Secure Tier Server

upperity

ABOUT
UPPERITY

Upperity is a group of solutions developed by Mercues Innovations sezc, a Cayman Islands company with offices in Montreal, Canada and in USA, through its partner FlightStart Solutions LLC. Upperity has positioned its brand in two specific industries, security and (regtech) Regulatory technology.

Business model

Upperity works as a registration form and login portal that can be incorporated into web and desktop applications. Its user management and authentication services provide KYC process combined with SaaS and BaaS infrastructure to secure personal and confidential customers information and facilitate the use of blockchain technology to stay compliant with privacy laws.

Secure Tier Connection

Upperity Secure Tier Connection is an application that can be installed by the user on its mobile device and computer to create personal secure connection to 3rd party servers.

The application connects Upperity personal's smart contract with the Secure Tier Server and makes the user undetectable from any third party. The user cannot leave anything behind on their mobile device or computer and hackers cannot intercept and steal anything. Once the session ends, the virtual environment is completely destroyed and all data ceases to exist.
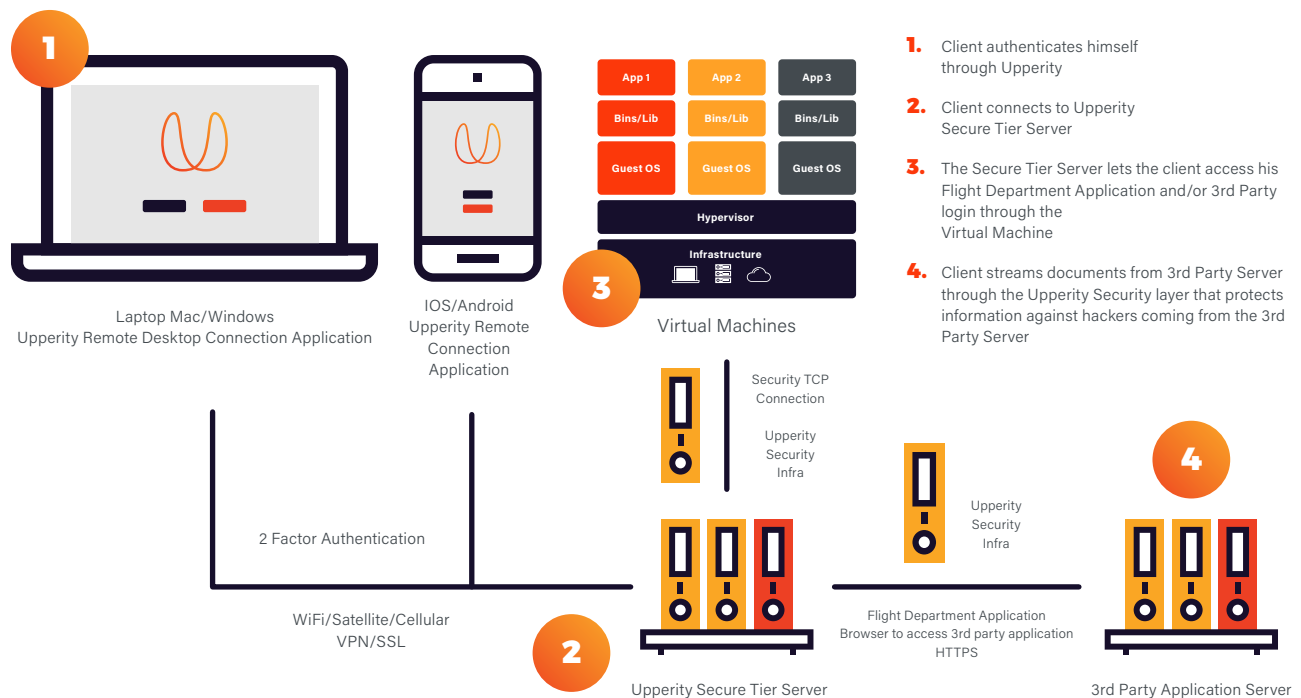
As you travel

Upperity helps companies and their IT department to keep their users safe, while on the road outside their own IT infrastructure by creating a extra secure on demand environment to connect on 3rd party servers and transfer data, without the risk that hackers can monitor or hijack entire management sessions or inject their own data into the session, add their own code to the modem, send links and execute codes, create fake passwords, capture cookies and alter onboard guidance for cyber secure satellite terminals.

Each time a user connects to a third-party server, Upperity creates an on-demand virtual environment based on the user's profile which is provided by the user's personal smart contract directly on Upperity's blockchain. This virtual environment cannot be audited or monitored neither from the inside nor from the outside. These environments can only be created and destroyed.

How it works

Clients embed the Upperity solution into their web and software applications allowing customers to register in complete confidence by keeping sovereign their personal information. The customer's information passes through the client application only when the customer authorizes it and only for the time required to process the information to execute the intended function. When the customer logs out, no information is kept in the client's database. Furthermore, there is no possibility of using the client application if the customer is not registered and associated with the entity's smart contract. This removes the risk of identity theft and fraud because Upperity takes the responsibility to keep this information and smart contracts safe. Upperity temporarily stores customers information, actions taken during processes and their digital certificates in smart contracts within a decentralized blockchain. No information will be stored in database reducing to zero the risk of theft.

1 Laptop Mac/Windows
Upperity Remote Desktop Connection Application

IOS/Android
Upperity Remote Connection Application

App 1   App 2   App 3
Bins/Lib   Bins/Lib   Bins/Lib
Guest OS   Guest OS   Guest OS
Hypervisor
Infrastructure

3 Virtual Machines

1. Client authenticates himself through Upperity

2. Client connects to Upperity Secure Tier Server

3. The Secure Tier Server lets the client access his Flight Department Application and/or 3rd Party login through the Virtual Machine

4. Client streams documents from 3rd Party Server through the Upperity Security layer that protects information against hackers coming from the 3rd Party Server

2 Factor Authentication

WiFi/Satellite/Cellular
VPN/SSL

Security TCP Connection

Upperity Security Infra

2 Upperity Secure Tier Server

Upperity Security Infra

Flight Department Application
Browser to access 3rd party application
HTTPS

4 3rd Party Application Server

For end users who want to connect to a third-party server securely

State of the art technological security components

The end user downloads the Upperity App and installs it on their mobile device or desktop computer. The user authenticates itself through the Upperity App. Upperity blockchain services, with a two factor authentication system will connect the user, based on its personal information stored in the Upperity blockchain, to a virtual environment created on demand in the Secure Tier Server. Once the virtual environment is created, the end user will be able to stream data from a 3rd party server in complete confidence and out of range of an hacker. The hacker does not know when and where the connection has taken place and for how long. At the end of the session, the virtual environment is destroyed.

The Secure Tier Server offers a complete security environment on demand monitored by strong IDS (Intrusion Detection System), IPS (Intrusion Prevention System) and firewalls and other proprietary security solutions. We monitor in real time all network packets you send and receive to detect malicious activity. We monitor all suspicious packets and take immediate action before it goes to your virtual environment. A high Security firewall blocks access to the network and logs any attempt in the blockchain. Upperity blockchain services log all suspicious activities so hackers cannot erase their actions to stay undetectable. We have designed multiple customized security tools to enhance the security even more on our Secure Tier Server by interacting with Upperity blockchain services in a novel way.

Upperity's Secure Tier Server relies on different components to protect our users from being hacked.

The complete security offering in a nutshell for a monthly subscription, eliminates the start-up costs (infrastructure, specialists, software, hardware, and consultants) and operational costs of a self-hosted environment, PKI and blockchain.

For end users who want to connect to a third-party server securely, the Secure Server Connection App removes the risk, for a fraction of the price, hackers that monitor or hijack entire management sessions, they inject their own data into the session, add their own code to the modem, send links and execute codes, create fake passwords, capture cookies and alter onboard guidance terminals.

Upperity works with FlightStart Solutions to create distinctive benefits for its customers

01.

Upperity creates a digital identity with Personal Identifiable Information that is NOT stored in a database and protected by digital signature certificates (encrypted).

02.

State-of-the-Art environment compliant with SOC 1, SOC 2, PCI-DSS, securely monitored by strong IDS (Intrusion Detection System), IPS (Intrusion Prevention System) and firewalls and other proprietary security solutions especially designed for this kind of environment. This allows the corporate users to interface with third party servers securely out of the rang of hackers.

03.

Resulting in the end user to use an environment that does not require a special training and does not change the way people interact with their own applications.

upperity

Mercues Innovations SEZC

Strathvale House
2nd Floor,
90, North Church Street, POBOX 10315
Grand Cayman, KY1-1003
Cayman Islands

info@upperity.com