External Security FAQs

Where does our Smartsheet data reside?

- ✔ **Smartsheet Commercial environment:**
  AWS East regions (Virginia/Ohio)
- ✔ **Smartsheet Gov environment:**
  AWS GovCloud West region (Oregon)
- ✔ **Smartsheet EU environment:**
  AWS EU regions (Germany/Ireland)

How is High Availability and Business Continuity achieved and maintained?

Smartsheet's Business Continuity/Disaster Recovery implementation maintains current data through the use of three availability zones - essentially, data is backed up to separate AWS regions to ensure business continuity. The punchline? **Smartsheet provides a 99.9% Availability SLA.**

What types of [encryption] key management does Smartsheet provide?

By default, Smartsheet provides and manages encryption keys on behalf of our customers. This is done based on AWS issued certificates, enhanced by Smartsheet use of a private CA. Alternatively, Smartsheet offers CMEK (Customer Managed Encryption Keys), as a premium capability customers can elect to purchase.

How are backups managed and protected?

Smartsheet conducts daily incremental and weekly full backups. Backups are maintained in dedicated AWS S3 buckets. Smartsheet has security controls in place to protect the confidentiality, integrity, and availability of Smartsheet backup information at storage locations. Access to backups is restricted to appropriate personnel, replicated across two availability zones, and encrypted in S3 utilizing AES 256-bit encryption.

What logging capabilities are available?

Smartsheet provides several types of exportable logs within the application, which customers are able to review at their discretion. These include reports on user login history, sheet access, a sheet-level activity log, and cell history within individual sheets.

Additionally, Smartsheet offers Event Reporting as an advanced capability for enhanced monitoring of actions that occur in Smartsheet.

With Event Reporting, customer administrators gain access to a [JSON] feed showing all events logged via our API, including account level actions. Data can then be sent to a log analysis platform such as a SIEM or CASB service – Smartsheet provides dedicated integration with the Skyhigh Cloud Access Security Broker (CASB) and Microsoft Cloud App Security (MCAS) platforms.

What controls do you offer to oversee how users leverage the application?

Smartsheet offers flexible and robust administrative functionalities that can help provide peace of mind about how your employees are able to collaborate in Smartsheet. For example:

Approved Domain Sharing List (also called Safe Sharing)

- ✔ Control the domains and email addresses that users are able to share data with.

Data Egress Policies

- ✔ Prevent unwanted data from leaving your organization.
- ✔ This control allows Admins to set policies on who can export, save as new, and download data from Smartsheet sheets, reports, and dashboards.

Event Reporting

- ✔ Advanced monitoring of actions that occur in Smartsheet.
- ✔ Through this capability, customer administrators gain access to a (JSON) feed showing all events logged via our API, including account level actions. Data can then be sent to a log analysis platform such as a SIEM.

These controls - and more - are detailed in our comprehensive security whitepaper, which we recommend checking out.

How is data segregated and protected?

["I want to ensure that other companies can't access our data. There should be complete separation from other tenants in Smartsheet's cloud environment."]

Smartsheet is a multi-tenant SaaS solution, employing a data access protection layer. The data access protection layer sits between the application and database components, and handles requests to the database by the application.

This service ensures that customers are only able to access data specific to their account and not another customer's data. It also ensures that direct interaction between sensitive layers of the application does not occur.

Furthermore, Smartsheet uses encryption for data-in-transit (HTTPS utilizing TLS v1.2) and data-at-rest (AES 256-bit).

“Some of the data in our sheets is sensitive - is there a way of exposing only part of what’s included?”

If there’s a particularly sensitive data set that someone would like to share parts - but not all of - they can use Smartsheet Dynamic View to maintain confidentiality while making specific elements visible or editable by a broader team.

“Some of our attachments are sensitive - I don’t want all sheet users to be able to access every document we attach. I want to be able to put limits on attachments.”

User access to linked documents will respect permissions set in the third-party application.

Smartsheet Admins can choose sources that are enabled for user attachments; “Upload from Computer” (or any of these options) can be disabled to ensure employees are only able to attach items from approved sources.*

File library temporarily excluded

Smartsheet attachments do not create copies of documents from cloud-storage providers, only reference URLs, so content will always reflect the latest.

How can I integrate Smartsheet with the rest of my tech stack?

Smartsheet offers a range of connectors, integrations, and other ways to connect our application to your enterprise tech stack.

You can read about these in more detail on our connectors and integrations page online, but in brief, we offer:

- ✔ Smartsheet-created (and maintained) bi-directional connectors to Salesforce, Jira, and MS Dynamics 365.
- ✔ Identity Provider (IdP) integrations with Google, Microsoft Entra ID, and SAML 2.0 compatible identity providers like Okta or ADFS
- ✔ A bi-directional connector to Servicenow through our partner Rego consulting.
- ✔ 100+ additional integrations to other primary applications like Slack, apps from our partners like Microsoft and Google, and additional integrations with Docusign, Adobe, and much more.
- ✔ Data Shuttle, which allows you to upload or offload CSV or XLSX files between Smartsheet and your ERPs, CRMs, and other systems — enabling you to create and maintain a centralized source of truth.
- ✔ Open Smartsheet API that allows developers to create custom-built integrations with Smartsheet.

I just found out that sensitive data may be in Smartsheet; should I be concerned and how should I think about the security of that enterprise data?

✔ It's important to take data governance seriously, and Smartsheet provides enterprise-grade capabilities to help organizations protect and manage sensitive data effectively.

A strong security posture combines **governance policies, administrative controls, and user best practices** tailored to your organization's needs. Smartsheet empowers IT and security teams to enforce governance policies through:

- **Access and sharing controls** – Safe Sharing, enforcing MFA or TOTP (temporary one-time passcode) requirements for external collaborators, domain validation, and SAML authentication to prevent unintended data exposure
- **Audit and monitoring** – Asset- and account-level insights via access reports, activity logs, and event reporting.
- **Technical safeguards** – Administrators can enforce data egress policies to prevent unauthorized data export via downloads, email attachments, printing, or external publishing. Customer Managed Encryption Keys (CMEK) enable organizations to control their own encryption keys for an added layer of security. Offline form submission controls restrict mobile data collection when required. Web Content Widget Controls allow organizations to define approved domains for embedded content, reducing external data risk.

We recommend working with your IT and security teams to establish governance policies that align with your organization's risk posture. Smartsheet provides resources for IT teams, including best practices for technical controls and policy enforcement.

For additional guidance, our **Office of the CISO (OCISO)** is available to help navigate best practices for secure collaboration and data protection within Smartsheet.

Is Smartsheet HIPAA Compatible? What compliance frameworks do you support?

✔ Yes; many Smartsheet customers elect to use our service to receive, maintain, or transmit some types of PHI in accordance with their HIPAA obligations. For specific product eligibility, control configurations, and recommendations, please see our [HIPAA article](#).

✔ For an overview of additional compliance frameworks Smartsheet supports, please visit [our compliance page](#).