Wundamail Security Overview

Executive Summary

Wundamail has a commitment to security that is unparalleled in the ‘software-as-a-service’ field. The main driver of this commitment is from the founders of the business.

Before the founders began Wundamail they founded (and later sold to Aspect Software as part of a $150m transaction) a business called Qivox that provided security and fraud detection services to the very best in public and private sector organisations.

Customers included Lloyds Bank, Halifax, TSB and Bank of Scotland. In fact, these customers still use Qivox fraud detection today, to secure their digital online and mobile banking facility.

Suffice to say, the team at Wundamail are more than familiar with providing secure services that operate at the highest levels of banking security. To this end, you can be assured that data security is the highest priority that Wundamail has, and is backed by a team that really knows what they are doing.

Wundamail Limited

support@wundamail.com
www.wundamail.com

wundamail

Wundamail Hosting Overview

Wundamail is hosted on Heroku - a cloud application platform used by organizations of all sizes to deploy and operate applications throughout the world. The platform allows Wundamail 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 Wundamail can focus on their business. The platform inherently protects 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.

To give you an idea of the quality and scalability of Heroku, Salesforce.com - the largest software-as-a-service provider in the world also runs on Heroku.

Our Commitment to Trust

Trust is a core principle of Wundamail, 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.

wundamail

Security Assessments and Compliance

Data Centers

Wundamail and 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)

Penetration Testing and Vulnerability Assessments

Third party security testing of the Wundamail application and Heroku 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

Wundamail 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.

wundamail

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 backup 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.

wundamail

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. Wundamail 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. When port scans are detected, they are stopped and access is blocked.

wundamail

Data Security

The Wundamail Application

Wundamail runs within its own isolated environment and cannot interact with other applications or areas of Heroku. 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

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 Wundamail including testing for OWASP Top 10 web application vulnerabilities and customer application isolation. Wundamail works closely with external security assessors to review the security of Wundamail and apply best practices.

The Wundamail Database

Customer data is stored in a separate access-controlled database. The database requires a unique username and password that is only valid for that specific database and is unique to Wundamail.

Connections to the database requires SSL encryption to ensure a high level of security and privacy. When deploying applications, Wundamail takes advantage of encrypted database connections.

Stored data is encrypted at rest. Wundamail also has processes in place to manage data storage, key management, and data retention.

wundamail

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

Heroku undergoes penetration tests, vulnerability assessments, and source code reviews to assess the security of the application, architecture, and implementation. Heroku third party security assessments cover all areas of the 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.

wundamail

Backups

Applications

Wundamail is automatically backed up as part of the deployment process on secure, access controlled, and redundant storage. These backups are used to deploy Wundamail across Heroku and to automatically bring the application back online in the event of an outage.

Databases

Continuous Protection keeps data safe on the Wundamail database. Every change to 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 have implemented further backup processes to meet our backup and data retention requirements.

Configuration and Meta-information

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

Heroku Platform

From instance images to our databases, each component is backed up to secure, access-controlled, and redundant storage. Heroku 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.

wundamail

Disaster Recovery

Application and Database

The Wundamail application and database is automatically restored 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. The 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.

Data Retention and Destruction

Wundamail defines what data to store and has the ability to purge data from databases to comply with our data retention requirements. If we 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

wundamail

Privacy

Wundamail has a published privacy policy that clearly defines what data is collected and how it is used.

We takes steps to protect the privacy of our customers and protect data stored within the platform. Some of the protections inherent to Wundamail include authentication, access controls, data transport encryption, HTTPS, and encrypted stored data.

Access to Customer Data

Wundamail staff does not access or interact with customer data as part of normal operations. There may be cases where Wundamail is requested to interact with customer data for support purposes or where required by law. Customer data is access controlled and all access by Wundamail 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 Wundamail, Heroku and salesforce.com employees undergo pre-employment background checks and agree to company policies including security and acceptable use policies.

Secure Development Practices

We apply development best practices to mitigate known vulnerability types such as those on the OWASP Top 10 Web Application Security Risks.

We manually peer review code to ensure adherence to our desire to employ development best practices and mitigate against the introduction of vulnerabilities.

We also use several automated tools to police code quality and monitor security. These include CodeClimate and Gemnasium.

Authentication

To prevent unauthorized account we use a strong passphrases for both our 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.

wundamail

Wundamail and GDPR

Wundamail is committed to European General Data Protection Regulation (“GDPR”) compliance, which takes effect on May 25, 2018.

Wundamail has taken many steps to protect the personal data of our customers, including but not limited to:

- Wundamail offerings are provided using established and industry-leading cloud services platforms. These providers have stated their commitment to compliance with GDPR.

- Wundamail offerings are localized in the region where our customer is located unless the customer expressly designates another locality.

- Wundamail maintains and administers a security policy with physical, technical, and administrative safeguards designed to protect the security, integrity and confidentiality of customer data.

- Wundamail’s hosted solutions may be used by customers for, among other things, the collection, processing, and storage of personal data. In such cases, Wundamail acts as a data processor. Customers generally act as the data controller deciding what data to collect, how long it is stored and how it is used. Since each business is unique, Wundamail recommends that each company perform their own GDPR readiness assessment.

- Our up to date privacy policy is available on the Wundamail website at https://www.wundamail.com/privacy-policy

- Our detailed GDPR specific policy statement is available on the Wundamail website at https://www.wundamail.com/gdpr

You may direct questions to support@wundamail.com

Wundamail Limited

support@wundamail.com
www.wundamail.com