Security & Privacy FAQ

Nikhil Sharma

The security and privacy of our customers is of the utmost importance to Qentinel. For more information on this, please have a look at the frequently asked questions below.

How does Qentinel take privacy?

Your privacy is very important to us. When you use Qentinel services, you trust us with your information. We have implemented technology and policies with the objective of protecting your privacy from unauthorised access and improper use and will update these measures as new technology becomes available, as appropriate.

What sort of personal data does Qentinel Pace collect and store?

We collect personal information such as name, e-mail address, picture (if you have given one) and phone number with your consent when you register with us or place an order for products or services. When you use our digital services, we automatically collect and store certain information in log files, such as details of services used, including time stamps, crashes and system activity. Some of our services include surveys and those results are collected and stored. However, Qentinel does not collect the application data outside of the scope of tests and defined measurements.

How does Qentinel Pace collect and handle personal data?

We use network monitoring products to monitor and analyse the network traffic. We and our partners use various technologies to collect and store information when you visit a Qentinel service, such as cookies, to identify your browser or device. Qentinel Pace uses JSON Web Tokens which are an industry standard. Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity.

For further information visit AboutCookies.org or All About Cookies.org. You can set your browser not to accept cookies and the above websites tell you how to remove cookies from your browser. However, some of our website features may not function as a result.

Where does Qentinel Pace store my data?

Qentinel Pace uses AWS data centers located in the European Union.

However, the help desk and chat application integrated into Qentinel Pace, Intercom, is hosted in a U.S. data center, provided by Amazon Web Services, Inc. (AWS). All data flows go through AWS (AWS Region: US East (N. Virginia)). AWS is Privacy Shield certified, so data transfers from the European Economic Area (EEA) are covered by AWS Privacy Shield certification. EU law and regulators recognize the Privacy Shield and the EU Model Clauses as equally valid and accepted legal means of transferring personal data from the EEA to the U.S. Since Intercom relies exclusively upon the Privacy Shield certification to receive data transferred from the EEA, our policy is not to sign any external EU Model Clauses.

What information about my application, data, and network does Qentinel Pace transfer to the cloud?

Since the system under test is accessed by robots in cloud, all the information that is visible on the applications user interface is essentially available as screenshots and videos, along with test results and logs, in Qentinel Pace's data warehouse located in AWS cloud. It is important to note that customer specific information is only visible to that specific customer.

If necessary, the secrets containing test logs can be obfuscated from all the logs and test results. A lot depends on the implementation of a project, and it is not mandatory to take screenshots or video recordings, should you not wish to do so.

In some very sensitive hybrid implementations, refer appendix, we do not send any data to the cloud except for the execution minutes.

Is Qentinel's privacy policy valid for other websites?

Our web application contains links to other websites. This privacy policy only applies to pace.qentinel.com. Should you link to other websites, you should read their own privacy policies.

How can I audit what information Qentinel Pace has collected about me, my organization, my application, my data, and my network?

You have the right to request a copy of the information that we hold about you. If you would like a copy of some or all of your personal information, please email us at the following address: privacy@qentinel.com. We want to make sure that your personal information is accurate and up to date. You may ask us to correct or remove information you think is inaccurate.

How does Qentinel Pace protect and guard the information it has collected?

Security is of utmost importance to us. Hence, development of Qentinel Pace is conducted by following the best practices in secure software development process including skilled developers trained for security, code analysis and review practices, mitigating OWASP top 10 risks, microservices with only absolutely necessary permissions, authentication, secure APIs, secure secret and key management, logging, and infrastructure-as-code (secure infrastructure). Qentinel Pace's security policies and governance are based on and continuously developed according to ISO 27001 policies and controls.

Qentinel Pace makes use of Kubernetes to ensure high availability and for eliminating the need of human input when deploying to and scaling up the production environment resources. Microservices exist within a Kubernetes cluster and they are all behind public gateway services, which are handling all incoming traffic from the internet. This way none of the service containers are directly accessible for users and all traffic can be easily monitored and authenticated.

Qentinel Pace is securely hosted on AWS by carefully following the AWS Security Best Practices such as:

- separate production and development accounts,
- data encryption,
- virtual private clouds and subnets,
- bastion host controls for SSH connections – no SSH connection to production machines,
- load balancers used only over HTTPS,
- system internal traffic is managed using security groups and microservices have only required permissions for AWS services through IAM roles.

All changes to the production infrastructure are made through infrastructure-as-code. Because of this, the current state of the environment is always available in a version control with traceable history. All infrastructure events are also logged and are auditable by using AWS CloudTrail.

All Qentinel services and APIs require valid token or other authentication method and access to different resources is restricted with user configurable permissions. Authentication token can be acquired by signing in with Qentinel Pace user account or with supported Single sign-on (SSO) method.

All stored user passwords are hashed in non-invertible way. Other stored sensitive information, which can include different secrets given by the user, are encrypted using AWS KMS. When AWS KMS is used, each customer (and project) has their own encryption key that is rotated regularly.

How does Qentinel Pace access the application under test?

This depends on the application. Web applications are accessed over HTTP/HTTPS using web browser.

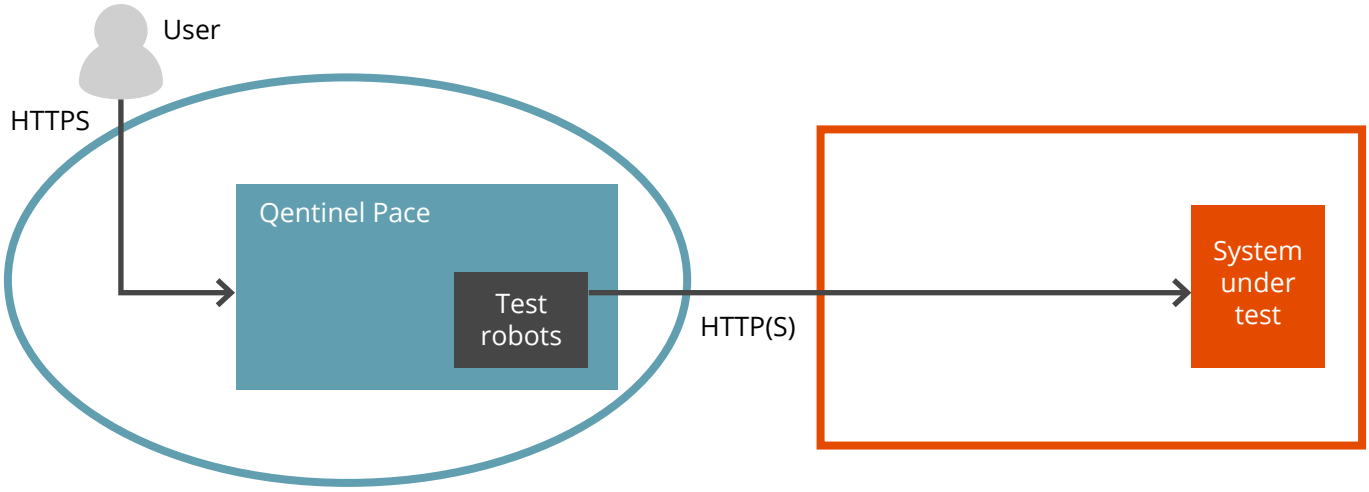
Native mobile applications require installing the application binary on the mobile device (or device emulation).

UI applications are either accessed over underlying API (such as win32) or if the underlying API's are not available the applications are accessed over visual screenshots, virtual keyboard and virtual mouse. Depending on the use case also other methods such as API's, VPNs and other lower level network protocols may be used. **For detailed information please see the appendix at the end.**

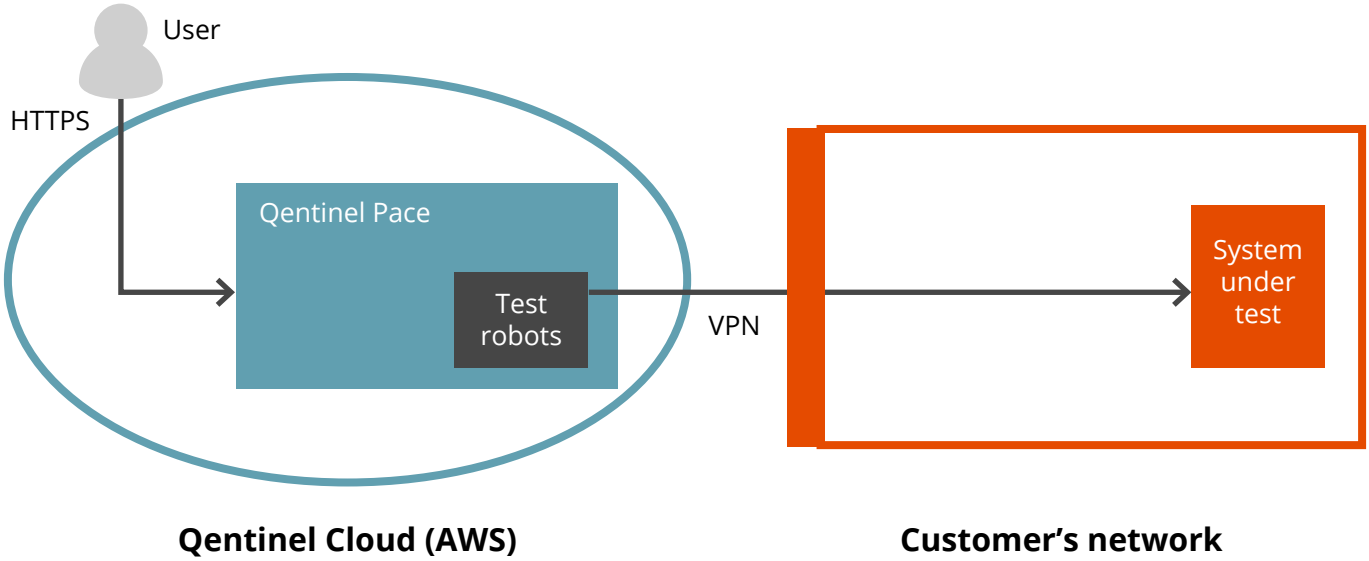
APPENDIX

Pace accessing system under test (SUT)

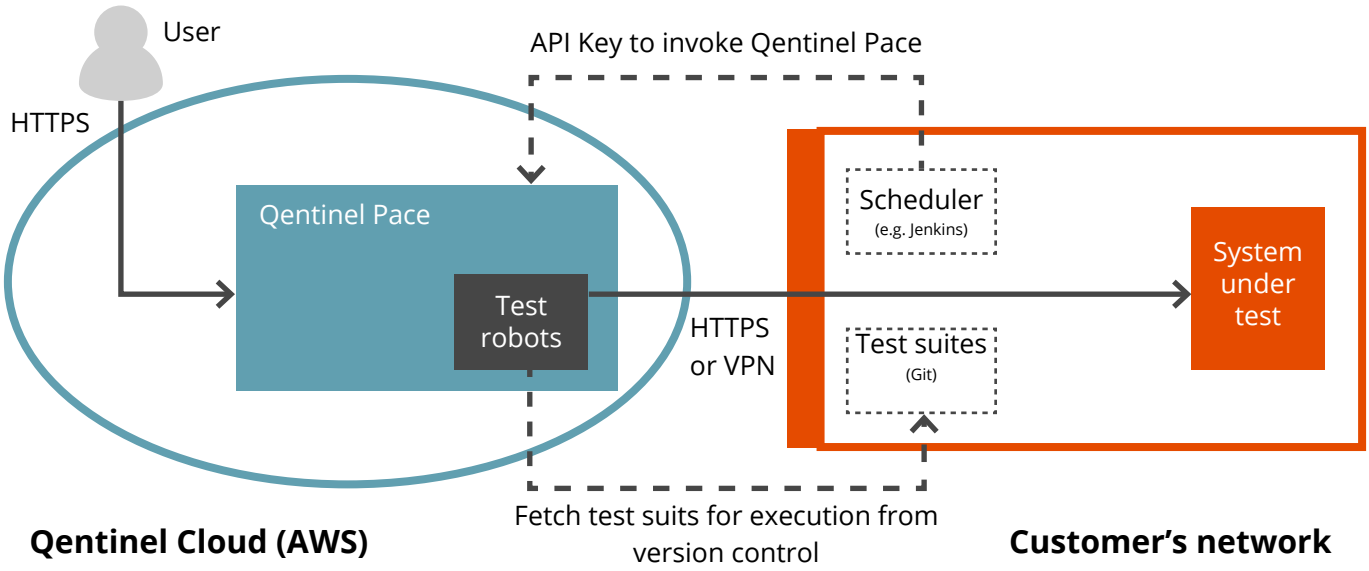
Case 1: *Web setup*
SUT available over internet, mobile and web testing.



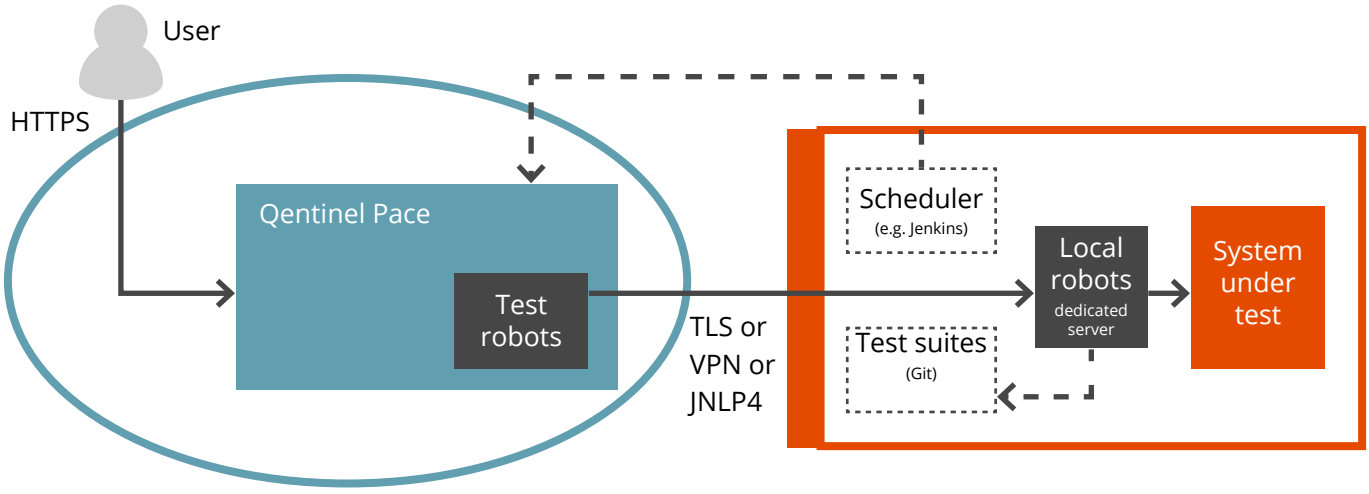
Case 2: *Tunnelled setup*
SUT available behind a firewall, mobile and web testing.



Case 3: *Pipeline setup*
SUT available behind a firewall and Qentinel Pace is integrated in customer's CI/CD pipeling, mobile, web & native testing.



Case 4: *Hybrid setup without connector*
SUT cannot be accessed outside the company network.



Case 5: *Hybrid setup with connector*
SUT cannot be accessed outside the company network and post-processing of result is needed.