Pingboard Security Brief

May 14, 2018

Introduction

Pingboard enables companies to securely share employee directory and org chart information with their employees. Helping to protect the confidentiality, integrity, and availability of our customers' data is of the utmost importance to Pingboard, as is maintaining customer trust and confidence. This document is intended to outline the security features Pingboard has put in place to protect customer data.

Pingboard Security Features:

- SSL restricted traffic for all client-server communication.
- Multi-factor authentication.
- SAML 2.0 based single sign-on.
- Network and host based firewalls with least privilege rules.
- Data encrypted at-rest.
- Change control process with vulnerability scans and peer code reviews.
- Least privilege role based user management and regular reviews of access levels.
- Access controls to limit the data that users can view or edit.
- Audit log, including an offsite replica of the log.
- Routine software patching, including 24-hour patching for major security threats.
- Routine penetration testing.

Security FAQ

Where do we host our services?

Pingboard hosts its software-as-a-service at Heroku and Amazon Web Services (AWS) for their unparalleled security, scalability and availability. Heroku is a platform for hosting and scaling applications running in AWS data centers. Utilizing AWS infrastructure, Pingboard inherits AWS-network, ops and monitoring to satisfy stringent physical and network intrusion requirements. AWS is SOC 2 Type 2 Certified, HIPAA compliant, and PCI compliant.

When was our hosting facility audited (SOC 2, ISO, etc.) and what were the detailed results?

The AWS SOC 1 and SOC 2 audit was completed within the last 18 months, and AWS received a favorable unbiased opinion from its independent auditors. The control objectives and control activities of AWS are focused on operational performance and security to protect customer data. A copy of the report is available from AWS upon request and with an executed NDA in place with Amazon. Pingboard has reviewed the SOC 2 audit in detail and is satisfied that AWS infrastructure meets or exceeds all critical SOC 2 audit protocols.

In addition, AWS has been accredited under the cloud specific standards ISO 27017:2015 and ISO 27018:2014, as well as ISO 9001, ISO 27001, PCI Level 1, FISMA Moderate, Sarbanes-Oxley (SOX).

What physical security controls in place to protect the environment processing or storing customer data?

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

Is our network based on a 3-tier structure? How is the internal network separated from the DMZ, and the DMZ is separated from the external network?

Yes. External HTTP requests are received by a load balancer that handles SSL termination. From here they are passed to a set of routers that are responsible for determining the location of application server to handle the request and forwarding the HTTP request to one of these servers. Application servers are only accessible on a private network and do not have an IP address or direct connection to the public Internet. Further, the application itself runs in an isolated virtual environment that connects to database servers using a dedicated private network and applications are denied access to the management infrastructure as each is within its own network security group and access is not allowed between the two. Additionally, our corporate network has no backdoors into our staging or production systems.

What network security devices, such as firewalls and IDS/IPS are in use to protect critical systems and sensitive data?
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 applications from establishing localhost connections over the loopback network interface and further limit inbound and outbound connections as needed.

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. Application isolation, operating system restrictions, and encrypted connections are used to further ensure risk is mitigated at all levels. 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.

What change control and security code review procedures are in place?
The network and infrastructure systems are managed by our infrastructure provider, Amazon AWS. AWS data center operations have been accredited under: ISO 27001, SOC 1 and SOC 2, PCI Level 1, FISMA Moderate, Sarbanes-Oxley (SOX).

Changes to the Pingboard application go through the following process:

1. Automated test suite is run on changes before being merged into the code base.
2. Static security analyzers are run as part of the test suite. Any potential vulnerabilities must be either confirmed as false positive or fixed before the change moves forward.
3. Peer code review is performed, for code quality and security.
4. Change is merged and deployed to a staging environment.
5. Final testing is done by the QA team.
6. Change is then available to be merged to the production environment

What is the patch management process (for network, application and databases - hardware & software). What is the length of time between patch availability and implementation?
For network, hardware, and database software, our infrastructure provider 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, ranked based on risk, and assigned to the appropriate team for resolution.

For application software, the security team is subscribed to notifications for CVE's affecting third party software and libraries in use. We also regularly run static analysis tools which are updated with CVE's against new code changes. Security patches are applied within 24 hours of release.

Are all servers and software at the current patch levels and fully supported?
Yes. New servers are deployed with the latest updates and security fixes, and existing servers are upgraded on a rolling basis, which is expedited for critical security patches.

Where is customer data is retained? Is the data stored on laptops, mobile devices or removable media?
Data is retained in the application database and onsite and offsite backup copies of the database used for disaster recovery purposes only. In order to improve and support the Pingboard application, limited data is also stored in our analytics and customer support database. Data is not retained on any laptops, mobile devices, or removable media.

How is customer data is protected when hardware is decommissioned?

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.

How is one customer’s data segmented from other customers’ data?
All customer data is tenanted within our database, and no access is allowed by the application outside of the logged in tenant. Tenants are logically separated at the application level. Optional access controls are also available inside the application to limit which information customer employees can view about other employees in the same company.

At the operating system layer, AWS currently utilizes a highly customized version of the Xen hypervisor. Because paravirtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, the guest OS has no elevated access to the CPU. This explicit virtualization of the physical resources leads to a clear separation between guest and hypervisor, resulting in additional security separation between the two. Different instances running on the same physical machine are isolated from each other via the Xen hypervisor. In addition, the AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance’s neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.

Explain the (1) access control management (is it role based model?) and (2) how are access to data policies enforced (in all relevant layers, platforms, network devices etc.).
Physical access is strictly controlled by Amazon 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. Data center access and electronic access to network devices is only provided to data center employees who have a legitimate business need for such privileges. When

an Amazon employee no longer has a business need for these privileges, his or her access is immediately revoked. All physical and electronic access to data centers by Amazon employees is logged and audited routinely.

Operating system access is limited to staff who have a legitimate business need. Security best practices in place to safeguard server instances include, but are not limited to, the disabling of password-based access to hosts, certificate-based SSH Version 2 access protocols, multi-factor authentication, unique key pairs, and a privilege escalation system with per-user logging.

AWS does not possess access rights to the operating system of Pingboard server instances. This separation of power provides a necessary structure of checks-and-balances to protect the integrity of the application.

Access to customer data stored in Pingboard is limited to staff who provide customer support and DevOps. Pingboard employees are trained to access this data only when there is a legitimate business need and all access is logged.

Is single sign-on (SSO) supported?
The Pingboard application supports single sign-on using the SAML 2.0 standard, which is the standard used by popular identity management systems such as Okta and OneLogin. Pingboard also supports single sign-on using Google Apps. Authentication via password credentials can be disabled so that single sign-on is enforced.

What monitoring capabilities are implemented to identify access to customer data and servers that contain customer data?
All physical and electronic access to data centers by Amazon employees is logged and audited routinely. All application logins by customer's users and Pingboard employees is logged. All changes to customer data by a customer's users and Pingboard staff are logged to an audit trail which tracks the change made, the time of the change, and the user who made the change. The last 40 revisions of every piece of data is retained. After 40, the oldest change in the audit trail is discarded.

What encryption mechanisms are in place both for data in transit and data at rest?
Data in transit is encrypted using TLS or SSL using a SHA-2 SSL certificate. Data is encrypted at rest using AES-256, block-level storage encryption.

How long will customer data be retained? What options exist to destroy customer data at the end of the engagement?
When a customer deletes data or terminates service with Pingboard, data is marked as deleted and kept in the production system for recovery purposes for up to 90 days. Data can be purged from the production system sooner upon request. To the extent the data has been archived to backup systems, that archived copy will be destroyed in accordance with Pingboard's standard backup destruction procedures, within 90 days from the date it was backed up.

Are the production environment is physically and logically separated from development and test environments? Will customer data be in use in the development or test environment?
The production environment is completely separate from development and test environments. Customer data is not in use in the development or test environments.

What is the password policy for systems that host customer data, or allow access to systems that store/process customer data.
All system passwords are changed on a confidential defined schedule, and passwords comply with best practices in length and complexity. All passwords stored in the Pingboard application are stored using a one-way hash with the bcrypt algorithm.

What is the user management processes for Pingboard staff?
Pingboard employees are granted least privilege access to systems storing customer data on an as needed basis. Access-levels that include access to the customer application data must be approved by the CTO. Access to the customer support systems must be approved by the Support Manager.

Each Pingboard employee's access level is reviewed whenever their role changes, either through adding new access-levels or removing old ones. When an employee is terminated, their access to Pingboard systems and customer data is terminated on the day of termination, if not before.

Pingboard employees are required to use 2-factor authentication to access the hosting environment and the Pingboard application.

What user account management capabilities are available for customer user accounts?

Customer users of Pingboard will have one of 2 roles, “Company Admin” or “Regular User”. Company Admins can view and edit information about other users. They also can control the viewing permissions of Regular Users. Each employee data field can be made either viewable to all Regular Users inside the customer’s account, restricted to just Company Admins, or restricted to just Company Admins and the Regular User who owns the profile. Company Admins have the power to change a Regular User’s role and make them a Company Admin, or change another Company Admins role and make them a Regular User.

What are our audit trail and logging capabilities?

All application logins by customer’s users and Pingboard employees are logged. All changes to data in the application database are logged to an audit table which tracks the change made, the time of the change, and the user who made the change. Changes are tracked for 40 revisions. This audit logging applies to both customer users and Pingboard staff.

How do we protect the audit trails?

Audit trails are stored in a centralized database server. Every change 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 containing the audit trail to within seconds of its last known good state.

What are the redundancy features of Pingboard?

Our hosting platform is designed with redundancy at all layers to prevent single points of failure, is able to automatically migrate workloads from failed components, and utilizes multiple data centers designed for resiliency. Application software is backed up as part of the deployment process and stored on secure, access controlled, and redundant storage. Application configuration and meta-information is backed up every minute to capture changes to the running applications after deployment. These backups are used bring the application back online in the event of an outage.

Pingboard databases operate in high availability clusters designed to increase database availability in the face of hardware or software failure. Databases are replicated using write-ahead logs, which are shipped to multi-datacenter, high-

durability storage. When a primary database fails, it is automatically replaced with a standby database containing a live replica of the primary database.

Binary backup copies of the database and write ahead log files are pushed to Amazon's S3 object store. Committed transactions are recorded as write ahead log files, which are able to be replayed on top of the binary backups, providing a method of completely reconstructing the state of a database.

The server infrastructure of AWS is known as Elastic Compute Cloud, or EC2. EC2 uses Availability Zones ensure failure-resilient operations with planned fault separation. Availability Zones are physically separated facilities engineered to remain insulated from any failure in other locations. Availability Zones in the same geographic region are located on different floodplains, in areas determined to be seismically stable, and maintain low-latency connectivity with each other. Server instances running in separate Availability Zones safeguard an application from the failure of a single location.

Data traffic between Availability Zones is transmitted across AWS-controlled private network infrastructure, which provides minimal latency, transmission consistency, and end-to-end security.

Each facility receives power from different grids, and from independent utilities to further protect against single points of failure. In addition, discrete uninterruptable power source (UPS) systems, batteries, and onsite diesel backup generators standby to regulate flow, prevent spikes and brownouts, and convey clean power in the event of utility failure.

Each Availability Zone maintains redundant connections to multiple tier-1 transit providers to guarantee unbroken network connectivity at all times.

The AWS data storage infrastructure, named S3, is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. To help provide durability, S3 Put and Copy operations synchronously store data across multiple facilities before returning Success. Once stored, S3 helps maintain the durability of objects by quickly detecting and repairing any lost redundancy. S3 also regularly verifies the integrity of data stored

using checksums. If corruption is detected, it is repaired using redundant data. In addition, S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

How do we detect, prevent and mitigation DDoS attacks?
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.

What is our Business Continuity Plan?
In the event that the Pingboard corporate office incurs a power outage, network outage, or disaster, we have arranged on-demand access alternate office space, sufficiently sized for our team to re-establish operations. In addition, we have created redundancy in our staff's knowledge and ability to respond to issues, by routinely rotate escalated customer support and incident response roles, with a clearly defined flow of responsibility if the primary staff is unavailable.

What is covered by our penetration tests?
We regularly engage with an independent, certified third party security firm to perform penetration testing on the Pingboard services. Testing attempts to identify extraneous services, known software vulnerabilities, and misconfigurations at the network and server levels. At the application level, testing includes input validation, authentication and authorization, and information disclosure.

What kind of background checks are performed prior to employment?
All new employees undergo pre-employment background checks, showing felonies, misdemeanors, sex offenses and more at the state and county level, plus results from terrorist watchlists. Employees also agree to company policies including security and confidentiality policies.

Do you have well defined and practiced incident response procedures?
Pingboard has defined threat response protocols. When an incident occurs, we follow these steps:

1. Move to a central chat room to ensure everyone is on the same page.
2. Designate a point person to lead the response effort.

3. Respond to customers and proactively reach out to customers as appropriate.
4. Assess the problem.
5. Mitigate the problem.
6. Coordinate response.
7. Manage ongoing response.
8. Post-incident cleanup.
9. Post-incident follow-up.

Forensic capabilities include analyzing user access logs, transaction logs, and working with our infrastructure providers to understand the extent and nature of an incident.

What notification and escalation processes exist in case of security incident? Is there a process to notify Customer about incidents that affect Customer's business or data?
All security issues and suspicious activity are escalated to our CTO. Pingboard shall notify customer without undue delay after becoming aware of a confirmed security incident, and provide reasonable information (to the extent that such information is known or available to Pingboard) and cooperation to customer so that customer can fulfill any data breach reporting obligations it may have. Pingboard shall take the steps as Pingboard deems necessary and reasonable in order to remedy or mitigate the effects of the security incident. The obligations herein shall not apply to incidents that are caused by customer or customer's users.

How often are the security policies and procedures reviewed?
Security policies and procedures are reviewed bi-annually.