Security and GDPR

Overview

Marvin XR is a **security first SaaS platform**. The core foundation of this platform is to ensure enterprise grade security for your WebAR campaigns. Core features of this platform are based on **DevSecOps model**.

DevSecOps stands for development, security, and operations. It's an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.

Marvin XR is the first WebAR SaaS platform that is 100% GDPR compliant and secure.

Environment and Data Security

- **Linux based Operating System**:

  Linux systems are rarely infected by malware such as viruses, worms etc, thereby making it as a very secure OS. As a normal user, we will never come across a situation where Antivirus software is been sold for Linux.

  When a Linux system is compromised, virus or malware will not get the root access to damage system wide. Only local files and programs of users will be affected, as the normal user will not have access permission to all the files in the system. This leads to least effect of virus in systems with Linux. As Linux users don’t have root access, it is difficult to cause damage on Linux.

- **Application Security Framework**:

  Marvin XR platform is developed based on the globally highest ranked, most secure application framework, among many. By default, it prevents most of the common security vulnerabilities like

  - Cross site scripting (XSS) protection
  - Cross site request forgery (CSRF) protection
  - Safe password hash (SHA-256 hashing algorithm)
  - SQL injection protection
  - Clickjacking protection
  - Encrypted connection

- **Containerized Architecture**:

  WebAR campaigns represents isolated containers running microservices separated from each other and the network. This includes both in transit and at rest data, since both can represent high-value targets for attackers. All container storage are encrypted with hashing algorithm to ensure their integrity, security and least possibility to transmit data in between them. Thus, if any live AR campaign, if gets compromised, will never impact any other in the system. The removal of a rogue campaign can ensure safety of the environment.

- **Auto Renewal SSL Certificate for AR Campaign**:

  SSL certificate is authorized to every AR campaign by Lets Encrypt Certificate authority to enable HTTPS.

  SSL (Secure Sockets Layer) is the standard encryption technology which establishes a secure connection between a web browser and the server. This ensures that all the data which passed during the connection remains private and encrypted. SSL is used to protect the sensitive information entered by visitors.

  To enhance security, every 60 days, the SSL certificate is auto-renewed. This minimizes the chance of further security vulnerabilities.

GDPR (General Data Protection Regulation) Compliance

- **EU Based Cloud Datacenter**:

  Marvin XR is an AWS global startup partner and its datacenter is located within EU. Location restriction ensures that all the intellectual assets and data remain inside EU arena.

- **Data Controller**:

  Marvin XR works as a data controller of its customer campaign related data. Being a data controller, it ensures that all the data remains safe inside the secure cloud infrastructure with necessary safety measures like network layers, access-control based OS and permission check for them to be accessed only by its customers and admins of the platform.

- **Data Protection**:

  The platform keeps record of all user data and does not store any personal data with which a person can be identified individually. This is to ensure inidividual data privacy.

At the same time, Marvin XR does not use any third party plugin like Google Analytics which can feed on AR campaign generated user data and store somewhere beyond the control and reach of Marvin XR and its customers. This policy is to ensure absolute control of campaign related data remains with the platform.

- **Data Deletion**:

  Marvin XR ensures that upon deleting any AR campaign, all historic and current data related to the campaign are deleted instantly without the chance of reverting back. This is to provide freedom to the customers if they choose to delete all their campaign data if they want to leave the platform. At the same time, Marvin XR cannot hold the responsbility to access, manipulate and use the data afterwards.

Conslusion

There are many more security insights built inside Marvin XR platform making it a robust and trustworthy SaaS platform for enterprises where security is the preliminary level of qualification for software adoption. It differentiates itself from the market competitors with advanced level of security that no other competitor offers today. This is the right solution for your business to start growing with WebAR experience.

Revision #5
Created 20 February 2023 19:17:15 by Admin
Updated 27 March 2024 10:49:18 by Admin