intertrust®

Secure Execution Environments

Product Brief

Platform

Enterprise IT operations are under pressure to remain flexible in testing and deploying a growing number of applications, from a diverse set of vendors. Coupled with multiple third-parties and multi-party cloud services, organizations struggle over choosing the best strategy for adopting data application management services.

Fortunately, a sound data orchestration strategy can reduce the time to market for these applications—plus reduce complexity, help them scale, and make managing them much easier.

A platform for data interoperability

To benefit from their data, businesses need to analyze it, which requires collaboration across locations and formats. But whether internal or external, data sharing is risky.

Using secure data virtualization, Intertrust Platform™ eliminates the risks inherent in moving or copying data. With the Platform, businesses can develop analytics securely, in containerized workflows, without losing control over IP or data rights, using identity and access management.

The Intertrust Platform leverages Kubernetes containers where operational and interactive workloads run without allowing data egress. The Platform's Secure Execution Environments can enforce strict network constraints so data moves within the boundaries of the Platform, but not beyond it.

Key features

- Workload execution environments that auto-configure required compute and memory resources. The service also provides a manual configuration option for the memory and compute resources for the particular cluster based on customer requirements.
- Enables third-party analytics providers to deploy and run algorithms within a secure virtual sandbox.
- Fine-grained control or preventable access to original source data.
- Eliminates the need to deploy an operating system to onboard applications.

This solution can also be used for interactive scenarios, where third-party users are granted access to a remote environment within the Intertrust Platform for data exploration. For example, data scientists can access a Jupyter notebook to perform analysis on sample data without handing the actual files. Besides eliminating the risks inherent in data movement, the solution also saves on data transportation and storage costs.

Secure container-based application development

The Secure Execution Environments feature of the Intertrust Platform is built to secure Kubernetes-based application orchestration and integrate that with the organization's data assets in a secure way. It provides an environment where organizations can share proprietary data in a controlled manner to allow collaboration with partners and third parties. Internal IT operations can now bridge the 'trust gap' between third-party application developers and enterprise organizations by promoting transparency through secure data sharing operations.

Key benefits

Portability and ease of management on different infrastructure setups

- The same orchestration tools can be used across multiple platforms.
- The service compatibility across different platforms avoids infrastructure and cloud provider lock-in, and enables a multi-cloud strategy and setup for diverse businesses.

Workload scalability, security framework, and robust availability SLAs

- The service ensures efficient utilization of hardware resources with features like horizontal scalability, replication controllers, and auto/manual scaling.
- The service provides industry-leading SLAs to manage containers running mission-critical data operations and applications.

Securely collaborate with third-party applications and developer ecosystem

- Intertrust Secure Execution Environments prevent data egress in a containerized system, ensuring that the data never leaves the premises, while making it usable by authorized third-party collaborators.
- Intertrust Secure Execution Environments add a supplementary security layer for the application data access ecosystem.

Centralized Kubernetes-based orchestration service for internal/ external applications

- The Intertrust Secure Execution Environments service enables application clusters to perform centralized DNS Management, networking policies, resource monitoring, logging, and storage orchestration.
- The service also unifies resource monitoring, network and policy management, and automated scaling and troubleshooting operations.

The solution

Intertrust Platform is an edge-to-cloud data interoperability layer that uses secure data virtualization and identity and access management to enable governed data collaboration in secure workflow environments. It is designed to facilitate secure and efficient data orchestration for multiple entities and stakeholders, internal or external. It works securely across hundreds of data silos and clouds and ensures compliance with data security regulations and privacy protections.

Intertrust Platform™

The Platform leverages container orchestration technologies such as Kubernetes and Docker to make deployments cloud-agnostic.

Identity and Access Management
Device and user identity, authentication, and authorization; maintains platform objects and their relationships.

Data Virtualization
Data object definitions, permissions, restrictions. Provides data interfaces, manages DBs and virtualized datasets.

Secure Execution Environments
Secure network-isolatable environments for workload execution and controlled, interactive data exploration.

Time Series Database
Scalable, efficient, high performance database designed for time series data.

The Platform works as a collection of microservices deployed on Docker containers orchestrated by Kubernetes. The Platform primarily uses its own Kubernetes service, but, if needed, can also use a service provided by a cloud service vendor (such as Amazon EKS).

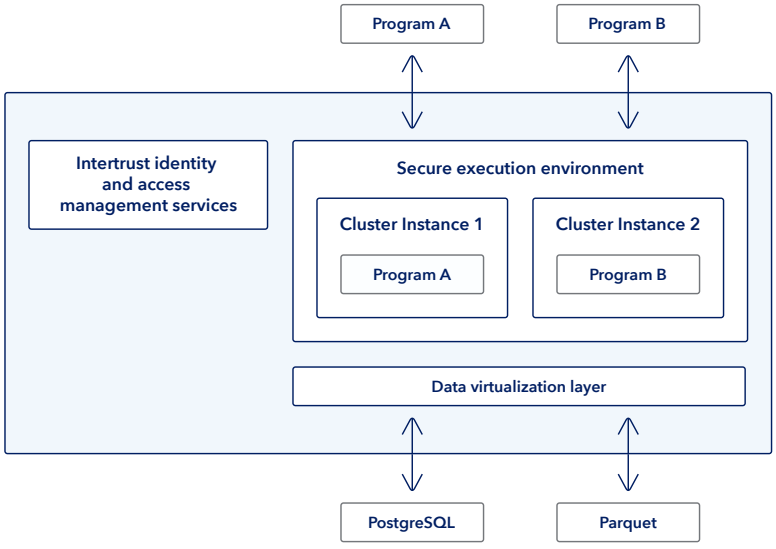
Aiding the Kubernetes-based governed application ecosystem

The Intertrust Secure Execution Environments service works in close conjunction with the Identity and Access Management (IAM) and the Data Virtualization features of the Platform. Whenever an application or program accesses any data component or service inside an organization, the IAM service controls the access to the program or application, which is then deployed in Secure Execution Environments.

Key functions

- Enables secure, isolated workflow execution environments for executing workloads against governed data.
- Defines Clusters (required resources), and deployments (the running state of a program within a Cluster instance).
- Allows the Program output to be written back as a new dataset in any database which is also governed by the Platform.
- The Secure Execution Environment creates an end-to-end workflow for application governance that expands how organizations share and use data.

Organizations can run parallel programs that are interfaced with a common virtualization layer. This brings scalability, trust management, and ease of centralized orchestration.



Adding value to native Kubernetes services

- Secure Execution Environments use Kubernetes APIs to provide network-isolated environments to run containers. In addition, the environment also creates the ability to provide a shared disk space, which can be mounted into several containers at once, along with granular permission management on the disks. All of this enables the environment, by default, to remain secure and isolated, even with concurrent workloads and varying networking parameters.
- Intertrust Secure Execution Environments are closely integrated with Intertrust Data Virtualization, which allows the system to access certain datasets, and only if the request emanates from a SEE-managed Kubernetes cluster. **This powerful feature allows data ingestion, storage, and processing without the data ever leaving the system.**

A native Kubernetes orchestration system cannot do these things without a significant engineering overhead. The SEE liberates IT operations from worrying about networking, compliance, and audit gaps while enabling collaboration ecosystems with third parties.

Advantages

1. Intertrust Secure Execution Environments offer a managed service, which isolates and protects users from having to deploy a full engineering team associated with container development and orchestration workflows, with industry-leading SLAs.
2. Intertrust Secure Execution Environments ensure that the containers under the service management layer are deployed in a least-privileged model, which ensures that only those access rights that have been explicitly granted would be enabled in operations.
3. Intertrust Secure Execution Environments enable agile interoperability between multiple services inside the Kubernetes environment for organizations that have varying data and infrastructure needs.
4. Intertrust Secure Execution Environments enable true interoperability by providing the ability to collaborate and connect workloads across multiple clouds and on-premises instances. This inherently makes the system more secure and helps the organization to save on egress costs for data that needs to be consumed in the container application.

Conclusion

Businesses today depend on data to improve workflows, run more efficiently, and discover new opportunities. The Intertrust Platform enables the development of value-added services and applications by providing role-based or rule-based access to diverse data ecosystems. The Platform facilitates multi-organization collaboration, cross-cloud data sharing, and interoperability. With secure governance environments that enable analytics to go to the data, data never gets moved, is always protected, and always stays in your control.

Use cases

Some examples of services powered by Intertrust Secure Execution Environments are mission-critical energy data operations, third-party data operations ecosystems, and automotive incubation centers.

E.ON
Energy Grid Data

Intertrust Secure Execution Environments enable E.ON to manage data operation applications around their mission-critical electrical grid data and share it seamlessly with multiple stakeholders in the energy ecosystem in an agile process, with the best data security practices.

Read more: https://bit.ly/Planning-Optimization

Leading Automotive OEM
Collaboration Ecosystem

One of the world's largest automakers uses Intertrust Secure Execution Environments to create a trusted data exchange ecosystem that helps them collaborate with third-party firms needing to use the automaker's internal data to develop applications.

Read more: https://bit.ly/Auto_OEM

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035