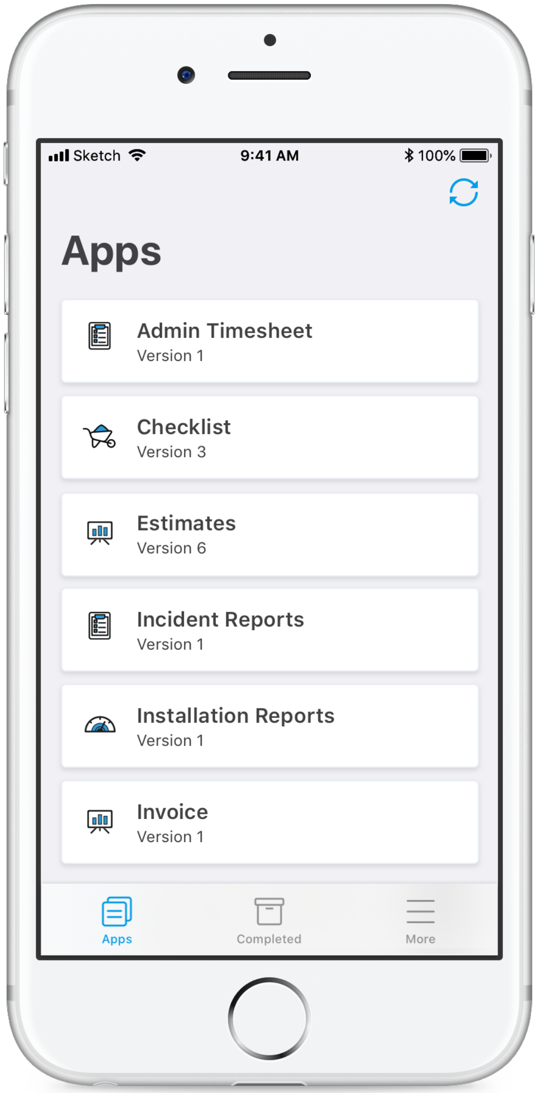
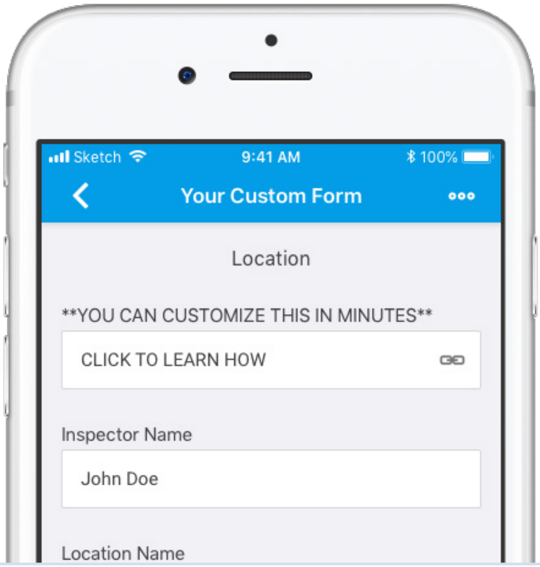
MAY 2021

Security and Infrastructure Overview

gocanvas

Table of Contents





Inspector Name
John Doe

Location Name

Introduction

Our mission at GoCanvas is to simplify the lives of our customers by giving them the tools necessary to eliminate wasteful spending and reinvest back into productivity. We believe protecting your data is one of our most important responsibilities and are committed to being open and transparent about our security practices. Canvas Solutions Inc. provides the GoCanvas SaaS product as a robust platform which provides GoCanvas customers with a stable, highly available, and secure solution to submit, store, and access data at all times. GoCanvas provides these capabilities across both the mobile and hosted infrastructure of the GoCanvas product.

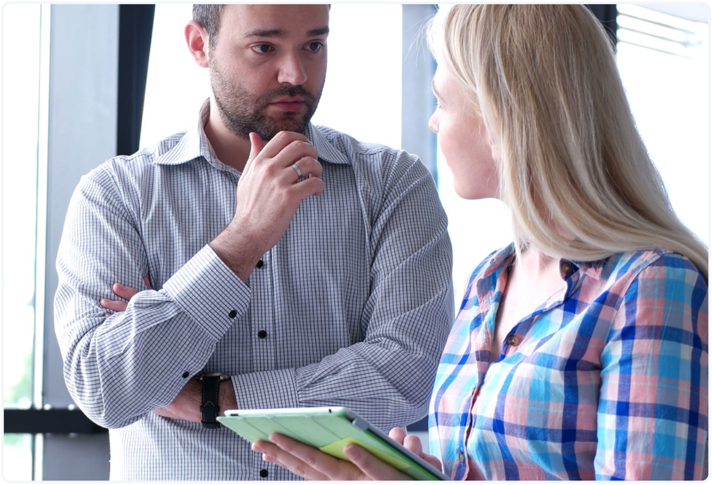
Access

At GoCanvas, we adhere to the principles of least privilege and role-based permissions. Employees are only authorized to access data that they must handle in order to fulfill their current tasks or responsibilities. All production access is reviewed quarterly through a combination of automated and manual processes.

Sensitive Data Handling

The GoCanvas product is primarily self-serve in order for customers to have control regarding what data is collected utilizing the GoCanvas platform. Following best practices such as encryption-at-rest and encryption-in-transit, GoCanvas ensures that data being collected is handled securely. In addition to these best practices, GoCanvas implements a number of additional measures to make sure data is handled appropriately, including:

- Security training for all employees
- GDPR training for all employees
- HIPAA training for all employees
- Least responsibility model for all employees
- Background checks for employees with infrastructure access



Infrastructure and Availability

GoCanvas is built on a highly available web application architecture utilizing best practices to achieve high availability, fault tolerance, and the capability to scale to meet future demands. The GoCanvas hosting environment and physical hardware is currently provided by Amazon Web Services' Cloud Computing Services (AWS).

The Amazon Web Services' Cloud Computing Services security processes and practices are detailed through a number of white papers, reports and certifications – which are made available via the AWS security section of its product website – which can be found at http://aws.amazon.com/security/.

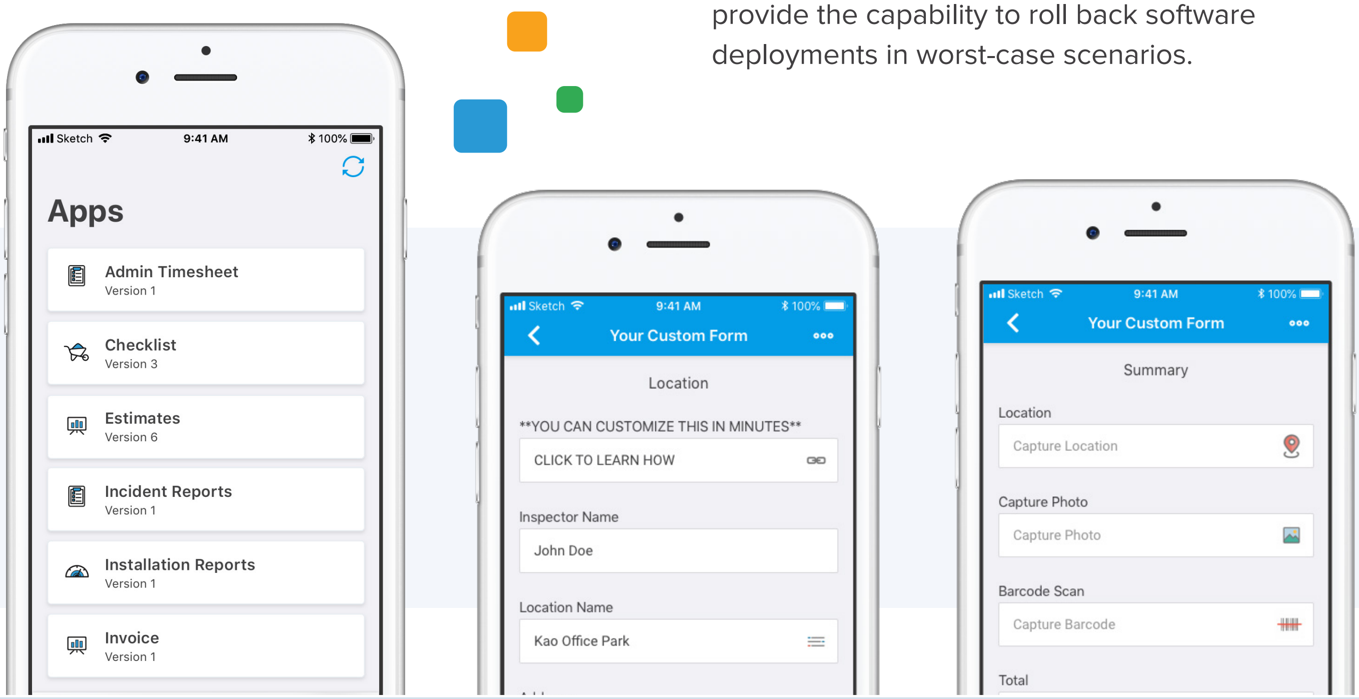
GoCanvas maintains two separate infrastructures. One infrastructure is for https://www.gocanvas.com, which is hosted in a data center located in Northern Virginia, USA; the other is for https://au.gocanvas.com, which is hosted in a data center in Sydney, Australia. Customer data does not flow between the two infrastructures. Within both regions the hosting architecture, failover methodology, monitoring and security are all held to the same standards which follow best practices. In addition, Amazon Web Services maintains the same infrastructure and operating protocols across all regions.

Disaster Recovery and Failover

GoCanvas leverages best practices for failover and recovery to ensure data integrity and service continuity. GoCanvas is hosted across several different physical data centers to provide redundancy for each architectural component within the GoCanvas application stack. The data centers are located within different locations separated by enough geographic distance to be isolated from any local specific issues, but close enough to not incur any latency issues when communicating between the regions. This availability is accomplished by leveraging several AWS availability zones within the relevant regions to support the GoCanvas infrastructure.

Configuration Management

GoCanvas employs industry best practices regarding software development (including source control, automated builds, peer reviews) to ensure that change management and configuration management are performed in a consistent and secure manner. The GoCanvas software is developed and managed through a change management system which then is versioned, built, and deployed automatically. By utilizing automated systems wherever possible, risk and potential downtime are minimized. In addition, the automated systems provide the capability to roll back software deployments in worst-case scenarios.



Monitoring

The GoCanvas infrastructure has embedded monitoring tools at key points to evaluate performance and availability 24 hours a day, 7 days a week. When any performance metric is outside of operational bounds, a notification is sent to the appropriate team based on the severity and type of deviation. This allows GoCanvas to not just react to problems, but proactively address potential issues.

Backups and Data Redundancy

The GoCanvas operational data store is replicated in near real time to multiple data centers. If needed, this allows us to recover in real time to a backup data center to ensure availability of the system and integrity of your data. In addition, the complete operational data store is fully backed up on a nightly basis and is isolated from the production environment. This added layer helps ensure the integrity of the data for the GoCanvas customers.

GoCanvas customer data is retained in backups for 90 days. This is a balance between our security, recovery, and privacy concerns. After the retention period, data is automatically removed from our backup infrastructure.

Authentication, Authorization, and Logging

All access to the GoCanvas servers and infrastructure is governed by the principle of “least privilege” where only personnel, who absolutely need to have access, have access. Where appropriate, access is granted on a limited time basis for personnel to execute a specific task, at which point, the access is revoked.

All access and remote file transfers are always through encrypted protocols. All access to the GoCanvas infrastructure is logged and regularly reviewed for policy and procedural violations.

All remote web browser access to the GoCanvas website, which may display sensitive information in addition to any authorization information, is required to be accessed via 256-bit encrypted TLS version 1.2

Account Security

GoCanvas secures credentials using industry best practices including salting and hashing authentication passwords stored within the GoCanvas product. GoCanvas customers also have the ability, within their account settings, to configure password complexity, expiration, and lockout preferences for their GoCanvas account. In addition, GoCanvas integrates with both LDAP and SAML protocols for leveraging external authentication when desired by our customers.

More information regarding password settings can be found at our password help topic: https://help.gocanvas.com/hc/en-us/articles/115006654407-How-to-add-advanced-security-requirements-for-passwords

More information regarding LDAP can be found at our LDAP help topic: https://help.gocanvas.com/hc/en-us/articles/115006830428-How-to-enable-LDAP-authentication

More information regarding SAML can be found at our SAML help topic: https://help.gocanvas.com/hc/en-us/articles/360000529108-How-to-enable-and-configure-SSO

(Hypertext Transfer Protocol Secure). All access to the GoCanvas website, and access to specific user information, is logged and regularly reviewed for policy and procedural violations.

GoCanvas Network Security

GoCanvas servers reside behind a complete firewall solution with all access defaulting to deny incoming traffic. Only the minimum necessary protocols and traffic are allowed access to the GoCanvas environment. Any changes to the firewall configuration require the appropriate access level and validation via the GoCanvas change management process. This validation prevents unauthorized access or modification of GoCanvas firewall rules. All firewall changes are reviewed by the security team on a monthly basis and are analyzed by automated tooling.

All access to GoCanvas over a network interface, which may contain sensitive information, is required to utilize encrypted communication. This includes both the GoCanvas website and mobile device access.

GoCanvas Infrastructure Security

Our server infrastructure is a highly maintained and monitored environment. We follow best practices regarding real-time monitoring, security patching, and user access. All servers are part of an internal Intrusion Detection System (IDS) network to monitor all changes and access made to the environments.

Security patching is scheduled based on standardized threat levels (CVE).

Patch Type	Description	Interval
Standard	Updated local packages which do not include HIGH threat rating	Applied to all environments on the quarterly basis.
Critical	CVE rating CRITICAL (HIGH)	Immediately applied to test environments and applied to production after testing and approval.

GoCanvas Data Security

All user supplied information is encrypted, using the industry accepted AES encryption algorithm, before being written to any permanent data storage (data at rest encryption). All backups and replication of the GoCanvas data store are also encrypted in the same manner. All data stored by the GoCanvas client, whether it is data read from the GoCanvas server or data entered by a user, is encrypted using an encryption algorithm recognized as industry-approved before being stored to disk. The encryption algorithms utilized vary by device. The current algorithms are:

Client	Algorithm
Windows	AES 256
iOS	AES 256
Android	AES 256
AWS	AES 256

All communication with the GoCanvas server infrastructure is always secured by 256-bit TLS (currently 1.2), which cannot be disabled by a user of the GoCanvas client (data in transit encryption).

User Defined GoCanvas Data Security

In addition to the security controls put in place across the GoCanvas product, GoCanvas customers can also choose to enable HIPAA compliance controls for a specific account. This feature sets a compliant user-idle timeout and then automatically logs the user out of the system. The feature also restricts the saving of passwords on the user's devices to comply with HIPAA. These controls are in place to prevent unauthorized data access if a mobile device is lost or a terminal is left unattended. In addition, GoCanvas disables all in-application e-mail capabilities for accounts specified as being HIPAA compliant.

Incident Response

GoCanvas maintains security management policies and procedures in accordance with current best practices. These processes and procedures are overseen by the Chief Technology Officer and are tested on an annual basis. These policies provide a framework on communication, classification, and resolution of any incidents that occur. As part of this process, we create possible attack scenarios based on our past experience, the external threat environment, and threat intelligence for simulation and testing of our controls. These scenarios include, but are not limited to, data exfiltration, vulnerability remediation, unauthorized access to integrated systems, and zero-day response.

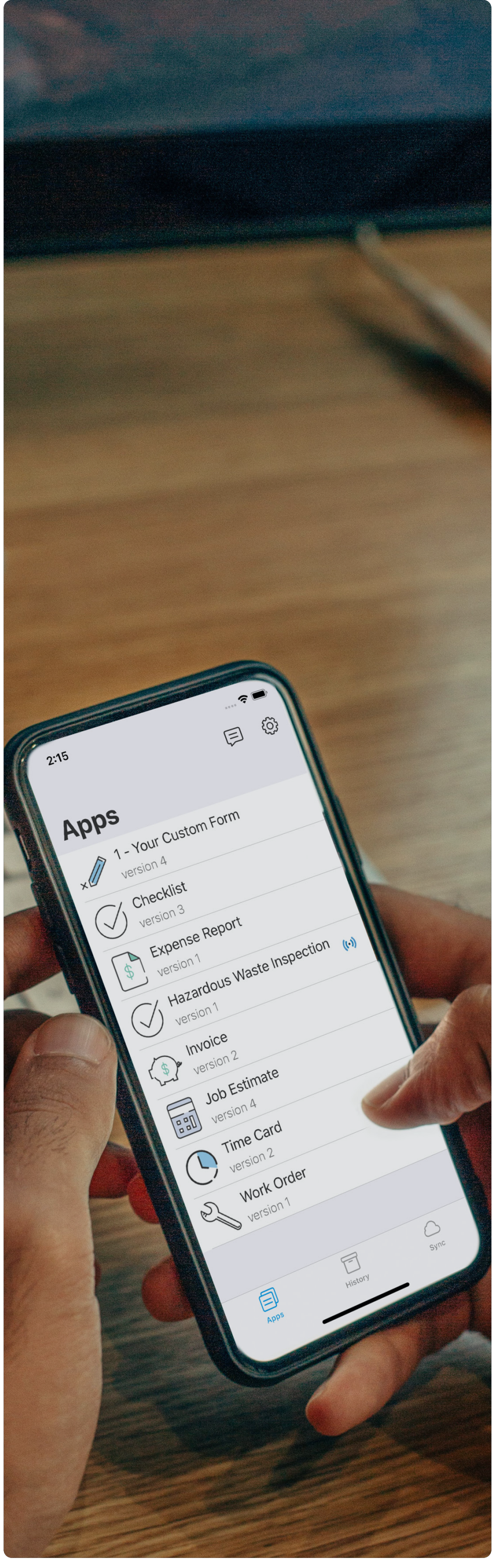
Vulnerability and Risk Management

At GoCanvas, the security of our products, infrastructure, and customer data is a top priority. We leverage a suite of different systems, technologies, and processes to identify, mitigate, and respond to vulnerabilities against the GoCanvas platform.
To ensure the security of customer data, GoCanvas has invested in the following capabilities:

- Regular penetration tests run by external third parties
- Continuously running internal penetration tests
- Static code vulnerability scanning
- Library and operating system vulnerability scanning

Change management

GoCanvas maintains a change management process for production releases and production changes. This includes a defined Software Development Life Cycle (SDLC) which incorporates documentation and ticketing associated with every software change. This formalized process reduces the risk of mistakes, unintentional interactions, and vulnerabilities into our code base. Additionally, GoCanvas implements a rigorous QA process with segmented environments for testing, validation, and sign-off before production releases occur.
Infrastructure changes and updates follow a change control process which allows for proper checks and balances. This allows us to quickly diagnose any erroneous system behavior and identify and correct the cause.



Policies

Terms of Service

Privacy Policy

Privacy Policy for California