freshservice

Security Practices

Freshservice Security Practices

Freshservice is online IT service desk software that allows IT teams of organizations to support their users through email, phone, website and mobile. Freshservice is hosted on Amazon web services (AWS). The safety and security policies that AWS provided to us would be applicable to you as well, as customer of Freshservice.

Certifications

AWS continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

AWS's data center operations have been accredited under:

- ISO 27001
- SOC 1/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)
- HIPAA (at the server level)

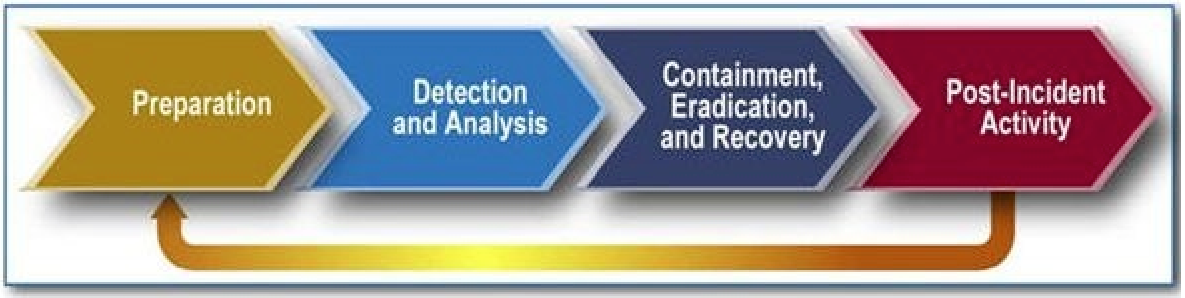
Amazon is a global leader in cloud services and much of their safety and security measures go well beyond the industry requirements. The scope of these assessments varies, and, depending on the need, is performed either in house, or by a third- party.

Our billing page transparently redirects to Braintree for payment processing services.

We are PCI compliant. We use Ruby on Rails and in general Rails takes care of all the OWASP framework requirements. We closely follow rails security patches and bring them in.

Information Security Program: Incident Response process

We use advanced monitoring tools to monitor availability and performance of our Application, Database servers and Virtual Servers. Automatic monitoring of server and application performance incidents are carried out using New Relic. We also use Pagerduty to monitor on-call schedule, escalation and incident resolution. Pagerduty immediately escalates an Incident when the application goes down to the first level of escalation team. Freshservice also has a 99.99% S LA and 24/7 dedicated support from AWS. Any issues with regard to application or database falls directly under our purview and incidents at the server level or database can be handled directly by us.



Control Measures to safeguard information

We continuously monitor the application health via new relic to see the server load, abnormal activity etc. We have a spam watcher inside the app which takes care of such load if it detects some user pumping lot of tickets etc we will automatically block them. All the passwords entered in the system are encrypted. We won't store any credit card details on our servers. All credit card info is stored in a secure PCI compliant vault at our Payment processor Braintree.   For attacks like DDoS we have a mechanism where we can simply enable read access and write access for admins of only authorized accounts. Every piece of code which will go into our repository is thoroughly reviewed by our CTO and will be tested by the QA team.

AWS and Freshdesk jointly share security responsibilities across different domains. These responsibilities include:

IaaS Provider (AWS)	**Freshservice**
● **Virtualization layer** ● **Network security (including DDOS, spoofing, and port scanning mitigation)**	● **Access Control** ● **Application code (non-platform related)** ● **Compliance**

● **Physical and environmental security** ***More details on AWS's security can be found at: https://aws. amazon.com/security***	

Firewalls-

The Freshservice cluster is protected by an AWS security group, which provides ingress network filtering from the broader Internet. By default, all access is denied with only explicitly defined ports and protocols permitted to enter the Freshservice environment.

Distributed Denial of Service (DDoS) Mitigation -

AWS's proprietary DDoS mitigation techniques lessens Freshservice's exposure to successful DDoS attacks. Also, AWS's networks are multi- homed across a number of ISPs to provide further Internet access diversity.

IP Spoofing -

Our instances are unable to send spoofed network traffic. The AWS- controlled firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

Port Scanning-

AWS maintains the capability and responsibility for detecting illicit port scans. When unauthorized port scanning is detected, AWS blocks the scan and notifies Freshservice via their abuse process.

Logging & Monitoring-

We maintain extensive logs including those specific to the application, operating system, and database layers. From a security perspective, this includes syslog, auth.log, HTTP connections to application logs, and writes to the database server.

We work together with other services that have SSL protocol so that all the data is encrypted. As we are on AWS, we are part of a security group so it won't open access to others. For more info http://support.rightscale.com/12-Guides/Dashboard_Users_Guide/Clouds/AWS_Region/EC2_Security_Groups/Concepts/About_EC2_Security_Groups

We follow strict security protocols that are internalized as part of the security awareness training that is provided during new hire employee onboarding. It clearly addresses each employee's security responsibility. The topics covered are:

- Importance of policies
- Ensuring customer data protection
- Corporate security considerations including confidentiality of information, the use of social media, and intellectual property protection
- Verification of identity of individual requesting access
- Understanding physical threats
- Importance of laptop security measures including hard drive encryption, VPN access, lockouts and regular patching
- Reporting security incidents to supervisor

To maintain the security and integrity of our workforce and data, we have implemented various controls. Customer data is restricted to only our operations team. Customer support team is granted access from time to time to resolve certain issues with the consent from our customers with our operations team overlooking and supervising the process. Sensitive details such as credit card information and passwords are not accessible to any employee in the organization.

Our team goes through internal training and the emphasis on security is ingrained into each and every member. Security measures are in place right from recruitment of an employee(full time, part time and contractual), oversight by a supervisor during the working tenure and proceeds to beyond termination of an employee. Some of the security measures followed at our organization are background checks prior to recruitment of candidates, adherence to Non- Disclosure Agreement and handover of security related data during the exit process. Background check evaluates past criminal and social media history along with reference validations.

Access to the production for administration and maintenance is still restricted to our intranet. Every access to the system is audited, logged and verified. A security team constantly checks for security related issues and updates teams on and upgrades and new technologies.

Control against threat of data theft/loss:

Your data would be stored on the cloud and hence the physical aspect of security issues would not arise here. Customer data is considered "confidential" information and is handled securely by our Company personnel. Customer data is not copied to Company assets, including employee laptops. Any troubleshooting that needs to be performed on customer data is performed in the customer's environment. Actions by Company personnel on a customer's system are limited to resolving the customer need, and nothing more. Once a customer is satisfied with the result, and the ticket is closed, access is removed.

That being said, we at Freshdesk have strict security policies governing the entry of personnel, laptops, storage devices such as USB drives and external hard disks. Access to our facility is restricted through biometric profiling and surveillance.

The physical security at AWS has the following controls

- AWS data centers are housed in nondescript facilities.
- Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.
- Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.
- All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
- AWS only provides data center access and information to employees & contractors who have a legitimate business need for such privileges.
- When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services.
- All physical access to data centers by AWS employees is logged and audited routinely.

Privacy Practices

Specific Compliance Initiatives

- AWS has achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)
- Statement on Standards for Attestation Engagements (SSAE 16): AWS is SOC 1/SSAE 16/ISAE 3402 certified.
- Safe Harbor Certification: AWS is Safe Harbor certified. Information available at: http://aws.amazon.com/privacy/

Handling, protection and sharing of confidential data

External parties, whom Freshdesk may share sensitive data with, are required to sign an NDA with Freshdesk prior to any conversations occurring. External third parties, who Freshdesk may directly contract with, are required to go through our vendor security due diligence process. Prior to moving forward, all high risk findings are required to be mitigated to a level acceptable to Freshdesk.

Routine data backups

Application code and databases are written out to persistent storage volumes If the need arises to ever rebuild instances from scratch, we have the ability to restore data's from previous snapshots.

We use AWS's S3 service for backups. By default, database backups are taken daily and are rotated every 10 days. However, customers can customize their backup schedule to meet their needs within the dashboard. If a requirement, backups can be stored using PGP encryption.

Business Continuity Management

Our App servers are behind Amazon's Elastic Load balancers. This ensures that request from outside world are load balanced across all our App servers efficiently.In case if any appserver froze, Amzon's elb detects it and send's traffic to other servers. This ensures high availability of our apps.

We currently do not have a redundant data management and we are working on improving our disaster recovery procedures and practices.