SECURE CUSTOMER SERVICE

Zendesk Security

More than 90,000 customers trust Zendesk with their data. This 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.

Best Practices

Zendesk provides a range of security options to ensure data is protected and secure. But an ounce of prevention is worth a pound of cure. By following these ten best practices, you can increase the security of your Zendesk.

CUSTOMER PERSPECTIVES

"At Box, we pride ourselves on our product's simplicity, security, and performance. When looking for a solution to meet the support needs of thousands of customers, we required the same."

- Jon Herstein, Vice President of Customer Success

DATA CENTER & NETWORK SECURITY | APPLICATION SECURITY | PRODUCT SECURITY FEATURES | ADDITIONAL SECURITY METHODOLOGIES | COMPLIANCE CERTIFICATIONS & MEMBERSHIPS

Data Center & Network Security

PHYSICAL SECURITY

Facilities	Zendesk servers are hosted at Tier III, SSAE-16, PCI DSS, or ISO 27001 compliant facilities. Our cage space is physically and logically separated from other data center customers. The co-location facilities are powered by redundant power, each with UPS and backup generators.
On-site Security	Our data center facilities feature a secured perimeter with multi-level security zones, 24/7 manned security, CCTV video surveillance, multifactor identification with biometric access control, physical locks, and security breach alarms.
Monitoring	All systems, networked devices, and circuits are constantly monitored by both Zendesk and the co-location providers.
Location	Zendesk has data centers in the EU and United States. Customers can choose to locate their data in the US-only or EU-only. Learn more about our EU data hosting policies **Only available with Data Center Location Add-on*

NETWORK SECURITY

Dedicated Security Team	Our Security Team is on call 24/7 to respond to security alerts and events.
Protection	Our network is protected by redundant layer 7 firewalls, best-in-class router technology, secure HTTPS transport over public networks, regular audits, and network intrusion detection/prevention technologies (IDS/IPS) that monitor and block malicious traffic and network attacks.
Architecture	Our network security architecture consists of multiple security zones of trust. More sensitive systems, like our 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)	A security incident event management (SIEM) system gathers extensive logs from important network devices and hosts systems. Thel SIEM creates triggers that notify the Security team based on correlated events. The Security team responds to these events.
Intrusion Detection and Prevention	Major application data flow ingress and egress points are monitored with Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). The 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	In addition to our own capabilities and tools, we contract with on-demand DDoS scrubbing providers to mitigate Distributed Denial of Service (DDoS) attacks.
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 you and Zendesk servers are encrypted via industry best-practices HTTPS and Transport Layer Security (TLS).
Encryption at Rest	Zendesk supports encryption of customer data at rest. **Only available with Advanced Security Add-on*

AVAILABILITY & CONTINUITY	
Uptime	Zendesk maintains a publicly available system-status webpage that includes system availability details, scheduled maintenance, service incident history, and relevant security events.
Redundancy	Zendesk's service clustering and network redundancies eliminate single point of failure. Our strict backup regime ensures customer data is actively replicated across both systems and facilities. Our database data is stored on efficient Flash Memory devices with multiple servers per database cluster.
r Recovery	Our disaster recovery program ensures that our 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 testing.

AVAILABILITY & CONTINUITY	
Enhanced Disaster Recovery	With enhanced disaster recovery, the entire operating environment, including customer data, is replicated in a secondary site to support taking over the service when the primary site becomes fully unavailable. Zendesk has defined a targeted return time objective (RTO) and recovery point objective (RPO) for this service. **Only available with Advanced Security Add-on*

Application Security

SECURE DEVELOPMENT (SDLC)	
Security Training	At least annually, engineers participate in secure code training. This training covers OWASP Top 10 security flaws, common attack vectors, and Zendesk security controls.
Ruby on Rails Framework Security Controls	We utilize Ruby on Rails framework security controls to limit exposure to OWASP Top 10 security flaws. These include inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.
QA	Our QA department reviews and tests our code base. Several dedicated application security engineers on staff identify, test, and triage security vulnerabilities in code.
Separate Environments	Testing and staging environments are separated physically and logically from the production environment. No actual customer data is used in the development or test environments.

APPLICATION VULNERABILITIES	
Dynamic Vulnerability Scanning	We employ a number of third-party, qualified security tools to continuously scan our application. Zendesk is scanned daily 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	Our 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 parts of the application.
Responsible Disclosure / Bug Bounty Program	Our Responsible Disclosure Program gives security researchers an avenue for safely testing and notifying Zendesk of security vulnerabilities through our partnership with HackerOne.

Product Security Features

SECURE DEVELOPMENT (SDLC)	
Authentication Options	For admins/agents we support Zendesk sign-in, SSO, and Google Authentication. For end-users we support Zendesk sign-in, SSO, and social media SSO (Facebook, Twitter, Google).

SECURE DEVELOPMENT (SDLC)

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 Zendesk access. Zendesk only grants access to users that have been authenticated by you. Both JSON Web Token (JWT) and Security Assertion Markup Language (SAML) are supported. Learn more about SSO **SAML is only available for Professional and Enterprise accounts* **JWT is only available for Team accounts and above*
Configurable Password Policy	Zendesk provides the following levels of password security: low, medium, and high. Zendesk allows you to set one password security level for end-users, and a different one for admins and agents. Only admins can change the password security level. On the Professional and Enterprise Plans, you can specify your own custom password security level.
Two-factor authentication (2FA)	If you are using Zendesk sign-in, you can turn on 2-factor authentication (2FA). Zendesk supports SMS and apps like Authy and Google Authenticator for generating passcodes. 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 l readable format, and only as the result of a secure, salted, one-way hash.
API Security & Authentication	Zendesk API is SSL-only and you must be a verified user to make API requests. 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

ADDITIONAL PRODUCT SECURITY FEATURES

Access Privileges & Roles	Access to data within your Zendesk is governed by access rights, and can be configured to define granular access privileges. Zendesk has various permission levels for users (owner, admin, agent, end-user, etc.) accessing your Zendesk. Learn more about access levels
IP Restrictions	Your Zendesk 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 accounts*
Private Attachments	You can configure your Zendesk so users are required to sign-in in order to view ticket attachments. If not configured, the attachments are accessible via a random token ticket ID.
Transmission Security	All communications with Zendesk servers are encrypted using industry standard HTTPS. This ensures that all traffic between you and Zendesk is secure during transit. Additionally for email, our product supports Transport Layer Security (TLS), a protocol that encrypts and delivers email securely, mitigating eavesdropping and spoofing between mail servers.
Email Signing (DKIM/DMARC)	We support 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, Zendesk 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.

ADDITIONAL PRODUCT SECURITY FEATURES	
Automatic Redaction	Automatic Redaction provides the ability to redact, or remove, digits from credit card numbers found in ticket comments or custom fields so that you can protect confidential information. The data is redacted from an incoming ticket to prevent the full credit card number from being stored in Zendesk. Learn more about our Redaction Tool **Only available for Professional and Enterprise accounts*
Spam Filter for Help Center and Web Portal	Zendesk supports 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 and filtering spam in Web Portal

Additional Security Methodologies

SECURITY AWARENESS	
Policies	Zendesk has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to, all employees and contractors with access to Zendesk information assets.
Training	All new employees attend a Security Awareness Training, and the Security Team provides security awareness updates via email, blog posts, and in presentations during internal events.

EMPLOYEE VETTING	
Background Checks	Zendesk performs background checks on all new employees in accordance with local laws. These checks are also required to be completed for contractors. The background check includes Criminal, Education, and Employment verification. Cleaning crews are included.
Confidentiality Agreements	All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.

Compliance Certifications and Memberships

SECURITY COMPLIANCE	
SOC 2 Type II	We have our own SOC 2 Type II report, available upon request and under NDA. For more information contact security@zendesk.com.
ISO 27001:2013	Zendesk is ISO 27001:2013 certified.
ISO 27018:2014	Zendesk is ISO 27018:2014 certified.

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.

MEMBERSHIPS	
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	We've received TRUSTe's Privacy Seal signifying that our privacy statement and our practices have been reviewed for compliance with the TRUSTe program, viewable on their validation page.
US-Swiss Safe Harbor programs	Zendesk has certified compliance with the U.S. - Swiss Safe Harbor Frameworks as set forth by the United States Department of Commerce.
Privacy Policy	Learn more about privacy at Zendesk

INDUSTRY BASED COMPLIANCE	
HIPAA	Zendesk has successfully completed a HIPAA/HITECH assessment and can make its Business Associate Agreement (BAA) available for execution by subscribers. **HIPAA/HITECH assessment passed at all plan levels, BAA only available with Advanced Security Add-on*
Using Zendesk in a PCI Environment	View our whitepaper on PCI compliance or learn more about our PCI compliant field.

*Some of the above may not apply to Zopim security. Click here to learn more about security for Zopim. HIPAA BAA is available to Zendesk Voice customers on the Advanced Voice plan and the Advanced Security Add-on. Click here for more details

**Some of the above may not apply to certain customer-enabled features such as Insights and Voice. Click here to learn more.

This could be the beginning of a beautiful relationship.

Start your free trial

OUR PRODUCTS
Support
Help Center
Chat
Talk
Message
Inbox Team Email
Explore
Connect
Integrations & Apps
Embeddables
Insights & Analytics
Product Updates

TOP FEATURES
Ticketing System
Knowledge Base
Community Forums
Help Desk Software
IT Help Desk
Security
Tech Specs

RESOURCES
Product Support
Request a demo
Library
Zendesk Blog
Live webinars
Training
API & Developers
Services & Partners
For Retailers
Relate by Zendesk
Customer Stories
Services

COMPANY
About us
Press
Investors
Careers
Neighbor Foundation
Contact Us
Sitemap
System Status
Product Help
Legal

FAVORITE THINGS
Zendesk for Startups
Sh*t Agents Say
Zoe Calls Home
Zendesk Benchmark
Zendesk for Small Business
Gartner CRM Magic Quadrant
Hiring Great Support Teams

ENTER THE FOLD

Join the elite group of other people who have also signed up for our mailing list.

What's your email?

Search Zendesk