Table of contents

Introduction

Design considerations
Data feeds
Data workflows
Data storage

Data security & privacy controls
Organizational security
Data security controls
Data privacy controls
Compliance audits

Data protection culture

Conclusion
Introduction

As an analytics platform, Mode operates in a contentious space when it comes to data security and privacy. Services and platforms that utilize or enable analytics are consistently under scrutiny when it comes to meeting security and privacy obligations, particularly under the emerging laws such as GDPR and CCPA.

How does Mode, an analytics company, maintain a platform that protects customer data from risks while also providing business value? The answer lies in our three-pronged approach to security:

- Designing and building a solid architectural foundation for security and privacy from day one.
- Implementing a combination of security, privacy and compliance controls that address data protection risks through the entire data lifecycle.
- Promoting a company culture that encourages each and every member of our team to uphold our commitment to protect customer data.

This paper details Mode’s approach to security, including the processes, certifications, and protocols that help our customers meet their data protection and compliance requirements and keep our platform secure.
Design considerations

Privacy and security were built into the foundation of Mode’s architecture from the very beginning, as seen in a few specific product areas.

Data feeds

At Mode, we know the importance of sanitizing data feeds in order to handle sensitive customer data appropriately. We ensure that this data is kept out of databases that are not designed specifically for that purpose. We do that by excluding tables and columns with any reasonable expectation of containing sensitive data from the database. This includes certain queries, notebook cells, and report descriptions among others. There is a dedicated script that sanitizes the data feed that goes into the analytics databases, which ensures that applications that are not designed to analyze sensitive personal data won’t have access to it.

Data workflows

Identifying where personal data exists in the data processing pipeline helps businesses avoid accidentally violating associated data privacy obligations when processing or analyzing that data. At Mode, we split the data processing pipeline into projects that include sensitive customer data, and those that do not. Doing so allows us to maintain different levels of scrutiny, depending on the sensitivity of the data processing pipeline. For example, we allow certain third party scripts that collect data from user browsers to run across our marketing pages, but they would not be allowed to run on pages in our application that process sensitive customer data.

Data storage

At Mode, we take a conservative approach when handling sensitive data. We believe that it is acceptable to add friction to the process in order to prioritize protection of customer data. We introduce that friction by isolating sensitive data and limiting access to it based on need. We do this by separating the storage of customer query results from the metadata behind those queries. Because the sensitive information is found in the results of the query, and typically not in the query itself, storing the results separately allows us to isolate the repository to which we needed to apply the most restrictive policies. These policies include requiring encryption at rest, minimum necessary access based on need, & applying data retention rules.
Data security & privacy controls

Mode’s industry-leading security program is based on the concept of defense in depth: securing our organization, and your data, at every layer: retrieval, storage, access, and sharing.

We track the data that we collect, process and store, as well as maintain adequate and reasonable controls to protect it. Our security program also includes the obligations that we must accept or enforce to honor our commitments to protect our customer’s data. By focusing on the purpose of keeping the data, we have identified controls that reduce data protection risks for us and consequently for our customers. We undergo annual compliance audits which serve as an independent attestation of the effectiveness of our data protection controls.

Organizational security

Mode’s security team is responsible for the implementation and management of our security program. The members of Mode’s Security Team focus on the following areas: product security, security engineering and operations, and data protection compliance.

Data security controls

The focus of Mode’s data security controls is preventing unauthorized access to customer data. Our team of dedicated security practitioners, working in partnership with peers across the company, identify and mitigate risks and implement best practices.
Secure SDLC

Starting with the development of our application, we have implemented a secure software development life cycle that includes scanning and remediating security issues early in the design phase, before they make their way into our product. Our web development follows industry-standard secure coding guidelines, such as those recommended by OWASP, and we regularly install security updates and patches on its servers.

Encryption: Data in transit

All data transmitted between Mode and our clients is done so using strong encryption protocols. Mode supports the latest recommended secure cipher suites to encrypt all traffic in transit, including use of TLS 1.2 protocols, AES256 encryption, and SHA2 signatures, whenever supported by the clients.

Any attempt to connect over HTTP is redirected to HTTPS. We also use HSTS to ensure browsers interact with Mode only over HTTPS.

Encryption: Data at rest

Data at rest in Mode’s production network is encrypted using industry standard AES 256. All encryption keys are stored in a secure server on a segregated network with very limited access. Additionally, Mode has implemented safeguards to protect the creation, storage, retrieval, and destruction of secrets, such as encryption keys and service account credentials.

Mode's servers are hosted in the SOC-2 Type II certified AWS data centers in the US. It offers state-of-the-art physical protection for the servers and infrastructure that comprise the Mode operating environment. See Amazon compliance and security docs for more detailed information.

Each Mode customer’s data is hosted in our shared infrastructure and logically separated from other customers’ data.
Network security and server hardening

Mode logically segments its systems into separate networks to better protect sensitive data. Modern, restrictive firewalls protect all connections between networks.

Systems supporting testing and development activities are hosted in a separate network from systems supporting Mode’s production infrastructure. All servers within our production fleet are hardened according to industry standard CIS benchmarks.

Network access to Mode’s production environment from open, public networks (the Internet) is restricted, with only the load balancers accessible from the Internet.

Mode logs, monitors, and audits all system calls and has alerting in place for system calls that indicate a potential intrusion or exfiltration attempt.

Endpoint security

All workstations issued to Mode personnel are configured by Mode to comply with our standards for security. These standards require all workstations to be properly configured, updated, tracked and monitored by Mode’s endpoint management solutions.

Mode’s default configuration sets up workstations to encrypt data at rest, have strong passwords, and lock when idle. Workstations run up-to-date monitoring software to report potential malware.
Access control

To minimize the risk of data exposure, Mode adheres to the principles of least privilege and role-based permissions when provisioning access—workers are only authorized to access data that they reasonably must handle in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly.

To further reduce the risk of unauthorized access to data, Mode employs multi-factor authentication for access to internal systems. In addition, VPN and SSH is required for accessing our production environment.

Mode requires personnel to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

System monitoring, logging, and alerting

Mode monitors servers and workstations to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in Mode’s production network are logged and monitored. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel.

Disaster recovery and business continuity plan

Mode utilizes services deployed by its hosting provider to distribute production operations across separate physical locations (or availability zones). These distributed zones protect Mode’s service from loss of connectivity, power infrastructure, and other common location-specific failures.

Mode performs daily backups and replication for its core databases across these zones and supports restore capability to protect the availability of Mode’s service in the event of a site disaster affecting any of these locations. Full backups are saved at least once per day and transactions are saved continuously. Mode tests backup and restore annually to ensure successful disaster recovery.
Responding to security incidents

Mode has established policies and procedures for responding to potential security incidents. All security incidents are managed by Mode’s dedicated Incident Response Team. The policies and procedures define the types of events that must be managed via the incident response process and classify them based on severity.

In the event of an incident, affected customers will be informed via email from our customer success team. Incident response procedures are tested and updated at least annually.

Penetration testing

In addition to our compliance audits, Mode engages independent entities to conduct application-level and infrastructure-level penetration tests at least twice per year. Results of these tests are shared with senior management and are triaged, prioritized, and remediated in a timely manner. Customers may receive executive summaries of these activities by requesting them from their success team representative.

Research and disclosure

Mode Analytics is committed to working with security experts across the world to stay up to date with the latest security techniques. To show our appreciation for our security researchers, we offer a monetary bounty for certain qualifying security bugs. If you believe you have discovered a problem or have any questions, please contact us at security@modeanalytics.com.
Data privacy controls

Mode’s data privacy controls are designed to honor our obligations around how we collect, process, use and share personal data, as well as our processes to support data retention and disclosure in compliance with legitimate business purposes.

Data processing and sharing

Mode adheres to obligations under laws such as GDPR and CCPA related to processing and sharing customer data.

We acknowledge and abide by the principle to only collect, process, and store customer data after fully recognizing the obligations attached to it. This includes our obligations to protect this data and provide you with the right to access or delete it at any time.

We provide controls for deleting customer data when it is no longer needed for a legitimate business purpose and also providing users the option to opt-out of tracking cookies on our website.

We also provide controls to make sure that any vendors agree to the use of customer data only for the purpose of provision of services.

Data retention and disposal

Customer data deletion may be performed or requested by the end user at any time during the subscription period. The data is removed by default after a period of inactivity post termination of subscription period.

Mode relies on its hosting providers for ensuring removal of data from storage media. They are certified for maintaining industry standard security practices, including performing data deletion in a responsible manner before the media is repurposed.
Vendor management

Mode relies on sub-processors to run its services efficiently. We recognize that our critical sub-processors may impact the security of Mode's production environment, and we take appropriate steps to ensure our security posture is maintained by establishing agreements that require sub-processors to adhere to confidentiality commitments we have made to users.

Mode monitors the effective operation of the critical sub-processing organization's safeguards by conducting reviews of their controls before use and at least annually. The list of our critical sub-processors is maintained on our website.

Compliance audits

Our security program is aligned with ISO 27000, AICPA Trust Service Principles, and NIST standards, and is constantly evolving with updated guidance and new industry best practices.

Mode is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and Mode's security and compliance team. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner.
Data protection culture

Mode has built a company culture that educates and holds every team member accountable to fulfilling their obligations to protect privacy and security of customer data. Mode’s company-wide security awareness program is focused not just on a point-in-time training but a process that comprises continuous learning. In addition to formal training, we communicate about security on an ongoing basis in the form of security tips, newsletter, and posters that reiterate important security messages.

Data protection culture at Mode reflects a level of encouragement that embraces everyone making prudent decisions to keep our platform secure. Users are trained on how to avoid phishing scams in order to prevent account credentials from being compromised. Engineers are trained on secure coding practices to help prevent security vulnerabilities in our software. Leadership communicates with the security team on important risk decisions related to our product and our vendors.

A key element of the program is recognition for employees who demonstrate a security mindset in order to promote security culture within the organization in an organic manner. This keeps the employees motivated to adopt best security practices.

Conclusion

Mode is built on a strong foundation for security that helps protect our customers from emerging data protection risks. Our approach to security puts us in a position to meet data protection and compliance requirements while keeping our platform secure. If you have questions or concerns at any time, please contact your Customer Success Manager.