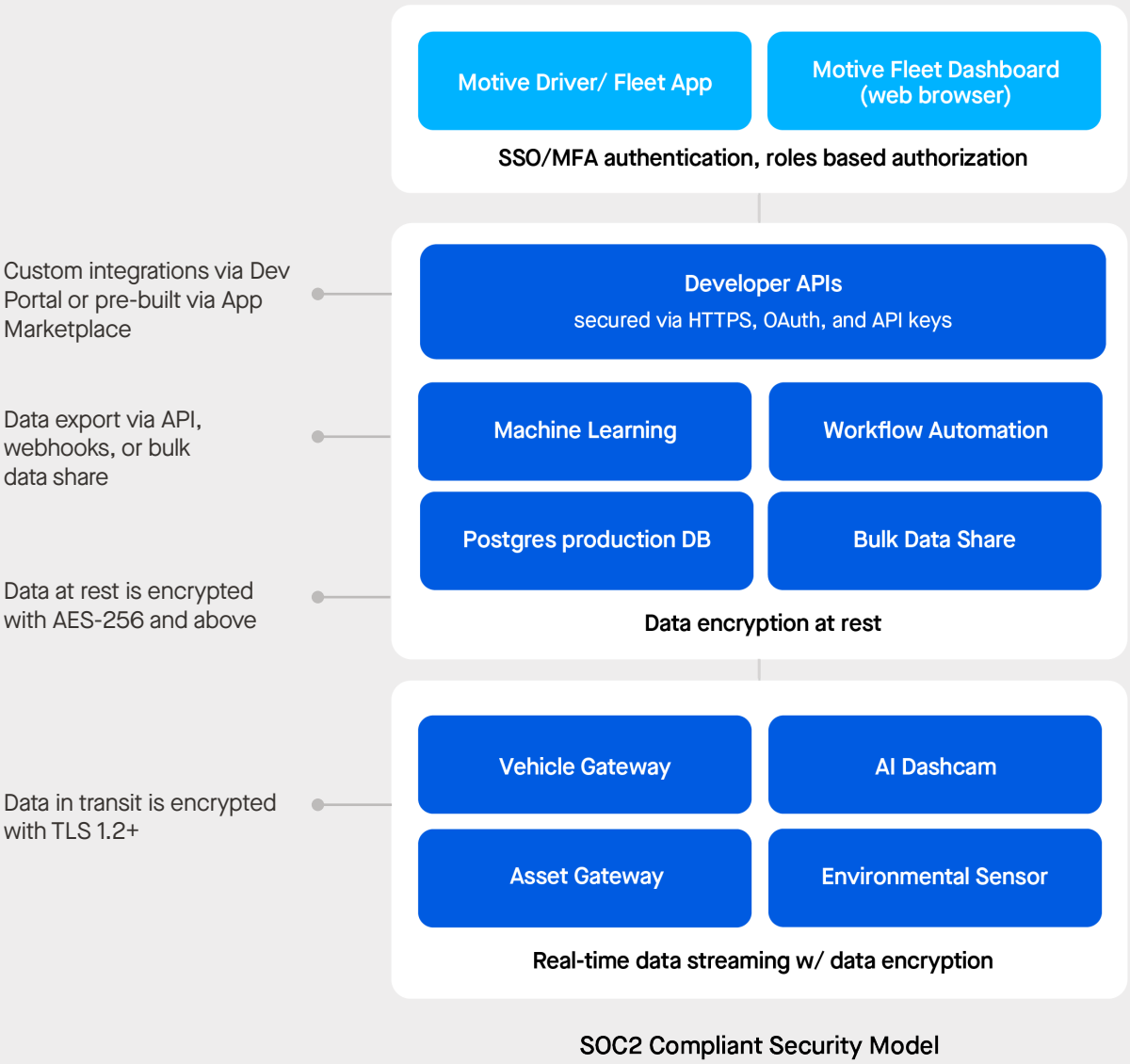
motive

Security Overview

Motive builds technology to improve the safety, productivity, and profitability of businesses that power the physical economy.

We operate infrastructure designed to provide security across the entire suite— from the physical security of hosting environments to the security protections of our IoT hardware and software applications, to the processes we use to support operational security.



SOC2 Compliant Security Model

Information security office	Motive employs dedicated Information Security teams with a focus on specialized application security, enterprise security, and cloud security. In addition, dedicated security and privacy legal counsel helps ensure compliance with applicable laws and regulations. In coordination, these teams create and manage the formalized Information Security Policies that are adopted across the entire organization.
Security awareness	Security awareness training for all employees focuses on identifying social engineering, phishing attempts, and securing workstations. Annual security awareness training and information security policy acknowledgment is required. Phishing simulations with on-demand training reduce risk and reinforce awareness.
Secure workforce	Next-generation anti-virus, anti-ransomware, logging, and extended detection response capabilities are installed on all endpoints operated by our employees. Whole disk encryption is required across all workstations. Robust Mobile Device Management (MDM) is leveraged to enforce secure configuration and security updates. Multi-Factor Authentication (MFA) is required across all systems.
Security operations	A round-the-clock Security Operations Center monitors enterprise and production workloads for anomalous behavior. A formal Incident Response Plan, Tabletop Exercises (TTX), and incident response playbooks support operations. Motive also maintains an incident response forensics team with a leading third-party firm as well as cyber liability insurance as a reactive control.
Vulnerability management	Robust internal, external, and agent-based vulnerability scanning provides near real-time identification of vulnerabilities for remediation. Annual penetration testing is used to validate controls and identify opportunities to improve security controls. A bug bounty program allows authorized penetration testers to continuously test applications for additional vulnerabilities.
Secure application development	Our Secure Software Development Lifecycle with CI/CD process is used for a full audit trail of code pushed to production. Infrastructure as code ensures all infrastructure resources are provisioned as per defined policies and best practices. Application security scanning, software composition analysis (SCA), and risk-driven manual security review validate the functionality and security of code being released to production.

Secure cloud infrastructure	Motive applications run on AWS secure cloud infrastructure, which is ISO 27001 and SOC 2 Type II certified, to ensure the confidentiality, integrity, and availability of our customer applications. This elastic infrastructure seamlessly scales with business requirements. Secure VPN and Multi-Factor Authentication (MFA) is required for access to production environments for authorized Motive team members.
Physical device protection	For Motive IOT hardware such as ELDs, dash cams, etc., security controls are in place to prevent malicious access. All universal asynchronous receiver-transmitter (UART) connections are password protected to prevent unauthorized access to devices. Wireless communication is protected by Wi-Fi Protected Access (WPA) WBP encryption, LTE connection authentication/encryption, Bluetooth standard encryption, and by Motive-specific connection authentication. Security patches and firmware updates are applied from the cloud via an authenticated and encrypted connection. All devices validate signed firmware images before executing any code/ binary to prevent non-Motive code from running on the device.
Data protection	Customer data in transit is encrypted with Transport Layer Security TLS 1.2+. Customer data at rest is encrypted with AES-256 and above to safeguard it against unauthorized access via brute force data attacks. An internal Data Classification Standard is enforced to ensure that customer data is protected.
High availability, disaster recovery	High availability infrastructure spanning multiple AWS availability zones allows for resilient applications. Periodic disaster recovery testing is performed to validate Recovery Time Objective. Database restoration testing is performed to validate integrity and Recovery Point Objective.
Authentication and authorization	Motive supports Single Sign-On (SSO) using SAML and OIDC authentication methods as well as Multi-Factor Authentication (MFA) and Universal Login. Robust authorization capabilities enable administrators to assign roles and permissions via pre-built or custom definitions, which further enhance the security of applications and data.

Information security assurance

Motive has attained SOC 2 Type I certification with full report availability upon request. Motive expects SOC 2 Type II completion in the first half of 2023. Our Information Security staff remains current with certifications and training including:

- **International Information System Security Certification Consortium (ISC2)**
  - Certified Information Systems Security (CISSP)
  - Certified Cloud Security Professional (CCSP)
- **Information Systems Audit and Control Association (ISACA)**
  - Certified in Risk and Information Systems Control (CRISC)
  - Certified Information Systems Auditor (CISA)
- **Certified Incident Handler (GCIH)**
  - Strategic Planning, Policy, and Leadership (GSTRT)
  - Security Essentials (GSEC)
- **International Association of Privacy Professionals**
  - Certified Information Privacy Professional (CIPP)
  - Certified Information Privacy Technologist (CIPT)

motive

gomotive.com

855-434-3564

sales@gomotive.com