Tableau Online Security in the Cloud

tableau

Contents

Introduction

The security and privacy of your data are fundamental to the success of your organization, and this is why Tableau makes protecting it a top priority. This whitepaper provides an overview of the how Tableau works to ensure the security and availability of customer data in Tableau Online.

Data published to Tableau Online is protected by enterprise-level security features that include:

- Physical Security
- Operational security
- Data security and privacy
- Account security
- Security of data in transit
- Application security

Underlying all of this is an infrastructure that is continuously monitored for availability, performance, capacity, and security. The output of this monitoring is used to drive regular improvements that help to ensure the confidentiality, integrity and availability of your data.

Tableau has implemented a multi-layered security model designed to provide effective protection against a wide range of known and zero-day threats. As part of Tableau's incident response protocol, any breach of security will be reported via the Trust website (https://trust.tableausoftware.com) or directly to impacted customers. Incident reports will include scope, severity and resolution.

Tableau continuously strives to maintain a secure, world-class hosted service so you can be confident your data is safe.

Operational Security

SOC 2 and ISAE 3402

Each year, Tableau works with an independent Certified Public Accounting firm to perform an in-depth audit of the control objectives and activities for Tableau Online. Tableau is proud to announce that the control procedures for our Tableau Online service have been verified in a SOC 2 Type II report prepared under terms of the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standard on Assurance Engagements (ISAE) No. 3402. The Tableau Online SOC 2 Type II report is available upon request.

Data Centers

Tableau Online services are hosted in enterprise-class, independently audited data centers that have redundancy built in to all critical services. The data centers are equipped with fire suppression and other monitoring systems designed to detect environmental issues and respond to them before they cause an outage. Additionally, the hosting providers have contracts with suppliers to ensure they can maintain operations in the event of a sustained power outage.

Upon execution of a non-disclosure agreement, Tableau can share the audit reports for its data center providers upon request. For more information, please contact your Tableau account representative.

System Maintenance

The team responsible for maintaining the Tableau Online infrastructure performs regular maintenance to ensure system stability, security and performance. Scheduled maintenance windows are posted to the Tableau Trust site a minimum of two days in advance. Additionally, site administrators receive email notifications of upcoming work and users all will see a notification upon logging into the Tableau Online site.

Data Security and Privacy

Privacy Shield

With respect to personal data relating to residents of the European Economic Area (EEA), Tableau is a certified Active Participant in the Privacy Shield Framework and is subject to the investigative and enforcement powers of the Federal Trade Commission.

Backup and Recovery

Backups are made of all critical components. Backup media is encrypted and always maintained in a secured facility. Disk-based backups are stored in secured data center facilities. Backups made to external backup providers are encrypted in transit and in storage. Only approved system administrators have access to backups.

Per Tableau Online backup policy, daily backups are retained for 31 days.

These backups enable Tableau to restore the entire Tableau Online system. The backups do not currently allow for the restoration of a single customer site, meaning Tableau cannot restore individual customer workbooks or data that were lost due to events other than a system failure.

Disaster Recovery

For each instance of the Tableau Online service, Tableau maintains primary and backup data centers in geographically diverse locations. Should a primary data center become unavailable, systems are staged at the backup site that would be reconfigured to service production traffic. Data would then be restored from the most recent backup.

Since Tableau Online is a read-only application and the data is generally provided from customer-managed data sources, it is possible to republish visualizations by pulling the information directly from the source versus having to restore from a backup. This can dramatically reduce the recovery point objective.

Data Governance

Your data is your own, even when stored in Tableau Online. Only individuals you authorize have access to data or workbooks stored in your site—Tableau employees and other customers do not have access to your data. The only exception is a small and controlled number of trusted Tableau administrators that are responsible for managing the systems that run the service. There is a documented process for authorizing users with this level of access, and all administrative-level access is reviewed and approved on a quarterly basis.

Something to keep in mind is that the bulk of your data remains securely stored in your own data sources. Only workbooks, data extracts and cached data are stored within Tableau Online.

Tableau does have access to, and may monitor, metrics that have to do with system utilization, account status, and performance. Such metrics include:

- Total storage used by account and by user
- Total bandwidth used by account and by user
- Total number of workbooks and views by account and by user
- Access dates and times by user (logins)
- Number and type of data sources (e.g., SQL Server, Salesforce.com) by account and by user
- Dates and times of data refresh by account and by user
- Site performance metrics

Data enters Tableau Online in one of four ways:

1. By publishing a workbook with the data embedded in it.
2. By "pushing" data from an on premises source to a Tableau data extract. This method always results in a data extract, not a real-time connection, so there is no need to create a virtual private network (VPN) or secure tunnel into your corporate environment. For data sources that Tableau Online cannot reach directly, you can publish data extracts and use the Tableau Online sync client to schedule automatic refreshes.
3. Connecting to a web service via an application programming interface (API). For most cloud data sources, such as Salesforce.com and Google Analytics, the API connection is used to generate data extracts which can be scheduled to update regularly.
4. Direct connection to data hosted on a cloud platform. For these data sources, Tableau Online can create a real time live connection or one that is extract-based.

User and Data Source Filters

You can define additional security in your workbooks and data sources by adding User and Data Source Filters. User filtering is a special kind of filter that allows you to limit the data any given person can see in a published view. For example, in a sales report that gets shared with regional managers, you may want to only allow the Western Regional Manager to see the western sales, the Eastern Regional Manager to see the eastern sales, and so on. Rather than create a separate view for each manager, you can define a user filter that allows each manager to see the data for a particular region.

A user filter is defined for an individual field. Users or groups are given permission to see a subset of the members in that field. In the sales report example above, the user filter is defined for the Region field, and each manager is given permission to see a corresponding region.

Data Source Filters operate in a similar fashion to User Filters and allow you to set a filter on a published data source that applies globally. Data source filters can be useful for restricting the data users can see when you publish a workbook or data source. When you publish a data source to Tableau Online, the data source and any associated files or extracts are transported in entirety to the server. As you publish a data source you can define access permissions for downloading or modifying the data source, and you can also choose the users and groups who can remotely issue queries through Tableau Online against that data source. When users have the query permission and no download permission, you can share a rich data model having calculated fields, aliases, groups, sets and more – but only for querying.

Furthermore, users who query this data source will never be able to see or modify any data source filters present on the originally published data source, but all the users' queries will be subject to those data source filters. This is a great way to offer access to a restricted subset of your data.

User Security

Access and Authentication

Only users you explicitly add to your site have access to your content and workbooks. Administrators that you designate are responsible for all account management functions including adding and removing users and assigning permissions. Account management is completely in your control. If a user is no longer authorized in your site, simply remove them and they will no longer have access to content stored in Tableau Online.

There are two methods of authentication available within Tableau Online and you have the flexibility to configure your site to use one or both of them.

1. Tableau Account

Tableau Accounts are used by default and are secured in a Tableau-maintained identity store. This method of authentication provides site administrators the ability to quickly configure users without the need to integrate with a separate identity provider. The accounts are managed by customers and enable secure authentication to Tableau Online. The account is also used to access other Tableau services and resources such as the Tableau Website, Tableau Customer/Partner Portal, and Tableau Forums.

Users are authenticated using their email address as the username and a user-selected password. When administrators add users to their site, an email is sent to the user with instructions on how to setup their password. Administrators

do not set user passwords nor can they retrieve stored passwords. Passwords are salted and hashed using a strong hashing algorithm.

Accounts are locked out after 10 failed attempts for a period of 10 minutes and the lockout time doubles for each successive lockout. A user may have no more than five concurrent sessions which timeout after eight hours.

Passwords are required to be a minimum of eight characters in length and must include letters and numbers.

2. SAML

SAML allows administrators to configure their site for single sign on using their own SAML 2.0 capable identity provider (IdP). For additional information refer to the Site Authentication section of the Online Product Guide.

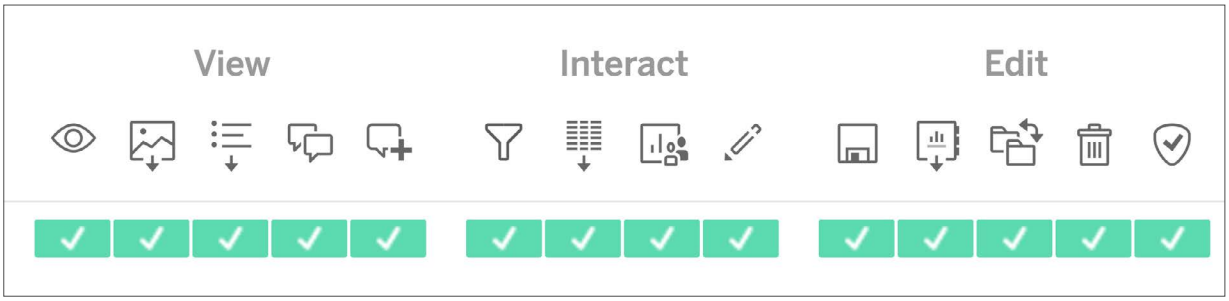
Note: Features related to SAML and single sign-on are currently only available by request. To request these features, contact Tableau Support.

Tableau Online enforces a session time-out after a two hour period of inactivity.

Roles and Permissions

Access within Tableau Online is controlled through a combination of site roles and permissions. Every user added to Tableau Online must have an associated site role. The site role is assigned by the administrator and determines the levels of permissions allowed for a user, including whether a user can publish, interact with, or only view content published to Tableau Online. Additional details on Site Roles can be found here. Permissions are assigned to content (projects, workbooks, views, and data sources) and can be assigned to individual users or groups. When you specify permissions, you use rules to specify who is allowed to work with that content.

Permissions can be used to grant permissions such as create, view, modify, and delete. Permissions assigned to a projects control the default access level all workbooks and views published to the project. Administrators can create groups such as "Finance Users" to make permission management easier.



The permissions window

There are over 20 parameterized customizations available to help manage object security. For more information, see the Manage Permissions section in the online documentation.

Transmission (Network) Security

Encryption

All communication between the client (Tableau Desktop or a supported browser) and Tableau Online is encrypted using TLS which provides protection of data in transit.

Connections to data sources may or may not be encrypted based on encryption capabilities of the data source. Customers should understand the encryption options available for the data sources they plan to use.

In addition, Tableau products have many built-in security mechanisms to help prevent spoofing, hijacking, and SQL injection attacks. Tableau also actively tests its products for vulnerabilities and responds to new threats with regular updates.

Be aware that features using email, such as subscription emails are sent using SMTP which, by standard, is not encrypted.

Application Security

Application security is a combination of secure design practices that include defining security requirements, threat modeling, code reviews, and security testing. Automated and manual

vulnerability testing is done as a part of the development process and third-party security firms are leveraged to conduct penetration testing of applications prior to major releases. Tableau is committed to working with third-party security experts to test, discover, validate, and address security concerns.

Additionally, Tableau has implemented a third-party vulnerability scanning service that continuously scans the company's Internet-facing resources and services for vulnerabilities including Tableau Online. Any findings generate an alert which is triaged to assess severity and impact. Priority of any remediation efforts that may be required is based on this assessment.

Multi-tenant Architecture

Tableau Online is a multi-tenant solution and does not provide dedicated environments for each customer. The application enforces segregation between customers by logically partitioning users, data, and metadata by site. All data uploaded or linked to the service is programmatically connected to the customer that owns the data. These controls ensure a customer cannot access another customer's data.

Administrative Dashboards

Tableau Online publishes a default set of dashboards that provide usage statistics for your site. Some of the details that are made available include user activity, view counts, and data source usage. Administrators can use these default dashboards to get a sense of how their site is being used.

For details on using these dashboards please refer to the Administrative Views section of the online product guide.

Conclusion

The Tableau Online service is built and operated based on a robust security model that is informed by industry best practices and validated by third party security experts. Tableau understands how important your data is and takes the responsibility to protect it very seriously.

About Tableau

Tableau helps people transform data into actionable insights that make an impact. Easily connect to data stored anywhere, in any format. Quickly perform ad hoc analyses that reveal hidden opportunities. Drag and drop to create interactive dashboards with advanced visual analytics. Then share across your organization and empower teammates to explore their perspective on data. From global enterprises to early-stage startups and small businesses, people everywhere use Tableau's analytics platform to see and understand their data.

Resources

Download Free Trial

Why Business Analytics in the Cloud?

5 Best Practices for Creating Effective Campaign Dashboards

See All Whitepapers