BRAZE SECURITY, PRIVACY, AND ARCHITECTURE DATASHEET

(effective as of May 2023; subject to change without notice)

Introduction

The goal of this document is to provide high-level information to our customers regarding Braze's commitment to security and data protection.

Braze's Corporate Trust Commitment

Braze is committed to achieving and maintaining the trust of our customers. Our goal is to be as transparent as possible with our customers in offering state-of-the-art security and protections to meet and exceed expectations in today's modern computing world.

1. Policy Ownership

Braze has a documented information security policy that all employees must read and acknowledge. This policy is reviewed and updated annually. Security policy development, maintenance, and issuance is the responsibility of the Braze Security Team.

2. Braze Infrastructure

Braze customers may elect US or European hosting options.

For US-hosted customers, Braze hosts the Braze Services with Amazon Web Services in their US-East-1 region, Virginia, USA, with some S3 backup storage containers in the US-East-2 region, Ohio, USA and US-West-2 region, Oregon, USA. Some Braze Services may also be hosted on Microsoft Azure in their East US region.

For Europe-hosted customers, Braze hosts the Braze Services with Amazon Web Services in their EU-Central-1 region, Frankfurt area, Germany, with some S3 backup storage containers in EU-West-1 in Ireland.

Certain databases are managed by ObjectRocket, a Rackspace company, which provides database support services in either the US or Germany based on data center needs.

3. Third-Party Architecture

Braze may use one or more third-party content delivery networks to provide the Braze Services and to optimize content delivery via the Braze Services. Content items to be served to subscribers or end-users, such as images or attachments uploaded to the Braze Services, may be cached with such content delivery networks to expedite transmission.

Information transmitted across a content delivery network may be accessed by that content delivery network solely to enable these functions.

4. Audits, Certifications, and Regulatory Compliance

Braze is ISO 27001 certified and SOC 2 compliant. Braze also enters into the EU Standard Contractual Clauses with its Customers that require it, self-certifies to the EU-US and Swiss-US Privacy Shield Frameworks, and is HIPAA-compliant.

Security Controls

5. Organization Security

Braze's CTO is responsible for the overall security of the Braze Services, including oversight and accountability. Braze's contracts with third-party hosting providers such as Rackspace and Amazon Web Services include industry-standard information protection requirements.

6. Asset Classification and Logical Access Control

Braze maintains an inventory of essential information assets such as servers, databases, and information. All Customer Data is classified as Confidential by Braze.

Braze adopts the principle of least privilege for all accounts running application or database services, as well as with its own staff. For example, Customer Success Managers only have access to the regions for which they are directly responsible. Braze maintains separate development, staging (or sandbox), user acceptance testing, and production environments access to each environment and within each environment is strictly controlled.

Access to Braze's servers is controlled via revocable SSH keys managed via configuration management and rotated at least annually. All access to Braze's servers or Customer Data is logged and can only be accessed through Braze's VPN, which uses multi-factor authentication. Database access is controlled via 32 and 64-character passwords with IP whitelisting.

Braze's HR onboarding and off-boarding processes handle provisioning and de-provisioning of accounts and access.

7. Personnel Security and Training

All employees at Braze sign a non-disclosure agreement when their employment begins. In addition, Braze conducts background checks of its employees as part of its onboarding process. All employees are informed of, and agree to comply with, Braze's security policies and practices as a part of their initial onboarding. All Braze employees undergo annual security and privacy training.

System administrators, developers and other users with privileged access receive special and ongoing training and are subjected to additional background screening.

8. Physical and Environmental Security

Access to Braze facilities is controlled by 24-hour security. Additionally, all Braze offices are protected by locked access and are under 24-hour video surveillance. All Braze employee workstations are encrypted and password protected, and all Braze user accounts require two-factor authentication.

Data centers and servers are managed and controlled by our Cloud hosting providers, Rackspace, Microsoft, and Amazon Web Services. Braze employees have no access to any of these data centers.

Details regarding the security practices and controls applicable to these facilities can be found at their websites:

AWS: https://aws.amazon.com/security/

Rackspace: http://www.rackspace.com/security/

Microsoft: https://azure.microsoft.com/en-us/overview/security/

9. Policies and Logging

The Braze Services are operated in accordance with the following procedures to enhance security:

- User passwords are never transmitted or stored in clear text
- Braze uses industry-standard methods to determine password validity
- API key information for third-party services provided by the customer are encrypted for storage
- Braze keeps audit logs for all access to production servers
- Server access is controlled via public key access, instead of passwords, and only permitted while on VPN that requires multi-factor authentication
- Logs are stored in a secure centralized host to prevent tampering
- Braze application and ssh audit logs are stored for one year
- Passwords are not logged under any circumstances
- Access to Braze mail and document services is only allowed on approved mobile devices that have automated security policies enforced, such as encryption, autolock and passwords
- All access to customer dashboard accounts by Braze Employees must be done through an internal service that is accessible via a 3-factor VPN only
- As part of Braze's Employee Information Security Policy, employees may not store any Customer Data on removable media

10. Intrusion Detection

Braze leverages Crowdstrike, an Endpoint Detection & Response solution (EDR). This solution is designed to review and conduct signature, heuristic, and behavioral analysis, granting the ability to detect advanced threats to both on our cloud infrastructure and corporate network. Logs from this system are centrally collected for further analysis and threat detection.

Additionally, Braze may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the Braze Services function properly.

Braze's APIs and Dashboard use strict role-based access controls and user permissioning. Unauthorized web requests and API calls are logged and automatically alert Braze's engineering team.

11. Security Logs

All Braze systems used in the provision of the Braze Services, including firewalls, routers, network switches, and operating systems log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis. Braze has automated alerts and searches on these logs.

12. System Patching and Configuration Management

Braze patches its servers and rebuilds its entire cloud infrastructure from configuration management systems on a regular basis, which ensures that the latest patches are applied and that we "reset" back to a known, clean state. Braze's configuration management system regularly applies patches via Linux repositories. Braze uses the Chef configuration management tool and Kubernetes to automate this entire process, and our entire infrastructure.

Braze maintains multiple environments and tests changes in containerized development environments and in live staging environments before making changes to production environments.

13. Vulnerability Management

Braze's infrastructure and applications are continuously scanned by a Vulnerability Management System. Alerts are monitored by our Security Team and addressed at least monthly by the Braze Vulnerability Management Team. Braze also maintains a list membership to various CVE vulnerability mailing lists. Patches and 'critical' and 'high' vulnerabilities are remediated no later than 30 days following discovery.

Braze also uses static code analysis tools during the build process (such as Brakeman and bundler-audit) to perform static security analysis.

14. Third-Party Penetration Testing

Braze undergoes a third-party penetration test of the Braze Services on an annual basis.

15. Monitoring

For technical monitoring, maintenance and support processes, Braze uses a combination of tools to ensure that processes and servers are running properly, including but not limited to:

- Process monitoring
- CPU, disk, and memory monitoring
- Uptime monitoring
- Functional monitoring
- Database monitoring
- APM performance monitoring
- Error monitoring
- Office monitoring

16. Customer Access Control

The Braze Services employ a variety of security controls. These include, but are not limited to:

- API IP Whitelisting - Defines the range of IP addresses from which a customer's users can access the Braze API to prevent unauthorized third parties from accessing the Braze Services.
- Dashboard Account IP Whitelisting - Defines a range of IP addresses from which a customer's users can access the Braze Dashboard to prevent unauthorized parties from accessing the Braze Services.
- Single-sign on with a Google Account - Braze customers can access the Braze Services by means of a Google Account, which allows customers to configure such access to require two-factor authentication.
- Single-sign on via Okta - Braze customers can access the Braze Services via Okta, which allows customers to configure access via their Okta installation.
- Mobile Authenticator - Braze customers can enable two factor authentication via Authy which allows a mobile authenticator to be required for access to the Braze Dashboard.

- Customer-Configurable Roles and Permissions - Braze customers have the option to manage their users of the Braze Services through selective and granular permissioning described in our documentation at https://www.braze.com/docs/user_guide/administrative/manage_your_braze_users/user_permissions/.
- All requests on the Braze Dashboard have cross-site request forgery (CSRF) protection. All web services use encrypted HTTPS for all traffic and disallow all HTTP traffic via HTTP Strict Transport Security ("HSTS").
- Braze does not use cookies for session storage to avoid replay attacks. Sessions expire after a few hours of inactivity.
- User passwords on the Braze Dashboard must meet minimum password length requirements. At the customer's request, Braze can add password complexity requirements, such as lowercase, uppercase, numeral, and special characters, and set a password expiration policy such that users must change their passwords regularly.
- User password history of the last six passwords prevents the reuse of User passwords.
- Failed login attempts are recorded and an account is locked out with the owner notified after multiple failed attempts.
- Braze's REST APIs are accessed with separate API keys, which can only be provisioned by Braze dashboard user accounts with administrative access. API keys are granted access to specific API endpoints when created.

17. Development and Maintenance

Braze uses tools such as GitHub and Jenkins to effectively manage the development lifecycle. During testing, Braze generates sandbox accounts and fake data for testing. Braze does not use production data in sandbox accounts.

Application source control is accomplished through private GitHub repositories. Braze has controls in place to ensure that all code must be approved before being merged to Braze's main code branch; only the CTO and approved employees are granted access to promote code to production.

Braze developers receive additional security training as part of their onboarding, and undergo regular and periodic security training during the term of their employment. Braze maintains a list of core security principles for engineering and high-level guidelines on security topics for secure software development.

18. Malware Prevention

As a mitigating factor against malware, all Braze servers run LTS editions of Operation Systems, as well as the endpoint detection and response(EDR) service, Crowdstrike.

Braze adopts the principle of least privilege for all accounts running application or database services. Proper change management ensures that only authorized packages are installed via a package management system containing only trusted software, and that software is never installed manually.

All Braze employee computers have virus scanners installed and updated definitions sent out from a central device management platform.

19. Information Security Incident Management

Braze maintains written and regularly-audited security incident management policies and procedures, including an Incident Response Plan to be enacted in the event of an incident.

Braze has 24x7x365 on-call incident management staff. Braze uses tools such as PagerDuty to ensure complete coverage with defined escalation policies.

20. Data Encryption

The Braze Services use industry-accepted encryption practices to protect Customer Data and communications during transmissions between a customer's network and the Braze Services, including 256-bit TLS Certificates and 4096-bit RSA public keys at a minimum.

Braze audits the TLS ciphers used in connection with the provision of the Braze Services with third-party security auditors to ensure that anonymous or weak ciphers are not used. These audits also confirm that the Braze Services do not allow client renegotiation, support downgrade attack protection and forward secrecy.

Data shipped to Amazon Web Services is encrypted in transit and at-rest using AES-256 encryption via Amazon's managed encryption key process. Data shipped to Rackspace is encrypted in transit and at-rest using AES-256 encryption via Rackspace's managed encryption key process.

Where use of the Braze Services requires a customer to provide access to third party services (for example, AWS S3 credentials for data exports), Braze performs additional encryption of that information.

21. Return and Deletion of Customer Data

The Braze Services allow import, export, and deletion of Customer Data by authorized users at all times during the term of a customer's subscription. Following termination or expiration of the Braze Services, Braze shall securely overwrite or delete Customer Data within 60 days following any such termination in Braze's production instance, and in accordance with the Agreement, applicable laws and the Documentation.

22. Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Braze Services is stored on a primary database server with multiple active clusters for higher availability. All database servers replicate in near real-time and are backed up on a regular basis. Backups are encrypted using AES-256 encryption and verified for integrity.

23. Business Continuity Management and Disaster Recovery

Braze has a written Business Continuity and Disaster Recovery Plan, which is tested annually. Braze tests database backups and failovers as part of our Business Continuity Plan. Backups are encrypted and stored in Amazon Web Services- and Rackspace-provided backup services.

24. Mobile Device Management Policies

Braze uses Mobile Device Management ("MDM") platforms to control and secure access to Braze resources on mobile devices such as phones, tablets, and laptops. Braze uses Google for its phone and tablet MDM policy, and enforces common security settings such as, but not limited to, encryption, lock screen passwords, password expiration, display timeouts, and remote location and remote wipe. Braze uses JAMF for laptop and desktop management to enforce common security settings, including but not limited to, hard disk encryption, security patches, and remote location and remote wipe capabilities.

25. Blocking Third Party Access

The Braze Services have not been designed to include any backdoors or similar functionality that would allow the government or any third parties to access Customer Data. We do not voluntarily provide any government or other third party with encryption keys, or any other way to break our encryption.

26. Forensics

Braze uses the CrowdStrike EDR solution to investigate and respond to security incidents involving Braze user endpoints. The solution allows the Security Team to collect valuable forensic information from affected systems to better understand what occurred in the system and to take steps to contain and/or remediate the threat.

For forensic disk acquisition, Braze uses Cellebrite's Digital Collector tool to collect a forensically-sound bit-by-bit copy of a storage device from a compromised asset.

To analyze forensic disk images, Braze uses Cellebrite Inspector. This tool allows the Security Team to recover deleted or hidden data and establish a complete picture of activity that occurred on a compromised asset.

27. Contacts

Braze's Security Team can be reached by emailing security@braze.com.