cadasio

Security Policy

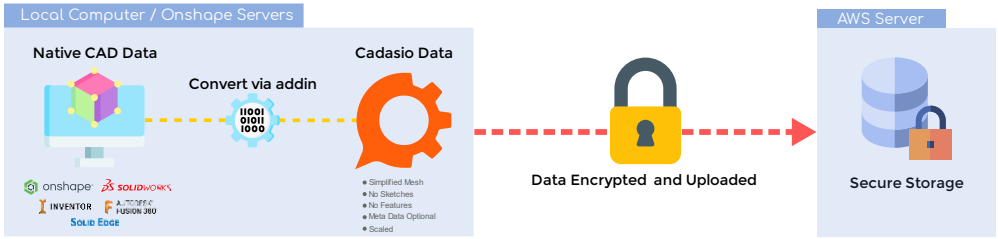
Updated 18/09/2021

We take security seriously at cadasio. We understand how important data protection is to our customers and we work hard to maintain your trust. To help you feel comfortable using our software we aim to be as transparent as possible about our data management practices.

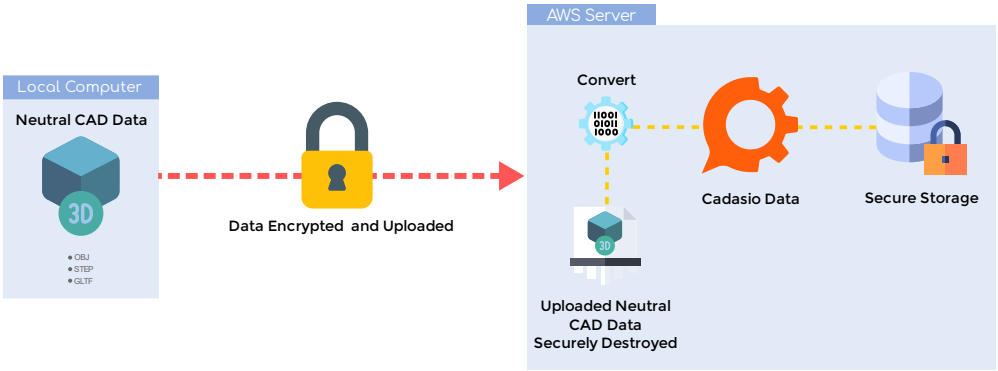
3D Data

We only ever work with mesh display data. The sketches and features used to create the model are of no interest to us. Your original CAD files are converted to our own format and encrypted. If you use one of our addins, the conversion takes place on your machine (or on the Onshape servers), and it is only the converted files that are uploaded securely to our servers. If you upload via our website, then the conversion takes place on our servers and as soon as it has been completed your original data is discarded securely.

Addin Data Flow



Website Upload Data Flow



Encryption

We apply the most advanced encryption technology publicly available to secure data. We encrypt all data at rest and all network traffic, including on payment pages, and into and out Amazon Web Services (AWS).

Hiring Policy

We only hire people with exceptional track records and references to be part of our team. We provide extensive internal and external training opportunities to all of our developers. Our employees work closely with each other in crews and teams, leaving no single employee alone with confidential and critical knowledge.

Hosting

We partner with an industry leading hosting provider to create a redundant and reliable hosting infrastructure. We host our data on Amazon Web Services (AWS) located in the United States.

Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure which is trusted by over a million well known organisations. AWS data centers are housed in nondescript facilities, and physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and escorted continually by authorized staff.

If you'd like to learn more about AWS security practices, please check out these links:

ISO Global Certification:

Service Organisation Controls Report

AWS Customer Case studies

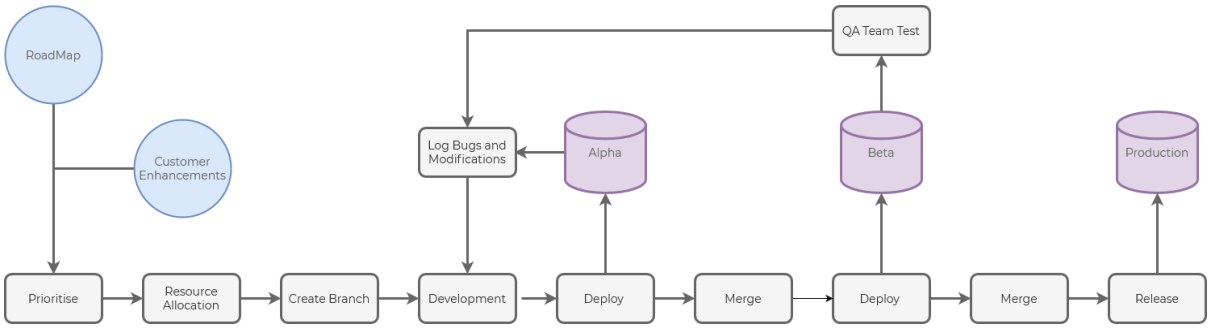
We make frequent automated backups of customer data. We store backups in a redundant way and test our recovery frequently to reduce the likelihood of data loss and minimize downtime in a large-scale disaster. We have built redundancy into all our services to eliminate single points of failure in our infrastructure.

All cadasio services are redundant across several physically isolated and resource independent availability zones. That ensures multiple data centers can go offline simultaneously while we continue to provide customers with a great experience.

We use AWS CloudFront to efficiently serve content globally. CloudFront has numerous locations around the world, which lets us speed user access to content.

Engineering and Quality Assurance

We develop all software inhouse using GitHub as our code source repository. Our team develops software and conducts code reviews in local repositories using pull requests. Then, developers publish to our alpha staging environment in protected branches. Once the development has progressed sufficiently the branch is merged and then published to a Beta environment for QA and business stakeholders to test. Only once all tests have passed then it will be released onto the main website, usually at the weekend at a time when our servers are quiet.



Disaster Recovery and Incident Management

Our team is prepared to respond to any emergency or interruption. We have a simple process we follow to make sure we communicate with anyone who's affected and do everything possible to prevent similar incidents from happening again. During any outages, we'll post updates on all our social media channels so please subscribe to ensure you receive notifications.