

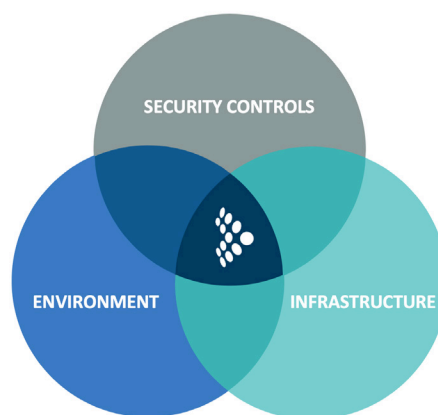
PRODUCT DATASHEET

Tealium Data Security and Privacy Tools: Controls and Infrastructure That Are Designed to Protect Your Customer Data

Customer data is essential to delivering an exceptional customer experience. As data sources and usage grow, it's essential for organizations to detect, mitigate and minimize the risk associated with sharing 1st, 2nd and 3rd party data across the technology stack.

To do this at scale and in compliance with current and evolving regulations, a secure and scalable environment for processing customer data and orchestration of that data is vital.

Tealium's Private Cloud solution leads the industry in security and compliance. In addition to implementing the highest level of safeguards for unparalleled data security, Tealium's Private cloud provides the robust orchestration and activation features that are trusted by over 800 enterprises. Tealium Private Cloud enables enterprises to leverage their data in real time, orchestrate and activate data, and sleep at night knowing they are using the best in breed security and privacy controls to maintain their customer's loyalty and trust.



Key Benefits:

Visibility and control over data supply chain - Integrated tools managing data over its full lifecycle

Certified Solution - Tealium's Private Cloud has achieved a pedigree of 3rd party security and privacy certifications: HIPAA, ISO 27001 and 27018 and SSAE18 SOC 2 Type II.

Tools and controls to manage data flow - Functionality to restrict and enable any and all data sharing when needed

HIPAA Regulated Features of Tealium's Universal Data Hub

Stringent safeguards for processing and storing protected customer information designed to protect the confidentiality, integrity, and security of ePHI.

Security Information and Event Management ("SIEM"), which is fully managed by Tealium.

All environments are audited for compliance by a third party.

All processes must authenticate to access the data.

Data encryption at rest and in transit.

Infrastructure

Tealium's Universal Data Hub ("UDH") hosted in a Private Cloud provides an end-to-end data orchestration platform for collection, standardization, transformation, integration and activation of data. This enables customers to have end-to-end granular control over the data supply chain, and track the flow of data across the MarTech stack for each individual customer (and the customer base as a whole), all while protecting and honoring the privacy of the individual customer data.

Tealium Private Cloud is built and developed in accordance with industry standard security controls and procedures that are designed to protect client data. By using Tealium as the single source of 1st party data enrichment and universal segmentation, an organization can meet its data security requirements while simultaneously augmenting the organization's ability to deliver consistent and powerful customer experiences

"Tealium iQ users can be assigned preconfigured permission sets and granted separate security permissions based their a role...so that all users can be given proper access to the Data Layer."

Environment

From the beginning, data security and customer privacy have been at the forefront of Tealium's development strategy. Tealium is committed to the principles of Privacy by Design and Default. Tealium's Private Cloud has achieved a pedigree of 3rd party security and privacy certifications: HIPAA & HITECH, ISO 27001 and 27018, Privacy Shield and SSAE18 SOC 2 Type I & II.

For organizations that need to comply with strict privacy and security rules under regulations like HIPAA, Tealium Private Cloud provides an ideal solution. With Tealium Private Cloud, the customer is the only tenant and the data is secured to HIPAA standards. Private Cloud customers may confidently integrate Tealium's platform in their HIPAA controlled environments knowing that the data sent to the Private Cloud is safeguarded in accordance with the same HIPAA controls already in use in their data processing stack.

Security Controls

In addition to the Private Cloud infrastructure security features, the products hosted within Private Cloud offer additional security features that allow customers to align the data processing with the requirements of the HIPAA security rules. For more information on security controls or to see a full list of security features, visit us at www.tealium.com.

Role-Based Access Control

Tealium iQ users can be assigned preconfigured permission sets and placed into separate security tiers based on role. Users can be given a range of permission from "view-only" to full administrative control so that all users can be given proper access to the Data Layer. This role-based access and control approach is provided in an intuitive GUI wizard-based configuration tool.

Create New User

Create User

You'll be guided through the following steps to set up a new user account.

- 1 **Create User**
- 2 **Set Account Permissions**
(Shown only if you have manage account permissions)
- 3 **Add user to profiles**
(Shown only if you have manage user permissions for other profiles)
- 4 **Assign profile permissions**
(Shown only if you have manage user permissions)
- 5 **Overview / Confirmation**

To begin, enter the user's email address.

New User Email:

Cancel **Next**

Tag Marketplace Controls

The Tealium Tag Marketplace can be configured to only allow usage of a predetermined set of tags; making it easy for the TiQ admin to work with their InfoSec teams to only allow approved vendors to be deployed using Tealium.

Data Layer Controls

The [data layer provides a single point of control](#) for modeling the necessary data needs of an organization.

Tealium iQ admins can assign access only to specific parts of the data layer to specific groups within their organization. This can be accomplished using “tag labels” and “resource locks”. Resource locks and labels can be applied to elements of a Tealium iQ profile to prevent unauthorized users from making changes to those elements.

For example, a third-party agency might want to add analytics tags to the data layer. Using tag labels, the Tealium admins can give access to only the pieces of the data layer that the agency needs to change in order to develop this tag logic and mapping. All other data sources within the data layer would read-only by the agency.

Password Policy and Multi-Factor Authentication (MFA)

Tealium provides industry standard password policy and MFA capabilities through the Tealium iQ Admin Console. Password restrictions, authentication requirements, and password rules can all be implemented by InfoSec teams here. Tealium also fully supports SSO federated access using SAML 2.0.

Tealium encryption policy requires the use of common, well-understood ciphers including AES 256, Triple DES, SHA 256 (preferably with salt) and SSL/TLS 1.2 or stronger.

Manage Password Policy

Global Password Configuration

Current Settings

Global password settings will be applied to all users on this account. The default settings allows for:

- Minimum 8 characters in length
- Minimum 1 number character
- Minimum 1 uppercase character
- Minimum 1 special character

Strength: Strong

Minimum Password Length

8 Characters

-

+

Minimum Uppercase Characters

1 Characters

-

+

Minimum Numeric Characters

1 Characters

-

+

Minimum Special Characters

1 Characters

-

+

Password History Restriction

1 Passwords

-

+

Use Default Settings

Use Recommended Settings

Multi-Factor Authentication

Use codes generated from the Google Authenticator app to sign in to Tealium.

[Learn More](#)

ENABLED

Disable MFA for this account

To setup MFA on your user account, please log off and re-log in

Cancel

Update Password Settings

Deployment Environment Controls

In addition to role-based access controls, Tealium also enables user access to be designated by target environment (e.g. Dev, QA, Production) to help enforce existing separation of duties within the organization.

Encryption and Hashing

Tealium iQ provides organizations with the ability to designate which data elements should be hashed through the use of a [built-in extension](#) that eliminates the coding requirements of this task and simplifies the process. Additionally, data can be configured to be transmitted only over HTTPS to the platform. Data is always encrypted in transit within the Tealium platform as well as when it is at-rest.

Visitor Data Controls

As first-party data is collected in Tealium, data types that are identified as sensitive can be labelled “restricted” based on InfoSec and IT requirements.

iPhone IDFA (5210)

Add Label

☐ Private PII Data

Manage Labels

Apply

iPhone IDFA

Visitor

Visitor ID

Attribute Id : 52

Restricted Data

Configuring attributes as restricted will control the flow of data at a foundational level with tools supplying visibility over data flow and the capability to restrict the distribution of identified information.

Data that is labeled as restricted is also prohibited from being exposed on Tealium's Data Layer Enrichment (DLE) feature. Restricted data is still capable of being orchestrated if there is a requirement to do so.

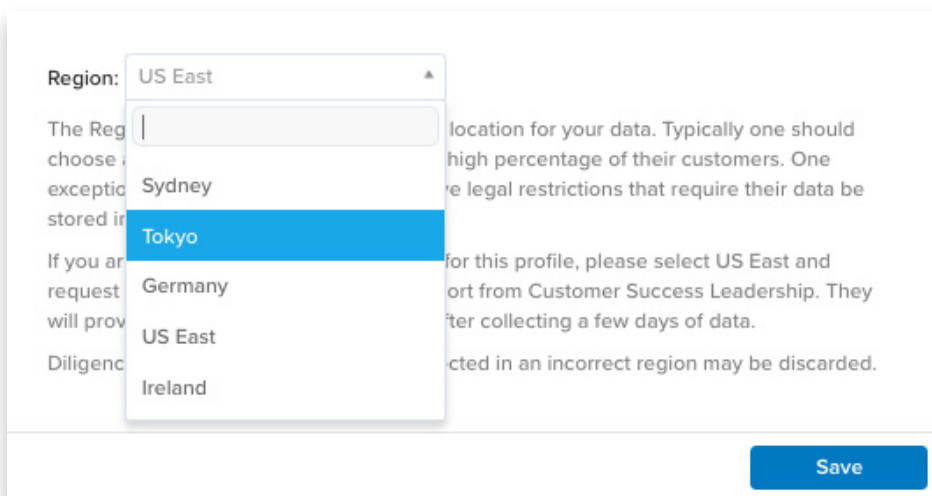
Capture IP Address

Based on an organization's privacy policy, personal information such as IP address may or may not be prohibited to enter the company's infrastructure and network.

There is an option within Tealium AudienceStream to enable or disable the capturing of IP addresses.

Geographical Data Storage

Many organizations must comply with legal requirements that mandate their customer data is stored in a specific geographic location. Tealium's platform can be configured to store all data in the chosen global location.

A screenshot of a web interface showing a dropdown menu for selecting a region. The label "Region:" is followed by a dropdown box currently displaying "US East". The dropdown menu is open, showing a list of regions: Sydney, Tokyo (highlighted in blue), Germany, US East, and Ireland. To the right of the dropdown, there is explanatory text: "location for your data. Typically one should choose a location with a high percentage of their customers. One should also consider any legal restrictions that require their data be stored in a specific location." Below the dropdown, there is a "Save" button.

Tealium supplies tools to manage data flow based on geography to help clients comply with standards and industry regulations that vary from region to region, like GDPR.

Event Connector Marketplace Controls

Similar to the "Tag Marketplace Controls" in Tealium iQ, EventStream provides an ability to disable/enable any of the desired EventStream Connectors for your organization.

Some organizations may want to tightly control where event data is sent. Tealium offers the ability to disable event connectors, which guarantees that the event data is only transmitted outbound from the UDH to authorized vendors and internet endpoints.

Data lineage enforcement is important to organizations due to the volume of data, the complexity of systems and growing compliance requirements. Tealium's UDH gives customers end-to-end visibility and control across the entire data life cycle.

Data Obfuscation and De-Identification

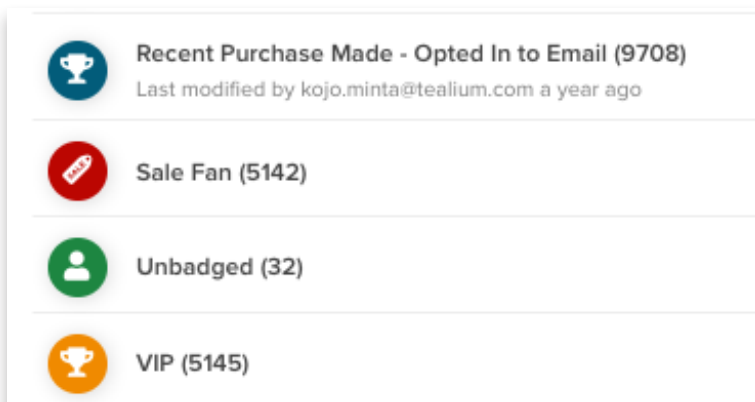
Tealium AudienceStream provides the ability to build attributes that represent the characteristics of a particular visitor that is engaging with the organization via one or more touchpoints.

As the event data enters the UDH in real time with demographic, navigational and transactional information generated from their interactions on websites, apps and other devices, AudienceStream is configured to process this incoming data and form new, enriched data that represents a specific state, persona, or achievement of that customer.

These attributes are psychographic data in nature, allowing the business to efficiently reduce the data load and data processing requirements needed by their vendors to continue working with that data. This psychographic data, called badges, effectively obfuscates and de-identifies the required dataset because it represents only the outcome of the visitor and not the sensitive information that produced it.

For example, if a visitor has purchased several products from a company, that visitor may have a very large dataset with a great deal of sensitive information in it, and he has logically become a “VIP Customer” after all of these purchases. The company wants to engage with its VIPs via a marketing email channel. Since the VIP Badge is configured in AudienceStream to be linked to the right threshold of purchases and automatically form and attach itself to the appropriate customer datasets, there is no need to transmit all of the historical purchase details to the email server platform as might have been the case beforehand.

Since the badge, “VIP Customer”, effectively tells the email marketing personnel all they need to know about the user, only an email would be required alongside the VIP Badge to kick off this campaign. This relieves the organization of having to send sensitive data from technology to technology, vendor to vendor, and assures that a single point of control can govern the management of personal information to the most effective level possible.



The data privacy controls and infrastructure within the UDH are just one way that Tealium can help organizations build a secure and scalable data infrastructure.

To learn more about Tealium's approach to data privacy and trust, [visit our website](#) or [request a custom demo](#) to see how Tealium can address your specific challenges.



Collect, Enrich and Take Action On Customer Data

[Tag Management](#) | [API Hub](#) | [Customer Data Platform](#) | [Data Management](#)

Tealium revolutionizes today's digital businesses with a universal approach to customer data orchestration – spanning web, mobile, offline, and IoT devices. With the power to unify customer data into a single source of truth, Tealium offers a turnkey integration ecosystem supporting over 1,200 client-side and server-side vendors and technologies. The Tealium Universal Data Hub encompasses tag management, API hub, customer data platform, and data management solutions that enable organizations to leverage real-time data to create richer, more personalized digital experiences across every team, technology, and customer touchpoint. More than 850 businesses worldwide trust Tealium to power their customer data strategies.

For more information, visit www.tealium.com.

© 2019 Tealium, Inc. All rights reserved. Tealium, AudienceStream, and all other Tealium marks contained herein are trademarks or service marks of Tealium. All other marks are the property of their respective owners. Rev. 110819