Spigit Statement of Security and Architecture Standards

Contents

1 General Information

1.1 Planview Headquarters

Planview HQ address:

12301 Research Blvd.

Building V, Ste. 101

Austin, Texas 78759

No customer data is stored at Planview Corporate HQ. However, to protect against any possible fraudulent access to any internal systems, all Planview vendors, guests, and visitors are escorted upon arrival.

The Planview Corporate HQ building is accessible only by keycard access.

1.2 Spigit Information Security

Information is a critical asset for Planview. Information security is the protection of information from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. All Planview information security policies, standards, guidelines, and practices are coordinated through the Planview Operations teams, which are responsible for ensuring a consistent enterprise-wide approach in developing, implementing, and managing information systems security.

Planview's corporate wireless is secured with WPA2 Enterprise. This protocol known as 802.1X is an IEEE standard framework for encrypting and authenticating a user who is trying to associate to a wired or wireless network.

WPA2-Enterprise uses TKIP with AES encryption.

To ensure the confidentiality and integrity of the customer data, servers hosting customer data can only be accessed by authorized Planview support personnel with back-end access requiring VPN and SSH along with multifactor authentication and front-end access requiring VPN and multifactor authentication.

Privileged user access is reviewed on at least a semi-annual basis for the Spigit production tools, server access, source code access, and privileged access. Access flagged for modification or removal is tracked in a ticket and removed upon completion of the review. The review includes a comparison of the application user access listings to the list of active employees to identify terminated users who no longer require access. The review also incorporates an assessment of access based on current job responsibilities to identify users who no longer require access to perform their job requirements.

Planview has documented user access policies and procedures and implemented supporting business processes and technical measures for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and Spigit application interfaces and infrastructure, network, and systems components.

Access to the Spigit hosing infrastructure is granted on a least-privilege, need-to-know basis and requires a separate VPN connection and two-factor authentication.

Access to, and use of, audit tools that interact with the Spigit solution infrastructure is appropriately segmented and restricted to prevent compromise and misuse of log data. User access to diagnostic and configuration ports on Spigit network components are restricted to authorized individuals and applications.

1.3 Separation of Data

Spigit keeps a clear separation between its internal IT operations and the production infrastructure where the Spigit application is hosted. Corporate headquarters includes all normal operational divisions of the company, including Sales, Marketing, Services, Internal IT, and so on. The Spigit application is hosted by Rackspace. Backup hosted at AWS S3 facilities.

1.4 Service Level

Note: This service level is subject to the limitations set forth in the Master Service Agreement.

Spigit service is available 24 hours per day, 7 days per week, and 365 days per year, 99.5% of the time. Refer to the Master Service Agreement for information about scheduled downtime and remedies for uptime that falls below 99.5%,

2 Third-Party Audit and Attestation

Planview has obtained a SOC 2 Type 1 attestation for the Spigit solution from BPM Accountants & Consultants. SOC 2 Type I provides a snapshot of operations and procedures in place at a certain point in time. The SOC 2 Type I report is available with a signed NDA.

Planview has also completed independent, third-party audits such as application vulnerability scans, and network penetration tests. The results of the application vulnerability scans and network penetration tests are available with a signed NDA. Because Planview products do not store or process any medical related data, the solutions do not fall under the requirements for HIPAA compliancy.

Similarly, Planview products do not process credit card information, and thus do not require PCI (Payment Card Industry) certification.

3 Service Partners

All Spigit Production primary data is hosted by Rackspace.

Rackspace is a highly secure data center that utilizes state-of-the art electronic surveillance and multi-factor access control systems and is staffed 24x7 by operations support staff. Environmental systems are designed to minimize the impact of disruptions to operations.

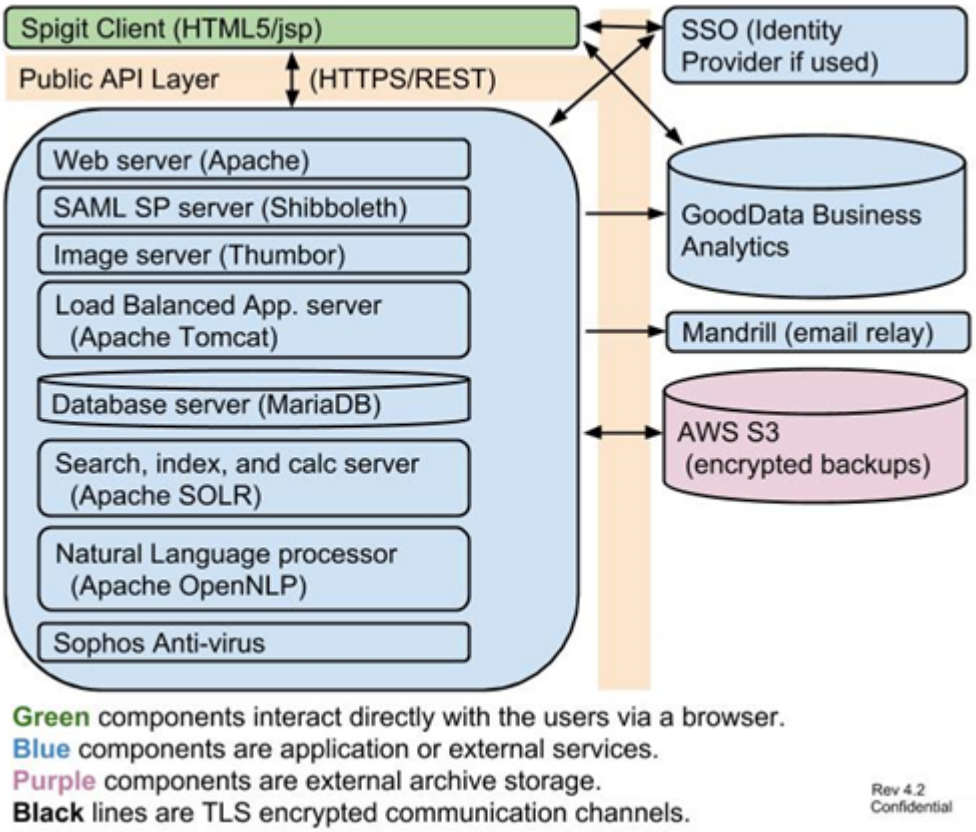
Backup hosted at AWS S3 facilities.

Third-party service providers for the Spigit service do not have logical access to customer data stored within the Spigit solution.

The service providers that host primary and backup data for the Spigit solution have robust security in place, adhering to compliance with industry and government requirements for security and data protection. The IT infrastructure that these service providers is designed and managed in alignment with best security practices and a variety of IT security standards. Rackspace and AWS S3 both hold SOC 2 Type II attestations, and both providers are ISO 27001 certified.

4 System and Network Security

This section provides an overview of the Spigit Network topology, describes the different environments covered by the Spigit network, and lists the security measures taken to keep systems secure at the login level. These security measures are in addition to standard security that is already applied by Rackspace to its full infrastructure.



The Spigit technology stack consists of state-of-the-art products paired with industry leading applications to monitor the SaaS for the following:

- SLA Management
- End User Performance Management
- Application
- Application and OS
- Network
- Vulnerability Management and Compliance

All event logs recording user activities, exceptions, faults and information security events from critical Planview infrastructure and applications are produced and retained for at least one year.

Independent 3rd-party Application Vulnerability Scans and Network Penetration tests are performed on the Spigit system annually. Test results can be obtained with a signed NDA.

Access to the Spigit hosing infrastructure is granted on a least-privilege, need-to-know basis and requires a separate VPN connection and two-factor authentication.

One-way SSL is supported. The Spigit service does not employ mutually-based authentication for accessing its UI, and therefore sharing keys is not an option. Planview recommends that clients with a high-risk profile implement SSO and/or IP whitelisting to ensure the UI is only accessible by authorized users.

The Spigit solution infrastructure systems are on a logically separate network, accessible through VPN via two-factor authentication from the Planview office. Access to servers hosting customer data can only be accessed by authorized Planview support personnel with back-end access requiring VPN and SSH along with multifactor authentication and front-end access requiring VPN and multifactor authentication.

All personal computers that need access to the production network are configured to comply with VPN and Network policies. Only VPN clients approved by Spigit Operations can be used. To obtain access to a production network, an employee must be approved for specific access as part of their standard role. If access is requested by an employee whose role typically does not permit access, the access is reviewed and approved by Spigit Operations team members.

5 Application Level Security

This section describes how the Spigit application itself is protected, and it describes the application architecture.

5.1 Passwords

Individual access is governed by a strong password policy, and the passwords are stored in a one-way hash using a SHA-256-bit cipher.

There are two ways to configure how password authentication is handled.

- Passwords can be authenticated against a company's internal directory/identity service by integrating the Spigit solution with a SAML-based SSO application.
- The application can be configured to manage password authentication locally against its own database.

Spigit Strong Passwords

In both scenarios listed above – integrating Spigit services with an SSO application or managing password authentication locally against its own database – the customer administrator for the Spigit solution can choose to globally use strong passwords.

Strong passwords are at least eight but no more than 50 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 (that is, characters in range [\x00-\x1F].

Password Properties

- First Login — If authenticating against a local database, users must create a new password the first time they log in.

- Minimum Password Age — If using SSO, your identity management password change policies are used for password changes. If using application authentication, there is not a configurable minimum wait time for consecutive password changes.
- Password Expiration — If using SSO, your identity management system policies are used for password expiration settings. If using application authentication with a UserID/Password, then password expiration settings are not available in the application.
- Password Reuse — If using SSO, your identity management system policies are used for password history. If using application authentication with a UserID/Password, then password history settings are not available in the application.
- If SSO is not in use, the customer administrator can configure user accounts to require password changes upon first login, but expiration intervals are not available.
- In the SSO scenario, Spigit never collects the user's credentials. If a customer is configured for SSO, users are redirected to the customer's SSO Identity Provider (idP) for authentication. Once authenticated, the idP provides an assertion containing the user's Spigit UserID and the user will bypass the Spigit login process. In addition to the benefits mentioned above for delegated authentication, SSO has the following advantages:
    - Spigit never sees the user's credentials, and this method is more secure because user passwords are only exchanged between the web browser and the idP. There is no chance for an external application to capture passwords.
    - Users can login once with the idP and bypass the login process for all web application that are configured for SSO.
    - User passwords can be administered in a central repository under the control of the customer. This allows customers to administer the level of password security their organizations desire or are comfortable with.

5.2 Cookies

Session 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.

5.3 IP Whitelisting

IP Ranges allow your organization to specify exactly which IP addresses can access your instance of Spigit. This gives your organization an extra layer of control and security. These IP address ranges can be configured by the local administrator.

5.4 Role-Based Permissions

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.

5.5 Logical Separation

The hosting environment is a single tenant private cloud where each client has a separate and unique application stack to provide logical separation from other clients.

5.6 Data Storage

The Data Access tier is responsible for all reading and writing of data and interaction with the back-end MariaDB database.

The Spigit solution encompasses enterprise class SSD storage configured in fault tolerant RAID 10 configurations with full disk encryption (AES256). All data is stored within a MariaDB database.

Database servers are accessible from outside the production network only by VPN with two-factor authentication.

Access and server logs recording user activities, exceptions, faults and information security events are produced with central log correlation and analysis in Alert Logic. Log data is encrypted in transit and in storage. The data is available online to internal Planview staff for analysis or reporting for 365 days. Clients may request a report via the customer portal by submitting a ticket.

The Spigit service can offer an audit extract upon request.

5.7 Data in Transit

All data transmission is performed using transport layer security (TLS) for all API and user communications between the users' browser and the application using strong Diffie Hellman ciphers and SSL digital certificates with RSA 4096-bit key strength.

5.8 Integrations

Integration with the Spigit application is enabled through an open API platform. One option is for the customer to directly connect with the Spigit solution using the open API platform. The other option is to engage with the Planview Services team to build a custom integration. From a security perspective, both options still connect through the same layers of processing as the standard UI. All application and database tier security are still applied and fully enforced.

6 Backups and Disaster Recovery

The Spigit system hosts offsite backup at AWS S3 facilities.

The Spigit service categorizes RTO as follows. The RPO for all RTO categories is 24 hours:

- Category 1 – 4-hour RTO

  This would be characterized by single or multiple hardware failures within the primary data center, or the intentional destruction of data within the data center. This would include disk, server, network firewall, or other equipment failure(s), or human induced non-physical destruction of data or environment. This damage would require the repair of the affected components, and the recovery of data.

- Category 2 – 2-day RTO

  This would be characterized by single or multiple hardware destruction within the primary data center. This describes serious and non-repairable damage to the hardware or rack infrastructure. This damage would likely require relocation within the data center facility, extensive equipment and software replacement, followed by data recovery.

- Category 3 – 7-day RTO

  Primary data center is destroyed or seriously compromised. Recovery requires replacing destroyed SaaS infrastructure in alternate data center, and recovery of data. RTO (Recovery Time Objective) is 4 hours.

Spigit backup processes include a nightly full backup that is encrypted and housed in AWS S3 facilities in the same geographical region as the primary storage. Backup is retained for 30 days.

Internally, customer data is never backed up to removable media. All data will be returned to the client in an encrypted flat file at the end of term.

7 Incident Response

Escalation procedure requires immediate notification of a security breach. An email notification can be sent to customercare@planview.com. Submissions are stored as uniquely numbered tickets in the system and automatically routed to a Customer Care Consultant. Planview team members can investigate the case and escalate accordingly.

In the event of a security breach or customer impacting event, Planview follows the standard communication policy, as communicated in the Master Service Agreement, for Severity 1 and 2 errors. Severity 1 and 2 errors are followed by a formal Incident report that is sent to the designated Spigit administrators for all impacted customers.

Planview will use commercially reasonable efforts to restore service or remedy a security breach/event as soon as possible. In the event of a security breach, all external services would be disabled immediately while the breach is analyzed and resolved. Planview will work with customers to disclose all areas breached.

Planview targets a 24-hour delivery of formal Incident reports. To date, Planview has not encountered a security breach that had the potential to expose sensitive data.

8 Change Management Procedures and Processes

Planview has change control processes in place to protect all Production Assets from unauthorized modification. All changes adhere to the Planview Change Control Process. Planview follows a traditional six-step change control and change management process:

- Record/classify
- Assess
- Plan
- Build/test
- Implement/post-implementation review
- Close/customer acceptance

All changes are scheduled during maintenance window unless there is an emergency for security or severity reasons. Planview formally holds a weekly architectural review board meeting prior to any changes to production, and Planview holds emergency meetings on demand. This practice ensures that changes are implemented with minimal services disruptions and, although a rollback plan is always documented, backout activities are rarely seen. Refer to terms of service for information about the maintenance window for your Planview product(s).

All system and network additions, replacements, changes, and upgrades adhere to the standard Planview change control process.

Planview operations teams regularly monitor Technical Service Bulletins issued from vendors and implements recommended patches or fixes according to severity and security threat. All patches are implemented in accordance with the standard Planview change control process. Planview also runs vulnerability scans monthly and adheres to their remediation methods.

When code updates have passed testing and have been approved, operations team members apply the changes to production. The process of code change and release include thorough regression and validation testing by QA. Staging environments include but are not limited to testing for authentication, authorization and accounting functions. All application changes to production are also monitored from an infrastructure standpoint to record changes and establish baselines.

New Developers

All developers are required to attend 2 weeks of intensive in-house training on the codebase and application stack with emphasis on security policies and best practices. Planview uses PMD to search for source code problems and suboptimal code.

Source Code Control

Planview Spigit team members use GitHub for revision control and source code management system.

Binary Code Analysis Review

Binary Code Analysis review can be coordinated on an as-needed basis.

Miscellaneous practices

The following practices are not standard but have been requested by various customers/prospects in the past. These can be coordinated and, with an executed non-disclosure agreement, performed during a scheduled maintenance window:

- Black Box Testing
- Application Penetration Testing

9 Human Resources Security

Planview adheres to a standard screening process for all individuals seeking employment with the company. Reference checks are performed on all employees, and individuals offered employment from Planview must read and sign the Information Security Policy, Employee Handbook, and a Non-Disclosure Agreement before gaining access to Spigit services production systems. Policy acknowledgements are retained in employees' permanent personnel files.