PRIVACERA ENCRYPTION: FINE-GRAINED DATA SECURITY

To enable self-service analytics, data democratization is desired as it puts data in the hands of as many users as possible for advanced analytics, which partly accounts for digital transformation's dominant theme of migrating to the cloud to improve data access. However, managing the inherent data security and privacy risks of making data widely available has become an arduous task. This concern is magnified across modern hybrid- and multi-cloud architecture in which data access policies are consistently applied across settings and tools. The cybersecurity community has come up with defensive mechanisms like the layered security approach and the zero-trust architecture, but at the core of them is securing mission-critical information at the data level.

Privacera provides comprehensive, end-to-end cloud data protection consisting of automated sensitive data discovery and classification, centralized access control with distributed native enforcement, and dynamic data masking. One critical capability that supports the entire data protection value chain is Privacera Encryption.

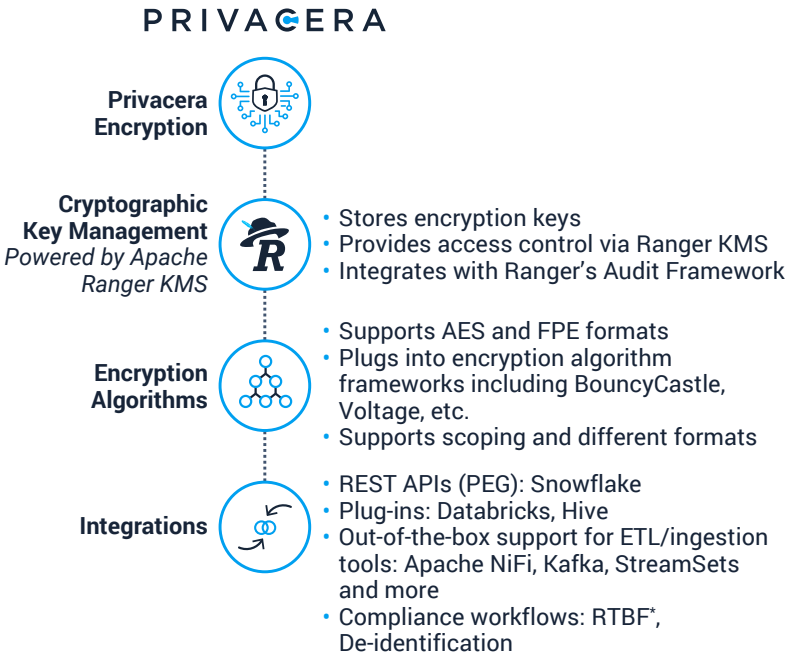
Privacera Encryption

Privacera Encryption has extended Apache Ranger's encryption capability beyond big data to cover cloud services. With Privacera Encryption, organizations can encrypt data at the table, column, row, field, or attribute level instead of the entire data. This granular level of encryption enables the data science and analytics teams to utilize more data to build models and extract insights to drive new business opportunities, leading to increased customer satisfaction and optimized business efficiency. After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access the data. The user experience of accessing encrypted data on a disk or in the cloud is identical to accessing non-encrypted data.

questions@privacera.com
privacera.com
510.413.7300
privacera @privacera

Privacera Encryption supports both Advanced Encryption Standard (AES) and Format-Preserving Encryption (FPE) formats. And to support the dynamic cloud services and data sources, Privacera Encryption offers four types of encryption integrations with major cloud applications:

- Compliance workflow for the Right To Be Forgotten (RTBF). Users can create a policy with a mapping for RTBF scheme. The policy can then scan for Hadoop, Amazon S3, and Azure Data Lake Store (ADLS) applications. It hides sensitive information such as user name and moves it into a quarantine folder.
- Plug-ins for Databricks and Hive.
- Out-of-the-box support for ETL/ ingestion tools such as StreamSets and more.
- Application programming interface (API) for Snowflake and more.



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

The API is a standalone service called Privacera Encryption Gateway (PEG). It significantly lowers the operational burden on infrastructure and security teams as they are not required to install, manage, and update separate encryption and decryption tools. It provides data encryption to protect digital data confidentiality as it is stored and transmitted. Encryption algorithms support security initiatives including authentication, integrity, and non-repudiation.

Privacera Encryption Gateway (PEG)

PEG is a robust, scalable API gateway that provides flexible encryption schemes—as well as policy-based encryption and decryption using NIST standards-based encryption algorithms, such as AES-128, AES-256, hashing, and FPE—to customers' sensitive data and personally identifiable information, without the need for manual processes.

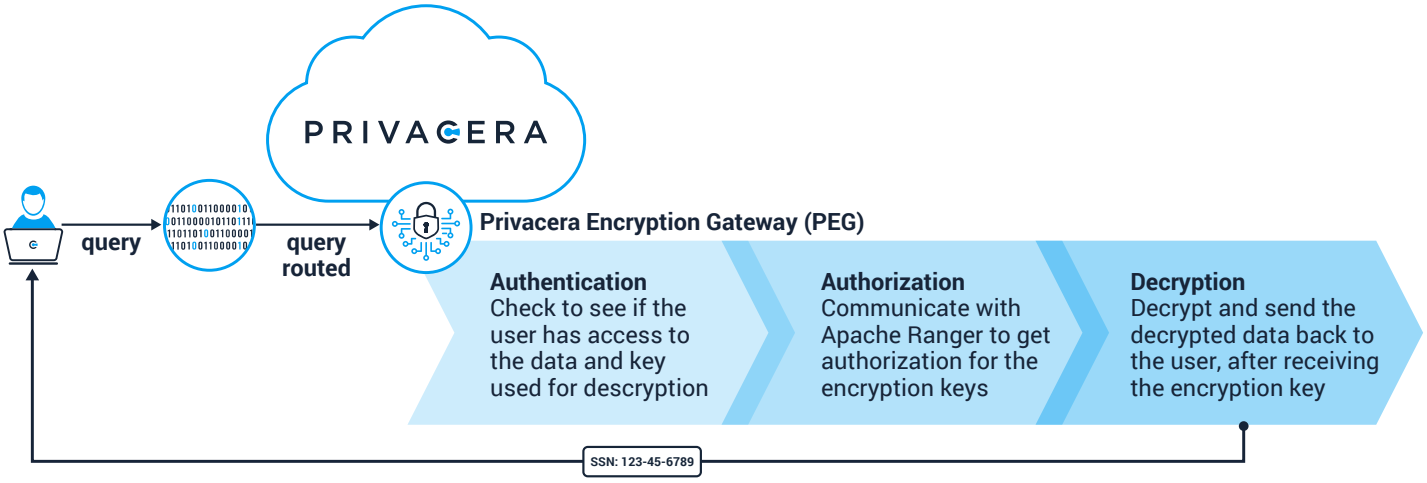
PEG is a cloud service that exposes REST API calls for encryption and decryption of data at rest and in motion. With PEG, companies can confidently migrate encrypted data from on-premises data lakes to the cloud and safeguard it against breaches in the cloud until it is ready to be decrypted for analytical purposes. PEG is ideal for data transformations and ETL use cases. Companies can use SparkSQL, Apache NiFi, Apache Kafka, StreamSets and other ETL/ingestion engines as potential data sources for PEG.

questions@privacera.com
privacera.com
510.413.7300
privacera @privacera

PRIVACERA

PEG Workflow

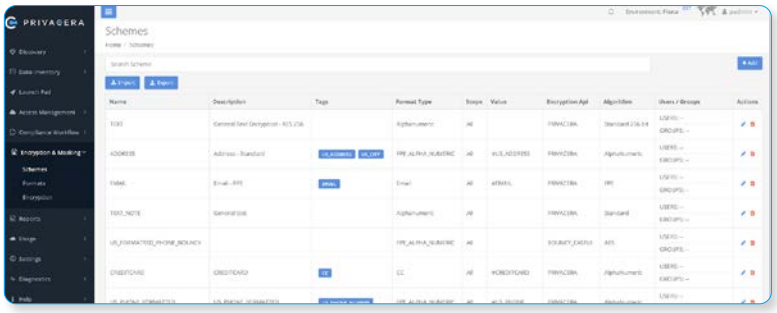
When a user writes queries against sensitive data, that query is routed through PEG to perform the following operations:

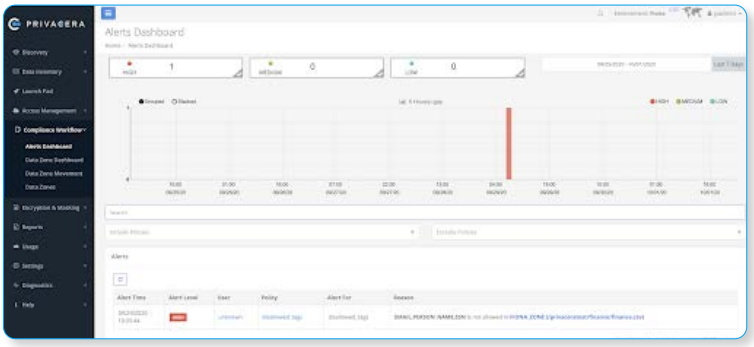


KEY BENEFITS

Maximize Data Protection

Privacera Encryption provides fine-grained security that data is encrypted at the table, column, row, field, or attribute level in connected systems. Even if the data are accessible by policies created in Privacera Access Manager, the encrypted data cannot be seen.





Ensure Data and Privacy Compliance

Data protection is mandated and a high priority for many organizations. With Privacera Encryption, data is protected for organizations to comply with industry and government regulations, such as HIPAA for healthcare providers, GDPR in Europe, CCPA in California, LGPD in Brazil, and PCPD in Hong Kong.

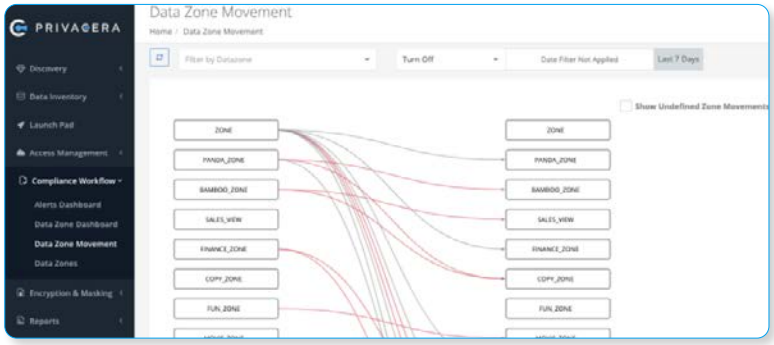
questions@privacera.com
privacera.com
510.413.7300
privacera @privacera

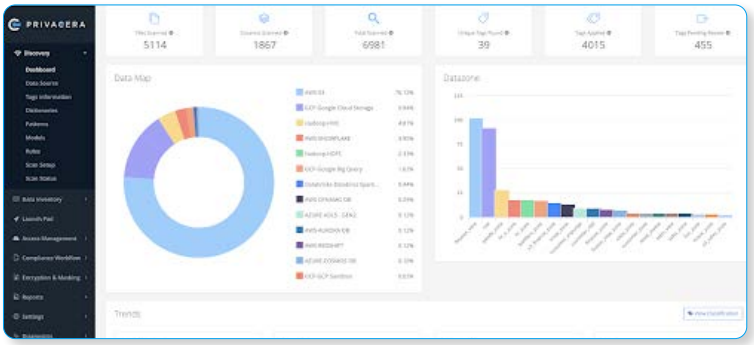
PRIVACERA

KEY BENEFITS

Increase Operational Efficiency

With PEG, users don't have to worry about upgrading or maintaining PEG as it is managed by Privacera. Companies can simply point their data to the service in order to have it encrypted or decrypted instantly.





Optimize Data Utilization

By supporting the entire data governance lifecycle, Privacera Encryption enables analysts and data scientists to utilize more regulated data to extract insights. Moreover, PEG is built on Kubernetes so it can scale horizontally to accommodate the increasing number of data inputs in today's hyper-connected cloud data ecosystem.

Ready to get started with Privacera?
Visit https://privacera.com to learn more, or contact us at sales@privacera.com.

questions@privacera.com
privacera.com
510.413.7300
privacera @privacera

PRIVACERA