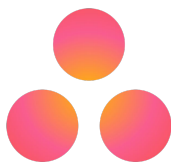




Security Features Comparison of 5 Top-Rated PM Software



Asana



Jira



Notion



Smartsheet

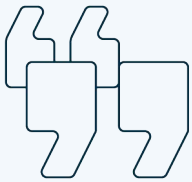


Trello

Security is the top reason businesses switch project management software

Tension between protection and productivity

Project management (PM) software is more than a workflow tool. It's a system of record that stores sensitive data, such as budgets, contracts, pricing sheets, and client deliverables. Businesses need encryption, access controls, and audit trails, with easy to use tools. Protecting sensitive data can slow teams down, and that tradeoff is why security is top of mind. That tension, between protection and productivity, is tough to resolve, and it's why security is a top concern.



Our latest study finds that **71%** of buyers rank security as their No. 1 concern, and it's also the leading source of **satisfaction and dissatisfaction**.

AI adoption raises the stakes

As more teams add generative AI and predictive analytics, new data flows and integration points emerge, creating fresh targets for attackers. That's why we've analyzed top-rated PM tools through a security-first lens, helping businesses find the right system to protect sensitive data without sacrificing usability.

What you'll learn from this guide

This guide helps you choose a project management tool that keeps your data secure without slowing your team down. You'll understand what PM security features to look for, what to ask vendors, and which products deliver the right balance of usability and protection.

Here's what you get:

- **Top rated PM software picks:** Compare top-rated PM tools (listed alphabetically) and see how they protect sensitive data with features, such as encryption and access controls.
- **Key PM security features explained:** Learn what eight essential safeguards mean for your business in simple, practical terms.
- **Tool-by-tool insights:** Discover how each platform handles compliance, integrations, and AI-driven risks.
- **Questions to ask vendors:** Get a ready-to-use checklist to assess whether a PM tool meets your security standards.

By the end, you'll know which PM software fits your team's needs and keeps your projects safe and efficient.

8 key security features in project management software

- **Context-aware access controls:** Let the system adjust who can see or edit information based on where they are, which device they use, the time, or how sensitive the project is.
- **Least-trust architecture:** Require users to prove who they are every time they access data and keep access limited only to what's needed.
- **Granular encryption controls:** Protect not just the whole database but also specific files or fields, like individual attachments or budgets.
- **Audit trails and activity logging:** Keep a clear record of every change or login, and spot unusual behavior that might signal a threat.
- **API governance and endpoint protection:** Control how other apps connect to your system and block unsafe or unknown connections.
- **Network-level protection:** Set firewall rules and other defenses to keep out unauthorized traffic before it reaches your tools.
- **Data loss prevention (DLP):** Automatically detect and block sensitive details (like passwords or personal info) from being shared where they shouldn't be.
- **Compliance support:** Help your business meet privacy and security rules such as GDPR, SOC 2, HIPAA, or ISO/IEC 27001.



Top project management tools and security features comparison

See which tools go beyond task tracking to keep your data safe.

Overview: Side-by-side view of key security capabilities in top-rated-project management tools

	Asana	Jira	Notion	Smartsheet	Trello
Context-aware access controls					
Least-trust architecture					
Granular encryption controls	Partial	Partial	Partial		
Audit trails and activity logging			Partial		Partial
API governance and endpoint protection					Partial
Network-level protections			Partial		
Data loss prevention		Partial		Partial	
Compliance support					

Key: Confirmed native capability. Non-native capability
Note: 'Partial' means feature is available in limited capacity.
All features and product capabilities were analyzed as of October 2025.



Asana helps teams plan, organize, and track their work in one place. It lets users create tasks, set deadlines, assign responsibilities, and monitor progress through lists, boards, or timelines. Teams can also automate routine actions, track company goals, and connect Asana with tools, such as Slack, Google Workspace, and Microsoft 365 to reduce manual coordination and keep work moving.

Asana Security

Asana includes many built-in protections to keep business data secure. You can control who accesses projects, approve logins only from trusted accounts, and set limits on session time or password strength. It supports two-step verification for safer sign-ins and uses encryption to protect data at rest and in transit. Admins can review activity logs, manage permissions, and restrict sharing outside the organization. Asana also meets compliance standards such as GDPR and HIPAA to protect sensitive data.

Who is this fit for? Mid-and-large teams managing cross-departmental projects, especially marketing, operations, and product teams that need visibility and secure collaboration.

Pricing:

Starts at \$10.99 per user, per month (billed annually)

Free plan available



What users say:

"There were tons of opportunities to integrate it with other third-party tools and I like the fact that it has enhanced security features." — Aaron E., Management Consulting

How Asana supports security

Security feature	Support type	How Asana supports it
Context-aware access controls	Non-native (via integrations)	Works with IAM tools to manage access by location or device. Supports SSO, MFA, and IP allowlisting.
Least-trust architecture	Non-native (via integrations)	Uses SSO, MFA, and IAM integrations to verify every login and restrict access.
Granular encryption controls	Partial native / via integrations	Encrypts data in transit and at rest. Adds CASB or DLP tools for file-level protection.
Audit trails and activity logging	Native + integrations	Logs user actions through the Audit Log API and connects with SIEM tools for monitoring.
API governance and endpoint protection	Native + integrations	Manages API tokens and permissions. Integrates with CASB tools for added endpoint control.
Network-level protections	Native + integrations	Uses IP allowlisting and domain control. Pairs with firewall or CASB tools for stronger defense.
Data loss prevention	Non-native (via integrations)	Integrates with tools like Nightfall to detect and block sensitive data sharing.
Compliance support	Native	Meets GDPR, SOC 2, HIPAA, and ISO 27001 standards for secure data handling.

Note: "Native" means built into Asana. "Non-native" means available through external security integrations.



Jira

[Visit Page](#)

Jira helps teams plan, track, and deliver work with clarity and flexibility. Whether you're managing software, marketing, or operations projects, Jira lets you break down large goals into tasks, assign work, track progress with Kanban or Scrum boards, and customize workflows to fit how your team works. It connects work to goals and gives visibility across teams so everyone stays aligned.

Jira Security

Jira builds security into its offering with strong access controls, logging, and cloud infrastructure protections. You can enforce multi-factor authentication, configure permissions per project or issue, and audit user actions through logs. Atlassian also uses encryption, secure development practices (like anonymization and tokenization), and regular security testing across their systems.

Who is this fit for? Software, IT, and product teams that manage complex projects using Agile methods and need detailed tracking, issue management, and strong security controls.

Pricing:

Starts at \$7.53 per user, per month for 300 users (billed monthly)
Free plan available



What users say:

"The cost and configuration efforts required can also be significant, but the integration capabilities and scalability often make it worth the investment."

— Ishvarya K., Cloud Security Analyst

How Jira supports security

Security feature	Support type	How Jira supports it
Context-aware access controls	Non-native (via integrations)	Works with Atlassian Access and IAM tools to manage access by user, device, or location. Supports SSO and MFA.
Least-trust architecture	Non-native (via integrations)	Uses IAM and Atlassian Guard integrations to verify every login and limit access.
Granular encryption controls	Partial native + integrations	Encrypts data in transit and at rest. Adds Guard or ACLI for field-level control.
Audit trails and activity logging	Native + integrations	Tracks user actions with logs and history. Connects with SIEM tools for monitoring.
API governance and endpoint protection	Native + integrations	Secures APIs with OAuth and scoped access. Uses Guard for advanced monitoring.
Network-level protections	Native + integrations	Offers IP allowlisting and firewall setup. Extends security through Guard.
Data loss prevention	Partial native + integrations	Provides basic data protection. Adds DLP with Access, Nightfall, or McAfee.
Compliance support	Native	Meets GDPR, SOC 2, HIPAA, and ISO 27001 standards for data security.

Note: "Native" means built into Jira. "Non-native" means available through external security integrations.



With Notion, you can plan projects, document processes, and manage tasks all in one place. Create pages for projects, assign tasks, set due dates, and link related information like meeting notes or design specs. Teams can customize views as lists, boards, or tables and connect Notion with tools like Slack, Google Workspace, and GitHub to keep work organized and communication clear.

Notion Security

Notion offers encryption, access controls, and role-based permissions. You can decide who can view or edit pages, approve trusted devices, and monitor activity through audit logs. Enterprise users get extra safeguards like single sign-on (SSO), advanced admin controls, and detailed usage reports. Notion also complies with global standards such as SOC 2 and ISO 27001, helping you store and share information securely.

Who is this fit for? Knowledge-driven teams, like product, design, and operations, who want a flexible, all-in-one workspace that keeps information secure and collaboration simple.

Pricing:

Starts at \$10 per user, per month (billed annually)

Free plan available



What users say:

"We have different pages for each department, and it's helpful that you can restrict permissions or share certain pages only with external providers who need to see information.

— Sophie S., Operations Manager

How Notion supports security

Security feature	Support type	How Notion supports it
Context-aware access controls	Non-native (via integrations)	Uses role-based access control (RBAC) for permissions. Full context-aware access requires IAM integration.
Least-trust architecture	Non-native (via integrations)	Supports SSO, MFA, and encryption. Full Zero Trust setup needs external IAM or ZTNA tools.
Granular encryption controls	Partial native	Encrypts data at rest and in transit. No field-level encryption or customer-managed keys.
Audit trails and activity logging	Partial native	Provides activity logs and limited anomaly detection. Lacks centralized enterprise-grade audit trails.
API governance and endpoint protection	Non-native (via integrations)	Offers limited API documentation and community tools. No dedicated endpoint protection features.
Network-level protections	Partial native	Includes admin controls and local security settings. Does not provide firewall or network-level policy controls.
Data loss prevention	Non-native (via integrations)	Integrates with tools like Nightfall for DLP scanning and redaction of sensitive data.
Compliance support	Native	Meets GDPR and SOC 2 standards. Does not currently support HIPAA or ISO 27001 certification.

Note: "Native" means built into Notion. "Non-native" means available through external security integrations.



Smartsheet lets you manage projects using familiar grid layouts that feel like spreadsheets, while still supporting automation, dependencies, calendars, and dashboards. You can assign tasks, set due dates, attach files, and coordinate with teams across functions. Smartsheet also integrates with tools like Microsoft 365, Google Workspace, and Slack to keep work synchronized across systems.

Smartsheet Security

Smartsheet builds in encryption for data in transit and at rest, firewalls, identity controls, and secure access via SSO and MFA. It gives administrators control over permissions, form access, and attachment restrictions. You also get audit logs and regular security testing. Smartsheet supports global compliance standards (like HIPAA, FedRAMP) and lets you choose where your data is stored in some regions.

Who is this fit for? Mid-and-large teams managing data-heavy or cross-functional projects, especially operations, PMO, and marketing teams that need structured workflows, automation, and strong security controls.

Pricing:

Starts at \$9 per user, per month (billed annually)
30 days free trial available



What users say:

"The software helps to keep the data at one stage and can be easily accessible on various devices by the users also helps to manage the record." — Sanjana C., HR recruiter

How Smartsheet supports security

Security feature	Support type	How Smartsheet supports it
Context-aware access controls	Non-native (via integrations)	Works with IdPs to control access by user, device, or location. Supports SSO and role-based permissions.
Least-trust architecture	Non-native (via integrations)	Applies least-privilege access and SSO; full Zero Trust via external ZTNA tools.
Granular encryption controls	Native	Encrypts data in transit and at rest. Supports CMEK for field-level protection using AWS KMS.
Audit trails and activity logging	Native + integrations	Tracks user activity and events; integrates with CASB or SIEM for deeper insights.
API governance and endpoint protection	Native + integrations	Controls API tokens and access; extends protection with CASB or SIEM tools.
Network-level protections	Native + integrations	Offers IP restrictions and domain sharing; works with CASB and Defender for added security.
Data loss prevention	Partial native + integrations	Limits sharing and access; full DLP through Nightfall or Microsoft Information Protection.
Compliance support	Native	Meets GDPR, SOC 2, HIPAA (Enterprise), and ISO 27001 standards.

Note: "Native" means built into Smartsheet. "Non-native" means available through external security integrations.



Trello helps teams organize tasks visually using boards, lists, and cards. You can create tasks, set deadlines, assign owners, and move work across stages to track progress. Its drag-and-drop design makes it easy to see what's being worked on, who's responsible, and what's coming next. Trello also integrates with tools, such as Slack, Google Workspace, and Microsoft Teams, helping teams collaborate and stay organized without extra effort.

Trello Security

Trello keeps your data safe with encryption, access controls, and permission settings. You can manage who can view or edit boards, enforce SSO and two-step verification, and control data sharing within or outside your organization. All data is encrypted in transit and at rest, and Atlassian (Trello's parent company) runs regular audits and vulnerability testing. Trello also meets major standards like ISO 27001, SOC 2, and FedRAMP, ensuring your information stays protected.

Who is this fit for? Small and midsize teams that need a simple, visual way to manage tasks and projects securely, especially marketing, design, and operations teams focused on collaboration and clarity.

Pricing:

Starts at \$5 per user, per month (billed annually)

Free plan available



What users say:

"The WYSWYG design function is beneficial to even novice users - you can move things how you see fit without major processes involved." — Jonathan G., Chief Button Pusher

How Trello supports security

Security feature	Support type	How Trello supports it
Context-aware access controls	Non-native (via integrations)	Uses basic permissions; full context-based access via Atlassian Access or IAM tools.
Least-trust architecture	Non-native (via integrations)	Supports SSO and MFA; full Zero Trust through third-party integrations.
Granular encryption controls	Non-native (via integrations)	Encrypts data in transit and at rest; deeper control through Atlassian Guard.
Audit trails and activity logging	Partial native + integrations	Offers activity logs; detailed audit trails via Atlassian integrations.
API governance and endpoint protection	Partial native + integrations	Uses API tokens and OAuth; expanded control with Atlassian Guard.
Network-level protections	Native + integrations	Enables domain-based access and firewall setup; works with Atlassian Guard.
Data loss prevention	Non-native (via integrations)	Adds DLP through tools like Nightfall or Netskope.
Compliance support	Native	Meets GDPR, SOC 2, and ISO 27001; HIPAA not supported.

Note: "Native" means built into Trello. "Non-native" means available through external security integrations.

Recap:

Asana vs. Jira vs. Notion vs. Smartsheet vs. Trello

	Overall rating	No. of reviews	Starting price	Native security support	Ease of use rating
 Asana	4.5/5	13,440	\$10.99 user/mo	Audit trails, API governance, Network-level protection, compliance support	4.4/5
 Jira	4.4/5	15,168	\$7.53 user/mo	Audit trails, API governance, Network-level protection, Compliance	4.1/5
 Notion	4.7/5	2,621	\$10 user/mo	Compliance	4.3/5
 Smartsheet	4.5/5	3,442	\$9 user/mo	Encryption, Audit trails, API governance, Network-level protection, Compliance	4.3/5
 Trello	4.5/5	23,388	\$5 user/mo	Network-level protection, Compliance	4.5/5

Note: Ratings, reviews, pricing, and features analyzed as of October 2025.



Our Findings

Discover how different project management solutions offer security.

Our findings

The analysis shows a clear shift in project management software towards stronger security. Every tool offers protection, but what matters is how each one applies it—not which one has “more security.”



Best for secure cross-team project management

Asana combines task organization, project tracking, and workflow management in one platform. It earned a **4.4/5 ease-of-use rating**, reflecting its accessible interface and structured layout. Security features include encryption, role-based permissions, and access limits, with integrations for zero-trust access, data loss prevention, and firewall control. Asana complies with GDPR, SOC 2, HIPAA, and ISO 27001 standards to help teams manage projects securely across departments.



Best for Agile and enterprise-grade project management

Jira supports Agile project tracking with configurable workflows and detailed reporting. It holds a **4.1/5 ease-of-use rating**, suitable for users managing complex projects. Data protection includes encryption, access permissions, and activity logs, while Atlassian Access and Guard provide options for zero-trust authentication, DLP, and API monitoring. Jira aligns with GDPR, SOC 2, HIPAA, and ISO 27001 requirements for data security and compliance.



Best for knowledge management and collaborative workspaces

Notion combines notes, databases, and project tracking in one workspace. It has a **4.3/5 ease-of-use rating**, reflecting its adaptable and user-friendly design. The platform uses encryption, access controls, and admin permissions to protect information. Integrations extend capabilities for context-aware access and DLP. Notion adheres to GDPR and SOC 2 standards, supporting secure information sharing and documentation.

Our findings

Smartsheet

Best for enterprise-scale, spreadsheet-style project management

Smartsheet applies a grid-based interface for project planning, automation, and reporting. It has a **4.3/5 ease-of-use rating**, indicating a familiar layout for spreadsheet users. Security includes encryption, IP restrictions, and role-based permissions, with integrations for endpoint protection, DLP, and zero-trust access. Smartsheet meets GDPR, SOC 2, HIPAA, and ISO 27001 standards for enterprise data management and compliance.

Trello

Best for visual and easy-to-use task management

Trello organizes work with boards, lists, and cards to help teams track progress visually. It has a **4.5/5 ease-of-use rating**, the highest among these tools. Security measures include encryption, permissions, and domain-based access control, with integrations for zero-trust and DLP via Atlassian Guard. Trello complies with GDPR, SOC 2, and ISO 27001 to support secure collaboration for smaller teams and departments.



Questions to ask vendors

Ask the right questions to find tools
that truly protect your data.

Questions to ask vendors

Before choosing a project management tool, ask how each vendor protects your data. Every solution claims to be secure, but what matters is how those protections work in practice and how consistently they are applied.



What compliance standards do you follow?

Compliance proves credibility. Standards like GDPR, SOC 2, HIPAA, and ISO 27001 show the vendor meets global data privacy and protection rules.



Do you offer protection against data leaks or file misuse?

Data loss prevention tools stop accidental or intentional sharing of confidential information, especially useful if your team handles client files.



What happens to our data if we cancel or switch tools?

This protects your ownership. Knowing how and when your data will be deleted or transferred ensures you stay in control after leaving the platform.



How often do you update your security protocols?

Frequent updates mean fewer vulnerabilities. Vendors who test and patch regularly protect you from emerging threats.



Are integrations with other apps secure?

Integrations expand capability but can open doors for attackers. Secure, verified connections ensure external apps don't compromise your data.



How do you manage data used in AI features?

AI tools may store or process sensitive information. Ask how your data is used, trained, and retained to avoid privacy risks.

Methodology

To be considered for this list, products had to:

- Earn top scores in a proprietary methodology combining user ratings with popularity.
- Have at least one of the key security features identified for PM software
- Have at least 20 unique product reviews published on Software Advice within the past two years, with an average rating of 4.0 or higher.
- Meet our market definition for project management software: "Project Management software automates task assignment, resource allocation, scheduling and milestone tracking for all phases of a project. Project Management tools and systems may take one of several approaches: collaborative, when multiple people work on a project; top-down, when one person works on a project at a time; or integrated, when multiple aspects of the organization are involved."

For details about each product's security features, we referenced to publicly available sources, primarily vendor websites, as of October 2025. In some cases, vendors supply us with information, which our research team then validates via public sources.

Product ratings are based on an analysis of our verified user reviews as of October 2025. Our independent and objective research is based on market demand signals along with analysis of our proprietary data, including product information.

Review excerpts are passages extracted from longer reviews written by verified reviewers. We obtain these excerpts by applying an algorithm that considers factors including, but not limited to, length, sentiment, topic coverage, and thematic relevance. Excerpts represent user opinions and do not represent the views of, nor constitute, an endorsement by Software Advice or its affiliates. Excerpts are trimmed for brevity.

*Project Management (PM) Software Trends Survey was conducted in July 2025 among 2,545 respondents in Australia (n=240), Brazil (n=227), Canada (n=227), France (n=241), Germany (n=224), India (n=216), Italy (n=227), Mexico (n=236), Spain (n=239), the U.K. (n=237), and the U.S. (n=231). The goal of the study was to understand the PM methodologies and software that companies are using, their benefits and challenges, and the impact of AI on project management. Respondents were screened for full-time employment at companies with more than one employee, working in management-level roles or above. Respondents were also confirmed to be at least partially responsible for PM software purchase decisions and operations within their organization.



**Get a personalized
software list
aligned to your
needs**



Free Consultation

Talk to a real-life advisor and get a personalized software list in less than 15 minutes.

888-257-7842



About Capterra

Looking for software? Capterra is the web's most comprehensive software resource and research tool. We connect you to data, helpful guides, comparison tools, and software reviews from real users to help you confidently find, buy, and get the most out of technology. Conduct research, filter software, compare choices, and save your favorites to your free personalized profile.

Join the millions of people who use Capterra monthly to find software for their business.

Get started now

