Heroku Security

Heroku Overview

Heroku is a cloud application platform used by organizations of all sizes to deploy and operate applications throughout the world. Our platform allows organizations to focus on application development and business strategy while Heroku focuses on infrastructure management, scaling, and security. Heroku applies security best practices and manages platform security so customers can focus on their business. Our platform is designed to protect customers from threats by applying security controls at every layer from physical to application, isolating customer applications and data, and with its ability to rapidly deploy security updates without customer interaction or service interruption.

Heroku's Commitment to Trust

“Nothing is more important to our company than the privacy of our customer’s data." -- Parker Harris, salesforce.com EVP, Technology

Trust is a core principle of salesforce.com and Heroku. It’s this commitment to customer privacy and inspiring trust that directs the decisions we make on a daily basis. Trust is the responsibility of each and every employee and one we take seriously.

To learn more about Salesforce.com efforts to protect customer privacy and actions customers can take to protect their data visit the Salesforce Trust And Compliance Policies.

Vulnerability Reporting

As part of our commitment to working with security researchers to make our platform safer, Heroku operates a bug bounty program to reward those who find and report bugs in our platform. Our bug bounty program is managed through Bugcrowd. To see the terms of the program and participate, go to Bugcrowd and sign up as a tester. If you have identified a vulnerability, please report it via Bugcrowd to be eligible for a reward.

For other security inquiries, please open a support ticket.

Security Assessments and Compliance

Data Centers

Heroku’s physical infrastructure is hosted and managed within Amazon’s secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon’s data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

PCI

We use PCI compliant payment processor Braintree for encrypting and processing credit card payments. Heroku’s infrastructure provider is PCI Level 1 compliant.

Sarbanes-Oxley

As a publicly traded company in the United States, salesforce.com is audited annually and remains in compliance with the Sarbanes-Oxley (SOX) Act of 2002.

Penetration Testing and Vulnerability Assessments

Third party security testing of the Heroku application is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team.

Physical Security

Heroku utilizes ISO 27001 and FISMA certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three 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.

Amazon only provides data center access and information to employees 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 and electronic access to data centers by Amazon employees is logged and audited routinely.

For additional information see: https://aws.amazon.com/security

Environmental Safeguards

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Climate and Temperature Control

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data

centers are conditioned to maintain atmospheric conditions at optimal levels. Monitoring systems and data center personnel ensure temperature and humidity are at the appropriate levels.

Management

Data center staff monitor electrical, mechanical and life support systems and equipment so issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

For additional information see: https://aws.amazon.com/security

Network Security

Firewalls

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Host-based firewalls restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

DDoS Mitigation

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Heroku utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

Port Scanning

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

Data Security

Customer Applications

Each application on the Heroku platform runs within its own isolated environment and cannot interact with other applications or areas of the system. This restrictive operating environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system using LXC while host-based firewalls restrict applications from establishing local network connections.

For additional technical information see: https://devcenter.heroku.com/articles/dyno-isolation

Heroku Postgres

Customer data is stored in separate access-controlled databases per application. Each database requires a unique username and password that is only valid for that specific database and is unique to a single application. Customers with multiple applications and databases are assigned separate databases and accounts per application to mitigate the risk of unauthorized access between applications.

Customer connections to postgres databases require SSL encryption to ensure a high level of security and privacy. When deploying applications, we encourage customers to take advantage of encrypted database connections.

Stored data can be encrypted by customer applications in order to meet data security requirements. Customers can implement data storage, key management, and data retention requirements when developing their application.

Add-ons

Customers can extend the functionality of applications by using Heroku Add-ons. Add-ons are offered and managed by 3rd party companies and implement their own security controls and processes.

For additional information see: https://addons.heroku.com

System Security

System Configuration

System configuration and consistency is maintained through standard, up-to-date images, configuration management software, and by replacing systems with updated deployments. Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems.

Customer Application Isolation

Applications on the Heroku platform run within their own isolated environment and cannot interact with other applications or areas of the system to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system while host-based firewalls restrict applications from establishing local network connections.

For additional technical information see: https://devcenter.heroku.com/articles/dyno-isolation

System Authentication

Operating system access is limited to Heroku staff and requires username and key authentication. Operating systems do not allow password authentication to prevent password brute force attacks, theft, and sharing.

Vulnerability Management

Our vulnerability management process is designed to remediate risks without customer interaction or impact. Heroku is notified of vulnerabilities through internal and external assessments, system patch monitoring, and third party mailing lists and services. Each vulnerability is reviewed to determine if it is applicable to Heroku's environment, ranked based on risk, and assigned to the appropriate team for resolution.

New systems are deployed with the latest updates, security fixes, and Heroku configurations and existing systems are decommissioned as customers are migrated to the new instances. This process allows Heroku to keep the environment up-to-date. Since customer applications run in isolated environments, they are unaffected by these core system updates.

To further mitigate risk, each component type is assigned to a unique network security group. These security groups are designed to only allow access to the ports and protocols required for the specific component type. For example, user applications running within an isolated dyno are denied access to the Heroku management infrastructure as each is within its own network security group and access is not allowed between the two.

Heroku Application Security

We undergo penetration tests, vulnerability assessments, and source code reviews to assess the security of our application, architecture, and implementation. Our third party security assessments cover all areas of our platform including testing for OWASP Top 10 web application vulnerabilities and customer application isolation. Heroku works closely with external security assessors to review the security of the Heroku platform and applications and apply best practices.

Issues found in Heroku applications are risk ranked, prioritized, assigned to the responsible team for remediation, and Heroku's security team reviews each remediation plan to ensure proper resolution.

Backups

Customer Applications

Applications deployed to the Heroku platform are automatically backed up as part of the deployment process on secure, access controlled, and redundant storage. We use these backups to deploy your application across our platform and to automatically bring your application back online in the event of an outage.

Customer Postgres Databases

Continuous Protection keeps data safe on Heroku Postgres. Every change to your data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the database to within seconds of its last known state. We also provide you with the ability to backup your database to meet your own backup and data retention requirements.

For additional technical information see: https://devcenter.heroku.com/articles/pgbackups

Customer Configuration and Meta-information

Your configuration and meta-information is backed up every minute to the same high-durability, redundant infrastructure used to store your database information. These frequent backups allow capturing changes made to the running application configuration added after the initial deployment.

Heroku Platform

From our instance images to our databases, each component is backed up to secure, access-controlled, and redundant storage. Our platform allows for recovering databases to within seconds of the last known state, restoring system instances from standard templates, and deploying customer applications and data. In addition to standard backup practices, Heroku's infrastructure is designed to scale and be fault tolerant by automatically replacing failed instances and reducing the likelihood of needing to restore from backup.

Disaster Recovery

Customer Applications and Databases

Our platform automatically restores customer applications and Heroku Postgres databases in the case of an outage. The Heroku platform is designed to dynamically deploy applications within the Heroku cloud, monitor for failures, and recover failed platform components including customer applications and databases.

Heroku Platform

The Heroku platform is designed for stability, scaling, and inherently mitigates common issues that lead to outages while maintaining recovery capabilities. Our platform maintains redundancy to prevent single points of failure, is able to replace failed components, and utilizes multiple data centers designed for resiliency. In the case of an outage, the platform is deployed across multiple data centers using current system images and data is restored from backups. Heroku reviews platform issues to understand the root cause, impact to customers, and improve the platform and processes.

Customer Data Retention and Destruction

You have the freedom to define what data your applications store and the ability to purge data from your databases to comply with your data retention requirements. If you deprovision an application and the associated database, we maintain the database's storage volume for one week after which time its automatically destroyed rendering the data unrecoverable.

Decommissioning hardware is managed by our infrastructure provider using a process designed to prevent customer data exposure. AWS uses techniques outlined in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data.

For additional information see: https://aws.amazon.com/security

Privacy

Heroku has a published privacy policy that clearly defines what data is collected and how it is used. Heroku and salesforce.com are committed to customer privacy and transparency.

We takes steps to protect the privacy of our customers and protect data stored within the platform. Some of the protections inherent to Heroku's products include authentication, access controls, data transport encryption, HTTPS support for customer applications, and the ability for customers to encrypt stored data. For additional information see: https://www.heroku.com/policy/privacy

Access to Customer Data

Heroku staff does not access or interact with customer data or applications as part of normal operations. There may be cases where Heroku is requested to interact with customer data or applications at the request of the customer for support purposes or where required by law. Customer data is access controlled and all access by Heroku staff is accompanied by customer approval or government mandate, reason for access, actions taken by staff, and support start and end time.

Employee Screening and Policies

As a condition of employment all Heroku and salesforce.com employees undergo pre-

employment background checks and agree to company policies including security and acceptable use policies.

Security Staff

Our security team is lead by the Chief Information Security officer (CISO) and includes staff responsible for application and information security. The security team works closely with the entire Heroku organization and customers to address risk and continue Heroku's commitment to trust.

Customer Security Best Practices

Encrypt Data in Transit

Enable HTTPS for applications and SSL database connections to protect sensitive data transmitted to and from applications.

Encrypt Sensitive Data at Rest

Customers with sensitive data can encrypt stored files and data within databases to meet their data security requirements. Data encryption can be deployed using industry standard encryption and the best practices for your language or framework.

Secure Development Practices

Apply development best practices for your chosen development language and framework to mitigate known vulnerability types such as those on the OWASP Top 10 Web Application Security Risks.

Authentication

To prevent unauthorized account access use a strong passphrase for both your Heroku user account and SSH keys, store SSH keys securely to prevent disclosure, replace keys if lost or disclosed, and use Heroku's RBAC model to invite contributors rather than sharing user accounts.

Logging

Logging is critical for troubleshooting and investigating issues. We provide you with three main options for interacting with their system, application, and API logs. Customers can receive all 3 types of logs via syslog from the Heroku platform, choose to send logs to a Heroku add-on, or interact with logs in real-time through the Heroku client.

For additional technical information see: https://www.heroku.com/how/observe

Use of Third-Party Solutions

In developing your application on Heroku you may choose to use third party services for added functionality such as Amazon's S3, an email service provider, or any of our add-on partners. Be mindful of the data shared with these providers and their security practices just as you would be with Heroku.

HEROKU IS A COMPANY

heroku.com Terms of Service Privacy Cookies