Platform Data Security Overview

Company Name:	Su-Sea, Inc
Owner(s):	Security Team and Legal
Updated Date:	2025-05-05

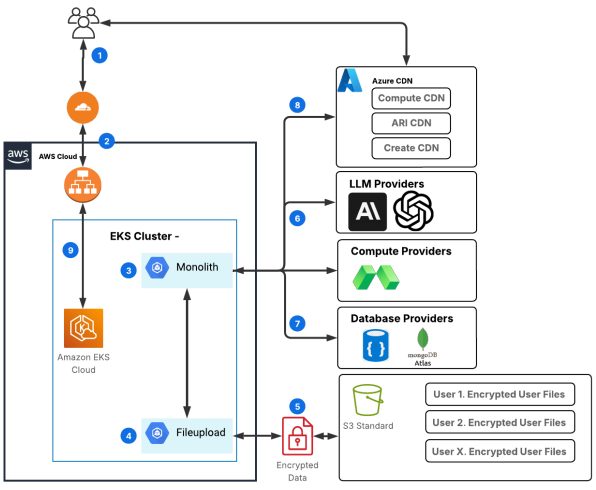
Introduction

In an era where data breaches and cyber threats are increasingly prevalent, the imperative to protect sensitive information has never been more critical. SuSea, Inc. (SuSea) is at the forefront of this challenge, dedicated to safeguarding data through innovative strategies and robust security measures. Our approach leverages the You.com (YDC) Platform and Agents, Research, and Insights (ARI) to implement a comprehensive Defense-in-Depth strategy, which integrates policy, process, and technology to create a resilient security framework.

This whitepaper outlines our commitment to data protection, detailing the methodologies we employ to enumerate, manage, and track data effectively. By focusing on isolation, access control, and data security, we aim to mitigate risks associated with unauthorized access and potential breaches. Our internal processes ensure that employees handling sensitive data are well-informed and compliant with established data handling policies, while our technical controls are designed to thwart common data leak vectors. Contractors rarely have access to internal sensitive data, and those who do, must review and acknowledge all SuSea security awareness training and policies before they are allowed to work on internal systems.

As we delve into the specifics of our data repositories, security operations, and data security measures, this document will provide a comprehensive overview of the inherent and residual risks associated with our data management practices. By articulating our strategies and controls, we aim to demonstrate how SuSea not only meets but exceeds industry standards in data protection, ensuring that our customers can trust us with their most sensitive information.

Platform Overview



This figure below provides a simple overview of the You.com Platform. **1.** the customer sends a query to the platform in an HTTPS request using TLS 1.2+. The request passes through the Cloudflare Web Application Firewall (WAF) where it is inspected for any potential security attacks.

At **2** and **3**, the request is forwarded to the Platform Elastic Kubernetes Service (EKS)

ingress and then to our *Monolith* service. **4.** If a file is being uploaded, the request is forwarded to *Fileupload* service where the content is analyzed for compatibility and security, relevant features are extracted, and it is stored. At **5,** the file and artifacts are encrypted and stored in logical paths belonging to the user.

To process the query, the Monolith will decide on the agent to use for the query. At **6,** If the platform needs to compute or analyze data, *Modal* will be used to execute the code in a sandbox. The relevant data is mounted in an ephemeral S3 path that will be deleted after the chat concludes. If the platform selects an LLM, the query will be sent to the LLM provider to get a response. Note, data is protected from retention and training when enterprise customers use approved Zero Data Training (ZTR) and Zero Data Retention (ZDR) models.

At **7,** When the response is rendered, the results are saved in a NoSQL database, and the response is returned to the customer. At **8,** If the response includes a graphic or chart, this will be uploaded to the CDN. Access to this artifact is controlled using a signed URL with an expiration.

Platform Data Inventory

The Platform data repositories consist of logically separated file storage based on customers identifiers, databases, and content delivery networks. When files are uploaded and processed, the artifacts are encrypted and stored in a users folder. For *individuals*, these files are deleted when they are removed from a conversation or the account is deleted. For *organizations*, this data may also be deleted based on an established retention policy.

Each user conversation and activity are stored in a NoSQL database. This database will include the query and response. This data will be deleted when the conversation is deleted, the account is deleted, or based on the organization's data retention policy. Other activity that is recorded in the database includes the file uploaded by the user and relevant information to help protect against unauthorized activity. This data is encrypted when it is at rest in storage.

Platform Security Operations Overview

Platform security operations are achieved through a combination of security monitoring, detection, response, and threat intelligence. Cloud, infrastructure, and application logs are monitored, and anomalous events are investigated for any potential security issues. Our team performs a table top exercise to practice incident response plans on an annual basis. Threat intelligence from trusted security vendors helps us monitor for threats targeting the platform. Additionally, these services help us identify potential vulnerabilities, abuse, or unauthorized access. All credible events are investigated and issues are investigated and remediated.

Platform Data Security Overview

Data is protected end-to-end, and the logical cloud storage is encrypted at rest. All communication into and out of the platform is encrypted using TLS 1.2 or better. The communication passes through the Cloudflare Web Application Firewall onto our platform clusters.

Customer AI conversations are stored in a database, where they are encrypted at rest. Uploaded files and artifacts are encrypted and stored in a logical container. Production data storage and databases are protected from insider access through a combination of access control, process, and policy. Strict access controls are applied to data storage and databases. These access controls limit *who* and *what* can access the data using AWS IAM Roles and Policies. *Security Groups* control the access at the network layer, limiting access to acceptable services and ports like Cloudflare, HTTPS and internal services IPs.

StrongDM is a permission access management service that we use to control who can authenticate and access customer data. Employees must have permission to authenticate to a specific role, perform multifactor authentication, and go through YDC single-sign on services to access the data. A business justification signed off by legal and security are required before employees or engineers can access the data. Internal policy also establishes what access is justified, how to obtain permission, and guidelines for accessing or using any customer data.

Conclusion

At SuSea, Inc., safeguarding data and preventing breaches is more than a priority— It is a responsibility embedded into every aspect of our operations. Through the implementation of a comprehensive Defense-in-Depth strategy, we combine robust policies, processes, and cutting-edge technologies to minimize risks and protect sensitive information. From role-based access controls and advanced encryption to monitoring and threat intelligence, our multi-layered approach ensures that data security is thoroughly addressed at every level.

The Platform exemplifies this commitment by employing logical data separation, enforcing strict access controls, and encrypting customer data both in transit and at rest. Our security operations continuously monitor for anomalies, leveraging threat intelligence and incident response exercises to stay ahead of potential threats. Furthermore, by requiring justified, limited, and auditable access to customer data, we create an environment of accountability and transparency.

Our proactive and adaptive measures significantly reduce vulnerabilities, ensuring that customer data is handled responsibly and securely. By maintaining a strong focus on prevention, detection, and response, we remain committed to earning and keeping the trust of our customers. We will continue to evolve its security practices, adhering to the highest standards

and leveraging innovative solutions to protect data. Our policies, processes, and technology, demonstrate our commitments to a secure and trustworthy platform for all users.