Trackops Security Overview

Last Revised 05/03/2017

Network & Physical Security

The Trackops network is entirely hosted on the Amazon Web Services (AWS) cloud. Amazon is a leading cloud service provider, and is trusted by enterprises around the world for their outstanding reputation for security and stability. Visit the AWS Cloud Compliance website for the latest compliance and certification information.

Information about Amazon SOC 1, SOC 2, and SOC 3 reports are available via the Amazon SOC Compliance website. End users must request copies of SOC 1 and/or SOC 2 reports, as they are only released under a strict NDA.

AWS servers are housed in multiple nondescript SAS70 Type II data centers, located within the continental United States. Critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. 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. Data center access and information is only available 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. All physical and electronic access to data centers is logged and audited routinely.

All Trackops systems operate in multiple US-based physical availability zones, which ensures that systems remain online even if an entire physical data center is incapacitated. In addition, all Trackops AWS servers are preemptively patched on a daily basis to ensure the latest security patches are in production as quickly as possible.

Web Application Firewall

Trackops utilizes the Incapsula Web Application Firewall (WAF) to scan all incoming traffic for potential threats in real time. This Level 1 PCI-certified WAF ensures that Trackops is always protected against any type of application layer hacking attempt (e.g. SQL injection, cross site scripting, illegal resource access, and other top 10 OWASP threats). In addition, incoming traffic is also scanned for bad bots (e.g. vulnerability scanners), and backdoor access attempts.

DDoS Protection

Trackops utilizes Imperva/Incapsula DDoS protection, to mitigate denial of services attacks in real time. These include network-based attacks (e.g., Slowloris, ICMP or TCP & UDP floods) as well as application layer attacks (e.g., GET flood) that attempt to overwhelm server resources. Supporting Unicast and Anycast technologies, the service leverages a many-to-many defense methodology, automatically detecting and mitigating advanced DDoS attacks that exploit application and Web server vulnerabilities, hit-and-run DDoS events, and large botnets.

Vulnerability Scanning

Trackops utilizes Amazon Inspector to conduct routine vulnerability scans against our internal network for open exploits, misconfigurations, outdated packages, and other security vulnerabilities. This powerful appliance tests our systems against the Common Vulnerability Scoring System (CVSS), which includes thousands vulnerability signatures.

Network & Application Penetration Testing

Trackops retains Redspin as its third party partner for both network level and application level penetration testing. Redspin is routinely tasked to test and probe both network devices and the Trackops case management system to discover weaknesses and vulnerabilities in our security. RedSpin employs professional and experienced penetration testers that use both automated and manual testing techniques. Penetration tests are conducted annually, or whenever significant changes are made on network infrastructure or application code. Letters of attestation are available upon request.

SSL/TLS Encryption

All web traffic in and out of the Trackops network is encrypted using high grade 256-bit SSL (TLS) encryption. Non-SSL traffic is not permitted under any circumstance. In addition, outgoing email transmissions sent from Trackops are encrypted using TLS, ensuring that outgoing email content cannot be compromised.

For security, we do not accept SSL connections using SSLv2 or SSLv3 protocols.

Application Security

Trackops utilizes a number of security mechanisms to ensure that customer data is safe from unauthorized access:

- User accounts are protected by a username and strong password (with rules enforced).
- Minimum password length is configurable to control password entropy.
- Customers can configure mandatory password rotation intervals, ensuring that employees and clients change their passwords over time.
- Brute force attacks are mitigated through the use of challenge questions, and automated account locking after multiple invalid login attempts.
- Trackops also offers Multi-Factor Authentication (MFA), which provides enhanced security by requiring a personal authentication device (e.g. smartphone) in addition to your standard username and password to access the system. This additional security measure ensures that unauthorized users cannot login to your account without access to your phone, even if they have obtained your username and password.
- Once authenticated, user access is scoped through the use of User Roles (i.e. User Access Lists), ensuring that users only have access to the data they require. System administrators have the ability to configure permissions or remove a user's access instantaneously.

Database Security & Backups

Trackops utilizes Amazon RDS for all primary and redundant database storage. All databases operate in multiple availability zones for maximum uptime and complete redundancy. Data is fully encrypted at rest with industry standard AES-256 bit encryption. Encryption keys are managed via the Amazon Key Management Service (KMS), and are rotated annually.
Database backups can recover data up the minute, and fully encrypted database snapshots are taken on a daily basis.

File Storage & Backups

All files stored on our network are backed up to the minute using the Amazon S3 cloud storage service. Customer data is redundantly stored multiple times in multiple physical locations to ensure the highest level of data integrity. In the unlikely event of a complete hardware failure or uncontrollable natural disaster, you can be rest assured knowing that your data is safe.

Customer files and backups are securely encrypted at rest using high-grade AES-256 bit encryption.