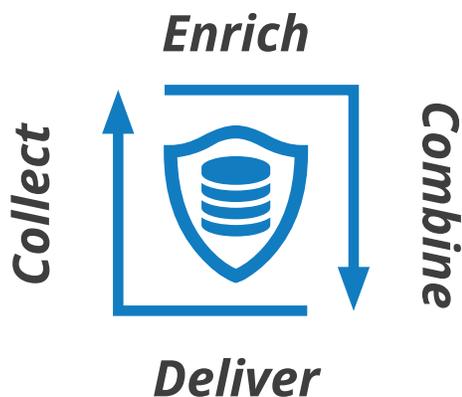**TEALIUM**

DATASHEET: INFOSEC

Ensure Information Security in an Increasingly Complex Data Landscape

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.

For organizations to function most effectively it's becoming increasingly important to make use of disparate data sources spread across many systems. Managing the flow of data through the data supply chain presents challenges with securing that data at rest and in motion, providing visibility and control over data flows, and complying with customer expectations and government regulations.

As a data orchestration platform, Tealium's Universal Data Hub ("UDH") is built and developed in accordance with industry standard security policies and procedures to ensure protection of client data. Additionally, the UDH assists organizations in gaining end-to-end control over the data supply chain, auditing the flow of data across an organization for each individual customer (and the customer base as a whole), and protecting customer data.

Enrich

Collect   *Combine*

Deliver

Benefits:

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

Secure the organization's flow of data - Built to the strictest InfoSec requirements and fully audited by nationally recognized 3rd party auditors

Precise control for program managers and customers - Functionality to restrict and enable any and all data sharing when needed

Minimizing Risk

Independently evaluated security controlled environment

AICPA SOC
aicpa.org/soc
Formerly SAS 70 Reports

HIPAA

GDPR READY
General Data Protection Regulation

TRUSTED PRIVACY
P
EU data protection
ePrivacyseal

Privacy Shield Framework

Certified Type 1 and Type 2 SOC2 Compliance

Tealium's information security control environment is independently evaluated by a third party audit firm in the form of a Service Organization Control (SOC) 2 Type 1 and Type 2 report. A SOC 2 report is designed to meet a broad set of reporting needs about the controls at a service organization in the form of a CPA firm's independent attestation report. Tealium's SOC 2 report shows Tealium's demonstrable commitment to and practice of security, availability, processing integrity and confidentiality principles.

"As new global privacy regulations come into effect – such as the General Data Protection Regulation and EU-US Privacy Shield – it's essential companies work with providers who place data security, availability, and confidentiality as a priority. Achieving SOC 2 type II compliance demonstrates we're perfectly placed to lead companies through this change – we can be trusted to keep our customers' sensitive data secure."

— Mike Anderson, Founder and CTO, Tealium

Secure Data Enrichment and Transmission

After data is collected at the source, it must be enriched, combined and delivered to other systems for analysis or activation. This involves data-in-motion security mechanisms. The UDH uses advanced industry-standard data encryption methods to help safeguard confidential information when in motion and at rest. 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.

Importantly, the UDH strategy enables an organization's data supply chain to function in a completely integrated and secure manner from initial collection, to enrichment and unification, all the way through activation. By using Tealium as the single source of 1st party data enrichment and universal segmentation capabilities, an organization can secure data, while simultaneously augmenting the organization's ability to deliver consistent and powerful customer experiences.

Implement Precise "Need to Know" Data Activation Practices with Data Governance Capabilities

Legacy technology installations have forsaken robust security practices for ease of implementation, leaving many companies with a mystery box of data management needs. Tealium's services help organizations to avoid blanket tracking approaches or one-size-fits-all data sharing by giving visibility and discrete control over the sharing of data between all business systems. Customers can use the tools provided by Tealium to gain precise control over what data is used to trigger marketing activities and share only that minimum amount of data between systems.

Customer Success

We know everybody isn't an InfoSec expert, so we're here to help. Tealium has you covered with our renowned customer success program to help you define and implement the right practices.

Reduced Scope of Security

By using Tealium as the single source of 1st party data enrichment and universal segmentation capabilities, an organization can secure data, while simultaneously augmenting the organization's ability to deliver consistent and powerful customer experiences.

Lock Down Data Security

With tools for user and data access management, conditional tag loading, restricted data controls, data encryption and geographic-based data management, businesses can not only reduce risk, but gain precise control over data to power revenue generation initiatives.

❖ TEALIUM

With tools for user and data access management, conditional tag loading, restricted data controls, data encryption and geographic-based data management, businesses can not only reduce risk, but gain precise control over data to power revenue generation initiatives.

Extra Control and Visibility for When You Need It

Tealium's UDH comes equipped with robust features providing an extra level of control over certain data. Functionality for encrypting data, hashing, and flagging restricted data to limit sharing, means companies gain critical and flexible InfoSec capabilities allowing compliance with strict security requirements.

Support Compliance Efforts for Regulated Industries & Geographic Areas

Certain industries and geographic regions have especially strict regulations requiring a higher level of data protection. For example, the General Data Protection Regulation (GDPR) in the European Union, HIPAA for healthcare organizations in the US, or the special geographic requirements in Germany, China and Brazil.

Tealium partners with organizations to provide flexible and robust tools and practices to secure data in accordance with regulatory requirements and industry standards, including offering a private cloud environment for organizations that need to comply with the privacy and security rules under regulations like HIPAA and PCI. In the Private Cloud the customer is the only tenant and the data is secured to HIPAA and/or PCI standards but is not intended to be a repository of Health Records or Cardholder Data. Customers may confidently integrate Tealium's software in their HIPAA and PCI controlled environments knowing that the data sent to the Private Cloud is safeguarded with the same level of controls as their own HIPAA and/or PCI environments.

Security Tools

Tealium's UDH provides an extra level of control over data when you need it. Functionality for encrypting data, hashing, and flagging restricted data to limit sharing, means companies gain critical and flexible InfoSec capabilities allowing compliance with strict security requirements.

Tealium Global Data Center Network

TEALIUM

Tealium revolutionizes today's digital businesses with a universal approach to managing the ever-increasing flows of customer data - spanning web, mobile, offline and IoT, With the power to unify customer data from a single source of truth, combined with a turnkey integration ecosystem supporting more than 1,000 vendors and technologies, Tealium's Universal Data Hub (UDH) enables organizations to gain real-time, actionable insights and create richer, more personalized digital experiences. More than 700 global businesses worldwide trust Tealium to power their data strategies and data governance practices.

For more information, visit www.tealium.com.