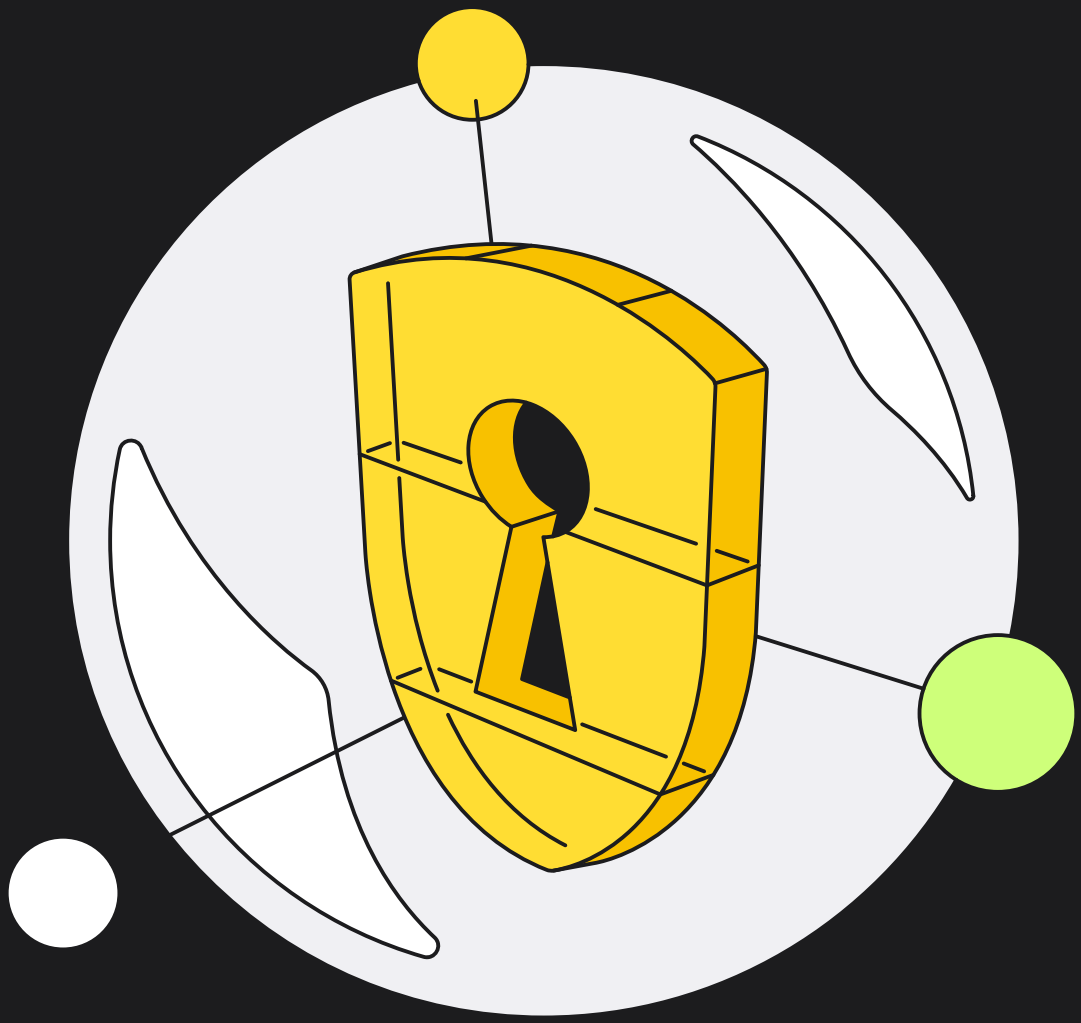


Encryption at Miro:

Ensuring Data Privacy, Protection & Trust

miro

miro.com
October 2023

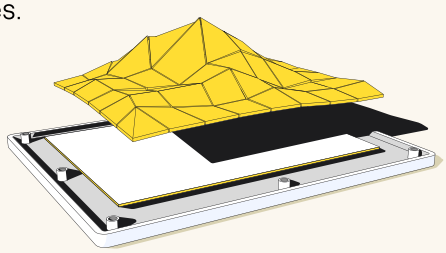
Table of Contents

Overview 3
How encryption works at Miro? 4
Miro data in transit 5
Miro data at rest 7
Miro Enterprise Key Management 7
Why Miro at your enterprise 8



Overview

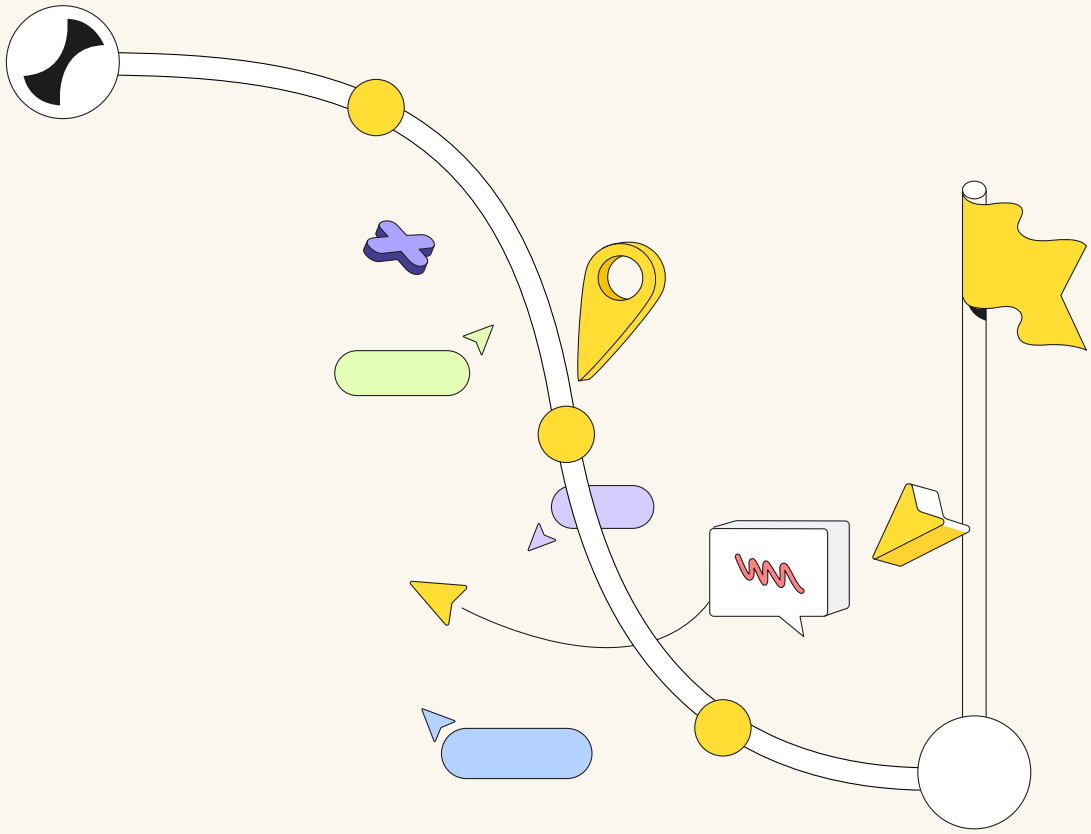
In the digital age, data has become the lifeblood of organizations, powering critical operations, enabling innovation, and driving strategic decision-making. However, the increasing volume and complexity of data bring forth new challenges, especially when it comes to safeguarding sensitive information from unauthorized access and breaches.



This is where enterprise encryption emerges as a crucial pillar of comprehensive data security. Enterprise organizations are looking for robust encryption measures to ensure confidentiality, integrity, and compliance.

At Miro, we must balance the maximum amount of data security with the technical requirements of the enterprise organizations that depend on our platform.

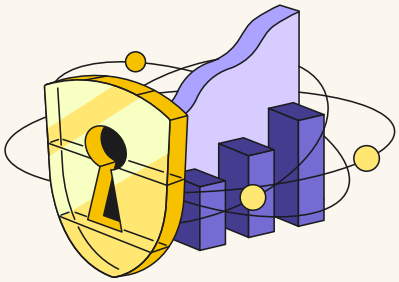
Let's explore the different encryption methods used by Miro to protect user data.



How encryption works at Miro

Miro users connect to the service via a web browser or a dedicated Miro app (referred to as “Miro client”). The Miro client is a wrapper for the content on the Miro cloud service (referred to as “Miro”). Therefore, no matter which user interface is used, the data connection, transmission, and encryption remain the same.

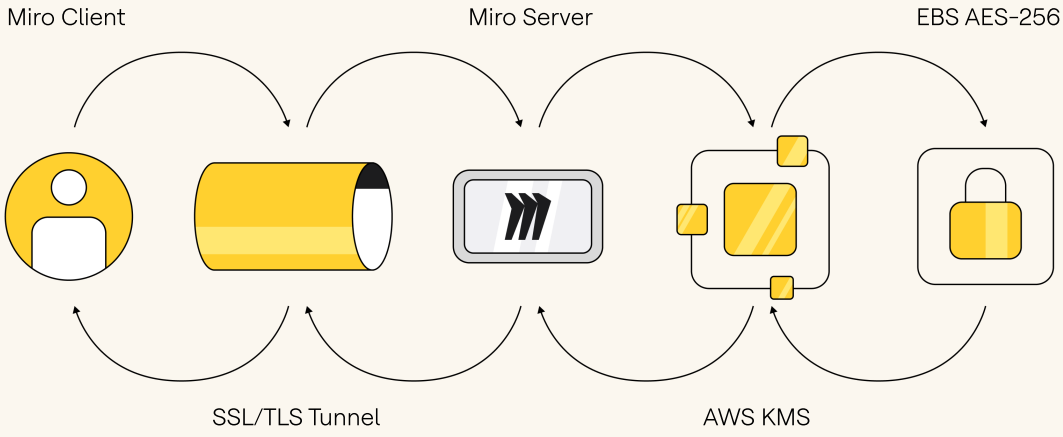
In order to ensure the security, privacy, compliance, and trust of Miro’s service offering, Miro leverages encryption both in transit and at-rest. Data in transit between our customers and Miro uses an encrypted tunnel with Transport Layer Security (TLS), which is a cryptographic protocol that provides end-to-end security of data sent between applications over the internet.





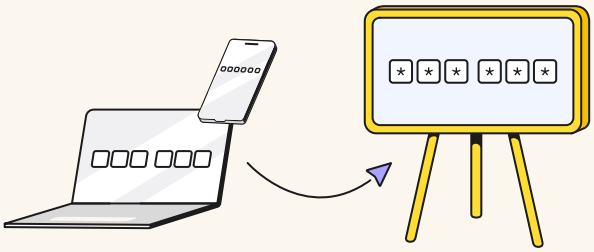
At Miro, we use the latest version of the TLS protocol: **TLS 1.3**. Data at rest is fully encrypted using **AES-256** with AWS Key Management Service (KMS) for managing Elastic Block Storage (EBS) volumes and S3 buckets. In combination, these encryption technologies ensure that data is secure while it is transferred and at rest. This is an industry standard for data protection and Miro invests the appropriate resources and effort to stay up to date with the latest protocols, versions, and algorithms.

Another way of looking at it, at a high level, is that Miro leverages TLS 1.3 when communicating with their customers and AES-256 encryption when storing the information. This combination ensures end-to-end encryption throughout the data lifecycle.



Miro data in transit

Sensitive data must be protected, especially when it is in transit. Encryption provides the most practical means to do so and helps establish trust and preserve anonymity. That's why as the latest version of the TLS protocol, TLS 1.3 encryption is ideal for protecting communication over the internet.



In addition to TLS 1.3, data connections between Miro's customers and Miro leverage PKI Certificates issued by AWS. The strength of the encryption and specific ciphers used for connections will depend on the client used to access the site, and the results of the common encryption method negotiated.

Benefits of encrypting data in transit

TLS provides two important advantages for web browsing: **privacy** and **anonymity**.

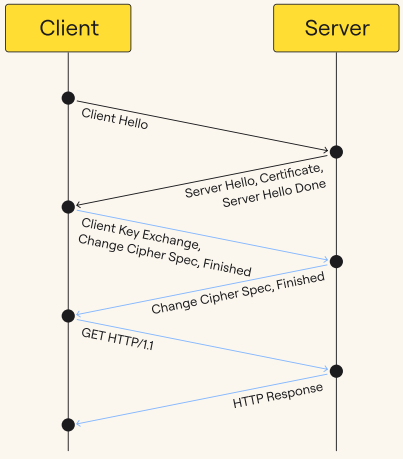
Privacy means data contained within the secure tunnel cannot be seen by or shared with another party.

Anonymity means users browsing behavior is hidden from any parties between the customer side and Miro. While anonymity shields information, it does not provide anonymity of the IP addresses involved. This can be addressed with the use of proxies.

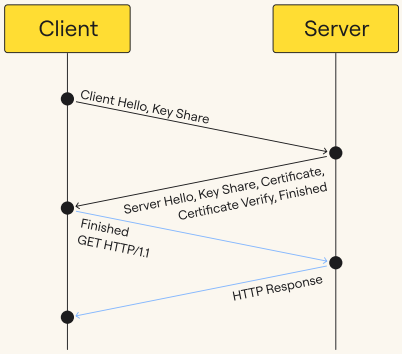


Diagram of a TLS Handshake

TLS 1.2 (Full Handshake)



TLS 1.3 (Full Handshake)

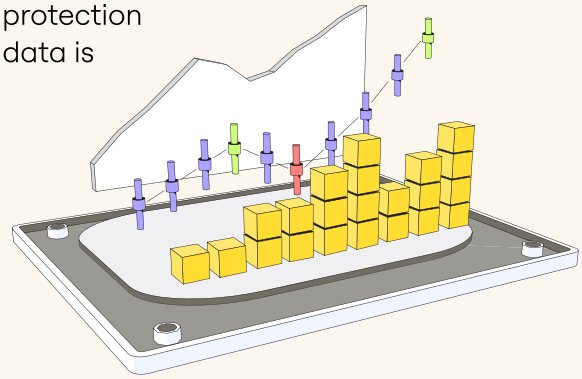


miro

The importance of TLS 1.3

In August 2018, a new and improved version of the TLS protocol called TLS 1.3 was released. Compared to the earlier TLS 1.2, this update made encrypted connections faster and safer. TLS 1.3 fixed the problems found in the previous version and now uses only the best security techniques available, making it much more secure.

In addition, TLS 1.3 increased privacy by adding extra protection to the initial steps of the connection process, so your data is safe from potential snooping or spying.



Features removed in TLS 1.3:

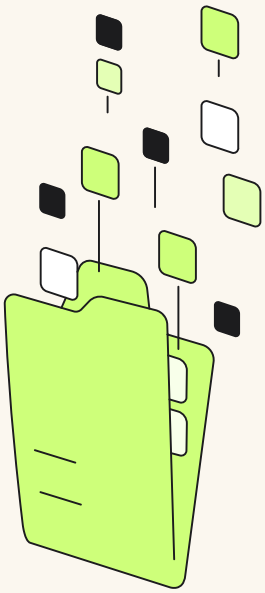
- Static RSA handshake
- CBC MtE modes
- RC4
- SHA1, MD5
- Compression
- Regeneration

How TLS negotiation works

TLS establishes a secure tunnel between the Miro client and Miro by using third-party validated public-key certificates. These certificates are used to establish the chain of trust for data in transit. This happens during the process of a TLS handshake.

A TLS handshake occurs whenever a user navigates to Miro and the Miro client begins to query the website's origin server. A TLS handshake also occurs whenever communications use HTTPs.

The following actions occur during a TLS 1.3 handshake:

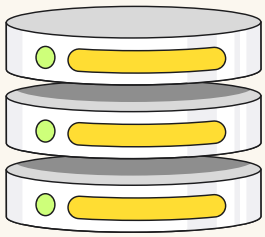


- **Client Hello** — Includes TLS version and cipher suites supported by the client and a string of random bytes known as "client random."
- **Key Share** — Contains client's public key shares for the key exchange.
- **Server Hello** — In response to Client Hello and Key Share, the server sends a message containing the server's certificate, chosen cipher suite, and a string of random bytes known as "server random."
- **Key Share** — Contains server's public key shares for the key exchange.
- **Certificate** — Server sends its certificates, which carries its public key.
- **Certificate Verify** — Server sends a message to client, with the authentication value computed with the session hash.

Miro data at rest

Miro leverages different AWS solutions for storing data (including EBS, S3, and DynamoDB) which support encryption at rest using native integration with AWS KMS.

All customer data loaded in Miro is therefore secured at rest with AES-256 encryption using keys managed by AWS KMS. AWS KMS is a managed service that allows Miro to concentrate on the cryptographic needs of the service while AWS manages the availability, physical security, logical access control, and maintenance of the underlying infrastructure.



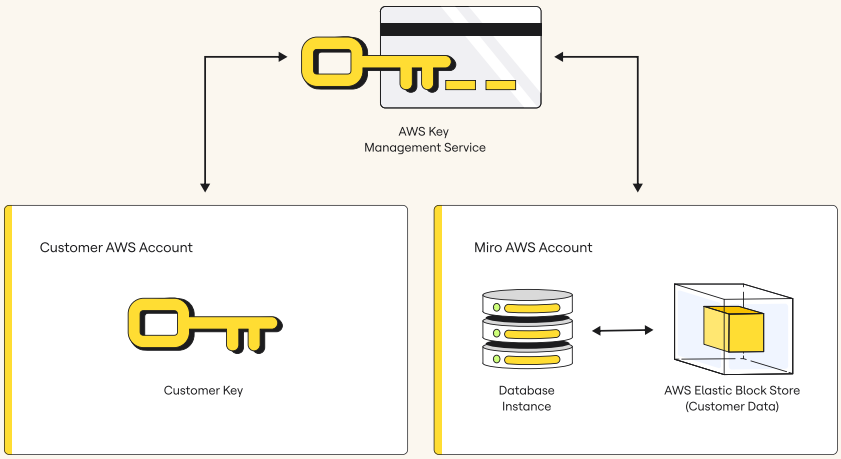
Miro Enterprise Key Management

Miro supports key management with a key hosted in your own AWS account via AWS KMS. With Miro Enterprise Key Management (available with some licenses), customers gain greater auditing visibility and increased access control over user-generated content, such as shapes, widgets, and uploaded files. In addition, when customers bring their own key ("BYOK") they can audit usage of the keys by accessing the logs of all API calls made on them, to help meet compliance and regulatory requirements.

Why Miro EKM

Miro supports key management with a key hosted in your own AWS account via AWS KMS.

1. **Easy to implement:** 100% cloud-based solution. No hardware to install or maintain.
2. **Full control over key access:** Revoke your key at any time to render all encrypted data unreadable to Miro and end users.
3. **Detailed access visibility:** Monitor activity logs related to your encryption key via AWS CloudTrail.



miro

Why Miro for your enterprise

Miro encrypts all data when it's stored, in transit over the internet, and traveling between our primary and secondary data centers. At Miro, we constantly strive to meet the ever-changing security needs of our customers.

Learn more about Miro's commitment to security.

Contact us today if you're ready to get started.

Resources

Security at Miro
Miro Trust Center
Security and compliance (Help Center)
Terms of Service
Privacy Policy
Miro Enterprise

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 1,500 employees in 12 hubs around the world.

To learn more, please visit miro.com.

Miro Enterprise Plan
miro.com/enterprise/

X (formerly Twitter)
twitter.com/MiroHQ

LinkedIn
linkedin.com/company/mirohq/

Miro Blog
miro.com/blog/