



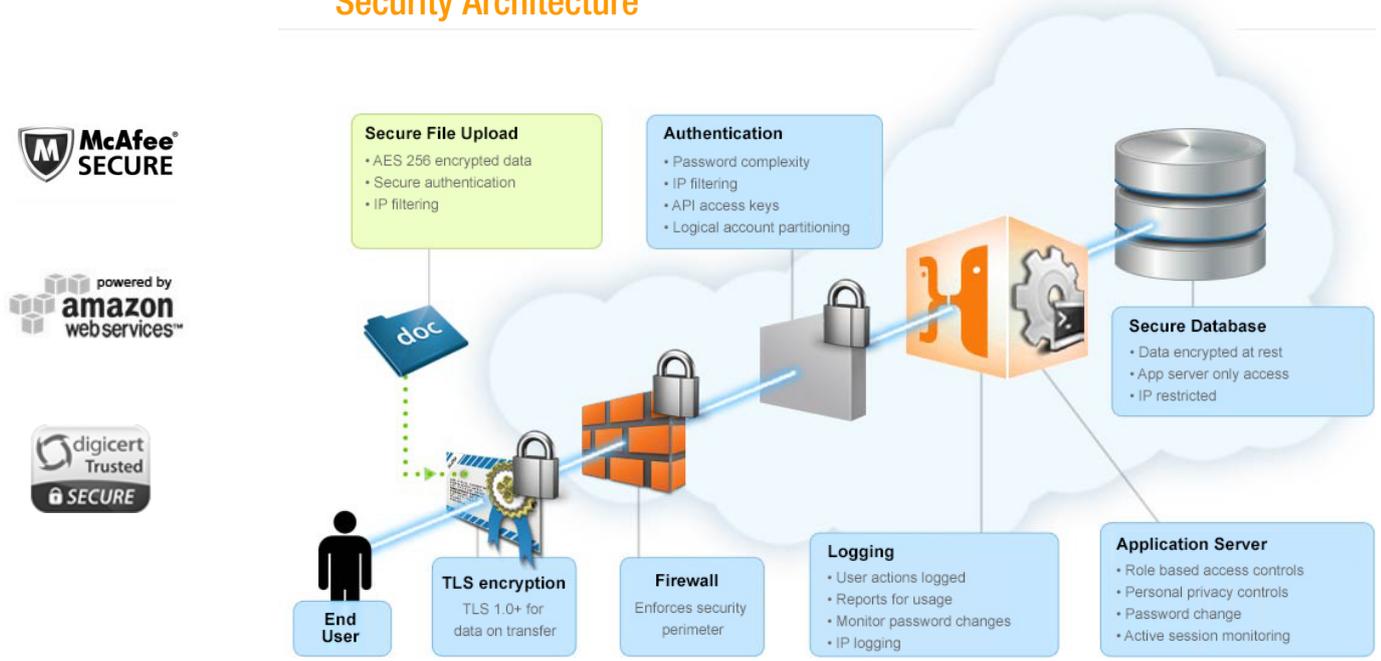
Security is our top priority

Secure, robust, SaaS platform



Some of the world's most respected blue-chip companies use Datahug to manage their business relationships and drive sales efficiency. Datahug employs leading industry standards for security at every level in order to deliver the maximum protection for our customers' data.

Security Architecture



In addition to 99.9% network availability, Datahug Enterprise customers benefit from:

- Data encryption on transfer**
Data is encrypted using TLS 1.0+ on transfer. Data can only be accessed over TLS 1.0+.
- IP Range Lockdown**
Restrict application and upload access to a specific IP range.
- Header data only**
Datahug monitors traffic rather than content.
- Strong Authentication**
We use strong password, email verification and CAPTCHA verification steps to restrict access.
- Secure Integration (API)**
Integrate with enterprise systems using our API that supports both secure credential, token based access and SSO.

- Data encryption at rest**
Password and user information is stored encrypted on the database. Enterprise customers can upload encrypted data.
- ISO 27001 data centres**
Data is stored at rest within ISO 27001 certified data centres.
- Role-based controls**
Admin, search and passive permissions.
- Administrative control**
Manage users, access, ETL uploads and user activity.
- Access logging**
Full audit trail and logging of user actions.



Best practice security at every level, for every user

Datahug commits extensive resources to the design, implementation, monitoring and maintenance of our security infrastructure. This includes:

- Highly scalable and redundant online infrastructures
- Constant monitoring of production systems
- Daily vulnerability scanning and threat assessments
- Rapid deployment of industry-standard security technologies

Together, from the point users log into Datahug to how and where data is loaded into Datahug, protection is built in at every level.

Datahug Sales
Call 1855-Datahug
www.datahug.com

Protection at the application level



- Fine grained Authentication/Authorization.
- TLS 1.0+ encryption.
- Brute force prevention (Captcha verifications, user lock-out).
- Unique, randomly-generated IDs are applied to all connection URLs.

Protection at the network level



- Sophisticated firewalls and application gateways selectively grant access to network resources.
- External penetration testing performed for system security and validation.
- Multiple internet backbone connections provide routing redundancy and high performance connectivity.
- Access by Datahug administrators only via Secure Shell.

Protection at the facilities level



- Servers hosted in ISO 27001 certified facilities, which are automatically backed up on a daily basis.
- Data centers implement ongoing audits, 24/7/365 monitoring and surveillance, on-site security staff, and strict access controls.
- Power systems feature multiple power feeds, UPS devices and backup generators ensure continuous operation.
- Environmental systems have N+1 redundant configuration to ensure fault tolerance.

Learn more

If you would like to learn more about Datahug's security features, practices and policies, contact our sales team at 1855-Datahug.