Virtuoso

Document

Technical Overview

Jan 5, 2023

Virtuoso

Document

Virtuoso

Document

General Disclosure

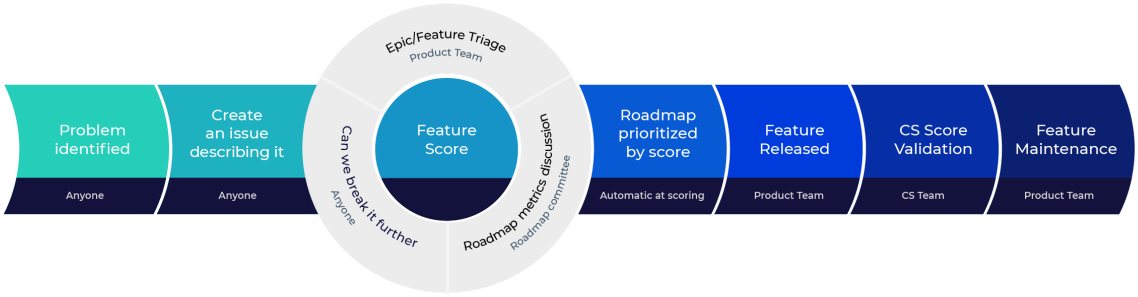
Virtuoso is a SaaS (Software as a Service) provider for an intelligent test automation platform dedicated to safe security practices. Please note that the details listed in this document may have changed since the document was last published. Get in touch for the latest information.

Product Lifecycle Processes

Software Development Lifecycle (SDLC)

The Virtuoso team develops software with an Agile process that uses 2-month, short-term milestones, and 2-week development sprints. Team members can then share their interest in roadmap items, and teams form around those items. Changes are shipped frequently to production, and engineers can simply flag them when they are confident about the feature with full autonomy. Anyone in the company can place items on the roadmap backlog.

Roadmap & New Product Management



Our roadmap process starts with anyone being able to first identify a problem and then create an issue describing the problem. Then there is a three-pronged approach to the “feature score” where anyone can test if they can break it further, the product team focuses on an epic/feature triage, and the roadmap committee discusses the metrics. The roadmap is then automatically prioritized through the feature scoring method, which has criteria with different weights. There is requirement risk, value to the customer, risk mitigation, cost/effort risk, and effort estimation to release MVP. Then, the product team releases the feature, the customer success team does the score validation, and finally, the product team maintains the feature.

Software Release Cycle

Virtuoso has a continuous release model where changes are deployed to test environments as soon as code changes are created. We are currently aiming for a complete, continuous deployment

model where changes will be deployed to production as and when they happen. Feature toggles are used to turn features on or off on demand so the user can customize their experience.

Information Security Management Practices

All Virtuoso employees are fully trained, vetted, have the required certifications, and have signed non-disclosure agreements.

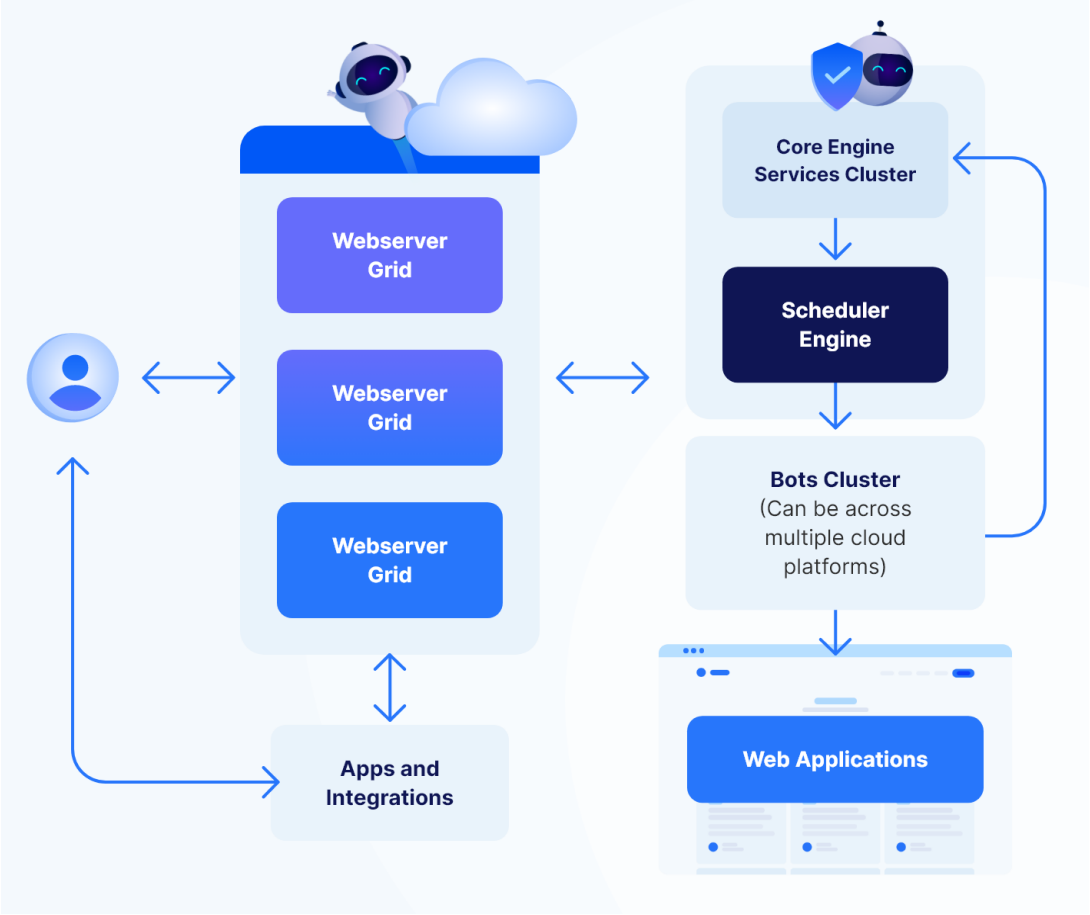
Information Security Management policies and procedures have been developed and include administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Senior executives and management fully support and enforce initiatives for following information security best practices.

Our engineering team ensures that security is built in throughout the entire development process. Autonomous environments are maintained for Development, Staging, and Production. All software releases are performed using our CI/CD toolchain under the control of the development team.

Platform Architecture & Security Controls

Architecture Overview

Virtuoso is a SaaS platform solution. Auto-scaling workloads aim at growth efficiency, while the platform has a core service-based distributed application architecture. It is extensible through a service-oriented architecture for apps and integrations.



Technology Stack

The following technologies are used as part of Virtuoso's tech stack:

- **Distributed architecture**: Java services
- **Core application**: Java 11, Typescript / Javascript (ES6+) / Node.js, Go, Python
- **Front-end**: Vue ecosystem
- **Relational database**: PostgreSQL
- **Infrastructure**: AWS (ECS, S3, CloudFront, ALB, Lambda, SQS, etc.) and K8S
- **Infrastructure management**: Terraform
- **Metric monitoring**: Prometheus
- **Logging**: DataDog
- **Error tracking**: Sentry
- **Source control and product management**: Github
- **CI / CD**: CircleCI
- **UI / UX**: Figma

Virtuoso is always looking out for the latest technologies. Our tech stack may expand, so we'll be sure to keep this list updated.

Cloud Hosting

Virtuoso's platform is deployed via AWS and hosted in the EU. AWS is responsible for the secure provision of compute instances that we use to provide the Virtuoso service, as well as the physical security of the infrastructure. Within the shared responsibility model between Virtuoso and AWS, Virtuoso is responsible for security at and above the network layer. Virtuoso is deployed within a virtual private cloud, using security groups to segregate different services on the principle of least access. Direct access to the network is only available for users with an approved account on a bastion host. All other ingresses into the Virtuoso VPC must be via a load balancer, which is only configured to pass traffic to systems running the web service component of the Virtuoso platform. Any other incoming traffic is rejected.

AWS is a leader in cloud security and holds ISO27001 and SOC Type II certifications. Our supplier takes suitable measures to ensure availability, including redundant power supplies, UPS backup systems, and fire suppression systems. The data centers used by our suppliers include physical security measures to prevent unauthorized access. AWS provides a full overview of the measures they take in a whitepaper. In addition to the measures undertaken by our supplier, we follow their best practice by running redundant services in multiple availability zones.

Customer Tenancy

All users must use a password that is at least 8 characters to access Virtuoso. Users can only join an organization and register an account through a valid invitation, or through manual account creation by the organization owner. Access to projects is limited by per-user permissions and can be revoked by the project owner at any time. Virtuoso maintains a revision history of each goal within a project, allowing changes to be reviewed and reverted if required.

SSO

SSO is available to log in to Virtuoso for authentication. Full details on SSO capability can be found in the documentation here.

Security

All changes to the Virtuoso application go through a thorough review process. Access control is required on internal documentation and tooling, and customer data-access policies are in place for additional security. Security reviews are part of the engineering process and yearly security assessments are carried out by an external entity. Access to resources within Virtuoso's VPC is limited to a subset of authorized administrators, who are only able to access the VPC through a bastion host using public key SSH authentication.

Security Overview

- All communication with Virtuoso is TLS encrypted with the latest protocol versions
- All API requests go through access control, the code for which is always at least double validated to ensure that our endpoints are secure
- We perform regular external third-party pentesting audits
- We perform regular internal pen-testing, hacking, and chaos testing exercises to try to break into/break our system
- We prevent against attacks with the help of Cloudflare and AWS, and our requests go through a load balancer which will scale based on demand

Human Resources Security

Virtuoso has the necessary processes in place to do background verification checks of certain employees if the customer requires this. These checks are performed in compliance with the local laws and regulations of the place where the employee is based.

All employees, sub-contractors, and suppliers have to sign a confidentiality and non-disclosure agreement with us as part of their overall agreement. Virtuoso also communicates the need for confidentiality to all employees and holds them properly accountable for this responsibility.

Operations Security

Virtuoso installs anti-virus and anti-malware software on all the laptops used by employees. In addition, these laptops are password protected and in most cases encrypted. We carry out a quarterly audit on all laptops to make sure they are well protected.

Network Security

Virtuoso is deployed in a virtual private cloud. Our infrastructure provider (AWS) manages the physical security of the infrastructure and the security of the network and virtualization layers on which Virtuoso operates.

External access to Virtuoso resources is limited and only permitted strictly by necessity using security groups. By default, no ports are remotely accessible to Virtuoso's infrastructure. A single

bastion host has its SSH port (22) exposed to remote traffic which is only available to authorized administrators with an authorized private key pair.

None of our resources is directly accessible from the internet, which is enforced using security groups. All public services are exposed internally to a load balancer, which allows requests from the internet to be routed internally to our application servers without directly exposing them to the internet.

Virtuoso's private cloud is organized into distinct security groups that limit internal traffic to pre-approved ports. We use security group segregation to ensure that our different environments (development, staging, production, and any test environments) have no connectivity to one another. Remote access to our internal network is only available to approved team members via a secure shell connection using public key cryptography to encrypt communication and authenticate users.

Security in Development and Deployment Processes

Source code for Virtuoso is stored in a private repository on GitHub. Deployments are automatically orchestrated from CircleCI, and only privileged engineers have the right to make pushes to repositories that are deployed to our production environment. All team members are required to use two-factor authentication. Only authorized administrators are able to make configuration changes to our application servers or the software running on them. When engineers leave the organization, their access rights to the repositories are revoked.

Audit Trails

Virtuoso's application logs are aggregated centrally within our VPC, and we hold application-level access logs and also maintain system-level logs from our infrastructure. All changes made to the infrastructure are logged by our cloud provider AWS. Additionally, Virtuoso's GitHub repository allows us to audit the code that was pushed with each release. Third-party service providers are assessed for their compliance with security standards by third-party auditors.

Compliance

SOC 2 certification was completed in Q3 2022.

Third-Party Security

The following suppliers provide services that we use to help deliver Virtuoso:

Supplier	Website	Service provided	Compliance
Amazon Web Services EMEA	https://aws.amazon.com/	Network, Compute, Database, Database	ISO27001, SOC 2 Type II

SARL (AWS Europe)		Backup	
Datadog Inc.	http://datadoghq.eu	Application log collection and storage	SOC 2 Type II
GitHub Inc.	https://github.com/	Source code repository	CSA (self-assessment)
Circle Internet Services, Inc.	https://circleci.com/	Continuous Integration	FedRAMP
BrowserStack Limited	https://www.browserstack.com/	Cross-browser testing	SOC 2
Functional Software, Inc. (Sentry)	http://sentry.io	Error monitoring	Self-assessed

Security of these providers is assured through their compliance with SOC2, ISO27001, or FedRAMP security standards, all of which are assessed by third-party auditors. We also make use of Sentry to collect and monitor error events raised in the application. Sentry does not have a certification but does have a comprehensive compliance document (https://sentry.io/security/)

Penetration Testing

Virtuoso undertakes annual third-party auditing for penetration testing, where those auditors hold the following certifications: CompTIA Security+, CompTIA Pentest+, CompTIA CySA+, Offensive Security OSCP, Offensive Security OSWE, SANS GWAPT, SANS GEVA, EC-Council CEH, ISC2 CISSP. Any issues identified through penetrating testing are triaged and remedied accordingly. Copies of penetration tests will be provided upon request, including remediation reports.

Data Management, Availability & Security Controls

Data Storage & Availability

Virtuoso's data is stored at rest using AES encryption with keys managed by our cloud provider AWS. In SaaS deployments, Virtuoso takes daily snapshots of the database that stores your data. In addition to the snapshots, our compute provider allows point-in-time recovery for data at least 5

minutes old. 30 days of these backups are maintained by Virtuoso. If we experience an outage from our compute provider that causes the permanent loss of both our database and its standby, we will use our computer provider's backup restore procedure to create a new database with the most recent backup.

Whenever we have to perform a restore operation, we will advise you of the point-in-time when the snapshot was taken. Our database backup procedures are designed to protect your data from outages or service interruptions beyond our control. The Virtuoso application records your data in versioned snapshots, meaning you will always have access to your data, although snapshots can be deleted forcefully.

In the event that you require access to data that has been removed/deleted from Virtuoso by you, we will provide a service to retrieve it from our backups (provided the deletion was not made before the earliest snapshot we hold). This may incur an additional support charge.

As we do not manage the data stored on-premise, it is the client's responsibility to ensure that data is backed up and an appropriate DR process is in place. We will work with the client to advise on how data should be backed up/stored redundantly according to their requirements.

Data Backup & Disaster Recovery

We take regular backups in line with our Backup and DR policy. Databases and their backups are encrypted with industry-standard AES-256 encryption to protect them from unauthorized tampering or access. We use a redundant database configuration to protect from outages caused by a fault with the machine, in line with the supplier's best practices for the service. Our supplier is responsible for maintaining the storage of Virtuoso's backups, and we use their access control system to ensure that only authorized administrative staff have access to restore the backups.

Data Security

All data sent over the internet between users and application servers is secured in transit using industry-standard TLS encryption. Virtuoso's internal systems can only be accessed with transport encryption in place with suitable authorization. Access to source code, administrative tools, and monitoring over the internet is secured using either SSH or TLS with authentication.

Data Encryption

Passwords are individually salted and stored using PBKDF2 with HMAC-SHA256 with 65536 iterations, per NIST guidelines on memorized secrets. Clients can only use Virtuoso over TLS, and traffic is encrypted between your browser and our load balancer.

Ciphers

- For app.virtuoso.qa (the platform), the following Ciphers are used, where Virtuoso currently supported TLS1.2 and TLS1.3 only:
  https://developers.cloudflare.com/ssl/ssl-tls/cipher-suites

- For api.virtuoso.qa (Virtuoso APIs), the following Ciphers are used, under column: TLS-1-2-2017-01: https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-policy-table.html

Access Control

Only authorized administrators are allowed limited access to our infrastructure console and must authenticate using two-factor authorization. Only the CEO and the CTO of SpotQA have access to the root credentials for our infrastructure provider. All other staff uses managed accounts with limited privileges.

Access to production data is limited strictly to administrators and subject to client authorization in accordance with the SpotQA Access Control Policy document. As soon as an employee leaves the company, we terminate all access for that employee throughout the organization.

Virtuoso

Document

Support Services

Support Overview

Virtuoso support included as standard with software license **Access to Virtuoso user documentation, Training material and Knowledge base resources**	8am-6pm UK Monday to Friday
Support channels	support@spotqa.com or via our online support chat https://knowledge.virtuoso.qa/knowledge/support
Support packaging	Included with software license
Support team	Virtuoso Customer Success Team
Product Deployments	Virtuoso SaaS Virtuoso On-Premise
Phone support	Yes
Support entitlements	Product admins & authorised users
Initial response time **L1: Application Down** **L2: Serious Degradation** **L3: Moderate Impact** **L4: Low Impact / Inquiry**	L1: 1 business hour L2: 1 business hour L3: 2 business hours L4: 2 business hours
Support hours	10 hours per day Monday to Friday

Support Types

There are 2 Virtuoso support types in operation that cover SaaS deployments. The first support type Xcovers the platform and infrastructure, and the second type covers the operational use of Virtuoso and user support.

Platform and Infrastructure Support

This covers any instance where there is a loss or degradation of service to Virtuoso as a whole or as a subcomponent or feature set. Issues of this nature must be raised by sending an email to support@spotqa.com or via our online support chat https://knowledge.virtuoso.qa/knowledge/support.

Issue Severity Classification

Virtuoso has several different levels of severity to help prioritize larger problems over smaller ones:

Severity 1 (label: Critical) - The problem has a severe and total impact on the platform/service, all users are unable to access the service, there is a Data Breach. Examples include Virtuoso not being accessible, users unable to perform core tasks, or all or most of the users getting unexpected errors. The response time for this severity is 2 hours.

Severity 2 (label: Urgent) - The problem has an impact on certain aspects of functionality, but the users can access the application. Users can perform other tasks using other systems, but no workaround is available. The problem impacts a high volume of users. Examples include a business-impairing/showstopper/blocking issue for a specific user, a user cannot automate a particular scenario and requires a workaround/solution (otherwise cannot continue with their needs), or a high-impact problem is affecting many users (e.g., test executions take unreasonably long times or unpredictable results). The response time for this severity is 2 hours.

Severity 3 (label: Major) - The problem is a non-blocking issue, and it could impact a small number of users for a specific use-case and is non-reproducible in other cases. Examples include a non-business-impairing/non-blocking issue for a specific user, which is yet still affecting core workflows (e.g., exploration outcome panel fails to load/is throwing errors for a subset of users). The response time for this severity is 4 hours.

Severity 4 - (label: Minor) - The problem is a low-impact issue affecting a single user and does not impact critical user functionality. An example would be low priority issues that still impact users, but the user is aware of workarounds (e.g. users not getting automatically logged out after changing the password and getting errors on further interactions instead). The response time for this severity is 4 hours.

Operational and User Support

This covers any instance where a user requires support in overcoming a specific blocker, guidance on best practice, or help using a specific feature or capability within Virtuoso. This also includes the onboarding and training of new users.

Level 1 - This is for when the user is blocked from current activities. Examples include the user needing support to solve a specific use case, such as building and

executing a natural language test or extension, and they cannot progress any other work streams (blocked on all activities). The response time for this level is 2 hours.

Level 2 - This is for user support on a specific use case when the user is not blocked from all current activities. Examples include the user needing support to solve a specific use case, such as building and executing a natural language test or extension, but they can continue working on other workstreams and remain productive for a period of time (e.g. 3-5 hrs). The response time for this level is 2 hours.

Level 3 - This is for user advice on the best practice for a specific use case. Examples include when the user has a solution to a specific use case, such as creating random data or using variables but would like to understand if there is a more eloquent or efficient solution, or when the user is unsure of how to best configure environment setups or goal and journey configurations. The response time for this level is 4 hours.

Level 4 - This is for general inquiry. Examples include general questions, where to find information in the docs, etc. The response time for this level is 4 hours.

Core Operating Hours

Virtuoso support operates a 12-hour day with support available between 8am and 6pm GMT Monday through Friday.

Virtuoso platform and infrastructure support core hours are between 8am and 6pm GMT Monday through Friday.

Virtuoso operational and user support core support hours are between 4am and 6pm GMT Monday through Friday.

Maintenance Events and Upgrades

In addition to unforeseen outages caused by events beyond our control, we may perform routine releases or schedule downtime for the Virtuoso platform to carry out maintenance or upgrades. We will endeavor to make these changes at times that minimize the impact on the majority of our customers.

Releases of the product will be made subject to our internal release policy and are not expected to affect the availability of the platform. Releases are generally made at least once every month. The latest release updates can be found in Virtuoso's documentation.

During maintenance, we will aim to provide availability of unaffected services throughout the period, but we may notify you that they could potentially be affected. Whenever maintenance is scheduled, we will advise you at least 7 calendar days prior to the event with the following information: the maintenance reason, the components affected, the at-risk period (if any), and the expected completion time. We will advise you when the maintenance is complete.

Patching and Upgrades

Routine patching and upgrades will be performed on a 6-month cycle and will be agreed upon with the client 1 month in advance. It is the responsibility of the client to ensure that all data and digital assets are backed up prior to any patches or upgrades being deployed. We will provide instructions on how to perform the release for each release or update, including details on how to revert the upgrade (before availability is restored) if required.

Paused or Declined Patches & Upgrades

The client has the right to pause or decline a routine patch, however, if the client declines 2 or more consecutive patches, Virtuoso cannot guarantee the reliability or stability of the platform. Where technically feasible, we will backport hotfixes (i.e. apply fixes without changing the minor version of the platform otherwise) for up to 2 months.

Incident Management Procedures

Our aim in the architecture of Virtuoso is to avoid failures using application-level mitigations. Failures that expand beyond the scope of these mitigations are considered disasters and will result in visible degradation or reduced availability of Virtuoso. In these scenarios, we will resolve them as quickly as possible and provide specific guidance during the outage.

Throughout all outages, except those in the following section, our RTO for data loss is 6 business hours. Our backup mechanism retains data continuously and has an RPO of 5 minutes. We will ensure that data that is more than 5 minutes old will be recovered within at most 6 business hours of an outage that causes loss of both our primary and hot-standby database instances.

Outages Beyond Our Control

In the event that the redundancy mechanisms in our architecture are unable to maintain availability during an outage caused by our provider, you may experience some performance degradation. Our commitment to ensuring the integrity of data guarantees that you will be able to resume operations once the outage has passed without any loss of existing data.

Jobs undergoing execution during an outage may, however, be affected. If this happens, you may experience sudden termination of jobs or reduced performance during the outage. Virtuoso's snapshot feature means that any changes arising from a suddenly terminated job can be rolled back in the event of such a failure.