ENGAGEMENT SOLUTIONS

PRODUCT: DECLARE

FULL TECHNICAL OVERVIEW

TABLE OF CONTENTS

SECTION 1

1.1.Network

Civica: Engagement Solutions's Declare application along with the application databases reside on high powered servers within defined security level segments. All hardware devices within Civica UK Ltd's live hosting environment are duplicated to facilitate a highly redundant and resilient network.

Market leading security appliances at the perimeter provide rich stateful inspection of traffic flows protecting the application servers from malicious activity. The Intrusion Detection and Prevention Systems detect suspected efforts of network intrusion by using specially designed intrusion detection parameters and automatically block these attempts at security breaches.

All servers and network devices follow the CIS (Center for Internet Security) guidelines which help reduce the attack surface through implementing best practise security configurations.

The application servers are load balanced to enhance performance and improve availability. Should one of the servers fail the other will automatically service the load until the failed server is returned back to its functioning state.

The database servers are hosted within an isolated network forcing database requests to be inspected a second time by the firewall. All databases, using live replication software, are replicated to a secondary offsite server which provides redundancy and disaster recovery *(explained in section 2)*. The databases are further protected with database level passwords and access-granting security features.

Weekly scans ensure our web sites, servers, and security devices are free of known vulnerabilities. It also determines whether our site passes the SANS Top 20 Internet Security Vulnerabilities list as defined by SANS, the FBI and FedCIRC.

Quarterly scans are carried out by an Approved Scanning Vendor (ASV) ensuring that the systems and Internet facing IPs adjacent to these systems are in line with PCI Compliance.

1.2. Secure Hosting

Civica: Engagement Solution's hosting environment is contained within the secure facilities managed by one of the world's leading communications providers. These facilities are in line with UK Government's exacting security standards:

- *Card key entry systems* – the facility provides a secure environment that allows only authorized users to access the resources they need.

- *Diesel-powered emergency generators* – the site is able to provide uninterrupted power in the event of an electrical power outage.

- *Climate-controlled environment* – sensors help maintain climate conditions at the facility to prevent any problems that may be precipitated by changes in temperature, moisture, etc.

- *Secure cabinets* – within the facility, secure, tamper-resistant storage cabinets further protect the data.

- *Redundant Internet connections* – redundant connections provide assurance that breakdowns in Internet connections do not disrupt online processes.

- *24-hour security* - the hosting facility provides 24x7 monitoring, maintenance, and security, including video camera surveillance and dry fire suppression.

1.3. Data Access

The security, integrity, and confidentiality of data is protected with a limited number of Civica: Engagement Solutions' employees allowed access to the databases. Accessing the production databases requires passwords from each member of the technical teams.

1.4. Application Development

Application development proceeds through four discrete levels: *Programming, Testing, Client Review,* and *Production.*

Change Control manages the transition of the application through the four levels of the development process. This ensures division of work and minimizes the potential for collusion.

- *Programming* develops the application and has access only to test data.

- *Testing* is performed by the QA department. The QA department has read-only access to the QA machines. Strict exit criteria must be passed for an application to be considered acceptable and to be moved to the next level.

- *Client Review* is the final phase of testing, where the final application build becomes production version of the application for the client to review.

- *Production* oversees the hosting facility and is responsible for the security of the application. *Production* is the only group to use real data.

SECTION 2

2.1. Application Architecture

The product is designed from the ground up as a secure, high-availability, n-tier internet-facing application.

The software is structured to take advantage of current mainstream Microsoft .NET technologies deployed in a secure Windows server-farm environment with redundancy and fail-over designed in.

The product does not require the installation of any software on the user's systems. A standard browser is all that is needed.

2.2. User Interface Layer

The user interface layer utilises the Declare system built in ASP.Net V4.

2.3. Presentation Layer

The Declare presentation layer runs on Web Servers.

2.4. Data Layer

The data layer is implemented by connecting to an SQL Server database.

2.5. Communication Security

The security layer is handled by ASP.Net in-built authentication and SQL Server stored procedures.

2.7. Path taken by Secure Session through Web Hosting Environment

Figure 1 displays and explains the logical path a secure web session takes when entering the hosting network.

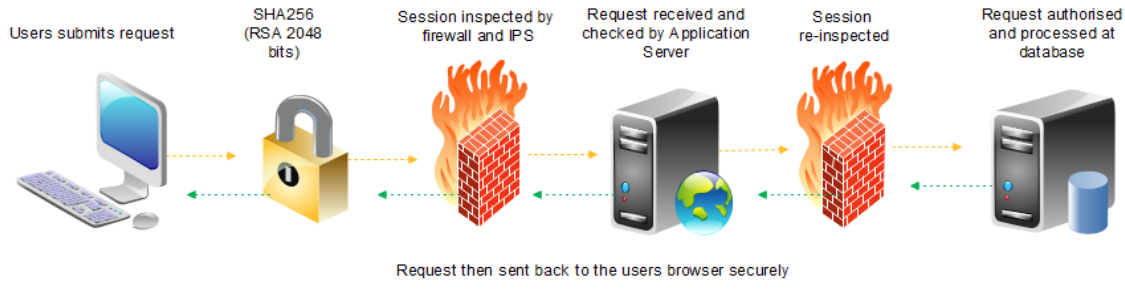

Figure 1

SECTION 3

3.1. Disaster Recovery

Civica: Engagement Solutions have implemented a disaster recovery plan to facilitate Web Service continuity should a major catastrophe take place at the Datacenter. The procedure would involve all Web Services being redirected to Divisional Head Office (DHO) where a 'skeleton network' would then service all incoming requests. This environment has redundant internet connections via two separate Points of Presence.

This would allow DHO to make the necessary arrangements to recover the Datacenter, or in worst case scenario, implement a new hosting environment at one of our service provider's alternate locations.

3.2. Web Hosting and Disaster Recovery Base Design

Figure 2 displays DHO's live hosting infrastructure along with the skeleton network hosted at the failover site.

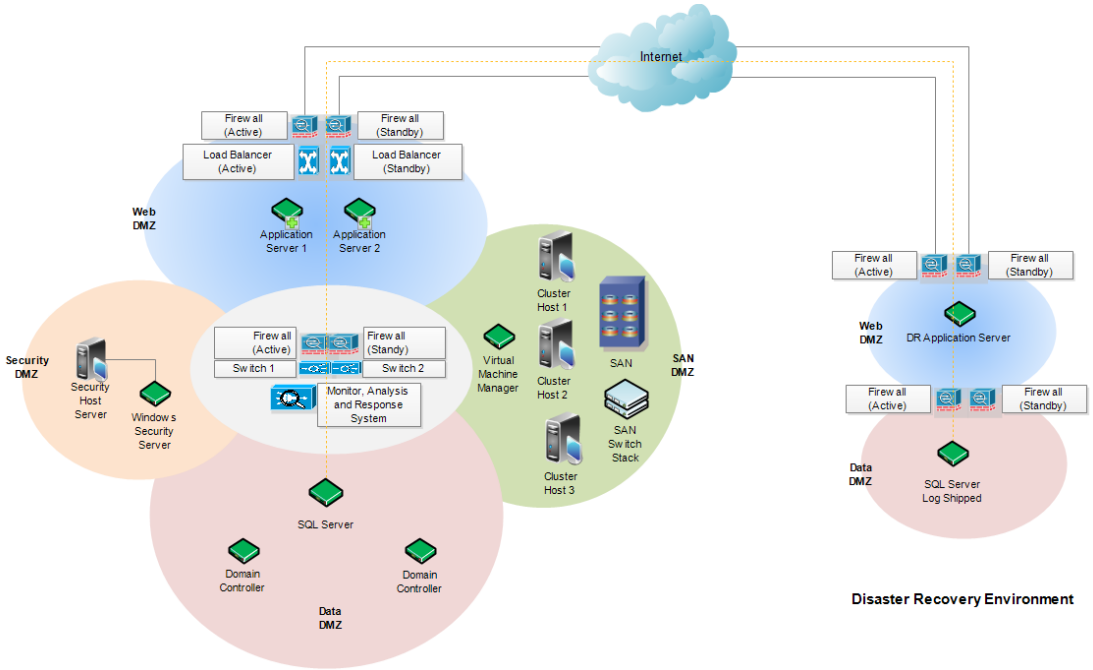

Figure 2

SECTION 4

4.1. Web Services and Network Monitoring

Civica: Engagement Solutions have implemented several 24/7 monitoring services in order to proactively counteract and eliminate downtime.

Third party Web Site Performance Monitoring provides us with graphical overviews including Total Response Times and Overall Uptime Status. This monitoring platform takes place from three separate locations namely, London, New York and Los Angeles where thresholds within the monitoring have been set. Should they be exceeded, engineers are automatically notified via text message and email.

Further to that, we have implemented our own internal monitoring, not only on Web Service responses, but all critical systems within the network. Again, should thresholds be exceeded engineers are notified via text message and email.

SECTION 5

5.1. Summary

Civica: Engagement Solutions utilizes industry best practice, third party software and multiple levels of security to safeguard its client's information. Civica: Engagement Solutions strives to meet the highest levels of Web Service availability possible through its resilient and fully redundant network.

Authors: Nick Goodman
Hiran Wijeratne
Damian Coverly

written: 20/09/19
Last reviewed: 20/09/19