Security FAQs
Updated 4/2025

Do you have audit reports such as SOC2 or ISO 27001?

We do not have SOC2 or ISO 27001. Our role is limited to providing Salesforce native applications that operate entirely within your Salesforce environment. These applications will not send any data out of your Salesforce environment, except for:

1. Non-sensitive debugging information when the application encounters an exception during usage or installation (code error messages, code stack traces), via email and Salesforce's provided functionality: https://developer.salesforce.com/docs/atlas.en-us.packagingGuide.meta/packagingGuide/packaging_notification.htm
2. Application usage data, collected via Salesforce's *AppExchange App Analytics* feature, via Salesforce feature parameters, and via email.

Salesforce's SOC2 report can be downloaded by customers with a valid Salesforce login here:

https://compliance.salesforce.com/en/documents/a005A00000k50uvQAA

See our Privacy Policy's 'Use of Your Information' section for details on how we use this information: https://www.passagetechnology.com/privacy-policy

For all other data, Salesforce, not us, acts as the data processor and is responsible for ensuring compliance with data security standards. Please refer to the following links for Salesforce's audit reports:

https://compliance.salesforce.com/en

https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf

What kind of security audits or security programs do you have?

Our applications are audited by Salesforce to ensure data security via Salesforce's security review process, which is mandatory for an ISV application to be publicly listed on the AppExchange:

https://developer.salesforce.com/docs/atlas.en-us.packagingGuide.meta/packagingGuide/security_review_overview.htm.

Adhering to Salesforce's security requirements, we also have multiple internal processes to identify code vulnerabilities, including a continuous static analysis process, a strict release management process, and code reviews performed by Salesforce certified professionals.

As the first security check, every proposed code change will be scanned automatically by a static code analysis engine that prevents common security vulnerabilities from being introduced into our code base. The scan includes checks such as SOQL injection protection, CRUD access checks, and sharing violations. The static code analysis provides a developer with feedback that needs to be addressed prior to a code change being eligible for further code review.

Furthermore, before making any changes to our applications, a proposed code change is manually reviewed and tested by developers and the service owner for security issues among other factors. If the change is a more significant update to the application it may also require reviews from additional team members, which includes Salesforce certified Sharing and Visibility Architects who have extensive experience working with the Salesforce security team.

When code change makes it into a new version of the application, the service owner and product owner will run the code through the Force.com Code Scanner in addition to testing in sandboxes and in our own production environment. After a period of monitoring for quality issues and seeking out any issues related to the application's security, the new version will be push-upgraded to applicable sandboxes with a much longer period of monitoring. Once we are confident with the new version's security and performance, we will finally publish it as a released version of the application.

What are the implications of a "Salesforce native application"?

Our applications are 100% native, meaning they operate entirely within your Salesforce environment except for diagnostic and usage data collected via email, feature parameters, and Salesforce's *AppExchange App Analytics* feature.

Salesforce native applications have the following benefits:

- Enhanced security and up-time as they are contained in your Salesforce environment
- Faster performance without the delay of external callouts
- Real-time access to data with no delays from third-party servers
- Seamless integration with other native apps on the Salesforce platform

This comes with a trade-off of limited processing power due to Salesforce's multitenant nature.

Do you use any APIs?

Some of our applications use internal Salesforce Platform APIs such as the Metadata API. However, we do not store any kind of access token anywhere. Our applications also do not transmit any data outside of Salesforce via these APIs.

For example, the Metadata API is used for trigger and field deployment within your Salesforce environment. It uses User Session ID for authentication, which is only accessed for the duration of an Apex transaction, and remains inaccessible for all other users besides the owner. The entire deployment process occurs within your Salesforce environment and does not require any external connections.

Are there additional resources available regarding data and privacy?

Here are some other resources with more information regarding your data and privacy:

https://www.passagetechnology.com/privacy-policy

https://www.passagetechnology.com/master-subscription-agreement

https://www.passagetechnology.com/terms-of-service

https://www.passagetechnology.com/data-processing-agreement-processor