Cybershore

Vendor Report

Vendor Report for RealtimeBoard, Inc. dba Miro

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.

March 2024

Miro – Vendor Summary

Launched in 2011, Miro (RealtimeBoard, Inc. dba Miro) is a leading online collaborative whiteboarding platform enabling distributed teams to collaborate effectively, from brainstorming with digital sticky notes to planning and managing agile workflows. It features tools for real-time collaboration, project management, and interactive workshops, offering integrations with various productivity apps and services. Miro's platform supports creating diagrams, mapping user stories, and facilitating remote meetings, making it a versatile tool for teams of all sizes.

Pricing for Miro includes a free tier with basic features, with premium subscriptions available for additional functionality, security, and support. Two different Terms of Service apply: Standard Terms of Service and Master Cloud Agreement (MCA). This report mainly focuses on the Enterprise Plan which falls under the MCA.

Miro's Trust webpage provides information about:

- Security measures and data protection practices, including Miro's Artificial Intelligence (AI) Principles.
- Compliance with global privacy laws and regulations.
- Legal terms, policies, and information on how Miro supports secure and compliant use of its services.

Miro – Key Risk Drivers

- Users can create and share their boards and submit support tickets to the customer support team, including personal or classified information, posing potential data privacy risks. While boards by default are private, if published publicly, they are accessible by anyone with the link to the board and can be on-forwarded or distributed online. The public sharing functionality can be turned off if a customer uses the Enterprise Plan.
- Users can invite others, embed, or publish their private boards. If they improperly set sharing permissions or the Administrator inadequately configured Miro's access permission, it can lead to data leaks or unauthorised access.
- Miro connects with over 130+ apps. Integrating Miro with other apps, such as Atlassian Jira and Confluence, Slack, and Google Drive, introduces risks such as data security vulnerabilities, privacy concerns, compliance challenges, and potential loss of control over data flow if not adequately monitored.
- Miro offers customers the option to opt in or out of using Miro Assist, Miro's AI service. While Miro does not train AI models with user data, it allows AI to process user-submitted prompts, sharing limited data with third parties like Microsoft. This introduces concerns about third-party data security and the potential impact on user data safety.
- There are discrepancies between what is stated on the Miro website and the SOC3 report published online. For example, the SOC3 report and various web pages state that TLS1.2 is used for in-transit encryption, whereas other web pages refer to TLS1.3. Potential clients should read the latest SOC3 report once available and thoroughly review that and any other external assurance reports.

Miro – Vendor Due Diligence Review

Security, Privacy & Compliance

- Certifications, among others: ISO/IEC 27001, NIST, CSA and SOC2 Type II/SOC3 (December 1, 2021 to November 30, 2022). Sub-processors are published on the Miro website.
- Miro's Customer Support is provided by sub-processors (PartnerHero, Inc., Gainsight, Inc., InSided, Inc.) based in the United States, Philippines, and the Netherlands. It cannot access customer data unless chosen to be included in a support ticket. Miro relies on the protections afforded by the new EU Standard Contractual Clauses (as amended by the UK International Data Transfer Addendum where applicable) and relevant supplementary measures to legitimise any transfers to the vendor
- Miro restricts access to the production environment to a limited number of IP addresses and employees.
- Miro's Privacy Policy highlights data handling practices and user rights and states that Miro does not sell user data to third parties.
- Customer content, compute infrastructure, production data, and backup data are stored within the EU by default, using Amazon Web Services (AWS). Miro asserts compliance with GDPR and CCPA standards.
- Security information and event management (SIEM) integrations are available for IBM QRadar and Splunk. AzureDevops, Splunk, and ServiceNow are only available on the Enterprise Plan.
- A Dev Platform is available, with key components being REST API, Web SDK and Live Embed. Miro also has a public bug bounty program on HackerOne.

Miro – Vendor Due Diligence Review

Data Management & Backup

- Regular data backups ups are performed. Miro's Data Protection Policy specifies data retention policies, classifications, and protection levels (for example, Sensitive Personally Identifiable Information (SPII)).
- Data retention is set to the service termination day plus 180 days. Customer data can be exported, and Miro removes customer-created content from backup systems after 180 days or upon request.
- A Transparency Report detailing government requests for user data and account actions is published annually. The report for January 1 2022, up to and including December 31 2022, noted that no government requests were made.

Access Control & Encryption

- The Enterprise Plan includes several access control features, i.e., Sharing policy, Link access, and Domain controls. Advanced user management and permission, plugin management, data classification for boards, advanced search and content admin permissions, audit logs, and idle session timeout are additional controls that can be enabled.
- Single Sign-On (SSO), SCIM (System for Cross-domain Identity Management), and two-factor Authentication (2FA) are available for integration.

Miro – Vendor Due Diligence Review

Access Control & Encryption

- Data at rest is encrypted using AES 256-bit encryption, and data in transit is encrypted using Transport Layer Security (TLS) 1.2 (HTTPS connections through IPsec Prisma Access VPN tunnels; VPN required for remote access).
- AWS Key Management Service (KMS) is used to manage encryption keys for AWS tools. Encryption keys for the VPN, EC2 instances with Elastic Block Store (EBS), backup encryption, BitLocker, FileVault, and HTTPS/TLS systems through the native key management systems for each of those tools and systems. The Director of Trust and Reputation and the Infrastructure Team Lean jointly manage encryption keys.
- Miro offers customers the option to “bring your own key” (BYOK) through the cloud-based AWS EKM (Enterprise Key Management).

Artificial Intelligence (AI)

- Miro has defined AI principles (Transparency, Trust, Human Control, Fairness & Equity) that guide the use and development of AI. Customers can opt in or out of AI services.
- User data is not used for AI model training.
- Users retain intellectual property rights to their AI-generated content.

References

- Miro Trust Center: https://miro.com/trust/ and Miro security and compliance: https://help.miro.com/hc/en-us/articles/360012346599-Miro-security-and-compliance
- Security & Compliance One Pager: https://drive.google.com/file/d/1-SlQN-EAjvVqi6mwM_1Oy83gYfh2wUui/view
- SOC3 Report (December 1, 2021 through November 30, 2022): https://assets.ctfassets.net/w6r2i5d8q73s/1h3NDkPtNJcu5ZfzapyCv0/aafafcff781d99b2f34f1746cf1f1ed4/2022_Miro_SOC3_TypeII_FInal.pdf
- Privacy & governance at Miro: https://miro.com/trust/privacy-and-governance/
- Privacy Policy: https://miro.com/legal/privacy-policy/
- Miro's Annual Transparency Report 2022: https://assets.ctfassets.net/w6r2i5d8q73s/3Yg6sPgMD4X2DYPmJ84ZLz/7f0ef61ceee8587993609fe28073c87b/Miro_Annual_Transparency_Report_2022.pdf
- Data Encryption Whitepaper (required download through a form): https://miro.com/trust/data-encryption-whitepaper/ and Miro Enterprise Key Management: https://drive.google.com/file/d/1B04scZ5f7YGuCHk9HMnzkkqjDVp1geTS/view
- AI principles: https://miro.com/trust/ai-principles/

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.