Smartsheet Security

An in-depth view of Smartsheet security capabilities, practices, and protections

Executive Summary

At Smartsheet, we understand that enterprise-grade software as a service (SaaS) platforms must offer multiple layers of defense and a myriad of IT protections and controls to keep sensitive company data secure. It's also important for these solutions to be flexible and integrate with existing data security systems and processes.

This whitepaper is intended to showcase Smartsheet security and governance capabilities, protections, and practices. Primarily, we'll focus on the customer controlled capabilities that Smartsheet recommends implementing in order to maintain a secure, compliant, and well-governed work environment. Please note: This whitepaper does not include security capabilities that are not yet generally available.

Overview

To best secure your organization, we recommend implementing controls around three main areas of focus: identity and access management, data governance, and global account configuration. In addition to these topics, this document includes high-level information regarding Smartsheet security, privacy, and compliance practices.

- **Identity and Access Management** focuses on controlling how your users gain access to Smartsheet, ensuring that each user's role and identity within the platform aligns with your organizational structure and policies. Additionally, we'll discuss how to ensure security when collaborating with external users, based on your security preferences.

- **Data Governance** must be enforced at both a user level and across the organization. For users, a least privilege approach is the default in Smartsheet, with additional controls available to further constrain and control visibility so users are only exposed to what they need, when they need it. At the organizational level, we'll cover both simple mechanisms like safe sharing and user reports, as well as optional advanced capabilities available like data egress policies.

- **Global Account Configuration** enables you to customize the aesthetics of your Smartsheet environment to match your organization's brand. Even something as simple as a visual cue confirming that users are within the organization's protected environment can help ensure your security. Ensure consistency by locking that branding and customization in place so each and every asset created will be in line with your brand.

- **Security, Privacy, and Compliance Practices** refer to the actions and protections Smartsheet maintains outside our platform, to help ensure customer data remains highly secure. Smartsheet has implemented industry leading, defense in-depth strategies through a combination of people, processes, and technologies to protect the confidentiality, integrity, and availability of Smartsheet environments and assets.

Table of Contents

Identity Management

Managing a user's identity in Smartsheet and, as such, their access to the system is just as important as managing data in the platform.

Early in your Smartsheet deployment, you'll decide which authentication method you want to use. Smartsheet offers different options: email and password, and Single Sign-On (SSO) methods from Google, Microsoft, SAML 2.0 providers, and Apple.

You can select one or more methods for your organization, though we recommend enforcing a single SSO authentication method for all users, with other methods disabled. We also recommend adding another layer of security by implementing Multi-factor authentication (MFA) when you configure your SSO.

For organizations with multiple domains or federated IT structures, Smartsheet also supports domain-level SSO enforcement. This allows system administrators to specify that users from a given email domain—like "@regionaloffice.com" or "@subsidiary.org"—must authenticate using a designated identity provider, such as Google or Azure. This ensures strict login enforcement by domain, enabling tailored identity policies across business units while improving governance and risk mitigation.

Smartsheet has a robust set of REST APIs. The Smartsheet API uses OAuth 2.0 for authentication and authorization. An HTTP header containing an access token is required to authenticate each request. For additional security, use OAuth 2.0 for any integrations you build as a best practice.

Access Management

Managing users and their access is a core administrative function that can impact both security and your organization's adoption of Smartsheet. Organizations must strike a delicate balance, encouraging collaboration while managing risks as data and teams become increasingly distributed. To support this, Smartsheet offers three distinct governance models in line with the primary ways our customers have looked to manage the application.

Smartsheet Governance Models

The first approach is our decentralized (federated) model, where individual business units control their own purchasing and plans directly. In this model, IT is typically not involved in administration, and plan billing, governance, and user management are left to departmental discretion. This model generally applies for companies earlier on in their Smartsheet journey.

Our second approach is the centralized (consolidated) model, where Smartsheet plans have all been consolidated into a single, IT-governed subscription. This provides direct control over spend, user management, and security controls. This model is best suited for IT teams that want to maintain close oversight over every aspect of their Smartsheet experience.

Finally, our shared (hybrid) model is meant to provide a middle-ground approach, where IT controls organization-wide settings using Enterprise Plan Manager, while license and user management are governed directly by line of business system admins. Billing is also separated by plan, supporting departmental billing, or a model where Smartsheet spend is incorporated into departmental budgets versus centrally billed to IT.

To ensure high standards for security, Smartsheet recommends our shared or centralized models, which provide more direct IT control over your plan(s).

User Administration

As various teams in your company independently adopt Smartsheet for their own needs, multiple, separated plans may be created. Mergers and acquisitions can contribute to an environment with multiple Smartsheet plans.

To manage users in these plans using the decentralized model, we recommend enabling Account Discovery for each of those plans. As new users are exposed to Smartsheet, that allows them or any person from your organization's domain to see a list of the Smartsheet plans associated with your company, providing a centralized means to request to join one of those existing plans, rather than starting a new one. Those requests are automatically routed to your system administrators (via the Smartsheet Admin Center) for review and approval.

If you have multiple separated plans and wish to manage users with the centralized model, you may have to complete an account consolidation. Note: customers with Advance capabilities such as Dynamic View, Connectors, and Control Center will need to partner with Smartsheet support for additional assistance with some aspects of consolidation.

If you're using the shared model and Enterprise Plan Manager, a best practice is to organize plans around departments/teams/cost centers. That enables you to define a policy to automatically assign users to the relevant plans based on their affiliation to one of these entities.

Licensing/Subscription models

New Smartsheet customers universally enjoy access to our updated pricing model, which provides enhancements like more transparent, predictable pricing, faster value realization, and increased ease of management. However, some customers remain on our legacy collaboration model and you may find yourself working to understand the differences between these two models.

Legacy Collaborator Model

Our legacy collaborator model was built on the foundation of giving creators access to the product while enabling free collaboration as an Editor or Commenter. That resulted in significant growth through viral adoption, but also resulted in fewer users being able to take full advantage of the platform. Only users who needed to create sheets, reports, dashboards, or workspaces were required to pay. Under this model, System Admins faced challenges in understanding Smartsheet user types, effectively managing their users, assigning licenses appropriately, and demonstrating the platform's value to their leadership teams. We made it more difficult than necessary for customers to do business with us.

User Subscription Model

While creation is important, Smartsheet is a collaborative work management platform; collaboration is at our core. The power and value of the Smartsheet platform truly stand out in enabling teams to create processes, programs, and projects, and collaborate on critical business initiatives. The user subscription model overcomes all the challenges of our legacy model. It adapts to your evolving business needs, helping you achieve your goals as your organization grows, through the introduction of:

- New User Types.
- Provisional Use.
- Reconciliation Periods and True Ups.

Read the brief for more on these changes and our User Subscription Model.

User Management

Smartsheet understands that adding users one at a time may not scale as adoption grows to dozens, hundreds, or even thousands of users. As such, when getting started, we recommend leveraging the bulk user import feature in our Admin Center, which easily adds up to 1,000 users at a time to your Smartsheet organization. Similarly, you can also use bulk update to edit roles and user types en masse.

Mergers or acquisitions often result in rebranding, with users getting new email addresses. User Merge can help you bulk update the primary email addresses of users and clean up any duplicate accounts.

A consolidated Smartsheet plan can use three additional capabilities to further streamline and automate user management:

- User Auto Provisioning (UAP) automates the process of adding users to an enterprise account. As users sign up or sign in to Smartsheet with their company email address, they will automatically be added to your account. Additionally, you can choose whether users should be granted licenses versus automatically joining the account as non-licensed (free) collaborators.
  - If you've adopted our consolidated model, we recommend enabling UAP so employees automatically join the central, IT-controlled account.
  - If using our shared model (and if your organization has documented department/cost-center information for your user list), we recommend turning on UAP, as that information can be imported to automatically associate users with the right plan when they request a license. It can also be used to automate the movement of unlicensed users between plans.
- Directory Integrations allow you to directly sync your Microsoft Entra ID or Okta Directory users into Smartsheet. Plug Smartsheet into your existing automation in Entra ID or Okta to fully automate user onboarding and offboarding, minimizing the risk of users lingering in or revisiting their Smartsheet accounts. As an added benefit, user-level attributes such as department/cost center/division are included in a Smartsheet Chargeback Report, which is available in Admin Center and can be used to facilitate internal chargeback. A recommended best practice is to sync all users in the Directory into your organization's Smartsheet account. This prevents those users from creating additional "shadow IT" Smartsheet accounts when logging in for the first time. As a second layer of defense, you can also leave UAP enabled as a catch-all for users who may not already be synced through the Directory.

When a person leaves your organization, it is important to remove their access to Smartsheet. We offer two ways to do so. Deleting a user removes them and assets they own from your Smartsheet account, but this can cause items still in use to be removed, potentially breaking solutions that rely on that data. Instead, Smartsheet recommends Deactivating Users. This still fully prevents them from accessing Smartsheet, but preserves accessibility to their content, eliminating any necessary considerations around solution stability or ownership transfers.

Roles and User Types in Smartsheet

Regardless of your user provisioning method, you will need to determine Smartsheet roles for the people in your organization.

Note that a role assignment doesn't give the person access to Smartsheet assets in your organization. The assets must also be directly shared with those people. As such, both role and asset access permissions will determine what stakeholders can see and do in Smartsheet. Smartsheet supports the following primary roles:

- Licensed User: Use licensed features, such as creating sheets.
- Group Admin: Create and manage Smartsheet groups. (must also be a licensed user)*
- System Admin: Manage users, account settings, and security controls.

We strongly recommend assigning at least two active system administrators for your organization's Smartsheet account so that there is no disruption if one System Admin is unavailable at any given time.

Group Admins can create Smartsheet groups, allowing users to share content with the group rather than requiring users to share with each member individually. Group Admins can only manage groups they own. As needed, to limit external collaboration, restrict group membership to only stakeholders within your organization.

If you don't assign any of the above roles to a user, their access will be limited to only those Smartsheet assets (sheets, reports, dashboards, or workapps) shared to them. In order to create Smartsheet assets, stakeholders must be licensed users, and can request a license through the Smartsheet app directly. System Admins can track and respond to requests individually or in bulk through the Admin Center's License Request Management section. If you already have an established process for managing license requests, you should consider taking advantage of a Custom Upgrade Screen to direct users to submit their license requests via those internal processes.

External Collaborators

Any stakeholder outside of your domain who is shared to your Smartsheet assets is considered an external collaborator. Smartsheet empowers your organization to collaborate freely with any trusted external parties, with no associated cost for these external collaborators. To ensure security when partnering externally, we recommend leveraging three central admin controls:

Safe Sharing lets you specify domains or email addresses that are trusted and authorized for external collaboration.

Sheet Access Reports provide a list of external collaborators who have access to your organization's Smartsheet content.

Revoke Access to Items, centrally through the Admin Center, so external collaborators are removed from content they no longer need to access.

External Collaborator Authentication Controls

To further protect sensitive content when collaborating with users outside your organization, Smartsheet offers enhanced authentication verification for external collaborators, ensuring only authorized users are granted access to your content.

External Collaborator Single Sign-On (EC-SSO) allows system admins to **enforce the use of corporate identity providers**—ensuring that only users verified by SSO have the ability to access content shared.

Additionally, External Collaborator Multi-Factor Authentication (EC-MFA) gives administrators the ability to **require MFA enforcement for external users as a condition of access**. When enabled, Smartsheet checks with the external user's identity provider at the time of login to confirm that MFA was used—blocking access if that requirement is not met.

These capabilities provide enterprise IT and security teams with the flexibility and confidence to scale collaboration securely, particularly in highly regulated or risk-sensitive environments.

Data Governance

Effective data governance is indispensable for today's enterprise to ensure the information owned by the organization is created, used, shared, and protected in line with the applicable regulations, company policies, and industry best practices.

These controls are needed not only for regulatory purposes but also to ensure efficiency, business confidentiality, and business continuity:

At the user level, the organization needs to provide effective tools to constrain visibility; only showing relevant stakeholders relevant information.

At the organization level, the enterprise needs to be armed with applicable tools for effective policy creation and enforcement.

Data Governance at the User Level

Most users are familiar with permission levels in Smartsheet (viewer, editor, admin, and owner). Dynamic View and WorkApps provide additional, more-granular controls and flexibility, helping provide effective data governance capabilities at the user level. Limiting access to only the most relevant content both helps ensure process efficiency (as users must necessarily focus on items needing attention), but also ensures security by extending the Smartsheet approach of least privilege by default to a more granular scale.

Dynamic View

Not all business processes warrant full transparency. Many processes — order management, vendor collaboration, projects involving mixed internal and external teams — require tight control over what is shared with whom.

Dynamic View allows collaboration without compromising on confidentiality. Using Dynamic View, sheet owners can selectively share relevant rows and fields with specific collaborators — without sharing the underlying sheets. This enables several use cases wherein specific business users can selectively share elements with vendors, mixed internal and external teams, or across organizations, inviting collaboration only on certain fields. Everyone has access to the information they need — and only the information they need.

WorkApps

WorkApps allow you to streamline your work and simplify collaboration using easy-to-navigate apps built directly from your sheets, forms, dashboards, reports, and more. You can tailor each app's experience for your team members based on each person’s role, and work together from the same underlying datasets. Apps scale using the same enterprise-grade, multi-level security as the Smartsheet platform.

WorkApps eliminate the need to share the underlying assets that constitute the WorkApp. You can create a WorkApp with a filtered view of selected sheets and reports, but none of those sheets or reports need to be shared with the end-user. They only see the “WorkApp” view of those assets.

Data Governance Policy Controls at the Organization Level

Smartsheet empowers administrators to ensure the capabilities of the platform are used within the organization’s governance policies. These controls allow admins to implement good data governance guardrails to ensure data is handled correctly and by only those who need to interact with said data.

Administrators can pick and choose how they want users to interact with specific features. Should sheet owners be able to publish their sheets and create new automations? Do you have a specific storage system that files must be attached from? Should external collaborators be able to download content shared with them? These are examples of questions administrators should ask themselves to effectively evaluate the appropriate organization-wide controls to implement.

These policy controls also extend to safe sharing. If you want to limit data and asset sharing to specific domains or email addresses, this is the tool to use. As previously mentioned, safe sharing also determines whether your organization can share Smartsheet items with other organizations, such as vendors and partners.

Web Content Widget Control

Dashboards support the ability to embed interactive content (videos, charts, docs, and more). Admins have the ability to enable or disable this feature and define an approved list of supported domains for the web content widget. As a best practice, we recommend limiting this to internal company domains.

Automation Permissions

Control who can receive automation from sheets. Options are organized from Restricted (only enables actions for users shared to the sheet) to Unrestricted (where automation is applicable to any email address and third-party integration, such as Slack). We recommend that you review this control to ensure that its configuration matches your organization’s desired level of internal and external collaboration.

Attachment Controls

Determine whether plan members can upload files from their own computers, by attaching a link (URL) to a site, or from third-party cloud storage services including Google Drive, OneDrive, Box, Dropbox, Evernote, or Egnyte. To prevent the ingestion of data from unapproved sources, enable only those attachment providers that are approved for use based on your organization’s internal policies.

Publish Controls

Publishing a sheet, report, or dashboard generates a unique URL that anyone can access without logging in to Smartsheet, and iframe code that you can embed within the source code of a website to display the sheet or report.

You can disallow the publishing of sheets, reports, dashboards, and iCal — the Publish button no longer appears on the Smartsheet asset. You also can restrict access to published items to only people within your Smartsheet organization. We have observed that security-conscious customers generally allow publishing, but limit access to published items to people within their account.

Safe Sharing

Use this capability to restrict sharing by domain or by specific email addresses (e.g. to ensure that sheets are shared only to people with a company email address). Smartsheet strongly recommends implementing safe sharing to control external collaboration. Additionally, to simplify updates and maintenance of your safe sharing list, we recommend that you collect any update requests using a Smartsheet webform.

Offline Form Submission Controls

When using the mobile app, Smartsheet automatically enables forms to be submitted while offline, to support use cases where users may not have a consistent connection (e.g. on a construction work site). This control provides admins the ability to turn offline form submissions off (or back on) to control whether a user is able to launch the mobile app without a connection, to submit forms.

Communication Integration Controls

Smartsheet supports Google Chat, Microsoft Teams, Slack, and Cisco Webex as supported communication services. Account administrators can enable one or multiple services, at your discretion.

Logging and Reporting

You can download reports covering different aspects of Smartsheet usage across your organization for ongoing visibility into Smartsheet usage, users, content, billing and access:

Sheet Access Report

Generates a CSV listing the names of all sheets, reports, and dashboards owned by the plan on the account, the name of the workspace these items are saved in (if applicable), the collaborators shared on each sheet, and the timestamp of last modification. We recommend reviewing this report periodically to audit the list of external collaborators who have access to assets owned by people in your organization.

Published Items Report

Generates an Excel file listing all items that have been published. Great for data security or tracking down who published specific items.Use this report to inform the configuration of the Publish control as needed.

User List Report

Generates a CSV listing all members (both invited and active) on the plan, a timestamp for when they were added to the plan, their access levels (System Admin, Group Admin, etc), the number of sheets they own, and the timestamp of their last login to Smartsheet.

Login History Report

System Admins on multi-user accounts can use Admin Center to receive a report with a list of recent login history via email.

Chargeback Report

Available in Admin Center, customers using directory integration can use Chargeback Reports to facilitate internal chargeback. This adds columns for division, department, and cost center to the existing report created when customers download their user list, providing the data needed to perform internal chargeback reporting.

Other logging/Monitoring Mechanisms

- **Activity Log:** Provides an audit trail of changes made to an asset, who made them, and when they were made. This includes edits such as row deletion (with the data that was deleted), who has viewed the item and sharing permission changes.

- **Cell History:** Displays a log of changes made on the cell level, detailing who made the changes, what they were, and when they were made. Users can easily use copy-paste from cell history to restore previous information that may have been improperly deleted or changed.

- **System Columns:** Show the time that each row was last edited and the collaborator who made the change.

- **Security Score:** Helps SysAdmins assess and strengthen their Smartsheet security posture by providing a data-driven score based on implemented security capabilities. Rooted in industry best practices, the score includes a categorized policy breakdown and an intuitive metric to track security strength and improvements over time. Accessible within the admin center.

- **Event Reporting:** An advanced capability that provides visibility into over 100 types of security and user activity events for a comprehensive audit trail. (See more about Event Reporting below.)

Advanced Data Governance Controls

Smartsheet offers a number of advanced capabilities that provide data governance control for clients with particularly stringent data security needs. These capabilities are included in Smartsheet Advance Platinum and Smartsheet Safeguard.

Data Egress Policies

Sharing data always involves some level of risk, but when dealing with particularly confidential content, ensuring that company data remains only in your account and in your control is paramount.

System administrators can use data egress policies to protect confidential information through granular control over how data can be exported both within and outside your organization.

Data egress policies can be implemented to prevent internal and external collaborators from taking the following actions on sheets, reports, and dashboards:

- Save as new
- Save as template
- Send as attachment
- Publish.
- Print
- Export

Users that attempt a restricted action will receive notification that the behavior is prohibited due to the data egress policy your organization has implemented.

These limits are designed to prevent collaborators from saving or sharing confidential information for malicious purposes.

Event Reporting

To ensure information security, many enterprises require ongoing insight into how their business applications like Smartsheet are being used. It is prudent to maintain visibility into:

- Who is creating sheets?
- Who is creating workspaces?
- Who is deleting objects?
- Who shared a sheet with whom?

Event Reporting provides granular visibility into user behavior and activity within your organization's Smartsheet account. This feature enables you to monitor data loss and identify anomalous patterns in usage, so you can more tightly enforce organizational security and compliance policies.

Event Reporting provides a JSON data feed of Smartsheet usage events ("Events") within a plan (org), accessed via the Event Reporting API. The service reports on more than 120 events in Smartsheet and stores up to six months of data, beginning with the date when the feed is enabled.

To benefit from that feed, Event Reporting data is typically integrated with other security systems that provide monitoring, notification, policy creation and enforcement, and data loss prevention (DLP). These apps are sold by third parties — typically Cloud Access Security Broker (CASB) systems, Security Information and Event Management systems (SIEMs), or a combination of CASB and SIEM working together. Sometimes enterprises develop their own monitoring and response systems, instead of relying on those provided by third parties.

Event Reporting key use cases:

- Data loss prevention
- Personally identifiable information (PII) data handling
- Data governance
- Gain insights on collaboration

Data Retention Controls

The more content your organization has in any SaaS application, the more risk your business takes on.

Smartsheet Data Retention Controls give organizations the ability to create a policy that dictates when content should be deleted, based on the criteria they elect to enforce.

These policies can be based on the date a sheet was created or the last time it was modified, ensuring only active or recent content is maintained within your Smartsheet instance and limiting your risk profile.

Customer Managed Encryption Keys (CMEK)

Important note: Effective on August 16, 2024, CMEK is no longer included in Smartsheet's Advance Platinum or Safeguard offerings. CMEK is available to purchase as a standalone offer for customers who meet the purchase criteria.

Smartsheet uses encryption to secure customer data and help customers maintain control over it. Customer managed encryption keys (CMEK) are intended for organizations that have sensitive or regulated data that requires them to manage their own encryption key. CMEK allow enterprise organizations to use cloud SaaS applications while maintaining data control comparable to that of an on-premises installation, adding a customer-managed layer of encryption to Smartsheet data storage to support advanced data security and governance policies.

To use CMEK, customers must have access to Amazon Web Services Key Management Service (AWS KMS), as customer keys are set up and managed directly within AWS.

Smartsheet uses CMEK to encrypt your organization's data such that it remains under your control at all times. Specifically, Smartsheet does not store or control these encryption keys and Smartsheet must request and retrieve the keys from our customer's AWS Key Management Service (KMS) whenever Smartsheet needs to access your sheet data.

As your organization controls the CMEK stored in AWS Key Management System, you can revoke Smartsheet access to the CMEK and, thereby, access to your data at any time. By destroying the master keys in the AWS Key Management System, your organization can effectively delete your data from Smartsheet systems. A malicious party with a copy of the Smartsheet database, source code, and cloud encryption keys could still not read any of the data encrypted with CMEK.

Global Account Configuration

Account security isn't limited to technical features such as data encryption, classification or authentication options. Security can be something as simple as including your organization's logo on each and every item that belongs to it.

Global account configuration controls allow you to implement visual branding (and other restrictions) so your users know they're accessing the right information.

System Admins can add logos globally to bring your Smartsheet deployment in line with organizational branding requirements. Use the branding lock to ensure each new asset is branded the same.

Smartsheet customization controls and account configurations also allow you to set up custom welcome screens. You can create custom help screens with descriptions on how to get started, license request screens to help your users contact you, or customized and branded welcome screens that appear when a user logs in. Screens can include a requirement that a user approves the terms of service before they access more information.

Combining consistent visual identity along with custom information helps users know they're accessing the right tools and information and enhances your security.

Smartsheet Security, Privacy, and Compliance Practices

Utilizing a holistic approach, the cybersecurity, privacy, and data protection programs at Smartsheet begin with strategic information security policies defined and supported by the Smartsheet Information Security Steering Committee (ISSC) and the executive leadership team. These policies are designed to align with the organization's strategic risk management practices, proactively manage and monitor security risks, promote security through process maturity and effective system architecture, and enable users to make prudent decisions about security risks through training and awareness.

Data Security

We build security into our platform to ensure that your most valuable asset — your data — is protected. Smartsheet contracts with third parties to complete audits of our security practices, including a SOC2 Type II assessment and attestation, and third-party technical security assessments with penetration test firms. Furthermore, the Smartsheet vulnerability management program automates the identification and remediation of network and system vulnerabilities across Smartsheet corporate and production environments. Smartsheet uses encryption to secure your data and help you maintain control over it. Here's what you can rely on from Smartsheet: all data is durably stored with National Institute of Standards and Technology (NIST) approved ciphers, transport layer security (TLS) technology, AES 256-bit at-rest encryption, and Amazon's S3 service to store and serve uploaded files.

Privacy

At Smartsheet, we value your privacy and respect your right to know how information about you is collected and used. Our privacy notice describes how Smartsheet collects, uses, and discloses personal and other information we gather through our websites, our mobile applications, and the Smartsheet work execution platform.

- We recognize the privacy rights of our prospects, customers, and partners and adhere to global privacy regulations, including the European Union's General Data Protection Regulation (GDPR).
- We offer a Data Processing Agreement for our customers who require specific terms for the processing of content that includes personal information. If you have determined that you require a DPA with Smartsheet, you may submit a form agreeing to the terms of the DPA at smartsheet.com/legal/DPA.

Operational Management

We have implemented policies and procedures designed to ensure that your data is secure and backed up to multiple physical locations. Our teams are continually evaluating new security threats and implementing updated countermeasures designed to prevent unauthorized access or unplanned downtime of the subscription service. Access to all Smartsheet production systems and data is limited to authorized members of the Smartsheet Technical Operations team based on the principles of least privilege and need-to-know. Smartsheet publishes system status information on the Smartsheet status site. Smartsheet typically notifies customers of significant system incidents by email and/or text message, if they have signed up for automatic updates on the Smartsheet status site.

Data Center Security, Continuity, and Redundancy

We work with industry-recognized hosting partners to ensure that you can deliver services to your organization confidently on a platform you can trust. We have multi-site data redundancy, hosting at AWS facilities, and our facilities are SOC 1, SOC 2, ISO 27001, and FISMA examined and certified. Our monitoring includes biometric scanning protocols, continuous surveillance, and 24x7 production environment management. Smartsheet maintains internal processes and plans in order to address business continuity events and disaster recovery scenarios. These plans are reviewed and tested on an annual basis and are distributed to applicable staff throughout the organization. Our data centers are geographically isolated (approx. 600 mi) from each other to prevent the data centers from being impacted simultaneously in the event of a large-scale natural disaster.

Smartsheet Regions

Smartsheet Regions offers international data hosting options to support clients with regional data storage requirements or compliance obligations. To learn more, visit the Smartsheet Trust Center and our Data Residency page.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to core application services within Smartsheet.

- **SOC 2/SOC 3:** Smartsheet undergoes annual examination and testing as part of the SOC auditing process. The resulting external audit reports attest to the design and operating effectiveness of internal controls across our business, including security, availability, and confidentiality.

- **EU-U.S. and Swiss-U.S. Privacy Shield Certification:** Customer data submitted to the Covered Services is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the SwissU.S. Privacy Shield Framework as administered by the U.S. Department of Commerce. The current certification is available at privacyshield.gov/list by searching under “Smartsheet.”

- **HITRUST Readiness**: Smartsheet has achieved HITRUST Readiness status, reflecting our alignment with the HITRUST CSF framework and commitment to robust security and privacy controls. This designation underscores our ability to support customers with rigorous compliance requirements, including those in healthcare, finance, and other highly regulated sectors.

- **FedRAMP (moderate):** Smartsheet was selected for the FedRAMP Connect program by the Joint Authorization Board (JAB), which prioritized Smartsheet Gov for certification based on demand from federal government agencies. Smartsheet Gov is a separate Smartsheet environment with FedRAMP authorized status and is assessed at DoD Impact Level 4 (IL4), making it easier for the U.S. government to use Smartsheet for managing their work while helping them meet their security and compliance requirements.

- **Sarbanes-Oxley Act of 2002:** As a formerly public company, Smartsheet was previously required to comply with the Sarbanes-Oxley Act (SOX). While we are no longer subject to this regulatory requirement, Smartsheet has elected to maintain SOX-aligned internal controls to support strong financial governance and ongoing audit readiness. This continuity reflects our commitment to operational excellence and organizational integrity.

As noted on our legal webpage, Smartsheet uses infrastructure provided by Amazon Web Services, Inc. (“AWS”) to host customer data. Information about security and privacy-related audits and certifications received by AWS, including ISO 27001 certification and SOC reports, is available from the AWS Security website and the AWS Compliance website. For a full list of our certifications and additional white papers and data sheets, visit the Compliance page on the Smartsheet Trust Center.

Conclusion and Additional Resources

Work today (and tomorrow) needs a modern work management platform that is easy to use and secure. Through ongoing focus and investment, we've built Smartsheet from the ground up with strict data confidentiality requirements and capabilities. In addition to what's available today, we have a number of additional security features currently under development. To learn more about Smartsheet security capabilities, programs, and protections, visit smartsheet.com/trust and the additional resources below:

Smartsheet System Admin Online Help
Smartsheet Features by Plan
Smartsheet Integrations
Smartsheet API Documentation