Security and Privacy in Vibe™

09.04.2018

Overview

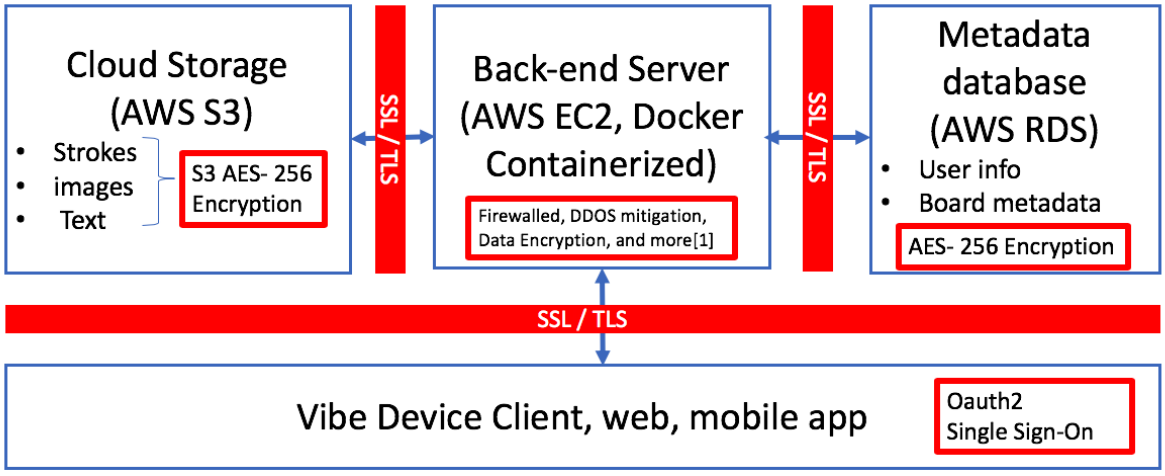
With the mission of empowering teams to collaborate, innovate and ideate in a unified canvas, Vibe is a unique all-in-one devices with customized operating system and cloud backed software. We understand that data security and privacy protection is paramount to our customers. In this paper, we explain what is under the hood of our Vibe system and how it handles user data as well as the measures we adopted to ensure the security and privacy of user data.

System Security measures

Our easy-to-use smart board software in Vibe is backed by a cloud infrastructure working behind the scenes to ensure real-time, reliable syncing, sharing and collaboration. Built by experienced system architects from Twitter and Microsoft on the world's most popular cloud infrastructure, AWS, our system is reliable, scalable, efficient and most importantly, secure.

System architecture

Vibe users can access the whiteboard drawings at any time from web, mobile devices as well as Vibe devices. All of those clients connect to secure servers to provide access and update.



[1] https://aws.amazon.com/security/

Figure 1. System diagram and its security measures

Security measures for each sub-system

Storage Servers:

The whiteboard content is stored in Amazon Web Services (AWS) object storage service called S3. It provide reliable, secure, efficient and scalable storage that millions of applications are already using. The data is further encrypted by the one of the strongest encryption method, AES-256, with keys automatically managed by S3 services. As the last line of defense, we never store your full content into a single image file in S3, but instead

break it into a series of stroke, text and images and scattered into the storage. The full image is only composed on the client side.

Metadata servers

We store users' account information, team's information and other board related metadata into mySQL database provided by AWS. User information includes username, email and company info. Team information includes its members, company website and etc. Board metadata includes its creation time, last modified, content URL to S3 and also members list. All information is as well encrypted by AES-256.

Backend servers:

The backend servers are responsible for retrieving content, syncing whiteboard change and also manage user's privilege to accessing content. It communicates with both storage servers and metadata servers via HTTPS with SSL/TLS.

We also implementing perfect forward secrecy with generating new token for each sign-on instance. In this way, our private SSL key can't be used to decrypt past Internet traffic.

By using AWS EC2, we enabled industry-standard protection techniques, including firewalls, network vulnerability scanning, network security monitoring, and intrusion detection systems to ensure only eligible and non-malicious traffic is able to reach our infrastructure.

As an extra line of defense, the service are contained in docker container so we can easily provide further separation between different customers.

Clients:

Vibe device clients include Vibe board, web app and mobile app. All clients communicate with server through HTTPS with SSL/TLS.

As a way to reduce the risk of keeping user authentication data, we only support Single Sign-on from trusted identity providers which supports both authorization and authentication (Oauth2 + OpenID), namely, Google, Microsoft and Slack. In this way, no user login information is ever transmitted or stored in our system.

Security as company value

Trustworthy is on top of our company values. At Inlight Interactive, we understand that building up trust with our customers is critical to our company's success. Ensuring Data-security and privacy protection are two pillars of trust building. We are continually improving the security, confidentiality, integrity, availability, and privacy of the Vibe system. As we are currently a small startup, the only way to ensure customer's data security is to

adopt drastically aggressive measures, even at the cost of losing engineering efficiency. Our current security policy includes,

- As Inlight is distributed in a few cities in China and USA, we make sure that all user related data are stored exclusively in US territory.
- Developers in China do not have access to user data, a developer server with mock data are used for development and testing purpose
- Only C-level managers have the keys to access board content data stored in S3, all of whom have enabled two factor authentication and encrypted their develop machine.
- Upton receiving the device, we will sign a non disclosure form with all our customers to guarantee their data are protected from leaking.
- Only C-level managers and marketers have the key to access user profile data stored in SQL server, they also will sign special NDA and abide by our privacy policy.

Privacy Policy

At Inlight, we value your privacy and the protection of your personal data. We use your Personal Information only for improving Vibe Services. By using the Vibe product, you agree to the collection and use of information in accordance with this policy.

Information collection and use

Account information.

We collect, and associate with your account, the information you provide to us when you do things such as sign up for your account, upgrade to a paid plan (like your name, email address, phone number, payment info, and physical address). In no cases we will sell these information to advertisers or other third parties

Usage information

We collect information related to how you use the Services, including actions you take in your account (like sharing, editing, viewing, and moving boards or folders, apps launched on the devices). We use this information to improve our Services, develop new services and features, and protect Vibe users. This Log Data may include information such as your computer's Internet Protocol ("IP") address, browser type, app version, the pages of our Site that you visit, the time and date of your visit, the time spent on those pages and other statistics. These information will be kept anonymous and will not be shared outside the development and marketing team.

In addition, we may use third party services such as Google Analytics that collect, monitor and analyze this.

Communications

We may use your Personal Information to contact you with newsletters, marketing or promotional materials and other information.

Cookies

Cookies are files with small amount of data, which may include an anonymous unique identifier. Cookies are sent to your browser from a web site and stored on your computer's hard drive.

Like many sites, we use "cookies" to collect information. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Site.