

## PractiTest - Security Overview

We take every precaution to protect the confidentiality and security of your information. The following document provides an overview of PractiTest's main security measurements.

### Physical security

Our server cluster is hosted on Amazon's EC2 platform, which employs state-of-the-art security systems to protect their facilities. Access to our servers is protected by security professionals where authorized staff needs to pass two-factor authentication a minimum of two times to get access to our datacenters.

Our servers are redundantly connected to multiple tier-1 transit providers; they are constantly protected by discrete uninterruptable power source (UPS) and onsite back-up generators.

You can read more about Amazon's EC2 security here -

<http://aws.amazon.com/security/>

and here -

[http://media.amazonwebservices.com/pdf/AWS\\_Security\\_Whitepaper.pdf](http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

### Application security

All data is written to multiple disks instantly, backed up 4 times a day, and stored in multiple locations.

Our software infrastructure is updated regularly with the latest security patches. Our network is protected by a firewall and carefully monitored. All servers are fully redundant to ensure minimal downtime.

Access to your project is protected by password and 128bit SSL encryption. Your data will be completely inaccessible to your competitors or anyone outside of your project(s).

At no time does PractiTest use cookies to store passwords or customer data on the user system. Cookies are used for session information and user convenience, but at no time is that information sensitive nor can it be used to break into a user's account.

### Want to know more?

Please submit your security questions to [security@practitest.com](mailto:security@practitest.com).