

Are You Using the Right Tool? Project Management Tool Security Review

BY: Charles DeBarber, Cybersecurity Advisor

EXECUTIVE SUMMARY

A Project Management Tool (PMT) is a suite of collaboration software, which incorporate these functions: communication, file sharing, task lists, reporting, and productivity evaluation. Most are commercial (e.g., Monday, Basecamp, Asana), but some are open-source, such as OpenProject, The Hive, ProjectLibre. Commercial PMTs are “off-the-shelf,” visual, and easy to use. Open-source PMTs have the advantage of predominantly operating internally to an organization. However, the collaborative open-source nature of these tools makes them vulnerable to exploitation by skilled adversaries.

This white paper will evaluate solutions objectively, without bias to functionality. Because online research data is limited, a couple of anonymous call inquiries were made to vendors regarding their product security.

Commercial PMT Assessments



Product Description: "Asana is a software-as-a-service designed to improve team collaboration and work management. It helps teams manage projects and tasks in one tool. Teams can create projects, assign work to teammates, specify deadlines, and communicate about tasks directly in Asana."

Network Control: Asana uses Amazon Web Services (RDS & S3) to manage user data. Data is stored in SSAE 16 audited facilities in the United States. [Source – Security Page](https://asana.com)

Encryption: TLS 1.1 and above. Prohibits all TLS 1.0 & below communications or RC4.

Multifactor Authentication: Authentication is through Google Accounts.

User Management: Administrations can audit logs, including user activity, user status, and what users can see from the administration interface.

PROJECT SPECTRUM

API Usage: Uses OAuth 2.0 for authentication. Personal Access Tokens (PATs) interface. Some legacy API Key functionality will be phased out at an undisclosed date.

Cybersecurity Certifications: SOC 2 (Type 1) & SOC (Type 2)

Internal OPSEC: Customers can set who may access different projects, teams, and tasks. Outsides (e.g., contractors) without an e-mail address on the organization's domain can have limited access as guests.

Known Incidents: None. Asana has a bounty program for exploits found.

Summary: Asana's greatest weakness is the lack of a stable multifactor authentication system outside of Google. Unless an organization uses a Google mail domain service, the option is unavailable.



Basecamp

<https://basecamp.com>

Basecamp

Product Description: "Basecamp is a real-time communication tool that helps teams stay on the same page; it's less for traditional project management tasks (e.g., resource planning and long-term scheduling). With to-do-lists, calendaring, due dates, and file-sharing, Basecamp provides a way for teams to keep track of priorities and actionable items."

Network Control: Basecamp utilizes its own data centers coupled with Amazon Web Services (AWS) in the United States.

Encryption: Uses SSL certificates. For data in transit, it uses AES-128-CBC with SHA2 for message authentication and ECDHE-RSA for key exchange. For data at rest, it uses AES-256/SHA-256 encryption. Backups encrypted with GPG. Passwords are hashed and salted using BCrypt. [Source – Whitepaper](#)

Multifactor Authentication: Basecamp used Google for 2FA until 2019. It now uses its 2FA solution.

API Usage: Uses OAuth 2.0 for authentication. [Source](#)

Cybersecurity Certifications: None. The company confirms it is not HIPAA compliant [via Twitter](#).

PROJECT SPECTRUM

Internal OPSEC: Customers can set who may access different projects, teams, and tasks. Outsiders (e.g., contractors) to an organization not on their e-mail domain can have limited guest access.

Known Incidents: Basecamp successfully endured a credential stuffing attack in 2019. One hundred twenty-four accounts were compromised, but the company reset all passwords as a preventive measure. [Source](#)

Summary: Basecamp is vague about its data centers. Much of their data is likely on AWS, but they carry no industrial certifications to validate the security of those data centers. Basecamp does not disclose if they are 3rd party services, or if they belong to Basecamp. The company offers a better 2FA solution.

Basecamp has a history of attacks via DDoS and credential stuffing, but they responded well. However, had they been using 2FA, it would have impeded credential stuffing attacks for any Basecamp users.



Product Description: "Celoxis is a popular project management app that is easy to use and affordable. It is an integrated solution you can use to manage your project portfolios, workflows, expenses, timesheets, and resources, and improve client and team collaboration."

Network Control: Fully Amazon Web Services (AWS)

Encryption: 2048-bit industrial-grade SSL certificates utilizes TLS 1.2 encryption. [Source](#)

Multifactor Authentication: Available via SAASPASS MFA, but not natively.

API Usage: Web-based using PATs.

Cybersecurity Certifications: It fully uses AWS letting it 'piggyback' off their certifications (HIPAA, FISMA Moderate, FEDRAMP, ISO 27001/27017, PCI DSS Level 1, FERPA) and the SOC 2 & SOC 3 compliance standards.

Internal OPSEC: Customers can set who may access different projects, teams, and tasks. Outsides (e.g., contractors) without an e-mail address on the organization's domain can have limited access as guests.

P R O J E C T S P E C T R U M

Known Incidents: there is a cross-site scripting (XSS) vulnerability out (CVE-2008-6094) that could affect legacy clients pre-2012.

Summary: Full reliance on AWS does allow them to claim several cybersecurity compliance requirements. No native 2FA.



FunctionFox

FunctionFox

<https://functionfox.com>

Product Description: "FunctionFox is an online project management software for creative experts, advertising agencies, and in-house teams. It is simple to use and decrease time, raise productivity and profits, and save money."

Network Control: FunctionFox does not disclose if they use a 3rd party for the enterprise's data or whether the enterprise's servers are under their control.

Encryption: Comodo SSL Certified. Their certification is vague, as Comodo certifies based on differing levels. [Source](#)

Multifactor Authentication: None.

API Usage: No API.

Cybersecurity Certifications: Comodo SSL Certified (Level Unknown)

Internal OPSEC: Customers can set who can access different projects, teams, and tasks. Accounts must be in the organization's domain.

Known Incidents: None.

Summary: No MFA. FunctionFox is vague on encryption and who stores their data.



Jira

Jira

<https://www.atlassian.com/software/jira>

Product Description: "JIRA is a tool developed by Australian Company Atlassian. It is used for bug tracking, issue tracking, and project management. The name 'JIRA' is inherited from the Japanese

PROJECT SPECTRUM

word 'Gojira' which means 'Godzilla.' The basic use of this tool is to track issues and bugs related to your software and Mobile apps."

Network Control: Jira uses Amazon Web Services (AWS). [Source](#)

Encryption: TLS 1.2+ with Perfect Forward Secrecy (PFS). AES-256 encryption at rest.

Multifactor Authentication: Enforced two-factor authentication (2FA)

API Usage: It has a restful API that uses OAuth 1.0a.

Cybersecurity Certifications: ISO 27001 and SOC 2 (Type 1)

Internal OPSEC: Customers can set who may access different projects, teams, and tasks. Outsides (e.g., contractors) without an e-mail address on the organization's domain can have limited access as guests.

Known Incidents: A zero-day exploit was found in 2019 in Jira's Server and Data Center that allowed attackers to execute code in version 4.4.0 remotely. (CVE-2019-11581). ([Source](#) & [Source](#)). Jira offers an exploit bounty program.

Summary: Jira's recent zero-day is disconcerting, but they executed a swift response and patching.



Monday.com

<https://monday.com>

Product Description: "Monday.com is a visual team management tool that enables them to quickly add members, assign tasks, customize workflow, and track the progress of their work to completion. It promotes transparency so that teams can stay on top of their work without the surprises."

Network Control: Utilizes Amazon Web Services (AWS) paired with Google Cloud Platform. ([Source](#))

Encryption: TLS v1.2 in transit and AES-256 at rest.

Multifactor Authentication: 2FA Natively

API Usage: GraphQL. It has a legacy restful API that is available.

Cybersecurity Certifications: SOC 2 (Type 2), ISO/IEC 27001, ISO/IEC 27018

P R O J E C T S P E C T R U M

Internal OPSEC: Customers can set who may access different projects, teams, and tasks. Outsides (e.g., contractors) without an e-mail address on the organization's domain can have limited access as guests.

Known Incidents: None.

Summary: Very transparent with the SOC 2 assessment information. A tertiary concern is partially foreign ownership of the company.



Scoro

<https://scoro.com>

Product Description: "Scoro is a comprehensive online business management software that combines project management, CRM, billing, and reporting into an all-in-one solution. It allows users to control their business processes and workflow from a single platform, so they do not have to use multiple apps and switch from one app to another."

Network Control: Linx Telecommunications BV and Amazon Web Services (AWS). However, Scoro is currently migrating its data exclusively to AWS. ([Source](#))

Encryption: Scoro uses HTTPS encryption protocol for every transaction. All passwords are encrypted with an aes-256-cbc cypher.

Multifactor Authentication: 2FA natively

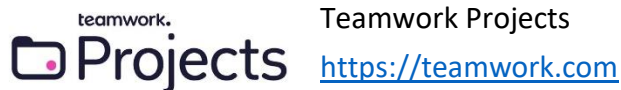
API Usage: Accessed by HTTP and JSON.

Cybersecurity Certifications: ISO 9001 and ISO 27001

Internal OPSEC: Internal OPSEC: Customers can set who may access different projects, teams, and tasks. Outsides (e.g., contractors) without an e-mail address on the organization's domain can have limited access as guests.

Known Incidents: Not known.

Summary: Meets many of the critical security needs but could use more security certifications to ensure its integrity.



Teamwork Projects

<https://teamwork.com>

Product Description: "Teamwork is a cloud-based project management solution that provides functionalities that enable businesses to manage project operations. Features include task lists, time tracking, file uploads, and messages. Teamwork helps teams manage group objectives, communicate, and establish business processes."

Network Control: Utilizes Amazon Web Services (AWS) in either the US or EU. ([Source](#))

Encryption: TLS 1.2 in transit, AES-256 at rest

Multifactor Authentication: 2FA natively

API Usage: Rest based. XML & JASON requests over HTTP.

Cybersecurity Certifications: SOC 2 (Type 1) certified.

Internal OPSEC: Customers can set who may access projects, teams, and tasks. Outsides (e.g., contractors) without an e-mail address on the organization's domain can have limited access as guests.

Known Incidents: None.

Summary: Strong transparency on their SOC 2 assessments.



Trello

<https://trello.com>

Product Description: Trello is a collaboration tool that organizes projects into boards. In one glance, Trello shows what is being worked on, who is working on what, and where something is in a process. Imagine a whiteboard, filled with lists of sticky notes, and each note represents a task for you and your team.

Network Control: Utilizes Amazon Web Services (AWS) and Google Cloud Storage (GCS)

Encryption: TLS 1.2 in transit, AES-256 at rest ([Source](#))

Multifactor Authentication: 2FA Natively or with Google OAuth.

API Usage: Restful API

Cybersecurity Certifications: SOC 2 (Type 2) certified. ISO/IEC 27001 certified. PCI-DSS certified.

Internal OPSEC: Customers can set who may access projects, teams, and tasks. Outsiders (e.g., contractors) without an e-mail address on the organization's domain can have limited access as guests.

Known Incidents: Trello has a history of insecure data. In late 2019, the Trello app had a critical vulnerability in its exposed internal boards that were unintentionally made public and aggregated into Google. Trello was reportedly first made aware of the issue in 2018.

Summary: The data leak did not involve a large amount of data, but it was careless and took nearly two years to patch.



Product Description: "Workfront is online project management software that allows you to manage your work in one place. It is the only comprehensive tool that eliminates extra work and simplifies everything from communication with real-time collaboration to project tracking and reporting. Workfront helps your organization improve the bottom-line by removing inefficiencies and clutter."

Network Control: Amazon Web Services (AWS)

Encryption: TLS 1.2 in transit, AES-256 at rest ([Source](#))

Multifactor Authentication: None.

API Usage: Restful over HTTP.

Cybersecurity Certifications: None.

Internal OPSEC: Customers can set access to different projects, teams, and tasks. Cannot invite outsiders with limited access.

Known Incidents: None.

Summary: No multifactor authentication. It pushes its single sign-on capability, but SSO is inferior to the benefits of MFA.

OPEN-SOURCE PMT SOLUTIONS



TheHive Project

<https://thehive-project.org/>

Product Description: "TheHive is a scalable 3-in-1 open source and free security incident response platform designed to make life easier for SOCs, CSIRTs, CERTs, and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly."

Network Control: Internally hosted.

Encryption: None.

Functionality: Task or subtask division, case management, state generation, observable data storage. TheHive is a Security Operations Center (SOC) IT-based PMT.

Multifactor Authentication: None natively.

API Usage: Restful through JSON over HTTP

Cybersecurity Certifications: None.

Internal OPSEC: Customers cannot set access to different projects, teams, and tasks. Cannot invite outsiders with limited access.

Known Incidents: None.

Summary: Good for an internal SOC/NOC, but it is only as strong as the network hosting it.



OpenProject

<https://www.openproject.org/>

Note: OpenProject has commercial cloud solutions, but this evaluation used the tool in its free, open-source form.

Product Description: "OpenProject is a web-based project management system for location-

independent team collaboration."

Network Control: Internally hosted.

Encryption: Passwords stored by OpenProject are securely stored using salted bcrypt. Alternatively, external authentication providers and protocols (such as LDAP, SAML) can be enforced to avoid using and exposing passwords within OpenProject.

Functionality: Task/subtask division, case management, states generation, messaging, file storage/transfer, time tracking, budgeting analysis, bug tracking

Multifactor Authentication: Not for free users.

API Usage: Restful API

Cybersecurity Certifications: None.

Internal OPSEC: Customers can set access to different projects, teams, and tasks.

Known Incidents: None.

Summary: OpenProject has a broader functionality, but the most secure functions are commercial offerings. Otherwise, it is only as secure as the network on which it is installed.

ProjectLibreTM ProjectLibre
<https://www.projectlibre.com>

Note: ProjectLibre has commercial cloud solutions, but this evaluation is using the tool in its free, open-source form.

Project Description: "ProjectLibre is an open-source project management software solution developed as an alternative to Microsoft Project. As with other project management tools, ProjectLibre maintains a list of tasks for users and automatically organizes and tracks tasks and projects as progress is made or they're completed."

Network Control: Internally hosted.

Encryption: None advertised.

Functionality: Task/subtask division, case management, state generation, messaging, file storage/transfer, time tracking, budgeting analysis, bug tracking. It is an open-source clone of Microsoft Projects.

Multifactor Authentication: Not for free users.

API Usage: Restful API

Cybersecurity Certifications: None.

Internal OPSEC: Customers can set access to different projects, teams, and tasks.

Known Incidents: None.

Summary: ProjectLibre is a good alternative internally for organizations familiar with Microsoft Projects.

FINAL ASSESSMENT

The most secure commercial products, from a cybersecurity perspective, are **Basecamp**, **Jira**, **Monday.com**, **Trello**, and **Teamwork Projects**. This review and compilation of research are based upon the criteria used to judge each.

Judging a "most secure" open-source solution is dubious if used internally to a network because its security is based on the network hosting it. Therefore, there are no cybersecurity conclusions for the open-source platforms.

Disclaimer: Project Spectrum is an impartial, trusted source whose sole purpose is to protect the Defense Industrial Base (DIB) and its supply chain. It is not influenced by any outside vendor or compensated for any information in this report.

ProjectSpectrum.io Continuously Monitoring & Securing Cyber