Replicant's Commitment to Security, Compliance, and Data Privacy

Customer trust is at the core of our business. We provide trustworthy solutions and services because we know that our customers share the same commitment to trust with their own customers. We uphold our dedication to customer trust by delivering enterprise-level security, compliance, and data privacy.

Our Commitment to You

Security Culture

At Replicant, we embody a secure by design culture. From the people we employ to the solutions we develop, we're committed to earning and maintaining your trust through:

- Data Confidentiality: Customer data is segmented from internal systems
- Data Integrity: Customer data is uniquely tagged and backed up regularly
- Platform Availability: Scaling infrastructure that meets Customer demands

Secure Platform

Replicant customers leverage features that give them the control to customize how their data is accessed, used, and retained. Some of these features include:

- Unique Replicant roles that align with Customers' access controls
- Data retention flexibility that aligns with Customers' regulatory requirements
- IP address restrictions that block unauthorized system connectivity

Data Security

Replicant's enterprise platform is fully compliant with current data protection regulations at the state and federal level. To maintain data privacy, Replicant leverages:

- Encrypted network traffic reduces the risk of data interception
- Encrypted customer databases reduce the risk of unauthorized disclosure
- Customer data backups reduce the risk of ransomware

High Availability

Replicant's platform provides high availability infrastructure that runs 24/7 with efficient load balancing across thousands of concurrent calls so that you can scale effortlessly and securely.

- Customer data is physically protected in Tier 1 datacenters with world class security controls
- The platform infrastructure is redundant to ensure minimal impact from natural threats
- Underlying infrastructure is designed to automatically scale with the needs of your business

Security Certifications & Standards

Replicant's platform security standards satisfy both industry-specific regulations, as well as state, federal, and international regulatory requirements around data privacy and protection. Replicant is a HIPAA, SOC 2, PCI, and GDPR compliant platform.

Data Protection, Storage and Disposal

Physical Data Security: Replicant is hosted on Google Cloud Platform (GCP) data centers within the continental United States. GCP data centers employ world class physical security controls which are certified to meet the highest standard of US and EU data privacy regulations.

Storage: All customer data is securely stored in GCP data centers within the continental U.S. and is only accessible virtually to internal employees with a valid need to know and enforced by role-based access controls, intrusion prevention systems (IPS), GCP KMS, and segmented network architecture.

Disposal: Replicant does not retain data for longer than is necessary to properly serve our customers. Customer Data is logically destroyed in accordance with internal policies and standards, state and federal regulations, and customer agreements.

Encryption: We securely encrypt all data at rest and in transit over public networks. For data in transit, we use TLS 1.2 with an industry standard ECDHE-RSA-AES128-SHA256 cipher. Data is encrypted at rest by default using GCP Key Management System (KMS) which leverages AES256 encryption cipher.

Pillars of Security

Security Attestation: Replicant conducts regular security audits and contracts independent third-party firms for application penetration testing, bug bounty program, and SOC 2 Type 2 annual audits.

Platform Monitoring: Replicant's platform leverages intrusion prevention and intrusion detection systems to monitor for unauthorized access, system misuse, and threats to system availability.

Incident Response: Security incidents are managed immediately and in accordance with the Replicant Incident Response Plan to identify, contain and remediate any internal or external threats. Furthermore, it is of the utmost priority for us to respond to incidents with urgency and transparency through frequent communication to all affected parties.

Defense in Depth: Replicant employs a layered security architecture which focuses on confidentiality, data integrity and system availability. Our defense in depth architecture serves to eliminate single points of failure and encompasses our people, processes, and technology.