Zendesk: 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 130,000 customers trust Zendesk with their data and this responsibility is something we take very seriously. 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 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, baked into everything we do. Security encompasses a number of key areas.

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

- ISO 27001:2013
- ISO 27018:2014
- SOC 2 Type II & SOC 3
- EU-US & Swiss-US Privacy Shield Certification
- TrustArc Privacy Seal

Data center and network security

Physical security

Facilities

Zendesk hosts service data in AWS data centers located in the United States, Europe, and Asia Pacific that have been certified as ISO 27001, PCI/DSS Service Provider Level 1, and/or SOC II compliance.

Customers can choose to locate their Service Data in the US-only or Europe-only (Zendesk Chat is Europe-only at this time). Learn more about our regional data hosting options.

Perimeter security

AWS perimeter security includes a number of features such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

Infrastructure

AWS infrastructure services includes back-up power, HVAC systems, and fire suppression equipment to help protect servers and ultimately your data.

Monitoring

All Production Network systems, networked devices are constantly monitored and logically administered by Zendesk staff. Physical security, power, and internet connectivity are monitored by AWS.

Network security

Dedicated security team

Our globally distributed Security Team is on call 24/7 to respond to security alerts and events.

Protection

Our network is protected through the use of key AWS security services, integration with our Cloudflare edge protection network, secure HTTPS transport over public networks, regular audits, and network intelligence technologies which monitor and/or block malicious traffic and network attacks.

Architecture

Our network security architecture consists of multiple security zones. More sensitive systems, like database servers, are protected in our most trusted zones. Other systems are housed in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the Internet, and internally between the different zones of trust.

Network vulnerability scanning

Network security scanning gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems.

Network security

Third-party penetration tests

In addition to our extensive internal scanning and testing program, each year Zendesk employs third-party security experts to perform a broad penetration test across the Zendesk Production Network.

Security Incident Event Management (SIEM)

Our Security Incident Event Management (SIEM) system gathers extensive logs from important network devices and host systems. The SIEM alerts on triggers which notify the Security team based on correlated events for investigation and response.

Intrusion detection and prevention

Service ingress and egress points are instrumented and monitored to detect anomalous or suspect behavior. These systems are configured to generate alerts when incidents and values exceed predetermined thresholds and uses regularly updated signatures based on new threats. This includes 24/7 system monitoring.

Threat intelligence program

Zendesk participates in several threat intelligence sharing programs. We monitor threats posted to these threat intelligence networks and take action based on our risk and exposure.

DDoS mitigation

Zendesk has architected a multi-layer approach to DDoS mitigation. A core technology partnership with Cloudflare provides network edge defenses, while use of AWS scaling and protection tools provides deeper protection along with our use of AWS DDoS specific services.

Logical access

Access to the Zendesk Production Network is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by our Operations Team. Employees accessing the Zendesk Production Network are required to use multiple factors of authentication.

Security incident response

In case of a system alert, events are escalated to our 24/7 teams providing Operations, Network Engineering, and Security coverage. Employees are trained on security incident response processes, including communication channels and escalation paths.

Encryption

Encryption in transit

Communications between Customer and Zendesk Support and Chat 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 protections of encryption at rest for their data. Service Data is encrypted at rest in AWS using AES 256 key encryption.

Availability & continuity

Uptime

Zendesk maintains a publicly available system-status webpage at https://status.zendesk.com/ which includes system availability details, scheduled maintenance, service incident history, and relevant security events.

Redundancy

Zendesk employs service clustering and network redundancies to eliminate single points of failure. Our strict backup regime and/or our Enhanced Disaster Recovery service offering allows us to deliver high level of service availability, as Service Data is actively replicated across availability zones.

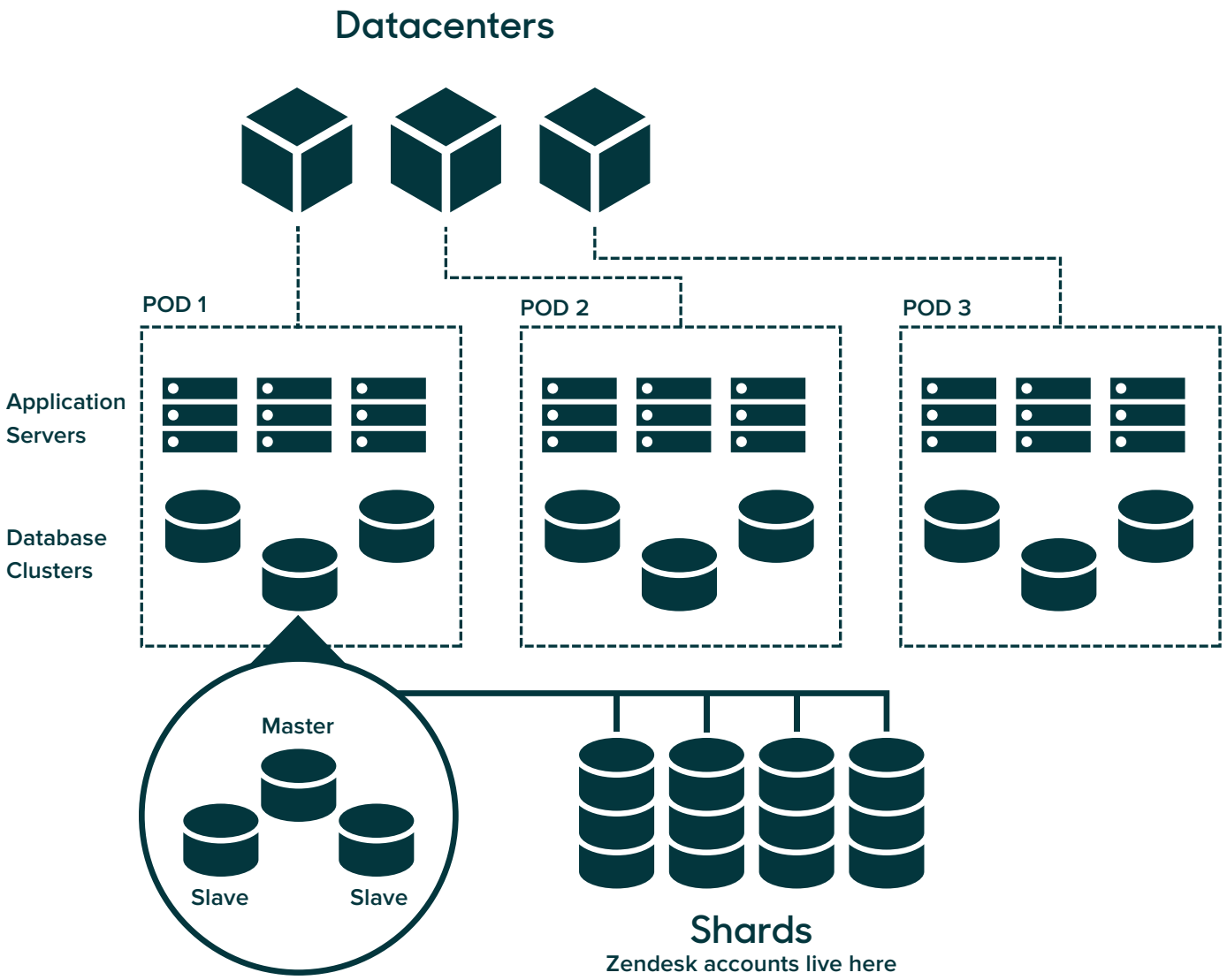
Disaster Recovery

Our Disaster Recovery (DR) program ensures that services remain available or are easily recoverable in the case of a disaster. This is accomplished through building a robust technical environment, creating Disaster Recovery plans, and ongoing testing activities.

Enhanced Disaster Recovery

Enhanced Disaster Recovery package adds contractual objectives for RTO and RPO. These are supported through our capability to prioritize operations of Enhanced Disaster Recovery customers during any declared disaster event.

Data Center Technical Architecture



Application Security

We take steps to securely develop and test against security threats to ensure the safety of our customer data. In addition, Zendesk employs third-party security experts to perform detailed penetration tests on different applications within our family of products.

Software development lifecycle (SDLC)

Security training

At least annually, engineers participate in secure code training covering OWASP Top 10 security risks, common attack vectors, and Zendesk security controls.

Ruby on Rails framework security controls

Most Zendesk products utilize the Ruby on Rails framework security controls to limit exposure to OWASP Top 10 security risks. These inherent controls reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.

QA

Our Quality Assurance (QA) department reviews and tests our code base. Dedicated application security engineers on staff identify, test, and triage security vulnerabilities in code.

Separate environments

Testing and staging environments are logically separated from the Production environment. No actual Service Data is used in the development or test environments.

Application vulnerability discovery

Dynamic vulnerability scanning

We employ third-party, qualified security tooling to continuously dynamically scan our core applications against the OWASP Top 10 security flaws. We maintain a dedicated in-house product security team to test and work with engineering teams to remediate any discovered issues.

Static code analysis

The source code repositories for both our platform and mobile applications are continuously scanned for security issues via our integrated static analysis tooling.

Security penetration testing

In addition to our extensive internal scanning and testing program, each quarter Zendesk employs third-party security experts to perform detailed penetration tests on different applications within our family of products.

Responsible Disclosure / Bug Bounty Program

Our Responsible Disclosure Program gives security researchers as well as customers an avenue for safely testing and notifying Zendesk of security vulnerabilities through our partnership with HackerOne.

Product Security Features

We make it seamless for customers to manage access and sharing policies with authentication and single-sign on (SSO) options, through the product, or leveraging their own enterprise-grade solutions. We also provide for 2-Factor Authentication and IP Restrictions to enable customers to determine who can access their service.

Authentication security

Authentication options

For admins/agents in Support and Chat, we offer Zendesk sign-in. For Zendesk Support, you may also enable SSO, and Google Authentication.

For end-users in Support and Chat, we support Zendesk sign-in. For Zendesk Support, you may also enable SSO and social media SSO (Facebook, Twitter, Google) for end-user authentication.

Single sign-on (SSO)

Single sign-on (SSO) allows you to authenticate users in your own systems without requiring them to enter additional login credentials for your Zendesk Support instance. Both JSON Web Token (JWT) and Security Assertion Markup Language (SAML) are supported. Learn more about security and sign-in settings.

*SAML is only available for Professional and Enterprise accounts
*JWT is only available for Team accounts and above.

Configurable password policy

Zendesk Support/Guide provides the following levels of password security: low, medium, and high, as well as set custom password rules for agents and admins. Zendesk also allows for different password security levels to

Two-factor authentication (2FA)

If you are using Zendesk sign-in on your Zendesk Support instance, you can turn on 2-factor authentication (2FA) for agents and admins. Zendesk supports SMS and numerous authenticator apps for generating passcodes. You may also choose to leverage 2FA in your own environment where coupling with enterprise SSO as your authentication method for Zendesk. 2FA provides another layer of security to your Zendesk account, making it more challenging for somebody else to sign in as you. Learn more about 2FA.

Secure credential storage

Zendesk follows secure credential storage best practices by never storing passwords in human readable format, and only as the result of a secure, salted, one-way hash.

API security & authentication

In case of a system alert, events are escalated to our The Zendesk Support API is TLS-only. You can authorize against the API using either basic authentication with your username and password, or with a username and API token. OAuth authentication is also supported. Learn more about API security.

Application Security

We take steps to securely develop and test against security threats to ensure the safety of our customer data. In addition, Zendesk employs third-party security experts to perform detailed penetration tests on different applications within our family of products.

Additional product security features

Role based access controls

Access to data within Zendesk applications is governed by role based access control (RBAC), and can be configured to define granular access privileges. Zendesk has various permission levels for users (owner, admin, agent, end-user, etc.) Learn more about Support user roles and user access & security.

IP restrictions

Zendesk Support and Chat can be configured to only allow access from specific IP address ranges you define. These restrictions can be applied to all users or only to your agents. Learn more about using IP restrictions.

*Only available for Enterprise Support accounts and Chat Enterprise

Private attachments

In Zendesk Support, you can configure your instance so users are required to sign-in to view ticket attachments. If not configured, the attachments are accessible via a long and random token ticket ID.

Transmission security

All communications with Zendesk UIs and APIs are encrypted using industry standard HTTPS/TLS over public networks. This ensures that all traffic between you and Zendesk is secure during transit. Additionally for email, our product leverages opportunistic TLS by default. Transport Layer Security (TLS) encrypts and delivers email securely, mitigating eavesdropping between mail servers where peer services support this protocol.

Email signing (DKIM/DMARC)

Zendesk Support offers DKIM (Domain Keys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting & Conformance) for signing outbound emails from Zendesk when you have setup an external email domain on your Zendesk. Using an email service that supports these features allows you to stop email spoofing. Learn more about digitally signing your email.

Device tracking

For added security, your Zendesk Support instance tracks the devices used to sign in to each user account. When someone signs into an account from a new device, it is added to the device list in that user's profile. That user can get an email notification when a new device is added, and should follow-up if the activity seems suspicious. Suspicious sessions can be terminated from the agent UI.

Additional product security features

Redacting sensitive data

Redaction for Zendesk Support and Chat provides the ability to redact, or remove sensitive data in ticket comments, custom fields, and Chats so that you can protect confidential information. The data is redacted from tickets to prevent sensitive information from being stored in Zendesk. Learn more about securing sensitive data.

*Only available for Enterprise accounts

Spam filter for Help Center and Web Portal

Zendesk Support offers a spam filtering service which prevents end-user spam posts from being published on your Help Center or Web Portal. Learn more about filtering spam in Help Center.

Audit logs

View a detailed list of critical changes that have been made to your Zendesk Support instance. Learn more about audit logs in Help Center.

Ticket Audits are a read-only history of all updates to a ticket. When a ticket is updated in Zendesk Support, an audit is stored. Each audit represents a single update to the ticket. Learn more about ticket audits in Zendesk Developer Portal - Support API.

Compliance certifications and memberships

We implement security best practices to meet not just industry-based compliance, but the most stringent requirements.

ISO 27001:2013

SOC 3

ISO 27018:2014

EU-US & Swiss-US Privacy Shield Certification

TrustArc Privacy Seal

SOC 2 Type II

Security compliance

SOC 2 Type II / SOC 3

We have a SOC 2 Type II available upon request and under NDA.

Additionally, at a non-NDA level, we have a SOC 3 report made available for direct download on our public security page.

For more information contact security@zendesk.com.

ISO 27001:2013

Zendesk is ISO 27001:2013 certified. The certificate is available for download here.

ISO 27018:2014

Zendesk is ISO 27018:2014 certified. The certificate is available for direct download here.

In addition to our SOC 3 and ISO certs, you may freely download our CSA CAIQ from our public security page.

Memberships

Skyhigh Enterprise-Ready

Zendesk received the Skyhigh Enterprise-Ready™ seal, the highest rating in the CloudTrust™ program. It is bestowed on cloud services that fully satisfy the most stringent requirements for data protection, identity verification, service security, business practices, and legal protection.

Cloud Security Alliance

Zendesk is a member of the Cloud Security Alliance (CSA), a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing. CSA has launched the Security, Trust & Assurance Registry (STAR), a publicly accessible registry that documents the security controls provided by various cloud computing offerings. We've completed a publicly available Consensus Assessment Initiative (CAI) Questionnaire, based on the results of our due diligence self-assessment.

Privacy certifications

TRUSTe® Privacy Certification Programs

Zendesk has demonstrated that our privacy programs, policies and practices meet the requirements of EU-U.S. Privacy Shield and/or Swiss-U.S. Privacy Shield. These companies have self-certified their participation in Privacy Shield with the US Department of Commerce at https://www.privacyshield.gov/list. TRUSTe verifies Privacy Shield compliance consistent with the requirements of the Privacy Shield Supplemental Principle on Verification.

EU - U.S. and Swiss - U.S. Privacy Shield Certification

Zendesk has certified its compliance with the EU-U.S. and Swiss-U.S. Privacy Shield frameworks to the U.S. Department of Commerce and has been added to the Department of Commerce's list of self-certified Privacy Shield participants. Our certifications confirm that we comply with the Privacy Shield Principles for the transfer of European and Swiss personal data to the United States.

Privacy policy

Learn more about privacy at Zendesk here.

Industry based compliance

HIPAA

We help customers address their HIPAA obligations by leveraging appropriate security configuration options in Zendesk products. Additionally, we make our Business Associate Agreement (BAA) available for execution by subscribers.

*BAA is only available with the purchase of the Advanced Security Add-on and only applicable to certain Zendesk products (special configuration rules apply).

Using Zendesk in a PCI environment

View our whitepaper on PCI compliance or learn more about our PCI compliant field for Zendesk Support.

*Enterprise account required

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

Protecting data is a critical component of every activity, product, and service at Zendesk.

Please feel free to contact us with any questions or concerns at security@zendesk.com as well as downloading the public security resources available from our security website at www.zendesk.com/product/zendesk-security.

zendesk