Apteligent

WHITE PAPER

Security and Information Policies
Data and Security Policies for 2017

Apteligent is committed to the security of your mobile application's data. We use a variety of industry-standard security technologies and procedures to help protect your information from unauthorized access, use, or disclosure.

Overview

Apteligent's Mobile App Intelligence delivers real-time user experience insight based on behavioral and operational metrics so that enterprises can maximize revenue, improve engagement and increase retention. Apteligent operates a massively scalable platform that delivers intelligence across iOS, tvOS, Android, HTML5 and Hybrid apps and is used by more than 23,000 apps, in 120 countries, recording 4 billion events per minute.

This document is intended to provide a high-level overview of the Apteligent Security Program and Practices, as well as, an overview of the security features and functionality of the Apteligent service. It addresses the most common concerns customers may have about security and privacy, while outlining the security controls available within Apteligent.

Security at Apteligent

Apteligent is committed to the security of your mobile application's data. We use a variety of industry-standard security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. The Apteligent security program is responsible for Application Security, Compliance, Privacy, Corporate Security, and Physical Security.

All Apteligent employees are informed of their security responsibilities and receive annual security awareness training.

Product Overview

Apteligent's Agent (SDK) collects data from mobile applications, uploads that data to the Apteligent service, and presents Mobile App Intelligence data through a secure website or RESTful API.

The basic components of the service works as follows:

• Develop your mobile app.

• Install the Apteligent Agent (SDK) into your app, either as an embedded library pre-compilation, or via post-compile wrapping.

• The Apteligent Agent (SDK) sends Mobile App Intelligence data to the Apteligent service in real-time while your app is running on the end-user's device.

• The Apteligent service aggregates and stores the Mobile App Intelligence data in tier 3, SSAE 16 certified data centers.

• Visualizations of the Mobile App Intelligence data are available via Apteligent's SSL-encrypted and password-protected website, API, or iPad app.

Data Collected

The Apteligent Agent (SDK) captures Mobile App Intelligence data including Userflows, Crash Reporting and Service Monitoring information. By default, Apteligent does not collect any personal information (PII) from our customers' customers. Apteligent will see (but not store) end-user IP addresses; the IP address is immediately translated into a geographical region and then discarded. The Agent generates a random identifier (device ID) on the device to uniquely identify that user.

Data Captured by Default

• App Loads occur whenever a user launches the app on their device. When the user begins using an instrumented application, the library automatically records an app load event.

• Unhandled Exceptions (Crashes) are run-time exceptions that occur due to some unexpected event that terminates the user session, causing the mobile application to exit suddenly. When an unhandled exception (i.e., crash) occurs in the app, the Apteligent Agent will retrieve a stack trace that shows which line of code caused the crash along with diagnostic data about the app and device. This information allows the developer to recreate the conditions of the crash (i.e., specific app version, etc.).

Optional Configurations

• Handled Exceptions (Optional) are anticipated, run-time errors that developers can log from a try / catch block in their code. Handled exceptions do not necessarily cause the app to crash. The same data that is collected for crashes is also collected for handled exceptions; that is a stack trace of the code being executed and diagnostic data about the app and device.

• Metadata (Optional) allows a company to set custom data about a user to be sent along with an Unhandled Exception (Crash) or Handled Exception. For example, this would allow companies to search for crashes by a username or see how many items were in a shopping cart.

• Rate My App (Optional) presents a dialogue box to the app user requesting information regarding the app. If you have enabled the Rate App Alert in your App Settings, the Apteligent library will receive and handle settings for Rate My App alerts as specified in the server. In order to enable Rate My App alerts and have them behave according to the server settings, two steps are required:

- Find out if a Rate My App alert dialog should be shown.
- Create the alert dialog and show it.

• Service Monitoring (Optional) occurs when the mobile application accesses an external service (network call). Each service monitoring message includes metadata about the device as well as HTTP performance data. Data is sent on a periodic basis with the frequency determined by the Apteligent server. Currently the default frequency is 10 seconds, and data is only sent to Apteligent when the app has performed a network request in the last 10 seconds. This feature can be disabled by calling a special method in the Apteligent Agent. If the feature is not explicitly disabled, the default behavior is to send service monitoring data to our server.

• Userflows (Optional) are arbitrary series of steps, which lead to a business outcome. Userflows can be defined by the app owner (developer) and assigned a name. The Apteligent service will capture the number of times that a particular userflow was started and track the result of the userflow. A userflow can either succeed or fail. If a userflow fails due to a crash then crash information will be reported along with the userflow.

Privacy & Confidentiality

Diagnostic data we collect is primarily used to display application performance information back to the account user. It is also used by Apteligent personnel to answer questions that our customers may have about their account, as well as, to develop and improve our products. We may also aggregate application data across multiple accounts and use this data to create and publish industry benchmarks or comparative application performance metrics. Individual transaction data collected by Apteligent is obfuscated by default. Except as otherwise stated in our privacy policy, we do not sell, trade, share, or rent the personal data collected from our services to third parties. You expressly consent to the “sharing of your personal data” as described in this policy. We do not use the data for marketing or sales purposes. Apteligent has received TRUSTe’s Privacy Seal signifying that our practices have been reviewed for compliance with the TRUSTe program. Additionally Apteligent is compliant with COPPA - Children’s Online Privacy Protection Act.

Any questions or concerns regarding the use or disclosure of your information should be directed to Apteligent by sending an email to privacy@apteligent.com.

More information on our privacy policies is available at: http://www.apteligent.com/privacy-policy/

EU and Swiss Considerations

Apteligent's data center in the U.S. is tier 3, SSAE 16 certified. By default, Apteligent does not collect any personal information from our customers' customers. Apteligent complies with the U.S. – E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. Apteligent has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. For select customers on the Enterprise tier, Apteligent offers the option to enter into EU Standard Contractual Clauses.

To learn more about the Safe Harbor program, please visit: http://www.export.gov/safeharbor/.

Apteligent Encrypts Data in Transit

All data transmission, including application load, crash, and metadata from the Apteligent Agent, is secured via 128-bit SSL encryption using a 2048-bit RSA encryption key. Client applications using the Apteligent SDK must be allowed TCP access to port 443 in order to send data. The Agent validates the SSL certificate on the server and only sends data if the certificate is signed by Apteligent and is from a trusted CA. Conversely, the server validates the Agent via the unique device ID.

Data Centers

Apteligent is hosted on Amazon Web Services in multiple geographic locations. 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 with extensive setback and military grade perimeter control berms, as well as other natural boundary protections. 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. (http://aws.amazon.com/articles/1697, retrieved 8-July-2013)

Certifications

AWS data centers are certified as:

1. Tier 3, SSAE 16.

2. PCI DSS Level 1. AWS has been independently validated to comply with the PCI Data Security Standard as a shared host service provider.

3. ISO 27001. AWS has achieved ISO 27001 certification of the Information Security Management System (ISMS) covering infrastructure, data centers, and services.

4. FISMA. AWS enables government agency customers to achieve and sustain compliance with the Federal Information Security Management Act.

Security Policy

Physical Security of our Workplace

Access to our facility entries is controlled via security personnel. Specific office entries also require an electronic access card. Employees wear badges or have identification cards. Our operation staff performs a monthly review of unauthorized access attempts into the facility/office. Unauthorized attempts are communicated to the building security personnel.

Network Configuration

All administrative traffic is encrypted. There are separate, firewalled areas for Internet DMZ, production databases, back office, and software development areas. Intrusion detection and prevention systems are in place at the perimeter and critical server systems. Intrusion sensors are monitored real-time, 24x7, for highimpact alerts and periodic review of other alerts. All remote communications occur over an encrypted tunnel (i.e., IPSec, SSL-VPN).

Incident and Change Management

There is a formal incident management process that includes IT security breaches (viruses, hacking, etc.) which is current and reviewed annually. There is a formal process to track and notify customers of loss or theft of systems with customer data. Our incident management process includes a step to contact affected customers in the event of a data breach. On a case-by-case basis, we are able to provide customers with necessary visibility and access to any data relating to information security investigations, which may include, but is not limited to, systems, data, and logs related to the incident.

Monitoring

Apteligent utilizes its own internal monitoring as well as the monitoring tools provided by AWS. Apteligent utilizes tools to monitor uptime, network latency, server responsiveness, workload size, and many additional metrics to assess the performance and secure state of its infrastructure. Apteligent's systems are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics.

Configuration Management

All Apteligent software and hardware configurations are logged in its revision control system. New machines are allocated using chef, which allows Apteligent to (1) easily scale (2) apply OS configuration changes across its cluster and (3) easily update new software when patches are released.

Backups & Storage

Customer data is stored redundantly in an on-line fashion. Each database shard contains a primary and a secondary server in an active-active configuration. Each secondary server contains a complete replica of the primary server. Data is stored on the primary and secondary servers as RAID 10 arrays to protect against individual disk failure.

Network Security

The AWS network provides significant protection against traditional network security issues. The following are a few examples of attacks in which protections are put in place: Distributed Denial Of Service (DDoS) Attacks, Man In the Middle (MITM) Attacks, IP Spoofing, Port Scanning, Packet sniffing by other tenants, and ARP cache poisoning. In addition, every server instance on AWS is protected by a firewall that, by default, blocks all ports. Apteligent only opens select ports needed to communicate between machines, and heavily restricts which machines can communicate with each other.

System Event Logging

Security event logging / auditing is enabled on all systems, and all devices have their clocks synchronized with a master time source via NTP. The audit log provides accountability by providing a trace of user actions and staff are immediately alerted to key security events. The audit trail supports after-the-fact investigations of how, when, and why events occurred, and on-line storage of audit logs are retained for a period of time. Access to audit logs is strictly controlled. All logs are consolidated on a dedicated log management system (which may be a distributed system). Access to the audit logs is strictly controlled with write/alter access only granted to relevant system tasks or copies of logs stored in a secure log repository system. There is separation of duties between personnel who administer the access control function and those who administer the audit logs such that access control administrators are unable to access/amend/delete the audit logs.

Application Security

Authorization

Access to the Apteligent web portal is secured via username and password authentication. Passwords are encrypted with an AES-256 hash and a random salt. In addition, Apteligent offers role-based security access to data at the app level. Organizational administrators have the ability to grant and revoke access to data segmented by business or engineering functionality. All data transmission on the Apteligent web portal is securely sent over HTTPS to ensure data is securely sent between two verified parties.

Secure Application Development

Apteligent software engineers are trained in the OWASP Top 10 (www.owasp.org) and abide by those best practices. Security requirements are defined as part of business requirements with security checkpoints performed at key stages of projects & development. We undertake code reviews to identify and mitigate application security vulnerabilities (application and presentation tier) and have in place manual checks to ensure secure coding practices are followed. We use separate environments for development, testing, and production systems. Software developers are restricted from accessing the production environment (unless their duties explicitly require them to have access). Access to software in development is restricted on a "need to have/ need to know" basis. We have processes in place to detect unauthorized changes to software in development.

User Management

Passwords must contain: Both UPPER and lowercase letters; at least one number; at least one symbol (e.g., !@#$%^&). Passwords must be between 8 and 64 characters in length, CAN NOT be reused, and must be changed at least every 180 days. Passwords are stored as one-way hash, using a randomly generated salt unique to each record. Users are locked out and forced to reset their password after 10 failed attempts..

Customers are responsible for managing their own accounts, including provisioning and de-provisioning their own users.

Compliance

Apteligent can be installed in a PCI-compliant environment. By default, Apteligent does not receive any cardholder data. In addition, the Apteligent Agent can be configured to run behind a proxy to satisfy the PCI requirement to not allow any direct connections between the Internet and the cardholder data environment.

Apteligent can be safely deployed in a healthcare environment without impacting HIPAA compliance obligations. By default, Apteligent will not receive any protected health information.

About Apteligent

Apteligent is the App Intelligence company trusted by the largest mobile apps in the world. Apteligent's software provides actionable mobile app insights to improve digital business on iOS, Android, and Hybrid apps. Product managers and developers use Apteligent's insights to diagnose app performances issues that impact user experience. The platform collects and analyzes app performance issues and connects problems to key business metrics. Mobile teams also have access to Apteligent's big data platform, as well as industry and app benchmarks. Apteligent is based in San Francisco.

Learn more at www.apteligent.com.