Security at Mapline

At Mapline, we believe that your data can tell you what you need to know to make the best business decisions. As such, we work extremely hard to protect your data and maintain your trust. In this page, we will outline general information regarding the security measures we have in place to keep your data safe.

Security of Data Centers

The security of the Data Center's infrastructure is designed in progressive layers starting from the physical security, continuing on to the security of the hardware and software that underlie the infrastructure, and finally the technical constraints and processes in place to support operational security.

- Only authorized personnel can enter the Data Centers. To protect against intruders, Data Centers are monitored by high-resolution interior and exterior cameras.
- The Data Centers we use are layered with custom-designed electronic access cards, alarms, perimeter fencing, metal detectors, and biometrics. The Data Centers floors feature laser beam intrusion detection.
- Our Shielded Virtual Machines are hardened by a set of security controls that help defend against rootkits and bootkits. They also help protect from threats like remote attacks, privilege escalation, and malicious insiders.
- We leverage advanced platform security capabilities such as secure and measured boot, a virtual trusted platform module (vTPM), UEFI firmware, and integrity monitoring.
- We use multiple servers, placed in world-class data centers around the United States. We have various zones and regions where our servers are located.
- Data stored on our servers has several layers of encryption at rest. This protects against unauthorized access and service interruptions.
- All communications to our servers are encrypted in transit. This means we verify the data at the source and destination, and we make your data

unintelligible while in transit to keep it private.

- Our network and infrastructure have multiple layers of protection to defend against denial-of-service (DoS) attacks.
- We have a documented infrastructure continuity plan in case any unexpected disruptions occur.
- While we are confident in these security measures, we also have operations teams to detect and respond to any threats both internal and external to our security infrastructure.

Protection from Data Loss

- We strive to avoid any data loss by regularly backing up all data.
- Account data is automatically backed up to a different region.
- We have multiple layers of logic that segregate user accounts from each other.
- We employ extensive logging and monitoring of network, system and application events.

Security Engineering Practices

- Mapline maintains a comprehensive set of information security Policies and Procedures that are approved by Senior Management and are reviewed and updated regularly to remain compliant with the law and current industry practices.
- Mapline's Engineering team ensures that security is a key component of the entire development process.
- In tandem with Senior Management, our engineers ensure security during our design reviews, test cycles, bug triage, releases, and all other development initiatives.
- All security issues are thoroughly researched, resolved, and then re-tested to ensure they are properly remediated.

Internal HR & IT Security

- All employees undergo extensive background checks prior to employment.

- We continuously train employees on best security practices, including how to identify social engineering, phishing scams, and hackers.
- Our offices are secured by keycard access.
- In order to protect our company from a variety of losses, Mapline has established a comprehensive insurance program. Coverage includes, but is not exclusive to:
    - Coverage for cyber incidents
    - Data privacy incidents (including regulatory expenses)
    - General error and omission liability coverage
    - Excess cyber liability coverage
    - Property and business interruption coverage

Security within our Application

- All login pages (from our website and mobile website) pass data via TLS.
- The entire Mapline application is encrypted with TLS.
- All data, including database backups, is encrypted at rest.
- Mapline account passwords are salted hashed. Our own staff can't even view them. If you lose your password, it can't be retrieved—it must be reset.
- Our application is also equipped to protect against rootkits.
- When necessary, Mapline will use reasonable means to communicate the risk of any security vulnerability and share any preventive measures that may be applicable.

Customer Managed Security Features

We provide account-level controls to help you protect your information. Mapline enables account level security features that allows you to always be in control.

- We make 2-Factor Authentication available to our customers.
- We also provide SSO capabilities.
- Certain changes to your account, such as to your password, will trigger an email notification.
- We provide the ability to determine user types for licenses on your account.

This allows you to establish tiered-levels of access for users.

- We enable you to determine what you share inside and outside of your account.

Payment Security

Mapline's credit card processing vendor has been audited by a PCI-certified auditor and is certified to PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry. To accomplish this, they make use of best-in-class security tools and practices to maintain a high level of security.

Mapline’s Continued Commitment to Security

We understand that new security tactics and threats are created every day. We review all security concerns brought to our attention, and we take a proactive approach to emerging security issues.

We understand that peace of mind that your data is protected is extremely important to you. If you ever have any concern about the security measures we have in place, please feel free to reach out to our team and we will be happy to walk through this information with you.

If you believe your account has been compromised or you are seeing suspicious activity on your account please visit https://mapline.com/contact-us/ to report it.

We are happy to have you in the Mapline team and look forward to continually unleashing the power of your data with maximum security.