Data Security Platforms

B3. Aishi Tyagi,
Elena Xuanhan Zhou,
Echo Zhu

03/03/2025

Introduction

- What is a data security platform?
  - a comprehensive suite of tools and processes designed to safeguard sensitive information and maintain data integrity within cloud-based systems

- Specialized tools developed in response to increase in data threats by 1980s.

Copyright ©

https://www.paloaltonetworks.com/cyberpedia/data-security-platform

Key Features/Terms

Data Discovery

Identifying and classifying sensitive data across the IT ecosystem.

Encryption

Securing sensitive data at both rest and in transit.

Converts data into unreadable formats.

Access Control

Defining who has access to data and what they can do with that data.

Uses Role-Based (RBAC) or Attribute-Based Access Control (ABAC).

Data Detection & Response (DDR)

Identifying and responding to potential security threats in real time.

https://www.paloaltonetworks.com/cyberpedia/data-security-platform

Key Features/Terms

Data Loss Prevention (DLP)

Preventing accidental or intentional leaks of sensitive data.

Compliance Management

Ensuring various regulatory requirements and standards (such as GDPR & HIPAA) are met.

Identity & Access Management (IAM)

Managing user identities and controlling access to resources.

Auditing & Reporting

Tracking and analyzing activity to provide data security reports.

https://www.paloaltonetworks.com/cyberpedia/data-security-platform

Role in Business Context

- Centralized security measures
- Managing Cloud Security
- Mitigating Data Loss (DLP)
- Preventing Data Theft (DDR)
- Meeting Compliance Mandates (GDPR, HIPAA, PCI DSS, etc.)

➔ Improving operational efficiency

➔ Improving company reputation

https://www.paloaltonetworks.com/cyberpedia/data-security-platform

Product Comparison

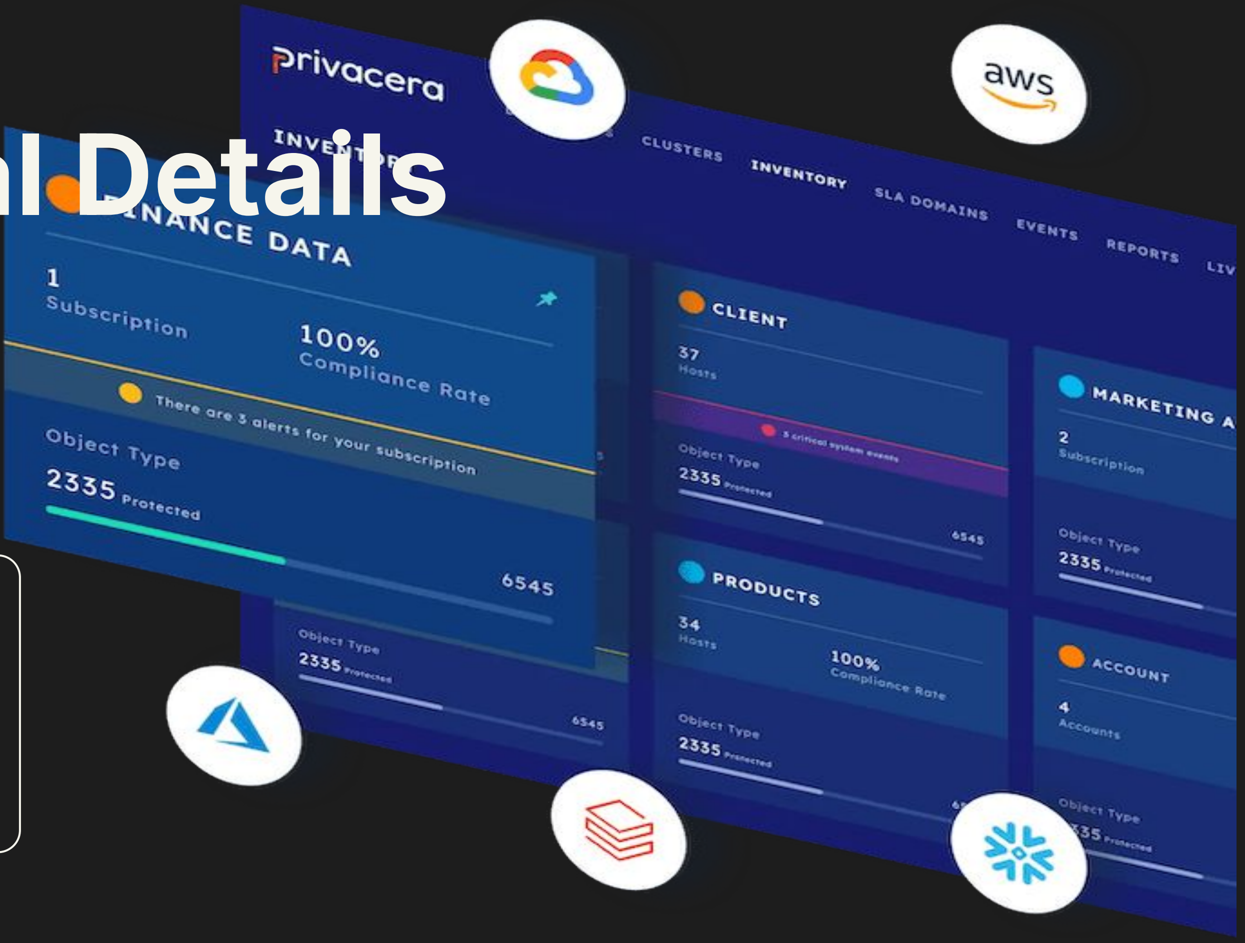
	Privacera	Immuta	IBM Guardium
Data Source Connectivity	Supports over 50 connectors. Structured and semi-structured data sources.	Supports 6 connectors. Focus on relational databases.	Extensive support for various databases and connections.
Data Discovery	✓	✓	✓
Access Control	✓	✓	✓
Compliance & Governance	✓	✓	✓
Scalability	✓	✗	✓
Primary Use Cases	AI Data Security, Privacy Compliance	Data Security, Privacy Compliance Dynamic Data Masking	Data Security, Auditing, Threat Detection
Deployment	Cloud, Hybrid, On-Prem	Cloud, On-Prem	On-Prem, Hybrid

Copyright ©

Technical Details

Privacera

Data security governance enable secure data sharing across hybrid environments and cloud services



There are 3 alerts for your subscription

Use Cases

Data Security Posture Management (DSPM)

- Sensitive Data Discovery
- Data Encryption and Masking
- Risk Assessment

Data Privacy and Compliance

- Automated Compliance
- Policy Enforcement

Data Access Governance

- Simplified Management
- Fine-grained Access Control

Financial Services

Retail

Healthcare

Tech Companies

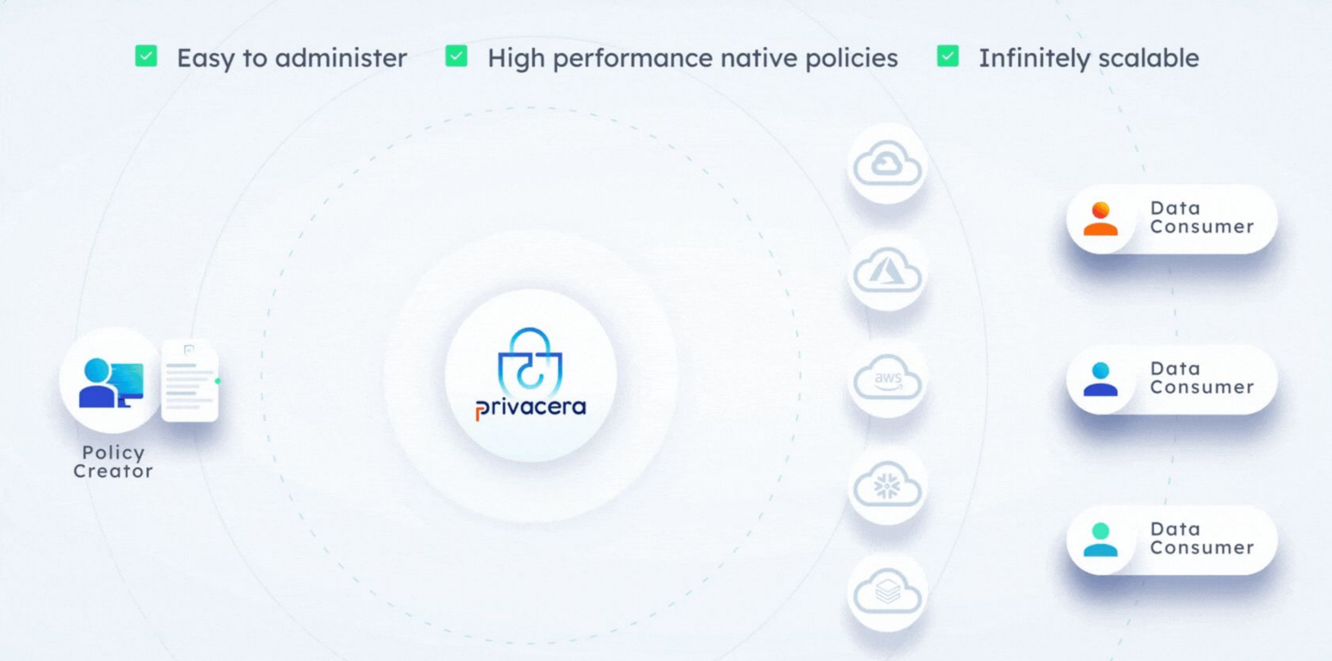
Manufacturing

Key Differentiator

Administration

High performance native policies

Infinitely scalable



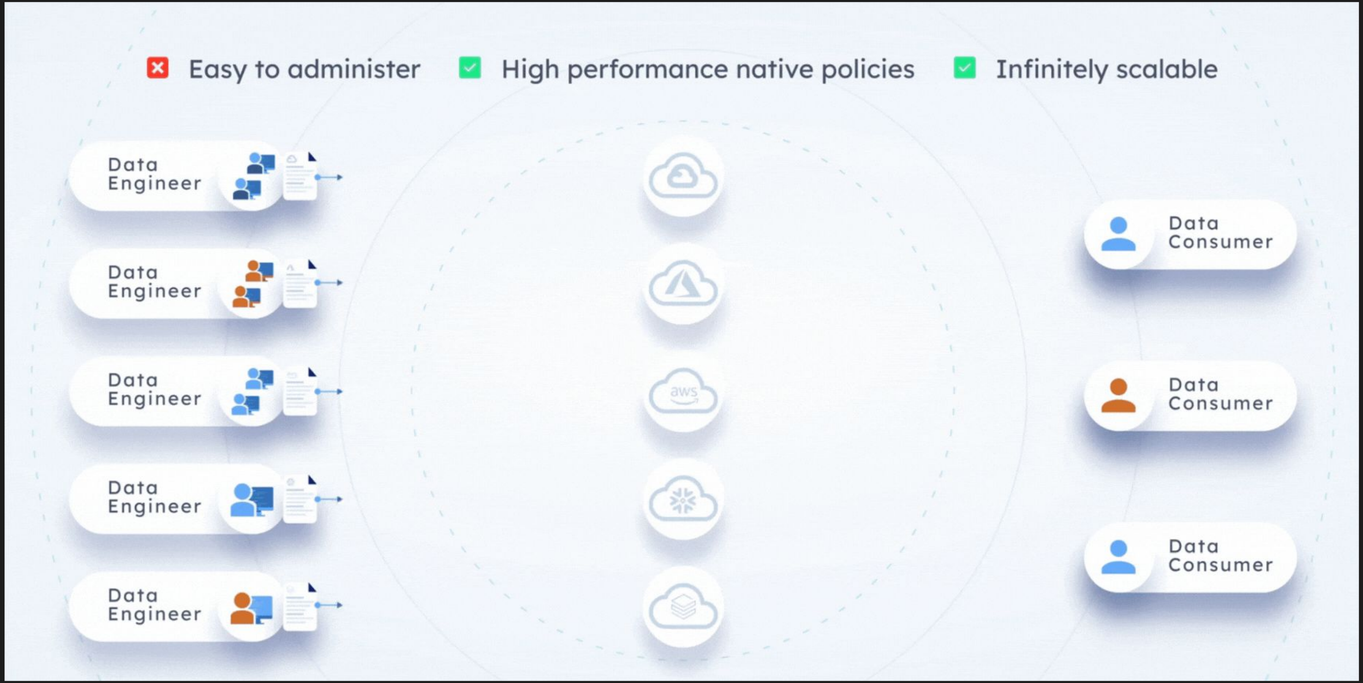
https://privacera.com/

Copyright ©

Key Differentiator

Administration

- Centralized, automated policy and compliance enforcement across all platforms
- No manual scripting required for each individual policy model



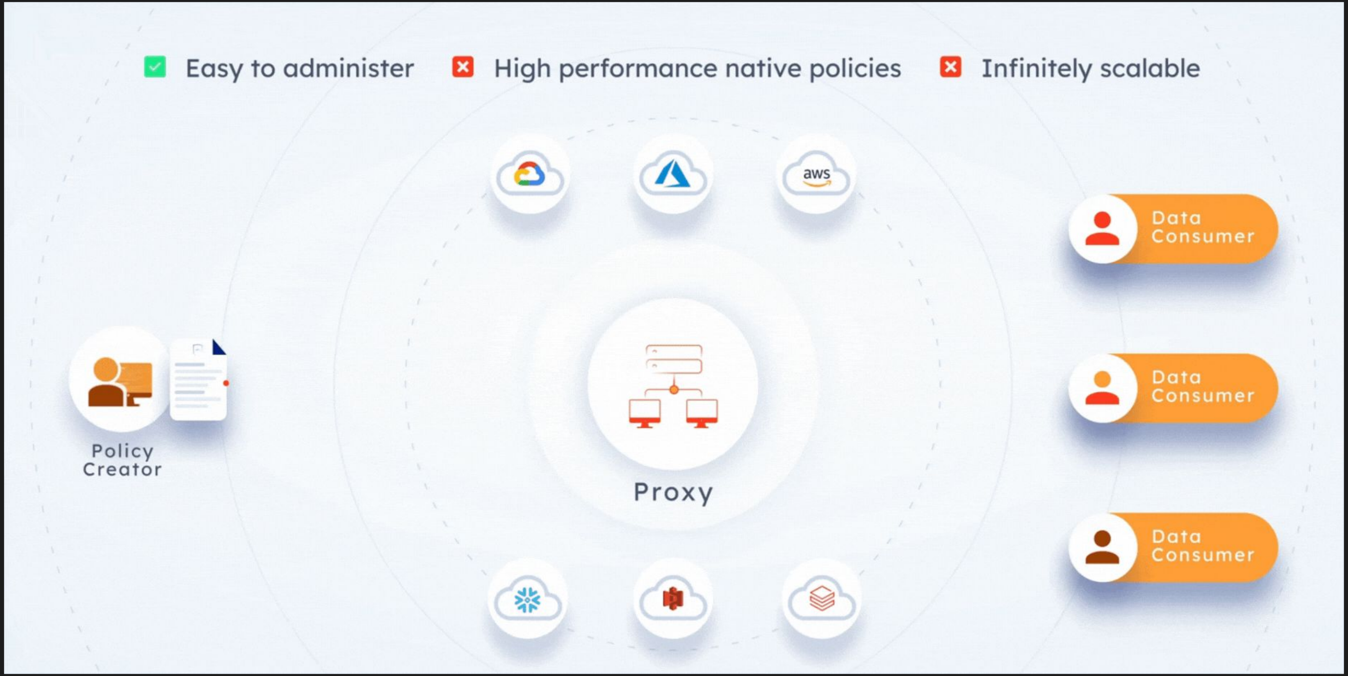
https://privacera.com/

Copyright ©

Key Differentiator

High performance native policies

- Direct integration with cloud-native security policies
- Eliminates latency issues and supports high-performance data access

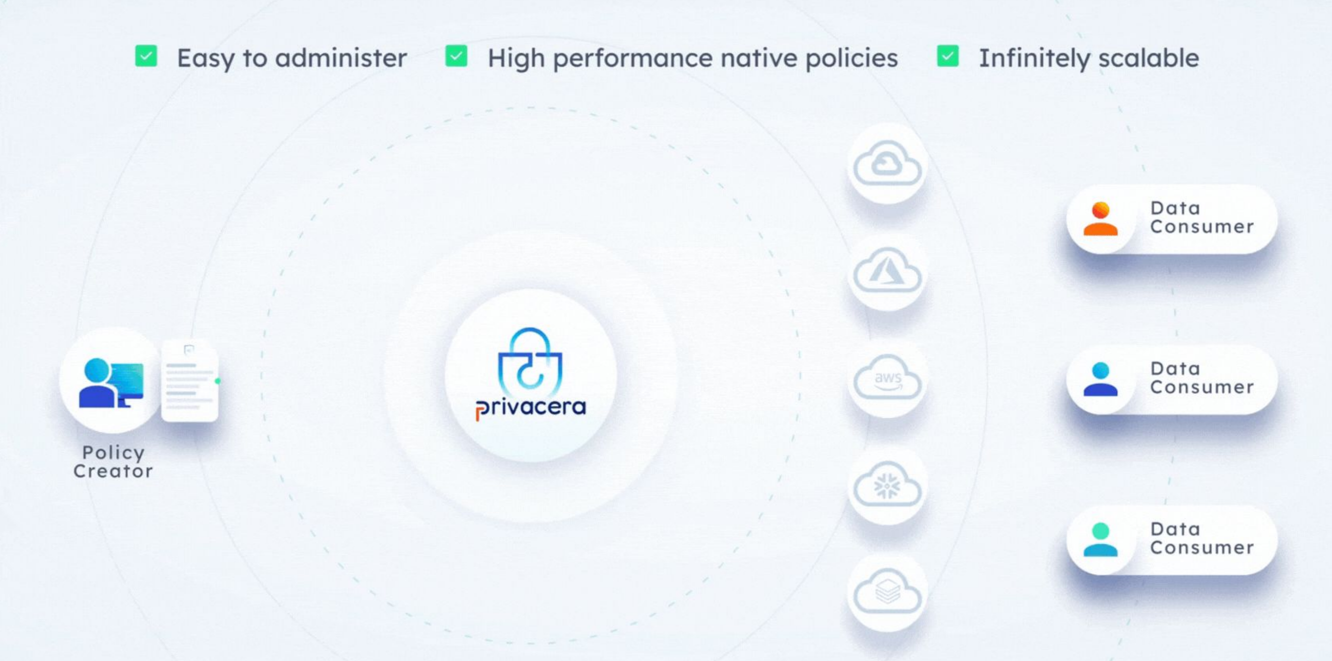


Copyright ©

Key Differentiator

Infinitely scalable

- Scales natively with cloud data services
- Supports hybrid & multi-cloud deployments efficiently



https://privacera.com/

Deployment

PrivaceraCloud SaaS

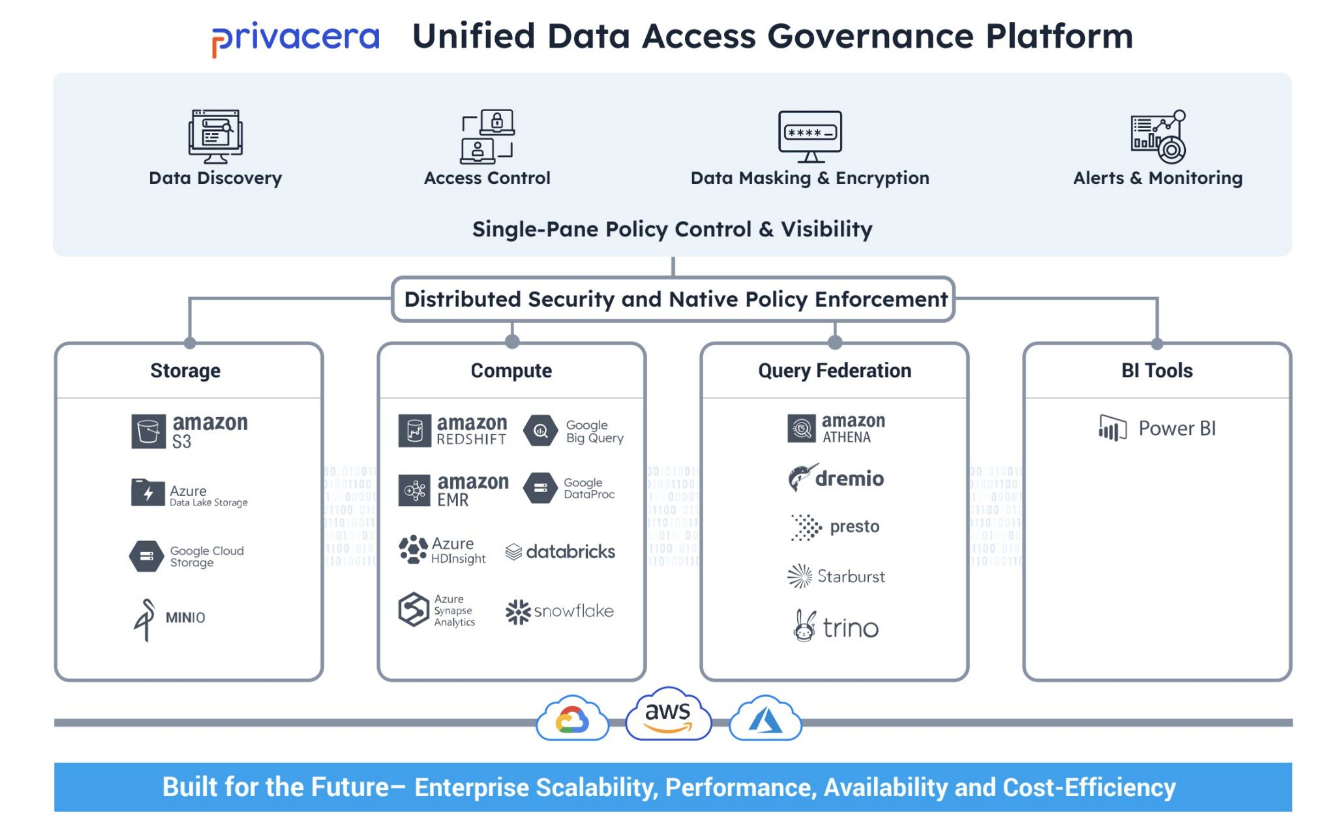
- PrivaceraCloud
  - No need for customers to handle software installation, maintenance, or updates.
- PrivaceraCloud Data Plane
  - A mix of SaaS and on-premises infrastructure
  - Ensure that data stays within customers' infrastructure instead of being sent to Privacera for processing
  - Create and manage policies and audit information while retaining full control over their data

Privacera Platform self-managed

- Self-managed Privacera Platform
  - runs on customer infrastructure, fully self-hosted deployment with no dependency on PrivaceraCloud
  - Full control of policy creation, storage, and enforcement

Copyright ©

Architecture



privacera Unified Data Access Governance Platform

Data Discovery

Access Control

Data Masking & Encryption

Alerts & Monitoring

Single-Pane Policy Control & Visibility

Distributed Security and Native Policy Enforcement

Storage

- amazon S3
- Azure Data Lake Storage
- Google Cloud Storage
- MINIO

Compute

- amazon REDSHIFT
- Google Big Query
- amazon EMR
- Google DataProc
- Azure HDInsight
- databricks
- Azure Synapse Analytics
- snowflake

Query Federation

- amazon ATHENA
- dremio
- presto
- Starburst
- trino

BI Tools

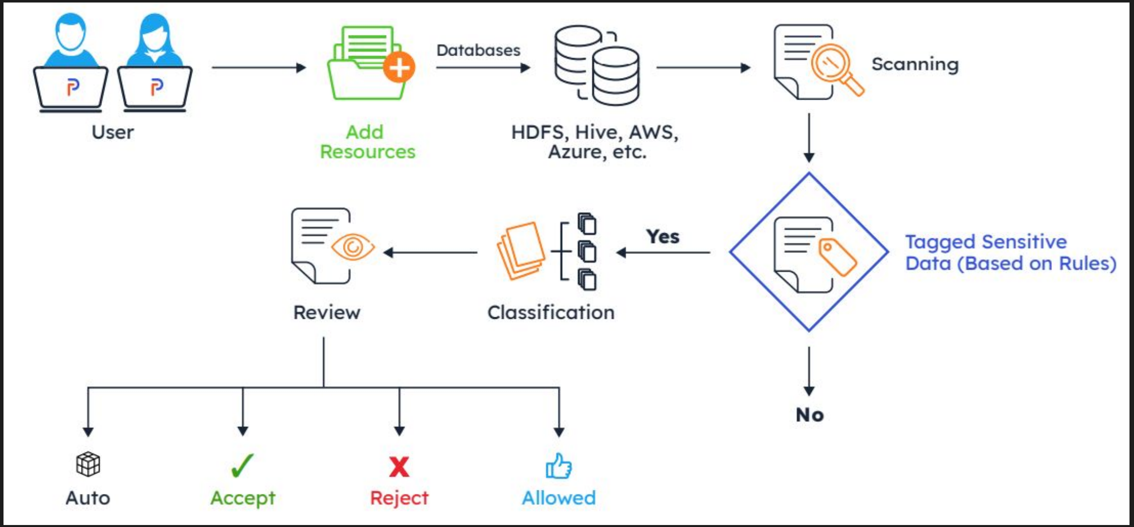
- Power BI

Built for the Future– Enterprise Scalability, Performance, Availability and Cost-Efficiency

https://privacera.com/docs/en/deployment-options--privaceracloud-and-privacera-platform.html

Discovery

- Data Scanning & Extraction
- Data Classification & Pattern Matching Algorithms
  - Rule-based classification: (RegEx, dictionary matching)
  - Machine Learning-based: (Named Entity Recognition NER models)
  - Custom Rule definition
- Policy-Based Protection
  - Applies masking, encryption, or access control based on data tags

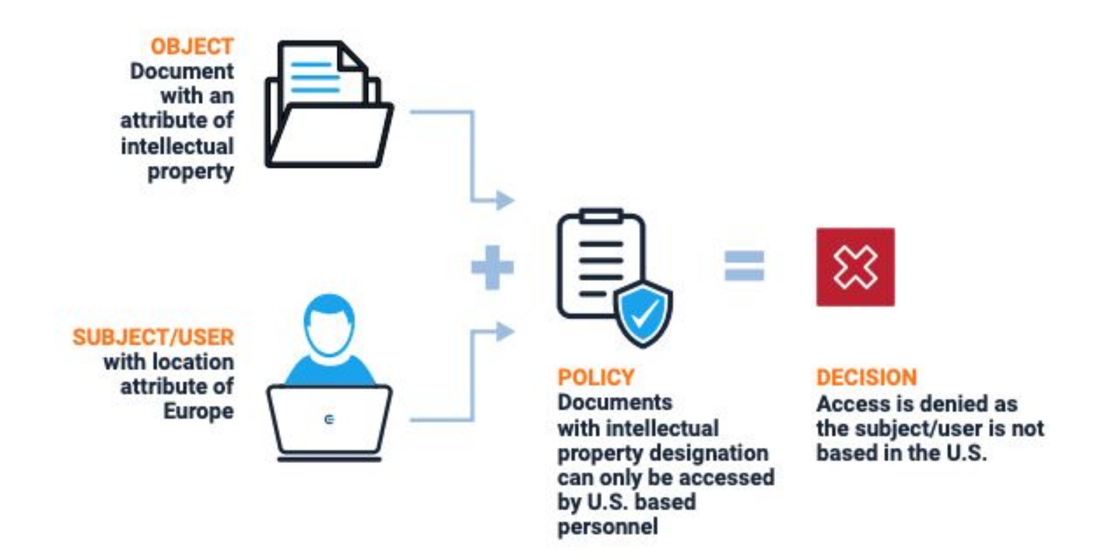


https://privacera.com/docs/en/deployment-options--privaceracloud-and-privacera-platform.html

Copyright ©

Access Control

- Role-Based Access Control (RBAC)
  - permissions are assigned to roles instead of individual users
  - Users are mapped to roles based on their job functions
- Attribute-Based Access Control (ABAC)
  - allow policies based on dynamic user attributes
- Fine-Grained Access Control: Apache Ranger API
  - Cloud-Native Security & Multi-Cloud Support
  - Row-Level Security (RLS)
  - Column-Level Security (CLS)


OBJECT
Document with an attribute of intellectual property
SUBJECT/USER
with location attribute of Europe
POLICY
Documents with intellectual property designation can only be accessed by U.S. based personnel
DECISION
Access is denied as the subject/user is not based in the U.S.

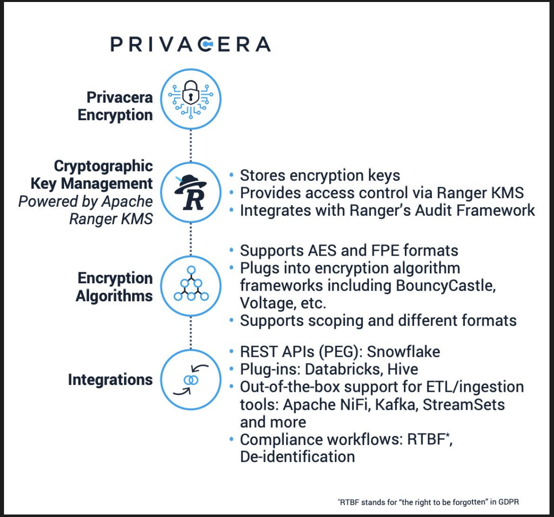
https://privacera.com/docs/en/deployment-options--privaceracloud-and-privacera-platform.html

Confidential

Copyright ©

Encryption

- Privacera Encryption Gateway (PEG)
  - Dynamic Data Masking (DDM)
    - Masks specific fields (e.g., SSN, credit card numbers) based on user roles
  - Advanced Encryption Standard (AES)
    - Uses AES-128, AES-256 encryption for sensitive columns in cloud data warehouses
  - Format-Preserving Encryption (FPE)
    - Encrypts data without changing its structure
    - allow masked data to be used in analytics



PRIVACERA

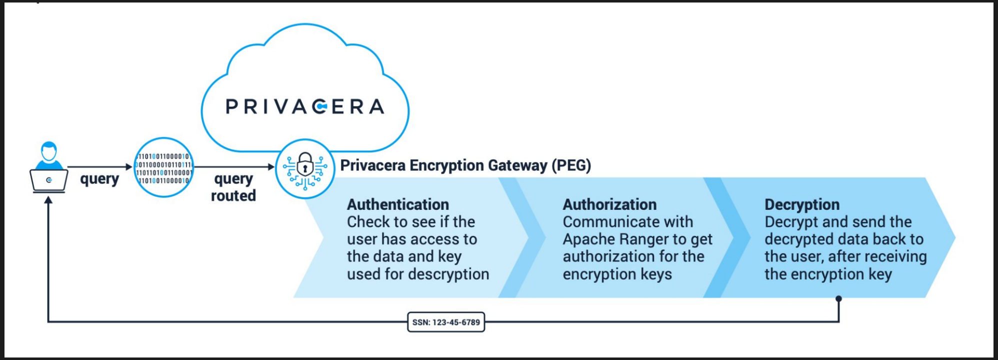
Privacera Encryption

Cryptographic Key Management *Powered by Apache Ranger KMS*
- Stores encryption keys
- Provides access control via Ranger KMS
- Integrates with Ranger's Audit Framework

Encryption Algorithms
- Supports AES and FPE formats
- Plugs into encryption algorithm frameworks including BouncyCastle, Voltage, etc.
- Supports scoping and different formats

Integrations
- REST APIs (PEG): Snowflake
- Plug-ins: Databricks, Hive
- Out-of-the-box support for ETL/ingestion tools: Apache NiFi, Kafka, StreamSets and more
- Compliance workflows: RTBF*, De-identification

*RTBF stands for "the right to be forgotten" in GDPR



PRIVACERA

Privacera Encryption Gateway (PEG)

Authentication Check to see if the user has access to the data and key used for descryption

Authorization Communicate with Apache Ranger to get authorization for the encryption keys

Decryption Decrypt and send the decrypted data back to the user, after receiving the encryption key

https://privacera.com/wp-content/uploads/2023/01/DS_Privacera_Encryption_Datasheet_FINAL.pdf

Sample Application1

Fintech Firm Enhances Data Governance and Security

Their data is stored in clusters that each catering to a different business segment, used by hundreds of analysts.

- **Comprehensive Data Visibility**: Real-time insights into data access, ensuring transparency and regulatory compliance.
- **Scalability**: Efficient management of petabytes of data without performance issues.
- **Regulatory Compliance**: Simplified reporting and adherence to industry regulations.
- **Faster Decision-Making**: Secure and quick data access for analysts, enabling real-time, data-driven decisions.

Positive Impact: Enhanced data security and compliance, leading to improved operational efficiency.

Negative Impact: Initial implementation complexity and the need for continuous monitoring to adapt to evolving regulations.

https://privacera.com/blog/scaling-data-governance-and-security-a-fintech-success-story-with-privacera/

Sample Application2

IMMUTA

Top Bank Automates Data Access Controls on Relational Databases

A leading multinational bank sought to streamline data access and enhance security.

- **Automation**: 95% of data access requests automated, saving over $50 million in resources.
- **Scalability**: Enabled self-service data access for over 5,000 users within six months.
- **Cloud Adoption**: Accelerated cloud adoption by decoupling on-premise data warehouses from cloud data access requests.

Positive Impact: Significant cost savings and improved data access efficiency.

Negative Impact: Potential challenges in managing automated systems and ensuring policy accuracy.

https://www.immuta.com/case-studies/thomson-reuters/

Future Trend

- Integration of AI in Data Protection
  - Advanced AI-driven tools can detect anomalies, predict potential breaches, and automate responses to security incidents, thereby strengthening organizational defenses.

- Data Privacy Regulations and Compliance
  - Governments worldwide are enacting more stringent data protection laws. Organizations must adapt to this complex regulatory environment to ensure compliance and avoid penalties.

- Decentralized Data Security Model
  - This shift is primarily driven by concerns over centralized vulnerabilities, increasing data privacy regulations, and advancements in distributed ledger technologies like blockchain.

Q&A