SECURITY OVERVIEW

Hudu Security

At Hudu, security is the primary concern for all development endeavors. Security is not a sitting target, and we continue to actively analyze, identify threats, and remediate threats; we continue to change our threat posture based on newly identified threats. By using strong, well-documented security processes and frameworks, Hudu reduces security risk to our valued customers. As part of our software development process, we also perform rigorous code reviews to ensure we limit any security exposures. We adhere to a set of principles that emphasize designing with security in mind from day one. We build features around secure defaults and adhere to the principles of least privilege.

This document provides an overview of Hudu's threat model, including relevant security controls we have in place. Hudu utilizes several security frameworks to comply with international standards, including SOC 2 Type 2, GDPR, HIPAA and PCI DSS. This includes using end-to-end encrypted communication channels, encrypting data at rest, ensuring our internet-exposed infrastructure never persists customer secrets, capturing an immutable audit log, limiting allowed actions via user roles, and providing several strong user authentication options. We rigorously review all code changes, write abstractions to minimize mistakes, harden all deployment infrastructure, and maintain strict corporate security policies.

Infrastructure

Hudu runs in two modes -- self-hosted and cloud-hosted. Both run the same code and have similar capabilities. Self-hosted allows you to store documentation on either your own internal server or using a third-party managed, hosting service (public cloud).

All Hudu instances that are hosted by Hudu Technologies are housed behind a network-based, stateful firewall. Inbound rules limit traffic to only the necessary ports and sources. Each Hudu instance further employs an instance-specific firewall and web filter that blocks excessive traffic.

Our hosted cloud environments run on a hybrid DigitalOcean/AWS infrastructure. We utilize best-of-breed infrastructure tools to make sure that the instances we host are very secure. Our hosted environment is also SOC 2 Type 2 certified.

Monitoring

We monitor instances to ensure confidentiality/integrity/availability of Hudu services. By doing so, we are tabulating several hundred unique metrics, from various services that Hudu uses to access control, configuration, and system utilization information. If anomalous behavior is detected in any of these metrics, we preemptively send notifications to our advanced support personnel so that we may identify and remediate any issues within roughly a minute of an issue's occurrence. These issues will also be routed to our support team via Zendesk and assigned to the appropriate level of support. Outside of security and availability applications, these metrics supply valuable real-time information about Hudu services to our development team, helping us to create a more tailored and effective documentation experience.

Encryption

Hudu utilizes military-grade encryption algorithms (AES 256-bit GCM, PBKDF2) to protect sensitive documentation, alongside techniques like tokenization to make sure that your keys are safe. All traffic is encrypted with a minimum supported TLS version of 1.2. Hudu employs HTTP Strict Transport Security (HSTS) with a max-age of 1 year with preloading enabled.

Hudu utilizes HaveIBeenPwned to power dark web vulnerability lookups for our customers. In order to protect the sensitivity of passwords, Hudu converts the password to a hash and searches it via a k-Anonymity model. Padding is also added to further protect the lookups and to prevent interceptions, as it ensures that all responses contain between 800 and 1,000 results regardless of the number of hash suffixes returned by the service.

Passwords and Key Storage

Hudu utilizes strong encryption keys that are stored in AWS KMS and automatically rotated regularly, along with complex passwords. All keys and passwords are stored in an encrypted vault. We take the least privilege very seriously.

Rigorous External Penetration Testing

Hudu contracts with external third-party penetration testers to fully test the main Hudu application, our mobile app, and our other products in all security modes. In addition to a team of third-party testers, Hudu utilizes continuous active controls to test programmatically daily and report any unusual access, third-party added software and monitor our employees' software usage and controls.

Hudu Employee Access and Control

Every Hudu employee undergoes continuous security awareness training. Each employee's access to services is strictly controlled and monitored. Each employee's computer is monitored, and security policies are enforced by automation and overseen by our security team.

Web Application Security

Building a secure web application is a multifaceted challenge. As one very small step, Hudu utilizes the latest HTTP security headers. Headers alone cannot protect a web app, but they can be a valuable tool for defense in depth. Hudu employs a strict Content-Security-Policy to help mitigate XSS. Additionally, all cookies are signed, marked HttpOnly, and use an explicit SameSite value of at least Lax.

Data Backups and Maintenance of the Server

On our hosted solution, Hudu takes care of data backups and maintenance of the server. We utilize instance-level backups and database-level backups (both stored on redundant servers and data centers).

For self-hosted instances, you take responsibility for backups and maintenance. Self-hosted environments also allow you to further control your security.

In the application, we have automated backup methods (S3 bucket storage). We recommend using this as part of a multi-staged backup plan (either utilizing our backup via our hosted option, or alternative backup methods on the self-hosted).

Additional App Security Measures

Hudu utilizes features like role-based access and group structures for additional security. This means you can control (as an example) which users have access to what folders. We have tried to make this process as painless as possible -- to make it easier to secure your information.

The Hudu app itself rate-limits and detects intrusive anomalies.

Password views are audited and added to a global activity trail, along with user information, IP address, date, time, and other information.

You can roll back and gain access to passwords that have been changed.

Bug Bounty Program

At Hudu, we love working with security researchers. If a security researcher believes they have found a potential security issue in the Hudu platform, we ask them to contact us immediately. We then make every effort to analyze the reported problem and, if it is found to be a valid security issue, we also pay a bug bounty for the report. Hudu works with top white-hat hackers to identify bugs, exploits and other security issues. Any valid security exploits are prioritized over all other development projects.

Active DDoS Mitigation

At the DNS layer, for our hosted solution, Hudu monitors for traffic pattern anomalies and spikes to ensure you can always access your documentation.

Self-Hosted Data Collection

One of the main appeals to self-hosting an application is that data is kept under your control. On self-hosted, the only telemetry we send back to the "mothership" is billing-related (number of users, etc.). We do not send sensitive information like passwords, files, or documentation -- this resides on the server itself.

Support and Maintenance

Hudu offers support services for all Hudu instances. Hudu employees do not have access to your data or trusted environments. In the rare case a Hudu support agent needs to access your workplace, you will need to manually grant them access by inviting their email in the user's page. It is recommended to restrict their access to only the companies and environments that need assistance. Once the support ticket has been closed, you should revoke the support agent's access.

Certifications

Hudu maintains ongoing compliance for:

Learn More

Security and threat mitigation continue to be central to Hudu's security profile. We are committed to ongoing improvements to keep us current with evolving protocols and security procedures.

Visit our Trust Center to learn more and to download our SOC 2 Type 2 report.