miro



Security and Compliance at Miro

Enterprise-grade collaboration you can trust

miro

Table of contents

Overview 2
Our shared responsibility 3
Infrastructure security 3
Data centers 4
Data encryption 6
Encryption key management 6
Secrets management 7
Access control and authentication 7
Network security 7
Vulnerability management 7
Change management 8
Security policies 8
Employee policy and access 8
Physical security 9
Reliability 9
Incident response 9
Disaster recovery 9
Compliance, auditing, and certifications 10
How Miro is compliant 10
How Miro protects personal customer data 11
Third-party data processing 12
Product security 12
Zero Trust Architecture 13
Artificial intelligence 15
Enterprise ecosystem integrations 15
Miro Enterprise Guard: Advanced data security and governance add-on 16
Find, classify, and secure sensitive content 17
Manage the lifecycle of content at scale 18
Key management 18
Conclusion 19
Resources 19

Overview

Enterprise organizations must innovate to survive. As the leading visual workspace for innovation, Miro helps organizations do just that. Miro is trusted by more than 180,000 successful and innovative organizations, including 99% of the Fortune 100, such as Google, Cigna, Nike, Ikea, Deloitte, and Cisco.

They use Miro to strategize and plan, design customer-centric products and services, and so much more. However, connecting global teams and employees requires a secure and reliable platform to collaborate over confidential information. In addition, everyone in the organization needs the right access when they need it.

In this whitepaper, we'll summarize how Miro helps organizations innovate with **enterprise-grade infrastructure security, compliance, product security controls,** and **privacy** top of mind.



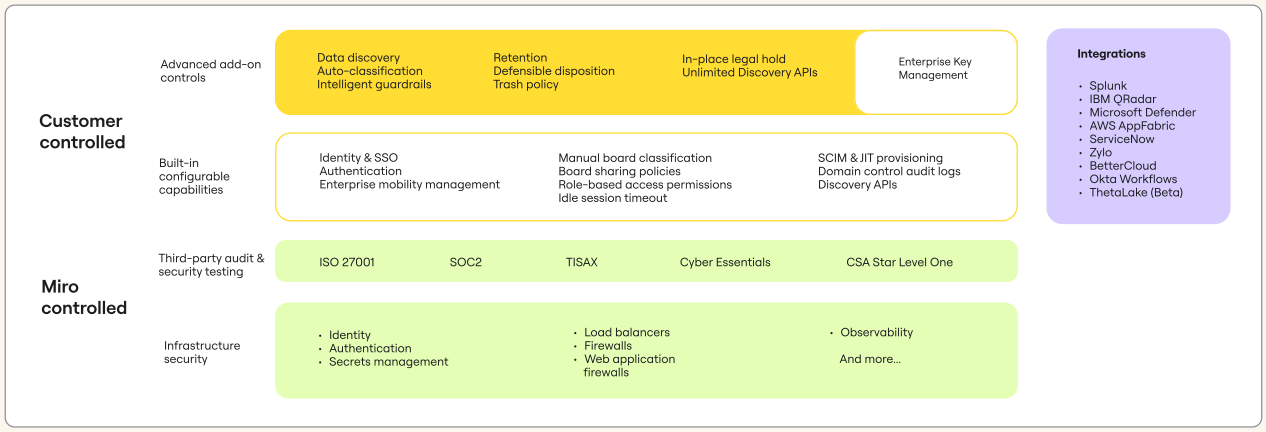
Our shared responsibility

This paper aims to explain our areas of responsibility and to educate on all the options available to bolster your organization's security posture further when using Miro.

This diagram outlines our approach to security. The bottom two layers are what Miro controls to ensure information security and support our compliance obligations. The top two layers represent the features we have built that you can configure based on your security and compliance needs.

We'll go through these features in detail throughout this paper.

Miro security & compliance architecture



Infrastructure security

As an enterprise-grade software-as-a-service (SaaS) platform, securing information is a big part of our overall security posture. This includes physical technology assets such as computers and networking systems, as well as cloud resources. Keeping these assets safe not only helps protect against traditional cybersecurity attacks, but also physical threats such as in-person theft and natural disasters. In turn, this secures our customers' information.

Data centers

Miro primarily uses Amazon Web Services (AWS) for its cloud computing infrastructure and leverages AWS security capabilities to secure the hosted data and workloads. Cloud computing builds on a shared accountability model.

AWS implements stringent security measures that include a variety of physical controls to the data centers, data privacy guarantees, and robust controls to its services. AWS computing environments are continuously audited, with certifications from accreditation bodies across geographies and verticals, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, ISO 9001 / ISO 27001, FedRAMP, DoD SRG, and PCI DSS Level 1.

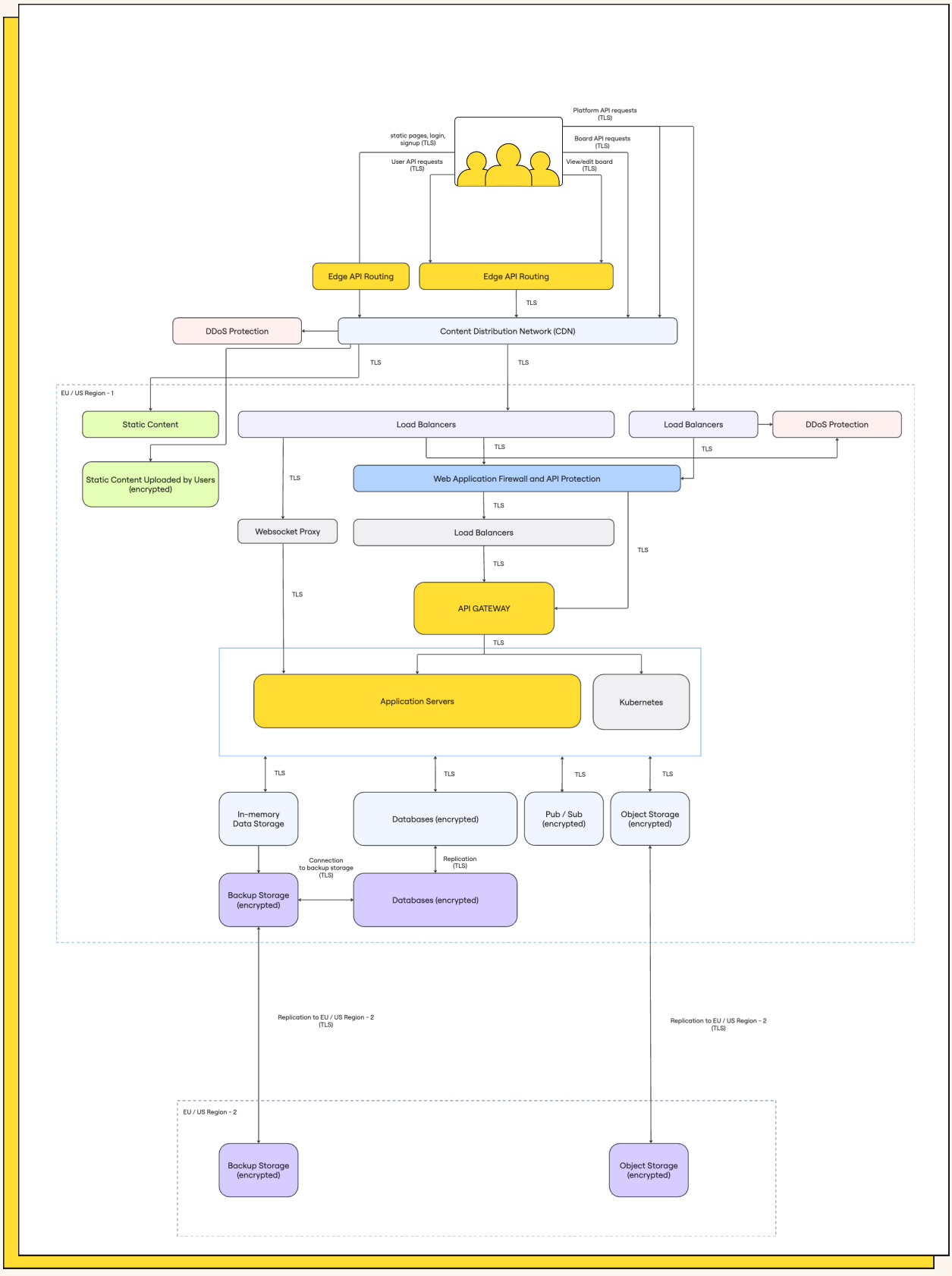
Miro primary production systems are housed at AWS data centers located in the EU (Ireland) and the US (Ohio). Additionally, AWS data centers located in EU (Frankfurt) and US (Virginia) are used to store backups and can be made operational according to the Disaster Recovery plan.

Within AWS cloud infrastructure, Miro is responsible for configuring the logical, network, and application security of the cloud infrastructure according to best industry practices and the AWS Well-Architected framework. Protective measures are implemented in a layered approach with the principle of least privilege and deny by default unless explicitly permitted. Management and access is strictly limited to specific employees and requires multi-factor authentication (MFA) and access from managed devices through virtual private network (VPN).

For more information, see AWS Shared Responsibility.



Data flow in the EU and US

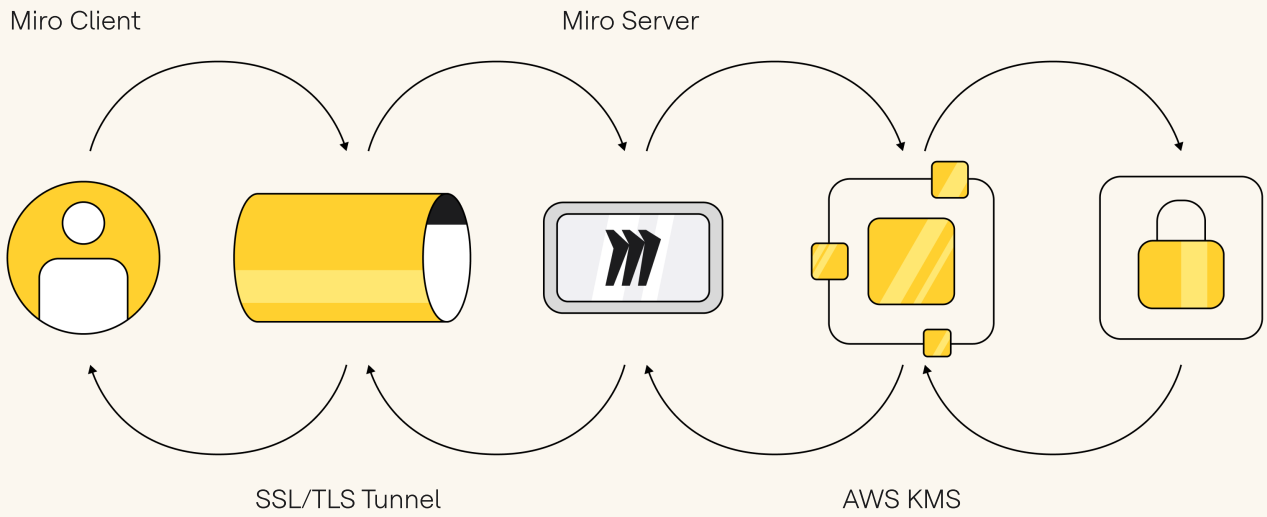


Data encryption

To protect user data, Miro balances data security with the technical requirements of our enterprise customers by employing a variety of encryption methods.

Miro adheres to the latest encryption standards for both at-rest and in-transit data protection. That means Miro supports **256-bit Advanced Encryption Standard (AES)** encryption at rest and **Transport Layer Security (TLS) 1.3**, besides 1.2, for data in transit. Together, this helps ensure end-to-end encryption throughout the data lifecycle.

Encryption at Miro



For more information, download our encryption whitepaper.

Encryption key management

Miro's key management infrastructure is designed with operational, technical, and procedural security controls in mind — with very limited direct access to keys. Encryption key generation, exchange, and storage are distributed for decentralized processing. Miro supports key management with a key hosted in your own AWS account via AWS Key Management System (KMS).

- **File encryption keys.** File encryption keys are created, stored, and protected by production system infrastructure security controls and security policies.
- **Internal SSH keys.** Access to production systems is restricted with unique SSH key pairs. An internal system manages the secure public key exchange process, and private keys are stored securely.
- **Key distribution**. Miro automates the management and distribution of sensitive keys to only the systems required for operations. The key distribution system is based on AWS KMS.

Secrets management

Sensitive data like passwords, API keys, database credentials, and certificates are stored securely in our secret management systems. Access to our secret management systems is authorized only for the services that require those secrets, and is limited to a small number of our operations engineers.

Access control and authentication



Miro's technical access controls and internal policies prohibit employees from arbitrarily accessing user boards and other information about users' accounts. Only a small number of engineers responsible for developing core Miro services have access limited to troubleshooting tasks and only with users' explicit consent. Miro support personnel do not have access to board content unless explicitly invited by the customer. All employee access is promptly removed when an employee leaves the company.

Network security

Miro maintains the security of the backend network with multiple layers of protection and defense, including security groups, proxies, network security monitoring and testing, intrusion detection systems, and auditing.

Access to the production environment internal network is restricted to only authorized user groups via VPN using single sign-on (SSO) and MFA, plus key authentication is required on all systems.

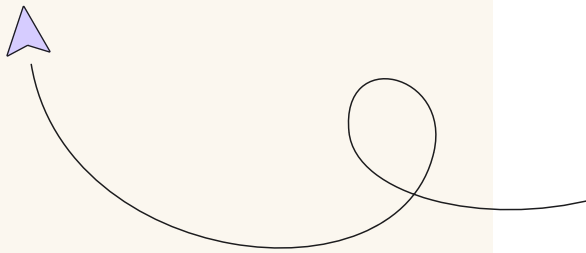
Vulnerability management

Miro's security team regularly performs automated and manual application and infrastructure security testing to identify and patch potential security vulnerabilities. Independent service providers are also used to perform annual external penetration tests, and issues identified are promptly fixed. Our public bug bounty program also incentivizes security researchers to submit any vulnerabilities that have been discovered in our products and services.

Change management

Miro has a formal change management policy that ensures all application changes are authorized prior to implementation into the production environment and that all security requirements are met. Changes to the Miro production environment are restricted to authorized personnel, while the security team ensures that server, firewall, and other security-related configurations are kept up-to-date with industry standards.

Through utilizing cloud security posture management, we can stay on top of most relevant threats in our cloud environment and be alerted to vulnerabilities or updates that are required in our cloud infrastructure.



Security policies

> At Miro, we assess risk and continually improve the security, confidentiality, integrity, and availability of the service. We review and approve our security policies (information security, Secure Software Development Lifecycle, incident response, logical access, and change management) at least annually. Additionally we monitor compliance with said policies, perform application and network security testing, and conduct internal and external risk assessments.

Employee policy and access

Where local laws permit, Miro employees undergo criminal background checks, sign a security policy acknowledgment, commit themselves to confidentiality, and complete mandatory security trainings to help ensure best practices are followed so that customer data is safeguarded.

Access between networks is strictly limited to the minimum number of employees and services, and firewall configuration is tightly controlled and limited to a small number of administrators. Access to other resources is granted through explicit approval by appropriate individuals, and a record of the access request and justification are recorded by management.

Physical security

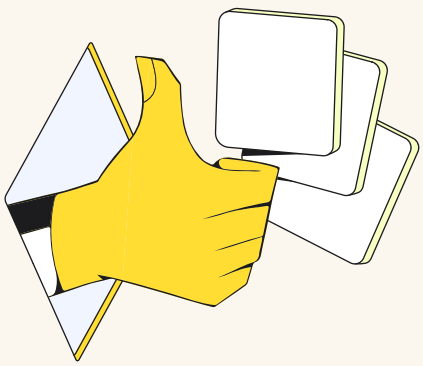
Miro uses a professional third-party provider to enforce its physical security policy and oversee the security of corporate offices. Physical access to corporate facilities is restricted to authorized Miro personnel via a badge access system, and a visitor badge system helps ensure only authorized individuals can access corporate facilities. Access to areas containing corporate servers is restricted to authorized personnel via elevated roles granted through the badge access system. The lists of authorized individuals approved for physical access to corporate and production environments are reviewed at least quarterly.

Reliability

Miro's server infrastructure provides secure data storage and high availability. All application services are running on multiple servers with a load-balancing/fault-tolerance system to increase redundancy. Cluster topologies are classified by the N+1 level of high availability. User data is replicated to multiple availability regions for protection and is encrypted and backed up regularly. In addition, daily database backups are stored separately from the main data center.

Incident response

Miro's incident response team is prepared to respond to any incident 24 hours a day, seven days a week. Incident handling policies address service availability, integrity, security, privacy, and confidentiality issues. Procedures include prompt response to incidents, severity evaluation, containment measures, communication with stakeholders, and status updates at status.miro.com.



Disaster recovery

In the event of a crisis or disaster impacting Miro business operations, our infrastructure team follows a disaster recovery plan (DRP) to address information security requirements. Findings are documented and tracked until resolution. The team reviews and tests this plan, including measurement of the recovery time actual (RTA), at least annually.

The DRP addresses both durability and availability disasters. A durability disaster is defined as a complete or permanent loss of primary data centers, or a lost ability to communicate or serve data from data centers.

The recovery time objective (RTO) is the duration of time and a service level in which a business process or service must be restored after a disaster. A recovery point objective (RPO) is the maximum tolerable period in which data might be lost from a service disruption.

Miro incident response and disaster recovery plans are subject to testing at planned intervals and upon significant organizational or environmental changes.

Compliance, auditing, and certifications

According to the Cost of a Data Breach Report 2023 from the Ponemon Institute, noncompliance with security regulations is one of the biggest factors contributing to data breaches. That's why at Miro, we take compliance seriously. Miro has a dedicated security department led by a chief information security officer, which includes several security teams dedicated to compliance and governance. Miro's data privacy officer manages and oversees data privacy to help ensure compliance with privacy regulations. An independent internal audit function is in place to ensure objective assurance and review of the governance.

How Miro is compliant

Miro is compliant with legal requirements according to the specific regions our business operates in. We are also transparent about the data security and privacy standards we follow that protect customer data from unauthorized access, breaches, and threats.



The auditing and attestation of these certifications and established standards allow us to assess our compliance and operational effectiveness of controls over the audit period, such as in SOC 2 Type II independent assurance reporting.

This includes:

- **Information security standards** such as SOC 2 Type II and ISO/IEC 27001
- **Data transfer standards** powered by a category-leading EU data residency solution and the use of Standard Contractual Clauses to provide an adequate level of data protection outside the EU and the UK that supports adherence to General Data Protection Regulation (GDPR)
- **Regional and sector-specific certifications** such as Cloud Security Alliance, Cyber Essentials, and TISAX
- **Recurrent third-party audits** driven by best-of-breed firms like the British Standards Institution (BSI)
- **Accessibility guidelines** and an Accessibility Conformance Report (ACR) based on VPAT

How Miro protects personal customer data



Privacy and data protection laws and regulations, such as GDPR in Europe, have become increasingly stringent, imposing strict obligations on how organizations collect, process, transfer, and store user data. Failure to comply with these regulations can result in hefty fines, regulatory scrutiny, and the loss of customer trust, potentially crippling a SaaS business.

Miro centers its privacy and data protection program around established industry practices with a large focus on protecting personal customer data through employee conduct and product design. Employees are required to adhere to data protection standards, commit to confidentiality, and are subject to technical limitations (see Employee policy and access). Miro's product design processes include regulatory checkpoints and legal reviews, and product and engineering teams are provided periodic training on design standards.

Miro's Privacy Policy lays out explicitly and transparently the categories of personal data that Miro processes as data controller along with the established business purpose. It also outlines the categories of third parties that Miro engages to process personal data, references how individuals can exercise their rights under data protection law, and the data transfer mechanism that Miro relies on to transfer personal data outside of the EU.

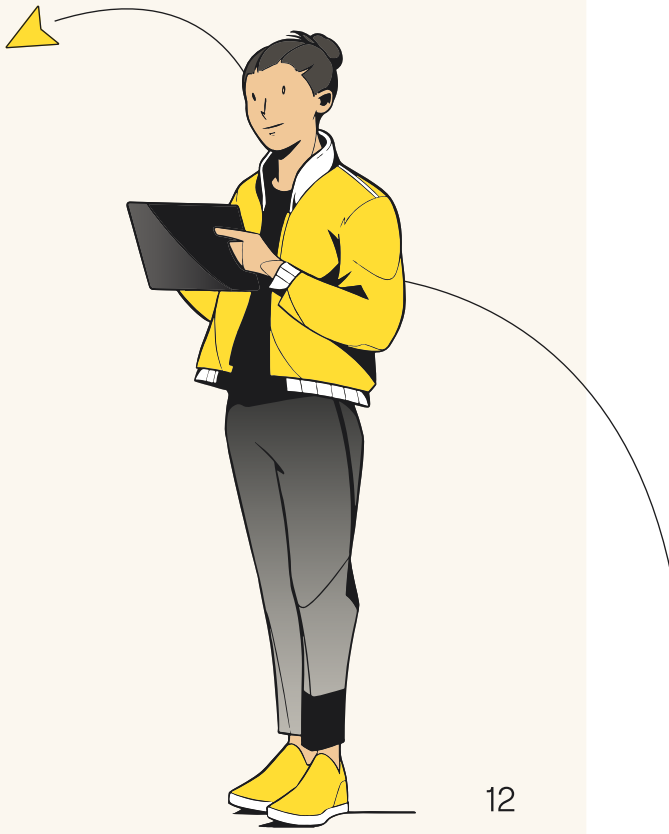
Where Miro processes personal data on behalf of its customer or transfers personal customer data outside of the EU, we agree to enter into appropriate terms, for example through our Data Processing Addendum (DPA), which include contractual commitments required by GDPR, the California Consumer Privacy Act (along with its modification through the California Privacy Rights Act), and other US and global privacy and data protection laws.

Third-party data processing

To the extent Miro engages third parties to process personal customer data, we require a strict procurement process that includes legal and security checks, and agreement with appropriate data processing and transfer terms. Miro provides the list of such third parties online, available through a link in its DPA, and informs customers of its intention to change or add any relevant third party to that list per the process laid out in the DPA.

Product security

As a cloud-based platform, Miro can be accessed from a web browser on both desktop and mobile devices, or via dedicated apps for both platforms. Because of these touchpoints and the nature of remote, distributed collaboration via a platform like Miro, we must help customers approach a Zero Trust Architecture (ZTA). This means not only empowering our customers to have the right security solutions, but also helping ensure they are deployed correctly.



Zero Trust Architecture

Unlike traditional security models that grant broad access based on a user's location or network entry point, ZTA assumes that threats can originate from anywhere, even within the organization. This has become increasingly important in the modern work environment in which employees access corporate resources from various locations and devices. ZTA advocates for continuous verification of identity, device security, and adherence to security policies throughout every user interaction with data and resources.

Miro helps enterprise organizations approach ZTA by empowering admins to set the right policies with granular permissions and controls, without compromising teams' ability to collaborate. These security controls include:

- **SSO:** With SAML-based SSO, users can access Miro through an identity provider (IdP) of their choice, including Okta, Azure AD, AuthO, Google SSO, and others. This eliminates the need for users to repeatedly enter their credentials for each application, saving them time while also reducing the number of attack surfaces.

- **2FA:** Two-factor authentication (2FA) works in Miro without requiring SSO, and adds an extra layer of protection when users access their organization's Miro subscription. 2FA applies to any users logging in with their email and password (external collaborators for companies with SSO or all users for organizations who do not have SSO configured). Users can set this up in their profile, or Company Admins can enable 2FA for an entire organization. Miro enforces 2FA with a time-based one-time password (TOTP) application such as Microsoft Authenticator, Google Authenticator, and Authy.

- **Idle session timeout:** Set limits on how long users can be inactive before being automatically logged out. This limit minimizes the window of time in which an attacker can try to steal and use an existing user session (either remotely or in-person via an unattended workstation).

- **Role-based access for admins:** There are multiple admin roles that can be assigned to users to perform workflows (e.g. Company Admin, User Admin, Content Admin), each with specific levels of access privileges, settings, and configurations. This securely distributes the administration workload, preventing admins from having unnecessary privileges or access to sensitive information.

- **Sharing policies:** Decide when and how your organization's content should be accessed, setting policies to:
  - Restrict sharing outside allowed domains
  - Restrict sharing via public link
  - Require passwords for public boards (Company level)
  - Restrict team-wide and company-wide sharing (Team level)
  - Restrict ability to move boards to other teams (Team level)
  - Restrict company-wide customer template sharing

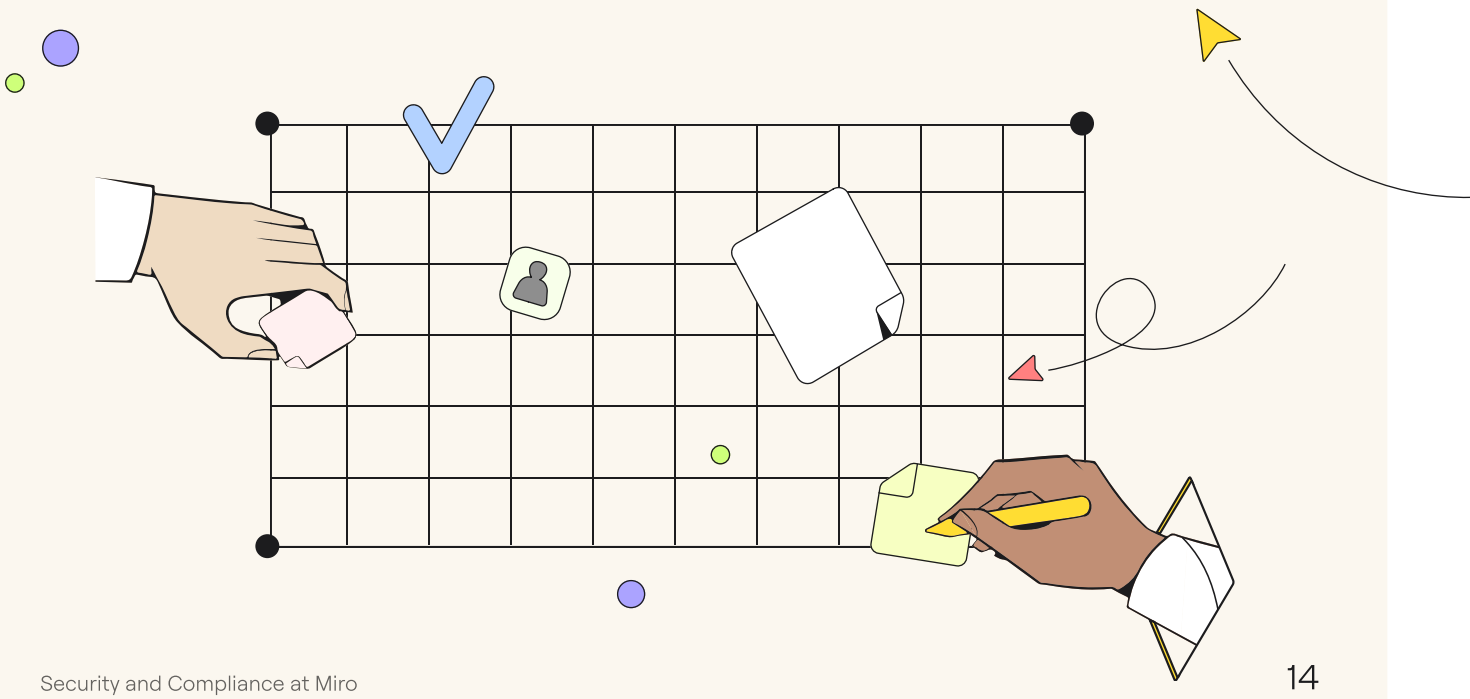
- **Enterprise Mobility Management:** Securely manage access to Miro from corporate-owned or personal devices with Enterprise Mobility Management (EMM) tool integrations such as Microsoft Intune and VMware Workspace ONE, supporting both Android and iOS

- **Audit logs:** Company Admins can view all activity within their organization. Logs help with troubleshooting or when a detailed report of important events is needed, such as changes to global security settings, invitations of new users, or the creation of new boards.

- **Classification:** Enterprise Plan users can assign classification labels to their board content to indicate sensitivity level. Default labels can be configured at the company or team level, and users can use these labels to filter boards in their dashboard.

- **Content lifecycle management:** Miro allows users to filter by company to efficiently manage the lifecycle of boards at the company level. Additionally, a global trash menu is easily accessed where trashed boards can be restored or permanently deleted.

- **Administration:** Automation plays a critical role in preventing errors and saves time when dealing with hundreds of thousands of boards and users. Leveraging SCIM or JIT provisioning automates user access and streamlines user lifecycle management.



Artificial intelligence

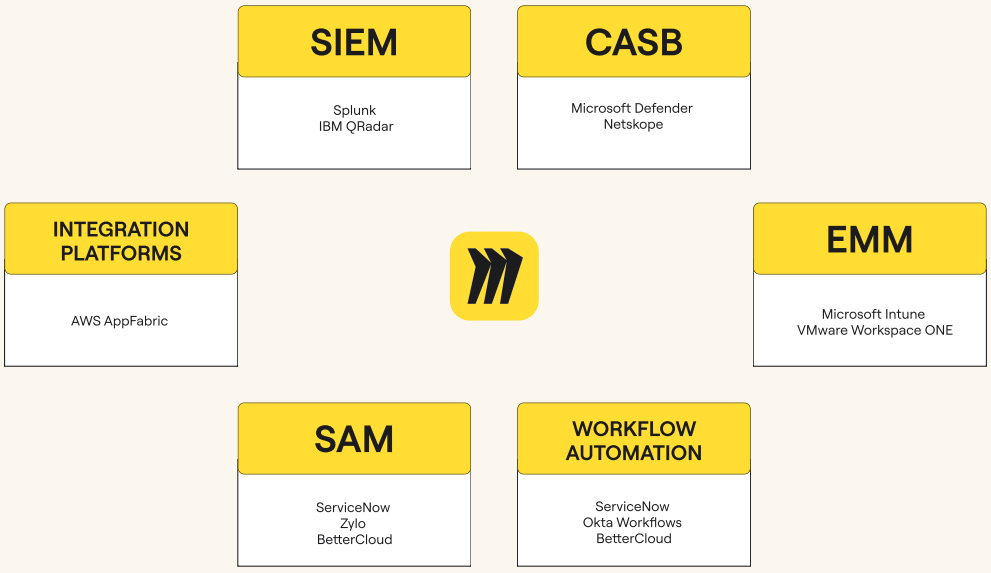
AI at Miro is treated with the same care and attention to security as the rest of the product. Our guiding principles and practices toward AI demonstrate our commitment to ethical and responsible AI development so that we maintain trust with customers, users, and partners.

This includes accountability through transparent AI models. We use data only as outlined in our privacy policy, or as explicitly agreed upon between Miro and the customer. Customers maintain full control over their content. We also allow customers to preserve control by opting in or out of AI services. Learn more in our whitepaper.

Enterprise ecosystem integrations

Enterprise plan customers can take advantage of a variety of security and compliance integrations including security information and event management (SIEM) solutions, cloud access security brokers (CASB), EMM, integration platforms, software asset management (SAM) tools, and workflow automation. Companies can also develop their own custom integrations.

Enterprise-grade integrations



miro | ENTERPRISE GUARD

Advanced data security and governance add-on

The work done in Miro is often strategic and requires governance. Customers increasingly use Miro to create and store confidential and proprietary data, and sensitive data can show up where you least expect it despite company policies. To add to this, the amount of content in Miro boards grows in our largest customers by a rate of 2.5x per year,[1] further increasing the risk surface for data security and governance.

Core enterprise-grade SaaS application security features such as authentication and SSO, as well as granular access controls, give most customers enough control over when and how they protect their data. But some customers want additional layers of protection on top of our standard security measures because of how strategic Miro is to their business, or because of the regulatory compliance requirements of their sector, or a combination of both.

That's where Miro Enterprise Guard — an advanced data security and governance add-on — comes in.

[1] Cumulative growth of boards in 1k+ Enterprise organizations from 2017 to 2023

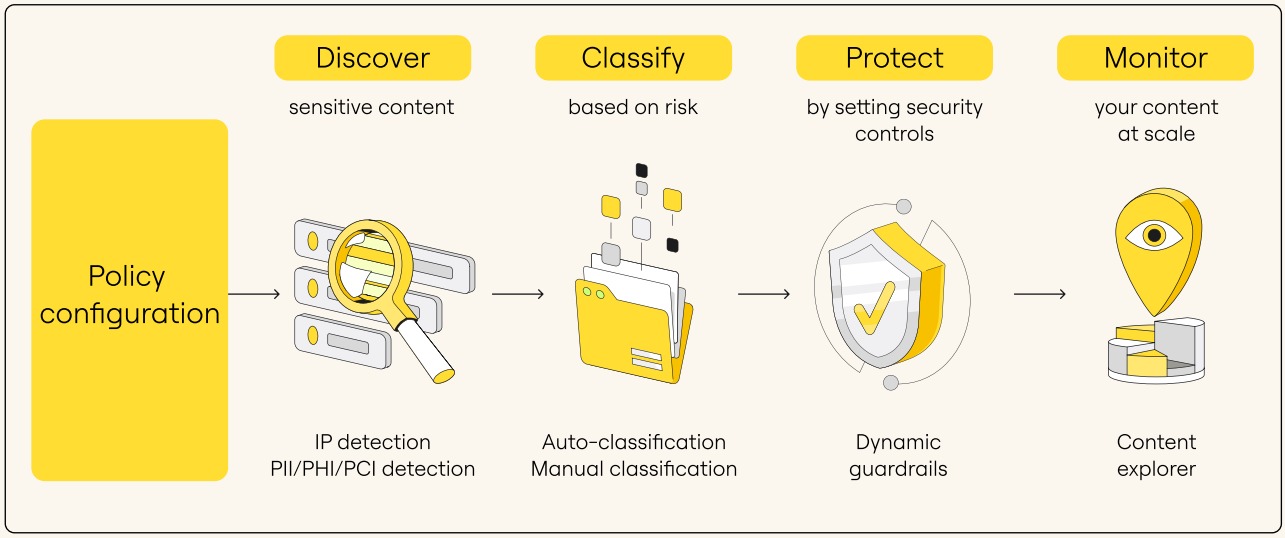
Find, classify, and secure sensitive content

Enterprise Guard automates the process of finding and classifying sensitive data across Miro and offers increased data security controls. Enterprise Guard:

- Scans your Miro boards, **identifying and classifying sensitive data** such as PII, PCI, PHI, and business-critical information.
- Applies **classification labels automatically** to what is found, based on predefined criteria that you can set in Miro or in other data security tools via integration.
- Applies **Intelligent Guardrails** based on board classification labels. Intelligent Guardrails are dynamic controls that you set according to your policy that can prevent certain user actions such as copying/pasting, public sharing, and board exporting.
- You can also get a unified view of all Miro boards with sensitive content and each board's classification labels with **Content Explorer**. You get increased visibility into what needs to be protected, and precision controls to do so, while supporting collaboration across your organization.

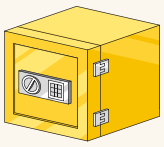


Adapting security to risk

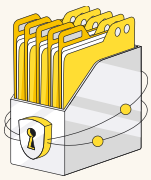


Manage the lifecycle of content at scale

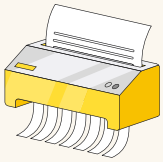
Enterprise Guard automates the process of managing the lifecycle of your boards to support you in meeting your compliance or organizational policy requirements.
With the features you can:



Retain boards according to policy with a full audit trail



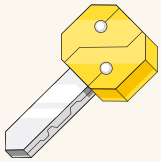
Delete boards according to policy with a full audit trail restoration



Define org-level trash policy for enhanced control over defensible permanent deletion and retention of your Miro board

Key management

Also included as part of the Enterprise Guard add-on bundle is the option for **Enterprise Key Management (EKM)**, which supports key management with a key hosted in your own AWS account via AWS KMS.
This provides greater auditing visibility and increased access control over data such as account names, project names, and user-generated content — including widgets, comments, and uploaded files.
Plus, when customers bring their own key ("BYOK"), they can audit key usage by accessing the logs of all API calls made on them, to help meet compliance and regulatory requirements.



Enterprise Key Management (EKM)

Conclusion

Most executives are unhappy with their organization's ability to innovate and compete. In fact, 82% of leaders believe a company will become extinct within five years if it fails to innovate. Some of the biggest blockers to innovation are technological challenges such as outdated, legacy tools. Leaders and information workers agree that legacy technology stifles creativity and impedes productivity. That's why many organizations have rushed to implement collaboration tools without fully considering the security implications.

With a visual collaboration workspace like Miro, innovation is made easy — and secure. Because we are committed to protecting the security and data of our customers, over 60 million users worldwide, including 99% of the Fortune 100, have entrusted Miro with their most valuable asset: their information. Join these leading companies and take advantage of a collaborative innovation workspace, knowing that throughout, you can feel confident that your data is safe and secure.

Contact our sales team to learn more.

Resources

Miro Trust Center
Encryption whitepaper
Data residency at Miro
Security & compliance FAQ (Help Center)
Annual transparency report
Privacy Policy
Terms of Service
Miro Enterprise
Accessibility guidelines



Miro is a visual workspace for innovation that enables distributed teams of any size to build the next big thing. The platform's infinite canvas enables teams to lead engaging workshops and meetings, design products, brainstorm ideas, and more. Miro, co-headquartered in San Francisco and Amsterdam, serves more than 60M users worldwide, including 99% of the Fortune 100. Miro was founded in 2011 and currently has more than 1,800 employees in 12 hubs around the world.

miro

To learn more, please visit miro.com.

Miro Enterprise Plan
https://miro.com/enterprise/

Miro Blog
https://miro.com/blog/

LinkedIn
https://www.linkedin.com/company/mirohq/

X (formerly Twitter)
https://twitter.com/MiroHQ