SuperDispatch

Security Overview

Super Dispatch is committed to delivering a secure and reliable all-in-one platform for streamlining and automating the entire logistic process in the auto transport industry. We prioritize safeguarding the confidentiality of our customers' data and ensuring its availability whenever required. To achieve this, we leverage reliable and well-established security tools, technologies, and practices that have demonstrated their effectiveness.

Standards & Certifications

Super Dispatch has completed a SOC 2 Type II audit, conducted by an independent evaluator accredited by the American Institute of CPAs (AICPA). This assessment is based on the AICPA's Trust Services Criteria, which measures the effectiveness of an organization's controls in areas such as security, availability, processing integrity, privacy, and confidentiality. The audit is performed on a yearly basis. Audit report is available to current and prospective customers under NDA.

Internal Security Operations

INFRASTRUCTURE SECURITY

Super Dispatch primarily operates on **Google Cloud Platform (GCP)** for enabling operations for both Super Dispatch and third-party services, as well as for storing customers' data and files. Additionally, Super Dispatch leverages **Amazon Web Services (AWS)'s** S3 service for the temporary storage of customer-related content. GCP and AWS data centers do not allow Super Dispatch employees physical access, and logical access to the cloud facilities is granted only to authorized employees with permissions relevant to the employee's role. Both cloud providers maintain stringent security standards for their data centers and hold multiple

certifications for their services: GCP, AWS. Super Dispatch adheres to cloud security and architecture best practices to ensure reliability and compliance for its operations across both GCP and AWS.

PHYSICAL SECURITY

Physical security aligns with the best practices outlined in the company's internal Physical Security Policy. Key measures include restricting access to workplace facilities, permitting entry only to authorized personnel, and strictly enforcing workstation security protocols. All assets are stored and managed in designated facilities with protection levels appropriate to their sensitivity, criticality, and associated information. Access is promptly revoked upon the termination of workforce members to maintain the integrity of physical security measures.

NETWORK SECURITY

All Super Dispatch platforms are accessible over HTTPS, ensuring all traffic is encrypted and protected from unauthorized interception. Super Dispatch follows the latest security practices, employing strong encryption algorithms.

Super Dispatch operates a multi-tier architecture that separates internal application systems from public internet access. Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees. Additionally, all major network activity is logged and monitored in a centralized, secure system.

AUTHENTICATION, ACCESS CONTROL & AUDIT

Super Dispatch provides robust tools to effectively manage, control, and monitor user activities across its platform. Key features include a comprehensive Role-Based Access Control (RBAC) system, support for separate development, testing, and production environments, detailed user activity audit logs, and centralized oversight for managing multiple workspaces. All users are required to be identified and authenticated before accessing any system resources. System security software ensures resource protection by verifying user identities, authenticating access requests, and validating them against authorized roles defined in access control lists.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Employees and authorized vendor personnel access cloud resources through Single Sign-On (SSO) using Super Dispatch's IdP. For systems or applications that do not support SSO, users must log in separately using passwords that comply with the company's security policies. Token-based (OTP) multi-factor authentication is mandatory for employees accessing cloud resources, as supported by each service provider. All cloud services are accessed exclusively through SSL-secured connections.

A dedicated manager determines the required access permissions for new employees in advance of their start date, following pre-established role-based access rules. These access rules are reviewed annually by the company's operations team to ensure they remain appropriate and secure. Additionally, the dedicated security team evaluates access granted to privileged roles during this review process and implements modifications as needed to maintain robust security controls.

APPLICATION DEVELOPMENT

Super Dispatch follows a thorough and well-documented software development lifecycle that prioritizes security and privacy at every stage. This process includes design and code reviews, checking code quality and potential security issues by using Static Application Security Testing (SAST), secret scanning, and conducting unit and integration testing.

Super Dispatch utilizes GitHub to host its source code repositories. To ensure resilience and continuity, daily backups of these repositories are stored securely within Super Dispatch's Google Cloud Platform (GCP) account. In the unlikely event of a catastrophic data loss at GitHub, the source code can be fully restored from the GCP backups, ensuring minimal disruption to operations.

PENETRATION TESTING & VULNERABILITY ASSESSMENT

Super Dispatch conducts annual application penetration testing along with infrastructure vulnerability audit through a certified third-party provider. Additionally, regular internal and external vulnerability scans are performed to maintain robust security standards.

All findings from testing and scanning are thoroughly analyzed, and vulnerabilities are prioritized and addressed based on their risk level and severity.

DATA PRIVACY & PROTECTION

Super Dispatch maintains a public privacy policy that outlines the personal information collected, how it is managed, and the privacy rights of its customers. Super Dispatch undergoes an annual SOC 2 Type II audit, which includes the Privacy Trust Principle.

All data on the Super Dispatch platform is encrypted both at rest and in transit, ensuring robust security. Stored data is encrypted at rest using the AES-256 encryption standard.

AVAILABILITY

Super Dispatch strives to deliver high availability and minimize service disruptions. This is achieved through measures such as running services in redundant clusters, utilizing multiple redundant cloud availability zones, and continuously replicating the application database to a standby system for failover support. Real-time system status and recent uptime metrics are accessible at https://status.superdispatch.com/

Super Dispatch securely stores customer data in production accounts within GCP and AWS, utilizing Google Cloud SQL, Google Cloud Storage, Amazon Redshift, and Amazon S3 databases. Both Google Cloud Storage and Amazon S3 provide highly durable infrastructure, designed to ensure 99.999999999% durability of stored objects.

To safeguard against catastrophic loss, Super Dispatch performs automated daily backups of all customer and system data. These backups are stored in a separate U.S. region to provide additional resilience. Backups are encrypted using the same robust encryption methods applied to live production data. Backup operations are continuously monitored using Google Cloud Monitoring, and any failures automatically trigger an incident alert to the DevSecOps team for immediate investigation.

In addition, Super Dispatch employs point-in-time recovery for its production systems, leveraging write-ahead log archiving. This enables the restoration of data to a specific moment, accurate to fractions of a second, ensuring precise recovery in the event of data loss or corruption.

INCIDENT RESPONSE & DISASTER RECOVERY

Super Dispatch has established a detailed Security Incident Response Plan which outlines roles, responsibilities, and procedures to follow in the event of an actual or suspected security incident, ensuring a swift and effective response.

A core goal of Super Dispatch's Information Security Program is to identify and address security vulnerabilities to prevent incidents and breaches whenever possible. Super

Dispatch is committed to protecting its employees, contractors, customers, and partners from harmful actions, intentional or otherwise. While incidents may still occur, the company prioritizes rapid response, including identification, containment, investigation, resolution, and communication.

The company employs automated tools to detect and report potential vulnerabilities, which must be addressed within defined timeframes based on severity. Confirmed incidents are investigated promptly, and breaches are managed following established procedures to ensure containment, resolution, and communication with relevant stakeholders.

VENDORS RISK MANAGEMENT

Super Dispatch ensures all third-party organizations, including customers, partners, subcontractors, and developers, comply with its security policies to maintain the integrity, security, and privacy of its data and systems. Third parties are prohibited from accessing Super Dispatch's information assets until they sign a contract that includes security controls. All vendors must comply with security policies outlined in the Information Security Program, including the Acceptable Use Policy. Information sharing is limited to contracted vendors with signed agreements or NDAs. Vendors must disclose subcontractors and their locations. Super Dispatch reviews the attestation reports and performs a risk assessment on all critical vendors on an annual basis.

PEOPLE & SECURITY OPERATIONS

Super Dispatch conducts background checks for employees, contractors, and advisors following applicable laws and business needs. All personnel must agree to employment terms, comply with acceptable use policies, and complete onboarding to familiarize themselves with systems, security, and procedures. Regular security awareness training is mandatory and audited.

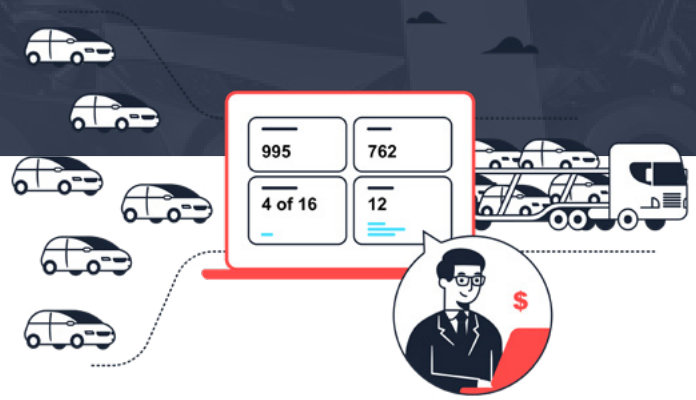
Offboarding ensures the return of company assets, removal of system access, and reinforcement of post-termination responsibilities. Measures are in place to prevent unauthorized sharing of corporate data via email or social media. A list of prohibited activities is provided during onboarding, with training offered for updates.

Super Dispatch: The Smarter Way to Move Cars

Brokers can now track and manage everything in one place to move cars faster and more efficiently.

Request a Demo Today

Contact Sales: +1 (816) 974-7002



About Super Dispatch

Company Overview

Super Dispatch is the end-to-end shipping platform backed by a digital suite of tools built to make the lives of auto transport industry professionals easier. Connecting shippers, brokers, and carriers with innovative software enables them to move cars faster while managing and growing their businesses. SuperPay is the all-new payment feature that streamlines the payment process and allows shippers to pay carriers in as little as one business day. Super Dispatch is headquartered in Kansas City, Missouri.