SECURITY AND ACKNOWLEDGEMENTS

Freshworks Data Security

Freshdesk, Inc. is now Freshworks, Inc.

Physical security

The Freshworks development center in Chennai is under 24x7 security protection, at both premises level and floor level to ensure only authorized individuals have access to the building and the Freshworks office. At the premises level, the building's perimeter is secured by barriers and guards. At the floor level, security guards and smartcard readers are present to authorize individuals before entry. Employees are granted access to the office only after authorization using smart cards. Critical locations in the office are accessible only to authorized individuals.

Important documents are stored in cabinets that can only be accessed by pre-authorized individuals. The office is equipped with surveillance cameras and their footage is monitored periodically by authorized individuals. Fire alarms and water sprinklers are in place to detect and mitigate damage in the unlikely event of a fire. Regular fire drills are also conducted by the premises management team to educate employees about emergency evacuation procedures. A policy has been implemented to approve and regulate visitor access to the building. The office is provided with 24x7 power supply, supported by an alternative uninterrupted power supply system to ensure smooth functioning in the event of power failure.

Freshworks hosts its application and data in industry-leading Amazon Web Services, whose data centers have been thoroughly tested for security, availability and business continuity. For more details, please read the AWS Security Whitepaper.

Application security

All of Freshworks products are hosted in Amazon Web Services. The infrastructure for databases and application servers is managed and maintained by Amazon.

At Freshworks, we take a multifaceted approach to application security, to ensure everything from engineering to deployment, including architecture and quality assurance processes complies with our highest standards of security.

Application Architecture

The application is initially protected by AWS's firewall which is equipped to counter regular DDoS attacks and other network related intrusions. The second layer of protection is Freshworks own application firewall which monitors against offending IPs, users and spam. While the application can be accessed only by users with valid credentials, it should be noted that security in cloud-based products is a shared responsibility between the company and the businesses who own those accounts on the cloud. In addition to making it easy for administrators to enforce industry-standard password policies on users, our products also come with features aimed at securing business data on the cloud:

- Configuring secure socket connections to portals
- Leveraging SAML and custom single sign-on
- Whitelisting IPs for exclusive access
- Identity management via Google and Facebook credentials
- Custom email servers, etc.

It should be noted that all account passwords that are stored in the application are one-way hashed and salted.

Freshworks uses a multi-tenant data model to host all its applications. Each application is serviced from an individual virtual private cloud and each customer is uniquely identified by a tenant ID. The application is engineered and verified to ensure that it always fetches data only for the logged-in tenant. Per this design, no customer has access to another customer's data. Access to the application by the Freshworks development team is also controlled, managed and audited. Access to the application and the infrastructure are logged for subsequent audits.

The in-line email attachment URLs for the product are public by design, to enable us to embed links within the email for end-user ease. This can be made private on customer request.

Application Engineering and Development

Our engineers are trained in industry-leading secure coding standards and guidelines to ensure our products are developed with security considerations from the ground-up. A security review is a mandatory part of application engineering (development and construction) process at Freshworks. The security review

leverages static code analysis tools, in addition to manual reviews, to ensure adherence to our highest standards.

Quality Assurance

Besides functional validation and verification, the quality assurance process at Freshworks also subjects application updates to a thorough security validation. The validation process is performed by a dedicated app security team with ethical hackers whose goal is to discover and demonstrate vulnerabilities in the application. An update to the application does not get the stamp of approval from the quality assurance team if vulnerabilities (that can compromise either the application or data) are identified.

Deployment & Post Deployment

Deployments to production servers are performed only by trusted and authorized engineers. Only very few pre-authorized engineers have access to Freshworks production environment. In order to view and inspect access logs, engineers need to go through a committee of authorized employees, who will then deliver the logs to them after validating their purpose.

Post-deployment monitoring is done by a dedicated 24x7 NOC team that monitors the application for suspicious activities or attacks. The application is engineered to detect and alert the NOC team about suspicious activities and abnormal load situations in the infrastructure. An escalation matrix up to two levels of engineers has been defined to address contingencies that might occur.

An information security team carries out periodic comprehensive application audits. The tests are performed with the help of static analysis tools and aided by manual analysis. Network penetration tests and other black box tests are performed to help identify security vulnerabilities in the application. The security team stays vigilant about common vulnerabilities and exposures and stays on top of updates to the US National Vulnerabilities Database.

Data Security

Freshworks takes the protection and security of its customers' data very seriously. Freshworks manages the security of its application and customers' data. However, provisioning and access management of individual accounts is at the discretion of individual business owners.

The Freshworks development team has no access to data on production servers. Changes to the application, infrastructure, web content and deployment processes are documented extensively as part of an internal change control process. The security review mandates that each version is compliant with the company's internal ISMS policies.

Our products collect limited information about customers - name, email address and phone - which are retained for account creation. Postal address is requested and retained by Freshworks PCI compliant payment processor for billing, along with the date of expiry of credit card and CVV.

Freshworks takes the integrity and protection of customers' data very seriously. We maintain history of two kinds of data: application logs from the system, and application and customers' data. All data is stored in Amazon's state of the art cloud computing platform, AWS. Backups are taken every five minutes at multiple locations.

Application logs are maintained for a duration of 90 days. Customers' data is backed up in two ways:

1. A continuous backup is maintained in different datacenters to support a system failover if it were to occur in the primary datacenter. Should an unlikely catastrophe occur in one of the datacenters, businesses would lose only five minutes of data.
2. Data is backed up to persistent storage everyday and retained for the last seven days.

In Europe & United States the data at rest is encrypted using AES 256bit standards (key strength - 1024) with the keys being managed by AWS Key Management Service. All data in transit is encrypted using FIPS-140-2 standard encryption over a secure socket connection for all accounts hosted on Freshworks.com. For accounts hosted on independent domains, an option to enable a secure socket connection is available.

Different environments are in use for development and testing purposes, access to systems are strictly managed, based on the principles of need to do/know basis appropriate to the information classification, with Segregation of Duties built in, and reviewed on a quarterly basis.

Data Deletion

When an account is deleted, all associated data is destroyed within 14 business days. Freshworks products also offer data export options which businesses can use if they want a backup of their data before deletion.

Operational Security

Freshworks understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity. The company has clear change management processes, logging and monitoring procedures, and fallback mechanisms which have been set up as part of its operational security directives. An information security committee is present to oversee and approve all organization-wide security policies.

Operational security starts right from recruiting an engineer to training and auditing their work products. The recruitment process includes standard background verification checks (including verification of

academic records) on all new recruits. All employees are provided with adequate training about the information security policies of the company and are required to sign that they have read and understood the company's security-related policies. Confidential information about the company is available for access only to select authorized Freshworks employees.

Employees are required to report any observed suspicious activities or threats. The human resources team takes appropriate disciplinary action against employees who violate organizational security policies. Security incidents (breaches and potential vulnerabilities) can be reported by customers through our portal at support.freshworks.com or via email: security@freshworks.com.

Freshworks maintains an inventory of all information systems used by employees for development purposes in an internal service desk, aided by automated probing software that assists in tracking changes to these systems and their configurations. Only authorized and licensed software products are installed by employees. No third parties or contractors manage software or information facilities, and no development activity is outsourced. All employee information systems are authorized by the management before they are installed or put to use.

In order to test the resilience of the hosted application, the company employs an external security consultant and additional ethical hackers who perform penetration tests. This is always conducted in an architecturally equivalent copy of the system with no actual customer data present. The production system is never subject to such tests. Should an individual attempt such a test in the production environment, it will be detected as an intrusion, and the source IP will be blocked. An alert will then be raised so engineers can attend to the incident.

The company has a privacy policy, approved by an internal legal counsel, available publicly at http://www.freshworks.com/privacy. The payment gateway used by all of Freshworks' products is PCI compliant.

Network Security

Network security is discussed in detail in this section from the perspective of the development center, and the network where the application is hosted.

The Freshworks office network where updates are developed, deployed, monitored and managed is secured by industry-grade firewalls and antivirus software, to protect internal information systems from intrusion and to provide active alerts in the event of a threat or an incident. Firewall logs are stored and reviewed periodically. Access to the production environment is via SSH and remote access is possible only via the office network. Audit logs are generated for each remote user session and reviewed. Also, the access to production systems are always through a multi-factor authentication mechanism.

All Freshworks products are hosted in AWS, with security managed by Amazon. The NOC and DevOps teams monitor the infrastructure 24x7 for stability, intrusions and spam using a dedicated alert system. Every three months, end-to-end vulnerability assessments and penetration tests are performed. The Freshworks application has an in-built spam protection system for businesses that use it, while the NOC team monitors and blocks individual accounts and IP addresses which attempt to access the Freshworks applications.

Regulatory Compliance

All formal processes and security standards at Freshworks are designed to meet regulations at the industry, state, federal and international levels. Freshworks has been awarded TRUSTe's Privacy Seal signifying that its privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe's program requirements and the TRUSTed Cloud Program Requirements including transparency, accountability and choice regarding the collection and use of customers' personal information. The TRUSTe program covers only information that is collected through our websites and platforms. Freshworks adheres to strict data security, access, integrity policies, among other principles defined in the safe harbor framework. The third party payment processor used by Freshworks is PCI compliant, meaning credit card data is securely stored and processed.

Use of our service by customers in the European Economic Area ("EEA"), will include the processing of information relating to their customers. In providing our service, we do not own, control or direct the use of the information stored or processed on our platform at the direction of our customers, and in fact we are largely unaware of what information is being stored on our platform and only access such information as reasonably necessary to provide the service (including to respond to support requests), as otherwise authorized by our customers or as required by law. We are data processors for our end customers, but data controllers for the customers from whom we collect data on our platform for purposes of the European Union ("EU") on our platform for purposes of the European Union ("EU") Directive 95/46/EC on Data Protection ("EU Directive") and the Swiss Federal Act on Data Protection. Our EEA or Switzerland based customers, who control their customer data and send it to Freshworks for processing, are the "controllers" of that data and are responsible for compliance with the Directive. In particular, Freshworks customers are responsible for complying with the Directive and relevant data protection legislation in the relevant EEA member state before sending personal information to Freshworks for processing.

As the processors of personal information on behalf of our customers, we follow their instructions with respect to the information they control to the extent consistent with the functionality of our service. In doing so, we implement industry standard security, technical, physical and administrative measures against unauthorized processing of such information and against loss, destruction of, or damage to, personal information as more fully described in Freshworks privacy policy.

If requested by European customers, Freshworks can store their data in the data center at Dublin, Ireland but the data may be processed outside the EU in connection with provision of our services, specifically:

a. Customer data is processed within the Freshworks group i.e. Freshworks Inc. and its subsidiaries and affiliates;

b. We use multiple third-party cloud providers as part of our architecture for the purposes of logging, billing and system monitoring. In connection with this data might be transferred outside our EU data center. Third party providers relating to the following are currently based in regions that are not within the EEA:

    i. Phone feature is not EU specific. The phone data can be stored anywhere in the world;

    ii. Chat feature service providers are based out of US;

    iii. Plugins;

    iv. App integrations;

    v. Third party payment processor

We work with our customers to help them provide notice to their customers concerning the purpose for which personal information is collected and sign Model Contract Clauses (for data processors) with them to legitimize transfers of personal data from EU to processors established in third countries as may be required under the EU Directive.

Freshworks privacy practices are TRUSTe certified and we are ISO 27001:2013 compliant. We are working towards SSAE-16 attestation and a SOC II report will be available shortly. Our data centers are hosted in AWS who are ISO 27001, SSAE-16 and HIPAA compliant.

Freshworks has now, also self-certified its compliance with the EU-US Privacy Shield 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 products include functionalities provided by third parties, which do not offer regional hosting and hence, we cannot restrict the transfer of data from the European Union, but the EU-US Privacy Shield acts as a way to legitimize such data transfer to the U.S. Our certification states that we comply with the Privacy Shield principles for the transfer of European personal data to the United States.

Having complied with the requirements of TRUSTe, Privacy Shield Framework and ISO 27001, the platform has been comfortably set for Freshworks to further work on GDPR compliance and achieve it by the time it's regulations come into effect. Currently, Freshworks is not HIPAA compliant.

Reporting issues and threats

If you have found any issues or flaws impacting the data security or privacy of Freshworks users, please write to security@freshworks.com with the relevant information so we can get working on it right away.

Your request will be looked into immediately. We might ask for your guidance in identifying or replicating the issue and understanding any means to resolving the threat right away.

We encourage you to encrypt your message with our public key to ensure that it it remains safe in transit. Please be clear and specific about any information you give us. We deeply appreciate your help in detecting and fixing flaws in Freshworks, and will acknowledge your contribution to the world once the threat is resolved.

Get in touch with us

If you have any questions or doubts, feel free to get in touch with us at support@freshworks.com, and we'll get back to you right away.