REPLICATED

Replicated Product, Process, Data Center & Network Security

GENERAL PLATFORM DATA OVERVIEW	
Enabling Enterprise Private instances	The Replicated Private Instance Delivery Platform is designed to enable application vendors to distribute a private, enterprise-ready instance of their application behind-the-firewall and into their customer's environment. When the distributed software (the vendor's application plus the Replicated deployable components) is running as a private instance in the customer environment **no data from the vendor's application** ever leaves the environment.
On-line Updates	If the customer is running the distributed software with "online updates" then, on an cadence controlled by the customer, specific metadata (the license ID & version information) is sent to Replicated to check if updates are available.
Airgap Mode	If the customer is running the distributed software in "airgap mode" then no data ever leaves the system (or is even attempted).

Replicated Data Center & Network Security

PHYSICAL SECURITY	
Facilities	Replicated service providers physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance according to the industry's standards. Amazon's data center operations have been accredited under: • ISO 27001 • SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II) • PCI Level 1 • FISMA Moderate • Sarbanes-Oxley (SOX)
On-site Security	Replicated utilizes ISO 27001 and FISMA certified data centers managed by Amazon. 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, state of the art 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.

REPLICATED

NETWORK SECURITY

Protection	All firewall infrastructure and management is provided by our service providers: Amazon AWS. 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 all 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 Signal Sciences, a virtual WAF that automatically blacklists and blocks suspicious traffic.
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, and 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 are called in to 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 logs and audit logs from user accounts.
DDoS Mitigation	Our service providers infrastructure provides 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 via 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.
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	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.

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.

Product Security Features

SECURE DEVELOPMENT (SDLC)

Secure disclosure	Replicated incentivizes secure disclosure through a private bug bounty 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 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. This data is available via the UI, but can also be accessed from the API for automated collection and centralization of event data.
Authentication Options	Replicated supports password based sign-in with 2FA and admin controlled password complexity options.
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, and made available to, 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.

REPLICATED

EMPLOYEE VETTING

Background Checks	Replicated performs background checks on all new employees in accordance with local laws. The background check includes Criminal, Education, and Employment verification.
Confidentiality Agreements	All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements.