 Zendesk Security

Customer data is one of the most valuable assets a company has. That’s why our top priority is delivering a high-performance solution with a focus on keeping our customers’ data safe and their interactions secure.

Cloud-based software is all about providing uninterrupted, reliable service, making information security a major focus for first-rate cloud vendors. Skilled resources, network redundancies, religious data back-ups, stand-by power, up-to-date security, and intrusion detection are mandatory components for an enterprise-class service.

This level of infrastructural investment would be overwhelming for a single organization or team. Zendesk customers of all sizes get the benefit of a comprehensive, high-performance solution with a low total cost of ownership—all while keeping their data safe, their interactions secure, and their businesses protected.

Our application and network infrastructure exceeds industry security expectations. Our high levels of performance, availability, and security are achieved through:

• A dedicated, deeply experienced security team
• Systems security monitoring 24x7x365
• Active performance and availability monitoring of all data centers 24x7x365
• Experienced engineering staff with ongoing secure code development training
• SSAE 16 Type II compliant data centers
• Restricted IP access, role-based application security with flexible single sign-on, data encryption, ongoing vulnerability scanning, and encrypted offsite backups
• Security features: password complexity / administrator-based single sign-out / roles and permissions / access restrictions
• User authentication and access control
• A secure, multitenant network architecture
• Frequent, human-driven security auditing via network and application penetration testing
• Automated vulnerability analysis via external platform and application vulnerability scans
• Static analysis
• Regular updates rolled out to all customers, ensuring everyone has the latest application and security innovations
• Employee programs to increase awareness, communication, collaboration, and education on security

PERFORMANCE. AVAILABILITY. SECURITY.

APPLICATION
Designed with a focus on security

INFRASTRUCTURE
Best-in-class firewalling

ACCESS SECURITY
For permitted users only

VULNERABILITY MANAGEMENT
Swift discovery and mitigation

Methodology

Zendesk continually performs risk analysis to achieve the highest level of security. Security concepts and techniques have been integral to our solution’s design right from the beginning, and we
continue to invest heavily in security improvements for our product, our process, our people, and our technology.

Zendesk performs full security audits of our product and infrastructure regularly, including quarterly third-party audits. Our risk assessment process aligns with the ISO 27002 standard.

**Physical Security**

Zendesk servers are hosted at Tier III, SSAE-16, or ISO 27001 compliant facilities.

Facilities features 24-hour manned security, biometric access control, video surveillance, and physical locks. The co-location facilities are powered by redundant supplies, each with UPS and backup generators. All systems, networked devices, and circuits are constantly monitored by both Zendesk and the co-location providers. Only a small group of our employees have physical access to the servers.

**Network Security**

Our network is protected by layer 7 firewalls, best-of-class router technology, SSL encryption, file integrity monitoring, and network intrusion detection that monitors for malicious traffic and network attacks. Network security scanning gives us deep insight for quick identification of out-of-compliance systems. A security incident event management (SIEM) system gathers logs from all network systems and creates triggers based on correlated events.

In addition to our own capabilities, and those of our hosting providers, we contract with on-demand DDOS scrubbing providers to allow us to mitigate DDOS attacks.

**Transmission Security**

All communications with Zendesk servers are encrypted by default using industry standard SSL. This ensures that all traffic between you and Zendesk is secure during transit. Unlike email-based communication, most of which flows unprotected over the Internet, your communication with Zendesk is completely protected.

**Access Control**

All access to data within Zendesk is governed by access rights. Every user who attempts to access your Zendesk is authenticated by username and password. The administrator of your Zendesk instance may define granular access privileges to individual users, and email notifications alert administrators when someone is granted admin access.

Our security architecture ensures that each request to Zendesk is accompanied by user identity credentials to ensure segregation of customer data. Additional access controls include network IP restrictions and stricter access restrictions for Zendesk mobile apps.

**Application Security**

Zendesk maintains a robust application audit log, to include security events such as user logins or configuration changes. Additionally, Zendesk follows secure credential storage best practices by storing passwords using the bcrypt (salted) hash function.

**Vulnerability Management**

Zendesk and its supporting data security infrastructure are frequently reviewed for potentially harmful vulnerabilities.

We use industry-recognized, third-party security specialists, enterprise-class security solutions, and custom in-house tools to regularly analyze the application and production infrastructure to ensure that any vulnerabilities are identified and swiftly mitigated. We employ a number of third-party, qualified security tools to provide both regular dynamic scanning of our application and continuous static analysis of our codebase. Our Responsible Disclosure Policy gives researchers an avenue for safely testing and notifying Zendesk of security vulnerabilities.

**Privacy**

Zendesk is certified under E.U.-U.S. and Swiss-U.S. Safe Harbor Programs and is registered with the U.S. Department of Commerce’s Safe Harbor Program.