# SMARTSHEET SECURITY

Abstract

This paper introduces the security policies, practices, and procedures in place at Smartsheet.

Readers will gain an understanding of the Smartsheet operating environment and application architecture, how security is built into this software-as-a-service (SaaS) product, and how the company's employees, partners and service providers safeguard customer data.

# Executive Summary

## The Consumerization of IT

Today's enterprise workers demand consumer-friendly collaboration tools that work in a mobile environment. This has led individuals and groups across the organization to search out and employ a variety of cloud-based apps (sometimes called "Consumerized IT"). Meanwhile, CIOs and CTOs struggle with growing concerns surrounding data security, privacy, and data governance related to these applications.

As Consumerized IT gains in both staff acceptance and workplace use, its adoption is prompting IT leaders to develop new policies and procedures that ensure better management and controls. But an organization's internal policies and procedures can only provide partial security. IT leaders need to have confidence in cloud apps' ability to secure data and provide robust, comprehensive reporting structures.

While enterprises are starting to define new security and management best practices for these cloud apps, corporate IT agrees on one critical point: The growing trend of employees finding and adopting cloud-based applications is the new reality.

For example, workers who want to increase team collaboration or streamline workflows often go in search of their own solutions without involving IT resources (or approvals) and find applications such as Smartsheet. As "Bring-Your-Own-Device" (BYOD) and "Bring-Your-Own- App" (BYOA) practices become entrenched in the workplace, developing policies to handle this movement has become a top priority for businesses of all sizes.

This paper provides an overview of Smartsheet's approach to security, including how security best practices have been incorporated into its application architecture from the ground up. It also describes how Smartsheet fits within the new governance requirements of corporate IT and examines how it handles customer data, monitors, verifies and manages ongoing security processes. Throughout, this paper provides proof points of Smartsheet's commitment to securing customer data.

## About Smartsheet

Smartsheet, a leading work collaboration platform, offers an innovative approach to collaborating on any project, task or business process. Accessible from any device or browser, Smartsheet combines the ease of use of a spreadsheet with collaborative file sharing and discussions, visual timeline management and automated workflow capabilities.

Organizations use Smartsheet to manage operational and project-based work throughout the enterprise. Its ease of use, robust security model and flexible capabilities have won support from both front-office and IT groups alike. Current uses include marketing programs, sales pipelines, product launches, strategic plans, HR processes, and core business operations. The platform provides a comprehensive API and comes pre-integrated with leading web services such as Google Apps, Box, Dropbox, Egnyte and Salesforce.com.

Since 2006, Smartsheet's proven track record for delivering an easy to use, secure and scalable system have made it a compelling choice for more than 74,000 organizations around the world, with millions of people collaborating in Smartsheet. Customers include small and medium sized businesses, Forbes Global 2000 companies, academic institutions, as well as local and federal government agencies.

# End to End Security: Architecture, Policies, Partners

For Smartsheet, keeping customer data private and secure is a key aim, as is access management and delivering a rich, built-in reporting structure to enable better management control. These objectives are at the heart of Smartsheet's application architecture, internal processes, and choice of technology partners.

The Smartsheet application is designed with many security layers, including safeguards that sanitize requests and responses as they enter and leave the product architecture. Smartsheet's core platform design separates business logic from data request and response processing, enabling Smartsheet to focus on building capabilities and business logic that leverage its built-in secure infrastructure.

Smartsheet has architected our networks and systems with "defense-in-depth" concepts in mind. Systems are built from hardened secure baseline images and assigned roles then deployed into pools of isolated like systems. Systems communicate via one way secure communication between source systems to target systems on defined ports and protocols.

Smartsheet's security practices are SOC2 examined and tested (Type II) and our application is penetration tested twice per year. Additionally, Smartsheet operates an ongoing Bug Bounty program to encourage security researchers to find security issues in our application.

> *"Unlike many SaaS applications, we started by building a secure programming framework and then created Smartsheet on top of it." – Mark Mader, Smartsheet President & CEO*

In addition to its secure development platform, Smartsheet employs a broad range of processes and policies to ensure data security. These include:

- A Secure Software Development Lifecycle (SDLC) process
- Risk management processes and procedures
- External audit and testing standards
- Twice annual application and network penetration testing
- Access control policies
- Cryptography controls policies
- Physical security standards
- Information classification, handling and disposal policies
- Incident response processes
- Disaster Recovery (DR) and Business Continuity Plans (BCP)

Smartsheet puts security first when we select technology providers and partners. Each undergoes examination by at least one third-party auditor to ensure it conforms to its own security policies and procedures. For example, Smartsheet's core hosting partner Rackspace undergoes annual SOC1 and SOC2 Type II auditing and is ISO 27001 Certified.

# The Smartsheet Operating Environment

Smartsheet's operating environment is illustrated in *Figure 1 – Logical Overview of Smartsheet Operating Environment* (below).

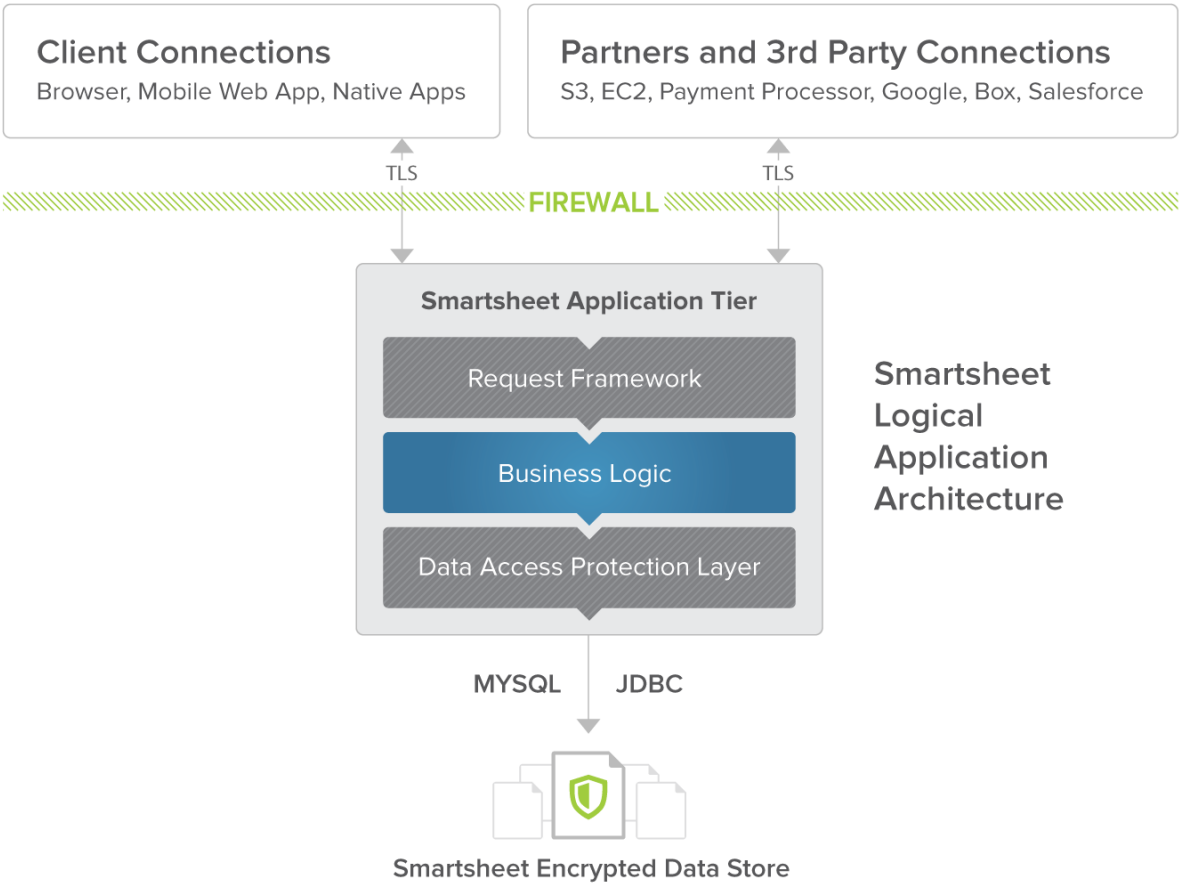


**Figure 1 – Logical Overview of Smartsheet Operating Environment**

Customers can access Smartsheet from desktop or mobile web browsers, the API, and native mobile applications. All communications between these clients and Smartsheet – as well as all third-party applications, such as those with a payment processor, Google or Salesforce – take place over a secure HTTP connection using transport layer security (TLS). This is also known as an "HTTPS" connection.

Smartsheet offers strong encryption for durably stored customer data and customer data while in motion, using proven 256 bit AES encryption for durably stored data TLS encryption from trusted, verified providers to protect all data transfers between your device and our servers.

The Smartsheet application is hosted on dedicated servers with Smartsheet's core hosting provider. Incoming traffic passes through an F5 BIG-IP firewall and load balancer. Smartsheet's application layer consists of servers running Security-Enhanced Linux (in enforce mode), Apache HTTPD, and Apache Tomcat. The Smartsheet application communicates with the Smartsheet Data Store built on Percona XtraDB MySQL Server, Lucene, and TokuMX, all running on a Security Enhanced Linux stack.

The Smartsheet Application Tier contains three components, or layers:

- Request Framework
- Business Logic
- Data Access Protection

The Request Framework and Data Access Protection layers are infrequently modified. Changes to either of these layers are permitted only after rigorous review and testing processes. Only requests by authenticated users are allowed to pass through to the Business Logic layer. The Data Access Protection layer prevents the Business Logic layer from reading or writing data if a user is not granted permission to do so.

The Request Framework performs input sanitation, data validation, session validity checking, and exception handling for incoming traffic. The Framework generates an immutable session object tied to the user making the request, thus limiting access to their user ID. It also manages transactional consistency and sanitizes responses to be browser-safe before passing data back to the requesting client.

Once the Request Framework Layer has performed its checks and has packaged the incoming request, it passes the request on to the Business Logic Layer where the majority of the application features are implemented. The Business Logic Layer uses the Data Access Protection Layer to enforce access control and data integrity, as well as logging historical data for later audit. The Smartsheet Data Store is only accessible to the Business Logic Layer through the Data Access Protection Layer.

## Designed and Tested for Availability

The Smartsheet application runs on load balanced servers designed with redundant components in a primary data center in Ashburn, Virginia with a secondary disaster recovery (DR) site in Chicago, Illinois. Smartsheet personnel perform disaster recovery testing of the service at least annually. Data replication between the primary site and the DR site typically occurs in less than 5 seconds and the DR site has the same capacity and security controls in place as our primary site.

Internally, Smartsheet performs routine monitoring of its servers. The Smartsheet platform automatically notifies the Technical Operations team if any metrics are reported back with out- of-range values. Multiple external monitoring systems track accessibility and performance of Smartsheet globally to identify issues before they can affect data security or network reliability.

## Smartsheet Permission Models

Smartsheet provides fine-grained access control to sheets and the data entered or uploaded into them by providing multiple role-based account level user types with corresponding permissions and similarly fine-grained, role-based sheet level permissions.

### Account Types

Smartsheet offers four different account level user types: SysAdmins, Licensed Users, Non-licensed Users and Free Collaborators. Licensed Users and Free Collaborators are available to all Smartsheet accounts. The SysAdmin role is exclusive to Team and Enterprise accounts, as is the Non-licensed user role. The Resource Viewer and Group Admin rights can optionally be granted to licensed users in Team and Enterprise account. The permissions of each account role are summarized in table 1.

*Table 1 – Overview of permissions for each type of account role.*

| | Team or Enterprise Accounts Only | | | All Other Accounts | |
|---|---|---|---|---|---|
| Permission | SysAdmin | Licensed User | Non-Licensed User | Licensed User | Free Collaborator |
| Manage account users | ✓ | | | | |
| Bulk transfer ownership of sheets | ✓ | | | | |
| Generate sheet access reports | ✓ | | | | |
| Removing sharing rights for sheets | ✓ | | | | |
| Download account user list | ✓ | | | | |
| View account user login activity | ✓ | | | | |
| Manage account settings | ✓ | | | | |
| Configure SAML integration | ✓ | | | | |
| Create and view reports | | ✓ | | ✓ | |
| Create templates | | ✓ | | ✓ | |
| Collaborate on sheets | ✓ | ✓ | ✓ | ✓ | ✓ |
| Create sheets | | ✓ | | ✓ | |
| Access resource views | | ✓★ | | | |
| Create and manage groups | | ✓★ | | | |

★ = The ability to view resources and create and manage groups are optional permissions that can be granted to licensed users in Team or Enterprise accounts only.

**Table 1 – Overview of permissions for each type of account role**

## Sheet Permissions

Smartsheet has four levels of sheet permissions:

1. Owner: Licensed user paying for account, typically the one who creates the sheet.
   *The sheet owner can then share the sheet to collaborate with others, and can define permission levels, including*
2. Admin: Able to manage sharing, sheet structure (columns), and locks.
3. Editor: Able to create, modify, and delete rows or cells. Editors can be granted permission to manage sharing on a per sheet basis.
4. Viewer: Able to view sheet data including attachments.

| Permission | Owner | Admin | Editor | Viewer |
|---|---|---|---|---|
| View Sheet | ✓ | ✓ | ✓ | ✓ |
| View Attachment | ✓ | ✓ | ✓ | ✓ |
| View Discussion | ✓ | ✓ | ✓ | ✓ |
| Send Row | ✓ | ✓ | ✓ | ✓ |
| Send Update Request | ✓ | ✓ | ✓ | |
| Edit Column | ✓ | ✓ | ✓ | |
| Edit Row | ✓ | ✓ | ✓ | |
| Lock Row/Column | ✓ | ✓ | | |
| Modify Sharing | ✓ | ✓ | | |
| Create a Sheet | ✓ | | | |

**Table 2 – Sheet Sharing Permissions Model**

## User Authentication Options, SSO, and SAML

There are multiple ways users can access their Smartsheet accounts:

1. **Direct:** Users can securely sign into Smartsheet (via https://www.smartsheet.com) with an email address and password.
2. **SSO (Single Sign On):** Users can securely sign on through external single sign-on providers such as Google and Azure AD.
3. **SAML:** For enterprise customers seeking additional security controls, Smartsheet has the capability of using a supported SAML 2.0 conformant identity provider for authentication. This gives organizations the ability to require more than a username and password for signing in. For example, an organization might also require:

    - Access to networks assets (through a virtual private network connection)
    - A password matching certain length and complexity requirements
    - Successful response to a security challenge
    - Multi-factor authentication (MFA)
    - Or any other mechanism available through the identity provider

    For a list of current identity provider partners, see the IDENTITY PROVIDER PARTNERS SECTION.

## Team Workspace Permissions

In Smartsheet, a workspace is an area in which sheets, reports, templates, and folders can be organized and shared with multiple people. New items added to a workspace inherit the sharing permissions of the workspace, and permissions apply to all contents within a workspace.

## Collaborating without providing access to data

Smartsheet provides several methods to gather data from users without providing access to the data contained in a sheet:

- **Smartsheet Web Forms**: Users can collect data into their sheet using a customizable web form generated from within Smartsheet. A unique link is created which can be emailed or embedded in a website for people to access. When someone fills out the form, the information is added to the sheet as a new row.

- **Smartsheet Update Requests**: Users can send ad-hoc requests via email to un-authenticated users. A unique link in the email allows the recipient to submit a one-time update to the requested data, directly from the email, without having to login.

- **Smartsheet Send Row / Sheet**: Users can send individual rows or an entire sheet to un-authenticated users via email.

### Publishing data for anonymous viewing

- **Smartsheet Publishing**: This optional feature allows users to publish data from their sheets to the web for access by unauthenticated users. Each published sheet format - HTML view, editable view, iCal calendar feed, etc. - has a unique link. Anyone with access to the link can access that particular format of the sheet data.

### Administrative Tools – Reports and User Controls

Smartsheet System Admins have access to a wide variety of reports and user controls, including:

- **Login Report**: This report captures a per-user login history for the last six months. This report can be downloaded for archiving and offline review purposes.
- **Sheet Reports**: These reports provide an overview of the sheets users have created.
- **Sharing Reports**: These reports identify the sharing permissions of sheets created by users on the team, including users outside the team.
- **Remove from sharing**: System Admins can remove an email address (user) from accessing all sheets.
- **Transfer ownership**: System Admins can re-assign sheets created by a user on the team to another user.

### Smartsheet API

Smartsheet provides a REST API built on the same core security model as the Smartsheet application. Because of the stateless nature of the REST API, Smartsheet uses OAuth 2.0 to securely manage authentication and authorization of API requests. This approach allows users to grant access to Smartsheet without providing their username and password. Access is also restricted to a specific set of scopes requested by the calling application at the time that access is requested and authorized by the user.

## Smartsheet Partners

Customers can further extend Smartsheet with pre-built integrations to leading web solutions, as described in the following examples:

### Cloud Storage Providers: Amazon, Google, Box, Dropbox, and Egnyte

When users attach files to a row or a sheet, Smartsheet uploads and stores those files on Smartsheet's encrypted Simple Storage Service (S3, from Amazon.com). As an alternative, customers can link to files in existing cloud storage accounts such as Google Drive, Box, Dropbox and Egnyte. These files are stored by those companies and are subject to the protections they provide. Lastly, users can provide links to files stored on servers behind company firewalls.

### Technology Partner: Salesforce.com

Smartsheet is an AppExchange partner with Salesforce.com. A Salesforce.com administrator can install the Smartsheet Project Management for Salesforce.com from AppExchange. Then, from within Salesforce.com, users can link Smartsheet project sheets to Salesforce.com accounts or custom objects, enabling secure, convenient single sign-on to Smartsheet with a user's Salesforce.com credentials.

### Identity Provider Partners

Smartsheet has pre-built integrations with the following SAML identity providers.

- **Active Directory Federation Services 2.0 or 3.0**: Microsoft's implementation of SAML 2.0
- **Okta**: www.okta.com
- **OneLogIn**: www.onelogin.com
- **VMware Horizon Application Manager**: www.vmware.com
- **Ping Identity**: www.pingidentity.com
- **Shibboleth**: shibboleth.net

## Native Mobile App Security

Smartsheet is committed to protecting customer data in native mobile applications. Our mobile clients store data in accordance with vendor best practices utilizing strong encryption.

## Customer File Storage and Backups

Smartsheet utilizes Amazon S3 for cloud data storage for two primary reasons:

- Amazon has a history of strongly protecting customer information.
- S3 provides several key features that align with our approach to security.

Smartsheet takes advantage of S3's fine-grained control set, including access control lists, query string authentication, and a storage proxy. Query string authentication, in particular, has allowed Smartsheet to build a highly flexible security model by enabling granular access controls for objects stored in S3.

### Attaching a Single File

When a user attaches a file to Smartsheet, it is sent to S3 over a secure connection and encrypted for storage. The files are encrypted using 256-bit Advanced Encryption Standard (AES-256).

## Retrieving a Single File

When the user downloads a file, the browser first makes a request to the Smartsheet application. The Smartsheet application generates a time-bound download token signed with Smartsheet's private key. The token is relayed by the browser to Amazon S3 which verifies the token and signature and then sends the file back to the browser. All communications take place over encrypted connections using the algorithm defined in RFC 2104 - Keyed-Hashing for Message Authentication. This flow is described in Figure 2 below.

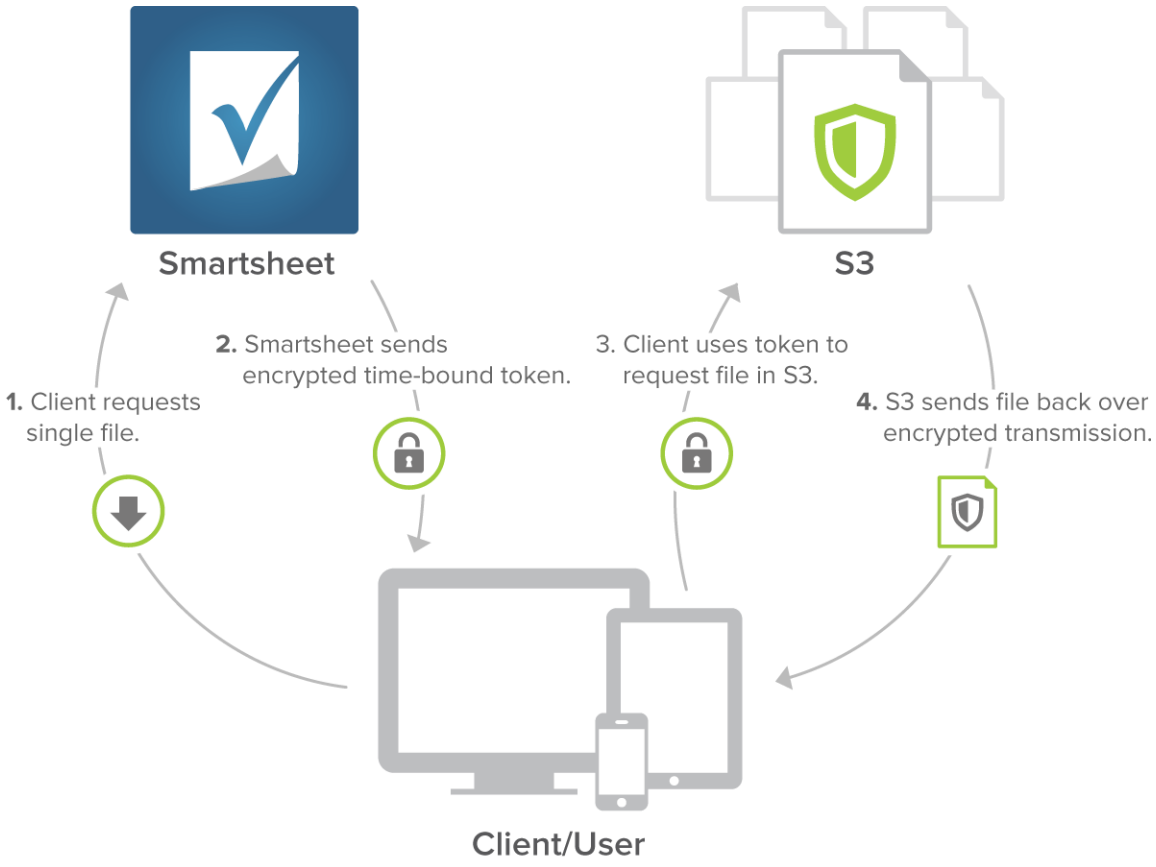


*Figure 2 – Retrieving a Single File Attached to a Sheet*

## Retrieving Multiple Files

Retrieving multiple files in a single download requires additional logic. Smartsheet created a proprietary S3 proxy service that runs on Amazon's Elastic Compute Cloud (EC2) to process multi-file download requests. This process collects files stored in S3, packages them into a single Zip file, and returns them to the user.

The process of responding to a request for multiple files involves using double-encrypted time- bound tokens. These encryption keys secure the list of time-bound tokens sent from Smartsheet to S3. Designing this process and creating the S3 proxy service are two examples of how Smartsheet has built security into the Smartsheet application.

### Customer Sheet Backup

In addition to the regular internal Smartsheet data store backup process, users can backup their sheets and attachments at any time. After selecting the data to backup, backup is a simple one- click method that downloads a Zip file containing the requested sheets and attachments. Recurring backups are available at certain plan levels and allow weekly automated scheduling and email delivery of backup links.

## Smartsheet Operational Processes

Smartsheet security is composed of a combination of application design, implementation processes, and internal operational policies and procedures.

### Privacy Policy

The Smartsheet Privacy Policy (www.smartsheet.com/privacy) outlines the very limited collection of personally identifiable information required to establish an account. For instance, Smartsheet requires customers who register to use the application to provide an email address, and upon subscribing, financial information such as billing name and credit card number.

All financial and billing information collected through Smartsheet is used solely to verify billing for prospective customers and to bill for the subscription. Smartsheet is not supported by advertising nor does it sell personal information to third parties.

Smartsheet is a licensee of the TRUSTe Privacy Program. To demonstrate its commitment to privacy, Smartsheet discloses its information practices and has its privacy practices reviewed for compliance by TRUSTe.

### Payment Data Safeguards

PCI DSS (Payment Card Industry, Data Security Standard) is a set of comprehensive requirements for enhancing payment account data security established by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International. It was developed to help the broad adoption of consistent data security measures on a global basis. On June 30, 2005, the regulations took effect as the PCI Data Security Standard. In October 2010, PCI DSS Version 2.0 took effect. Version 3.0 took effect in November of 2013.

In order to best safeguard customer payment card data, Smartsheet selected PayPal as its partner for processing all payment card transactions. Using PayPal means payment card data is never visible to any Smartsheet personnel, and is never stored in the Smartsheet Data Store. For account validation purposes, Smartsheet stores only the last four digits of account numbers. All payment processing is performed using PayPal's PCI DSS compliant merchant services.

Smartsheet encrypts all confidential information in transit from customer computer to PayPal’s servers using TLS with an encryption key length of at least 128 bits. PayPal’s servers sit behind a monitored firewall with extensive physical and logical controls and safeguards in place.

## Support Policy

Smartsheet employees have access to limited account information such as login history, historical error logs, sheet names, and limited account details. Smartsheet employees are unable to access data stored in sheets. For assistance with troubleshooting, the sheet owner/admin must first share the sheet with a Smartsheet Customer Support member. A Customer Support representative can also request the system to forward a copy of a sheet to the sheet owner via email, but the Customer Support representative cannot access the sheet.

### Password Reset Process

A password reset request can be made from the Smartsheet website or by contacting Customer Support. A link to reset account information will be sent to the registered Smartsheet email address and must be clicked by the customer to complete the process. At no time can Smartsheet Customer Support members view or directly reset passwords associated with a Smartsheet account.

Customers using a SAML identity provider can disable standard Smartsheet authentication so that password reset processes are entirely handled by the SAML identity provider.

## Technical Operations

The Smartsheet Technical Operations team manages the company's relationships with hosting providers and technology partners. They specify information security controls for the company and investigate escalated customer issues.

Like most online services, there are select Technical Operations team members who have extended access to manage and backup core Smartsheet systems. Members of this team must pass a rigorous hiring process including a detailed background check. A strict information security policy and technical access controls prohibit access outside of this team.

### Systems Management

Smartsheet's systems are built from hardened baselines designed to reduce attack surface. We enforce granular, limited user scope through the use of Mandatory Access Control (MAC) in the kernel of our Operating Systems. Vendor updates undergo risk analysis and are prioritized for deployment to production systems based on the outcome of this analysis.

### Internal auditing

Smartsheet has a formal information security review and audit policy and has developed processes to assure the routine review and confirmation of the efficacy of existing controls. Examples of these processes include quarterly system security reviews and an annual review of the audit program itself.

### External auditing

Smartsheet partners with an independent third party for twice-yearly penetration testing. This testing encompasses network and application penetration testing, social engineering attempts, code review, and more.

## Conclusion

The rapid adoption of cloud apps and mobile devices in the enterprise (Consumerization of IT) is fundamentally changing the way businesses think about data, access, and security. In order for cloud applications to gain IT approval for widespread deployment, they need to meet a growing list of requirements.

Smartsheet is focused on the privacy and security of its customers' data. This focus is reflected throughout the Smartsheet application and company. Smartsheet continues to meet and exceed users' expectations for ease of use and collaboration, while also winning the support of IT for data security and administrative controls. From application infrastructure to choice of technology partners, from data and internal process controls, ongoing auditing and third party testing – Smartsheet provides end-to-end security to secure customer account information and customer data.

Smartsheet has invested in this extensive end-to-end security to ensure that customers and their teams can confidently collaborate and share project information.

Additionally, when you consider many users often choose Smartsheet to replace tracking work in spreadsheets that are sent around via email, Smartsheet offers a superior security solution for business users and IT teams alike.

> *"It goes without saying: Smartsheet is heavily incented to offer customers the highest level of security – our business depends on it. When businesses choose Smartsheet, they're choosing a company with a proven track record of delivering a secure, scalable solution." – Mark Mader, Smartsheet CEO and President*

## Resources

Contact Smartsheet Sales at sales@smartsheet.com or 1-877- 765-0702 to discuss the options available through our Site and Enterprise Licensing program.