

A SMARTSHEET WHITEPAPER

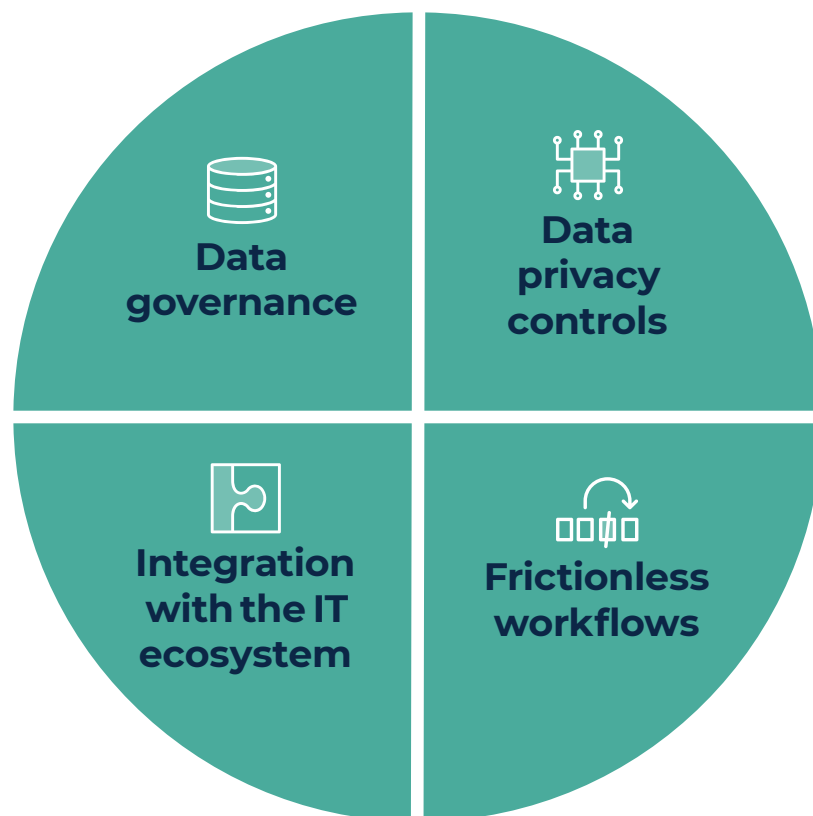
---

# 4 Essential Factors That Make a Collaborative Work Management Platform Enterprise-Grade

# 4 Essential Factors That Make a Collaborative Work Management Platform Enterprise-Grade

Data governance. Data privacy controls. Integration with the IT ecosystem. Frictionless workflows. A highly secure, enterprise-grade platform for collaborative work management (CWM) has to deliver these four essential factors. Here's what this means for you as you evaluate CWM platforms on enterprise-grade security, governance, and manageability.

Author: Chris Peake



In today's digital ecosystem, the term enterprise-grade gets thrown around a lot. But what does that term really mean, especially in the context of a cloud-based collaborative work management (CWM) platform?

Doing business requires seamless workflows that enable frictionless collaboration while maintaining a security-first approach to data. According to the [Spiceworks 2021 State of IT](#) report, 35% of organizations planned to rapidly move workloads to cloud-based services. This projection aligns with the pivots that many organizations are making to digital business objectives as they return to offices.





In a [IDG 2021 Pandemic Business Impact Study](#), return to office plans have understandably put more importance on increasing operational efficiency (65%) and internal collaboration (56%); and improving security (65%), business resiliency (61%), and customer experience (59%). Such findings further emphasize the need for businesses to adopt a CWM platform that supports key business objectives while ensuring data is secure.

As we move forward, the importance of a collaborative and secure remote workforce can't be ignored. In Nucleus Cyber's [2021 State of Remote Work Security Report](#), almost 80% of [IT] respondents cited security concerns with data leakage as the greatest potential threat, when it comes to supporting remote workers.

“ **80%** Almost 80% of [IT] respondents cited security concerns with data leakage as the greatest potential threat, when it comes to supporting remote workers. ”

Nucleus Cyber's 2021 State of Remote Work Security Report

So, as chief information officers (CIOs) and chief information security officers (CISOs) kick the tires on CWM platforms, they'll also need a platform that scales to the needs of their organization while offering:

-  **Dependable data governance**
-  **Transparent data privacy controls**
-  **Integration with the IT ecosystem**
-  **Frictionless workflows**

The ideal platform bakes in enterprise-grade security intelligently into every aspect of data — its governance, privacy, and workflows.

Enterprise-grade security is like an iceberg. On the surface, lots of applications and services “look” like they're enterprise-grade because they provide information about controls, compliance certifications, and security features like multi-factor authentication (MFA) and [single-sign on \(SSO\)](#). But the “real” commitments to making a platform enterprise-grade are more expansive than citing security-related table stakes on your corporate website.

Beneath the waterline is where the bulk of enterprise-grade security activities and commitments happen — an organization’s dedication to corporate security, identity access management, DevSecOps, code reviews, physical security, security architecture, and much more.

Such enterprise-grade security does not happen overnight. It takes years of systematic, security-first work to develop a CWM platform that is powerful, scalable, accessible, frictionless, easily-integrated — and secure across every interaction. This paper explores what each of the four key factors for enterprise-grade security looks like under the hood.





## 1 Dependable data governance

Given that data is vital in today’s business operations, policies around its use comprise the basic fabric of data governance. Data governance has broad purview over its availability, usability, integrity, and security. While these key parameters might have been easier to execute decades ago, over recent years, a number of factors have added to the challenges of data governance.

First, there is the sheer increase in the amount of data. Enterprises are gathering and using a lot more data from disparate sources. Second, digital transformation has accelerated the use cases for working with data.

At the same time, remote and hybrid work models have introduced added concerns about secure collaboration between teams. The sheer number of new work-from-home devices (endpoints) has also increased, which leads to questions about integrity and security of data flowing across networks.

The key tenets for enterprise-grade data governance in today’s work landscape include:

-  **Data sharing and data security occupy equal space.** Enterprises should be able to apply centralized policies related to threat management and other data governance procedures. Enterprise-grade data governance in this case means being able to apply guardrails around the usage of data. Companies need to be able to classify data according to levels of sensitivity and then manage specific types of data according to the types of sensitivity.
-  **The latest in data encryption techniques.** Since so much data flows in through multiple channels, protecting sensitive information is key. A powerful CWM platform must be built from the ground up with strict data confidentiality requirements and capabilities. [Customer managed encryption keys \(CMEK\)](#) give administrators control of their data’s encryption.
-  **Know where your data is stored.** Enterprise-grade security as related to data governance means knowing where your data is at all times. Being able to track data movement, especially as it flows from trusted to untrusted systems is critical, as is the ability to prevent data loss.
-  **Easily applied data governance policies.** Providing an enterprise-grade cloud-based solution means that the technology provider has to empower and enable customers to implement data governance policies from within the service. That is, both the IT organization and the end user need the ability to manage the protection of data from within the service. Equally important, data governance needs to be a shared responsibility between the technology provider and customer and work with all operations. Software vendors have

Data governance needs to be a shared responsibility between the technology provider and customer and work with all operations.

to help their customers fulfill their responsibilities by building in features that enable and facilitate the management of data governance and data protection.



**Control over data relevancy.** Our society is drowning in data. It is simply too easy to spin off another data set instead of having to find the relevant information that might exist under separate silos in large enterprise organizations. Finding and reducing outdated information not only helps performance, but is critical for data governance and compliance purposes.

## 2 Transparent data privacy controls

Dependable data governance might be critical to enterprise-grade security, but it is not the only factor to keep an eye on. The free flow of information, especially consumer data, is driving greater demands for privacy regulations. Consumers are frequently wary about how their data is being shared between enterprise organizations, as not all use cases are readily apparent. Second, consumers might not even be aware of data flows in the first place.

Data geographies are also an important consideration when conforming to regional laws concerning data use and handling. Regulations such as the [General Data Protection Regulation \(GDPR\)](#), for example, require enterprises to factor in data governance depending on where and how data is processed.

GDPR and the [California Consumer Privacy Act \(CCPA\)](#) provide consumers certain rights with respect to how their personal information is processed. The commonly coined “right to be forgotten” means individuals have the right to request that their information be scrubbed from online searches and other directories.

Customers can choose what information is shared, and also have more visibility and rights around how such information is being used.

“ While data privacy laws might be empowering for customers, they are challenging for enterprises to execute. ”

While such laws might be empowering for customers, they are challenging for enterprises to execute. When data forms the basis for complex algorithms and then is used in a variety of ways, it becomes hard to separate specific datasets from the overall models. Equally challenging, it is sometimes difficult for enterprises to control how data is being used by other organizations downstream.

An especially complex wrinkle for enterprises: consumers can consent to data processing in the beginning and withdraw their consent at any time. This means companies in turn need to be ready to handle such requests at any time without risking collapse of associated data models.

Enterprise-grade data privacy controls allow companies to accurately identify all personal data fields of a specific individual — no matter where the digital data crumbs lead. These enable enterprises to classify personal information in the right way, at the very beginning, so they can respond to individual data protection or subject access requests accordingly.

### 3 Integration with the IT ecosystem

While sound practices in data governance and privacy are key factors for an enterprise-grade platform, the best ones recognize that in today's enterprises, data can flow across entire ecosystems of connected programs and platforms.

In the IDG 2021 Pandemic Business Impact Study, 49% of IT leaders said that digital transformation will continue to accelerate. Digital transformation allows data to move freely between relevant stakeholders, so informed decisions can be executed following automated—or at least, orchestrated—workflows.

In modern business, CIOs and CISOs are invested in digital transformation in order to stay competitive, as it can make organizations more efficient and innovative at scale. Organizations also need to ensure that their data is secure and private in the platforms they use to get work done.

In such instances, enterprise-grade means partnering with trusted vendors who also place a high priority on vendor-to-vendor integrations that facilitate work throughout the IT ecosystem and undergo the enterprise's security audits to meet the highest industry standards and regulatory requirements. In the era of digital transformation, stand-alone applications that don't simultaneously enable data flow and security are a risk to businesses.

In the era of digital transformation, stand-alone applications that don't simultaneously enable data flow and security are a risk to businesses.

### 4 Frictionless workflows

A service provider that effectively addresses data governance, privacy, and IT ecosystem challenges, truly becomes an enabler for IT and solution builds across the business. Going one step further, IDG found in their [2021 State of the CIO](#) report that IT leaders are being tasked to create and sustain initiatives that generate revenue.

How are CIOs and CISOs getting there? They've found value in automating business and IT processes, working directly with customers, and mapping everything to a customer journey. And on top of these initiatives, 57% of CIOs said that "cybersecurity protections increased as a priority," largely due to the socio-economic conditions created during 2020.

“ **57%** of CIOs said that cybersecurity protections increased as a priority. ”  
IDG, 2021 State of the CIO

Cybersecurity safeguards will continue to be a primary goal for enterprise organizations, no matter the industry. With that in mind, it's critical that organizations adopt a CWM platform that is secure while empowering IT and business professionals to build scalable, streamlined solutions and automated workflows that have a positive financial impact on the business.

Enterprise-grade security in complex data ecosystems means being able to effectively manage information flow across services and among users. And while controls are a necessary component of being enterprise-grade, the service also has to be flexible enough to give users the freedom to solve work challenges in a way that suits their needs. Security-first frictionless workflows are key to enterprise-grade platforms.

# How Smartsheet raises the bar for enterprise-grade security

Over the past 15 years, the Smartsheet platform has been built from the ground up with security requirements and protocols to secure your data and give you control of user access to safely share information inside and outside of your organization.

Our product team is continuing to make key investments in these areas to deliver richer tool sets and capabilities to ensure IT has “control” needed to meet evolving security, compliance and governance mandates. We focus on empowering business users to effectively collaborate and manage work while also enabling IT to execute data governance policies seamlessly.

The many specific customer-centric solutions that Smartsheet has announced include:

## Data retention controls that simplify data management

These controls allow administrators to set up a policy that automatically removes sheets after a certain amount of time or period of inactivity. Enterprises can fine-tune these controls to match their specific requirements: time periods, restricted user access, and more. They can also choose to notify relevant stakeholders before deleting data so relevant entities can act on data accordingly.

## Integration with other software products

In addition to best-in-class security and governance controls, you also need a platform with the right ecosystem of connectors and integrations. Smartsheet integrates with your critical data sources while enabling you to consolidate many point and capability solutions to a more secure platform. And we will continue to expand our ecosystem to provide more ways to connect Smartsheet across your entire technology stack.

Smartsheet seamlessly connects with the systems of record and productivity apps your teams use everyday, helping improve visibility, collaboration, and decision-making across teams. We have integrations today with industry-leading platforms including [Adobe](#), [Atlassian](#), [Salesforce](#), and [ServiceNow](#). As well as integrations with popular productivity tools like [Box](#), [Dropbox](#), [Google Workspace](#), [Microsoft 365](#), [Microsoft Teams](#), [Slack](#), and more.

## More control over where work data is stored

To help address compliance requirements, Smartsheet Regions will give customers more control over where their Smartsheet content is stored, providing flexibility to select a specific region where their Smartsheet content is hosted. They will be able to leverage the same Smartsheet offerings they know and love while securely storing their Smartsheet content in the region where they need it.

## Partnership with McAfee's MVISION Cloud security platform

Smartsheet has also integrated its processes with [McAfee's MVISION cloud security platform](#). Such an integration allows customers to add controls created by McAfee to secure data and identify and flag use of sensitive and critical datasets. The service also includes threat and anomaly detection combined with data loss prevention policies. The McAfee security addition is one more step Smartsheet is taking to ensure that user data is secure.

## Leadership in the information security community

Ecosystems are about more than just sharing data across SaaS vendors. Smartsheet also belongs to the [Messaging, Malware, and Mobile Anti-Abuse Working Group \(M3AAWG\)](#), which falls under the umbrella of the larger information security community. We work with security peers in the software industry to develop standards and stay on top of an evolving threat landscape so we are always proactive when preparing for whatever comes next.



# Enterprise-grade now — and for the future

Work today (and tomorrow) needs a CWM platform that is easy to use and secure.

Enterprise-grade security is table stakes in today's business environment, and we take it to heart. We know it is about protecting data through all stages of its journey, about instituting the necessary privacy controls, developing customer trust through transparency, and spearheading security initiatives with the peer-to-peer business community.

Equally important, the Smartsheet platform is the CWM platform that gives IT the security, governance, and management tools they require while giving business users the flexibility to quickly build solutions, continuously innovate, and achieve more. We are enterprise-grade taken to the next level.

Learn more about [what Smartsheet can do](#) for your enterprise and [how we work](#) to earn your trust.

## About Smartsheet

Smartsheet is the enterprise platform for dynamic work. A leading cloud-based platform for work execution, Smartsheet empowers organizations and teams to dynamically plan, execute, and report on work at scale, resulting in more efficient processes, innovative solutions, and better business outcomes. Today over 90% of Fortune 100 companies and over 80% of Fortune 500 companies rely on the secure, scalable Smartsheet platform to connect the entire enterprise. The single platform gives people a solution flexible enough to adapt to the changing needs of dynamic work across a broad array of departments and use cases. To learn more about Smartsheet, visit [www.smartsheet.com](http://www.smartsheet.com).

