Tessian Security Datasheet

Infrastructure Security

Tessian is built on Amazon Web Services with an industry leading security and privacy framework at the core of our technology.

Encrypted in Transit

All API communication between the Tessian Server and the client-side environment is encrypted using AES-256 bit encryption via an SSL/TLS protocol.

Encrypted at Rest

All data stored within the Tessian database is encrypted at rest. By encrypting all data at rest, we ensure that if any disks were accessed or compromised, all data is fully encrypted and therefore unreadable.

Tenant Separated Schemas

Customer data is schema separated in Tessian databases. This ensures that data is never shared within the same tables and customers can easily request the removal of their schema from Tessian.

Built on AWS[1]

Tessian's infrastructure is hosted on Amazon Web Services, widely recognized as the world's leading infrastructure as a service platform and used by some of the largest companies and governments worldwide.

Data Residency

Tessian offers the option to host your data with Amazon Web Services in Ireland (Europe) or Oregon (US).

Data Retention

Tessian can remove all customer data from the platform at their request.

Platform Security

The Tessian Platform has extensive security settings to manage application and user access.

Application Authentication

All API communication between the Tessian Server and client-side software is authenticated using unique API tokens and domain whitelisting.

Single Sign On (SSO)

Access to the Tessian Platform can be managed through SSO.

2 Factor Authentication (2FA)

Tessian Platform access can be configured to require Two Factor Authentication.

IP Whitelisting

Tessian Platform access can be restricted to specific IP addresses.

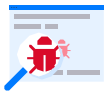
[1] More details on AWS Cloud Security can be found here: https://aws.amazon.com/security/

Company Security

Tessian adopts a number of best practice procedures to secure our company, people and technology.

Penetration Testing

We conduct annual penetration testing with a top-tier 3rd party.



Red Teaming

We work with a 3rd party security company on an ongoing basis who provide red teaming services as well as reconnaissance and vulnerability analysis and are involved in architecture design decisions.

Security Engineers

We have a dedicated team of security engineers who test our systems internally and write tools to empower our engineers to build securely.

Security Certifications

Tessian holds numerous industry certifications as part of our ongoing commitment to the highest standards of information security.

ISO 270001 CERTIFICATION

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

SERVICE ORGANIZATION CONTROL 2 & 3 (SOC)

Customer Trust

Tessian is trusted by world-leading organizations in the financial, legal, healthcare and technology sectors to secure the millions of emails they send and receive every single day.

Evercore · arm · BDO · RealPage · Investec · Graphcore · sanne · MSCI · ERT · Clyde&Co · Bracewell · GoCardless · Jefferies · JTC · BainCapital · affirm · Schroders · rightmove · K&L Gates · cordaan · PeaceHealth · Rand Merchant Bank · Herbert Smith Freehills · Intertrust · Man Group plc · Travers Smith · Hill Dickinson

TESSIAN

Human Layer Security

TESSIAN.COM

Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error - like data exfiltration, accidental data loss, business email compromise and phishing attacks - with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like Sequoia, Accel, March Capital, and Balderton.