CheckCentral Security

CHECKCENTRAL

BINARYFORTRESS

CheckCentral Security and Service

CheckCentral is a monitoring software used by enterprise-level clients and MSPs who must ensure their data and communications are well-protected.

Binary Fortress Software, the makers of CheckCentral, continue to implement security measures that support our clients' interests as well as our own. From the management website and mobile app to the storage of client data, full considerations have been made to create a solid and secure software experience.

Service Levels

CheckCentral service goals are 99.9% uptime annually and ticket responses of 1 business day. Our service status is available here: **https://status.checkcentral.cc**.

- 99.9% uptime
- 1 business day ticket response

Dashboard and Management Site

The dashboard and management site for CheckCentral clients is HTTPS-secured, with available two-factor authentication (2FA) for added security on login. Single Sign-On (SSO) with Azure AD and Google Workspace is also available. Passwords are salted with unique, random character strings, then hashed for secure storage. The mobile app is given the same security treatments.

- HTTPS-secured
- 2FA
- SSO
- Salted, hashed password storage

Email Security

CheckCentral software parses notification emails to match client-defined matching criteria for establishing check status conditions. As such, clients' select emails are sent to Binary Fortress email servers for parsing. SSL and TLS are used between client and server to protect and encrypt email details. This keeps sensitive information private and inaccessible to anyone outside this conduit of trusted communication.

- SSL/TLS communication protocol (when fully supported)

Data Security and PII

Once the clients' emails are received, the data within is stored on Binary Fortress servers for parsing and matching. Data moved between these servers is HTTPS-encrypted, and email contents are encrypted at rest. Only check names and high-level matching criteria are not encrypted at rest, but contain no detailed information about the clients' servers, employees, or sensitive data.

Personally Identifiable Information (PII) collected and stored by Binary Fortress is for CheckCentral user creation (i.e. names, email addresses, and phone numbers). This data is encrypted when in transmission.

- HTTPS-encrypted in transit
- Email contents encrypted at rest

Payment Information and Processing

Binary Fortress Software uses Stripe for storing client payment information and processing purchases. Stripe is a Level 1 PCI Service Provider. It uses HTTPS and HSTS for secure connections and encrypts all card numbers at rest with a separated infrastructure to prevent overlapping data access.

- Level 1 PCI Service Provider
- HTTPS/HSTS for secure connections/encryption
- Separated infrastructure to prevent overlapping data access

Data Centre Details

The facility housing client data is a tier 3 colocation data centre owned and operated by a large data centre provider located in Ottawa, Canada. There is redundant power, redundant Internet connections, and strict physical access controls including biometric scanners. The data centre facility has SOC2, SSAE 16, and ISAE 3402 certifications.

Audits and Disaster Recovery

Binary Fortress runs quarterly audits and tests for the following: security of in-house servers and employee machines (including data access and retention), internal code audits, and full disaster recovery.

- Quarterly security, code, DR tests/audits

Cyber Risk Management and Third-Party Integrations

Third-party services are always kept up-to-date, OS updates are performed monthly or on-demand as needed, and a bug bounty program is available for reporting security issues.

Notifications to third-party channel software such as external emails or Slack do not include sensitive information and only reference the state of checks. Integrations with external ticketing systems, giving access to more detail, use API keys and tokens to establish trusted communication between systems. Azure is used for incoming SMTP mail relays. Google and Amazon cloud services are used for OCR attachment processing.

- Third-party services always up-to-date
- API keys/tokens for ticketing system integration

About CheckCentral

CheckCentral Monitoring consolidates and simplifies backup, system, and software email updates into a clean, graphical dashboard, bringing peace of mind to IT administrators of SMBs, Enterprises, and MSPs.

To learn more about CheckCentral, visit: **https://www.checkcentral.cc**

About Binary Fortress Software

Binary Fortress has spent 17 years in pursuit of one goal: create software to make life easier. Our software ranges from display management and system enhancement utilities to monitoring tools and digital signage. IT administrators, professional gamers, coffee-shop owners, and MSPs all rely on Binary Fortress to make their days better, and their lives easier.

Binary Fortress Software
1000 Innovation Drive, Suite 500
Kanata, Ontario, Canada
K2K3E7
https://www.binaryfortress.com