Deploying Tableau Server in U.S. Federal Government Applications:

FISMA | NIST SP 800-53 | DISA STIG

Contents

Introduction

For U.S. federal government agencies, Tableau Server enables security administrators to meet control requirements for the Federal Information Security Management Act (FISMA) when deployed in an on-premise IT system or in a cloud environment, making it a compliance-friendly platform. Tableau Server also allows agencies to achieve a higher level of security through the use of the Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGs) which primarily focus on secure application implementation within an agency environment. Hardening guides developed under DISA requirements traditionally follow a more secure set of parameters than guides adhering to Center for Internet Security Level 1 Benchmarks, a configuration standard referenced in NIST 800-53, Rev. 4.

FISMA is federal law passed in 2002 that requires federal agencies to develop, document, and implement an information security program that prescribes to the National Institute of Standards and Technology (NIST) 800-53 security controls and the NIST Risk Management Framework (RMF). The NIST RMF is the product of the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Programs and was developed to improve information security, enhance risk management processes, and unify agency security standards.

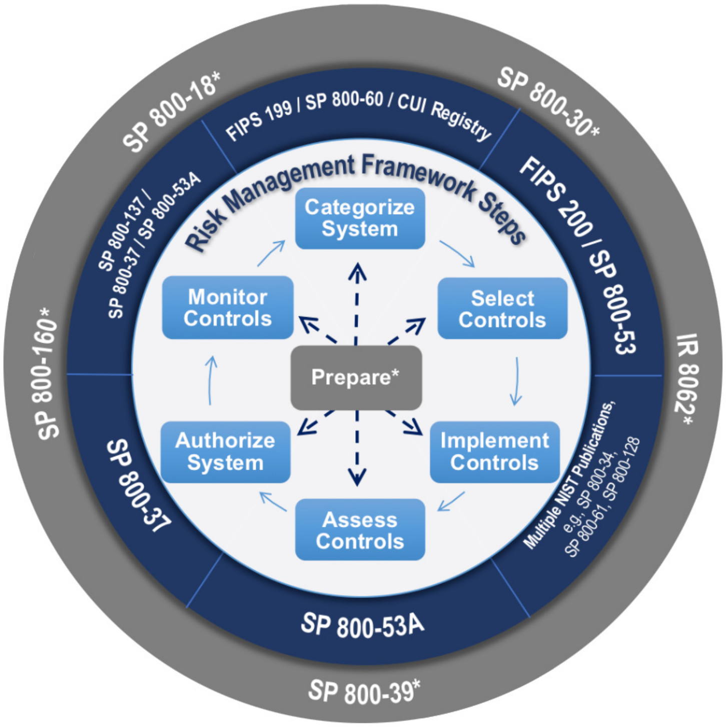

Figure 1 NIST Risk Management Framework (RMF)

The intent of this white paper is to provide information to IT professionals implementing Tableau Server within a FISMA-authorized on-premises or cloud-based IT system to ensure that Tableau Server adheres to the control requirements and overall security posture. This white paper assumes that IT professionals will integrate Tableau Server with an existing FISMA-compliant environment and that supporting controls such as centralized authentication (e.g. Active Directory), centralized log management, analysis and reporting capabilities through a Security Information and Event Management (SIEM), and network partitioning and network access control through virtual local area networks (VLANs) and firewalls are in place and may be integrated with Tableau Server where appropriate.

For FISMA, IT professionals must develop and maintain a System Security Plan (SSP) that addresses the implementation for each selected control. This white paper outlines Tableau Server's ability to support the implementation of applicable security controls, enabling IT professionals to update an IT system's SSP to address the secure deployment and use of Tableau Server. Tableau Server's features and core capabilities were compared with FISMA Moderate selected controls from NIST SP 800-53, Rev. 4 and analyzed for impacting or supporting control requirements.

This white paper only addresses control requirements that are relevant to the deployment, configuration, and maintenance of Tableau Server, with other control requirements being omitted as these will be addressed by underlying IT infrastructure. Lastly, control requirements were not independently tested by Coalfire. The opinions in this white paper represent Coalfire's judgement of documented Tableau Server features and controls from interviews with key Tableau personnel, product demonstrations, and published information sources supplied by Tableau.

Tableau Server Overview

Tableau Server offers Federal Agencies and government entities the ability to simplify sharing and collaborating on interactive data visualizations by offering the following advantages:

Simple Interface: Tableau Server makes it easy to find, explore, and interact with analytic dashboards for every type of user. Powerful search capabilities and intuitive navigation controls make discovering content, users, and data sources straightforward.

Flexible Data Architecture: If you have a fast database, Tableau Server can leverage that speed by maintaining live query connections back to that database. Alternatively, you can use Tableau Server to take in-memory snapshots of a data source (called extracts) and physically host that data on the Tableau Server platform.

Automatic Data and Content Updates: Tableau Server can refresh data extracts based on a set schedule, at specified intervals, or at incremental levels. You can also set alerts when data connections fail or use subscriptions to receive regularly scheduled emails about dashboards and reports.

Embedded Analytics: With Tableau Server, you can rapidly embed interactive dashboards within your organization's existing web portals. Built-in sharing capabilities quickly provide HTML snippets that you can use to place Tableau Server views directly into webpages, SharePoint portals, intranet wikis, and so on.

Scalable: Tableau Server scales with both hardware and memory to support a growing organization. Flexible content management, user permissions, and detailed administrative capabilities make managing a growing Tableau Server platform a straightforward process.

Enhanced Security: Tableau Server gives you security permissions at any level you need. With multi-tenancy, you can create multiple sites on the server to separate users and content. You can set individual permissions for projects, dashboards, or even users.

Mobility: You can view a dashboard from anywhere, on any device. All dashboards are automatically optimized for mobile tablets with touch-sensitive UI without requiring any additional authoring or configuration.

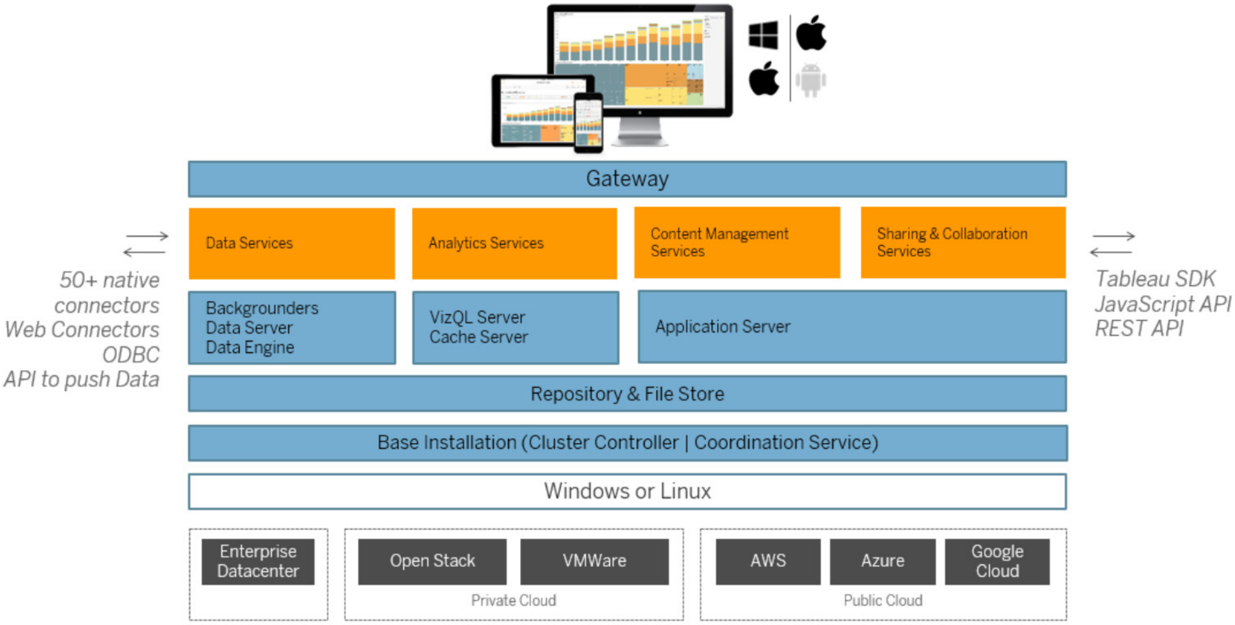

Figure 2 Tableau Server Architecture

FISMA Compliance with Tableau Server

Overview

Tableau has implemented select FISMA Moderate security controls in Tableau Server. The following tables provide Tableau Server's implementation description of select FISMA Moderate security controls from NIST SP 800-53, Rev. 4. Customers can leverage this information to properly implement Tableau Server within their existing FISMA-authorized solution (Figure 3) in accordance with FISMA requirements and security best practices. In addition to identifying Tableau Server capabilities that map to FISMA controls, the tables below denote the equivalent vulnerability identifiers from the DISA Application Security and Development STIG, Version 4. Each table has the following information:

Control ID (NIST SP 800-53, Rev 4)

Control Name (NIST SP 800-53, Rev 4)

Applicable CCI and CVE ID (Application Security and Development STIG, Version 4)

Implementation Description

The tables contain links to the definitions for each Control and CVE ID. For information on CCI IDs, please refer to the following U.S. Department of Defense DoD Cyber Exchange website.

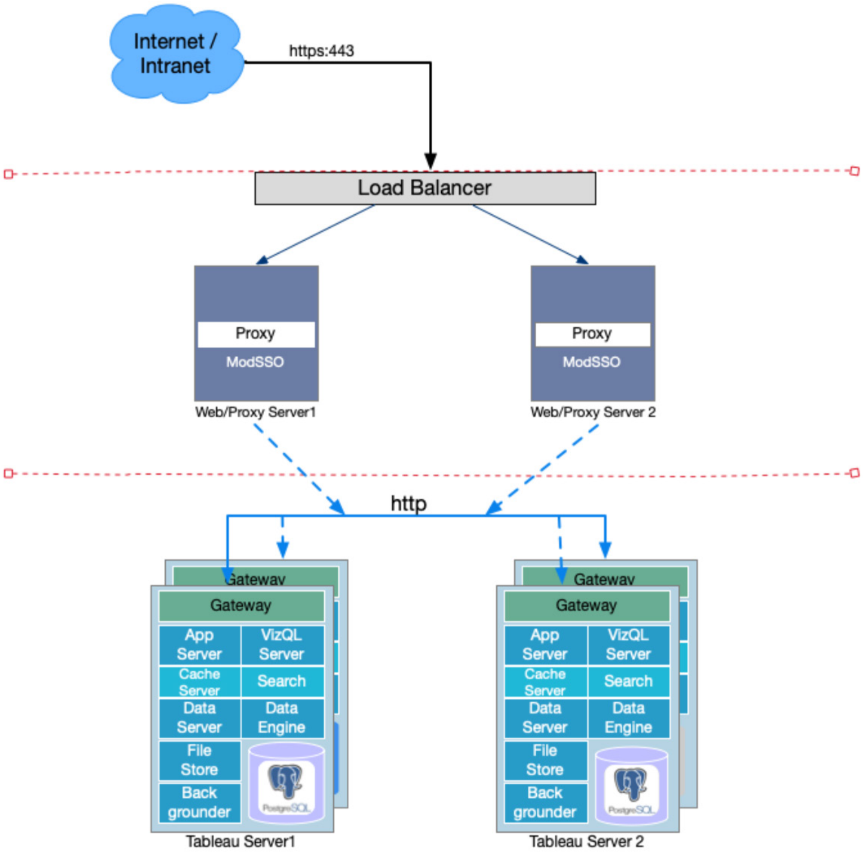

Figure 3 Example Placement of Tableau Server within FISMA-Authorized Infrastructure

Tableau Server affords its customers functionality and feature sets that allow a customer to adhere to FISMA-related compliance controls (e.g. NIST SP 800-53); however, in order to attain an enhanced security posture, Tableau Server customers must verify their customer responsibility of each control. Responsibility is identified with either a "CR" for Customer Responsibility in the Control ID column, or "SR" for Shared Responsibility. Controls without a dexsignation are, by default, met with Tableau Server's built-in functionality.

Access Control

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
Note: Tableau Server supports existing identity management solutions such as Active Directory to ensure functionality and compliance with NIST 800-53 Access Controls. Controls that require customer-provided identity management solutions are identified with "CR" in the Control ID column. Additional documentation pertaining to integration between Tableau Server and an existing identity management stores can be found **here**.			
AC-2 (1) CR	Account Management Automated System Account Management	CCI: CCI-000015 CVE: V-69295	Tableau Server, when integrated with an existing identity management store, enables customers to support the management of Tableau Server accounts.
AC-2 (3) CR	Account Management | Disable Inactive Accounts	CCI: CCI-000017 CVE: V-69301, V-69303	Tableau Server, when integrated with an existing identity management store, can enable system administrators to automatically disable inactive user accounts after 90 days.
AC-2 (4) CR	Account Management | Automated Audit Actions	CCI: CCI-000018, CCI-001403, CCI-001404, CCI-001405, CCI-001683, CCI-001684, CCI-001685, CCI-001686, CCI-002130, CCI-002132 CVE: V-69305, V-69307, V-69309, V-69311, V-69313, V-69315, V-69317, V-69319, V-69321, V-69323	Tableau Server, when integrated with an existing identity management store, can enable system administrators to log account creation, modification, enabling, disabling, and removal actions within the customer's existing security information and event management (SIEM) solution.
AC-3	Access Enforcement	CCI: CCI-000213 CVE: V-69329	Tableau Server uses role-based access control (RBAC) to restrict access to functionality and content. Additional information pertaining to Tableau Server permission configuration can be found here: Tableau Server User Site Roles Tableau Server User Permissions

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
AC-4	Information Flow	CCI: CCI-001368, CCI-001414 CVE: V-69333, V-69335	In an enterprise environment, Tableau Server can be deployed with a front-end load balancer which acts as a reverse proxy. Only the load balancer IP address will be exposed through the firewall to the Internet. An external firewall can filter the incoming traffic and allow only the traffic flow to the load balancer and only on desired ports like 443 with SSL encryption. Tableau Server can also be deployed in a demilitarized zone (DMZ) environment where proxy/web servers will be front ended in the DMZ or public subnet to Tableau Servers in the application/private subnet. In this scenario, there should be a firewall between the DMZ subnet and the application/private subnet which will control the network flow between these two subnets. This firewall should allow the communication flow only between the web/proxy servers in the DMZ to Tableau Servers in the private subnet, filtering ports and protocols. Customers can apply different policies on this firewall or network access control lists (ACLs) on the subnets to add additional flow controls for the communication between the subnets.
AC-6	Least Privilege		Tableau Server uses role-based access control (RBAC) to restrict access to functionality and content, thereby accommodating the principle of least privilege. Additional information pertaining to Tableau Server permission configuration can be found here: Tableau Server User Site Roles Tableau Server User Permissions Customers will have to follow least privilege principles when administering role-based access to Tableau Server.
AC-7 CR	Unsuccessful Logon	CCI: CCI-000044 (AC-7 a), CCI-002238 (AC-7 b) CVE: V-69343 (AC-7 a), V-69347 (AC-7 b)	Tableau Server, when integrated with an existing identity management store, can enable system administrators to configure account lockout after unsuccessful logon attempts. When configured with the customer's identity management solution, Tableau Server can enforce a configurable limit of consecutive invalid logon attempts by a user during a configurable time-period. User accounts that exceed this limit are locked and will require unlocking by the customer system administrator.
AC-11	Session Lock		Tableau Server includes the capability to configure the user session timeout value. Note: By default, Tableau Server is configured to terminate sessions after 240 minutes. To achieve FISMA Moderate requirements, system administrators must adjust the session lock period. For additional information on session timeout adjustments please reference the following documentation here.
AC-11 (1)	Session Lock | Pattern-Hiding Displays		Tableau Server displays a publicly consumable login page whenever a user has been idle long enough to trigger a session lock.
AC-12	Session Termination	CCI: CCI-002361 CVE: V-69241, V-69243, V-69245	Tableau Server includes the capability to configure the user session timeout value. Note: By default, Tableau Server is configured to terminate sessions after 240 minutes. To achieve FISMA Moderate requirements, system administrators must adjust the session lock period. For additional information on session timeout adjustments please reference the following documentation here.

Audit and Accountability

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
AU-2	Audit Events		For information about what Tableau Server logs to the internal PostgreSQL repository, please reference the following documentation found here. For information about log files for Tableau Server internal components, please reference the following documentation found here. The LogShark utility allows for analysis of Tableau Server log files and can be found here.
AU-3	Content of Audit Records	CCI: CCI-00130, CCI-000131, CCI-000132, CCI-000133, CCI-000134, CCI-001487 CVE: V-69421, V-69423, V-69425, V-69427, V-69429, V-69431, V-69433, V-69435, V-69437	For information about the content of logs that Tableau Server records, please reference the following documentation found here. For information about log files for Tableau Server internal components, please reference the following documentation found here. The LogShark utility allows for analysis of Tableau Server log files and can be found here.
AU-3 (1)	Content of Audit Records | Additional Audit Information	CCI: CCI-000135 CVE: V-69439, V-69441	For information pertaining to the additional content of logs that Tableau Server records, please reference the following documentation found here. For information about log files for Tableau Server internal components, please reference the following documentation found here. The LogShark utility allows for analysis of Tableau Server log files and can be found here.
AU-5	Response to Audit	CCI: CCI-000139 (AU-5 a), CCI-000140 (AU-5 b) CVE: V-69453 (AU-5 a), V-69455 (AU-5 b)	Tableau Server provides the ability for Tableau Server administrators to set permissions that would restrict unauthorized users from modifying audit information. For information about the locations of log files for Tableau Server internal components, please reference the following documentation found here.
AU-9	Protection of Audit Information	CCI: CCI-000162, CCI-000163, CCI-000164, CCI-001493, CCI-001494, CCI-001495 CVE: V-69483, V-69485, V-69487, V-69489, V-69491, V-69493	Tableau Server records events in which the internal PostgreSQL repository process fails and thereby retains failure information within the Tableau Server system. Additional information pertaining to the configuration of Tableau Server to alert when repository failures occur can be found here.

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
AU-12	Audit Generation	CCI: CCI-000169, CCI-000172 CVE: V-69363, V-69365, V-69367, V-69369, V-69371, V-69373, V-69375, V-69377, V-69379 (AU-12 a), V-69381, V-69383, V-69385, V-69387, V-69389, V-69391, V-69393, V-69395, V-69397, V-69399, V-69401, V-69403, V-69405, V-69407, V-69409, V-69411, V-69413, V-69415 (AU-12 c)	For information pertaining to audit generation records please reference the following documentation found here. For information about log files for Tableau Server internal components, please reference the following documentation found here. The LogShark utility allows for analysis of Tableau Server log files and can be found here.

Configuration Management

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
CM-6	Configuration Settings	CCI: CCI-000363 (CM-6 a), CCI-000366 (CM-6 b) CVE: V-70311 (CM-6 a), V-69513 (CM-6 b)	Tableau Server requires specific ports and protocols enabled to function as intended. For information pertaining to port configuration guidance please reference the following documentation found here.
CM-7	Least Functionality	CCI: CCI-000381 (CM-7 a), CCI-000382 (CM-7 b) CVE: V-69519 (CM-7 a), V-69521 (CM-7 b)	Tableau Server requires specific ports and protocols enabled to function as intended. For information pertaining to port configuration guidance please reference the following documentation found here.

Contingency Planning

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
CP-9	Information System Backup	CCI: CCI-000537 (CP-9 b), CCI-000540 (CP-9 d) CVE: V-70355 (CP-9 b), V-70357, V-70359 (CP-9d)	Tableau Server backups can be configured to support a customer's backup strategy, such as full backups at various intervals. For information pertaining to Tableau Server backups, please reference the following documentation found here.

Identification and Authentication

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
Note: Tableau Server supports existing identity management solutions such as Active Directory to ensure functionality and compliance with NIST 800-53 Access Controls. Controls that require customer-provided identity management solutions are identified with "CR" in the Control ID column. Additional documentation pertaining to integration between Tableau Server and an existing identity management store can be found **here**.			
IA-2 CR	Identification and Authentication (Organizational Users)	CCI: CCI-000764 CVE: V-69527	Tableau Server supports the capability for an organization's information system to uniquely identify and authenticate organizational users and process acting on behalf of organizational users. Actions undertaken by Tableau Server can be uniquely authenticated and identified to support after-the-fact reviews. Tableau Server logs the username/id of users initiating actions in all historical logs.
IA-2 (3) CR	Identification and Authentication | Local Access to Privileged Accounts	CCI: CCI-000767 CVE: V-69537	Tableau Server may be integrated with a customer-provided multi-factor authentication solution to provide Tableau Server with local access to privileged accounts.
IA-2 (12)	Identification and Authentication | Acceptance of PIV Credentials	CCI: CCI-001953, CCI-001954 CVE: V-69531, V-69533	Tableau Server provides the capability to operate with a customer's Personal Identity Verification (PIV) credentials such as a Common Access Card (CAC). For additional guidance on configuration please reference the following documentation found here.
IA-5 (1) CR	Authenticator Management | Password-Based Authentication	CCI: CCI-000205, CCI-000192, CCI-000193, CCI-000194, CCI-001619 (IA-5 (1) (a)), CCI-000195 (IA-5 (1) (b)), CCI-000196, CCI-000197 (IA-5 (1) (c)), CCI-000198, CCI-000199 (IA-5 (1) (d)), CCI-000200 (IA-5 (1) (e)), CCI-002041 (IA-5 (1) (f) CVE: V-69555, V-69557, V-69559, V-69561, V-69563 (IA-5 (1) (a)), V-69565 (IA-5 (1) (b), V-69567, V-69569 (IA-5 (1) (c), V-69571, V-69573 (IA-5 (1) (d), V-69575 (IA-5 (1) (e), V-69577 (IA-5 (1) (f)	Tableau Server, when integrated with a customer-provided identity management and authentication solution, can allow customers to configure minimum password complexity settings (upper-case letters, lower-case letters, numbers, and special characters) within the application. Customers can also leverage the identity management and authentication solution to configure additional password requirements such as: • Minimum number of changed characters when a new password is created • Storage and transmission encryption • Minimum and maximum lifetime restrictions • Minimum number of generations before password reuse is permitted • Forcing an immediate change of a temporary password to a permanent password
IA-6	Authenticator Feedback	CCI: CCI-000206 CVE: V-70157	Tableau Server obscures credentials entered into the application; however, customers can leverage their existing SSO integration and thereby meet this control through SSO password obfuscation.
IA-8	Identification and Authentication (Non-Organizational Users)	CCI: CCI-000804 CVE: V-70161	Tableau Server allows customers to create unique usernames for their users based on customer-defined policy.

System and Services Acquisition

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
SA-8	Security Engineering Principles		Tableau incorporates security engineering principles into all stages of the development of the Tableau Server application. Security engineering principles are considered and applied to Tableau Server during: • Specification • Design • Development • Implementation • Modification For more information on Tableau's security development practices, please refer to this website.
SA-11	Developer Security Testing and Evaluation	CCI: CCI-003173 (SA-11 b), CCI-003178 (SA-11 e) CVE: V-70381 (SA-11 b), V-70185, V-70383 (SA-11 e)	Tableau carries out thorough testing on the Tableau Server software and any changes made thereto prior to release, including but not limited to the following: • Creating and implementing a security assessment plan • Performing unit, integration, system, and regression testing • Producing evidence that a security assessment has been carried out • Implementing a verifiable flaw remediation program • Correcting any flaws identified during the testing process

System and Communications Protection

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
SC-2 SR	Application Partitioning	CCI: CCI-001082 CVE: V-70199	Tableau Server provides customers the ability to segregate user functionality from application management functionality. Users must access the application with different credentials to access different functionality within Tableau Server. Any individual attempting to access management functionality in Tableau Server must log in with credentials for that specific role. Users without such authorization are unable to access management functionality with only user credentials.
SC-8	Transmission Confidentiality and Integrity	CCI: CCI-002418 CVE: V-70245	Tableau Server has the ability to encrypt data communications between Tableau Server components and the internal PostgreSQL repository using TLS. For additional information pertaining to the transmission of data between these components please reference the document found here.
SC-13 SR	Cryptographic Protection	CCI: CCI-002450 CVE: V-70189, V-70191, V-70193, V-70195, V-70197	Tableau Server is compatible with customer configured load balancers. Customers are able to deploy Tableau Server behind a load balancer using FIPS 140-2 Validated encryption.
SC-28	Protection of Information at Rest	CCI: CCI-001199 CVE: V-70225	Tableau Server is compatible with customer configured volume or disk encryption. Customers are able to deploy Tableau Server on volumes or disks encrypted with FIPS 140-2 Validated modules.

System and Information Integrity

CONTROL ID	CONTROL NAME	APPLICABLE CGI AND CVE ID	IMPLEMENTATION DESCRIPTION
SI-2 (2)	Flaw Remediation | Automated Flaw Remediation Status		Tableau runs automated scans to detect flaws and vulnerabilities in Tableau Server. Acunetix is run for each build Tableau deploys at a monthly frequency. BlackDuck Binary Analysis is used for binary analysis and run daily. Static analysis is run using Coverity and Veracode on a weekly basis.
SI-10	Information Input Validation	CCI: CCI-001310 CVE: V-70257, V-70259, V-70261, V-70263, V-70265, V-70267, V-70269	Tableau employs the use of secure coding practices and leverages the use of code analysis and vulnerability scanning tools prior to code release to provide information input validation.
SI-11	Error Handling	CCI: CCI-001312 (SI-11 a), CCI-001314 (SI-11 b) CVE: V-70273 (SI-11 a), V-70275 (SI-11 b)	When an error occurs in Tableau Server, the message displayed to end users is generic. Only customer administrators can view detailed error information.

Conclusion

The Tableau Server solution can be implemented in an existing FISMA-authorized environment in a manner that maintains the existing security posture and compliance assurance. Federal Agency IT professionals can deploy the solution into their environment, knowing the security controls detailed in this white paper support and meet FISMA compliance requirements. The built-in capabilities and mechanisms of Tableau Server ensure that security and compliance requirements are maintained.

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

About Tableau

Tableau helps extract meaning from information. It’s an analytics platform that supports the cycle of analytics, offers visual feedback, and helps you answer questions, regardless of their evolving complexity. If you want to innovate with data, you want an application that encourages you to keep exploring—to ask new questions and change your perspective. If you’re ready to make your data make an impact, download a free trial of Tableau Desktop today.

Resources

Following are additional references related to Tableau Server security:

Tableau Security Website

Tableau Secure Software Development

Tableau Server Platform Security

Tableau Server Administrator Guide – Security Section

Tableau Server Security Hardening Checklist

Tableau Product Security Bulletins