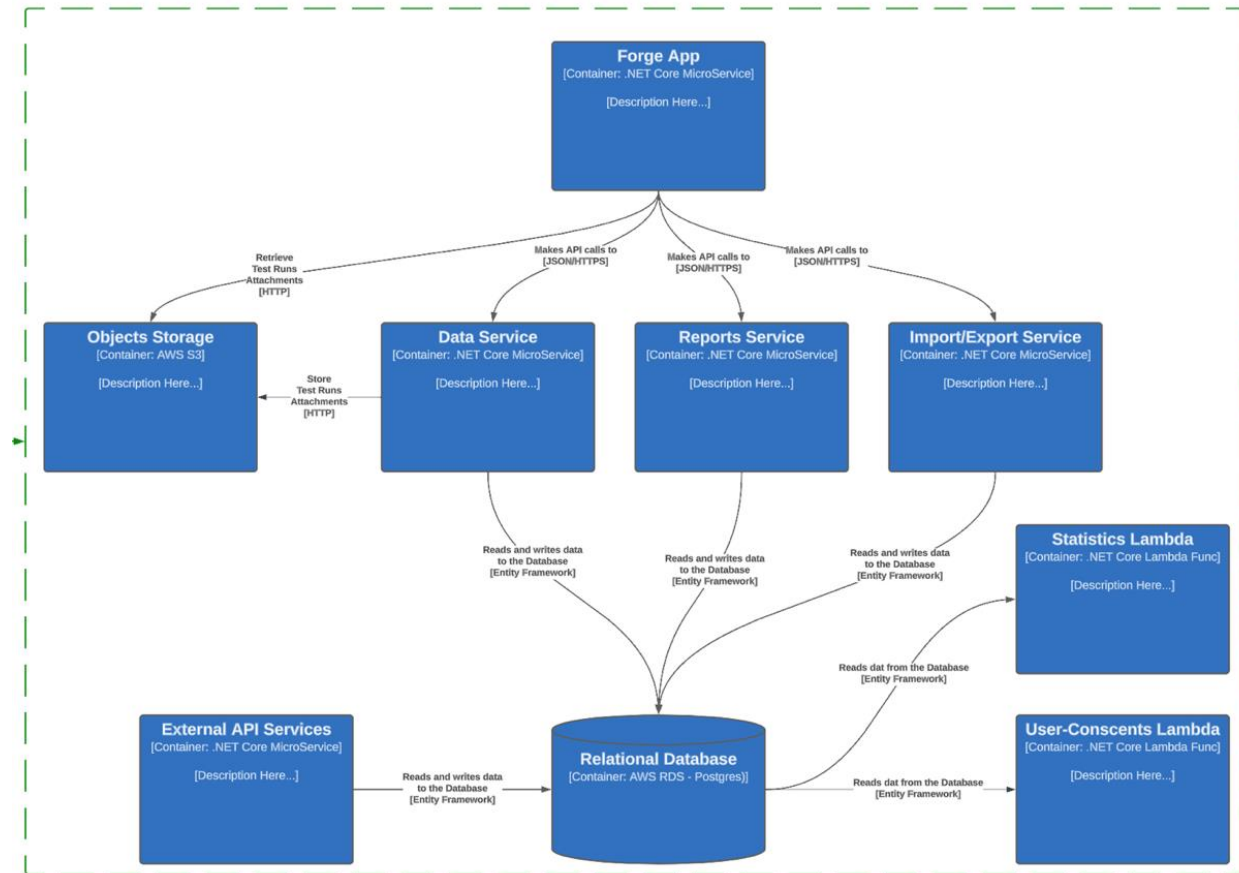
A Jira add-on (also known as a plugin) does exactly what you think it might do: it adds to the functionality of Jira.

TTM - Components of the System

Below is a C4 Level 1 diagram of the test management offering:



Below is a C4 Level 2 diagram of the test management offering:



Component 1: TTM4J Forge App

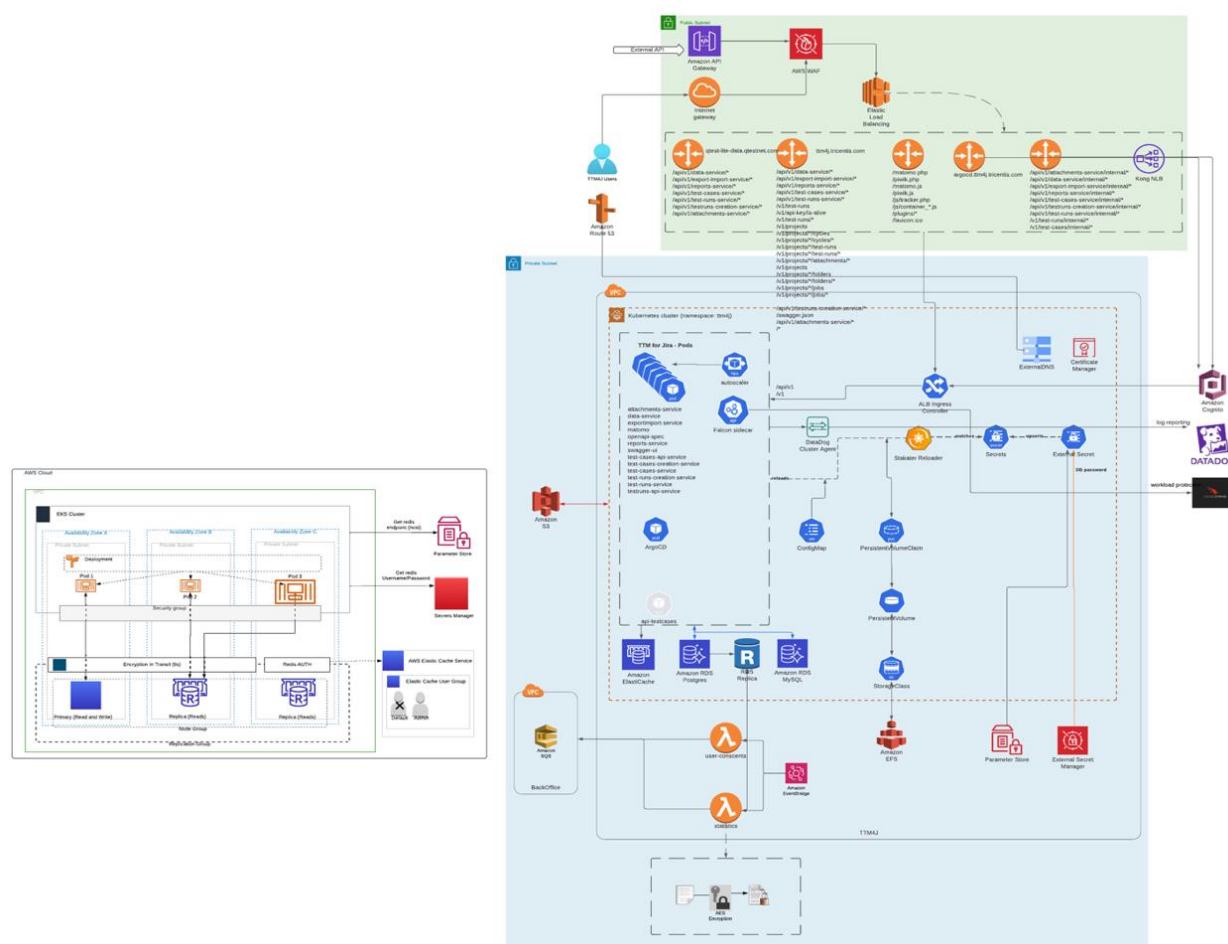
Forge makes it possible to build a fully functional app in just a few hours, with hosting, multiple development environments, and API authentication built in. Forge can be used to build custom apps and integrations or apps distributed through the Atlassian Marketplace.

Atlassian, <https://developer.atlassian.com/platform/forge/>.

TTM4J is a Forge application and therefore is deployed into the Atlassian cloud. Its main function is to serve a front end and the user interface for the users.

Component 2: The Tricentis Test Management for Jira Web SaaS Platform

Its main function is to allow the server-side computing and data storage/retrieval.



Infrastructure

Primary AWS components or services used to provide Tricentis Test Management for Jira SaaS application:

Primary Infrastructure		
Services	Type	Purpose
Containerized microservices	AWS EKS (Amazon Elastic Kubernetes Service)	Primary application supporting the products and service described above Docker Containerized micro-AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (VPC), to enable monitoring, scaling, load-balancing and fail-over of the services

Primary Infrastructure		
Services	Type	Purpose
Elastic Search	Elastic Cloud	Distributed, open-source search and analytics suite used for a broad set of use cases like real-time application monitoring, log analytics, and website search
Postgres SQL	AWS RDS	Persistent SQL storage for the Tricentis Test Management for Jira
Amazon Service Simple Storage Services (S3)	AWS S3	Private buckets for storing attachments for Test Runs
Application Load Balancer (ALB)	AWS ALB	Application Load Balancers that distribute incoming application traffic across multiple targets; Amazon Service EC2 instances, containers, and IP addresses. TLS1.2 Forward Secrecy Policies
Web application firewall	AWS WAF	Security system that controls incoming and outgoing traffic for applications and websites
Router 53	DNS Provider	Route end users to Internet applications by translating web address names (www) into the numeric IP addresses to connect to Amazon Service EC2 instances, Application Load Balancers
Amazon Simple Queue Service (SQS)	Distributed message queuing service	Schedule data intake into the Backoffice systems such as PowerBI

Software

Primary software integrations and other SaaS services used to provide Tricentis' SaaS includes the following:

Primary Software	
Software	Purpose
Pingdom	Web application availability monitoring
Slack	Integrated to Pingdom for alerts notifications
CrowdStrike Falcon Agent	Intrusion detection application that monitors for threat activity and alerts that there are security incidents. Next-Gen antivirus
Rapid7 Insight Agent	Vulnerability management
CloudWatch	Database performance monitoring application
*Datadog	Log aggregation tool utilized for monitoring and support
CloudFormation	Patch management for AMI
Docker	VM image management and deployment to AWS environment
Coverity / Sonarqube	Static application security Testing
Burpsuite	Dynamic application security testing

Primary Software	
Software	Purpose
Whitesource (Mend)	Software composition analysis
SgiSci	Runtime application self-protection
*Pagerduty	Incident response management
*Intercom Inc.	Business messaging, a way to chat with customers
*GainSight	Empowers companies to increase revenue, decrease customer churn, and drive advocacy
Atlassian Cloud	Jira, Confluence and Trello help teams organize, discuss, and complete shared work
Atlassian Marketplace	Platform for Atlassian customers to discover, try, and buy apps for Atlassian products
*Matomo	Open-source web analytics application to track online visits

*Indicates Subprocessors

Data

Data Required

- Jira site URL - customers use the Atlassian Marketplace to install the App into their Jira site.
- Geographical region - thus to indicate where their Test Runs attachments will be stored.
- Requirements, Test Case description and Test Steps.
- User consent (optional) - first name, last name, e-mail, company.

Collected Data

The data stored by Tricentis Test Management for Jira SaaS platform are:

- Test Runs, including:
 - Step result - passed/failed/blocked, etc.
 - Actual result description
 - Screen shots and attachments
 - Links to defects

VisionAI - Description of Services Provided

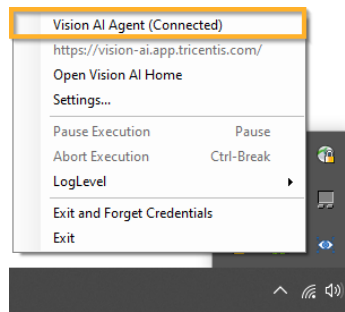
VisionAI is an AI-driven test automation technology that allows you to automate UI-based test cases, including cloud-native applications, remote desktop applications and even design mockups before any code is written, enabling you to test much earlier in the development lifecycle. VisionAI works just like the human eye and does not rely on the application's underlying technology to create test cases, which means you can use it to test virtually any application, regardless of technical expertise.

VisionAI Service Activation and License Management

VisionAI is a service provided alongside Tosca. All Tosca users will have access to VisionAI. As VisionAI is a cloud-based service, the requirements of activation require a separate license management process:

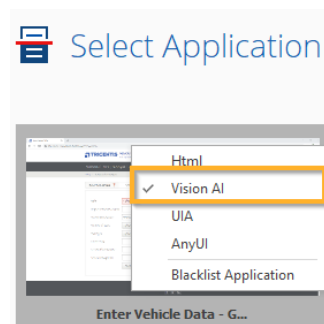
1. Install VisionAI agent along-side Tosca
2. Request VisionAI access via licensing service
3. Complete Registration and create a Tenant
4. Log in to VisionAI through the downloaded agent

The VisionAI Agent will be running and can be seen in the user's system tray.

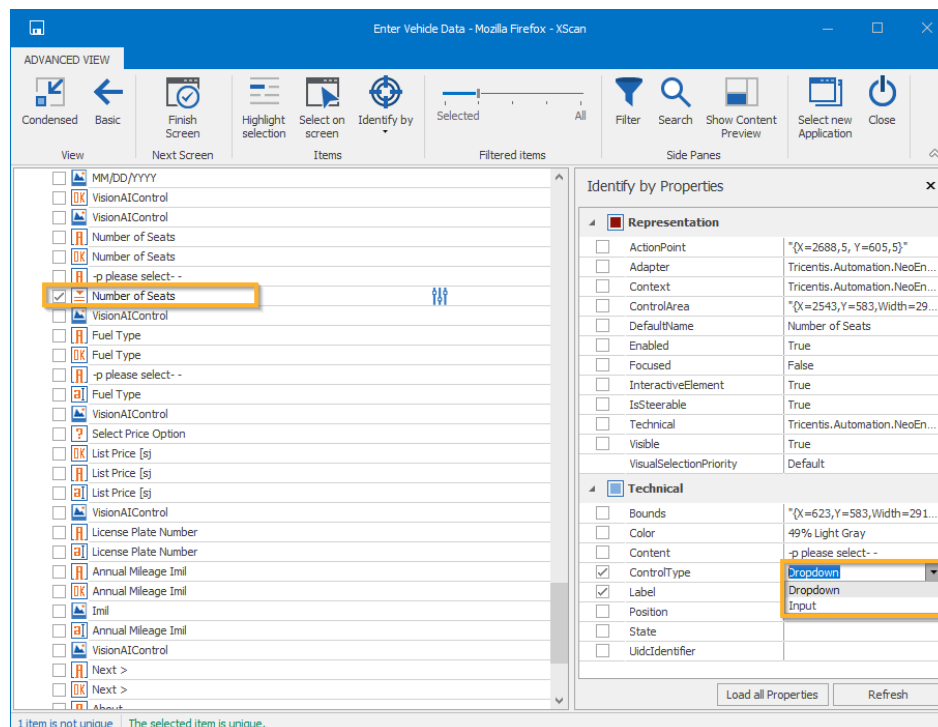


Authoring and Executing Tests Using VisionAI

1. Once you have logged into the Agent, you can start creating modules by scanning a page through VisionAI as shown in the screenshot below:



2. You can then select the controls needed for the test as shown in the screenshot below:



3. Once a Module is scanned using VisionAI, you can create a test case using the Module on Tosca and run it as normal.
4. Running the tests that use a VisionAI module will use the agent for control detection and steering on the selected UI.

VisionAI - System Requirements

Tricentis' AI-based test automation technology, VisionAI, is a cloud-based software as a service platform which is integrated with Tricentis Tosca, Tricentis' continuous testing platform. VisionAI can be independently updated in most instances without requiring onsite installations or upgrades to Tricentis Tosca. With more significant updates, however, the Tricentis Tosca integration may have to be updated but those updates are typically bundled with major Tricentis Tosca releases.

VisionAI - Components of the System

VisionAI Cloud Services

VisionAI is composed of several cloud-based services that are responsible for the various tasks involved in AI-based test automation. Neural networks used for control detection and optical character recognition form part of these services and are, in turn, consumed by other services performing various pre- and post-processing tasks.

VisionAI Agent

The VisionAI Agent is effectively an onsite service client which is bundled with Tricentis Tosca to allow integration with VisionAI's cloud services. Tricentis Tosca employs the VisionAI Agent to perform tests that are driven by the AI-based test automation technology provided by the VisionAI platform.

VisionAI Web Portal

VisionAI's web portal allows customers to sign up for VisionAI, configure preferences, manage test assets, and migrate data between different geographical regions. The portal also includes functionality for administrators to manage customer accounts and licensing concerns.

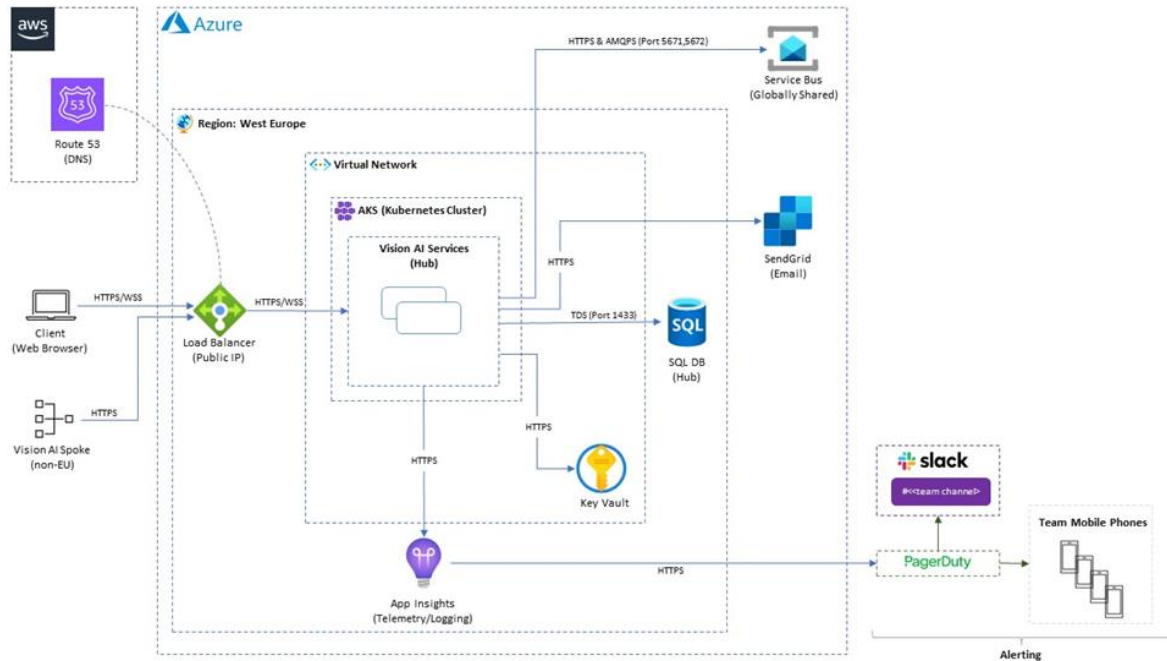
VisionAI can be used directly by users through the Tricentis Tosca desktop application or integrated into continuous integration (CI) pipelines by using Tricentis Tosca's built-in CLI tools and APIs.

Components of the System

The marketed SaaS AI-based test automation offer follows a hub-spoke design. Each spoke represents an instance of VisionAI in a geographical location where processing and related data storage takes place. The hub represents a component which is shared between various spokes and is responsible for maintaining shared data and configurations. Spokes retrieve the required shared data directly from the hub at startup after which any further changes to the shared data are received via messages propagated by a globally shared service bus.

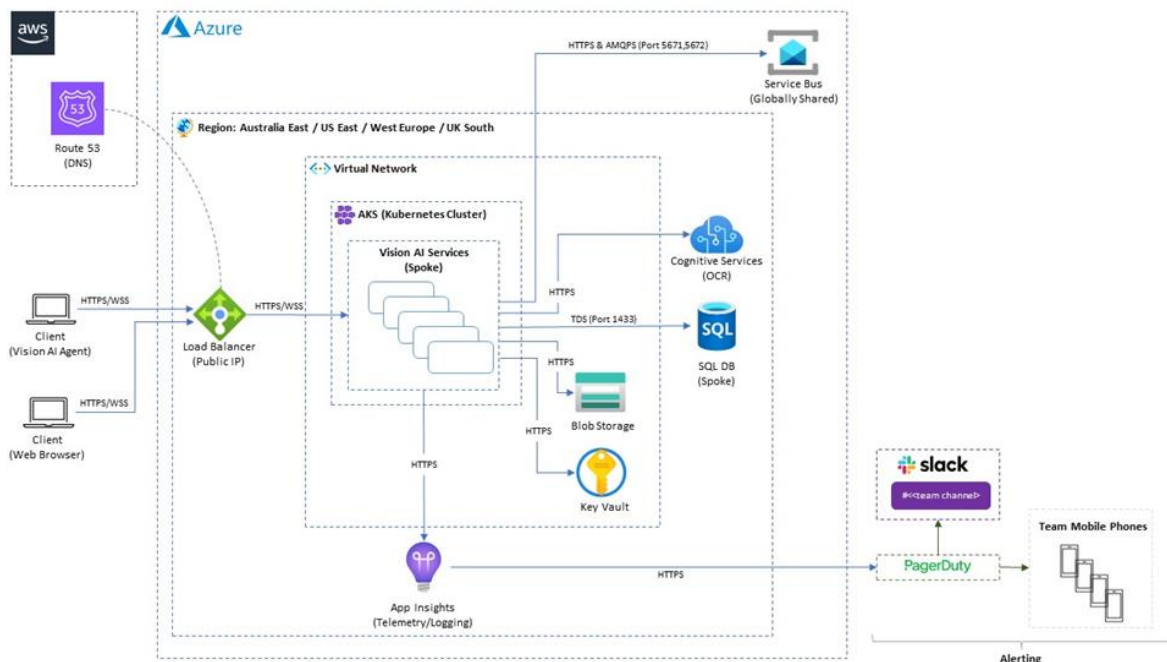
Component 1: VisionAI Hub (SaaS Platform Component)

The hub is responsible for centralized customer management, signups, tenancy (i.e., which spoke a tenant belongs to), and maintaining customer preferences. No test automation tasks are performed by the hub nor is any test-related data stored by the hub.



Component 2: VisionAI Spoke (SaaS Platform Component)

VisionAI spokes are responsible for performing the actual AI-based test automation which includes the required pre- and post-processing and storage of test-related data.



Infrastructure

Primary AWS and Azure components or services used to host the VisionAI SaaS platform:

Primary Infrastructure		
Services	Type	Purpose
DNS	AWS Route 53	Public DNS entries are managed by AWS Route 53. The DNS entries will resolve to the various Azure Public IPs associated with the different regions in which VisionAI is offered
Load Balancer	Azure Load Balancer	The Azure Load Balancer distributes incoming application traffic across multiple targets inside the Kubernetes cluster hosting the various application services
Containerized services: <ul style="list-style-type: none">VisionAI spoke services (front and backend services) [Australia East, East US, West Europe, UK South]VisionAI hub services (front and backend services) [West Europe]	Azure Kubernetes Services	Hosting of the primary application supporting the products and services described above. Fully managed Docker containerized micro services are orchestrated by Azure Kubernetes Services (AKS) with scaling support, Azure Identity and Access Management (IAM), and Azure Virtual Network (VNET) to enable monitoring, scaling, load-balancing, and fail-over capabilities for the application services
SQL (Hub and Spoke)	Azure SQL	Persistent SQL storage for the VisionAI platform
Blob Storage	Azure Storage Accounts	Private storage accounts for storing test-related assets referenced in the persistent SQL storage
Key Vault	Azure Key Vault	Securely stores application secrets and certificates used by the various application services
Cognitive Services	Azure Cognitive Services	Provides OCR detection capabilities that supplement internal neural networks
Service Bus	Azure Service Bus	Facilitates the synchronization of shared data hosted in the hub database between spokes in the various regions to ensure that each spoke has up to date data when changes are made to the shared data
Mailing System	SendGrid	The SendGrid subscription service is used to send e-mails relating to customer signups
Telemetry/Logging	Azure Application Insights and Azure Log Analytics	Provides logging, monitoring, alerting, and application-level telemetry

Software

Primary software integrations and other SaaS services used to provide Tricentis' SaaS includes the following:

Primary Software	
Software	Purpose
Pulumi	Patch management for Azure Resource Manager (ARM)
Docker	VM image management and deployment to Azure environment
Coverity / Sonarqube	Static application security testing
Mend	Software composition analysis
Pagerduty	Incident response management
Slack	Integrated with Pagerduty for alert notifications

Data

Data Security

Data is always transferred over a secured connection using HTTPS (TLS 1.2). Typically, sensitive data (e.g., screenshots, execution data) is only kept temporarily in memory, and not written to disk, except in the circumstances explicitly mentioned below.

Service Providers

The cloud components of the VisionAI solution are run on the Microsoft Azure platform and are operated by personnel at Tricentis. No third-party is involved in operating the service, except for the Azure OCR component (see below). Sensitive data (e.g., screenshots, execution instructions, test case data) cannot be accessed by either Tricentis or Microsoft personnel, as the data is only kept temporarily during processing. See below for more specifics on storage, transmission and processing of sensitive data.

Data Processing Region

The service is located in Azure's data centers. Each customer can specify where their data is stored and processed, currently available regions are:

- Europe (the Netherlands, with backup servers in Ireland)
- UK (London)
- USA (Washington)
- Australia (New South Wales)

Note that authentication and top-level customer settings are processed and stored in the European data centers.

Azure OCR

Some screenshots are processed by the Azure OCR service, when more precise recognition or recognition in languages other than English is required. This service is operated by Microsoft in the same data processing regions as the VisionAI service. Customer data is not retained by this service and is deleted after it has been processed.

Data Storage

The following table describes how each category of data is stored and processed in the VisionAI service. Note that enabling some features (e.g., Self-Healing) enables storage of certain data required for the feature to function. All such features can be disabled if desired so that no data is written to disk in the cloud.

Data Category	Description	Agent Machine	Cloud Nexus	AI Cluster	Azure OCR
Authentication Information	Authentication is performed using the OpenID Connect standard (built on OAuth2). Username and password credentials are exchanged for an access token, which is converted to a short-lived Bearer token. On the agent, a long-lived refresh token is also stored. The Bearer Token includes the user id, e-mail, tenant id, tenant name, and user group information.	Refresh Token, Access Token (Disk, Encrypted)	Bearer Token (Not stored)	Bearer Token (Not stored)	
Screenshots	Screenshots are transmitted to the Nexus server and AI Cluster but are never stored to disk. The screenshot is taken from the window being steered.	Screenshot Data (Memory)	Screenshot Data (Memory)	Screenshot Data (Memory)	Screenshot Data (Memory)
Control and OCR Data	The result of the screenshot processing (identified controls and text on screen). This is transmitted from the AI Cluster back to the Agent. *Optional Features: Self-Healing, Detection Caching	Control Data (Memory)	Control Data (Memory/Disk*)	Control Data (Memory)	Text Data (Memory)
User Identified Controls	The control definition is stored in the Nexus server database. *Optional Features: Control screenshot storage	N/A	Control Definition (Disk), Screenshot (Disk*)	N/A	N/A
Execution Data	Test steps, results, and logs are transmitted via the Nexus server from assistant to agent.	Execution Logs (Disk)	Execution Data (Not stored)	N/A	N/A

Data Category	Description	Agent Machine	Cloud Nexus	AI Cluster	Azure OCR
Telemetry	Telemetry data includes information about what operations are taking place, but not the content of those operations. The information stored includes user information, timestamps, counters, and operation names. Telemetry data is typically retained for 90 days.	Log files (Disk)	Telemetry (Disk)	Telemetry (Disk)	

Features Affecting Data Storage

Detection Caching

When re-running test cases, often the sequence of screenshots is identical from run to run. To save time running these screenshots through the neural networks every time, a hash code of the screenshot and the full detection result is stored. If an identical screenshot is detected, then the cached results are returned. This enhances the execution speed for repeated runs.

Enabling this feature enables storage of the detection results (Control and OCR Data) in the cloud (in your Azure data processing region).

Self-Healing

Self-healing enables a test case to recover when a control is not found, due to its properties being different since the last time the test case ran (e.g., renamed, different control type etc.). VisionAI stores previously successful detection results and analyzes these to determine what the new properties of the changed control should be. By analyzing the historical results, the most likely control can be identified, and the test case can continue.

Enabling this feature enables storage of the detection results (Control and OCR Data) in the cloud (in your Azure data processing region).

User Identified Control Screenshots

When reviewing User Identified Controls in the VisionAI configuration portal, being able to see an image of the defined controls enhances identifying which User Identified Control is which. A cropped screenshot of the control can be saved with the definition.

Enabling this feature enables storage of a cropped screenshot of the control in the cloud (in your Azure data processing region).

Tricentis Test Automation for Salesforce - Description of Services Provided

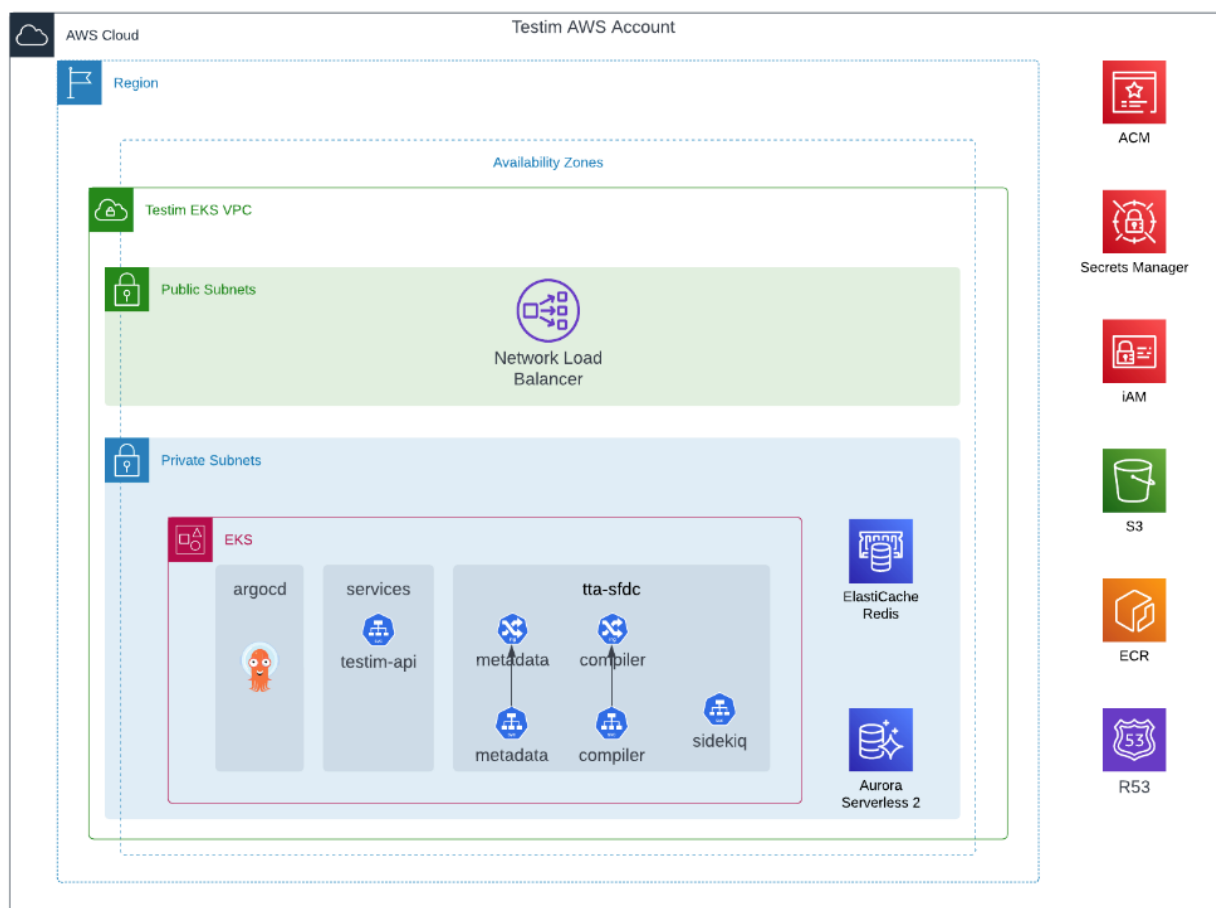
Tricentis Test Automation (TTA) for Salesforce (TTA for SFDC) is an automated no-code testing tool designed specifically for Salesforce professionals (testers, admins, developers, and architects) to help them easily create test cases and to then manage those tests. TTA SFDC has enhanced features for Salesforce testing including: 1) pre-built steps for fast test case creation, 2) connection to the customer's SFDC environment to quickly identify fields and objects when authoring tests, 3) a recorder for no-code test case creation, and 4) reports and dashboards to manage and evaluate test execution and results. It is a fully integrated part of Testim, a cloud-based SaaS Platform with separate license agreements.

TTA for SFDC - System Requirements

TTA for SFDC is a cloud-based, software-as-a service application. Hence no onsite installations or upgrades are required.

TTA for SFDC - Components of the System

TTA for SFDC is designed to operate as a part of Testim infrastructure. It is deployed in a separate namespace in the same AWS EKS cluster. Below diagram just highlights the major components of the TTA for SFDC. It is best to view this along with the architecture diagram of Testim suite to better understand all the components.



Infrastructure

Primary AWS components or services used to provide Testim SaaS application including TTA for SFDC:

Primary Infrastructure		
Services	Type	Purpose
Containerized services: <ul style="list-style-type: none">Testim web platform (backend services, US-WEST-2)	AWS EKS (Elastic Container Services)	Primary application supporting the products and service described above Fully managed Docker Containerized micro services and integrated with AWS EKS cluster, Auto Scaling Groups, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (VPC), to enable monitoring, scaling, load-balancing and fail-over of the services
Elastic Search	AWS open search service	Distributed, open-source search and analytics suite used for a broad set of use cases like real-time application monitoring, log analytics, and website search
Mailing System	Mandrill	Mailchimp add-on service to send e-mails
VPC Peering	AWS VPC peering	A VPC peering connection is a networking connection between two Virtual Private Clouds that enables you to route traffic between them
SSO	Azure, Okta	Used for connecting to customer SSO provisioning
Amazon Service Simple Storage Services (S3)	AWS S3	Private bucket for cloud load generation service settings storage Object storage service that provides scalability, data availability, security, and performance for attachments received in Testing Services communications
Cloud Atlas MongoDB	Atlas MongoDB	Persistent storage service for the main business services exposed
Application Load Balancer (ALB) Network Load Balancer (NLB)	AWS ALB and NLB	ALB and NLB that distribute incoming application traffic across multiple targets; Amazon Service EC2 instances, containers, and IP addresses. TLS1.2 Forward Secrecy Policies
Web application firewall	AWS WAF	Security system that controls incoming and outgoing traffic for applications and websites
DNS provider	External to AWS (CloudFlare)	Route end users to Internet applications by translating web address names (www) into the numeric IP addresses to connect to Amazon Service EC2 instances, Application Load Balancers

Primary Infrastructure		
Services	Type	Purpose
CloudTrail	AWS CloudTrail	Log, continuously monitor, and retain account activity related to actions across AWS infrastructure. CloudTrail logs event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. Provides file integrity monitoring (FIM) within the AWS infrastructure This service is leveraged for file integrity management also (pointing to the YAML based configuration files)
Redis	AWS ElastiCache Redis	TTA for SFDC specific caching for better performance. This is an AWS managed service
Postgresql	Aurora Serverless V2	TTA for SFDC specific Data storage. This is an AWS managed service
Container Repository	AWS ECR	AWS managed container image repository service

Software

Primary software integrations and other SaaS services used to provide Tricentis' SaaS includes the following:

Primary Software	
Software	Purpose
Slack	Integrated to Pingdom for alerts notifications
CrowdStrike Falcon Agent	Intrusion detection application that monitors for threat activity and alerts that there are security incidents. Next-Gen antivirus
Rapid7 Insight Agent	Vulnerability management
CloudWatch	Database performance monitoring application
CloudFormation	Patch management for AMI
Docker	VM image management and deployment to AWS environment
Coverity / Sonarqube	Static application security Testing
Whitesource	Software composition analysis
Terraform	Managing AWS environment
Coralogix	Logging and monitoring

Data

Data Required

- Salesforce test environment connectivity information
- TTA for SFDC License, and current usage of the License
- Configuration settings related to the usage of TTA for SFDC SaaS platform: preferred language, charts
- User profile (first name, last name, e-mail, API tokens) and authentication data

Collected Data

The data stored by TTA for SFDC:

- Salesforce Test environment configurations
- Test results, including:
 - Overview information (summary and key indicators)
 - Statistics for each User Path element (min., average, count, error count, etc.)
 - Statistics for the monitored infrastructure (e.g., CPU load for machine X)
 - Errors, including the response of the server related to the error
 - Request URLs, server's hostname or IP addresses used in the test projects

Testim - Description of Services Provided

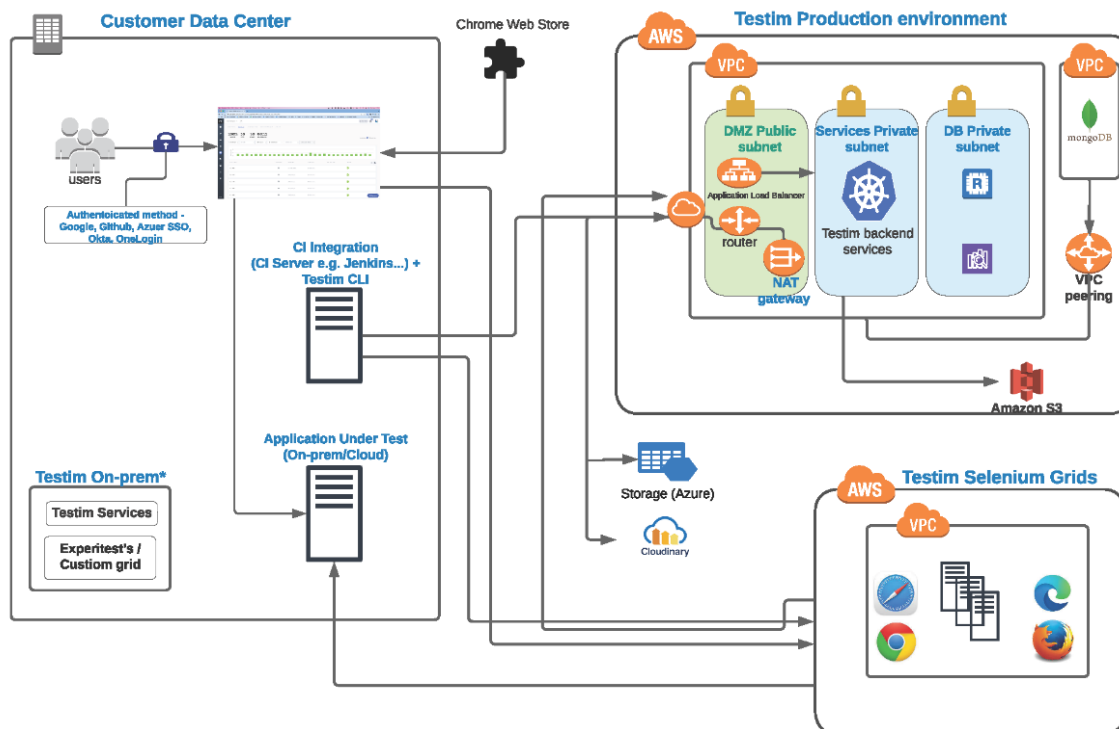
Testim simplifies and automates functional testing of web applications - a task that was previously either manual or required extensive coding and maintenance. The Testim Platform is cloud-hosted Software as a Service (SaaS) where users, primarily Software Developers and Quality Assurance Engineers, create tests they can run against their web applications to validate the software is functioning as intended. Testim uses AI to make it easy to write and maintain stable tests, enabling users to shift testing earlier in the development process and detect defects when they are cheaper and easier to fix. Testim integrates with other software development tools used for source control, continuous integration, collaboration, and browser testing to help streamline development workflows:

1. **Testim Platform** - The Testim Platform helps users create and automate tests that validate the functionality of web applications. Software tests are easily authored by recording user flows in web applications or by coding tests that represent user actions. Once created the tests can be fully customized to match nearly any web application experience by adding validations, conditions, configurations, or inserting data or custom code. The Testim Platform uses artificial intelligence to help make tests more resilient, reducing maintenance effort.
2. **Test Grid** - Tests can be triggered from the Testim Platform, CLI command, or through integration with a Continuous Integration (CI) system. Tests are run in parallel on the Testim Grid to simulate multiple browser types, screen resolutions, and configurations, accelerating test completion and shortening release cycles. In addition to the Testim Test Grid, customers can run their tests on third-party testing services.
3. **Testim Bug Capture** - Testim Bug Capture allows users to quickly document a web application behavior with video, screenshots, and the test steps to recreate the behavior. The user can add annotations or text to help highlight aspects of the behavior, such as a software defect. Bug Capture can be integrated with third-party bug management tools to simplify reporting.

Testim - System Requirements

Testim is a cloud-based, software-as-a service application, so no onsite installations or upgrades are required.

Testim - Components of the System



Infrastructure

Primary AWS components or services used to provide Testim SaaS application:

Primary Infrastructure		
Services	Type	Purpose
Containerized services: <ul style="list-style-type: none"> Testim web platform (backend services, US-WEST-2) 	AWS EKS (Elastic Container Services)	Primary application supporting the products and service described above Fully managed Docker Containerized micro services and integrated with AWS EKS cluster, Auto Scaling Groups, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (VPC), to enable monitoring, scaling, load-balancing and fail-over of the services
Elastic Search	AWS open search service	Distributed, open-source search and analytics suite used for a broad set of use cases like real-time application monitoring, log analytics, and website search
Mailing System	Mandrill	Mailchimp add-on service to send e-mails
VPC Peering	AWS VPC peering	A VPC peering connection is a networking connection between two Virtual Privates Clouds that enables you to route traffic between them

Primary Infrastructure		
Services	Type	Purpose
SSO	Azure, Okta	Used it for connecting to customer SSO provisioning
Amazon Service Simple Storage Services (S3)	AWS S3	Private bucket for cloud load generation service settings storage Object storage service that provides scalability, data availability, security, and performance for attachments received in Testing Services communications
Cloud Atlas MongoDB	Atlas MongoDB	Persistent storage service for the main business services exposed
Application Load Balancer (ALB) Network Load Balancer (NLB)	AWS ALB and NLB	ALB and NLB that distribute incoming application traffic across multiple targets; Amazon Service EC2 instances, containers, and IP addresses. TLS1.2 Forward Secrecy Policies
Web application firewall	AWS WAF	Security system that controls incoming and outgoing traffic for applications and websites
DNS provider	External to AWS (CloudFlare)	Route end users to Internet applications by translating web address names (www) into the numeric IP addresses to connect to Amazon Service EC2 instances, Application Load Balancers
CloudTrail	AWS CloudTrail	Log, continuously monitor, and retain account activity related to actions across AWS infrastructure. CloudTrail logs event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. Provides file integrity monitoring (FIM) within the AWS infrastructure This service is leveraged for file integrity management also (pointing to the YAML based configuration files)

Software

Primary software integrations and other SaaS services used to provide Tricentis' SaaS includes the following:

Primary Software	
Software	Purpose
Slack	Integrated to Pingdom for alerts notifications
CrowdStrike Falcon Agent	Intrusion detection application that monitors for threat activity and alerts that there are security incidents. Next-Gen antivirus

Primary Software	
Software	Purpose
Rapid7 Insight Agent	Vulnerability management
CloudWatch	Database performance monitoring application
CloudFormation	Patch management for AMI
Docker	VM image management and deployment to AWS environment
Coverity / Sonarqube	Static application security Testing
Whitesource	Software composition analysis
Terraform	Managing AWS environment
Coralogix	Logging and monitoring
ArgoCD	declarative, GitOps continuous delivery tool for Kubernetes
GitHub	Source Code Management

Data

Data Required

- Git access in case of the connection between Testim and a customer GIT repository
- User profile (first name, last name, e-mail) and authentication data
- access to personal information in databases is restricted to authorized Testim personnel including help desk personnel

Collected Data

The data stored by Testim SaaS platform are:

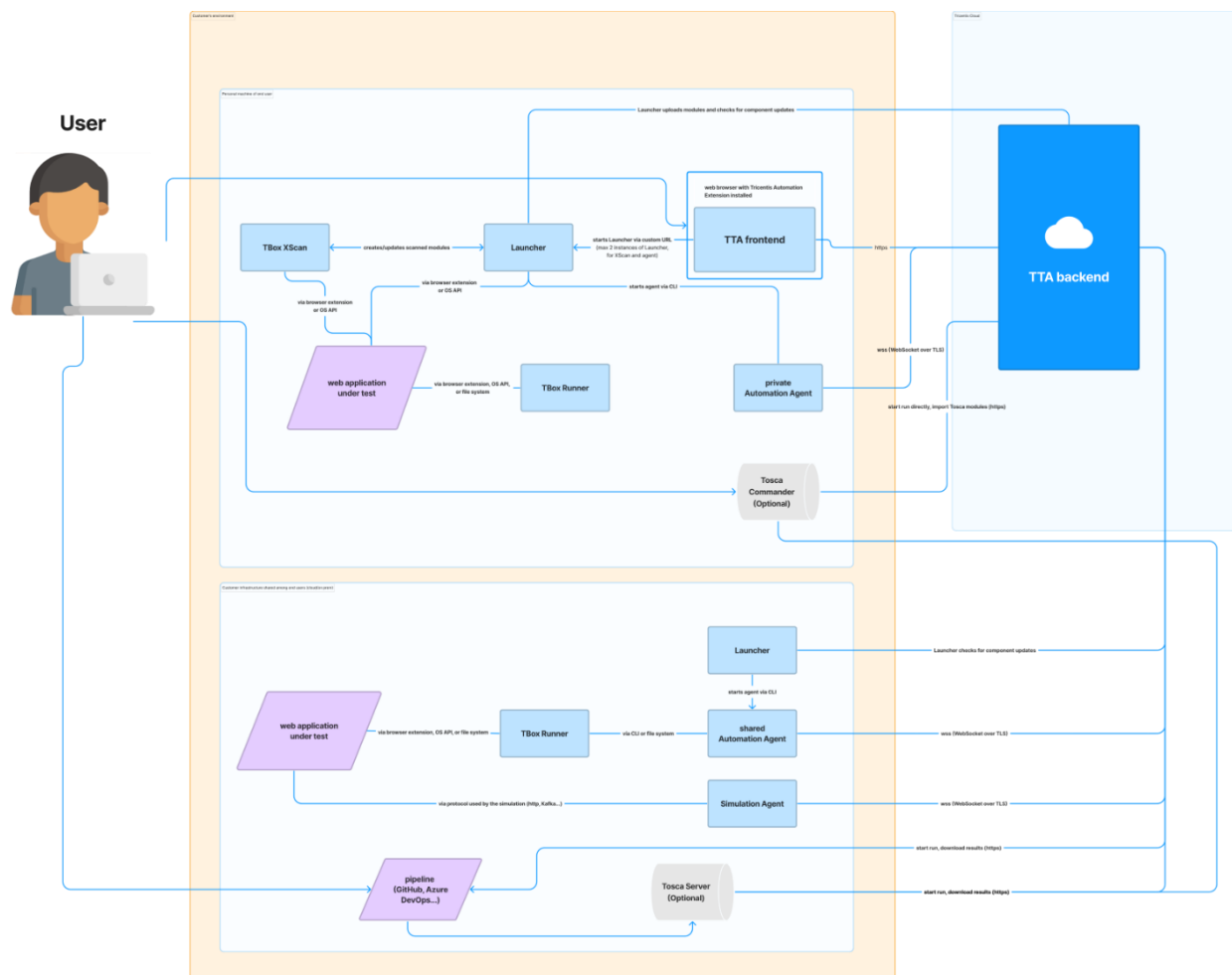
- Test results, including:
 - Screenshots and/or HTML files generated during test execution, to provide debugging tools for software development companies
 - Maintains personal information as part of test-results metadata and screenshots (e.g., visual screenshots and HTML files) that might have been captured during the recording of test results
 - Network logs

Tricentis Test Automation - Description of Services Provided

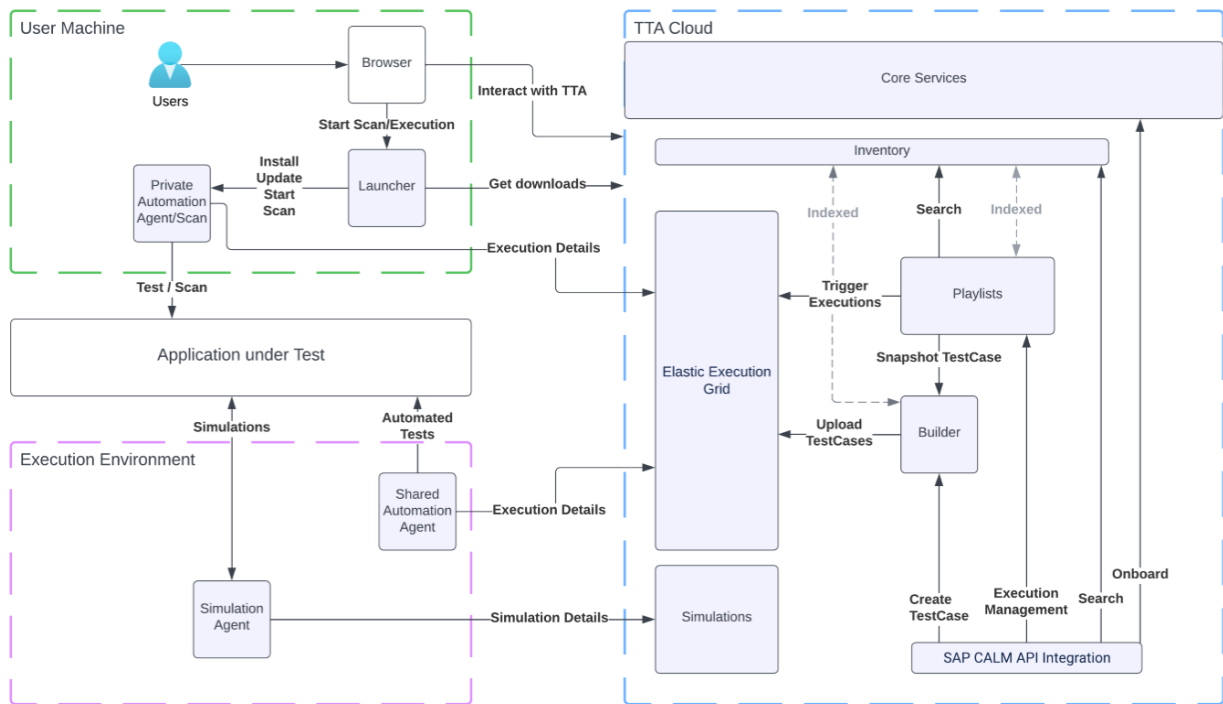
Tricentis Test Automation is a cloud-based toolkit that helps you automate end-to-end testing of your web applications. The core functionality is to automatically scan your web application and enable you to create modules. These modules then serve as reusable building blocks for your test cases. You can run your tests privately or in shared environments. You can also use a simulation feature to mock any service that you need for your tests.

The core of the Tricentis Test Automation (TTA) technology is the ability to automatically scan the HTML code structure of a web application and create reusable modules from that structure. These modules become the building blocks of your test cases, along with predefined and shared actions.

Users can group multiple test cases into playlists, which are handled and executed by an Automation Agent. You can run your tests locally with a private Automation Agent, or with a shared Automation Agent in dedicated environments, such as remote or virtual machines.



Services	Description
Core	Core components shared in all other services.
Inventory	Inventory of all test artifacts. Is used for searching and listing all test relevant objects.
Builder	Used for building Testcases.
Playlist	Used for collecting Testcases and executing them by sending the package to E2G.
Elastic Execution Grid (E2G)	Runs an execution package distributed on Agents via TBox execution engine.
Simulations	Used to simulate services for testing purposes.
SAP Integration	Integration interface to SAP. SAP CALM calls these services to integrate TTA. This mainly does transformation logic to map the SAP Domain to the TTA Domain.



Tricentis Test Automation - System Requirements

These requirements apply to the machines you will use for your work: to access Tricentis Test Automation (TTA), to create tests, and to run them. They serve as general guidance in case you are experiencing problems. To learn more about how the product works and what component it uses, check the architecture diagram.

Compatibility with Tricentis Tosca

Tricentis Tosca and Tricentis Test Automation use the same browser extension, so if you plan to use both products, please make sure you are using Tricentis Tosca 15.2 Patch 4 or newer to avoid compatibility issues.

Older versions of Tosca can be used too, but for an earlier version than Tosca 15.2, please make sure that the TOSCA Automation Service process is not running in the background before working with Tricentis Test Automation.

Hardware:

- CPU: i5 Dual-Core 2.4 GHz
- RAM: 8 GB
- Hard disk space: 10 GB
- Network: 100 Mbit/s

Software:

- .NET 6 installed

Operating System:

- Windows 10 and Windows 11, versions that support .NET 6 64-bit recommended.
- OS versions compatible with .NET 6.

Note: Tricentis Test Automation can be used on Mac machines with very limited functionality; features that require local components, such as scanning or running a test on a private agent, are not available yet.

Web Browser:

- Google Chrome

Tricentis Automation Extension for Chrome installed. The extension is not public, so you cannot find it in Chrome Web Store; instead, you will be offered to install it when you first scan your application.

For Automation Agents:

- To create recordings of failed test runs, the agent machine must have Windows Media Features installed.

For Simulations:

- Any OS version compatible with .NET 6.
- The Simulator Agent machine must be able to establish an outbound HTTP connection via WebSocket.

Tricentis Test Automation - Components of the System

Infrastructure

Primary AWS components or services used to provide Testim SaaS application:

Primary Infrastructure		
Services	Type	Purpose
Containerized services: <ul style="list-style-type: none">• Testim web platform (backend services, US-WEST-2)	AWS EKS (Elastic Container Services)	Primary application supporting the products and service described above Fully managed Docker Containerized micro services and integrated with AWS EKS cluster, Auto Scaling Groups, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (VPC), to enable monitoring, scaling, load-balancing and fail-over of the services
Elastic Search	AWS open search service	Distributed, open-source search and analytics suite used for a broad set of use cases like real-time application monitoring, log analytics, and website search
Mailing System	Mandrill	Mailchimp add-on service to send e-mails
VPC Peering	AWS VPC peering	A VPC peering connection is a networking connection between two Virtual Private Clouds that enables you to route traffic between them

Primary Infrastructure		
Services	Type	Purpose
SSO	Azure, Okta	Used for connecting to customer SSO provisioning
Amazon Service Simple Storage Services (S3)	AWS S3	Private bucket for cloud load generation service settings storage Object storage service that provides scalability, data availability, security, and performance for attachments received in Testing Services communications
Cloud Atlas MongoDB	Atlas MongoDB	Persistent storage service for the main business services exposed
Application Load Balancer (ALB) Network Load Balancer (NLB)	AWS ALB and NLB	ALB and NLB that distribute incoming application traffic across multiple targets; Amazon Service EC2 instances, containers, and IP addresses. TLS1.2 Forward Secrecy Policies
Web application firewall	AWS WAF	Security system that controls incoming and outgoing traffic for applications and websites
DNS provider	External to AWS (CloudFlare)	Route end users to Internet applications by translating web address names (www) into the numeric IP addresses to connect to Amazon Service EC2 instances, Application Load Balancers
CloudTrail	AWS CloudTrail	Log, continuously monitor, and retain account activity related to actions across AWS infrastructure. CloudTrail logs event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. Provides file integrity monitoring (FIM) within the AWS infrastructure This service is leveraged for file integrity management also (pointing to the YAML based configuration files)

Software

Primary software integrations and other SaaS services used to provide Tricentis' SaaS includes the following:

Primary Software	
Software	Purpose
Okta	Identity Provider
Mongo Atlas	User data storage
SendGrid	E-mail service

Primary Software	
Software	Purpose
Gainsight PX	Activity Tracking of Users in the Frontend
M3ter	Handle Limits
Launch Darkly	Feature Flag Solution
Microsoft Azure	Infrastructure hosting platform
Azure DevOps	Code Repository and CI/CD tool
PagerDuty	Application Availability monitoring and notifications
Slack	Integrated to Pagerduty and Azure DevOps for notifications
CrowdStrike - Falcon Agent	Intrusion detection application that monitors for threat activity and alerts that there are security incidents. Next-Gen antivirus
Rapid7 Insight Agent	Vulnerability management
Coverity / Sonarqube	Static application security Testing
Burpsuite	Dynamic application security testing
Whitesource	Software composition analysis

Data

Data Required

- User profile (first name, last name, e-mail, role, status, API tokens) and authentication data
- User preferences (custom filters, favorites)
- User license, current usage of license

Collected Data

The data stored by the TTA platform are:

- Tests, Test management data (test cases, modules, shared actions, simulation files, simulation/automation agent connection information, playlists)
- Agent screenshots
- Test results: summary, videos, logs

Principal Service Commitments and System Requirements

Tricentis designs its processes and procedures related to the qTest, TTA, Testim, VisionAI, TTA for SFDC and TTM for JIRA products to meet the compliance and security objectives that apply to the qTest, TTA, Testim, VisionAI, TTA for SFDC and TTM for JIRA testing services. Those objectives are based on the service commitments that Tricentis makes to user entities, the laws and regulations that govern the provisioning of qTest, TTA, Testim, VisionAI, TTA for SFDC and TTM for JIRA services, and the financial, operational, and compliance requirements that Tricentis has established for the services. The qTest, TTA, Testim, VisionAI, TTA for SFDC and TTM for JIRA testing services of Tricentis are subject to the security and privacy requirements state privacy security laws (Ex: GDPR, Australia Privacy Act, US States Privacy Laws, PIPEDA) and regulations in the jurisdictions in which Tricentis operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the qTest, TTA, Testim, VisionAI, TTA for SFDC and TTM for JIRA services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

Encryption technologies are used to protect customer data both at rest and in transit.

Tricentis establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Tricentis' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the qTest, TTA, Testim, VisionAI, TTA for SFDC and TTM for JIRA services.

People

Tricentis has a staff of approximately:

- 70 employees supporting qTest Application
- 50 employees supporting Tricentis VisionAI
- 15 employees supporting Tricentis Test Management for Jira
- 50 employees support Tricentis Test Automation for Salesforce
- 50 employees support Testim
- 50 employees support Tricentis Test Automation

Organized in the following functional areas:

- **Corporate:** Executives, senior staff, and company administrative support staff, such as legal, security and compliance, accounting, finance, business development and human resources. These individuals monitor the Tricentis SaaS Services primarily as a tool to measure product performance at an overall corporate level. This includes reporting done for internal metrics as well as for Tricentis' user entities:
 - The information security and compliance staff support the Tricentis SaaS Services indirectly by monitoring internal and external security threats and maintaining current antivirus software
- **Customer Success Operations:** Staff that administer the Testing Services. They provide the direct day-to-day services, such as customer administrative account setup, additional services provided as standard for product/platform in scope:
 - Customer Success representatives manage the onboarding process directly with customers. The onboarding process consists of a series of meetings with the Customers' Administrative user, and any additional team members required to set-up and configure the Testing Capabilities
 - Professional Services set up and support the customer's custom integrations to the Tricentis platform and Testing Services when contracted
 - Customer Support engineers provide support and issue resolution from basic level issues up to escalations to engineering for 3rd and 4th level support

- *Product Engineering, CloudOps*: Testing Services application development and advanced application support. AWS IaaS administration and AWS CloudOps User and Infrastructure administration:
 - The engineering staff develops and maintains the Tricentis Testing Services application and web UI. This includes the Testing Services conversation logic, supporting services and supporting utilities, and the external website that allows users to configure, operate, and report on the Testing Services activity. The staff includes application developers, application quality assurance, and engineering pipeline team. A senior engineer will deploy the releases of the Testing Services application and related services into the production environment
 - The CloudOps team manages the infrastructure, AWS IaaS networking, and systems administration and has no direct access to the Testing Services application. Rather, the team administers the Tricentis' AWS IaaS, which hosts Tricentis' application and web UI
- *Security Operations, Product Security, IT*: General security operations support and threat monitoring. IT help desk, IS hardware, office networking and security, and IT operations:
 - The SecOps staff supports the Tricentis Testing Services indirectly by monitoring internal and external security threats within the AWS infrastructure. This monitoring includes CVE and patch management that require immediate remediation following both Tricentis' incident management policy and change management policy, as well as, responding to immediate threats detected and routed to Tricentis' alert system
 - The Product Security team ensures privacy by design and security by design are in place for the Testing Services application, complete threat modeling, security application scanning (SAST, DAST, Penetration Testing, Open-Source Libraries) is performed, and manages the external annual third-party Penetration Tests are performed. Additionally, the Product Security team support Product Engineering in vulnerability confirmation, resolution, and rescanning to confirm vulnerabilities are mitigated or fully resolved to an acceptable risk level
 - IT operations maintain antivirus software and inventory of IT assets (laptops) and assigning access to the internal Tricentis Testing Services administrative dashboard based on the personnel's role and responsibility in response to manager's tickets for new hires, or changes to access based on a change in role, job description, or termination. IT personnel also manage user administration applications for business applications, network hardware and security monitoring of office networks, and telecom support

Limitations of Data (Restrictions from Tricentis Terms and Conditions)

It is under Customer's sole discretion and Tricentis has no control over the nature, scope, or origin of, the data processed by the Tricentis Products and Customer shall have sole responsibility for the adequacy, relevancy, accuracy, quality, and legality of it. Customer shall not use any Personal Data in connection with, to input into and process while using Tricentis Products. In no event shall Customer use sensitive Personal Data, such as information on health, sexual orientation, political orientation, race, etc. Unless a data processing agreement ("DPA") is executed, neither Party authorizes any exchange, use or processing of other Personal Data (other than Contact Data). Notwithstanding the foregoing, if a party requests a DPA to regulate the processing of Personal Data, the DPA shall be deemed an appendix Tricentis Terms and Conditions.

Components of the System

Processes, Policies and Procedures

Information security policies and procedures define key roles and responsibilities, risk management, and design principles. Management has direct responsibility to review these controls and complete all required activities to enforce the controls across the organization. Tricentis adheres to the following core security principles:

- Fulfill its obligations towards the security of customer data against threats and against unauthorized disclosure, access, or use of customer data

- Ensure employees, both permanent and temporary, comply with policies and procedures, also fulfilling its obligations towards the security of customer data (with least privilege access as the guiding principle)

Physical Security

The in-scope systems and infrastructure that supports Tricentis are hosted by AWS. AWS is responsible for the physical controls around Tricentis in-scope systems and infrastructure.

Logical Access

Documented standard build procedures are utilized for deployment of production servers. The production systems, including production servers, databases, application, and web application firewall (WAF), and backup systems, are configured to authenticate users via unique user accounts and require two-factor authentication or Encrypted Secure Shell (SSH). Password controls such as minimum length, password history, password complexity, and account lockout settings are in place to reduce the risk of unauthorized activity.

Virtual Private Network (VPN) connections in combination with Tricentis' single sign on (SSO) application and key passphrase for administrators are required to establish remote access to production servers. Tricentis users generate their own SSO password and are responsible for maintaining the security of their access credentials. Administrative access to the production systems is restricted to authorized personnel. The production systems are configured to log access related events and monitor system resources for availability using third-party tools. The tool is configured to send automated alerts to CloudOps and Security when predefined events occur.

Management has established security controls to ensure that access to production systems is limited to those who require access based on a business need based on a least privilege model. A formal provisioning process has been established for managing user accounts and controlling access to Tricentis resources within the production environment. New employees are granted standard levels of access based on their job role. New hire checklists are used to guide the onboarding process and manager-requested access. Prior to granting an individual access above the standard level of access provided upon employment, the background check for the personnel must be approved by Human Resources.

Upon voluntary or involuntary termination of an employee, a termination checklist is used to track and guide the termination process and help ensure the terminated user's access is removed and/or disabled upon the individual's departure from the organization.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Tricentis monitors capacity utilization of compute services to ensure that service delivery matches service level agreements. Tricentis evaluates the need for additional capacity in response to growth of existing customers and/or the addition of new customers.

Tricentis has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Tricentis system owners review proposed operating system patches to determine whether the patches are applied. Customers and Tricentis systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Tricentis staff validate that all patches have been installed and if applicable that reboots have been completed. If patches require any downtime that will impact Customers, notifications are sent to Tricentis Customers by the Customer Success team as required per Tricentis' Business Continuity Procedure.

Change Control

Tricentis maintains documented application and infrastructure change management policies and procedures to communicate expectations regarding the change management process to Tricentis personnel, and to ensure any unauthorized changes are not made to production systems. The change management process adds oversight, visibility, and control of changes to the Tricentis systems environment. These changes may impact systems, applications, systems software, hardware, network, or any other aspect of the information processing environment. Source code is stored within a version control system that allows for the rollback of application source code and restricts access to authorized personnel.

Changes follow a formal approval process prior to implementation. Changes to hardware, operating systems, and system or application software are authorized, tested when applicable, and approved by senior developers or management personnel prior to implementation. Changes to system infrastructure and system or application software are developed and tested in separate development or test environments before being implemented into production. Automated controls are in place to enforce changes by peer reviewed and pass automated testing procedures prior to being merged into the master branch. The ability to implement changes into the production environment is restricted to authorized Development or CloudOps personnel. Change management personnel involved in approving change requests document change approvals in the Continuous integration (CI) and continuous delivery (CD) application for each release. Changes to the system are formally documented in Jira and/or GitHub.

Data Communications

Firewall or WAF are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall or WAF is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, WAF, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Independent Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Tricentis. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by Product Security within the CI/CD pipeline with each major release in accordance with the Tricentis Policy. The Product Security team uses industry standard scanning technologies and a formal methodology specified by Tricentis. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are typically performed during non-peak windows. Tools requiring installation in the Tricentis system are implemented through the change management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system through the Internet through the use of leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services System, the development, sales, and support of which are performed in the Austin, Texas and Atlanta, Georgia, United States, Pune, India, Vienna, Austria, Brno, Czech Republic, Sydney, Australia, Lodz, Poland and Prague, Czech Republic offices.

This report does not include the cloud hosting services provided by AWS and Azure in the US-North-East-2 (US Customers) and EU-2 (EU and APAC customers) regions.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common Criteria/Security and Availability criteria were applicable to the qTest, Testim, VisionAI, Tricentis Test Automation, TTA for SFDC, TTM for Jira Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS and Azure in the us-east-1, us-east-2, us-west-1 (US Customers) and eu-west-1 (EU) ap-southeast-1 (APAC customers) regions.

Subservice Description of Services

AWS and Azure provide cloud hosting services for the Tricentis SaaS qTest, TTA, Testim, VisionAI, TTA for SFDC and TTM for JIRA services System and manages all physical and environmental security controls.

Complementary Subservice Organization Controls

Tricentis' services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Tricentis' services to be solely achieved by Tricentis control procedures. Tricentis assesses all subservice organizations to ensure that they establish their own internal controls or procedures to complement those of Tricentis.

The following subservice organization controls are implemented by AWS and Azure to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	Criteria	Control
Common Criteria / Security, Availability	CC6.4 CC7.2 A1.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems (IPS) are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	CC6.5 A1.2	AWS provides customers with the ability to delete their content. Once successfully removed the data is rendered unreadable.
		AWS retains customer content per customer agreements.
		AWS provides customers with the ability to delete their content. Once successfully removed the data is rendered unreadable.
		The design of systems is sufficiently redundant via multi-region availability zones to sustain the loss of a data center facility without interruption to the service.

Subservice Organization - Azure		
Category	Criteria	Control
Common Criteria / Security	CC6.4	PE - 1. Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		PE - 2. Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		PE - 3. Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		PE - 4. Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		PE - 5. The datacenter facility is monitored 24x7 by security personnel.

Subservice Organization - Azure		
Category	Criteria	Control
Availability	A1.2	PE - 6. Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		PE - 7. Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		PE - 8. Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		DS - 5. Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		DS - 6. Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		DS - 7. Customer data is automatically replicated within Azure to minimize isolated faults.
		DS - 8. Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		DS - 9. Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.
		DS - 11. Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		DS - 13. Production data is encrypted on backup media.
		DS - 14. Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

Tricentis management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Tricentis performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Tricentis' services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Tricentis services to be solely achieved by Tricentis control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Tricentis'.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Tricentis.
2. User entities are responsible for notifying Tricentis of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Tricentis services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Tricentis services.
6. User entities are responsible for providing Tricentis with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Tricentis of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.