Secure Development at Tableau

Introduction

At Tableau, we understand that your data's security and protection are critical to your business, and we take the safety of your data very seriously.

As part of Salesforce, trust is our #1 value, and delivering secure products to our customers is a key part of this trust. The secure software development life cycle (SSDL) process described in this document is the foundation for this delivery. For purposes of this document, the process outlined focuses on delivery to our on-premises customers.[1]

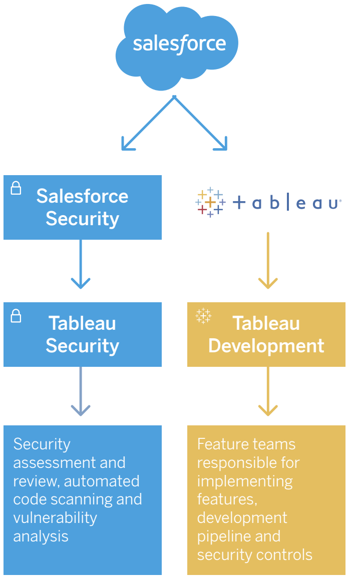
[1] While the core of our hosted offerings are based on our on-premises software, the whole of this document (with the exception of packaging the software into installers) is also relevant to Tableau Online.

Contents

Governance

Before we dig into our process for securely developing Tableau products, it's important to first understand the governance structures that direct its execution.

Accountable Teams


salesforce
Salesforce Security
tableau
Tableau Security
Tableau Development
Security assessment and review, automated code scanning and vulnerability analysis
Feature teams responsible for implementing features, development pipeline and security controls

This chart shows the various teams involved in building and delivering secure Tableau products. There are two primary teams responsible for secure development of Tableau products: the Tableau Security Team and the Tableau Development Team.

The Tableau Security Team is part of the larger Salesforce Security organization, dedicating all of its resources to securing the Tableau product line. The Tableau Security Team performs several functions including security reviews of Tableau products, automated code scanning, and vulnerability analysis. The Salesforce security team supports the Tableau Security team in several areas including incident response and governance functions, such as policy and standards development.

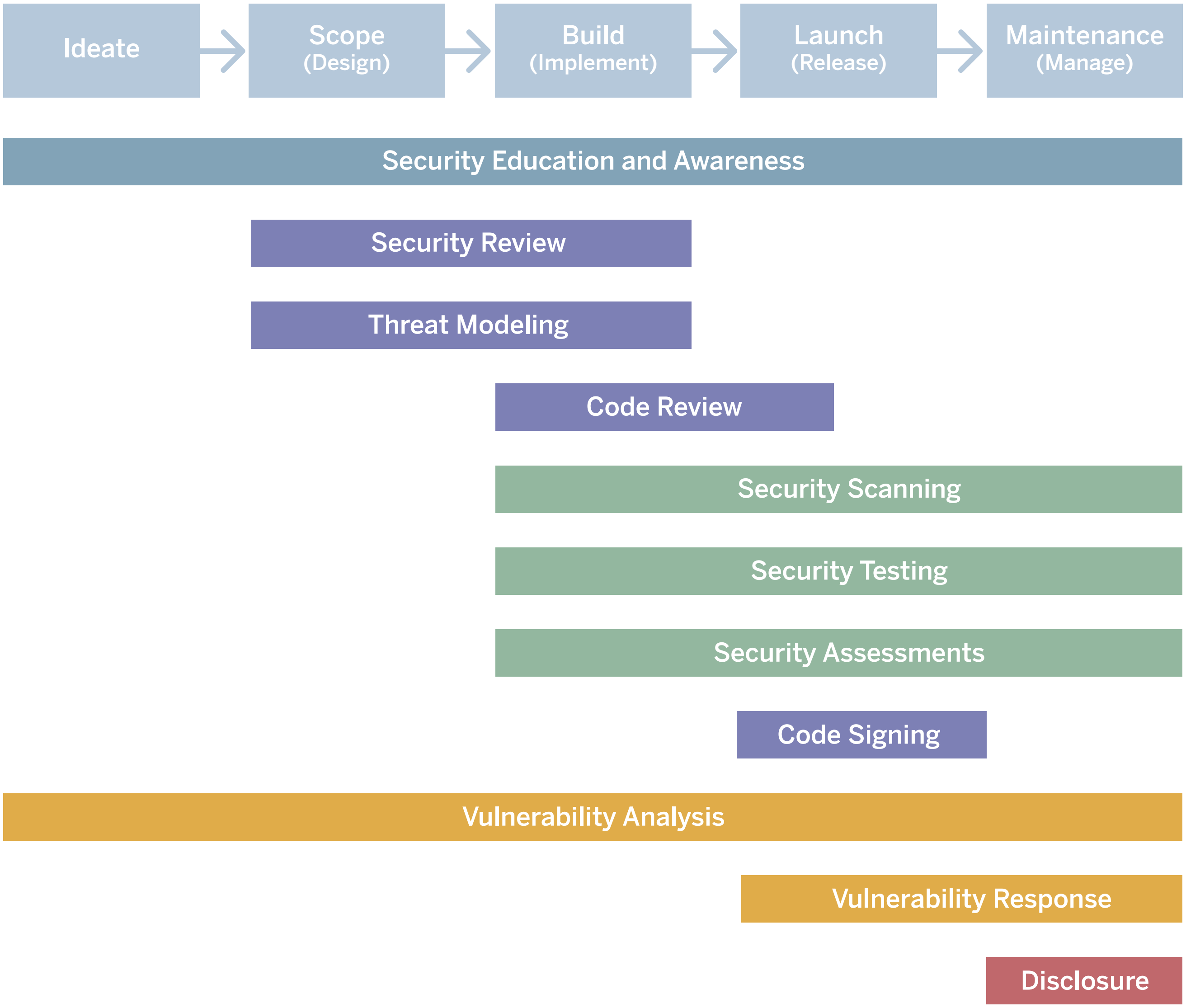
The Tableau Development team is oriented in the broader Salesforce product organization. This team maintains feature teams, which are staffed with project managers and engineers responsible for developing features, implementing security controls, and building the development pipelines in alignment with the standards set by the Security Team.

Policies and standards

As part of Tableau's Salesforce integration, the existing suite of Tableau security policies and standards were reviewed by the Salesforce Governance, Risk, and Compliance team for their comprehensiveness, suitability, and alignment to the wider Salesforce security standards. These policies were adjusted accordingly, and were additionally complemented by the other security standards maintained by Salesforce Security. This combination means that Tableau products are now governed by a comprehensive set of security policies and standards dedicated to maintaining our customer trust and the security, availability, and integrity of Tableau products. The details of these policies and standards are proprietary and not available externally, but are partially reflected in our SOC 2 (System and Organization Controls) report, which is available to customers at https://compliance.salesforce.com.

Secure software development life cycle

In order to illustrate the Tableau secure software development process, the following sections track a Tableau feature in its security journey through product launch and beyond. The diagram below provides an overview of the SSDL and how security is integrated throughout the process:



Development phases

The phases of the SSDL are summarized below to provide context for the security aspects described later in the document.

Ideate phase

The development process begins with the Ideate Phase. The purpose of the ideate phase is to develop a product idea and communicate it to teams so they can start working on scoping the work involved. Ideas for features often come from Tableau Customer Forums and other customer feedback mechanisms. Product managers and engineers work together to bring the feature to life. This phase includes customer meetings to understand feature requirements and analysis of Tableau Product Usage data to explore the applicable use cases. Not all features are visible to customers, as some features may be architectural, security, or other technical improvements driven by engineering that may not directly impact downstream customers.

Scope phase

Following the Ideate Phase, the Scoping Phase begins. The purpose of this phase is to scope the work required to build the feature so management can determine if the project should be approved and how resources would be assigned to the project. During this phase, product managers and engineers write specifications and test plans for the feature. The Feature Team engages with other Tableau teams, such as the User Experience, Performance and Security Team to define user interactions, security requirements, and performance considerations. The Feature Team assigns a preliminary estimate of the project's development size and complexity to help with resourcing and funding decisions. The product manager creates items in the work tracking system to track the feature through the build and launch phases.

Build phase

After a feature is scoped, the Build Phase begins. The purpose of the implementation phase is to build and test the feature to meet the requirements defined in previous phases. The Feature Team engineers write the code in accordance with the functional and design specifications. They also develop tests according to the test plan to test both functionality and security requirements. The Security Team conducts security reviews and security scanning to uncover risks and flaws introduced in design and implementation. The findings from these activities result in updates to test plans and new work items to track the required changes in the product.

Launch phase

The purpose of the Launch Phase is to build the final product binaries and installers to incorporate the newly implemented features for delivery to customers. In this phase, a final round of automated and manual testing is completed and any resulting high priority defects are fixed. The release team has a release checklist that validates that test sign-off has completed. If these criteria are not met then the product cannot release without approval at the executive level. If all items are checked off then the product is uploaded to the Tableau website and linked to the download pages for customers to access.

Maintenance phase (Post-release)

The purpose of the Maintenance Phase is to provide customers with software updates and to collect information about how the product is used. After the product releases, Development and Security Teams continue to monitor and maintain the product until it reaches end of life. Potential issues are discovered in our products through customer reports, penetration tests, monitoring of third-party vulnerabilities, crash reports and product telemetry. Maintenance releases deliver fixes for security vulnerabilities, if identified, to customers. An abbreviated launch phase progresses for maintenance releases with an abbreviated release checklist that ensures there are work tracking items documenting the reasons for changes in the release, reported issues have been fixed and required tests have passed. Maintenance releases are usually posted every month; however, they may be posted more often if a critical issue is found or less often if there are fewer issues found. Customer feedback and telemetry from deployed products collected during the Maintenance Phase help the development team identify new features to feed into the Ideate Phase for future iterations of the SSDL.

Security process detail

This section details the various security processes that integrate into the pre-release portion of the SSDL up to and including the launch of the product.

Security education and awareness

The security journey starts before the inception of a feature idea with a security awareness and education program. Tableau's initial security training efforts focused on an annual security awareness program educating members of the development organization on Tableau's security policies and secure development processes. With integration into Salesforce, Tableau gained access to an entire library of security-related Trailhead courses, which now are an integral part in meeting Tableau's security awareness requirements. Annual security training covers security requirements during all phases of the development process. In addition, the Tableau development team received supplemental security training on secure coding in the languages and frameworks they use for their daily job as part of the security integration with Salesforce.

Security review

The SSDL requires that all features delivered to customers must successfully complete a formal security review process. After entering the feature into Tableau's work tracking system, the Engineering Lead or Product Manager begins the review process by filling out a security review questionnaire. The Security Team creates the questionnaire to understand risks, such as those associated with complexity, different classifications of data, new interfaces, new 3rd party components and the use of certain technologies, such as encryption. The questionnaire also contains links to important documentation including the feature tracking work item, functional specification, design specification and threat model. The completion of this questionnaire opens a ticket with the Security Team, who triage the ticket and assign it to a Security Engineer to review the provided documentation and work with the feature team to assess the feature's risk.

For simple features, reviews for low-risk changes can be closed out by the security engineer by reviewing the provided documentation to understand the risk without having to meet with the Feature Team. For more complex and higher-risk features, the security engineer works with the feature team to understand the changes involved which, in some cases, requires one or more meetings to discuss how to mitigate risks associated with the feature's design, implementation and use. As a result of the review, prioritized work items are assigned to the feature teams to mitigate the identified risks prior to delivery. These work items may include updates to product code, tests, or documentation. Additional follow-up reviews, including manual code review, may be scheduled as the feature is refined. The security review process can start as early as the ideate phase and must complete (with approved resolutions, where applicable) before the launch phase. During the build phase, the Security Team or feature team may request additional security-focused code review of security-sensitive code if there is reason to believe there is a high risk with implementation errors, such as in authentication code and code that interfaces with cryptographic functions. As part of launching the product, the Security Team validates that product security features have the appropriate level of security review for the amount of risk introduced by the change.

Threat modeling

Threat modeling is a formal process used to identify a feature's security threats, risks, and their associated mitigations in a system. As part of the Salesforce integration, the Tableau Security Team worked with feature teams to develop threat models of existing components using Salesforce security standards. This effort not only identified places for security improvement within our system, but it also created a library of threat models to use as the basis for future security reviews and other security investigations. Teams must now reference a new or existing threat model in their security review questionnaires. Threat modeling can begin as early as the ideate phase and must complete before the launch phase. New threat models or updates to existing threat models are reviewed and findings are addressed as part of the security review process defined above.

Source control and build systems

Code is managed in a source control system that has security controls for read and write access and for tracking changes introduced into the code. Access to source control and build systems requires authentication against the enterprise identity systems. This ensures that changes to the source code are controlled and traceable. As part of the Salesforce integration, the Tableau source control and build systems have been hardened in accordance with Salesforce Standards for their respective platforms. These systems are continuously monitored for 3rd party vulnerabilities by the Security Team so they can be patched by the build systems team to address known vulnerabilities.

Software integrity

The release process incorporates newly implemented features into product binaries and installers. The binaries and installers for Windows and Mac OSX are digitally signed and notarized according to the best practices of their respective platforms. Additions, deletions or changes to the installer cannot be made without invalidating the digital signature. The signatures are based on a public trust root, allowing customers to verify the integrity and authenticity of the software they receive. Code signing and notarization happens during the launch phase of the process by the release team.

Third-party components

Tableau products include third-party open source (OSS) and commercial components, such as libraries and frameworks. In addition to providing feature functionality, these components help engineers implement security controls such as input validation, output encoding, encryption, and web application vulnerability protection, in a proven and consistent way. Before a third-party component is incorporated into a Tableau product, it must pass the security review process described above. Various tools are used to scan products and development artifacts for known third-party vulnerabilities (as described in the next section). Customers may request an Open Source Software Disclosure list for Tableau products through their account team.

The process for incorporating a third-party component into a Tableau product may start in the ideate phase. Addressing security vulnerabilities in 3rd party components continues through the maintenance phase as described in the vulnerability response section below.

Automated testing

Feature Team Engineers write automated tests to exercise new code and make sure it meets the requirements of the functional and design specifications. This testing includes security-related tests identified in the security review and threat modeling processes. The automated tests run in conjunction with the build process to make sure changes behave as expected. The goal is that any problems are discovered early before they have a chance to propagate into the product. Security vulnerabilities found during the testing processes before release are fixed by the feature team. All identified vulnerabilities affecting released products are handled through the vulnerability and response section described below.

Security and vulnerability scanning

The Tableau Security Team deploys and monitors a number of scanning tools from different vendors to further validate our products. The following are areas of security scanning:

- Static Analysis tools scan source and compiled code to identify security related coding flaws and vulnerabilities

- Software Composition analysis tools scan code for third-party software components that may contain known vulnerabilities

- Web Application Vulnerability Scanners continuously monitor pre-production and production systems hosting Tableau Server code for vulnerabilities

- Credential Scanning Tools scan source code to ensure that secret credentials are not incorporated into product source

- Container Scanning Tools scan container-based products, such as Tableau Server in Container, to uncover vulnerabilities in the layers that make up the container image

The Security Team processes the findings from these tools according to the vulnerability analysis and response section described below. As the integration with Salesforce continues, scanning tools will be added to cover searching for differing types of vulnerabilities in various types of code.

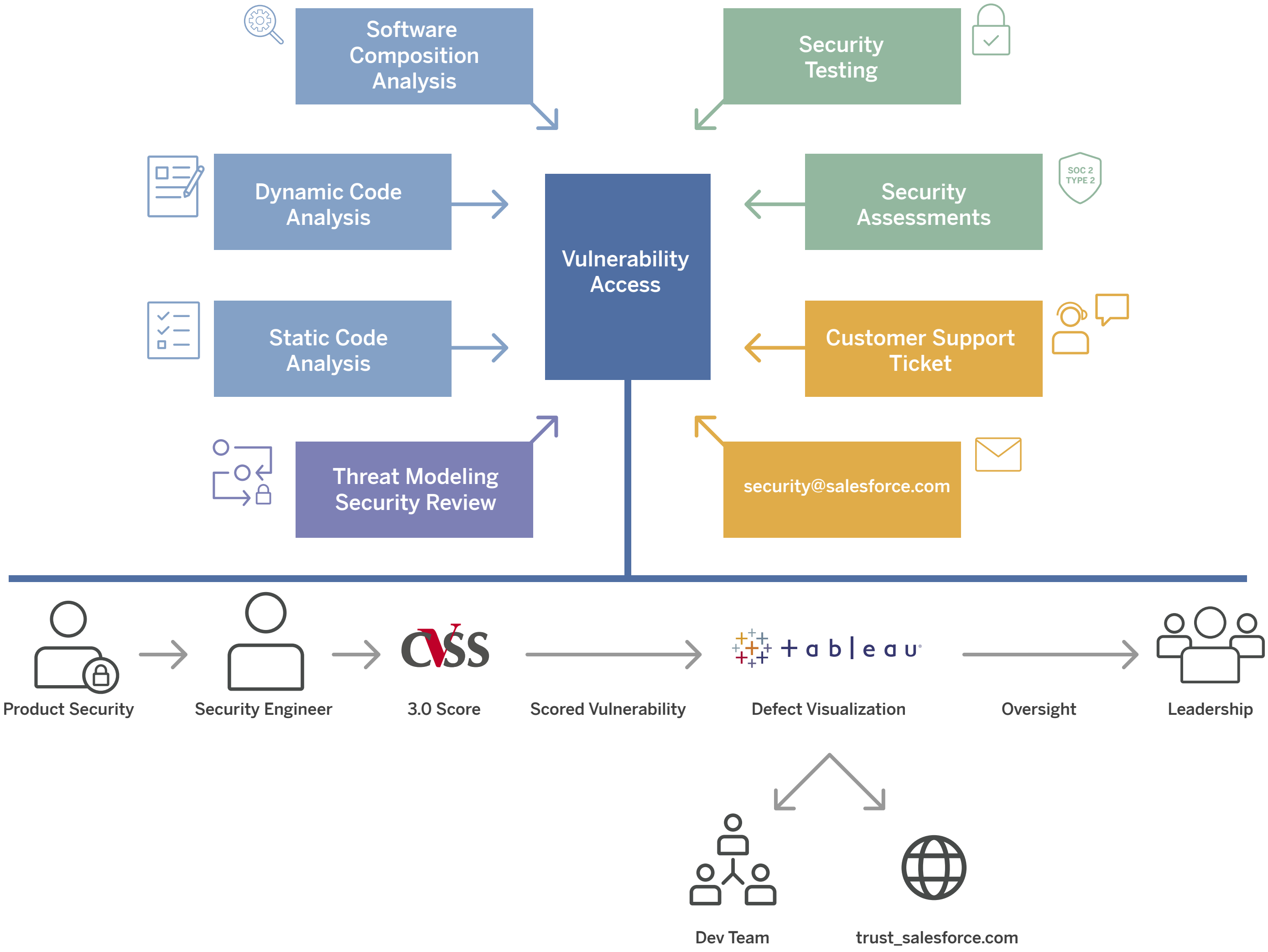
Automated tools scan code during the Build Phase. This scanning continues through the Launch Phase and into the Maintenance Phase.

Security assessments

Tableau engages with external security firms to perform periodic external security assessments (penetration tests) on an annual basis. These assessments apply extra scrutiny to any newly developed features since the previous assessment. In addition, the Tableau Security Team conducts internal security assessments on Tableau Products. Salesforce also maintains internal penetration test teams that supplement this security assessment coverage. As part of the Salesforce integration, extensive third-party security assessments were conducted on Tableau products. Customers can obtain letters of engagement for security assessments under NDA by contacting their account team. Any vulnerabilities found are handled as described in the vulnerability and response section, below.

Security assessments are conducted after there is a cutoff to changes in the area of the feature under test. This effort may begin in the Build Phase, but it is also carried out during the Launch and Maintenance phases.

Vulnerability Analysis and Response



In addition to the security controls described above, Tableau also maintains a comprehensive vulnerability analysis and response process to address any identified vulnerabilities that are inevitably discovered as both attackers and our codebase evolve. Vulnerabilities can be found and analyzed in any phase of the SDLC process. Tableau's Security Team hands off any issues identified before a product or feature is launched to the Tableau Development Team for remediation. For issues identified after launch, Tableau provides maintenance releases to address security vulnerabilities as described in the Maintenance Phase section, as well as security disclosures, described in a following section, to help customers assess the resulting risk to their environments.

Vulnerability reporting and analysis

As you can see from the previous sections, we continuously probe for vulnerabilities in our products. Vulnerability reports from automated scanners, customers, researchers, testers, security assessments and other sources are funneled to the Security Team for analysis. Customers and researchers may conduct their own tests on our on-prem products and report vulnerabilities through technical support channels or our public email address at security@salesforce.com. The product Security Team has a daily stand-up triage meeting to review reports from all of these various sources and assign them to security engineers for analysis to determine their scope, severity and impact.

The security engineer begins by understanding the vulnerability's impact on features and APIs within the product and on data generated, processed, stored, or transmitted by the product. Additional information is collected from the reporter as necessary to eliminate false positives. The engineer calculates an initial base vulnerability score using the Common Vulnerability Scoring System (CVSS) 3.0 and creates a defect assigned to the responsible feature team for remediation. The feature team works with the Security Team to further refine the impact and severity assessment. The feature team owns the responsibility of remediating the vulnerability in accordance with target timelines as determined by the severity and internal Salesforce Policy. The feature team uses their existing Root Cause Analysis (RCA) and post-mortem process to address underlying issues that contributed to the cause of the vulnerability.

Third-party components and known vulnerabilities

It is often the case that vulnerabilities are found in 3rd party components and disclosed through the National Vulnerability Database (NVD) and other sources. In this case, a CVSS severity is defined in the Common Vulnerabilities and Exposures (CVE) report associated with the component. The Security Team analyzes these reports as above to determine impact and severity to help prioritize the issue. In the past, this analysis could lower the severity of the issue if the analysis revealed that the impact of the vulnerability was mitigated by the way the component was used. With the security uplift we are modifying the process so the vulnerability score will not be lowered and the baseline remediation priority and timelines will be determined by the original CVSS severity scoring. This new criterion will put more emphasis on fixing these items which better aligns with customer expectations, however we have many existing components in need of an update and it will take several releases to complete this work. 3rd party component security updates will not usually be backported into older releases unless there is an executable code path that exposes the vulnerability.

Remediation and disclosure

Fixes for security issues are made available in maintenance releases. Tableau currently follows a coordinated disclosure process. When vulnerabilities of medium severity or higher are fixed within a maintenance release, Tableau publishes a disclosure informing customers of the issue so they can assess the risk to their environments. The Salesforce Security Advisory page lists the items fixed in a particular release. For higher-severity issues, a Common Vulnerabilities and Exposures (CVE) record will be published under the Salesforce numbering authority. Customers can also sign up to receive email alerts by registering a security contact for Tableau products through their customer portal.

Summary

As a member of the Salesforce product family, Tableau takes the security of its products seriously. Each step of the Tableau development lifecycle is designed to ensure security is integrated into every decision, regardless of whether a feature is in its early conceptualization or in its ongoing maintenance after delivery. Security considerations are injected into every phase of the Tableau development process, and include both automated processes and manual processes conducted by skilled security engineers. In addition, Tableau's robust vulnerability analysis and response process keep customers safe by fixing vulnerabilities and publishing security disclosures to keep them informed. Ongoing testing and external assessments ensure security is continuously reviewed and enhanced over time, and our standards are adjusted as needed to better align our delivery to maintain our customers' trust.

Additional resources

Salesforce Compliance Portal
Salesforce Security, Privacy & Architecture (SPARC)
Tableau Trust Portal
Salesforce Security Advisories
Cloud Security Alliance Cloud Control Matrix Self-Assessment
Tableau Help

tableau®