A secure-by-design cloud solution

Security is one of the top concerns for businesses moving to a cloud-based solution, and entrusting your data to a third-party SaaS service provider requires rigorous security measures.

More than 125,000 customers trust Zendesk with their data, and this responsibility is not something we take lightly. We combine enterprise-class security features with comprehensive audits of our applications, systems, and networks to ensure customer and business data is always protected. And our customers rest easy knowing their information is safe, their interactions are secure, and their businesses are protected.

In addition, we leverage secure components, such as FIPS-140 certified encryption solutions, to protect customer data. Portions of our solution can be configured to meet PCI and HIPAA/HITECH Attestation standards. Zendesk has also developed and created tools to allow our customers to meet their obligations under GDPR.

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

- ISO 27001:2013
- ISO 27018:2014
- SOC 2 Type II
- EU-US & Swiss-US Privacy Shield Certification
- TRUSTe Enterprise Privacy Certification

Zendesk starts delivering value within minutes and scales on demand thanks to its secure-by-design, cloud-native architecture built on Amazon Web Services (AWS). Security is a part of our DNA, and it's baked into everything we do. Security encompasses a number of key areas:

Physical security

We ensure the confidentiality, availability, and integrity of your data with industry best practices. In addition, Zendesk operates in data centers that have been certified as ISO 27001, PCI/DSS Service Provider Level 1, and/or SOC II compliance.

Network security

Zendesk maintains a globally distributed security team that is on call 24/7 to respond to security alerts. Through network vulnerability scanning, the use of intrusion detection and intrusion prevention systems, and by participating in several Threat Intelligence Programs, we keep a continuous watch on the security of our customers' data.

Application security

We take steps to securely develop and test against security threats to ensure the safety of our customer data. Zendesk maintains a Secure Development Lifecycle, in which training our developers and performing design and code reviews takes a prime role. In addition, Zendesk employs third-party security experts to perform detailed penetration tests on different applications within our family of products.

Availability and business continuity

Zendesk maintains a disaster recovery program to ensure services remain available or are easily recoverable in the case of a disaster. We employ service clustering and network redundancies to eliminate single points of failure. Customers can remain up-to-date on availability issues through a publicly available status website covering scheduled maintenance and service incident history.

Data security

Encryption In Transit: Communications between customer and Zendesk servers are encrypted via industry best-practices HTTPS and Transport Layer Security (TLS) over public networks. TLS is also supported for encryption of emails.

Encryption At Rest: Customers of Zendesk benefit from the protection provided by encryption at rest for their primary and secondary DR data stores and storage of attachments.

Product security features

We make it seamless for customers to manage access and sharing policies with authentication and single-sign on (SSO) options. We also provide for 2-factor authentication and IP restrictions to enable customers to determine who can access their service.

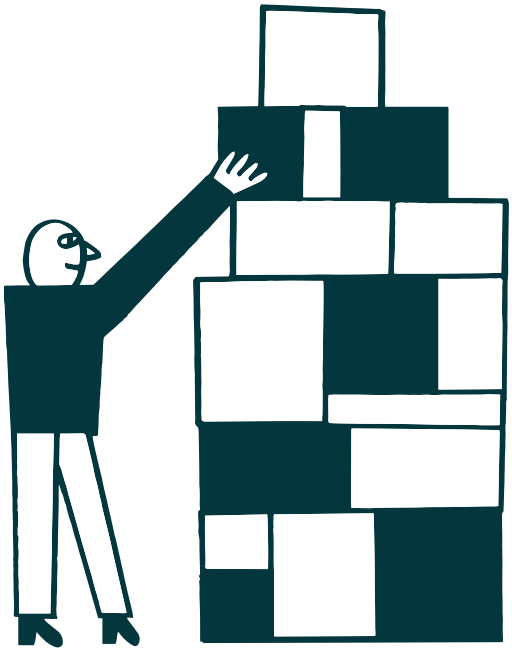
Compliance certifications and memberships

We implement security best practices—in addition to what AWS provides—to meet not just industry-based compliance, but the most stringent requirements.

Access to data by Zendesk

To help troubleshoot problems within a Zendesk account, admins can allow Zendesk Support to assume the role of an agent for a specific amount of time. The account assumption setting is part of a customer's security properties. By default, this setting is disabled and can only be enabled by an account admin. Access can be granted for a set period of time, or indefinitely, and can be turned off at any time.

Learn more



"When evaluating software for a U.S. government agency, we require all vendors to maintain the highest standards of security. Zendesk demonstrated their commitment to those standards via their SOC 2 type II, ISO standards, and Cloud Security Alliance Self Assessment. Combining that with the ideal product to meet the FCC's needs enabled us to switch from an on-premise to a SaaS solution."

Dustin Laun

Contractor, Sr. Advisor of Innovation/Technology

For any inquiries on our security and compliance posture or to access our SOC 2 report, please email us at security@zendesk.com.