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 service providers' physical infrastructure is hosted and managed within Amazon Web Services (AWS) secure data centers and utilizes AWS technology. AWS continually manages risk and undergoes recurring assessments to ensure compliance according to the industry's standards. AWS data center operations have been accredited under: • ISO 27001 • SOC 1 and SOC 2/SSAE 16/ISAE 3402 • PCI Level 1 • FISMA Moderate • Sarbanes-Oxley (SOX)
On-site Security	Replicated utilizes ISO 27001 and FISMA certified data centers managed by AWS. AWS data centers are housed in nondescript facilities, and 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, 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.
Location	Replicated service providers data centers are located in the United States.

NETWORK SECURITY

Protection	All firewall infrastructure and management is provided by our service providers: AWS and Cloudflare. Access to these systems is granted by a ZeroTrust implementation that analyzes the connection and the connecting device, with decisions made based on the characteristics of the request. Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to the ports and protocols required for a system's specific function in order to mitigate risk. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.
Vulnerability Scanning	Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Our service provider utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at multiple levels. Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.
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	Our service provider's infrastructure provides distributed denial-of-service (DDoS) mitigation techniques, including TCP Syn cookies and connection rate limiting, in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when 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.

REPLICATED

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.

AVAILABILITY & CONTINUITY

Uptime	Replicated availability has been 100% for the previous quarter and is continuously monitored. The availability reports are available at https://status.replicated.com
Redundancy	Replicated leverages a cloud-native architecture, including clustering and network redundancies, to eliminate single point of failure. For additional redundancy, offsite data backup is available for qualifying accounts to copy the customer's data to a separate cloud provider to mitigate against data loss from AWS.
Disaster Recovery	Our service provider's platform automatically restores customer applications and databases in the case of an outage. The provider's platform is designed to dynamically deploy applications within its cloud, monitor for failures, and recover failed platform components including customer applications and databases.

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 peer reviews and automated testing. These are independently reviewed during SOC2 audits.
Container Images	Our distributable products utilize Wolfi "distroless" images, known to be the most secure with the least number of known security issues. Every image is scanned before it is released and includes a Software Bill of Materials (SBOM).

REPLICATED

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.

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.

REPLICATED

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.