miro

Sécurité et conformité chez Miro :

une solide protection de niveau entreprise

miro

Table des matières

Généralités

Pour survivre, les entreprises doivent innover. En tant qu'espace de travail visuel numéro un conçu pour l'innovation, Miro aide les entreprises à atteindre ce but. Plus de 180 000 entreprises performantes et innovantes, dont 99 % des entreprises Fortune 100, telles que Google, Cigna, Nike, Ikea, Deloitte et Cisco, lui font déjà confiance.

Ces entreprises utilisent Miro pour élaborer des stratégies et planifier, concevoir des produits et services orientés clients, et bien plus encore. Cependant, établir une relation entre des équipes et des effectifs répartis dans le monde entier nécessite une plateforme sécurisée et fiable pour collaborer avec des informations confidentielles. Sans compter que toutes les personnes d'une entreprise ont besoin du bon accès, au bon moment.

Dans ce livre blanc, nous résumons la façon dont Miro aide les entreprises à innover en garantissant, à un haut niveau, **la sécurité de l'infrastructure, la conformité, les contrôles de sécurité des produits** et **la confidentialité.**

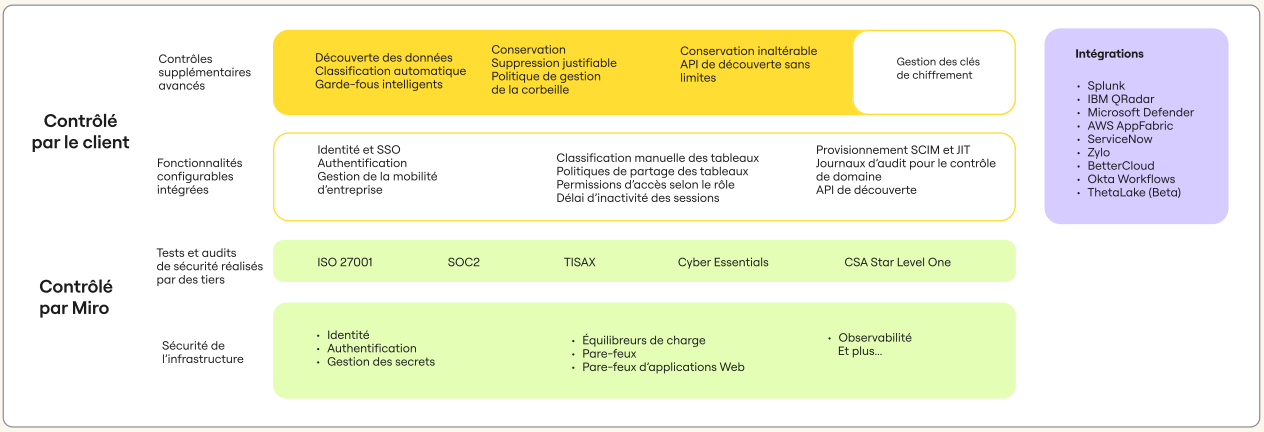
Notre responsabilité partagée

Le présent livre blanc détaille nos domaines de responsabilité et vous informe de toutes les options disponibles pour renforcer le niveau de sécurité de votre entreprise lorsque vous utilisez Miro.

Le schéma ci-dessous récapitule notre stratégie de sécurité. Les deux couches inférieures représentent les éléments que Miro contrôle pour protéger les informations et garantir le respect de ses obligations de conformité. Les deux couches supérieures représentent les fonctionnalités de Miro que vous pouvez configurer en fonction de vos besoins de sécurité et de conformité.

Nous étudierons ces fonctionnalités tout au long de cet article.

Architecture de sécurité et de conformité de Miro



Sécurité de l'infrastructure

Notre produit étant une plateforme SaaS (Software-as-a-Service, ou logiciel en tant que service) professionnelle, la protection des informations est la pierre angulaire de notre stratégie de sécurité globale. Cette protection recouvre les actifs technologiques physiques tels que les ordinateurs et les systèmes de réseau, ainsi que les ressources cloud. En sécurisant ces actifs, nous assurons une défense non seulement contre les attaques de cybersécurité traditionnelles, mais aussi contre les menaces physiques telles que le vol et les catastrophes naturelles. En d'autres termes, les informations de notre clientèle sont sécurisées.

Centres de données

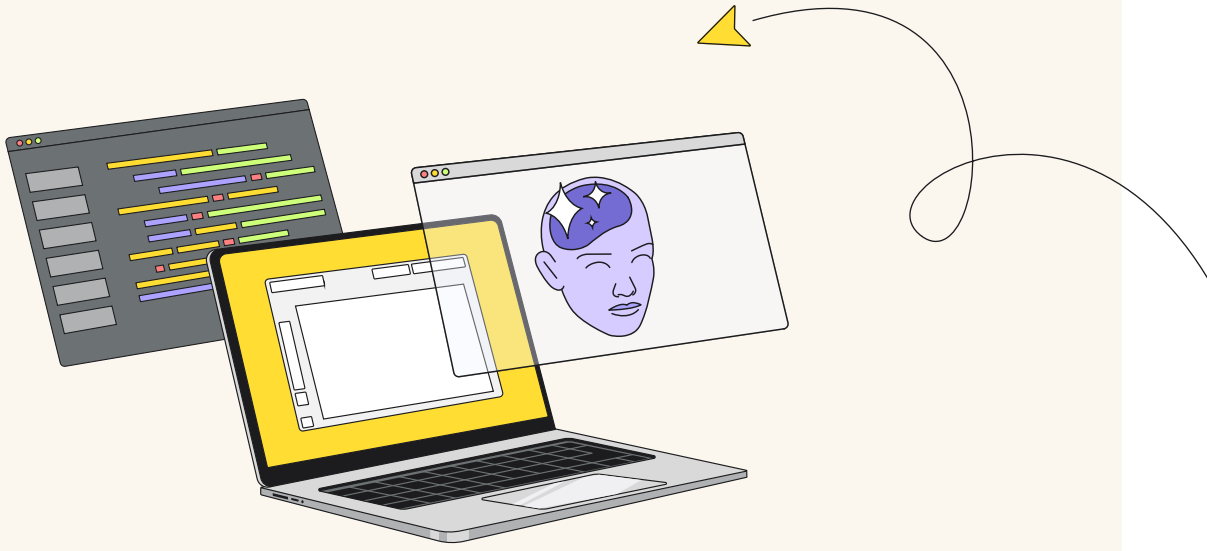
Miro utilise principalement Amazon Web Services (AWS) pour son infrastructure cloud, ainsi que les fonctionnalités de sécurité d'AWS pour protéger les données et les charges de travail hébergées. Le cloud computing s'appuie sur un modèle de responsabilité partagée.

AWS met en œuvre des mesures de sécurité strictes, par exemple des contrôles physiques variés au niveau des centres de données, des garanties de confidentialité et des contrôles en profondeur appliqués à ses services. Les environnements informatiques AWS font l'objet d'audits continus, renforcés par des certifications d'organismes d'accréditation dans différentes zones géographiques et différents secteurs d'activité, notamment SOC 1, SSAE 16, ISAE 3402 (anciennement SAS 70), SOC 2, ISO 9001, ISO 27001, FedRAMP, DoD SRG et PCI DSS de niveau 1.

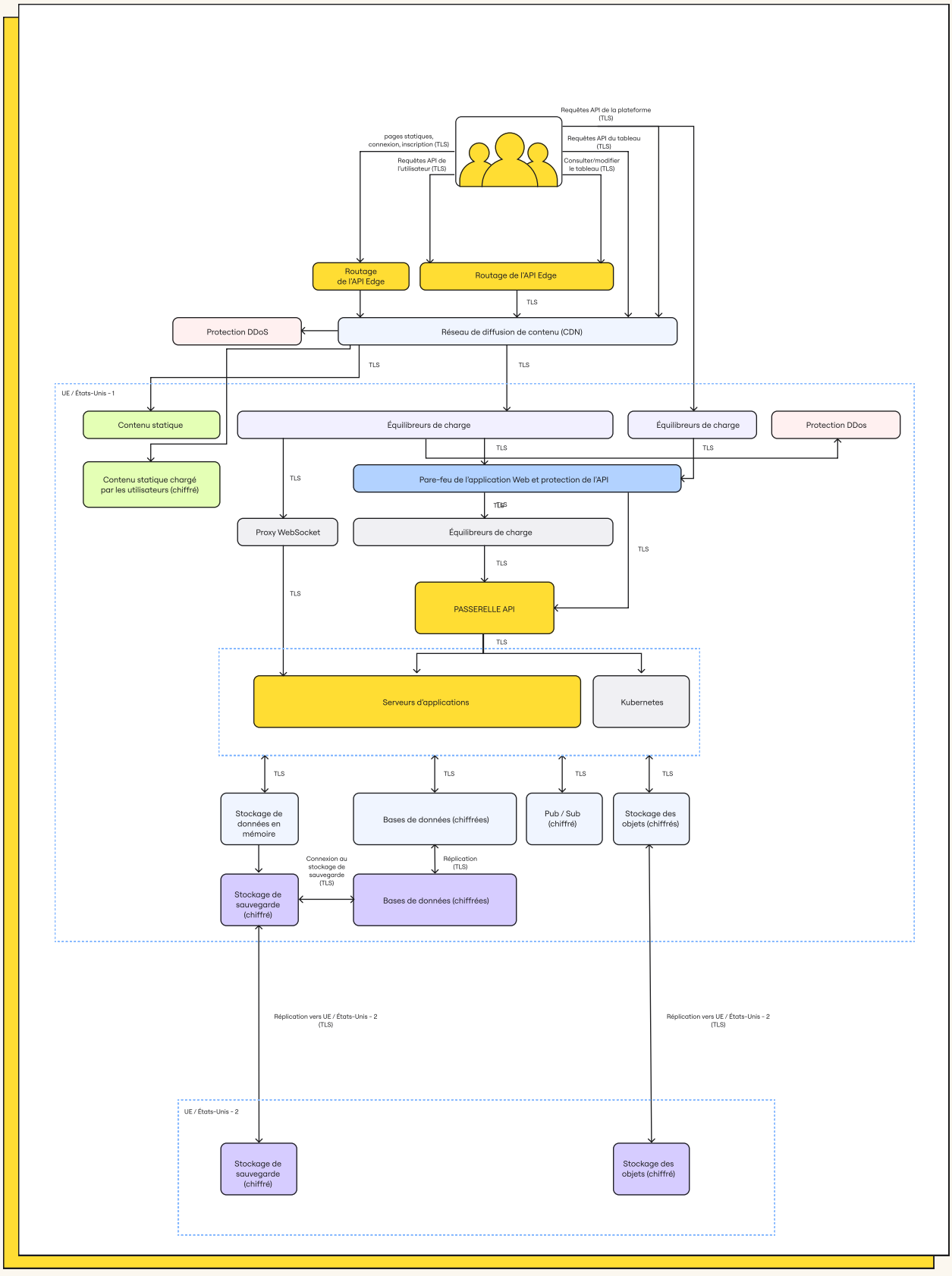
Nos principaux systèmes de production sont hébergés dans des centres de données AWS situés dans l'Union européenne (Irlande) et aux États-Unis (Ohio). En outre, des centres de données AWS en Europe (Francfort) et aux États-Unis (Virginie) permettent de stocker les sauvegardes. Ils peuvent entrer en opération conformément au plan de reprise après sinistre (PRS).

Dans l'infrastructure cloud AWS, Miro est responsable de configurer la sécurité logique, du réseau et des applications, conformément aux meilleures pratiques sectorielles et au cadre Well-Architected d'AWS. Les mesures de protection sont mises en œuvre selon une méthode à plusieurs niveaux, conformément au principe du moindre privilège et du refus par défaut, sauf autorisation explicite. La gestion et l'accès sont strictement limités à des membres du personnel spécifiques et nécessitent une authentification multifacteur (MFA) ainsi qu'un accès à partir d'appareils gérés via un réseau privé virtuel (VPN).

Pour plus d'informations, consultez l'article Modèle de responsabilité partagée d'AWS



Flux de données dans l'UE et aux États-Unis

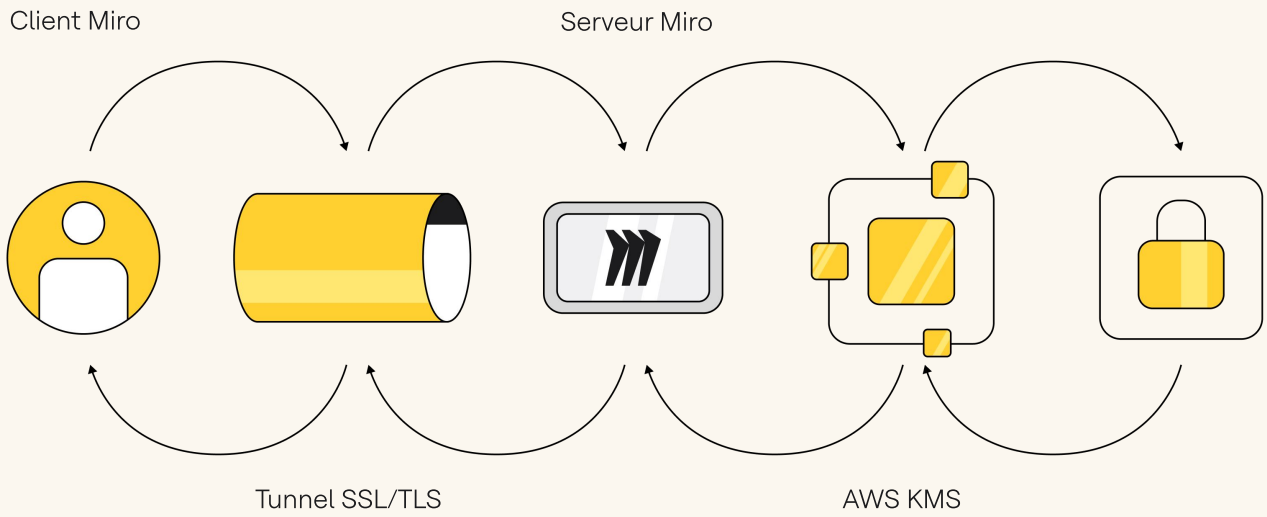


Chiffrement des données

Afin de protéger les données des personnes qui utilisent sa plateforme, Miro harmonise la sécurité des données avec les exigences techniques de nos entreprises clientes au moyen de diverses méthodes de chiffrement.

Miro respecte les dernières normes de chiffrement pour la protection des données au repos et en transit. Nous utilisons ainsi **le chiffrement AES (Advanced Encryption Standard) 256 bits** au repos et **le protocole TLS (Transport Layer Security) 1.3**, en plus de la version 1.2, pour les données en transit. Ensemble, ces normes garantissent un chiffrement de bout en bout tout au long du cycle de vie des données.

Chiffrement dans Miro



Pour plus d'informations, téléchargez notre livre blanc sur le chiffrement.

Gestion des clés de chiffrement

Notre infrastructure de gestion des clés intègre des contrôles de sécurité opérationnelle, technique et procédurale, et offre un accès direct très limité aux clés. Les opérations de génération, d'échange et de stockage des clés sont menées séparément, pour un traitement décentralisé. Nous assurons leur gestion à l'aide d'une clé hébergée sur votre compte AWS via AWS Key Management System (KMS).

- **Clés de chiffrement des fichiers** Les clés de chiffrement des fichiers sont créées, stockées et protégées par des contrôles et des politiques de sécurité dans l'infrastructure du système de production.
- **Clés SSH internes** L'accès aux systèmes de production est restreint à l'aide de paires de clés SSH uniques. Un système interne gère le processus sécurisé d'échange des clés publiques, et les clés privées sont stockées en lieu sûr.
- **Distribution des clés** Miro automatise la gestion et la distribution des clés sensibles aux seuls systèmes requis pour les opérations. Le système de distribution des clés est basé sur AWS KMS.

Gestion des secrets

Les données sensibles telles que les mots de passe, les clés API, les identifiants de base de données et les certificats sont stockées en toute sécurité dans nos systèmes de gestion des secrets. Seuls les services qui les nécessitent et un nombre restreint d'ingénieurs d'exploitation sont autorisés à accéder à ces systèmes.

Contrôle d'accès et authentification

Les contrôles d'accès technique et les politiques internes de Miro empêchent les membres de son personnel d'accéder de façon arbitraire aux tableaux des utilisateurs et utilisatrices ainsi qu'à leurs informations de compte. Seuls quelques ingénieurs en charge du développement des services essentiels de Miro ont un accès limité aux tâches de dépannage, et ce uniquement avec le consentement explicite des utilisateurs et utilisatrices. Notre équipe d'assistance n'a pas accès au contenu des tableaux, sauf si un client ou une cliente l'y invite explicitement. De plus, lorsqu'un membre du personnel quitte l'entreprise, les autorisations d'accès dont il disposait sont immédiatement supprimées.

Sécurité réseau

Miro assure la sécurité du réseau backend à l'aide de plusieurs couches de protection et de défense : groupes de sécurité, proxys, surveillance et tests de sécurité réseau, systèmes de détection d'intrusion et audits.

L'accès au réseau interne de l'environnement de production est limité aux groupes d'utilisateurs autorisés, via le VPN, et à l'aide de l'authentification unique (SSO) et de l'authentification multifacteur. L'authentification par clé est en outre requise sur tous les systèmes.

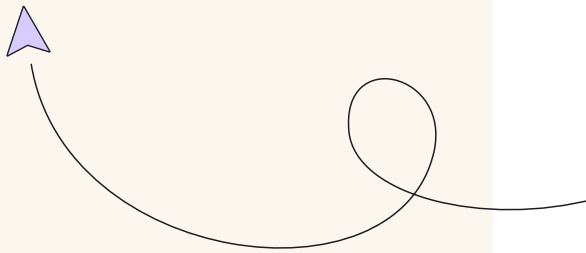
Gestion des vulnérabilités

L'équipe de sécurité de Miro effectue régulièrement des tests de sécurité automatiques et manuels sur les applications et l'infrastructure. Elle peut ainsi identifier et corriger les éventuelles vulnérabilités. En outre, des fournisseurs de service indépendants effectuent chaque année des tests d'intrusion externes, et les problèmes identifiés sont rapidement corrigés. Enfin, notre programme public de prime au bug incite les chercheurs en sécurité à soumettre toutes les vulnérabilités découvertes dans nos produits et services.

Gestion des changements

Miro dispose d'une politique formelle de gestion des changements selon laquelle toutes les modifications apportées à une application sont autorisées avant la mise en œuvre dans l'environnement de production et toutes les exigences de sécurité sont respectées. Seul le personnel autorisé peut apporter des modifications à l'environnement de production de Miro. De son côté, l'équipe de sécurité veille à maintenir à jour la configuration du serveur, du pare-feu et les autres configurations de sécurité, conformément aux normes sectorielles.

En gérant le niveau de sécurité dans le cloud, nous pouvons devancer les menaces les plus sérieuses dans notre environnement cloud. Nous recevons en outre des alertes concernant les vulnérabilités ou les mises à jour requises dans notre infrastructure cloud.



Politiques de sécurité

> Chez Miro, nous évaluons les risques et améliorons constamment le niveau de sécurité, de confidentialité, d'intégrité et de disponibilité du service. Nous révisons et approuvons au moins une fois par an nos politiques de sécurité (sécurité de l'information, cycle de vie sécurisé du développement de logiciels, réponse aux incidents, accès logique et gestion du changement). En outre, nous surveillons la conformité à ces politiques, nous effectuons des tests de sécurité sur les applications et le réseau, et nous évaluons les risques internes et externes.

Politique relative aux membres du personnel et accès

Lorsque la législation locale le permet, les membres du personnel de Miro sont soumis à des vérifications des antécédents judiciaires. Les équipes doivent par ailleurs signer une reconnaissance de la politique de sécurité, s'engager à respecter la confidentialité et suivre des formations de sécurité obligatoires afin de garantir la mise en application des meilleures pratiques et de protéger les données de notre clientèle.

L'accès entre les réseaux est strictement limité au nombre minimum de membres du personnel et de services, et la configuration du pare-feu est étroitement contrôlée et restreinte à quelques administrateurs. L'accès à d'autres ressources est accordé par l'approbation explicite des personnes concernées, et la demande d'accès et sa justification sont consignées par la direction.

Sécurité physique

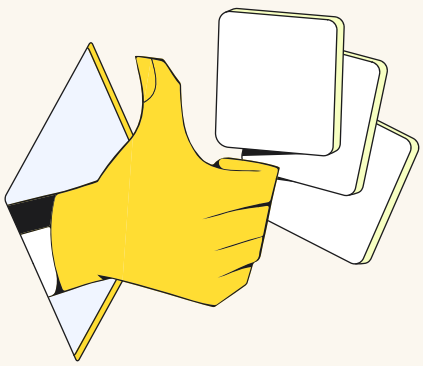
Miro fait appel à un fournisseur tiers professionnel pour appliquer sa politique de sécurité physique et superviser la sécurité de ses bureaux. L'accès physique aux locaux de Miro est limité à son personnel autorisé via un système de badges. En outre, un badge pour les visiteurs permet de s'assurer que seules les personnes autorisées peuvent accéder aux installations de l'entreprise. L'accès aux zones des serveurs d'entreprise est limité au personnel autorisé grâce aux rôles élevés attribués via le système de badges. La liste des personnes autorisées à accéder physiquement aux environnements de l'entreprise et de production est examinée au moins une fois par trimestre.

Fiabilité

L'infrastructure des serveurs Miro permet un stockage sûr des données et une disponibilité élevée. Tous les services d'application fonctionnent sur différents serveurs dotés d'un système d'équilibrage de charge/de tolérance aux pannes pour augmenter la redondance. Les topologies de groupe correspondent au niveau de disponibilité N+1. Les données des utilisateurs et utilisatrices sont répliquées dans plusieurs régions de disponibilité à des fins de protection, et elles sont régulièrement chiffrées et sauvegardées. De plus, les sauvegardes quotidiennes de la base de données sont stockées séparément du centre de données principal.

Réponse aux incidents

L'équipe d'intervention de Miro est prête à répondre à tout incident 24 h/24, 7 j/7. Nos politiques de réponse aux incidents traitent les problèmes de disponibilité, d'intégrité, de sécurité et de confidentialité des services. Les procédures incluent une réponse rapide aux incidents, une évaluation de la gravité, des mesures de confinement, la communication avec les parties prenantes et des mises à jour de l'état sur status.miro.com.



Reprise après sinistre

En cas de crise ou de sinistre affectant les opérations de Miro, notre équipe en charge de l'infrastructure suit un plan de reprise pour assurer la sécurité de l'information. Les problèmes détectés sont documentés et suivis jusqu'à leur résolution. L'équipe passe en revue et teste ce plan, y compris la mesure du temps de récupération réel (RTA), au moins une fois par an.

Notre PRS (plan de reprise après sinistre) tient compte des sinistres affectant la durabilité et la disponibilité. Un sinistre affectant la durabilité se définit par une perte totale ou permanente des centres de données primaires, ou par l'incapacité de communiquer ou d'utiliser les données des centres de données.

L'objectif de temps de récupération (RTO) est la durée et le niveau de service dans lesquels un processus ou un service doit être restauré après un sinistre. Un objectif de point de récupération (RPO) est la période maximale tolérable de perte de données en raison d'une interruption de service.

Les fonctionnalités de réponse aux incidents et de reprise après sinistre de Miro sont testées régulièrement, et suite à tout changement important apporté à l'entreprise ou à l'environnement.

Conformité, audit et certifications

Selon le rapport 2023 sur le cout d'une violation de données du Ponemon Institute, le non-respect des règlementations de sécurité est l'un des principaux facteurs contribuant aux compromissions. C'est pourquoi, chez Miro, nous prenons la conformité très au sérieux. Miro dispose d'un département de sécurité dédié, dirigé par un responsable de la sécurité de l'information, qui comprend plusieurs équipes chargées spécifiquement de la conformité et de la gouvernance. Le responsable de la confidentialité de Miro gère et supervise la confidentialité des données afin d'assurer la conformité avec les règlementations en vigueur. Un organisme d'audit interne indépendant est en place pour garantir une assurance et un examen objectifs de la gouvernance.

Comment Miro assure sa conformité

Miro est conforme aux exigences légales des régions spécifiques dans lesquelles il opère. Nos normes de sécurité et de confidentialité transparentes protègent les données de notre clientèle contre les accès non autorisés, les violations et les menaces.

L'audit et l'attestation de ces certifications et normes établies nous permettent d'évaluer notre conformité et l'efficacité opérationnelle des contrôles au cours de la période d'audit, comme dans les rapports d'assurance indépendants SOC 2 de type 2.

Il s'agit notamment :

- **de normes de sécurité de l'information** telles que SOC 2 de type 2 et ISO/CEI 27001 ;
- **de normes de transfert des données** appuyées par une solution de pointe de résidence des données dans l'UE, et par des clauses contractuelles types qui garantissent un niveau idéal de protection des données en dehors de l'UE et du Royaume-Uni, et assurent la conformité au Règlement général sur la protection des données (RGPD) ;
- **des certifications régionales et sectorielles** telles que la Cloud Security Alliance, le Cyber Essentials et TISAX ;
- **des audits récurrents par des tiers**, menés par des cabinets de premier plan comme le British Standard Institute (BSI) ;
- **des directives d'accessibilité** et un rapport de conformité en matière d'accessibilité (ACR) basé sur le VPAT.

Comment Miro protège les données personnelles de sa clientèle

Les lois et règlementations en matière de protection de la vie privée et des données, telles que le RGPD en Europe, sont devenues de plus en plus exigeantes, imposant un cadre strict pour la collecte, le traitement, le transfert et le stockage des données utilisateur. Le non-respect de ces règlementations risque d'entrainer de lourdes amendes, un contrôle règlementaire minutieux et la perte de confiance des clients, ce qui peut paralyser une entreprise SaaS.

Miro centre son programme de confidentialité et de protection des données sur les pratiques sectorielles établies, et met l'accent sur la protection des données personnelles en s'assurant que ses effectifs adoptent le comportement adéquat et que ses produits sont conçus de façon à répondre à ces exigences. Les membres du personnel sont tenus de se conformer aux normes de protection des données et de s'engager à respecter la confidentialité. En outre, ils sont soumis à des limitations techniques (voir Politique relative aux membres du personnel et accès). Chez Miro, les processus de conception des produits incluent des vérifications règlementaires et des examens juridiques. Les équipes produit et ingénierie reçoivent en outre une formation régulière sur les normes de conception.

La politique de confidentialité de Miro définit de manière explicite et transparente les catégories de données personnelles que Miro traite en tant que responsable du traitement, ainsi que l'objectif commercial établi. Elle décrit également les catégories de tiers auxquels nous faisons appel pour traiter les données personnelles, indique la manière dont les individus peuvent exercer leurs droits en vertu de la loi sur la protection des données, et mentionne le mécanisme de transfert de données sur lequel nous nous appuyons pour transférer des données personnelles en dehors de l'UE.

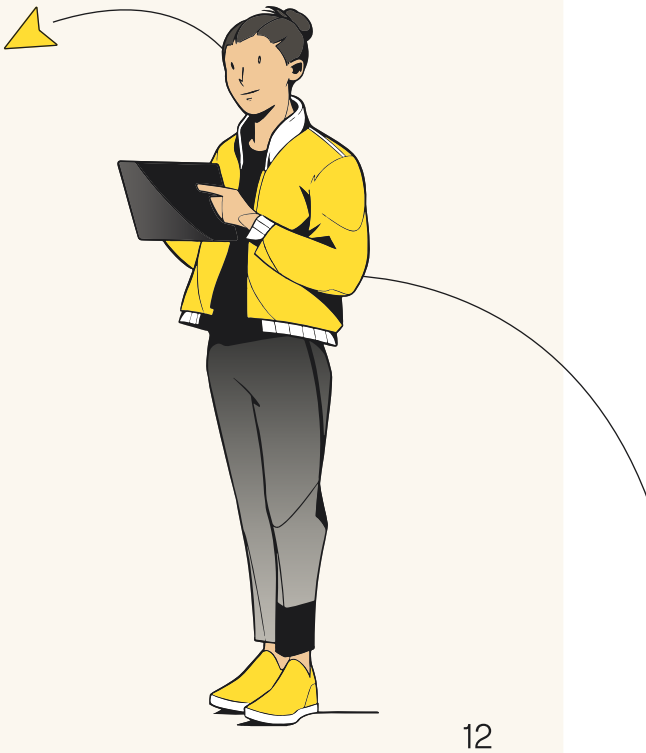
Lorsque nous traitons des données personnelles pour le compte de notre clientèle ou transférons des données personnelles de clients en dehors de l'UE, nous acceptons de respecter des conditions ad hoc, par exemple par le biais de notre addendum sur le traitement des données. Cet addendum inclut des engagements contractuels requis par le RGPD, le California Consumer Privacy Act (ainsi que sa modification par le biais du California Privacy Rights Act) et d'autres lois américaines et mondiales sur la confidentialité et la protection des données.

Traitement des données par des tiers

Lorsque Miro engage des tiers pour traiter les données personnelles de sa clientèle, nous appliquons un processus strict de recherche de fournisseurs qui comprend des contrôles juridiques et de sécurité, ainsi qu'un accord définissant clairement les conditions du traitement et du transfert des données. Miro fournit en ligne la liste de ces tiers via un lien figurant dans son addendum. En outre, nous informons notre clientèle dès lors que nous souhaitons modifier cette liste ou y ajouter d'autres tiers pertinents conformément au processus décrit dans l'addendum.

Sécurité des produits

En tant que plateforme basée sur le cloud, Miro est accessible à partir d'un navigateur Web sur PC et appareils mobiles, ou via une application dédiée à chacune de ces plateformes. En raison de ces points de contact et du fait que la collaboration sur une plateforme comme Miro s'effectue à distance et de façon distribuée, nous devons aider notre clientèle à adopter une architecture Zero Trust (ZTA). Autrement dit, non seulement nous donnons à notre clientèle les moyens de disposer des solutions de sécurité adéquates, mais nous nous assurons aussi qu'elles sont correctement déployées.



miro

Architecture Zero Trust

Contrairement aux modèles de sécurité traditionnels qui accordent un accès étendu en fonction de l'emplacement des utilisateurs ou du point d'entrée du réseau, la ZTA part du principe que les menaces peuvent provenir de n'importe où, même de l'intérieur de l'entreprise. La mise en place d'une telle architecture a acquis de plus en plus d'importance dans les environnements de travail modernes, où le personnel accède aux ressources de l'entreprise depuis des lieux et sur des appareils très variés. La ZTA préconise une vérification continue de l'identité, de la sécurité de l'appareil et du respect des politiques de sécurité tout au long de chaque interaction des utilisateurs avec les données et les ressources.

Miro aide les entreprises à aborder la ZTA en permettant aux admins de définir les politiques appropriées, accompagnées d'autorisations et de contrôles granulaires, sans pour autant compromettre la capacité des équipes à collaborer. Ces contrôles de sécurité comprennent :

- **L'authentification unique (SSO) :** avec l'authentification unique basée sur le protocole SAML, les utilisateurs peuvent accéder à Miro via le fournisseur d'identité de leur choix, par exemple Okta, Azure AD, AuthO, l'authentification unique Google et autres. Ils n'ont donc plus besoin de saisir leurs identifiants à chaque fois qu'ils se connectent à une application, ce qui leur fait gagner du temps tout en réduisant la surface d'attaque.

- **L'authentification à deux facteurs :** dans Miro, l'authentification à deux facteurs (2FA) fonctionne sans nécessiter le SSO. Elle offre en outre une strate de protection supplémentaire lorsque les utilisateurs accèdent à l'abonnement Miro de leur entreprise. La 2FA s'applique à tous les utilisateurs qui se connectent avec leur adresse e-mail et leur mot de passe (les collaborateurs externes pour les entreprises disposant du SSO ou tous les utilisateurs pour les entreprises qui ne l'ont pas configuré). Les utilisateurs peuvent paramétrer l'authentification à deux facteurs dans leur profil, ou les admins peuvent l'activer pour l'ensemble de l'entreprise. Miro applique l'authentification à deux facteurs en exigeant un mot de passe à usage unique basé sur le temps (TOTP), avec par exemple Microsoft Authenticator, Google Authenticator ou Authy.

- **Les délais d'inactivité :** cette fonctionnalité limite la durée pendant laquelle les utilisateurs peuvent rester inactifs avant d'être automatiquement déconnectés. Elle réduit le temps pendant lequel un acteur malveillant risque de profiter d'une session utilisateur existante (à distance ou en personne via un poste de travail laissé sans surveillance).

- **L'accès basé sur les rôles pour les admins :** plusieurs rôles d'admin peuvent être attribués aux utilisateurs pour exécuter des workflows (par exemple, admin d'entreprise, admin utilisateur, admin de contenu), chacun avec des niveaux spécifiques de privilèges d'accès, de paramètres et de configuration. Vous répartissez ainsi en toute sécurité la charge de travail d'administration tout en empêchant les admins de disposer de privilèges inutiles ou d'accéder à des informations sensibles.

- **Les stratégies de partage :** décidez quand et comment accéder au contenu de votre entreprise, en définissant des stratégies pour :
  - restreindre le partage en dehors des domaines autorisés ;
  - restreindre le partage via un lien public ;
  - exiger des mots de passe pour les tableaux publics (au niveau de l'entreprise) ;
  - restreindre le partage à l'échelle de l'équipe et de l'entreprise (au niveau de l'équipe) ;
  - restreindre la possibilité de déplacer des tableaux vers d'autres équipes (au niveau de l'équipe) ;
  - restreindre le partage de modèles client à l'échelle de l'entreprise.

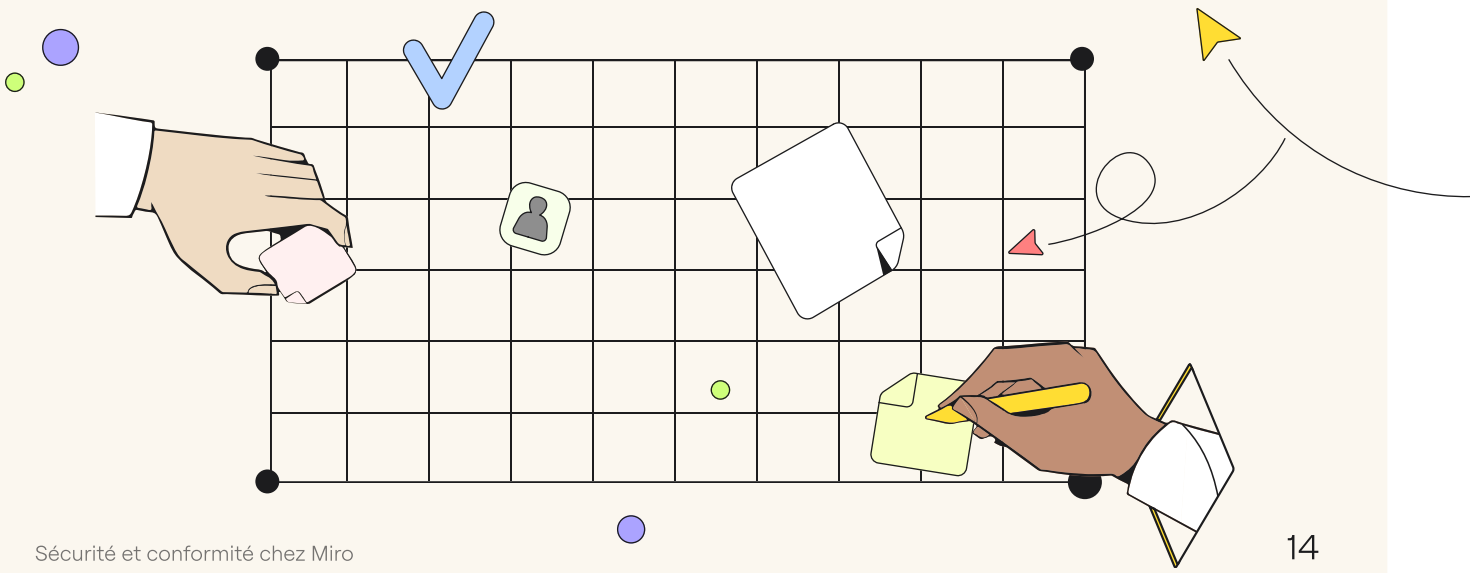
- **La gestion de la mobilité d'entreprise :** gérez en toute sécurité l'accès à Miro à partir d'appareils personnels ou professionnels grâce à l'intégration d'outils de gestion de la mobilité d'entreprise (EMM) telles que Microsoft Intune et VMware Workspace ONE, qui prennent en charge à la fois Android et iOS.

- **Les journaux d'audit :** les admins peuvent afficher toutes les activités qui se déroulent au sein de leur entreprise. Les journaux sont utiles en cas de dépannage ou lorsqu'un rapport détaillé des évènements importants est nécessaire, par exemple la modification des paramètres de sécurité globaux, l'invitation de nouveaux utilisateurs ou la création de nouveaux tableaux.

- **La classification :** les utilisateurs du forfait Enterprise peuvent attribuer des badges de classification au contenu de leur tableau pour indiquer son niveau de sensibilité. Les badges par défaut peuvent être configurés au niveau de l'entreprise ou de l'équipe, et les utilisateurs peuvent s'en servir pour filtrer les tableaux sur leur tableau de bord.

- **La gestion du cycle de vie du contenu :** Miro permet aux utilisateurs de filtrer par entreprise pour gérer efficacement le cycle de vie des tableaux au niveau de l'entreprise. De plus, une corbeille globale facilement accessible permet de restaurer les tableaux ou de les supprimer définitivement.

- **L'administration :** l'automatisation joue un rôle essentiel dans la prévention des erreurs, et permet de gagner du temps lorsque vous gérez des centaines de milliers de tableaux et d'utilisateurs. Le provisionnement SCIM ou JIT automatise l'accès des utilisateurs et rationalise la gestion du cycle de vie des utilisateurs.



Intelligence artificielle

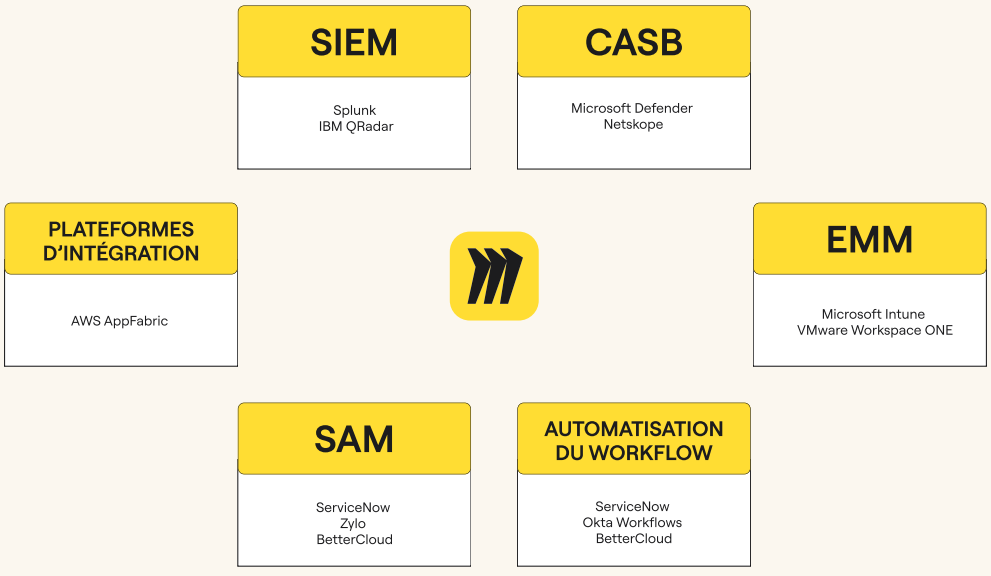
L'IA chez Miro est traitée avec le même soin et la même attention à la sécurité que l'ensemble du produit. Nos principes directeurs et nos pratiques témoignent de notre engagement en faveur d'un développement éthique et responsable de l'IA afin de maintenir la confiance des clients, des utilisateurs et des partenaires.

Ces pratiques et principes incluent la responsabilisation grâce à des modèles d'IA transparents. Nous utilisons les données uniquement comme indiqué dans notre politique de confidentialité, ou comme explicitement convenu entre Miro et sa clientèle. Vous gardez un contrôle total sur votre contenu. Vous avez par ailleurs le loisir d'accepter ou de refuser les services de l'IA. Pour en savoir plus, consultez notre livre blanc (en anglais).

Intégrations de l'écosystème Enterprise

Les bénéficiaires du forfait Enterprise tirent parti de diverses intégrations de sécurité et de conformité, notamment des systèmes de gestion des informations et des évènements de sécurité (SIEM), des brokers de sécurité d'accès au cloud (CASB), des solutions EMM, des plateformes d'intégration, des outils de gestion des actifs logiciels (SAM) et de l'automatisation des workflows. Les entreprises peuvent également développer leurs propres intégrations personnalisées.

Intégrations de niveau entreprise



miro | ENTERPRISE GUARD

Miro Enterprise Guard : module complémentaire avancé de sécurité et de gouvernance des données

Le travail effectué dans Miro est souvent stratégique et nécessite une gouvernance. Notre clientèle utilise de plus en plus Miro pour créer et stocker des données confidentielles et propriétaires, et les données sensibles peuvent apparaitre là où on s'y attend le moins, malgré les politiques de l'entreprise. De plus, la quantité de contenu dans les tableaux Miro augmente, chez nos plus grands clients, à un taux de 2,5 fois par an, ce qui augmente encore la surface de risque pour la sécurité et la gouvernance des données.

Les principales fonctionnalités professionnelles de sécurité des applications SaaS, telles que l'authentification et l'authentification unique, ainsi que les contrôles d'accès granulaires, donnent à la plupart des clients suffisamment de contrôle sur le moment et la manière de protéger leurs données. Mais certains clients souhaitent un niveau de protection plus élevé en sus de nos mesures de sécurité standards, en raison de l'importance stratégique de Miro pour leurentreprise ou des exigences de conformité règlementaire de leur secteur, ou une combinaison des deux.

C'est là qu'intervient Miro Enterprise Guard, un module complémentaire avancé de sécurité et de gouvernance des données.

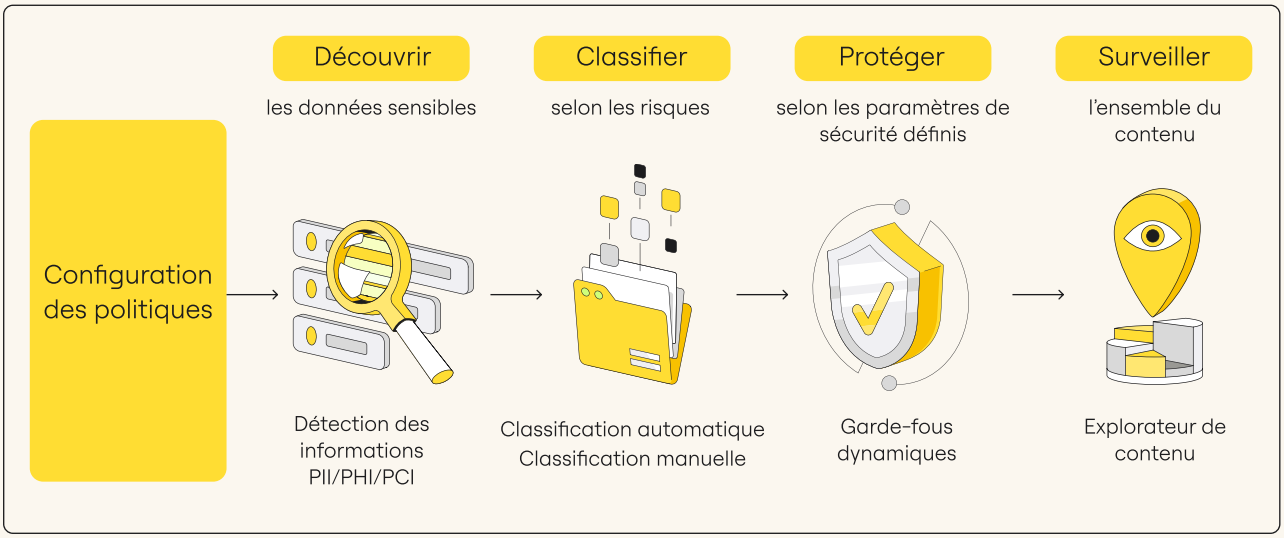
[1] Croissance cumulée des tableaux dans les entreprises de plus de 1 000 entreprises entre 2017 et 2023

Recherche, classification et sécurisation des données sensibles

Enterprise Guard automatise le processus de recherche et de classification des données sensibles dans Miro et offre des contrôles de sécurité accrus. Enterprise Guard :

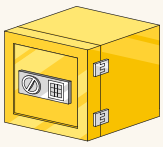
- analyse vos tableaux Miro, en **identifiant et classifiant les données sensibles** telles que les informations personnellement identifiables (PII), les informations relatives aux cartes de paiement (PCI), les informations médicales protégées (PHI) et les informations critiques pour l'entreprise pour vous permettre de les gérer, les supprimer ou les corriger ;
- applique **automatiquement des badges de classification** aux informations trouvées, en fonction de critères prédéfinis que vous pouvez paramétrer dans Miro ou dans d'autres outils de sécurité intégrés ;
- applique **des garde-fous intelligents** en fonction du badge de classification de chaque tableau. Les garde-fous intelligents sont des contrôles dynamiques que vous définissez en fonction de votre stratégie et qui peuvent empêcher certaines actions des utilisateurs, telles que le copier-coller, le partage public et l'exportation de tableaux ;
- **l'explorateur de contenu** vous fournit une vue unifiée de tous les tableaux Miro comportant du contenu sensible et leurs badges de classification. Vous bénéficiez d'une visibilité accrue sur les éléments à protéger et des contrôles de précision pour y parvenir, tout en favorisant la collaboration dans votre entreprise.

Adapter la sécurité au risque

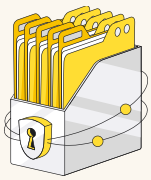


Gestion du cycle de vie du contenu à grande échelle

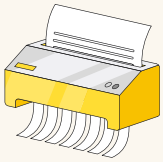
Enterprise Guard automatise le processus de gestion du cycle de vie de vos tableaux pour vous aider à répondre à vos exigences de conformité ou de politique organisationnelle. Grâce à ces fonctionnalités, vous pouvez :



Conserver des tableaux conformément à la politique avec une piste d'audit complète



Supprimer des tableaux conformément à la politique avec restauration d'une piste d'audit complète



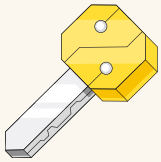
Définir une stratégie de mise à la corbeille au niveau de l'entreprise pour mieux contrôler la suppression et la conservation permanentes de vos tableaux Miro

Gestion des clés

Le module complémentaire Enterprise Guard inclut par ailleurs la possibilité d'opter pour la gestion des clés de chiffrement. Cette option vous donne un contrôle complet et indépendant sur vos clés de chiffrement via le service AWS KMS.

Vous disposez aussi d'une meilleure visibilité des audits et d'un contrôle d'accès accru sur les données telles que les noms de compte, les noms de projet et le contenu généré par les utilisateurs, y compris les widgets, les commentaires et les fichiers chargés.

De plus, quand les clients ajoutent leurs propres clés (chiffrement BYOK, ou Bring Your Own Key), ils peuvent en vérifier l'utilisation dans les journaux des appels API passés sur ces clés. Ils respectent donc les exigences de conformité et règlementaires.



Gestion des clés de chiffrement

Conclusion

La plupart des responsables ne sont pas satisfaits de la capacité de leur entreprise à innover et à rester compétitive. En réalité, pour 82 % des responsables, une entreprise disparaitra sous cinq ans si elle ne réussit pas à innover. Les défis technologiques tels que les outils hérités et obsolètes comptent parmi les plus grands obstacles à l'innovation. Les responsables et les spécialistes de l'information s'accordent à dire que les technologies traditionnelles étouffent la créativité et entravent la productivité. C'est pourquoi de nombreuses entreprises se sont empressées de mettre en œuvre des outils de collaboration sans tenir pleinement compte des implications en matière de sécurité.

Avec un espace de travail visuel collaboratif comme Miro, l'innovation est facilitée et sécurisée. Parce que nous nous engageons à protéger la sécurité et les données de notre clientèle, plus de 60 millions de personnes dans le monde, dont 99 % des entreprises Fortune 100, font confiance à Miro pour ce qu'elles ont de plus cher : leurs informations. Rejoignez ces entreprises de premier plan et profitez d'un espace de travail collaboratif et innovant, avec la certitude que vos données sont sures et protégées.

Contactez notre équipe de vente pour en savoir plus.

Resources

Miro Trust Center
Livre blanc sur le chiffrement
Résidence des données chez Miro
FAQ sur la sécurité et la conformité de Miro (Centre d'assistance)
Rapport de transparence annuel
Politique de confidentialité
Conditions d'utilisation
Miro Enterprise
Directives d'accessibilité

Miro est un espace de travail visuel qui permet aux équipes distribuées de toutes les tailles de donner vie à la prochaine innovation majeure. La toile infinie de la plateforme permet aux équipes de mener des réunions et des ateliers dynamiques, de concevoir des produits, de réfléchir à des idées et bien plus encore. Miro, une société basée à San Francisco et à Amsterdam, sert plus de 60 millions de personnes de par le monde, dont 99 % des entreprises Fortune 100. Miro a été fondé en 2011 et compte actuellement un effectif de plus de 1 800 personnes sur 12 sites, partout dans le monde.

miro

Pour en savoir plus, rendez-vous sur miro.com/fr.

Forfait Miro Enterprise
https://miro.com/fr/enterprise/

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

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

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