mixpanel

ANNEX 1 to Standard Contractual Clauses

MIXPANEL ARCHITECTURE & SECURITY OVERVIEW

mixpanel

EXECUTIVE SUMMARY

Mixpanel provides a robust data collection and analytics platform with high availability and dependability, which allows companies to track user behavior across platforms. Ensuring the confidentiality, availability, and integrity of our customer's analytics data is of the utmost importance to Mixpanel.

Mixpanel's security program is built with industry-standard security practices. We couple strong policies with automated tools and security controls to protect our customers and maintain a high level of trust and confidence.

This document provides an overview of the Mixpanel Security Program and Practices, including Data Collection, Physical Security, Employee Security Awareness, Incident Response, as well as an overview of the security features and functionality of the Mixpanel product. It also dives into the Application and Network architecture of the system.

PRODUCT OVERVIEW

Mixpanel collects behavioral analytics data from websites, mobile applications and other Internet connected devices. Our customers have the ability to configure their products to send the data they desire directly to Mixpanel's proprietary data store for instant analysis.

Mixpanel is fully HTTPS capable for all data transmission. Furthermore, once your data is stored in Mixpanel, that raw data is only accessible via API using private and secret key authentication.

Mixpanel uses Google Cloud Platform, an industry leader in security and availability, for data storage and processing. All data stored in Mixpanel is encrypted at rest, and logically separated from any other client's data. The data is stored redundantly in production and is also backed up at a geographically separate location.

DATA FLOW OVERVIEW

Data being sent to Mixpanel originates from a variety of sources on web or mobile

applications including:

- JavaScript on a website
- Library within an iOS or Android application
- Server-side libraries on customer's infrastructure
- RESTful API calls

A developer programmatically defines which actions and corresponding details of those actions they wish to track with Mixpanel. Mixpanel only tracks those actions that have been programmatically defined in the source code.

When a user visits a website or application with Mixpanel instrumented, the details of their interactions are captured and sent to Mixpanel through API calls over HTTPS/HTTP. All data transferred over HTTPS is encrypted. Furthermore, all data is encrypted at rest.

Customers access Mixpanel data through our web interface, which supports two-factor authentication and single sign-on integration, or through a number of APIs that are authenticated through key/secret credential combinations.

In general, Mixpanel access does not record an audit trail to the individual user level. See the Compliance section on page 12 for more information on this topic.

DATA PROCESSED

Mixpanel processes data only from the websites or applications where Mixpanel's library or SDK has been installed by a customer, or from other Internet connected devices that initiate requests to Mixpanel's REST API. The data that Mixpanel processes has been programmatically defined by the customer, within the application source code.

While Mixpanel relies upon third parties, such as MaxMind (maxmind.com), the industry leader in Internet protocol (IP) address intelligence, for databases of information that can help analyze data, we do not send customer data to them. IP addresses are not stored by Mixpanel unless the customer specifically enables it in the course of their data collection through our services. Customers who implement our JavaScript libraries install cookies on their site/application by default. However, cookies are not required, as Mixpanel offers a server-side integration as an alternative option.

All tracking cookies and data processing activities are logically isolated between

customers. There is no way to correlate between users of two different customers, even if they are the same person.

EXAMPLES OF PROCESSED DATA

The following are common examples of user behavior data that customers use Mixpanel to track:

- Button Clicks
- Website searches
- Product purchases
- Photo shares
- Video plays
- Game plays
- Post likes

EXAMPLES OF PROHIBITED DATA

It is important to note that certain sensitive information should never be sent to Mixpanel. Sending the following pieces of sensitive information will violate Mixpanel's Terms of Use:

- Credit Card Information including credit card numbers
- Social Security Numbers
- Driver License Numbers
- Passport Numbers
- Government Issued Identification Numbers
- Financial Account Information
- PII collected from children under the age of 13

mixpanel

PRIVACY & CONFIDENTIALITY

Mixpanel is committed to protecting the privacy of our customers and the confidentiality of their data. Information is processed and stored primarily to provide, maintain, protect, and improve current products and to develop new ones. In addition to the customer data that is processed, Mixpanel also collects data from visitors to the mixpanel.com website. Mixpanel uses personal information collected through the website to:

- Improve services provided
- Understand and enhance customer experience
- Provide and deliver products and services you request
- Respond to comments or questions and for Solutions team to provide service
- Send relevant information, including confirmations, invoices, technical notices, updates, security alerts and support and administrative messages
- Communicate promotions, upcoming events and news about products and services offered
- Link or combine with other information from third parties, to help understand needs and provide better service
- Protect, investigate and deter against fraudulent, unauthorized or illegal activity

Mixpanel takes reasonable steps to help protect your personal information in an effort to prevent loss, misuse, and unauthorized access, disclosure, alteration and destruction.

More information on how we use the data collected via our website is available on our public privacy policy.

DATA CENTER SECURITY & LOCATION

Mixpanel servers that persistently store customer data are hosted by Google Cloud Platform. Data is stored and processed in GCP's "us-central1" zone in Council Bluffs, IA. GCP's data center is SOC 1, SOC 2 and SOC 3 compliant. Additionally, Google logically isolates each customer's Cloud Platform data from that of other customers and users.

GLOBAL DISTRIBUTION

Mixpanel has been architected to receive data from many regions around the globe. Data is collected from users' devices and customers' servers via our REST API endpoints.

Mixpanel maintains endpoint clusters and uses dynamic DNS to route requests to the endpoint that is geographically closest to the client. These endpoints queue the incoming data and perform initial validation and sorting.

DATA CENTER FEATURES

ALL GCP DATA CENTER FACILITIES INCLUDE

- Strict access security:
  - custom-designed electronic access cards
  - alarms
  - vehicle access barriers
  - perimeter fencing
  - metal detectors
  - biometrics
  - data center floor features laser beam intrusion detection.
- Monitoring:
  - 24/7 high-resolution interior and exterior cameras that can detect and track intruders
  - access logs
  - activity records
  - camera footage is available in case of incident
- Personnel:
  - patrolled by experienced security guards
  - rigorous background checks and training
- Power availability:
  - redundant power systems
  - environmental controls
  - diesel engine backup generators - enough emergency electrical power to run at full capacity
  - cooling systems
  - fire detection and suppression equipment

FOR INFORMATION ON GCP SECURITY AND COMPLIANCE, REFERENCE THE FOLLOWING LINKS:

- Security Whitepaper
- Compliance and Certifications

- Cloud Security FAQ

DATA PROTECTION

All data sent over HTTPS to and from Mixpanel uses 256-bit encryption in transit. Data flows from the API clusters to the production data stores via GCP's backbone network infrastructure. Data is encrypted at rest, and it is stored in a proprietary analytics database format (i.e. not an off-the-shelf database). This database infrastructure was designed for high-speed queries with security in mind. Additionally, Google logically isolates Mixpanel's Cloud Platform data from that of other customers and users

Each Mixpanel project is logically separated from all other projects, so although the data is stored on shared hardware, the database architecture prevents data in one project from leaking into other projects.

APPLICATION SECURITY

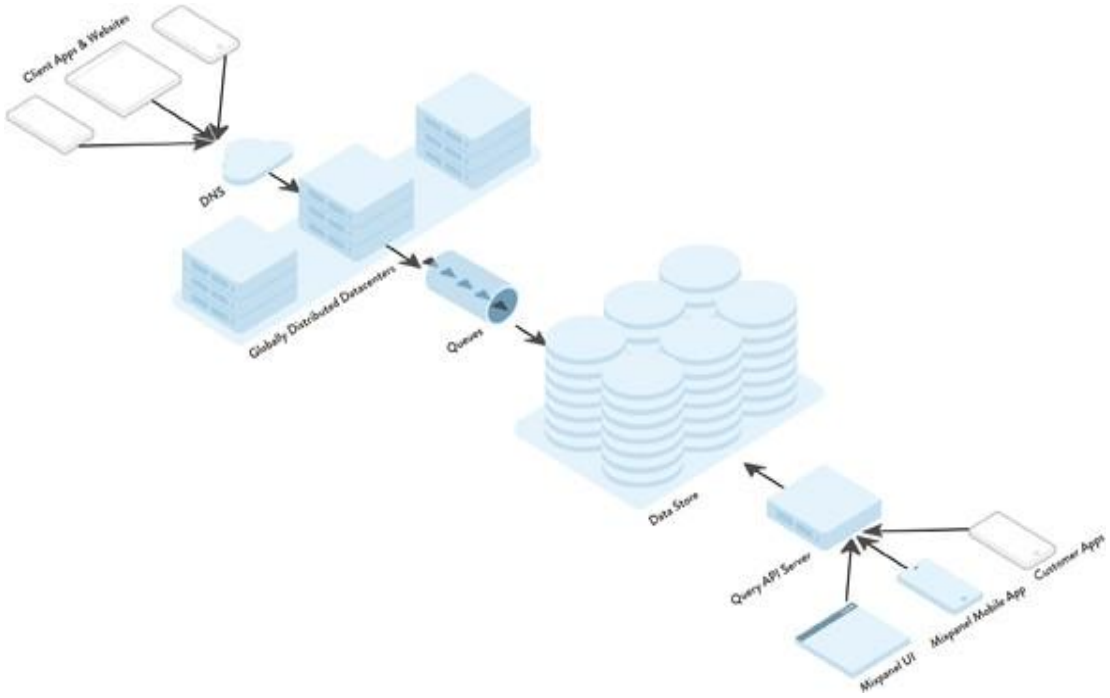
Mixpanel maintains a robust and comprehensive application security program. Security is an integral part of our entire development process:

- At design time, through security design reviews and threat modeling.
- At implementation time, with comprehensive security development training, secure code review guidelines,
- and static analysis tools to identify vulnerable code.
- At deployment time, with strict manual and automated code review requirements and automated deployment processes.
- In operation, with ongoing automated vulnerability scans, and monitoring controls to identify denial-of-service attacks.

Application monitoring controls are in place to identify denial- of-service attacks. Additionally, an independent 3rd party performs application-level penetration tests annually.

mixpanel

APPLICATION ARCHITECTURE



SECURITY POLICY

Mixpanel maintains compliance with the most demanding, security conscious enterprises. Security Policies that cover the following topics are maintained and updated annually:

- Employee Security Awareness Training
- Information Resource Management
- Information Classification
- Information Security Compliance
- Access Controls
- Technical Security
- Encryption
- Firewall Security
- Administrative Safeguards
- Vendor Security
- Security Monitoring
- Information Access
- Secure Workspace
- Physical Security

AUDITS

Mixpanel undergoes annual security assessments by an independent, third party security firm. These assessments ensure that Mixpanel is performing all of the necessary measures to protect production systems and ensure the integrity of our customer's data.

SECURITY CONFIGURATION

CONFIGURATION AND CHANGE CONTROL MANAGEMENT

Security risk analysis is conducted when implementing new components in production or development environments. Every change to application code is thoroughly reviewed for functional and security issues. A standard base image is used for all new systems, which are deployed by GCP. Machines are then customized to fit their role. These procedures are documented and have been audited.

DMZ

Following industry standard best practices, Mixpanel implements a "De-Militarized Zone" (DMZ). The DMZ is used to limit inbound and outbound traffic only to protocols that are necessary for the secure data environment. Firewalls have been implemented at each Internet connection and between the DMZ and internal network zone.

VULNERABILITY SCANS & AUDITS

We run automated network vulnerability scans on an ongoing basis. Third-party penetration tests are performed annually. Penetration tests include testing against the network perimeter from the Internet. High-risk vulnerabilities are resolved within 90 days of discovery.

UPDATES & ANTI-VIRUS SOFTWARE

Mixpanel uses Linux for all production systems. Our strategy to protect our Linux servers is to focus on making our production systems immutable and frequently recycle them. This prevents malware from gaining a persistent foothold, and ensures that there is a minimal window in which malware could stay memory-resident. Whenever a new vulnerability is discovered, software is updated within a month.

MONITORING

Mixpanel employs an in-house Security Information and Event Management platform, which provides 24x7x365 monitoring and alerting for security incidents in our networks and systems. Our SIEM collects information from our corporate infrastructure, from our cloud hosting provider, and from our production services, providing a comprehensive view of security-related activities at Mixpanel.

Google, our cloud hosting provider, adds further layers of monitoring, inspecting internal traffic at many points across their global network for suspicious behavior, such as the presence of traffic that might indicate botnet connections. Their network analysis is supplemented by automated analysis of system and network logs to identify unusual behavior, such as attempted access of customer data.

ACCESS CONTROL MEASURES

Access is granted to production servers only as required and is provisioned on an as-needed basis.

INCIDENT RESPONSE

The Mixpanel Incident Response Team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Any and all suspected or confirmed Data Security Incidents must be immediately reported to the Data Protection Officer. The DPO will engage the Incident Response Team and coordinate with management and the Legal Department to determine appropriate actions that will be taken in accordance with this policy to meet Mixpanel's legal obligations and to prevent or mitigate impact to consumers, employees or Mixpanel resulting from a Data Security Incident.

Roles and responsibilities of all individuals on the Incident Response Team are well documented in Mixpanel's Data Security Incident Response Plan.

BUSINESS CONTINUITY & DISASTER RECOVERY

Mixpanel maintains a Disaster Recovery (DR) plan for our service. This plan is updated regularly and has been tested. All data in the production environment will be frequently snapshotted and stored durably in multiple geographic locations in the US. Backups are maintained for the duration of the customer relationship and for one year after the termination of an agreement unless otherwise specified or required by law.

COMPLIANCE

Mixpanel can be implemented and used in such a manner that will maintain compliance with various regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Mixpanel operates as a Business Associate so that our healthcare customers can use the Mixpanel services in compliance with applicable laws. By default, Mixpanel does not receive any protected health information (PHI) or personally identifiable information (PII) data. Mixpanel can be safely deployed in a healthcare environment without impacting HIPAA compliance obligations provided that only the Mixpanel website is used to access data as Mixpanel does not currently have an auditable log for API access users.

EU Considerations:

Mixpanel has a considerable presence in Europe and works with customers that employ some of the strictest security requirements.

Mixpanel participates in and has certified its compliance with the EU-U.S. and Swiss - U.S. Privacy Shield Frameworks. Mixpanel is committed to subjecting all personal information received from European Union (EU) member countries, in reliance on the Privacy Shield Frameworks, to the Framework's applicable Principles. To learn more about the Privacy

Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List at https://www.privacyshield.gov/list.

Mixpanel is responsible for the processing of personal information it receives, under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Mixpanel complies with the Privacy Shield Principles for all onward transfers of personal information from the EU, including the onward transfer liability provisions.

With respect to personal information received or transferred pursuant to the Privacy Shield Framework, Mixpanel is subject to the regulatory enforcement powers of the U.S.

Federal Trade Commission. In certain situations, Mixpanel may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In addition to the Privacy Shield Frameworks, Mixpanel is developing the policies, procedures, and enhanced security measures required by the EU General Data Protection Regulation ("GDPR"), which comes into force on May 25, 2018. Mixpanel is committed to its compliance with the GDPR or any replacement regulation and the protection of its customer's data.

NOTICES

This document is provided for informational purposes only. It represents Mixpanel's current product offerings as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Mixpanel's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from Mixpanel, its affiliates, suppliers or licensors. The responsibilities and liabilities of Mixpanel to its customers are controlled by Mixpanel agreements, and this document is not part of, nor does it modify, any agreement between Mixpanel and its customers.

For these reasons and more, 20 thousand companies around the world trust Mixpanel with their data. Mixpanel is committed to investing in our platform to allow companies to leverage our services in a secure and transparent manner. For more information please contact compliance@mixpanel.com.