Vendor Report

Vendor Report for monday.com Ltd.

This report is based on publicly available information and does not consider artefacts such as external assurance reports or contract terms that may only be provided to clients. Refer to the References slide for a list of resources used to generate this report.

May 2024

Monday.com – Vendor Summary

Monday.com, founded in 2012, is a work operating system (Work OS) that helps organisations coordinate tasks, projects, resources, and team collaboration through a centralised platform. The system is equipped to facilitate communication among distributed teams with features like visual project tracking, customisable workflows, and automation capabilities. It integrates with various productivity tools and systems and is used across different business functions such as marketing, sales, IT, and operations. The platform also offers task management, milestone tracking, and real-time reporting, accommodating teams and enterprises of different sizes.

The pricing structure of monday.com features a free tier with essential functionalities and multiple paid subscription levels that offer additional features, enhanced security options, and premium customer support.

Monday.com provides Terms of Service for all users and requires Enterprise Plan subscribers to sign a Service Level Agreement (SLA) and the HIPAA Business Associate Agreement for Enterprise Plan subscribers with the HIPAA Compliance Feature enabled. Furthermore, when using specific services like WorkCanvas or monday AI Beta, users must adhere to the specific terms associated with these services.

The monday.com Trust Center provides information about:

- security measures & policies, data protection practices, and privacy compliance measures;
- compliance and certification with international standards and regulations; and
- how to report vulnerabilities.

There is also an option to download an assurance package (subject to agreeing with monday.com's Non-Disclosure Agreement) that includes external assurance reports such as SOC2 2 Type 2, ISO certificates, and security information and documentation such as network diagrams and certificate of insurance.

Monday.com – Key Risk Drivers

- Monday.com has many features, user types, and boards. Board types include Main Boards, Shareable Boards, and Private Boards; User types include Admins, Members, Viewers, and Guests. Functionalities differ at the different pricing tiers. The complexity of the platform may lead to:
    - users becoming overwhelmed as the many features of monday.com pose a steep learning curve. The required learning effort may cause user adoption to slow down, and insufficiently trained users may make mistakes that could compromise data security.
    - organisations choosing a pricing plan that does not meet their security and privacy requirements, such as activity log retention. If an organisation wants an extended log retention period, costs quickly increase.
    - challenges maintaining appropriate access control and oversight. This may lead to sensitive information being inadvertently shared with unauthorised personnel due to incorrect permission settings and user errors or lead to improper modification or deletion of data if privileged permissions of admins and members are not adequately monitored.
- Monday.com lets customers choose to opt in or out of using monday AI. While monday.com does not train AI models with user data, it allows AI to process user-submitted prompts, and data may be processed through third parties like Microsoft. This introduces concerns about third-party data security and the potential impact on user data safety. In addition, the monday AI is in beta status, with beta terms and conditions, which may frequently change and, if not adequately monitored, may introduce additional risks.

Monday.com – Key Risk Drivers

- Monday.com integrates with over 200 apps, such as Github, Slack, and Google Drive, which may enhance the user experience but introduces risks such as data security vulnerabilities, privacy concerns, compliance challenges, and potential loss of control over data flow if not adequately monitored. In addition, the platform may not be able to integrate with legacy systems or other tools an organisation may already use.
- Employees or team members may register for the Free Plan without organisational approval. If users use the free version without any oversight or training, improper usage could cause data breaches, loss of information, compliance risks, intellectual property risks, and accountability issues.
- The high level of functionality and the ability to deeply integrate monday.com within an organisation may result in vendor lock-in, making it difficult to change to a different tool in the future.
- As a cloud-based platform, monday.com stores user data on servers that may be located in different countries with varying levels of data protection regulations. Data breaches, unauthorised access, or data loss are risks, along with the dependence on internet connectivity. While users can see where their data is hosted within the admin section of their monday.com account, only Enterprise customers on the EU Data Region will have their Customer Data solely physically hosted within the EU Data Region. In addition, as monday.com headquarters are located in Israel, customer data will also be processed there.
- The global operations of monday.com require compliance with international data protection laws such as the EU's GDPR and California's CCPA, which may increase the challenges and risks faced by customers in terms of legal compliance, data security, and privacy protection, including complex regulations, potential legal penalties, and increased demands for data governance and security.

Monday.com – Vendor Due Diligence Review

Compliance and Information Security Policy & Organisation

- Monday.com has the following external assurance artefacts available: ISO 27001/ ISO 27017/ ISO 27018/ ISO 27032/ ISO 27701, HIPAA, CSA, and SOC1 Type II/SOC2 Type II/SOC3 (April 1, 2022 to March 31, 2023).
- Monday.com's Global Information Security Policy (GISP) covers human resources, asset management, access control, cryptography, physical security, operations, communications, supply chain, incident management, and product security.
- Monday.com's information security efforts are guided and monitored by the CISO, the Security Team and a Security Forum composed of representatives from the Infrastructure, R&D, Operations, and IT Teams.
- Monday.com's privacy efforts are guided and monitored by their Privacy Forum, which comprises representatives from the Legal, Privacy, and Security Teams and is led by the Data Protection Officer (DPO).
- Company policies are noted to be reviewed annually and updated as needed in response to significant changes affecting data confidentiality, integrity, or availability, with all updates requiring approval from senior managers.
- Monday.com has an internal security awareness program, which includes regular quizzes to measure effectiveness. Additionally, the R&D department undergoes security awareness training biannually.

Monday.com – Vendor Due Diligence Review

Infrastructure Security

- Monday.com hosts its system in multiple availability zones within Amazon Web Services (AWS), offers hosting in AWS data centres across the US, EU, and AU, and has established a disaster recovery site in another AWS region.
- Monday.com enhances network security by separating public and private subnets, placing load balancers in public areas and securing servers and databases in private subnets. It uses Web Application Firewalls (WAF), IP whitelisting, and port restrictions. Content Delivery Network (CDN) providers also help manage traffic and prevent DDoS attacks, supported by Network Intrusion Detection Systems (NIDS) and AWS security services for comprehensive monitoring.
- Infrastructure-as-Code tracks and audits configuration changes. The Infrastructure Team is reviewing and updating the perimeter network configuration quarterly.
- Monday.com are utilising NIDS to monitor network logs, SIEM systems for alarm review, and security tools to manage security groups and network access control lists (NACLs). The Infrastructure Team conducts quarterly reviews of the network configuration, while an independent auditor performs annual audits to review the network configuration.
- Servers are hardened according to Center for Internet Security (CIS) standards, and their EKS clusters employ AWS Bottlerocket AMIs, which are Linux-based operating systems optimised for running containers with only essential software included.

Monday.com – Vendor Due Diligence Review

Infrastructure Security

- AWS's Simple Storage Service (S3) is used for hosting file storage, including attachments and database backups, with automated malware detection for uploaded files and a blacklist of forbidden file extensions to prevent malware infection.

Access Controls

- Monday.com offer credentials authentication (usually username, user email address, and password), along with support for external identity providers such as Google SSO (available for Pro and Enterprise plans only), Okta, OneLogin, and custom SAML 2.0 (available for Enterprise plan only). Account administrators can optionally enable two-factor authentication (2FA) via text message or authenticator app to enhance security.
- SCIM (System for Cross-domain Identity Management) provisioning, IP address restrictions, tenant level restrictions, audit log, email domain blocking, panic mode, session management, and API token generation are only available for Enterprise plan customers.
- Monday.com uses role-based access control with need-to-know and least-privilege principles.
- Access to monday.com infrastructure servers is secured through a VPN that requires an Enterprise Identity Provider (IdP) for authentication, supports comprehensive auditing, and mandates strong password requirements and Multi-Factor Authentication (MFA).

Monday.com – Vendor Due Diligence Review

Data Encryption

- Encryption in transit uses TLS 1.3, and encryption at rest uses AES-256.
- Encryption keys are managed through AWS KMS (Key Management Service).
- A multi-round Bcrypt function is used to hash passwords, and passwords are also salted.
- Customer data is backed up and encrypted. Backups are distributed across multiple AWS Availability Zones and retained for 25 days. Activity log data is backed up to Google Cloud Platform (US, multi-region) and stored for seven days.

Application and IT Security

- Monday.com notes that it has security measures in its software development lifecycle, including static and dynamic application security testing, continuous vulnerability monitoring, and rigorous testing of new and existing features, all guided by OWASP Top 10 principles. Refer to the Security & Privacy white paper for more details.
- A Web Application Firewall (WAF) filters, monitors, and blocks application-level traffic.

Monday.com – Vendor Due Diligence Review

Application and IT Security

- Monday.com conducts annual application penetration testing through an independent third party using manual and automatic methods, complemented by regular security audits and penetration tests performed internally on various features. Testing results and assurance reports are available for download.
- A Dev Platform is available, with key components including sprint management, bug tracking, release planning, roadmap planning, feature requests, and agile project management.
- Monday.com has a public bug bounty program on HackerOne.
- Monday.com states that security measures such as endpoint protection, strong password policies, identity and access management, and secure communications are implemented to safeguard customer data against unauthorised access and cyber threats.

Operational Security

- Red team assessments, including penetration testing and breach simulations, are conducted twice a year, along with annual audits for ISO 27001, 27017, 27018, 27032, 27701, and SOC 1 Type II, SOC 2 Type II, and SOC 3.
- Monday.com states that incident response plans and data retention and disposal policies are defined.

Monday.com – Vendor Due Diligence Review

Operational Security

- A business continuity plan (BCP) and a Disaster Recovery Plan (DRP) exist and are noted to be tested twice a year.
- The service's availability can be monitored through the monday.com Status Page. Enterprise Plan customers receive a 99.9% uptime commitment.
- Sub-processors are listed on the monday.com website. They must adhere to data protection obligations like those specified in the Data Processing Addendum (DPA). The DPA also lists that sub-processor audits and inspections may be carried out at mutually agreed intervals. Monday.com remains liable for ensuring that sub-processors fulfil their data protection obligations.
- Monday.com notes that it has a vendor management process and maintains a central repository for services and software. It is overseen by specialised teams to categorise vendors based on data sensitivity and assess their risk levels for compliance with industry standards during initial usage and renewals.
- Physical IT assets, consisting of laptops and office network devices, are stated to be securely managed in a password-protected, environmentally-controlled server room with 24/7 CCTV monitoring. Office access is controlled through biometric identification, and company employees strictly regulate and monitor visitor movements.

.

Monday.com – Vendor Due Diligence Review

Privacy and Data Governance

- Monday.com notes to adhere to GDPR, CCPA, and other privacy regulations.
- Monday.com has established a Vendor Code of Conduct, requiring all suppliers, partners, and third-party representatives to adhere to the highest ethical and legal standards.
- The Privacy Policy outlines privacy and data processing practices for handling personal data for monday.com's purposes as a data controller.
- The Data Processing Addendum (DPA) ensures the protection and proper processing of personal data on behalf of customers when monday.com acts as a data processor.

AI

- Monday.com allows customers to opt in or out of using monday AI. Users are solely responsible for using Monday AI and content generated through Monday AI.
- Monday.com may use data from user interactions with monday AI, including inputs and outputs, to enhance and provide functionalities of the AI. They claim to not use this data for training machine learning models, nor do they allow others to use it.

Monday.com – Vendor Due Diligence Review

AI

- Monday.com and its associated sub-processors involved with generative AI may oversee your inputs and outputs to ensure they monitor, prevent, and troubleshoot any misuse, illegal, damaging, or unauthorised activities.
- Monday.com allows users to integrate and utilise third-party services with AI capabilities via the Monday AI Assistant. The use of these services is governed by the respective third-party terms outlined in the Terms of Service.
- Data used in monday AI might be processed by additional sub-processors beyond those listed on monday.com's designated page, including entities like Microsoft Azure.

References

https://monday.com/trustcenter

https://monday.com/l/privacy/privacy-policy/

https://monday.com/pricing

https://monday.com/dev

https://monday.com/l/privacy/dpa/

https://monday.com/l/legal/tos/

https://monday.com/l/legal/monday-com-additional-services-terms/

https://monday.com/l/privacy/https-monday-com-l-scc-controller-to-processor/

https://monday.com/l/privacy/https-monday-com-l-scc-processor-to-processor/

https://monday.com/trustcenter/faqs/

https://dapulse-res.cloudinary.com/image/upload/v1705583308/security/Security_and_Privacy_white_paper_V1.8.pdf

https://monday-soc-reports.s3.amazonaws.com/monday.com+Ltd._SOC3_Report_FY2023.pdf

NEED A DETAILED RISK ASSESSMENT OR VENDOR REVIEW?

GET IN TOUCH

Katja Feldtmann

0800 029 237

katja@cybershore.co.nz

www.cybershore.co.nz

Cybershore provides information for general purposes only. We are not liable for any potential risks associated with the use of this information, as the risks mentioned are presented as examples out of context.