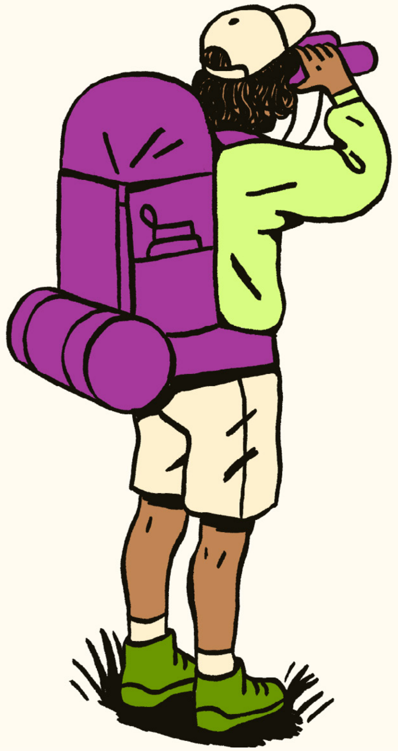
zendesk

A Secure-by-Design Cloud Solution

Security is top priority for any business considering a cloud-based solution.

Some of the world's most recognizable brands trust Zendesk with their data. Using customizable, best-in-class security features such as access management, advanced encryption and comprehensive auditing across applications, systems, and networks, we're able to empower our customers with a multi-layered, secure cloud-based solution that delivers powerful data protection.

Zendesk also adheres to security and data protection best practices and frameworks for compliance with applicable data protection regulations. This, in turn, helps our subscribers in their own specific compliance programs.



Thanks to secure-by-design cloud-native architecture built on Amazon Web Services (AWS), Zendesk is able to deliver value at scale, on demand, across key areas:

Physical security
To ensure the confidentiality, availability and integrity of your data, Zendesk only operates in data centers that adhere to industry standards and certifications including, but not limited to, ISO 27001 and SOC 2 Type 2. Biannual due diligence is also conducted to ensure such standards are met and maintained.

Network security
Zendesk maintains a 24/7 globally distributed security team that manages the security of our customers' data via continuous network vulnerability scanning, industry leading cybersecurity technology, and a proactive threat intelligence program.

Application security
We consistently develop and test against security threats to ensure the safety of customer data via our secure development lifecycle process and expert penetration testing.

Availability and business continuity
The Zendesk Disaster Recovery and Business Resilience Programs ensure service continuity and easy recovery in the event of a disaster. We also employ service clustering and network redundancies to eliminate single points of failure, and provide publicly available status updates on availability issues, scheduled maintenance and service incident histories.

Data security
Encryption In Transit: Communication between customers and Zendesk servers over public networks are encrypted via industry standard Transport Layer Security (TLS). TLS is also supported for email encryption.

Encryption At Rest: Zendesk also supports encryption at rest for primary and secondary recovery data stores and attachment storage.

Product security features
We make it seamless for customers to manage the security of their instance with authentication, single sign-on (SSO) and two-factor authentication (2FA) as well as IP restrictions, so customers can enable access management according to their specific needs.

Advanced data privacy and protection
For businesses that need a higher level of data privacy and security, Zendesk offers the Advanced Data Privacy and Protection add-on. The add-on includes capabilities for BYOK encryption, customizable data retention policies, data masking, PII redaction, and access logs.

Compliance certifications and memberships
Zendesk's CX products and solutions meet rigorous security, privacy, and compliance standards, including:

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

SKYHIGH ENTERPRISE-READY

FSQS

CERTIFY EY POINT
Certified against
ISO/IEC 27001:2013
by EY CertifyPoint
Certificate No: 2018-008

CERTIFY EY POINT
Certified against
ISO/IEC 27018:2019
by EY CertifyPoint
Certificate No: 2018-010

CERTIFY EY POINT
Certified against
ISO/IEC 27701:2019
by EY CertifyPoint
Certificate No: 2022-011

CERTIFY EY POINT
Certified against
Référentiel de Certification Hébergeur de Données de Santé version 1.1 Mai 2018
by EY CertifyPoint
Certificate No: 2021-012

Please visit the Trust Center for more information about our security and compliance posture or to request a SOC 2 report.