Replicated Product, Process, Data Center & Network Security

GENERAL PLATFORM DATA OVERVIEW

Enabling Enterprise Private instances	Replicated enables commercial software vendors to distribute a private, enterprise-ready instance of their application into their customers' environments. By doing so, software vendors can give their customers full control of all the data that the application processes. Additionally by controlling the environment, end-customers can monitor and block inbound and outbound traffic to improve compliance with data controls.
Online Updates	If the customer is running the distributed software with "online updates" then, according to criteria controlled by the customer, specific metadata (the license ID & version information) is sent to Replicated to check if updates are available. More details, see our Data Transmission Policy.
Air Gap Mode	If the customer is running the distributed software in "air gap mode" then no data leaves the system (or is even attempted) without direct action from the customer. Optionally data can be redacted before sharing.

Replicated Data Center & Network Security

PHYSICAL SECURITY

Facilities	Replicated's production platform is hosted on Latitude.sh, a Megaport company. Latitude.sh provides the underlying bare-metal infrastructure and hosting services. Replicated manages the platform software and its security configuration.
On-site Security	Latitude.sh is responsible for the physical security of its hosting facilities. Its published security measures include controls designed to prevent unauthorized physical access to offices and data centers. Physical security controls are operated by the hosting provider. Replicated's responsibilities include securing access to the systems and services it operates on that infrastructure.
Location	Replicated service providers data centers are located in the United States.
Hosting Responsibilities	Latitude.sh provides hosting for Replicated's Kubernetes infrastructure and object storage. Replicated operates the platform on this infrastructure and evaluates its hosting partners for service availability, networking, and operational reliability.

ENCRYPTION

Encryption in Transit	Communications between customers, vendors, and Replicated servers are encrypted according to industry best practices (HTTPS).
Encryption at Rest	Replicated supports encryption of sensitive customer data at rest.

REPLICATED

NETWORK SECURITY

Protection	Replicated uses Latitude.sh for hosting and Cloudflare for network security services. Access to administrative systems is controlled through a Zero Trust implementation that evaluates the connection and connecting device. Firewall policies restrict access from external networks and between internal systems. Access is limited to the ports and protocols required for each system's function and business need. Replicated manages the security configuration of the platform it operates on Latitude.sh.
Vulnerability Scanning	Replicated uses network access controls, application isolation, operating system restrictions, and encrypted connections to reduce the risk of unauthorized access. Latitude.sh's bare-metal hosting provides dedicated physical servers; security does not depend on a shared hypervisor. Suspected unauthorized network activity is investigated, with the hosting and network security providers involved as appropriate.
Web Application Firewall	Replicated leverages a suite of Cloudflare products to provide virtual web application firewall (WAF) that automatically blocks suspicious traffic and bots, and enables rate limiting.
Penetration Testing and Vulnerability Assessments	Third-party security testing of our service provider is performed by independent and reputable security consulting firms at least annually. Findings from each assessment are reviewed with the assessors, risk ranked, assigned to the responsible team for remediation, and then reviewed again.
Security Incident Event and Response	In the event of a security incident, our engineers gather extensive logs from critical host systems and analyze them to respond to the incident in the most appropriate way possible. Gathering and analyzing log information is critical for troubleshooting and investigating issues. Our service provider allows us to analyze four main log types: system, application, API, and audit logs from user accounts.
DDoS Mitigation	Cloudflare provides network security and distributed denial-of-service (DDoS) protection. Replicated works with its infrastructure and network security providers to respond to events and apply mitigation controls as needed.
Logical Access	Access to the Replicated production network is restricted by an explicit need-to-know basis. It utilizes least privilege, is frequently audited, and is closely controlled by our Engineering team. Employees accessing the Replicated production network are required to use multiple factors of authentication.

AVAILABILITY & CONTINUITY

Uptime	Replicated availability is continuously monitored. Current availability reports and incident updates are available at https://status.replicated.com

Redundancy	Replicated uses a cloud-native architecture, including clustering and network redundancy, to support platform availability. Production hosting is provided by Latitude.sh. Redundancy and recovery depend on the design and configuration of the Replicated platform.
Disaster Recovery	Replicated performs near-continuous backups and regular recovery exercises to support recovery of the platform services and data it operates on Latitude.sh. Replicated manages recovery of its platform and coordinates infrastructure incidents with the hosting provider.

Application Security

SECURE DEVELOPMENT (SDLC)

Framework Security Controls	We utilize frameworks for security controls to limit exposure to OWASP Top 10 security flaws. These include inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.
QA	In addition to automated testing, our QA department reviews and tests our code base. Dedicated application engineers on staff identify, test, and triage security vulnerabilities in code.
Separate Environments	Testing and staging environments are separated from the production environment. No actual customer data or vendor data is ever used in the development, staging, or test environments.
Development Best Practices	We follow development best practices, including independent code review by human reviewers or authorized AI review agents, together with automated testing.
Container Images	Our distributable products use minimal distroless container images built and maintained by Replicated. Every image is scanned before it is released and includes a Software Bill of Materials (SBOM).

APPLICATION VULNERABILITIES

Static Code Analysis	Our source code repositories are continuously scanned for security issues via our integrated static analysis tooling.
Dependency Analysis	Our application dependencies are continuously scanned for CVE information and remediated through automated pull requests when fixes are released.
Continuous updates to 3rd-party components	Our system continuously scans upstream 3rd-party components for updates and automatically generates pull requests when new versions are available to install. These update requests are reviewed daily for integration.
Vulnerability Reporting Program	The disclosure of relevant CVEs by Replicated to our customers and impacted parties is described in our Vulnerability Reporting Program Whitepaper that is available to customers and prospects upon request.

REPLICATED

Product Security Features

SECURE DEVELOPMENT (SDLC)

Secure disclosure	Replicated incentivizes secure disclosure through a private bug bounty program please contact security@replicated.com for inclusion in the program.
Secure Credential Storage	Replicated follows secure credential storage best practices by never storing passwords, but instead storing a 1-way hash of the salted password.
API Security & Authentication	Replicated API is TLS-only and you must be a verified user to make API requests. You can authorize against the API using an API token that is controlled on the teams and tokens page. APIs are rate limited to prevent brute force attacks.

ADDITIONAL PRODUCT SECURITY FEATURES

Access Privileges & Roles	Access to view and change your Replicated account configuration is governed by access rights, and can be configured to define access privileges. Replicated has various permission levels for organization (admin & read-only) and a fully customizable RBAC system for Enterprise users.
Account Audit Logs	Replicated accounts include a full audit log of the activity in the account. The audit logging system utilizes a Merkle tree design, which ensures data integrity. This data is available via the UI, and can also be accessed from the API for automated collection and centralization of event data.
Authentication Options	Replicated supports password based sign-in with two-factor authentication (2FA) and admin controlled password complexity options. Additionally, Replicated Enterprise Plan customers can leverage & enforce our SAML integration for user management.
Transmission Security	All communications with Replicated service provider servers are encrypted using industry standard HTTPS. This ensures that all traffic between you and Replicated is secure during transit.

Additional Security Methodologies

SECURITY AWARENESS

Policies	Replicated has developed a comprehensive set of security policies covering a range of topics. These policies are shared with all employees and contractors with access to Replicated information assets.
Training	All new employees attend a security awareness training, and the Engineering team provides security awareness updates via email, blog posts, and in presentations during internal events.

EMPLOYEE VETTING

Background Checks	Replicated performs background checks on all new employees in accordance with local laws. The background check includes criminal history and identity verification.

Confidentiality Agreements	All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.

SERVICE ORGANIZATION CONTROL (SOC 2)

SOC 2 Type 1 & 2	Replicated has completed validation of our SOC 2 Type 1 and Type 2 compliance for security and confidentiality trust principles.
Infrastructure and Subprocessors	We transparently share and maintain our list of infrastructure and subprocessors.