PractiTest

Test Management Tool Security and Compliance

Last Updated: January 2nd, 2020

About PractiTest

A leader in the test management tool market, PractiTest is a SaaS end-to-end QA management system with some of the most advanced and interesting features. With PractiTest, testers and test managers are able to focus on quality and their actual work rather than side tasks.

About PractiTest Security

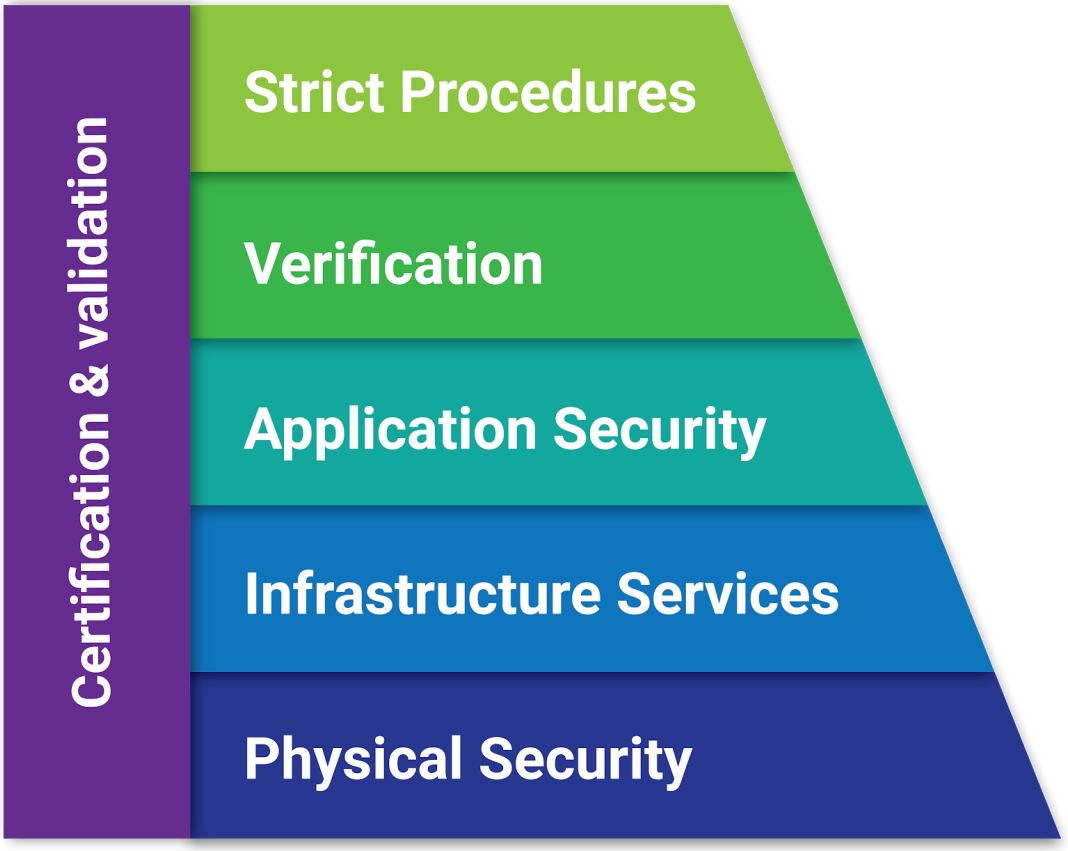
In PractiTest, we understand the importance of security, privacy and reliability of information.

Our platform was designed to make sure only you and your users can access your information, and we work with the best practices and top partners (such as E&Y for SOC, AWS, etc) in the business to make sure our system is always secure, available and accessible from anywhere in the world.

PractiTest is and always was a SaaS only platform; as such PT was designed and built from the beginning with all the security considerations in mind. Over the years, as our client base grew, we kept adding layers to make our system even more secure. Some of the practices that we have today are listed below. For the full SOC-II type 2 report, please contact us.

Security layers

From ground to top we see our security as layer by layer:



Layer 1 - Physical Security & Access

AWS provides physical data center access only to approved employees and authorized third parties. Access requests are granted based on the principle of least privilege, meaning access will be limited to the layer of the data center the individual needs access to, and is time-bound. To read more about this please visit: https://aws.amazon.com/compliance/data-center/

Layer 2 - Infrastructure Services

VPC

Amazon Virtual Private Cloud (Amazon VPC) lets us launch AWS resources into a virtual network that we defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS. This means complete control over our virtual networking environment. We also use VPC features, such as

Security Groups, to control network access between different resources (load balancers and machines for example).

Security Groups

Security groups act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level. For each security group, we have designated rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

RDS

We use Amazon Relational Database Service (Amazon RDS) to set up, operate, and scale our relational database. It provides us with resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees us to focus on the PractiTest application, so we can give our clients the fast performance, high availability, security and compatibility they need.
We use RDS security best practices: encryption, Network isolation (inside a VPC). In addition, all of our production environment databases are deployed in multiple availability zones to provide enhanced durability and high availability.

AWS Identity & Access Management - Manage User Access to AWS services and resources

AWS Identity and Access Management (IAM) assures the access to AWS services and resources is always secured.

PoLP configuration (Principle of Least Privilege)

The principle of least privilege is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. It is applied to restrict access rights for applications, systems, processes and devices to only those permissions required to perform authorized activities.

Multi-factor authentication (MFA)

MFA is an authentication method which requires more than one piece of evidence to verify a user's identity before login. We use MFA only to login to our AWS console.

AWS Certificate Manager - Provision, Manage, and Deploy SSL/TLS Certificates

With AWS Certificate Manager, PractiTest can provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks.

AWS CloudTrail - User activity and API usage Tracking

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing for our AWS account. With CloudTrail, we continuously monitor, and retain account activity related to actions across the AWS infrastructure. CloudTrail provides event history of PractiTest's AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

Monitoring

We use several monitoring services and open source utilities to get alarms, metrics, data and actionable insights. Here's a **partial** list:
Amazon CloudWatch - Application and Infrastructure Monitoring
Pingdom
PagerDuty
Monit

AWS WAF - Web Application Firewall - Protect your web applications from common web exploits

AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives us control over which traffic to allow or block to our web application by defining customizable web security rules.

Layer 3 - Application Security

All Communication via SSL (Encryption in transit)

All our communications are performed via encrypted channels. PT Web application can only be accessed using https, including the API, admin tools, plugins, and all aspects of the product. Communication between DevOps and DataCenter is done only via ssh, and using private keys only. AWS console can be accessed only by the relevant people (PoLP) with MFA.

Encrypted DB (Encryption at rest)

Amazon Relational Database Service (Amazon RDS) is where we set up, operate, and scale a relational database in the cloud.
Amazon RDS allows you to encrypt your databases using keys you manage through AWS Key Management Service (KMS). On a database instance running with Amazon RDS encryption, data stored at rest in the underlying storage is encrypted, as are its automated backups, read replicas, and snapshots.

Passwords are never stored on servers or logs

We filter parameters from writing to our logs, such as user passwords and api tokens.

RBAC - Role Based Access Control

Role-based access control (RBAC) is a method of restricting access based on the roles of individual users within an enterprise. RBAC lets employees have access rights only to the information they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

Audit Trail & log

An audit trail (also called audit log) is a security-relevant chronological record, that provides documentary evidence of the sequence of activities that have affected a specific operation, procedure, or event. This is critical to check during routine activities like updates and patching, and also to determine when a system component is failing or is incorrectly configured.

24/7 Monitoring - internal and external

We monitor our service availability from multiple locations around the world. We have alerts in place in case of service outages and the DevOps group are getting automatic SMS, emails and automatic phone calls when errors are severe.
To provide our customers full transparency we log each and every incident of our service (started on Jan. 2011). The full history is available at: https://status.practitest.com

Layer 4 - Verification

Since PractiTest is a SaaS only platform our processes (verified by E&Y) are in place to avoid human errors.

Penetration testing

We use a leading cyber & security consulting firm to carry out penetration testing to our server network at least once a year.
The tests are based on the “OWASP Testing Guide”.

Firm’s expert team is comprised of experienced professionals with international certifications and extensive knowledge in the field of WEB application, which allows them to provide us with quality and efficient service.

Code Reviews

All issues / fixes are handled via a separate pull request, which has to pass both actual code review (by a senior developer), and automated tests.

Amazon GuardDuty - Managed Threat Detection Service

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts and workloads. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs.

Static analysis

Source code is analyzed using Brakeman vulnerability scanner to allow detection of security issues during development.

Dynamic analysis — using OWASP ZAP

OWASP ZAP is used to detect security vulnerabilities during development and testing.

Amazon Inspector - Analyze Application Security

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of the PractiTest application. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings are then reviewed and solved.

Layer 5 - strict procedures

Access is restricted

According to PoLP - Only Devops users can access the PT servers, and only for the reason of their work.

Backups

PractiTest recognizes that the backup and maintenance of data is critical to the operations of PractiTest services, it is essential that certain industry best practices be followed to ensure that data is backed up on a regular basis and the integrity of the procedure is sound. The operations team is responsible for managing and performing backup tasks on various types of service-related.

Disaster recovery plan

PractiTest has developed a Disaster Recovery Plan (DRP) in order to continue to provide critical services. The DRP is tested on an annual basis. Moreover, PractiTest has developed a disaster recovery plan relying on AWS platforms which are operated according to, among others, SOC2 Type-II and ISO 27001:2013 standards and are designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.

Change Management Policy

Changes are documented by opening a ticket within the SDLC Application. Decisions to approve or reject and prioritize requirements are made by the relevant personnel. The decisions are taken after reviewing the change impact from different levels (e.g. security, availability, confidentiality and privacy).
Change management policy includes Pull Requests and code review.

Permission to deploy Master branch to Production is restricted to authorized personnel. PractiTest deployment to production is automated in order to ensure safe deployment after all appropriate tests are performed.

Patching policy

PractiTest utilizes Amazon Inspector to scan for common vulnerabilities and exposures (CVEs). Vulnerabilities ranked 4.0 and higher (Medium and higher based on CVSS 2.0 and 3.X standards) are reviewed by Change Advisory Board (CAB) and patches are installed when necessary.

Layer 6 - Certification & Validation

PractiTest is the most secure QA system in the market. Our client's safety and confidence is a top priority and so we employ multiple technologies for threat detection and prevention, to make sure your data will always be safe and available to you.

Furthermore, our solution complies with the strictest security standards in the industry making us the only SaaS test management you can fully trust.

Our compliances:

SOC 2 Type2 ensures that companies providing hosted solutions are following industry best practices and their operations comply with the highest levels of security standards. The SOC2 report is based on an audit made by an external party on a yearly basis; PractiTest is audited by E&Y, industry leader and standard setter for SOC reporting. The SOC 2 report describes the infrastructure, software, people, and procedures that the company has in place to protect data.

Part of the most popular information security standards in the world. ISO27001 provides reassurance to our customers that we have established and implemented an information security management system with international industry best practices, and that we are continually maintaining and improving it. The ISO27001 is based on an audit made by an external party and requires annual audits to maintain.

GDPR is an EU regulation on data security and privacy related to personal data, applying to all organizations operating within the EU (as well as non-EU organizations with customers who are individuals in the EU zone). As a GDPR compliant solution, PractiTest has an adequate privacy policy that accounts for what personal data is held, how it is held, and the tools available to the organization (now and in the future) to process that data.

Using multiple regions at the Amazon Web Services, PractiTest was certified as an AWS technology partner. Being an APN Partner, demonstrates that PractiTest has built a strong AWS-based business.