DATA SHEET

Security, Trust, and Assurance

A closer look at Planview Spigit safeguards

Security, trust and assurance

Security: Planview® protects all of your data

- ✔ Confidentiality
- ✔ Integrity
- ✔ Availability

Trust: Your data is yours

- ✔ Applicable legislation
- ✔ Data ownership and Data Retention
- ✔ Escrow and exit strategies
- ✔ Privacy statement
- ✔ Cookie information

Assurance: Tested and approved

- ✔ ISO-certified service
- ✔ Cloud Security Alliance- STAR
- ✔ Enterprise-ready service
- ✔ Independent audits

Security: Planview Protects All of Your Data

Confidentiality

Secure network environment

The Planview Spigit™ ("Spigit") production environment is protected by a robust network infrastructure that provides a secure environment for all customer data. The Spigit service is on a physically segregated network that requires VPN access and two- factor authentication for administrative access. Planview® monitors and analyzes system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats. Planview also uses other 3rd party tools and services to provide end-to-end network visibility and protection.

Permissions management

Spigit is a role-based permission system. Each user is assigned to a role when entering the system by the customer administrator. Spigit allows for each challenge and community have separate permissions for users which can be based on their roles.

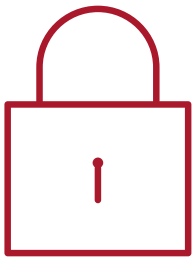
World-class security

Planview uses TLS 1.2 protocol with 256-bit AES encryption to protect data in transit in Spigit. All data transmission traffic, including APIs is encrypted. Furthermore, all data is encrypted at rest within the database. The encryption keys are stored separately, and precautions taken to prevent unauthorized access both to the encrypted document and its corresponding encryption key.

Strong passwords and unique user names

Spigit recommends customers manage user access and authorization through integrated SSO. Spigit supports SAML 2.0 for SSO. In circumstances where SSO is not possible, Spigit does support local usernames / passwords for user access. Strong passwords are at least eight but no more than fifty characters in length and include at least two characters from the following four groups:

- Numeric characters [0-9]
- Lower case alphabetical [a-z]
- Upper case alphabetical [A-Z]
- Special characters [^ 0-9a-zA-Z]



The password must not contain any non-printable characters.

IP Whitelisting

Spigit does have the ability to support IP whitelisting if so desired by a customer.

Integration with Single Sign-On (SSO)

No need to remember multiple passwords. Spigit supports single sign-on (SSO) and utilizes SAML and active directory federation service for its enterprise clients. Multi- factor authentication can be enabled for additional security.

Integrity

Physical and environmental measures

Customer instances, including data, are hosted in geographically disparate data centers. Customers may choose the location to host their data in based on corporate location or user base location in an effort to minimize latency.

Spigit uses ISO-27001 certified and SOC2/SSAE16 audited co-location facilities, which provide around-the- clock physical security and top-notch environmental protection. It includes comprehensive identification systems, automatic fire protection, redundant climate control and fail-over power supply.

Protection against malware

Planview provides anti-virus software for all its critical systems commonly affected by malware.

Audit logging, monitoring and traceability

Spigit has comprehensive traceability through object history, with all changes logged and visible. Spigit stores all data in a secure manner, with information intact from any changes in any manner.

Availability

System status

System availability is monitored by multiple 3rd party applications and / or services. This information is published on the Spigit support website. Why publish information about system availability? Because Planview believes system availability transparency provides customers with operational visibility and helps foster a trusting relationship with our customers.

Multi-layer redundancy

The Spigit network infrastructure is designed for maximum availability. In the event of failure, all operation-critical components, including network, web, application and database servers, as well as storage, have been deployed and configured for quick recovery.

Robust networking environment

Spigit capitalizes on the reliability, flexibility, security, scalable and high-performant network infrastructure that hosts our service.

The global footprint of our network allows us to deliver our services safely and quickly to all customers regardless of their location.

Disaster recovery and business contingency

The Spigit production database systems run in a primary and secondary mode to ensure data availability and integrity. Nightly full backups are shipped offsite to ensure business continuity. In the event of a major disruption or disaster, an emergency response team of selected Planview staff is summoned to activate the disaster recovery plan.

Backup and restoration

Planview has put into effect backup routines for its production databases. In the unlikely event of multiple server failure, the backups serve the sole purpose of restoring the whole production system.

Trust: Your Data is Yours

Data ownership

All customer data stored in Spigit is owned solely by the customer. Upon termination of service, all data can be returned to the client in an encrypted flat file.

Data retention

Data backups are retained for 30 days.

Privacy statement

The sole personal information viewable by Planview support and sales staff is the user contact information – i.e. name, e-mail address, address, phone number(s), and membership in projects.

Spigit administrators are able to view the names of all challenges or communities and its members created within the service. Planview does not share this information with anyone, nor does it ever sell or market this information to any third party. Planview employees are prohibited access to any user project data or uploaded documentation.

Planview has formulated a privacy statement which explains how the company gathers and disseminates user-related information. he statement is available on the Planview website: https://www.planview.com/legal/privacy-statement/.

Cookie information

Spigit and Planview.com use cookies to optimize the user experience. Cookies help make Spigit work according to user expectations. Cookies are used to keep track of user session information. No other data related to authentication or sessions is stored on the client. Session tokens expire after a period of non-activity by the user. This timeout period is configured by the customer, on the client system the user uses to access Spigit services.

Assurance: Tested and Approved

Cloud Security Alliance – STAR

The Security, Trust & Assurance Registry (STAR) of the Cloud Security Alliance® (CSA) is a publicly accessible registry, documenting the security controls provided by various cloud computing offerings, which help users assess the security of cloud providers they currently use or are considering using. It is a simple but powerful idea: cloud providers post self-assessments of their cloud services, which CSA makes publicly available so that cloud consumers can make more informed purchasing decisions. Planview's participation with Spigit in this initiative and openly publishes information about its security controls in place.

Independent audits

Planview commits considerable resources to continually assessing security threats, as well as developing its infrastructure and system's security functions. The Spigit infrastructure and application is subject to regular vulnerability scans (on a monthly basis) with annual penetration tests carried out by independent third parties. Additionally, Planview entrusts external auditors to evaluate its information security practices and general IT controls.

About Planview

As the global leader in work and resource management, Planview makes it easier for all organizations to achieve their business goals. We provide the industry's most comprehensive solutions designed for strategic planning, portfolio and resource management, product innovation, capability and technology management, Lean and Agile delivery, and collaborative work management. Our solutions span every class of work, resource, and organization to address the varying needs of diverse and distributed teams, departments, and enterprises. Headquartered in Austin, Texas, Planview's more than 700 employees serve 5,000 customers worldwide through a culture of innovative technology leadership, deep market expertise, and highly engaged communities. For more information, visit www.planview.com.