SafeLiShare

Empowering Zero Trust Confidential Collaboration

Overview

As of today, interest in zero trust security is largely driven by government mandates, ransomware attacks and the needs of a hybrid workforce. Different governments and parts of governments are creating mandates for some version of zero trust.

Zero trust forms a guiding principle for security strategies that shape an architecture, and that can improve security posture and increase cyber-resiliency.

Emerging and changing regulatory requirements are pushing enterprises to look for data protection and encourages organizations to create commercial data value on top of the protected baseline.

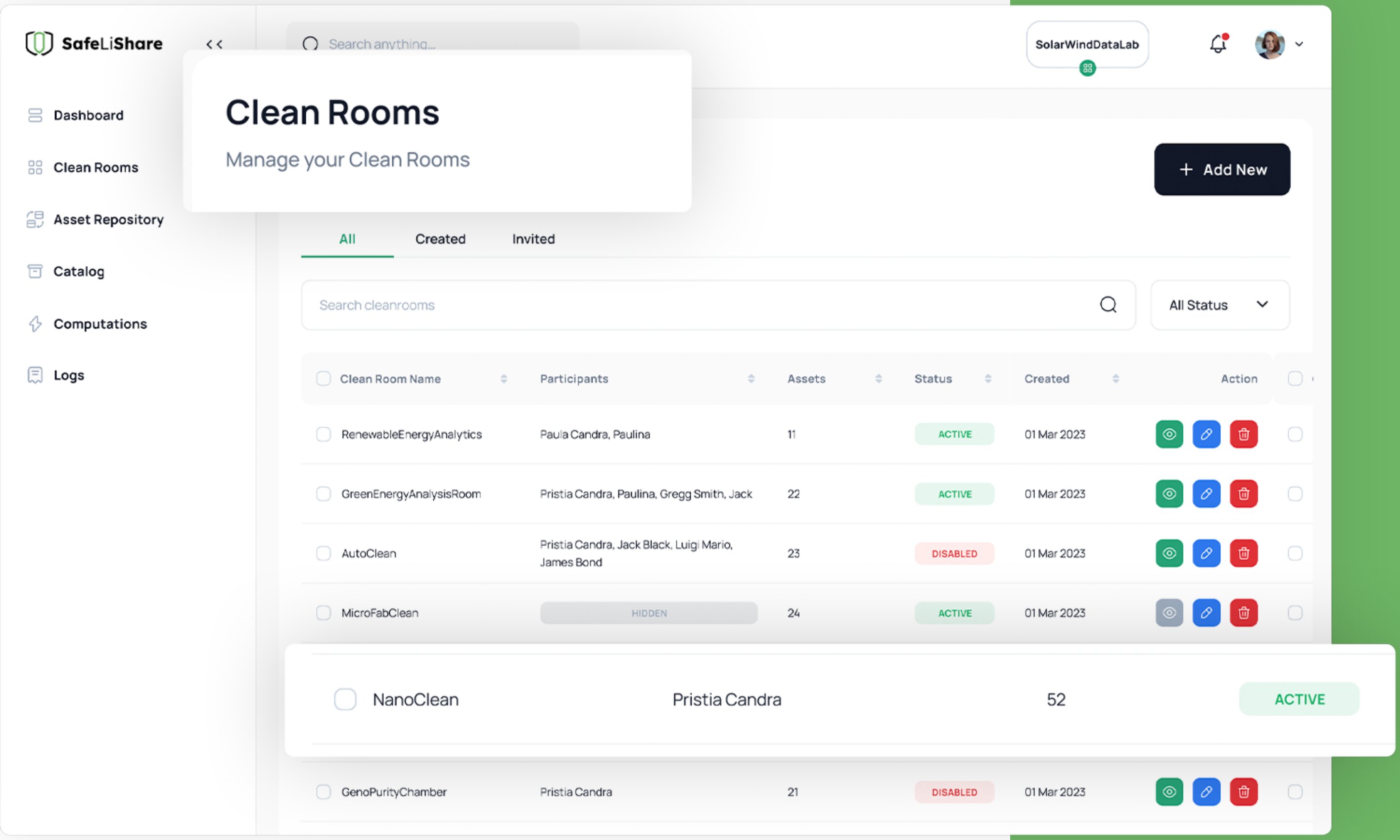
Available in leading Public Clouds, Confidential computing mitigates data security concerns for highly regulated enterprises and organizations preoccupied with unauthorized, third-party access to data in the public cloud. It facilitates advanced data analytics, business intelligence and training of AI models based on data confidentiality and privacy controls between competitors, data processors and data analysts — which is very difficult to achieve with traditional cryptographic methods.

Introducing SafeLiShare Clean Room

SafeLiShare Clean Room, represents a cutting-edge cloud-native solution for confidential collaboration across enterprises, strategically built upon the robust foundations of Zero Trust Architecture. In a world where cybersecurity threats loom large, the Zero Trust model, founded on the principle of 'never trust, always verify,' emerges as the preferred strategy for safeguarding critical assets.

SafeLiShare Clean Room is plug-and-play deployment of confidential computing and simplifies multiparty computation without additional cloud OPEX resources. Enterprises increasingly seek to maxmize the value of their data by exchanging and processing data for analytics, business intelligence (BI), and training of AI models with third parties. This drives the adoption of confidential computing to provide secure computing environments — AI and ML clean rooms — for model, data exchange and process activities.

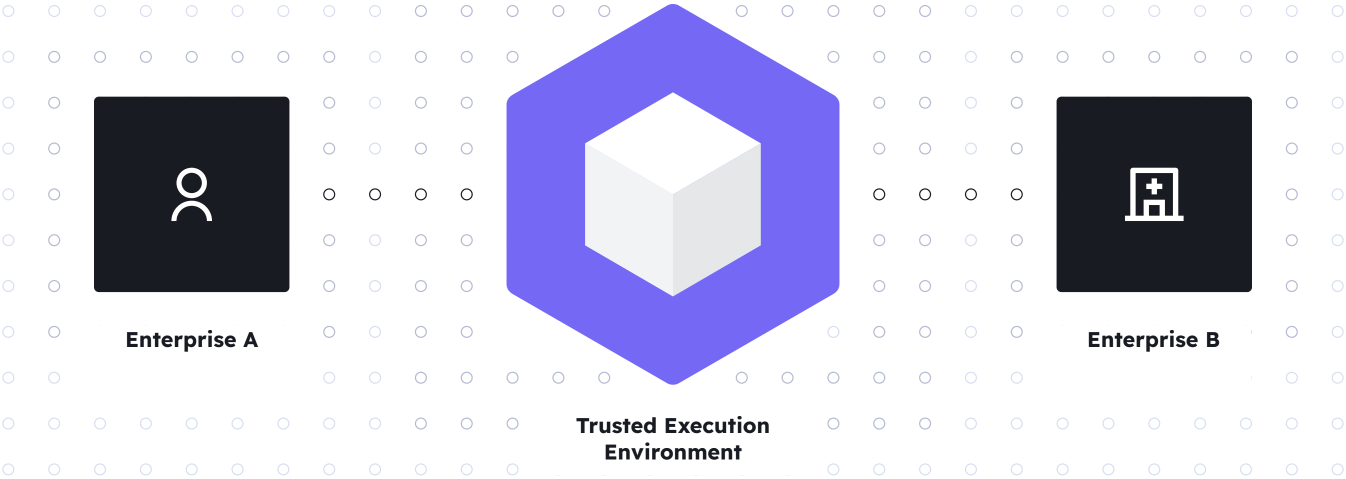
With end-to-end encryption, from encryption at rest, encryption in transit to encryption in use, SafeLiShare Clean Room offers enterprise-grade privacy-enhancing computation (PEC) integrated platforms without compromising real-time data. It is increasingly relevant to organizations with high-risk data assets and who need to perform multiparty computation across clouds.



Clean Rooms

Manage your Clean Rooms

□ Clean Room Name	Participants	Assets	Status	Created	Action
□ RenewableEnergyAnalytics	Paula Candra, Paulina	11	ACTIVE	01 Mar 2023	
□ GreenEnergyAnalysisRoom	Pristia Candra, Paulina, Gregg Smith, Jack	22	ACTIVE	01 Mar 2023	
□ AutoClean	Pristia Candra, Jack Black, Luigi Mario, James Bond	23	DISABLED	01 Mar 2023	
□ MicroFabClean	HIDDEN	24	ACTIVE	01 Mar 2023	
□ NanoClean	Pristia Candra	52	ACTIVE		
□ GenoPurityChamber	Pristia Candra	21	DISABLED	01 Mar 2023	



Key Features

☑ **Zero Trust Architecture:**
SafeLiShare Clean Room is underpinned by Zero Trust Architecture, revolutionizing security paradigms by replacing implicit trust with continuous assessments based on identity and contextual risks. This approach ensures that unauthorized access and data leakage are eradicated, even in collaboration with cloud service providers.

☑ **Decoupled Trust:**
Trust is liberated from the physical location of users and the applications they access, providing a dynamic and adaptive security posture.

☑ **Comprehensive Security:**
The platform operates completely out of the data path, control plane, and traditional trust equations, minimizing the risk of model inversion, infections, and potential attack spread.

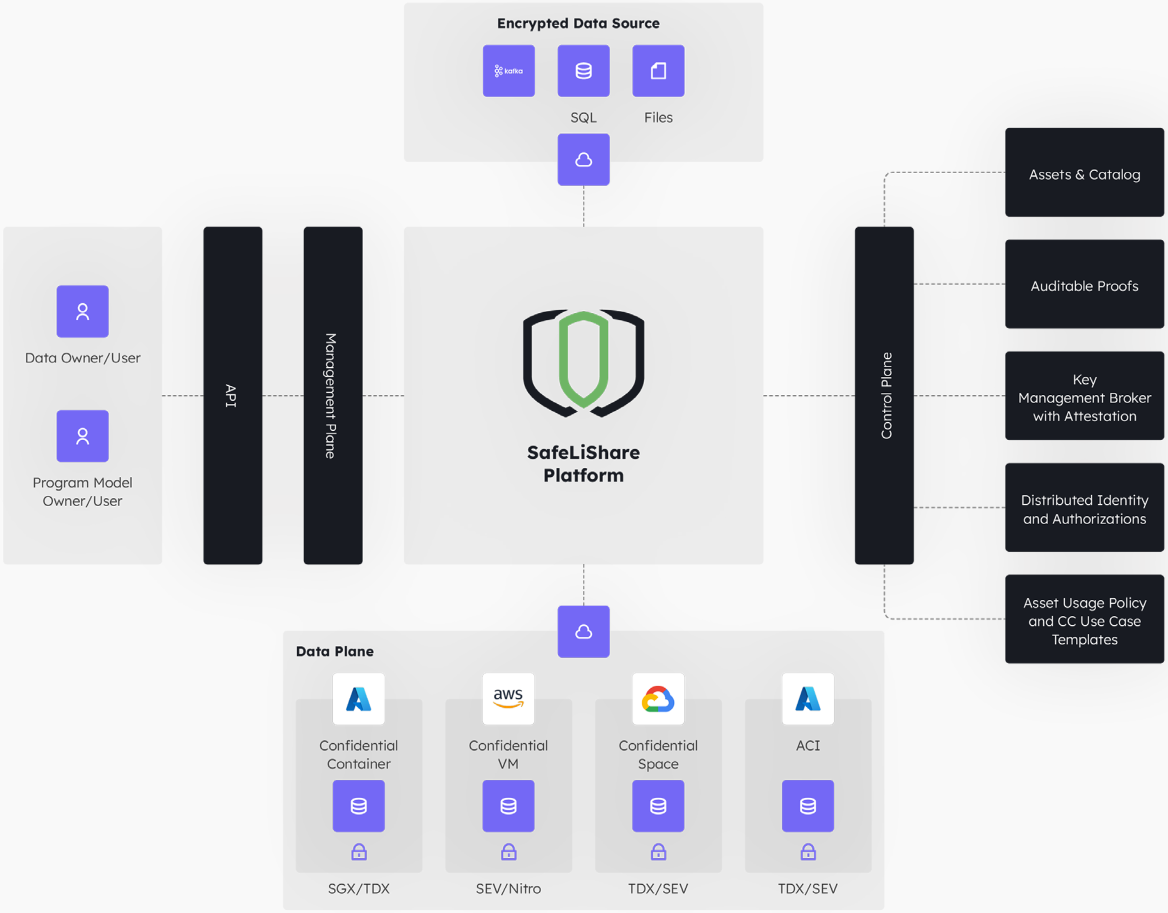
☑ **Regulatory Compliance:**
SafeLiShare Clean Room aligns with regulatory requirements, addressing the growing need for data protection. It not only safeguards data but also encourages organizations to derive commercial value on top of a protected baseline.

☑ **Confidential Computing:**
Leveraging chip-level Trusted Execution Environments (TEE) and conventional key management, SafeLiShare Clean Room enables secure computation facilities that remain inaccessible to infrastructure providers. This facilitates collaborative projects without compromising data or intellectual property security.

☑ **Privacy-Enhancing Computation (PEC):**
End-to-end encryption, encompassing encryption at rest, in transit, and in use, positions SafeLiShare Clean Room as an enterprise-grade PEC integrated platform without forklift upgrade. This is particularly beneficial for users with high-risk data assets, ensuring multiparty computation across clouds without compromising real-time data or introducing service degradation.

☑ **Cloud Scalability and Interoperability:**
The SafeLiShare Clean Room platform, offered as a plug-and-play deployment of confidential computing, simplifies multiparty computation without additional cloud OPEX resources. This is especially valuable as enterprises seek to exchange and process data with third parties for analytics, business intelligence, and AI model training.

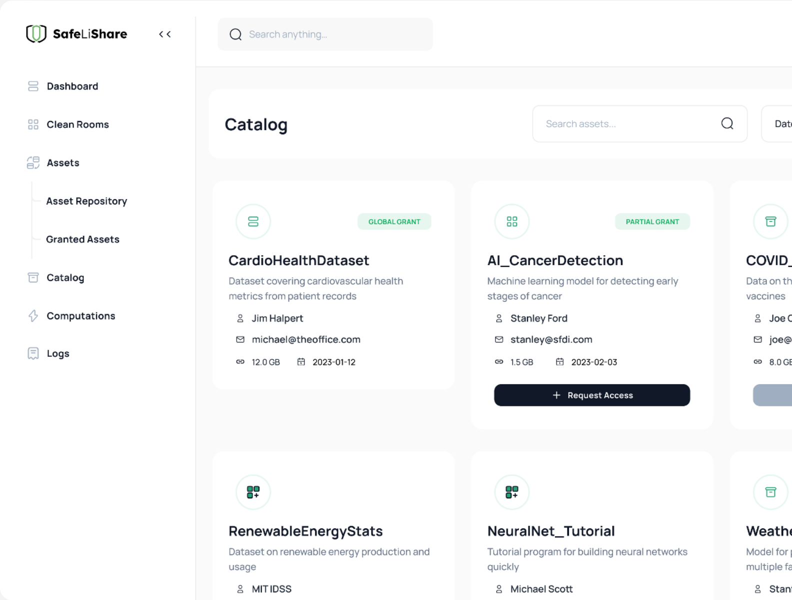
☑ **Unified Cloud Abstraction for Enterprise-Grade Protection:**
SafeLiShare AI & ML Clean Room provides a single and unified abstraction that conceals differences in trust models across various clouds and secure enclave technologies. This ensures robust protection of sensitive data-in-use, catering to diverse enterprise use cases.



Enable Revenue Data Sharing

SafeLiShare Clean Room offers a unique foundry for custom data products for AI ML models, data assets, notebooks, or automation templates. This providing a state-of-the-art model architecture to build, customize and deploy foundation models with ease in multiparty collaboration and computation.

The Catalog feature in SafeLiShare Clean Room technology can be used as a revenue data solution varying levels of first- and third-party data, creating a need for organizations to layer data sources together to maximize the value of their investments without losing the chain of custody.



Catalog

GLOBAL GRANT
CardioHealthDataset
Dataset covering cardiovascular health metrics from patient records
Jim Halpert
michael@theoffice.com
12.0 GB 2023-01-12

PARTIAL GRANT
AI_CancerDetection
Machine learning model for detecting early stages of cancer
Stanley Ford
stanley@sfdi.com
1.5 GB 2023-02-03

COVID_
Data on th
vaccines
Joe C
joe@
8.0 GE

RenewableEnergyStats
Dataset on renewable energy production and usage
MIT IDSS

NeuralNet_Tutorial
Tutorial program for building neural networks quickly
Michael Scott

Weathe
Model for
multiple fa
Stan

Get Started

SafeLiShare Clean Room is not just a solution; it's a paradigm shift in secure collaboration with full confidentiality and privacy controls. By embracing Zero Trust Architecture and incorporating cutting-edge technologies like confidential computing, it empowers enterprises to confidently navigate the challenges of data security, regulatory compliance, and collaborative innovation. Elevate your security posture with SafeLiShare Clean Room and embrace the future of confidential collaboration, please visit **https://safelishare.com/demo/** and start design or duplicate a sample application using one of the available cloud abstraction mechanisms in Microsoft Azure or Amazon AWS and deploy a clean room. Perform processing on datasets representing the kinds and amounts of sensitive information you expect in real production workloads. Doing so will help you determine whether confidential computing affects application performance and seek ways to minimize negative results.

Depending on the use case and the robustness required, SafeLiShare Clean Room for AI and ML analytics provides the single and unified abstraction that hides the differences in trust models demo across different clouds and secure enclave technologies for enterprise-grade protection of sensitive data-in-use. For more information, contact us at **cleanroom@safelishare.com**.

Gartner®

"By 2025, **65%** B2B sales organizations will transition from intuition-based to data-driven decision-making using technology that unites workflow, data and analytics."

About SafeLiShare

In an era when data has become the product for many enterprises, and faces increased scrutiny due to tightening global regulations, SafeLiShare was founded with a vision to provide application specific access to data. All operations on data by applications are made visible, auditable, and trackable. Multiple governance policies can be enforced simultaneously. Powered by confidential computing technology, policies drive compliance and governance throughout an enterprises' multiple business functions, data domains, and even across to external business partners engendering a new class of business models based on ownership of data and applications.