My Signage Portal CMS Server Security Statement

Revision date: 16/05/2025

Cloud Server:

The CMS is hosted on an **Amazon Web Services (AWS) server** https://aws.amazon.com, using an **SSL encryption** method and an **ISO 27001 Security Certification. Nexpose & OpenVAS Vulnerability** scan takes place monthly, as well as the operating system (OS) for the server being updated and patched monthly by **AWS**.

The cloud uses '**AWS: EBS Provisioned IOPS storage (SSD)**', which securely protects all saved data and keeps a continuous backup on the server. This is secure storage system and the second largest data centre in Amazon's global infrastructure. The server runs Red Hat Enterprise Linux 7, which is consistently kept up-to-date with the most recent and highest version of the OS. **Red Hat Enterprise Linux 7** is used instead of Microsoft Windows because of the much smaller quantity of vulnerability issues and known viruses on the Linux system. The Linux OS is also more reliable and secure when preventing malicious software making it much better at handling important data on a large system. The server also features a **Cloud Watch system**, which monitors the status of the server in real-time and sends updates to the engineers every minute. We have in place a scalable computing power system, allowing us to expand the server to suit our requirements if higher demands of data transfer are needed.

The network administrators for the content management system (CMS) are fully trained engineers, and have a minimum of 4 years' experience in our operations. Our very own development team also help maintain the server and processes. There is a locked IP that allows only our engineers to maintain and manage the server through a secure port.. This is connected to using an SSH server with the terminal emulator PuTTY. Our development team also help maintain the server and have a great understanding of the processes involved.

Security:

The cloud data has to go through Amazon's **Key Management Service (KMS)** https://aws.amazon.com/kms/ before any data has been transferred to the screen/player. The KMS is a managed server that enables us to easily create and control the keys used for cryptographic operations. The service provides a highly available key generation, storage, management and auditing solution for us to encrypt data within the CMS. Events that breach security are logged and analysed by the KMS in real-time. Amazon's KMS monitors all the system resources and protects the confidentiality and integrity of data. KMS uses FIPS 140-2 validated Hardware Security Modules (HSM).

Amazon's EC2 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) offers key features to help protect EC2 instances. Any breaches are logged and analysed by the IDS system. These monitor the inbound and outbound data, as well as the system resources. Any attempted intrusions will also be logged by the IPS. There are also engineers on standby 24/7 to respond to any vulnerability alerts. All security events are logged and reported. Any suspicious attempts are also reported immediately by AWS. The engineers and developers also have IT server maintenance training and server training, which is provided quarterly.

There are multiple security hardening procedures in place, such as trimming and restricting remote services on the AWS Server and minimisation of services the server is running. The CMS is also the only thing that the server hosts so there are no other processes being run on the server. It also features an **encrypted security key**, and uses **secured packages** when sending and receiving information. Each screen/player that is connected to the CMS will have a **security identifier**, which is unique for each screen/player. There is a **watchdog system** in place on the screen/player itself that will react to unwanted data or activity and begin restoring configurations from the server once abnormalities are detected. Finally, **two separate firewalls** are in place in front of all data going in and out of the server.

To keep accounts secure on My Signage Portal a **CAPTCHA** authentication system is in place to protect spam and password decryption. When logging into an account there is a simple test that requires the user to type out the exact numbers shown into a field that differentiates between human and computer access.

Ports and Protocols:

The server connects to the screen/player using the **HTTP+HTTPS web protocols**. HTTP is standard, but HTTPS is there for users that require it. If the HTTPS option is used, **this will encrypt the data both in and out with real-time generated security keys**, preventing any information being intercepted by others. On this same protocol, the server will transfer files via a **packet system**, and require the **screen/player to return a message** to the server every time it receives a part of the packet, allowing the next part to be sent.

Port **80 (or 8001)** using the HTTP protocol is used to **download media** from the server as well as configuration files. Port **4700** on the **UDP protocol** is used to send **remote commands** to the screen/player from the server. Port **4701** on the **TCP protocol** is used to let the screen/player **log into the server**, and also **register heartbeats** for monitoring purposes. Finally, ports **16732 and 16733** on the **UDP protocol** are used for local synchronisation of the content of multiple screens/players.

MY SIGNAGE PORTAL

MY SIGNAGE PORTAL ← **aws**

Scalable Server Computing Power:
Allowing us to expand the server to suit our requirements

Red Hat Enterprise Linux 7:
All software is running on the most up-to-date level operating system.

Hosting platform:
Amazon Web Service

Security Certification:
ISO 27001 Certification

Encryption:
SSL

Network Administration:
The network administrators on the CMS are trained engineers and have two years or more experience in our operations. The development team is also participating in the development and maintenance processes.

Remote Administration:
Multi-factor authentication is used for the remote access.

CloudWatch:
The real-time status of the server is being sent to our engineers in one minute time intervals.

EBS Provisioned IOPS Storage (SSD):
Media server is located at the second largest data centre in Amazon's global infrastructure.

AWS KMS (Key Management Service)

Security Events:
Events which breach security are always logged and analysed by our IDS system in real-time

AWS KMS:
AWS KMS is a managed service that enables us to easily create and control the keys used for cryptographic operations. The service provides a highly available key generation, storage, management, and auditing solution for us to encrypt data within the CMS.

IDS + IPS
- Monitoring on the inbound and outbound data packages.
- Monitoring the system resources.
- Logging all security events and reporting suspicious attempts.
- Application level inspection and filtering.
- Engineer to respond to vulnerability and intrusion alerts 24/7

Security Testing:
Nexpose + OpenVAS scans monthly basis

Double Security Firewall:
Built two separate layers of firewall in front of all data.

Security Hardening:
- Remote services on network - trimmed and restricted using tools on AWS.
- Services reduce to minimum of what CMS needs including ports and services.
- CMS is the only web application the server hosts.
- Encryption security key and secured packages when sending information. Hardware has identifier and security which is unique to each screen.
- Screens are trimmed to minimum to avoid vulnerabilities.
- Hardware has 'watch dog' built into system, monitoring digital signage and screen. Any unwanted data or activity will kick 'watch dog' in and the screen will be forced to restore configurations and will correct content from secured server.

Security Patching:
Operating system on the server is up-to-date patched. Other components are patched after the monthly vulnerability scan if applicable.

Port: 80/8001 Protocol: HTTP Function:
Downloading media and configuring files

Port: 4700 Protocol: UDP Function:
Remote control commands (stop, play, screenshots, etc.)

HTTP + HTTPS:
The Web-based content management console establishes a secure connection (HTTPS) between your device and cloud server. The data on both the in and out tunnels are encrypted based on a real time generated security key to prevent your login detail or media files intercepted by others.

Two Way Server Communication:
Our system files transfer via a packet system and requires the screen to return a message to the server every time it receives a part of the message so that the next part can be sent. We use the same port for this.

Port: 16732/16733 Protocol: UDP Function:
Local synchronisation (multi-cast)

Port: 4701 Protocol: TCP Function:
Logging into server and registering heart beat.

Watch Dog integrated onto Hardware:
A separate piece of hardware is built into the screen to constantly monitor the contents and processes on the main operating system. Any unexpected activity or data will trigger the watch dog, then the screen will be forced to restore configuration and correct the content from the secured server.

Advertising Display/ Touch Screen