Third Party Data Security

Encryption
All data in transit is encrypted between source and destination using SSL/TLS with RSA 2048 key encryption. This includes data between the client application and the API server and the API server and the database. Encryption at rest is also applied to the database.

Data Centers
Our infrastructure is provided by Amazon Web Services (AWS), an industry standard in hosting. Like us, they treat security as a top priority. You can read about their superior visibility, control, and permissions here.

Network isolation
All network infrastructure, except the load balancer, resides within a virtual private subnet. This ensures that only the load balancer is Internet-facing.
The virtual private subnet ensures that direct communication from the client application to the server, database, and storage servers cannot be achieved, thus increasing security through layers of defense.
All links to the stored files are served using temporary time-based signatures allowing the file to be indirectly accessed only after authentication.

Firewalls
Firewalls sit between the Internet and the load balancer and the load balancer and the API server to create a DMZ between the Internet and the virtual private subnet.
A firewall is also located between the API server and the database and file storage servers to ensure that only whitelisted. IP addresses have direct access to the database and storage servers.
Middleware on the API server also provides protection by implementing additional security protocols such as automated IP address throttling and temporary IP address blocklisting.

Authentication
All database read/write actions require authentication. Authentication is processed on the server during the login handshake, and a short-lived access token is provided to the client application allowing access to authenticated API requests. The access token is renewed regularly (at less than 5-minute intervals) to remove the risk of stolen authentication keys.
The API server also undertakes role-based authentication for each request, and the API server will process only operations allowed by the specific role.
Company-based authentication ensures that a user from one company cannot access or write data to another entity.

Throttling
Repeated communication attempts to any endpoint will result in a temporary ban to safeguard against brute force and denial of service attacks.

Password Management
Passwords are never stored in plain text within the database. An individual hash and salt are stored for each user, ensuring that the compromise of one password will not allow other passwords to be obtained.
Passwords are redacted in all logs.

Development Framework
All server-side software is scanned regularly (at least monthly) to test for common and 0-day security vulnerabilities within the software framework and libraries used. All vulnerable libraries are replaced or patched to ensure the vulnerabilities are removed.
The latest framework versions are also used on client and server applications, ensuring the latest security principles are adopted.

Staff Accessibility
Employees and contractors use a password manager that enforces strong passwords. They are only authorized to access data that they need to carry out their duties.
For assistance in setting up accounts, you may grant our support staff access. This can only be granted by an administrator of your account and can be revoked at any time.

Logging & Alerts
Content Snare is continually monitored for downtime, errors, and access. Logs are maintained for analysis and debugging. Critical alerts are flagged with our engineering team immediately.

Backups & Disaster Recovery
Regular backups are distributed across several physical locations. Both files and database can be restored to a specific point over the last 14 days, or a full recovery can be initiated from a snapshot.
Our backup and recovery procedure ensures minimum service disruption in the event of a total failure.

Data Protection & Privacy
We actively monitor regulatory guidance changes to ensure we continue protecting your data.