Cherre Security Overview

2021

Cherre, Inc.

cherre

Cherre Security Overview

We know your data is sensitive. That's why Cherre combines enterprise-grade security features with regular audits to ensure you're always protected.

Cherre Security Organization and Program

While security is a high priority for all teams across Cherre, a dedicated security team manages the Cherre security program. Our security framework is based on ISO 27001 and NIST 800-53 Information Security Standards and includes policies covering data classification, access management, cryptography, change management, secure server configuration, physical security, business continuity, vendor assurance, vulnerability management, security monitoring, and incident response. Security is represented at the company's highest levels, with our Head of Security meeting with executive management frequently to discuss risks and coordinate company-wide initiatives. Information security policies and standards are approved by management and available to all Cherre employees.

People Security

The people building and maintaining Cherre products are our most precious assets. We've implemented processes to ensure we're bringing in the right people and keeping them up to date on the latest security trends.

Here are some of the procedures we have in place:

- **Robust interview process:** Applicants must be interviewed by at least two relevant managers before acceptance. Interviewers rate applicants based on technical aptitude, ethical standards, and cultural fit.
- **Onboarding/offboarding process:** We use Rippling software to automate the onboarding and offboarding process and account provisioning.
- **Background checks:** All candidates must pass background checks by a specialized third party before being offered a position. For domestic candidates, these include a Social Security number trace, criminal county search (seven-year address history), multi-state instant criminal check, National Sex Offenders Public Registry check, Office of Foreign Assets Control (OFAC) search, professional references, and education verification.
- **Infosec training:** All new employees attend legal and security training during the onboarding process. In addition, all employees go through information security training once per year. The material is produced in-house and covers information security policies, security best practices, and privacy principles.

- **Continuous security education:** Cherre provides continuous education on emerging threats, performs phishing awareness campaigns, and communicates with the entire team regularly.

Product Security

Application Security

The Product Security program mission is to enable product teams to build solutions that are best in class when it comes to security. The following activities help us to achieve this mission:

- Internal security reviews before products are launched
- Continuous internal and external security tests
- Regular threat modeling exercises
- Regular penetration tests performed by reputable third party

Change Management

Through a formal change management process, all changes to Cherre software are tracked and approved. Automated controls ensure that changes are reviewed by at least one other team member and pass automated tests before being implemented.

Data Encryption

Cherre encrypts data in transit and at rest.

- **Encryption in transit:** All data sent to or from Cherre infrastructure is encrypted in transit using Transport Layer Security (TLS).
- **Encryption at rest:** All user data is encrypted in the database using the AES-256 encryption standard.
- **Extra encryption for sensitive data:** We secure sensitive dataset using industry best practices and extra security layers.

Penetration Testing

We partner with reputable security companies to perform regular penetration tests on Cherre applications and infrastructure

Application Monitoring and Protection

We have deployed an array of solutions to monitor and protect our applications, including:

- Technologies to monitor exceptions and detect anomalies in our applications.
- Collection and storage of application logs to provide an audit trail of our application activity.

Cloud and Infrastructure Security

Our infrastructure serves as a safe platform for Cherre applications, and our cloud security practices adhere to the Center for Internet Security (CIS). Our cloud security program is driven by four principles:

Asset Management

All cloud assets in Cherre's infrastructure are inventoried. Assets must have a defined owner, security classification, and purpose.

Infrastructure Management

Where possible, control planes are used to manage services running in production to reduce direct access to host infrastructure and data. Direct access to production resources is restricted to a handful of employees on the DevOps requiring access. Role-based access control is enforced through Cherre Single Sign-On (SSO). On top of that, strong multi-factor authentication, encryption protocols, and session auditing are enforced for these connections.

Defense-In-Depth

Cherre's production environment employs defensive security controls at all layers of its infrastructure, such as:

- **Network segregation:** Through the use of virtual private clouds (VPCs) and security groups, we ensure that only the most minimal network access to Cherre production networks is granted.
- **Identity and access management:** Cherre follows a least-privileged approach to manage user and application access to Google Cloud Platform (GCP).
- **Audit trail:** Cherre stores an audit trail for all access activity within its production GCP services
- **Security events monitoring:** We use GCP Cloud Armor to monitor security events in Cherre GCP accounts.

Cloud configuration monitoring

The Cherre Cloud assets are continuously monitored for adherence to security best practices. We leverage automation to identify any deviation from our technical standards and raise issues within minutes of the configuration change.

Vulnerability Management

The Vulnerability Management program establishes how Cherre identifies, responds, and triages vulnerabilities against our platform.

The program includes the following initiatives:

- Continuous automated scans on library dependencies used by Cherre's application.
- Vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process.
- Remediation service-level agreements (SLAs) defined according to the severity associated with the vulnerabilities discovered.

Security Monitoring and Incident Response

Continuous monitoring

Through the ongoing awareness of vulnerabilities, incidents, and threats, we can quickly respond and mitigate accordingly. Cherre leverages a comprehensive collection of application, infrastructure, and software-as-a-service (SaaS) log sources to identify and triage possible security events.

Incident response program

Cherre manages an incident response program. The program defines requirements under which security incidents are classified and triaged. The Cherre Security Incident Response Team evaluates the threat of all applicable vulnerabilities and security incidents and establishes remediation and mitigation responses for all events. The incident response process has precisely defined roles and responsibilities to ensure that any incident is triaged efficiently after detection and mechanisms for evidence collection that preserves confidentiality.

Physical Security

Data Center security

We use GCP data centers for all production systems and customer data. GCP follows industry best practices and complies with a comprehensive list of security standards.

For more information on Google Cloud Platform data center physical security, see the Google Whitepapers.

Office security

We have a security program that manages visitors, building entrances, CCTVs, and overall office security. Office access is protected by keycard/Bluetooth, using third-party access-control software. Access lists giving control to specific locations are managed by Cherre software. Logs of successful and unsuccessful entry attempts are maintained for three months.

Business Continuity/Disaster Recovery

Cherre leverages GCP infrastructure and adherence to configuration best practices to ensure best-in-class resiliency.

Multi-data center resiliency

Hosting our services on GCP gives Cherre the ability to remain resilient globally even if one location goes down. The GCP services we use, including VPCs, load balancers, Cloud storage, and Big Query - span multiple availability zones to ensure resiliency in the event of most failure scenarios, including natural disasters and system failures.

Data backups

Cherre performs continuous backups of critical data using Google Cloud Storage(GCS) replication capabilities across multiple regions. Our production database clusters are shared across multiple availability zones, and snapshots of their data are constantly backed up in GCS. All backups are encrypted in transit and at rest using strong encryption tactics.

Disaster recovery

We maintain a formal disaster recovery process that depicts the inventory of critical assets and personnel, and a plan to restore the availability of critical services. The disaster recovery plan is tested on a yearly basis.

Vendor assessment

Third parties are assessed before onboarding to validate that they meet our security and legal requirements. Once a relationship has been established, Cherre reviews security and business continuity concerns periodically. The program considers the type of access and classification of data being accessed (if any), controls necessary to protect data, and regulatory requirements.

Security compliance

Cherre complies with applicable legal, industry, and regulatory requirements as well as industry best practices. We hold the following certifications:
SOC 2 Type I (2020)