Solution Brief

# Securing Data Analytics with a Data Security Approach

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

**In a data-driven world, data analytics is vital for any organization. It is a strategic asset for enterprises for real-time delivery of insights, improved decision-making about new offerings, and powers better customer experiences. It also enables workforce collaboration across geographic regions as well as between internal and external users.**

**Data security** is a critical factor influencing the success and sustainability of data analytics. It has become even more complicated as data stores expand in size and scale. The advent of cloud data storage and cloud data lakes makes storing vast volumes of data a reality. However, this expansive data means you must strike the right balance between using and protecting data. You improve data analytics by having more data and letting more people and applications analyze it. This leads to more risks. More data means more sensitive information and more people and apps. means more chances for a breach. Protecting privacy, sovereignty, and data breaches is essential. This has moved data security as the top concern for enterprises, as it may lead to data breaches, cyber-attacks, reputational damage, financial losses, or other organizational problems.

## Challenges of Data Security in Data Analytics

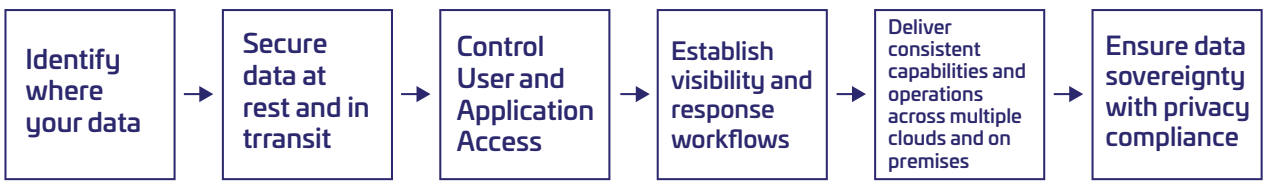
Taking a security-first approach and acknowledging data analytics security come with concerns and challenges; getting familiar with them is more than helpful in minimizing risk and securing sensitive data. Areas of focus should include:

- Upkeeping data privacy for personally identifiable information (PII) and compliance.
- Protecting data, whether it is at rest or in transit.
- Controlling access for third parties and application data scientists. Identifying and responding to external threats that target sensitive data.
- Protecting data, whether it is at rest or in transit.
- Supporting data sovereignty and internal, industry, and regional compliance requirements.

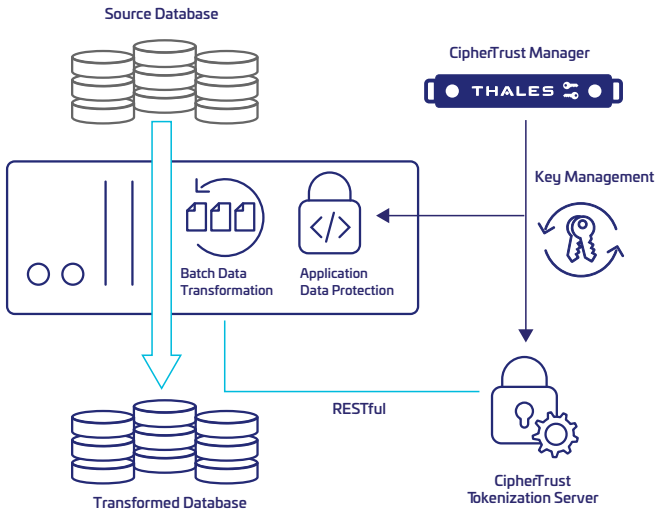
## Best Practices: Securing Data Analytics

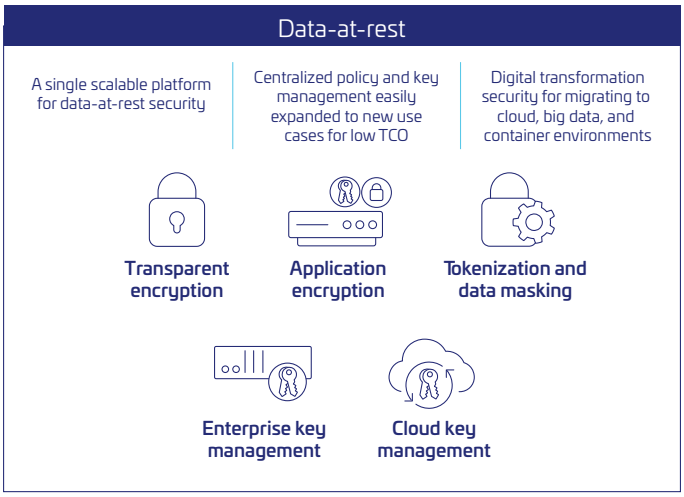
To mitigate these data security challenges, some of the best practices and solutions for data analytics security include:

- **Identify where sensitive data exists:** The crucial first step in managing data security challenges is to understand what constitutes sensitive data, where and how it is stored, and who can access it. CipherTrust Data Discovery and Classification and Imperva Data Security Fabric enable you to efficiently locate structured and unstructured regulated data across the cloud, big data, and traditional data stores in your organization with a single pane of glass. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
- **Secure Data at Rest and In Transit**
  - **Employ encryption and static data masking:** Encryption and tokenization for data at rest and in transit protect personally identifiable information (PII) and meet compliance demands.
    - **CipherTrust Application Data Protection** delivers on the promise to data scientists and data security experts of data portability between platforms and across different analytic tools while maintaining in the protected state. It operates with **CipherTrust Manager,** providing an architecture that centralizes encryption keys for applications. Enhanced separation of duties is provided with granular controls on both key users and key operational use.
      Organizations can prevent misuse of sensitive data while utilizing data sets by **static data masking**. Static data masking enables you to remove sensitive information before sharing it with internal or third-party developers and big data environments while simultaneously maintaining your data integrity and supporting mission-critical testing and analytical activities. **CipherTrust Batch Data Transformation** is part of the CipherTrust Data Security Platform that leverages the power of **CipherTrust Application Data Protection** and **CipherTrust Tokenization to protec**t vast quantities of data quickly.
    - Thales CipherTrust Transparent Encryption (CTE) with **Bringing Your Own Encryption (BYOE)** gives you higher confidence when compared to the native encryption solutions available from cloud providers. You can improve the security and access to your data in any cloud, including AWS, Azure, Google and more with CTE, which secures your data and helps comply with the compliance mandate.
  - **Secure data as it transits the cloud**
    With **Thales High Speed Encryption (HSE)** network encryptors, organizations can secure data in transit across network traffic between data centers, headquarters to backup and disaster recovery sites, in the cloud or on-premises for your data analysis.



## How does Static Data Masking work?




- **Control user and application access based on role and context:** Good data security requires both data and keys be controlled by stronger authentication methods.
  - **Identity and Access Management**: Access control/ management adds fine-grained control to all user interactions with a system. **Thales OneWelcome identity & access management** solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensure that the right user is granted access to the right resource at the right time; whereby minimizing the risk of unauthorized access.
  - **Control – Encryption Key Management** Controlling and maintaining data encryption keys is an essential part of any data encryption strategy. Key management safeguards cryptographic keys in a certified environment against misuse and loss; as keys control access to cryptographically protected data, key management becomes an important aspect of the overall security posture. **CipherTrust Manager** enables organizations to centrally manage encryption keys, provide visibility and auditability with granular access control, and configure security policies. It manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers developer-friendly REST API. CipherTrust Cloud Key Management (CCKM) increases efficiency by reducing the operational burden – even when all of the cloud keys are native keys. A dedicated external key management system – Hardware Security Modules (HSMs) is the best practice to manage your encryption keys. **Thales Luna Hardware Security Modules (HSMs)** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments.
- **Establish visibility and response workflows to thwart cyber-attacks:**
  - Organizations need more than built-in logging of traditional data platforms. To protect the organization from data breaches and compliance incidents, it is vital to augment traditional security approaches with controls for the data itself, to drive policy-compliant data handling, and help security staff pinpoint and mitigate data threats. **Imperva Data Security Fabric (DSF)** delivers visibility by monitoring and auditing all database activity to uncover hidden risks with data discovery, classification, and vulnerability assessments. This allows security staff to hone in on risky behavior for all users, including privileged users with real-time alerting or user access blocking of policy violations.
  - **DSF Data Risk Analytics (DRA)** identifies abnormal user and entity behavior that can lead to bad practices, hostile intrusions, and data compromise. The AI/Machine Learning analytics detect suspicious data activity and help translate complex technical events into plain language that IT operations teams can immediately understand. High-risk incidents are prioritized and grouped through machine learning to effectively align resources and elevate team skills.
- **Deliver consistent capabilities and operations across multiple clouds and on-premises** **Imperva Data Security Fabric (DSF)** simplifies regulatory compliance by automating and simplifying activities. It uses next-generation data warehousing technology to consolidate years' worth of database activity, enabling efficient use of current and retained data to meet regulatory compliance mandates. DSF can be utilized with cost-effective on-premises resources and has visibility into public clouds, third-party DBaaS providers, and big-data companies like Snowflake, Teradata, and Cloudera. It consolidates information across audited data assets and ensures consistent capabilities and operations, ensuring years of information is accessible for future retrieval.
- **Ensure data sovereignty with privacy compliance** Organizations can take charge of their **digital sovereignty** and find it easier to migrate sensitive workloads to the cloud to further secure sensitive data and meet compliance requirements by controlling encryption key access. With **Hold-Your-Own-Key (HYOK)** or **Bring Your Own Key (BYOK)** strategy over encryption keys, organizations can retain full control and ownership

of their data. **CipherTrust Cloud Key Management (CCKM)** allows organizations to separate the keys from the data stored in the cloud, preventing unauthorized data access by the Cloud Service Providers by using the **Hold-Your-Own-Key (HYOK)** or **Bring Your Own Key (BYOK)** technology. Organizations can secure your time and data with a single pane of glass view across regions for cloud-native BYOK and HYOK keys and one straightforward UI to manage all cloud key management services.

## About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.