import.io

Import.io Security Policies

Product Security

Product security is of paramount importance at Import.io. Import.io uses a software development lifecycle in line with general Agile principles. When security effort is applied throughout the Agile release cycle, security oriented software defects are able to be discovered and addressed more rapidly than in longer release cycle development methodologies. Software patches are released as part of our continuous integration process. Import.io performs continuous integration. In this way, we are able to respond rapidly to both functional and security issues. Well defined change management policies and procedures determine when and how changes occur. This philosophy is central to DevOps security and the development methodologies that have driven Import.io adoption. In this way Import.io is able to achieve extremely short mean time to resolution for security vulnerabilities and functional issues alike. Import.io is continuously improving our DevOps practice in an iterative fashion.

Physical Security

The Import.io production infrastructure is hosted in Amazon Web Services (AWS). Physical and environmental security related controls for Import.io production servers, which includes buildings, locks or keys used on doors are managed by AWS. “Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.”

Corporate Security

Import.io recognizes the diminishing utility of perimeter as concerns modern network security. Once that perimeter is breached services reliant on network security guarantees quickly fall. As such Import.io leverages internal services that require transport level security for network access and individually authenticate users, commonly by way of a central identity provider and leveraging two factor authentication wherever possible.

Secure Communication

All data transmitted between Import.io and Import.io users is protected using Transport Layer Security (TLS) and Hyper Text Transfer Protocol Secure (HTTPS). If encrypted communication is interrupted the Import.io application is inaccessible. Import.io does not “fail open.” Import.io is careful not to log sensitive values in clear text.

Customer Data Storage Location

Import.io service data currently resides in the United States of America and primarily in the state of Virginia.

Data Retention

For Service users, we will retain your personally identifying information (PII) for as long as your account is active or as needed to provide you access and use rights with respect to the Service. In addition, we may retain and use your information as necessary to comply with our legal obligations, resolve disputes and enforce our agreements.

Gathering of Personally Identifiable Information (PII)

Certain visitors to the Website and Service choose to interact with Import.io in ways that require Import.io to gather personally identifiable information (PII). The amount and type of information that Import.io gathers depends on the nature of the interaction. For example, when signing up for a trial of the Service, we may ask a user to provide the user's name and the name of the user's company, as well as an email address and telephone number where we may contact the user and/or another representative of the user's company. Each user is also expected to provide a username and password that, along with other information, we use to create and administer accounts. In each case, Import.io collects such information only insofar as is necessary or appropriate to fulfill the purpose of the visitor's interaction with Import.io.

Import.io does not disclose PII other than as described in the Import.io Privacy Policy. In addition, visitors can always refuse to supply personally identifying information, with the caveat that it may prevent them from engaging in certain activities.

Customer Data Access

A limited number of Import.io employees have access to customer data via access controlled and logged mechanisms. Technical operations employees have access to the raw service data storage. This access requires using a management VPN, authentication via public key and two factor authentication. Access to the staging and production management infrastructure is strictly logged. All other employees are prohibited from accessing customer data.

Patching

Servers in the production environment receive software patches released through our continuous integration process. Patches that can impact end users will be applied as soon as possible but may necessitate end user notification and scheduling a service window.

Single Sign On (SSO)

End users may log in to Import.io using an Identity Provider, via the Facebook, Google, Github, or LinkedIn Open ID service. These services will authenticate an individual's identity and may provide the option to share certain personally identifying information with us such as your name and email address to pre-populate our sign-up form.

Disclosure

If you believe you’ve discovered a bug in Import.io’s security, please get in touch at security@import.io and we will get back to you within 24 hours, and usually earlier. We request that you not publicly disclose the issue until we have had a chance to address it.