THALES

Building a future we can all trust

SAS and Thales: Securing Analytic and Data Management in the Enterprise

Using CipherTrust Transparent Encryption to Safeguard Sensitive Data for SAS Viya

Key Benefits:

- Transparent, performant file-system-level data encryption
- Centralized enterprise key management
- Policy-based access controls for granular, automated protection
- Detailed logging and audit trails for more accurate compliance reporting

The Problem: Data Warehouses Consolidate Highly Sensitive Data That Require Security

Data warehouses are powerful by nature of their ability to consolidate data and its relationships in order to serve it up to advanced analytics and management tools. SAS, as the market leader in the space, offers both warehouse and analytics technology that lets organizations innovate in their spaces. For enterprises, these tools allow them to make better decisions, derive maximum value from their data, and ultimately achieve faster outcomes for their business. However, there is risk associated with this consolidation. Having sensitive data – whether that is personally identifiable information or sensitive intellectual property – located in one place makes a highly attractive target for hackers. Complicating the conversation are the layers of industry or region specific regulations governing

how this data should be collected, used and ultimately secured. Any organization that wants to adopt these valuable technologies will need to address the twin obstacles of security and compliance before they can fully realize the value of their SAS strategies.

Fortunately, Thales partners with SAS to address these common security and compliance concerns.

The Solution

CipherTrust Transparent Encryption (CTE) secures SAS Viya data at the file system-level, and uses centralized key management, privileged user access controls and detailed data access audit logging to strengthen the quality of the data's security. With CTE, enterprises can safeguard their SAS data as it resides either on-premises or in cloud infrastructure.

CTE agents deploy quickly and simply on SAS servers. Administrators define which directories to encrypt so the agent will secure data as it is written to, or read from, those directories. By operating at the file-system layer, encryption and decryption is transparent to SAS Viya, its analytics tools and associated applications referencing this data. Organizations do not need to make architecture changes or plan for downtime in order to secure their sensitive data. CTE's transparent approach to encryption lets organizations address a broad range of data security and regulatory obligations with minimal disruption. CTE works together with the CipherTrust Manager, a FIPS 140-2 up to Level 3 validated centralized encryption key and policy platform.

Why Use Thales CipherTrust Transparent Encryption With SAS Viya?

Combining SAS Viya with CTE lets organizations secure their sensitive data while continuing to mine and analyze it to make better decisions and achieve faster outcomes. By centralizing their encryption key management on Thales' CipherTrust Manager, organizations can incorporate their SAS Viya security into their larger organization-wide strategy. Additionally, CTE's privileged user access controls and audit logging separate SAS Viya security and system administration responsibilities to increase oversight and facilitate an organization's regulatory compliance.

Simplified Deployment and Administration

CipherTrust Transparent Encryption minimizes the time and effort required to implement and maintain data security for SAS Viya. Implementing CTE does not require application code or database architecture changes, ultimately making deployment an easy process. CipherTrust Manager also serves as a consolidated, central management plane for encryption keys and policies for SAS and a wide range of enterprise storage, database and application security solutions.

Granular User Access Policy Controls and Enforcement

CTE has the ability to define and enforce granular, least-privileged user access policies (e.g. by user, process, file type, time of day) to SAS Viya. These policies allow specific individual users and processes access to data in clear-text while restricting the file system commands they can perform. Access controls serve as an additional layer of protection between data and systems that makes data safer. Under these types of access controls, system administrators can manage configurations and ongoing maintenance without ever having clear-text access to sensitive SAS data.

Comprehensive Compliance Controls and Audit Trails

CTE's detailed data access audit logging addresses many common compliance controls for encryption, key management, data sovereignty, least-privileged policy and data access auditing. Auditors use these logs to assess the effectiveness of encryption, key management and access policies. By virtue of CTE's location, logs show when, and under which policies, users or processes access data, whether requests were allowed, and even when a privileged user submits a command like "switch user" as an attempt to imitate another user. CTE's pre-built integration with leading Security Information and Event Management (SIEM) systems mean organizations can pull this log data into their visibility tools for immediately actionable insights.

About THALES

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced ith an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About SAS

SAS is the leader in analytics. Through innovative software and services, SAS empowers and inspires customers around the world to transform data into intelligence. SAS gives you THE POWER TO KNOW®.

For more detailed technical specifications, please visit https://cpl.thalesgroup.com/ or https://www.sas.com/