Security at Mapline

Date: October 28, 2024

Mapline, as a leading Software-as-a-Service (SaaS) Geo Mapping, Geo Analytics, and Geo Operations platform, has been providing business solutions since 2010 and helps organizations leverage the power of location in their data. From analyzing your business performance with maps and dashboards to creating route optimizations, highly customized scheduling, and automated workflow operations, Mapline enables you in ways no other platform can!

Mapline offers accessibility, cost-efficiency, continuous updates and enhancements, and expert support. By leveraging cloud-based technology, users can access the product via a web browser, eliminating the need for complex installations and facilitating seamless scalability.

Mapline values and respects the security and privacy of its clients. We understand the crucial importance of maintaining the confidentiality, integrity, and availability of your data. We have implemented numerous security controls, policies, and practices to protect your data at all times. This document details the various security measures in place.

1. Infrastructure Security

We prioritize the protection of our infrastructure, which is the backbone of our service delivery. Several steps have been taken to provide security.

a. **Data Centers**: Our data is hosted on cloud data centers located exclusively within the United States, adhering to data jurisdiction and regulation compliance. These data centers are **ISO 22301:2019** certified, enhancing business continuity through the robust design and deployment of these centers. The data centers follow rigorous physical security controls, including 24/7 security surveillance, stringent personnel access controls, environmental disaster protection, fire detection and suppression systems, and uninterrupted power supply systems. This robust security infrastructure safeguards your data against potential threats.

b. **System Hardening**: All components of our solution, including servers, databases, network devices, and applications, are hardened as per industry standards. This involves configuring these components in a way that reduces the attack surface by eliminating potential vulnerabilities, unnecessary functions, and configurations.

c. **Security Patches**: Regular patching is part of our maintenance routine to address known vulnerabilities and continually enhance the security of our infrastructure.

The process of system hardening establishes the robustness of our infrastructure, further strengthening our security posture.

2. Application Security

Our application is certified at Level-2 by the App Defence Alliance (ADA) under the Cloud Application Security Assessment (CASA) framework.

CASA has built upon the industry-recognized standards of the OWASP's Application Security Verification Standard (ASVS) to provide a consistent set of requirements to harden security for any application.

Achieving Level-2 CASA certification strengthens our security posture and aligns our practices with industry standards in application security.

3. Data Encryption

We employ comprehensive encryption measures to protect the confidentiality and integrity of your data.

a. **Transport Layer Security (TLS)**: All data in transit is initially encrypted using TLS 1.2. If a client doesn't support TLS 1.2, we step down to TLS 1.1, and if a client doesn’t support TLS 1.1 then to TLS 1.0. However, nothing older than TLS 1.0 is allowed.

b. **Disk-Level Encryption (Encryption at Rest)**: All our hard drives are encrypted for the security of data at the hardware level. This includes temporary storage devices used by our applications and servers.

c. **Database Level Encryption**: Sensitive data within our databases, such as password and financial information, is encrypted. This targeted approach to database encryption allows us to provide strong protection for sensitive data without compromising system performance.

d. **Database Backup Encryption**: All database backups are encrypted both in transit and at rest. This means that not just your live data, but also your backup data is secure from unauthorized access.

e. **Encryption Standards**: All our encryption methods, including symmetric encryption (AES256), LDWM(SHA-256), RSA (2048) and ECDSA(P-256) are FIPS 140-2 compliant.

These encryption protocols and methods collectively demonstrate the privacy, security, and integrity of your data both in transit and at rest.

4. Multi - Tenancy Architecture

We employ a multi-tenancy architecture, providing efficient use of resources while isolating data through logical separation. This means that while resources are shared, each tenant's data is isolated from others for the confidentiality and privacy of your data.

5. Access Control

We implement stringent access control measures to protect against unauthorized access to our systems and your data.

5.1. Employee Access

a. **Principle of Least Privilege (PoLP)**: We adhere to the Principle of Least Privilege (PoLP), meaning individuals are given the minimum levels of access necessary to complete their job functions. This reduces the risk of accidental or deliberate misuse of data.

b. **Access Revocation**: When an individual no longer requires access, either due to a change in duties or termination of employment, access rights are promptly revoked. This reduces the risk of unauthorized access or data breaches.

c. **VPN Requirement**: A Virtual Private Network (VPN) is required for internal network access, meaning that employees are securely connecting to our systems from remote locations.

5.2. Client User Access

a. **Secure Authentication**: We leverage SSL with TLS and for secure authentication, including support for two-factor authentication (2FA), to verify the identity of users before granting access. This protects against unauthorized access due to compromised credentials.

b. **Password Policies**: Strict password policies are enforced to ensure the complexity and uniqueness of passwords. All passwords are stored in a non-reversible encrypted format. This means that even in the event of a data breach, user passwords cannot be deciphered.

c. **Single Sign-On (SSO)**: We support Single Sign-On (SSO) capabilities using OAuth 2.0 and SAML protocols. For SSO-enabled accounts, this reduces the risk of password-related security incidents while providing a seamless experience for our users.

d. **Data Access**: Users only have access to the data on their own account and are restricted from viewing or editing data belonging to other accounts unless that data has been explicitly shared.

5.3. 3rd-Party Access

At times Mapline may need to share data with a third party in order to provide the services to you. For example, we may share the address information with a third party in order to verify the placement of pins on a map. Any information shared with third parties or contractors is based on access permissions. The access is governed by strict access control policies and legal agreements so that your data remains secure. Mapline's Terms of Service can provide additional details and can be found at https://mapline.com/terms-of-service/

These access control measures collectively limit data access to authorized individuals and such access is strictly regulated and monitored.

6. Network Security

To protect your data, we have implemented robust network security measures.

a. **Demilitarized Zone (DMZ)**: We utilize a Demilitarized Zone (DMZ) to create an additional layer of security. This network segment acts as a secure bridge between our internal network and the internet to help protect our system from unauthorized access.

b. **Zero-Trust Network**: With our zero-trust network model, every request is verified, authenticated, and encrypted, regardless of its origin. This model negates the concept of "trust" within our network and requires constant verification, enhancing the overall security posture.

c. **DDoS Protection**: Distributed Denial of Service (DDoS) attacks can disrupt service availability. Our robust DDoS protection mechanisms help to prevent these attacks so that our service remains uninterrupted. We utilize advanced rate-limiting controls, CAPTCHA implementations, and distributed networking infrastructures to safeguard against brute force and DDoS attacks.

d. **Web Application Firewall (WAF)**: We employ an advanced WAF to protect against web-based threats. The WAF monitors, filters, and blocks malicious HTTP/S traffic targeting our applications, effectively mitigating threats such as SQL injection, Cross-Site Scripting (XSS), and more.

e. **Secure Internal Data Transfers**: All data transfers within our internal network are secured. This protects the confidentiality and integrity of your data as it moves within our systems.

f. **SSL/TLS Encryption**: All data in transit is encrypted using the SSL protocol with TLS. This not only provides secure communication between client and server but also contributes significantly to our network security by preventing unauthorized access to data during transmission.

g. **Virtual Private Network (VPN)**: A VPN is required for all remote access to our internal network so that all communication between our network and remote users is secure, encrypted, and private. Additionally, the use of VPN further protects against potential breaches or unauthorized access.

h. **Phishing Mitigation**: To combat phishing attacks, we employ Domain-based Message Authentication, Reporting, and Conformance (DMARC) to prevent attackers from spoofing our domain. This ensures that our legitimate emails are delivered to recipients, while protecting our reputation. Additionally, our employees are trained to identify and handle spoof emails, adding a human layer of defense. Together, these measures strengthen our overall security and contribute to the broader effort of reducing phishing success rates.

7. DevOps and Software Development Security

We adhere to secure coding practices in our development process, guided by the principles of DevSecOps. This allows us to incorporate security measures at each stage of software development.

a. **Secure Code Practices**: All our developers are trained in secure coding practices. The code written is regularly checked for any potential security vulnerabilities, including those in the **OWASP Top 10** list of most critical web application security risks.

b. **Static Code Analysis**: We utilize static code analysis tools to rigorously analyze our codebase. This approach helps identify and rectify any potential security flaws before the software gets deployed.

c. **Vulnerability Assessment and Management**: We regularly perform comprehensive vulnerability scans on our systems including penetration testing. These scans and tests simulate real-world attacks, aiming to identify potential vulnerabilities and areas for improvement in our security posture. All findings are promptly addressed and retested to further the robustness of our security measures.

d. **Risk Assessment**: Our risk assessment procedures identify, evaluate, and prioritize potential security risks. This enables us to proactively implement effective controls and measures to minimize these risks.

e. **Privileged Access Management**: We strictly control access to sensitive parts of our system. Privileges are granted based on job function requirements, following the Principle of Least Privilege (PoLP).

f. **Environment Isolation**: We maintain separate environments for development, testing, and production. This isolation prevents untested or unsecured code from making its way into the production environment. Each environment has its own set of access controls, further reducing the possibility of unauthorized changes or data breaches.

g. **Codebase Security**: Our repositories, where we maintain our version-controlled source code, are secured with access controls. Only authorized personnel with valid credentials can access and modify the codebase.

h. **Build Server Access**: Access to our build servers is strictly limited. Build server, being a critical component of our CI/CD pipeline, can only be accessed by a select group of authorized team members.

i. **Limited Access to Deployment**: Deployment privileges are granted sparingly and only to those team members who require them. This practice reduces the risk of accidental or malicious alterations to our live environments.
file

By employing these stringent DevOps and software development security measures, we are able to enhance the robustness and integrity of our software, thus providing you with a secure and reliable platform.

8. Threat Management and Protection

Our platform incorporates advanced systems and strategies to protect against a diverse array of cybersecurity threats.

a. **Malware Protection**: We have implemented anti-virus solutions on all our servers. This includes real-time scanning for malware, viruses, and other malicious software. Regular updates are performed so that our systems are protected against the latest known threats.

b. **Ransomware Protection**: We employ sophisticated systems to detect and counter ransomware threats. Regular data backups and stringent access controls further enable us to quickly restore data in the event of an attack.

c. **Protection Against Targeted Attacks and Data Breaches**: Our advanced threat detection systems, along with strict access controls, provide a robust defense against targeted attacks and potential data breaches.

d. **Defense Against Fileless Attacks and Advanced Persistent Threats**: We utilize the latest security technologies and threat intelligence to protect against fileless attacks and Advanced Persistent Threats (APTs).

e. **Host-based Intrusion Prevention System** (HIPS): Our HIPS actively monitors and analyzes system activities for signs of any malicious behavior. Any suspicious activity triggers the HIPS, which then takes action to block potential attacks and report the incident.

f. **Network Attack Defense**: We have deployed robust network security measures, including firewalls and intrusion detection/prevention systems (**IDS**), to defend against network attacks.

g. **Brute Force and DDoS Attack Mitigation**: We utilize advanced rate-limiting controls, CAPTCHA implementations, and distributed networking infrastructures to safeguard against brute force and DDoS attacks.

h. **Botnet Defense**: We implement measures to detect and mitigate the risks posed by botnets, including network monitoring tools and firewalls, to prevent unauthorized access and stop potential Distributed Denial-of-Service (DDoS) attacks.

i. **UEFI Firmware Protection**: Our systems are safeguarded from threats to the UEFI (Unified Extensible Firmware Interface) firmware through secure boot processes, regular firmware updates, and hardware-level protections.

By adopting these defense mechanisms, we proactively reduce threats to security and enhance the integrity of our platform to protect your data.

9. Business Continuity and Disaster Recovery

Our business continuity and disaster recovery plans are designed to sustain the availability of our platform and preserve your data. We leverage the advanced capabilities of our cloud infrastructure provider to provide high reliability and resilience.

a. **Redundant Systems**: Utilizing the extensive resources available in the cloud, we have redundant systems deployed across multiple geographic service regions. This helps our services remain available, even in the event of a regional disruption, without any significant impact on performance or reliability.

b. **Data Backups**: We perform regular encrypted backups of all your data. These backups are securely stored in geographically separate locations to safeguard against localized incidents.

c. **Recovery Strategy**: In the unlikely event of a disaster, our well-tested recovery strategy enables our platform and your data to be quickly restored with minimal disruption to your operations.

d. **Scalability:** We closely monitor usage on a daily basis and adjust server resources accordingly. This approach enables us to scale our systems efficiently to meet the varying workload demands regardless of the load intensity.

e. **Remote Access Policy**: In the event of office outages or disruptions, we have a remote access policy in place for our employees and contractors. This allows authorized personnel to securely access necessary systems and continue operations, mitigating impact on our services.

We understand the critical importance of business continuity for our clients and have implemented rigorous measures so that our services are available when you need them.

10. System Monitoring and Reporting

To provide optimal performance and quick issue resolution, we employ real-time system monitoring:

a. **Real-Time Monitoring**: We use extensive monitoring tools to constantly track the health and performance of our systems. This allows us to detect any anomalies or issues in real-time, enabling swift mitigation to provide system reliability.

b. **Alerting and Issue Resolution**: In case of any detected anomalies or issues, the monitoring system immediately alerts our dedicated response team. This team is tasked with quickly resolving these issues, minimizing any potential impact on our services.

c. **Performance Reporting**: We maintain a comprehensive performance reporting system. These reports are regularly reviewed to identify any trends or potential areas of improvement to continually optimize our services.

Through these proactive monitoring and reporting practices, we are able to provide high availability and performance of our services, giving you a reliable and effective platform.

11. Incident Response and Management

Our robust Security Incident Response Plan is critical to our overall security strategy. We are prepared to respond swiftly and effectively to any security incidents.

a. **Incident Response Plan Applicability**: Our Security Incident Response Plan is followed by all personnel, including all employees, temporary staff, consultants, contractors, suppliers, and third parties operating on our behalf.

b. **Incident Detection and Reporting**: Our advanced monitoring systems are designed to detect potential security incidents in real-time. Additionally, we have a clear procedure in place for staff to report any perceived security incidents, encouraging a proactive culture of security awareness.

c. **Incident Analysis and Response**: Upon detection or reporting of a security incident, our dedicated incident response team is responsible for conducting a thorough analysis of the incident and determining the appropriate response measures.

d. **Incident Resolution and Recovery**: Our team works tirelessly to mitigate the impact of security incidents, resolve them promptly, and restore normal operations as quickly as possible.

e. **Post-Incident Review**: After the resolution of an incident, a post-incident review is conducted to identify the root cause, evaluate the effectiveness of the response, and determine any necessary improvements to prevent similar incidents in the future.

Through these comprehensive incident response and management procedures, we are prepared to protect our platform and your data in the event of a security incident.

12. Human Resource Security

At Mapline, we understand that our team is at the core of our operations, and as such, we have stringent procedures in place for the integrity and reliability of our personnel.

a. **Hiring Procedures**: Our hiring procedures include comprehensive background checks for all potential new employees. This enables us to verify the credentials and integrity of all individuals before they join our team.
data class

b. **Role-Based Access**: Once hired, the access levels for each employee or contractor are strictly determined based on the requirements of their role. This principle of least privilege means that each staff member only has access to the information necessary to perform their duties.

c. **Employee Termination**: Upon termination or change of employment, we have procedures in place to promptly revoke access rights to our systems and data. This process is vital to maintaining the security of our information.

13. Employee Training and Awareness

We recognize that our staff is our first line of defense against potential security threats. Therefore, we place a high priority on comprehensive employee training and continuous awareness programs:

a. **Security Awareness Training**: All our employees undergo regular security awareness training. This training includes recognizing and avoiding potential threats, understanding their roles and responsibilities in protecting our systems and your data, and the consequences of security policy violations.

b. **Policy Training**: Employees are also trained on key policies, such as our Incident Response Plan, Application Security Policy, Acceptable Use Policy, and Data Classification Policy. This training helps our team understand the procedures and protocols in place for different security-related scenarios.

c. **Data Classification and Handling**: Staff is educated on how to appropriately classify data, including identifying and handling sensitive customer information. This training covers the different levels of data sensitivity and the associated handling requirements.

d. **Continued Education**: Security training is not a one-time activity. Our training programs are updated regularly to keep pace with evolving threats, and employees are required to participate in these ongoing education initiatives.

By investing in employee training and promoting a culture of security awareness, we further protect our platform and your data from potential threats.

14. Vendor Management

In our global economy, Mapline contracts with all vendors to uphold the same levels of privacy and security as what we deliver. Our fully-owned subsidiary in India, which provides coding services, adheres to the same stringent security controls as our operations in the United States. All vendors, including our subsidiary, are subject to regular security reviews and audits.

15. Privacy

At Mapline, we understand the importance of protecting personal information. Our strict practices can be reviewed in our Privacy Notice found at https://mapline.com/privacy-notice. Regular audits are performed for the ongoing compliance with regulations and internal policies.

At Mapline, we prioritize the security and privacy of your data. We continually assess our security measures against the latest threats and adapt as needed for the continued safety and privacy of our customers' information. We believe that transparency is key to maintaining trust, and we welcome any further questions regarding our security practices.