intertrust®

Case Study

Platform

Identity and access management

Today's enterprise architecture systems are challenged by the need to remain scalable, while managing increasingly complex infrastructure. Enterprise IT systems have become multi-location infrastructure systems, each with a wide variety of analytics and overlaid user-facing services.

Introduction

Creating a unified trust and identity solution for end consumers and administrators that encompasses data management and use in enterprise applications is a sizable challenge. In most modern corporations, identity and access management services are used to ensure that only authorized personnel can access appropriate data assets or connect to the corporate network.

The Intertrust Identity and Access Management (IAM) component provides authentication and authorization services that govern objects within the Intertrust Platform™. The service is responsible for maintaining a directory of Platform objects (e.g., accounts, datasets, workloads) and the rules that govern them, ensuring that only authorized requests are allowed. It also ensures a close architectural coordination between the different Platform features that extend identity management services across user identities, application access policies, and deployment privileges.

Central access design

The central feature in the Platform's identity service revolves around classifying the governance hierarchy in terms of:

Subject: A directory entity of a type that can perform actions. Subject types include: Accounts, Users, Organizations, and Groups.

Priviledge: The action/operation the Subject is permitted to take.

Object: Any governable entity in the directory.

Restrictions: System- or externally-defined limitations on the Privilege.

The heart of the Platform offers a security service, which aims to provide a yes/no answer to governance questions, along with an ordered list of externally-defined restrictions, of the form: **"Does Subject S have Privilege P on Object O?"**

Key features

The Intertrust Identity and Access Management service includes security, directory, and metadata management. Together, these features define and enforce security rules by managing all relevant entities and providing identification and authorization services to the Platform ecosystem.

The core IAM features are focused on facilitating the required authentication and authorization workflows, including the following:

1. OAuth2 based identification and authorization.
2. Support for Time-based One-time Password (TOTP) and SMS methods of two-factor authentication within the Platform Identity Service (i.e., AuthX).
3. Support for third-party identity providers via SAML integration (e.g., Active Directory).

Key benefits

The Intertrust Platform is designed to ensure unified governance over multi-party data and application workloads, in line with organizational policies and access hierarchy. This includes:

1. Unified governance over all Platform objects, including data sources, datasets, and workloads.
2. Managed access to data located in multiple physical systems (e.g., relational databases, S3 buckets, etc.) and locations (e.g., AWS, Azure, on-premises) from a single control pane.
3. Granular data access control with row- and column-based restrictions.
4. Enabling developers to define their own entity types and privileges, to support governance in custom services and applications.

The Intertrust IAM difference

IAM's key differentiator is its ability to integrate with the DataOps services enabled by the Platform, including:

1. Interoperability across multiple cloud/ on-premises setups using Data Virtualization, eliminating the risk and expenses involved with creating data warehouses or data lakes.
2. The ability to facilitate the co-creation of value-added services in rights-managed, secure containerized workload environments.
3. Risk management processes that include granular organizational policies with data access.

The IAM service is an integral part of the Platform as it enables governed data and application access for an agile data operations team. It is not meant to act as an independent identity service provider, and instead enables the most important authentication and authorization functions of the Intertrust Platform. On top of that, the service also provides system administrators and developers with a full stack of features that are useful for third-party applications and services that integrate with the Platform. Some of these include:

1. The ability to define custom privileges
2. The ability to define custom entity types
3. The ability to attach metadata attributes to objects and query those attributes (or metadata components
4. The ability to attach restrictions to privileges which are returned by the IAM service (but without evaluation—in other words, it's the data server that is responsible for evaluating dataset restrictions returned by the IAM service).

Use cases

Some examples of services powered by the Intertrust Identity and Access Management solution are mission-critical energy data operations, third-party data operations ecosystems, and automotive incubation centers.

E.ON
Energy Grid Data

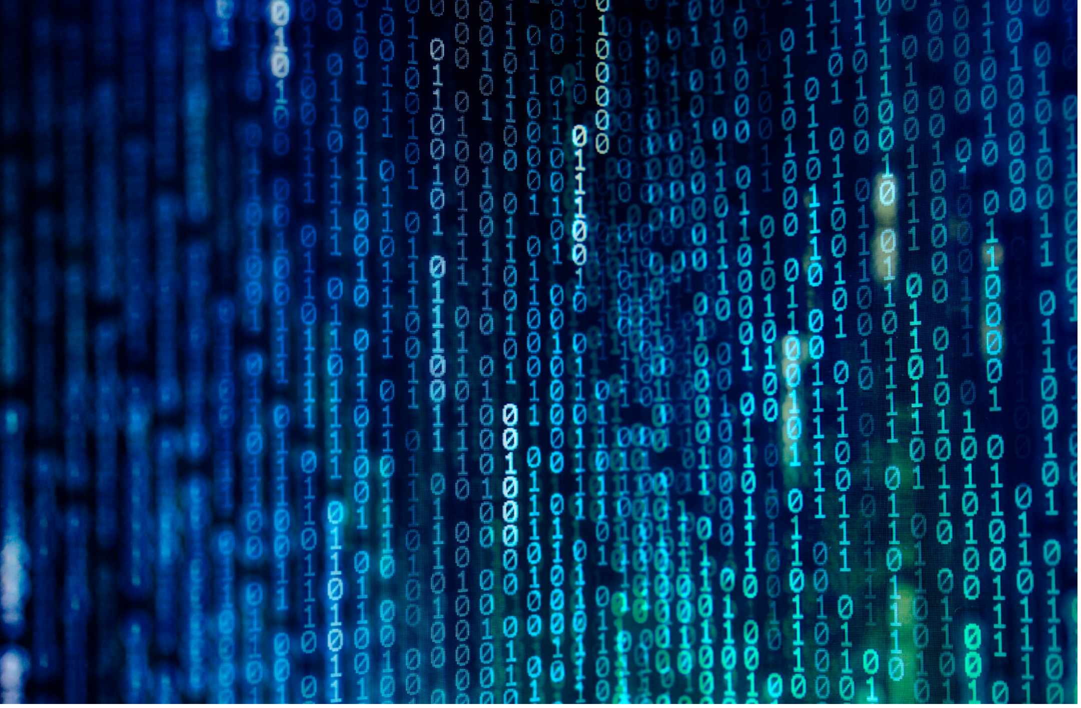
The Intertrust Identity and Access Management solution enables E.ON to authenticate and authorize data operation applications around their mission-critical electrical grid data and share it seamlessly with multiple stakeholders in the energy ecosystem in an agile process, with the best data security practices.

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

Leading Automotive OEM
Collaboration Ecosystem

One of the world's largest automakers uses the Intertrust Identity and Access Management solution to manage authentication and authorization services across a trusted data exchange ecosystem to manage workloads and applications running in an isolated environment. IAM also helps the right people interface with the right data inside the environment.

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



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.

Secure execution environment

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

Data virtualization

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

Time series database

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

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

Copyright © 2020, Intertrust Technologies Corporation. All rights reserved.