Applitools Security Overview

At Applitools, as an organization, we're committed to keeping customer data safe. We've invested in a robust cybersecurity architecture and have engaged top-tier cybersecurity firms to assist us. We take information security seriously and we view providing strong data protection as an essential obligation we have to anyone who uses our service.

Layers of Defense

Applitools's infrastructure is protected by numerous layers of defense, known in the information security industry as a "defense-in-depth" strategy. Our security architecture includes:

- ISO27001 Compliant vendor
- ISO27001, AICPA SOC1/SOC2 compliant server infrastructure
- Intrusion Detection and Prevention Systems
- Encryption of data in transit and at rest
- Regular vulnerability scanning and penetration testing
- Security Patch Management
- Single-Tenant, Isolated and Dedicated cloud environments per customer

We follow industry best practices for application security. Applitools conducts regular security risk assessments along with vulnerability and penetration testing. We pay special attention to the OWASP Top 10 and have tailored our development processes to identify and mitigate these issues.

Applitools also uses state-of-the-art technology combined with a full suite of information security policies to ensure our corporate environment is protected. Our safeguards include:

- Enforced two-factor authentication with machine learning and anomaly detection for all staff
- Enforced encryption of all employee computers and mobile devices
- Secure Software Development Lifecycle (SDLC) with code reviews/analysis
- Next-generation AntiVirus and anti-malware on all computers
- Mobile device management and security suites
- Endpoint Detection and Response (EDR) with forensics capabilities
- Policies and procedures for incident response and data breach notification
- Password Management and Single Sign-On
- Restricted, role-based remote access (VPN) based on the principle of least privilege

US Office
155 Bovet Road, Suite 600
San Mateo, CA 94402
Phone: 800-650-3123

Israel Office
3 Shoham St.
Ramat-Gan, 5250002
Phone : +972-3-524-5938

Data Ownership

If you should ever choose to stop using Applitools, while we'd certainly be sorry to see you go, your data remains yours! We will assist you with exporting all of your data from Applitools and will ensure you have a complete and valid copy.

Encryption

All Applitools data is stored behind firewalls. All server requests are authenticated against the user's API key or session token.

All communications use TLS 1.2 or greater (formerly SSL, Transport Layer Security) encryption in transit. Your data is stored and encrypted at rest using AES encryption.

Physical Security

Applitools is hosted in a state-of-the-art SOC 1 Type II, SOC 2 Type 1 and ISO27001 certified datacenter facility. Physical access is strictly controlled by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, and other electronic means.

Authorized personnel must pass multi-factor authentication no fewer than three times to access data center floors.

Application Security

Applitools has a formal application security program in place with all code being scanned for security vulnerabilities using an industry-leading static code analysis tool. To further enhance application security, Applitools conducts yearly penetration testing to help find security vulnerabilities in our service. Our application is also subject to regular vulnerability scans to ensure the Applitools app remains secured against emerging security threats.

Single Sign-On

Applitools supports the use of client-managed identity providers to provision and authenticate your users. We currently support SSO via:

- SAML 2.0-compatible systems, such as Active Directory Federation Services (ADFS)
- LDAP/LDAPS
- OAuth (currently via GitHub, with support for other providers planned)

Role-Based Access Controls
Applitools has a set of role-based access controls (RBAC) to allow its customers to manage users and permissions within the application.

Access to projects and running tests on Applitools is managed by company administrators, or "admin" roles.

Teams in Applitools are assigned individual projects, and have access to test history, results and to run additional tests.

Individual's access to projects is governed based on their team assignment(s).

Programmatic Access
In the Applitools web interface, API keys are provisioned on a per-team basis. Administrators may assign one person or a group to each team in the application.

API keys may be retrieved by individual users and then used for programmatic access to Applitools via a Selenium WebDriver connection.

The Selenium WebDriver must use ana HTTPS (TLS v1.2+) connection to communicate with the Applitools platform.

Dedicated Cloud Environment
Applitools offers a single-tenant hosted environment, utilizing a separate Azure Virtual Network (equivalent to an Amazon VPC) per customer. Each environment is completely separated from any other Applitools customer, and no data is shared nor can data pass between instances. Every environment has its own databases, application servers, firewall rules, and underlying server resources.

Individual Firewall Rules
Each dedicated environment has unique firewall rules, and we support limiting web client and Selenium WebDriver access to IP blocks of your choosing. Access can be then limited to hosts located in your corporate offices, datacenters or via your corporate VPN connection.

Internal Policies and Procedures

Applitools adopts and adheres to several internal procedures that make sure the way we build, test, and release our software is in line with both industry best practices and our customers' expectations that their data is secure and well-managed.

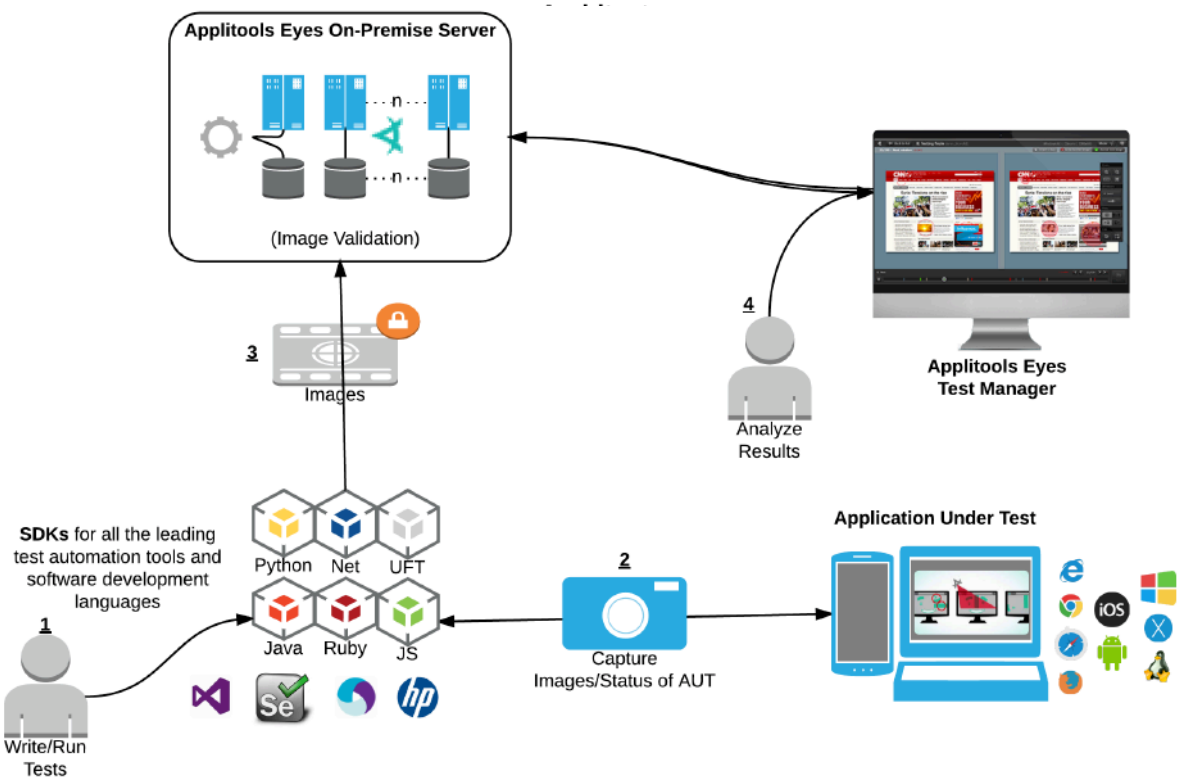
Our policies ensure we comply with needed standards and regulations, and also mean we have business continuity and customer notification plans that satisfy compliance obligations.

Compliance

In order to meet the security and compliance needs of our customers around the world, Applitools has achieved ISO27001 certification, one of the the top compliance regimes in the industry.

Applitools's infrastructure at Azure is compliant with numerous standards, and more details are available at: https://azure.microsoft.com/en-us/overview/trusted-cloud/

Applitools Eyes Dedicated Cloud Deployment Architecture



US Office
155 Bovet Road, Suite 600
San Mateo, CA 94402
Phone: 800-650-3123

Israel Office
3 Shoham St.
Ramat-Gan, 5250002
Phone : +972-3-524-5938