Smartsheet Advance Platinum:
Security & Governance Customer Implementation Guide

Note: for higher-level context and information on the capabilities described below, please refer to this companion whitepaper.

Customer Managed Encryption Keys (CMEK)

Prerequisites/notes or considerations relevant to implementation

- CMEK typically take 2-4 weeks to setup and configure
- A typical security engineer/system admin can set this up
- Must have access to AWS KMS (Key management service) to implement this feature
    - This feature is not available for Azure key management
- Regardless of your organization's physical location - or the Smartsheet region you have subscribed to (US or EU) - the encryption key you make must be created in the AWS "us-east-1" region
- We do NOT support custom third party key management systems, such as Thales CipherTrust - only AWS key management (KMS)
    - While customers may try to use third party systems at your own risk, Smartsheet can not support, debug, or troubleshoot your setup process
- Post-purchase, you will need to work with your Customer Success Manager to provision your organization's access to this feature
- This feature does not encrypt Attachments and Images on the row. Only data directly in cells / sheets (and not cell images) is managed by the CMEK key; all other data is managed by the Smartsheet key
    - If it's critical that your organization control encryption over these items, please use a custom Attachment provider. For example, Box (which can be directly integrated with Smartsheet) also offers a CMEK solution

Setup resources available from Smartsheet

- CMEK Help Article
- While there is no dedicated services pack to facilitate setup, resources from Smartsheet's support and Engineering teams are standing by to assist should questions or issues arise

Event Reporting

Prerequisites/notes or considerations relevant to implementation

- To implement, some knowledge of APIs is required. As such, event reporting is typically managed by a security engineer/system administrator
- To benefit from the JSON feed Smartsheet exports, organizations will need the means to parse this data. Typically, this capability is provided by a separate, dedicated company CASB (cloud access security broker) or SIEM (Security information and event management) system
- Events can only be accessed by System Admins. System Admins need an API access token to use the API endpoints for Event Reporting. Steps to generate a token here

- Smartsheet does not offer any native DLP (data loss prevention) capabilities. While customers may be able to set up custom alerts based on certain events noted in the JSON event log, specific capabilities and outcomes available are dependent on the controls available within the specific CASB/SIEM you have implemented
- Event Reporting cannot currently read events across accounts governed by the Enterprise Plan Manager; it can only read on one Enterprise plan-level account at a time
- Event Reporting does not perform data classification, and cannot specify the type of data contained on a sheet/within the account

Setup resources available from Smartsheet

- Beyond the online resources available below, Smartsheet offers a dedicated 10hr professional services package focused on implementation training/guidance for Event Reporting
    - This includes:
        - Brainstorming use cases
        - Help getting started / locating relevant API documentation
        - Demo of a “Get Event” API Call
        - A walkthrough of how to perform specific functions (ie Get Object, Event Id, Object Id, etc)
        - Advice based on best practices to help inform the best way to visualize the data output
        - A resource for questions through the implementation process
    - Not included:
        - Help writing custom API Scripts
        - Review/troubleshooting of Code
        - Help with outside integrations
- Getting started guide
- Help Article
- Event Reporting Documentation: information on setup, list of events you can report on, how to call them

Data Egress

Prerequisites/notes or considerations relevant to implementation

- Egress policies govern actions available to both internal and external collaborators

- At this time, egress controls only limit actions for *sheets, reports, and dashboards*. Additional controls over public APIs and the Smartsheet mobile app are planned as future enhancements
- Policies are turned off by default – the System Admin for the account needs to set up a policy for egress controls to be activated

Setup resources available from Smartsheet

- Setup should be simple and intuitive, even for non-technical stakeholders
- Here's a help article with straightforward instructions: Help Article

Data Retention

Prerequisites/notes or considerations relevant to implementation

- At this time, *retention policies apply only to sheets* - but since sheets are the data source for both reports and dashboards, deletion of that content will remove the base data from all assets
- Policies are turned off by default – the System Admin for the account needs to define a specific retention policy for the feature to be fully implemented

Setup resources available from Smartsheet

- Setup should be simple and intuitive, even for non-technical stakeholders
- Here's a help article with straightforward instructions: Help Article

sales@smartsheet.com
(844) 324-2360
smartsheet.com
/smartsheet
/company/smartsheet-com
@smartsheetplatform
/@smartsheet
/smartsheet
/smartsheet