GoCanvas – Security and Infrastructure Overview

August 2018

Contents

Introduction

Canvas Solutions Inc. provides the GoCanvas SaaS product as a robust platform which will provide 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 components and hosted infrastructure of the GoCanvas product.

Infrastructure

GoCanvas is built on the traditional 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' (AWS) Elastic Cloud Computing environment (EC2). The AWS EC2 environment provides the tools and environment for GoCanvas to provide fault tolerance across the application.

The Amazon Web Services' Elastic Cloud Computing environment 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 centered 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 to date. In addition, Amazon Web Services maintains the same infrastructure and operating protocols across all regions.

Configuration Management

GoCanvas employs industry best practices in regards to software development to ensure that change management and configuration management is 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 scenarios are minimized as much as possible. In addition to minimizing downtime, the automated systems provide the capability to roll back software deployments in worst-case scenarios. GoCanvas environment configuration leverages tools within AWS to create and maintain a consistent environment through snapshots which undergo thorough testing.

Monitoring

The GoCanvas infrastructure and key points such as domain uptime utilize monitoring tools to provide a robust infrastructure with a high level of availability. The monitoring tools in place provide the ability to notify key GoCanvas personnel when specific metrics get within warning and critical notification thresholds.

Failover and Disaster Recovery

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 distance to be isolated from any locale specific issues, but close enough to not incur any latency issues when communicating between the regions.

Backups and Data Redundancy

The GoCanvas operational data store is replicated in near real time to a separate data center from the primary operational data store. This provides the capability to fail over to a real time backup and continue operation of the GoCanvas product in a failure scenario. In addition to the real time replication, the GoCanvas operational data store is also fully backed up on a nightly basis.

Authentication, Authorization and Logging

All access to the GoCanvas servers and infrastructure is limited to a select few GoCanvas personnel, with access only being available via encrypted shell (SSH). In addition, all remote file transfers needed for administration of GoCanvas servers is also done via encrypted means (SCP). All access to the GoCanvas infrastructure is logged and appropriately recorded.

All remote web browser access to the GoCanvas website which may display sensitive information, in addition to any authorization information, are required to be accessed via 256-bit encrypted TLS version 1.0 (Hypertext Transfer Protocol Secure). All access to the GoCanvas website and access to specific user information is logged and recorded.

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 access to the necessary protected X.509 certificate in addition to a private key, which provides an extra layer of security to prevent unauthorized access or modification of GoCanvas firewall rules.

All access to GoCanvas over a network interface which may contain sensitive information is required to utilize encrypted communication. This includes a user accessing information on the GoCanvas website in addition to data submitted from the mobile device.

GoCanvas Infrastructure Security

The GoCanvas server infrastructure is a highly maintained environment, ensuring best practices are followed in regards to real-time monitoring, security patching and user access. All servers are part of an internal IDS network to monitor all changes and access made to the environments.

Security patching is scheduled based off of standardized threat levels and availability.

Patch Type	Description	Interval
Standard	Updated local packages which do not include HIGH threat rating	Applied to production environments every 30 days.
Critical	CVE rating CRITICAL (HIGH)	Immediately applied to test environments and applied to production after testing 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. 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 128

All communication with the GoCanvas server infrastructure is always secured by 256-bit TLS, which cannot be disabled by a user of the GoCanvas client.

User Defined GoCanvas Data Security

In addition to the security put in place across all GoCanvas customers, GoCanvas customers can also choose to enable HIPAA compliance, which will turn on additional security features for that specific account. By enabling this setting, a user-idle timeout has been implemented which will limit the amount of time that the GoCanvas application can remain idle before the user is logged out. The user is also no longer allowed to save their password on the device or on the website when accessing HIPAA compliant accounts. These features were put in place to prevent unauthorized data access in case a mobile device is lost or a terminal is left unlocked in an unsecure location. In addition, GoCanvas disables all in-application e-mail capabilities for accounts specified as being HIPAA compliant. Even though the HIPAA

specification is ambiguous in allowing e-mail correspondence, the GoCanvas team decided that the risk outweighs any potential benefits when it comes to e-mail communication and PHI.