

Swarm: The Next-Gen Data Security Protection



Demystify Data Security

Demystify data security, privacy & compliance and make it easy for everyone. Anyone, with any skill level can implement data level protection and compliance right away.

Enabling data protection by design and default along with the six magic elements is hard for most organizations as it takes a lot of time, resources, cost and diverts the companies focus away from their primary business.



How Does It Work?

Automatically crawls your systems and drives.

Automatically discovers and indexes your unstructured data.

Enables Granular Data Level Security Controls as recommended by the law.

Delinks Data & System for further protection.

Automatically deploys CISA & FBI recommendations for ransomware protection.

Automatically detects & responds to unstructured data threats.

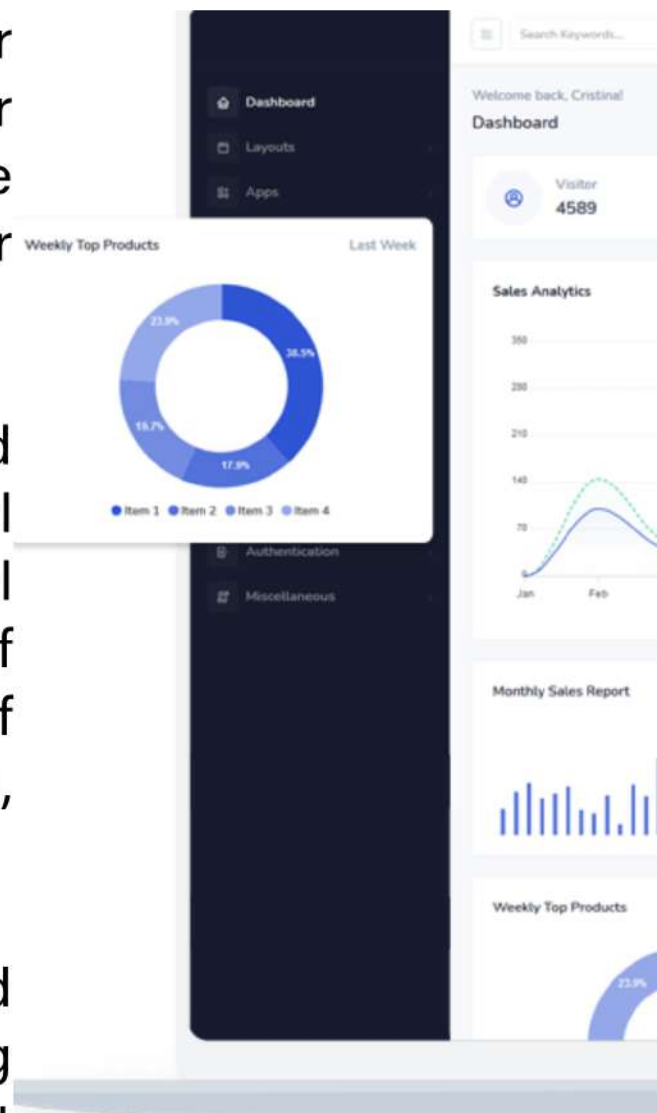
User regains full protection, control and visibility of their unstructured data at a granular file level.

User gets auditable compliance (HIPPA, GPDR, CPRA, VCDPA, NIST Zero Trust, State and Federal Encryption Laws, etc.)

Data Loss Can be Devastating

Hackers can penetrate 93% of organizational cybersecurity layers and get to their data.

- 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately.
- Organizations that are breached face reporting requirements, legal issues, financial issues, reputational issues, distrust issues, loss of property & information, loss of business advantage, ransomware, extortion, and more.
- Furthermore, the FTC has mandated that both banking and non-banking Financial Institutions must encrypt their data.



Data Security and Compliance have become too Complex

Integrating data protection and compliance with your daily business activities is a difficult process.

- *Securing data and keeping it compliant with the law has become too complex for most organizations.*
- *To make data security efficient, organizations should implement the “Data Security By Design & Default” strategy.*
- *The “Data Security By Design & Default” strategy has traditionally required a ton of money, time, attention and engineering.*
- *Organizations need to focus on their primary business, not on complex data security implementation.*



Structured and Unstructured data



Data security and compliance applies to both structured and unstructured data

Structured Data (stored in a structured database) is usually well-designed and protected by IT and Security Teams, and it makes up for only 10-20% of organizational data.

Unstructured Data (files, documents, pictures, videos, etc.) makes up for 80-90% of organizational data and is growing 3 times faster than structured data.

Unstructured data is the most vulnerable due to a breach

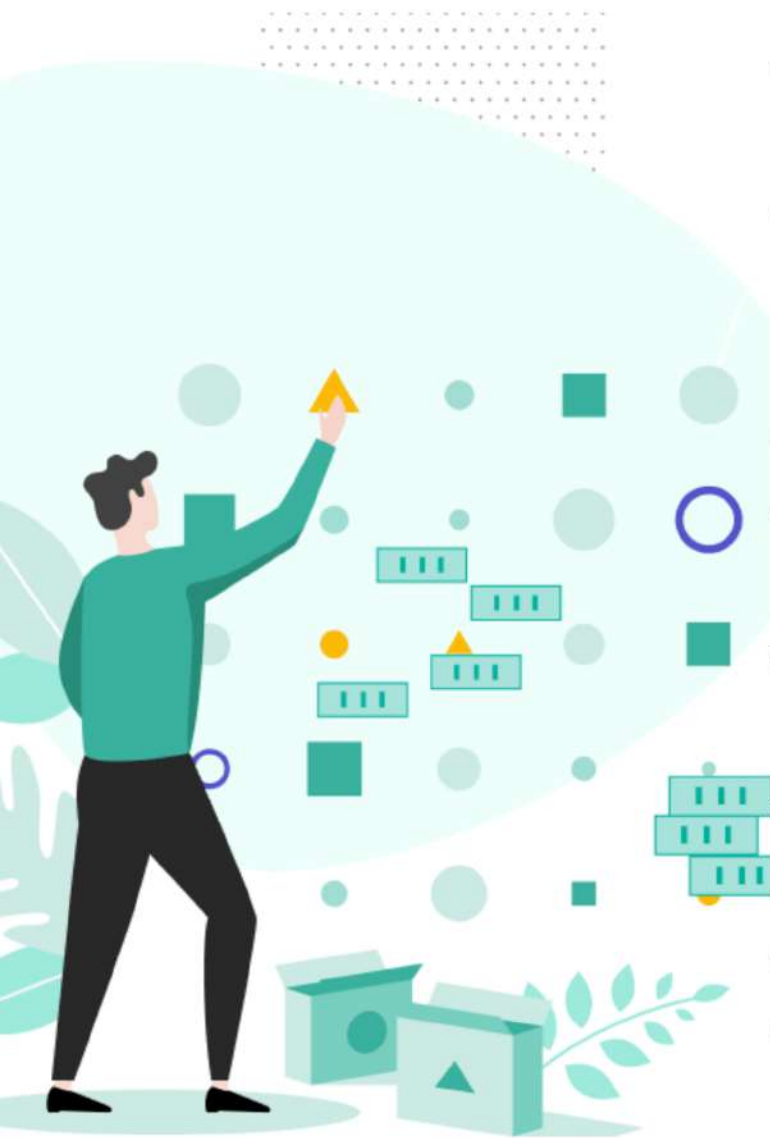
The lack of technological innovation, resources and quality user experiences make data security a nightmare.

- Unstructured data is hard to protect because it is easy to create, has low visibility, is easily moved around within and outside an organization.
- With today's connected enterprises, endpoint devices (laptops, desktops, smartphones, etc.) have become gateways into an organization's critical assets. Data protection has become more difficult in these widely distributed networks.
- Current data protection tools such as DLP's, Data Vaults, etc. are reactive, static and do not offer total protection.
- Implementing a well-designed and constantly evolving "Data Security By Design & Default" strategy is hard for most organizations as it takes their focus away from their primary business and increases costs.

Current Technology Challenges

Hackers have developed malwares that exploit weaknesses and get to your data

Current data security solutions:



- Depend extensively on humans
- Are expensive, complex and time-consuming to deploy and maintain
- Hinder user experience
- Are built to monitor rather than protect
- Fail to protect unstructured data
- Focus on complex rules instead of the data itself
- Have no Data Visibility
- Do not provide coverage for legal and compliance concerns