Unpacking Smartsheet Safeguard

Protect your most sensitive data.

Executive Summary

Smartsheet understands that security is a top requirement for enterprise-grade software. Secure collaboration is critical to prevent data breaches, leaks, ransomware attacks, and other adverse outcomes. To that end, this document seeks to make it easy for even non-technical stakeholders to understand our more advanced security controls – including what they do and how they work – so you can evaluate if these protections are relevant to secure company data within your unique context.

Customer-managed encryption keys

What are they?

Customer-managed encryption keys (CMEK) enable customers to control the key that Smartsheet uses to encrypt and decrypt your data. By maintaining control of this key via Amazon Web Services's Key Management Service (KMS), you can unilaterally and at your discretion prevent all parties from accessing any of your company data — even Smartsheet.

What's a simple way of understanding this?

At the risk of oversimplifying, think of paper in a physical warehouse. Encryption is the lock on the door to that warehouse, preventing malicious actors from being able to access usable information.

Generally speaking, you lease that lock from Smartsheet, and when you need to access your data we let you in using the key we control on your behalf to keep your data safe. With Customer-managed encryption keys, YOU own the lock and key. And while you've loaned it to us so we can help you access your data, you reserve the right — at any moment — to revoke Smartsheet's access to your key, thereby revoking our access to your data (anyone's access, really).

How does this protect my data?

This is the ultimate buck-stops-here control. If you suspect there's a malicious actor within your organization, or if you suspect Smartsheet has been compromised, you can fully prevent everyone from accessing your data to stem the breach. No decryption key equals no ability to read your data. Period.

Data egress policies

What are they?

Data egress policies govern collaboration and help prevent confidential data from leaving your Smartsheet account.

What's a simple way of understanding this?

It's a simple checkbox mechanism that lets you control a subset of the actions that are typically available for internal and external collaborators. Those actions all relate to the ways data can leave Smartsheet.

With data egress controls, you can prevent collaborators from taking the following actions on sheets, reports, and dashboards:

- Save as new (saving a copy)
- Save as template (copying a sheet and making it available as a template in their account)
- Send as attachment (sending the full sheet or report as an Excel file)
- Publish
- Print
- Export

How does this protect my data?

There is always some risk when data is shared internally; moreover, external collaboration represents a more prominent area of organizational vulnerability. With data egress controls enabled, you're able to prevent data leakage and collaborate with the confidence that what's confidential will stay confidential.

Event Reporting

What is it?

The ability to receive a running JSON feed that reflects a comprehensive list of events tracked by the Smartsheet API, with the ability to ingest that feed into common CASB environments, including Microsoft MCAS and McAfee MVISION.

What's a simple way of understanding this?

You may already be familiar with the event feed within the Smartsheet Activity Log.
That kind of event reporting comes standard with Smartsheet, and only shows a subset of events aimed at providing context for work in motion.

Smartsheet Event Reporting is intended to provide deep insight for IT admins around all the events that take place in Smartsheet, with tracking of over 100 different event types. These events are recorded as JSON code. While some can decipher JSON directly, for easier searching, parsing, and visibility, most will want to ingest that JSON feed into a CASB System.

CASBs (Cloud Access Security Brokers) are third-party tools that are built to read and display event feeds, with the ability to search across events and more as audit needs dictate. The two most adopted CASB systems are McAfee and Microsoft, and Smartsheet supports direct integration with both.

How does this protect my data?

Event reporting is primarily used for audit needs, acting as a detailed and searchable database of changes as they occur in Smartsheet.

Data loss prevention (DLP)

What is it ?

Additional functionality offered by CASBs that scans your event feed and enables trigger-based alerts around concerning events.

What's a simple way of understanding this?

Your company may have a CASB (Cloud Access Security Broker) in place to support event monitoring. Those systems sometimes sell DLP (Data Loss Prevention) capabilities that enable admins to configure trigger-based automation rules around specific events logged, enabling closer oversight around information entered into Smartsheet.

[It's important to note that this functionality is not offered by Smartsheet directly, and specific DLP capabilities may vary from vendor to vendor.]

How does this protect my data?

This capability takes your event feed — a passive audit tool — and turns it into an active mechanism that you can use to get notified around potentially concerning events. By setting triggers designed to flag and identify potential threats, you can take a proactive approach to investigation, enabling action before security incidents occur

Data retention policies

What is it?

The ability to define a retention policy based on the date assets were created or last accessed.

What's a simple way of understanding this?

There's a general rule of thumb with information security: The more data you house in a system, the more risk you're exposed to. It's unavoidable. So the best thing any company can do to lower its overall risk profile is to make sure the data that it's storing (wherever that may be), actually should be stored or retained!

Smartsheet data retention works simply. Set a policy based on creation and updated by date (i.e. "delete sheets if they haven't been updated in 60 days and were created over a year ago") and content will auto-delete based on that policy. Of course, content owners also get a notification that deletion is scheduled, giving them the opportunity to take action to prevent it.

How does this protect my data?

It lowers the overall risk profile of your business by removing unused content from your account.

Summary

Putting the pieces together: Security and governance as a whole

Smartsheet Safeguard supports our customers working with sensitive, private, or regulated data by providing a package inclusive of all the most powerful security and governance controls offered by Smartsheet. But it's important to note that these capabilities aren't meant to work individually — the benefits of each capability are compounded when combined with the others. Through Smartsheet Safeguard, you gain security and control of data at every stage of its journey:

- From base access, with **Customer-managed encryption keys** controlling who can decrypt your data
- To **data egress policies**, preventing internal or external collaborators from saving or exporting data
- To the deep auditability offered by **event reporting**
- Which can be made into an active notification vehicle through the implementation of **data loss prevention** capabilities
- And finally, the deletion of unused content is handled by **data retention policies**

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