test craft

Data Security at TestCraft

TestCraft offers a web-based, codeless Selenium platform for the creation and self-maintenance of automated tests for web applications. As many of our customers are highly sensitive to protecting their data and complying with certain industry and general data protection regulations (e.g., HIPPA, SOC2, PCI atc.) we are committed to meeting the highest security standards. As a SaaS platform, we offer the benefits of flexibility, scalability and license cost reduction that come with operating on the cloud, while also maintaining strict security measures.

Please contact us if you would like more details about our security policies and practices.

Connectivity

As TestCraft executes functional end-to-end tests against web applications, it requires that a connection is established between the TestCraft platform on AWS and customers' applications under test. There are several network setups that allow such a connection:

amazon web services Security BEST PRACTICES

ISO 27001

test craft

Data Security at TestCraft

Direct Connection over SSL

When the tested application is directly accessible from the Internet, TestCraft uses a standard SSL connection to execute automated tests against it. There are no special requirements for enabling this option.

Whitelisting of the TestCraft IP address on customers' firewalls

When the tested application is protected behind a network firewall, access from the TestCraft platform should be enabled. As TestCraft is using a single, static IP address for each of its platform deployments (US and Europe), it is easy to whitelist those IP addresses on the firewall to grant secure access, while still preventing unwarranted access from other IPs. During a TestCraft trial or onboarding session, we will provide you with the relevant IP address for your region.

Whitelisting of the TestCraft IP address on customers' firewalls

TestCraft offers the option to set up a dedicated AWS Virtual Private Cloud for specific customers and use VPN tunneling to connect this VPC to the applications under test in the customer network.

amazon web services Security BEST PRACTICES

ISO 27001

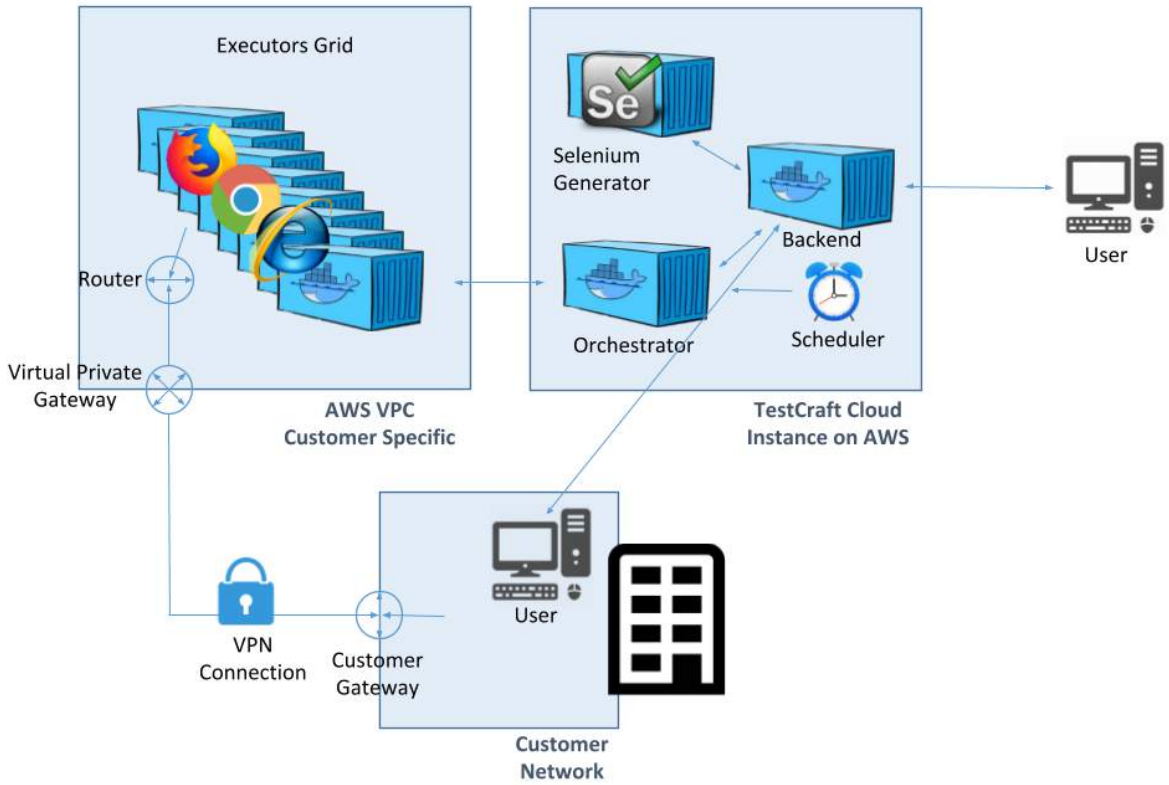
test craft

Data Security at TestCraft

Such a setup practically adds the VPC as a secure extension of the customer network and offers an easy, yet a very secure option for establishing a connection between the TestCraft platform and tested applications.

TestCraft Architecture - VPN

test craft



amazon web services Security BEST PRACTICES

ISO 27001

test craft

Data Security at TestCraft

Data Privacy & Secure Data Storage

Data Access

TestCraft's data is stored in AWS data centers. The following measures are taken to secure the AWS environment to ensure full data privacy:

- **Multi-factor authentication.** We use two-factor authentication for privileged access users.
- **Encrypted keys for SSH access.** Access to any SSH environment is done with encryption keys instead of user passwords.
- **Secure communications.** All communication is done in HTTPS over SSL transmission.
- **Closed environment.** The environment is closed off and allows access only to whitelisted IPs. Access to the environment is further restricted to only a handful of servers.
- **Firewall protection.** All information is stored behind a firewall with closed ports.
- **Anti-virus scanning.** All files that are uploaded to the AWS servers are scanned for viruses prior to use.

For more information about the security capabilities of these AWS cloud services, consult the Amazon Web Services: Overview of Security Processes whitepaper.

amazon web services Security BEST PRACTICES

ISO 27001

test craft

Data Security at TestCraft

GDPR Compliance

TestCraft has experience with storing data in specific environments to comply with GDPR locality requirements. To date, TestCraft manages environments based in the USA and Europe. All test creation, execution, and maintenance happen inside of these localities.

ISO Compliance

TestCraft holds an ISO 27001 certification, which confirms the company's adherence to information security best practices in the following areas:

- **Handling information security events.** TestCraft uses a wide variety of tools, materials, and resources to monitor, discover and resolve unauthorized activity occurring on the network, as well as equipment connected to the network.
- **Operational security.** Once every six months, TestCraft's system is examined to ensure that all the definitions are consistent with the company's requirements.
- **Access control.** At every level, there is a separation of privileges between regular users and those that manage and define the systems. Standard user accounts are not granted administrator status.

amazon web services Security BEST PRACTICES

ISO 27001

test craft

Data Security at TestCraft

- **Backup.** Backups are performed in accordance with the backup requirements for the most sensitive information/applications on the server. The frequency of the backups is defined in accordance with the most sensitive type of information/applications on it.
- **Employee security training.** TestCraft mandates periodical security training sessions as part of its employee training program. TestCraft's training program accommodates the adjustments warranted by GDPR requirements and includes dedicated data management and protection training specific to employees with access to personal data.

For more information about ISO 27001, please consult the updated list of mandatory requirements for ISO 27001 certification.

Control Over Sensitive Data

For additional data security, the customer can choose which data to keep within the TestCraft platform. To accomplish this, the customer can use a data file instead of entering the data directly in the TestCraft platform. The system would only use the data during test runs and deletes it following the run's completion.

amazon web services Security BEST PRACTICES

ISO 27001

test craft

Data Security at TestCraft

Role-Based Access

There are four access levels within TestCraft to manage permissions throughout your team:

- Administrator - Granted all permissions.
- Tester - Can create tests, but cannot invite other users.
- DevOps - Can see and run executions, but cannot build the actual tests.
- R&D - View-only mode.

amazon web services Security BEST PRACTICES

ISO 27001