monday.com

Security and Privacy white paper

Date	Version	Description of change
November 2021	1.0	Final version
January 2022	1.1	Periodical review and revisions
July 2022	1.2	Minor revisions
August 2022	1.3	Minor revisions
November 2022	1.4	Minor revisions
Jan 2023	1.5	Periodical review and revisions
Jan 2023	1.6	Minor update
Dec 2023	1.7	Periodical review and revisions
Jan 2024	1.8	WorkCanvas Update
August 2024	1.9	Periodic update and Privacy update
January 2025	2.0	Periodical review and revisions
April 2025	2.1	Minor revisions
October 2025	2.2	Periodical review and revisions
June 2026	2.3	Minor revisions

Table of contents

This white paper is intended to provide an overview of monday.com's security and privacy practices in existence on the date of publication of this white paper, which are subject to change without notice. Any description of future plans is subject to change or delay at monday.com's sole discretion. This white paper is for information purposes only and does not constitute legal advice or be perceived as supplementing or being incorporated into any terms and conditions in any contractual agreements.

1. Introduction

monday.com Work OS includes the product suite of Work Management, CRM and Dev. On these applications, monday.com manages the data of over 250,000 companies around the world, and with this responsibility, we are committed to providing our customers with the highest standards of security and data protection. We earn the trust of our customers by making data security our top priority. monday.com security and privacy programs are developed according to several industry-standard compliance standards to achieve the highest level of data protection. This includes an annual SOC 2 type II audit which demonstrates our commitment to meeting the most rigorous security, availability, and confidentiality standards in the industry. As well as ISO certifications such as ISO 27001, the most rigorous global security standard for Information Security Management Systems (ISMS). Please see section 7 of this document for more information.

monday.com follows strict international standards and regulations in order to keep your data safe, see our Compliance Hub for a full overview of all relevant policies, certifications, diagrams and documentation to review our security posture.

Disclaimer

Please note that some of the representations and functionalities described in this White Paper may not be available or applicable to WorkCanvas. For an overview of the main differences relevant to WorkCanvas please see section 8. For additional information on WorkCanvas please refer to its dedicated documentation or contact our support team at support@monday.com

Our mission statement

To give our customers peace of mind while managing their data on monday.com Work OS by providing an industry leading trustworthy service.

Our teams

monday.com's information security efforts are guided and monitored by our CISO, dedicated 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 our Privacy Forum, which is composed of representatives from the Legal, Privacy, and Security Teams, and led by our Data Protection Officer (DPO).

Useful Links

monday.com Trust Center
monday.com Legal portal
monday.com's Status page
monday.com's Compliance Hub
Sub-Processors, subsidiaries, and support
Security and Privacy at monday.com - FAQ
Report vulnerabilities

Support and Knowledge Base
Pricing and plans
monday.Engineering Blog
AI FAQ
Platform API

---

2. Infrastructure security

Hosting providers

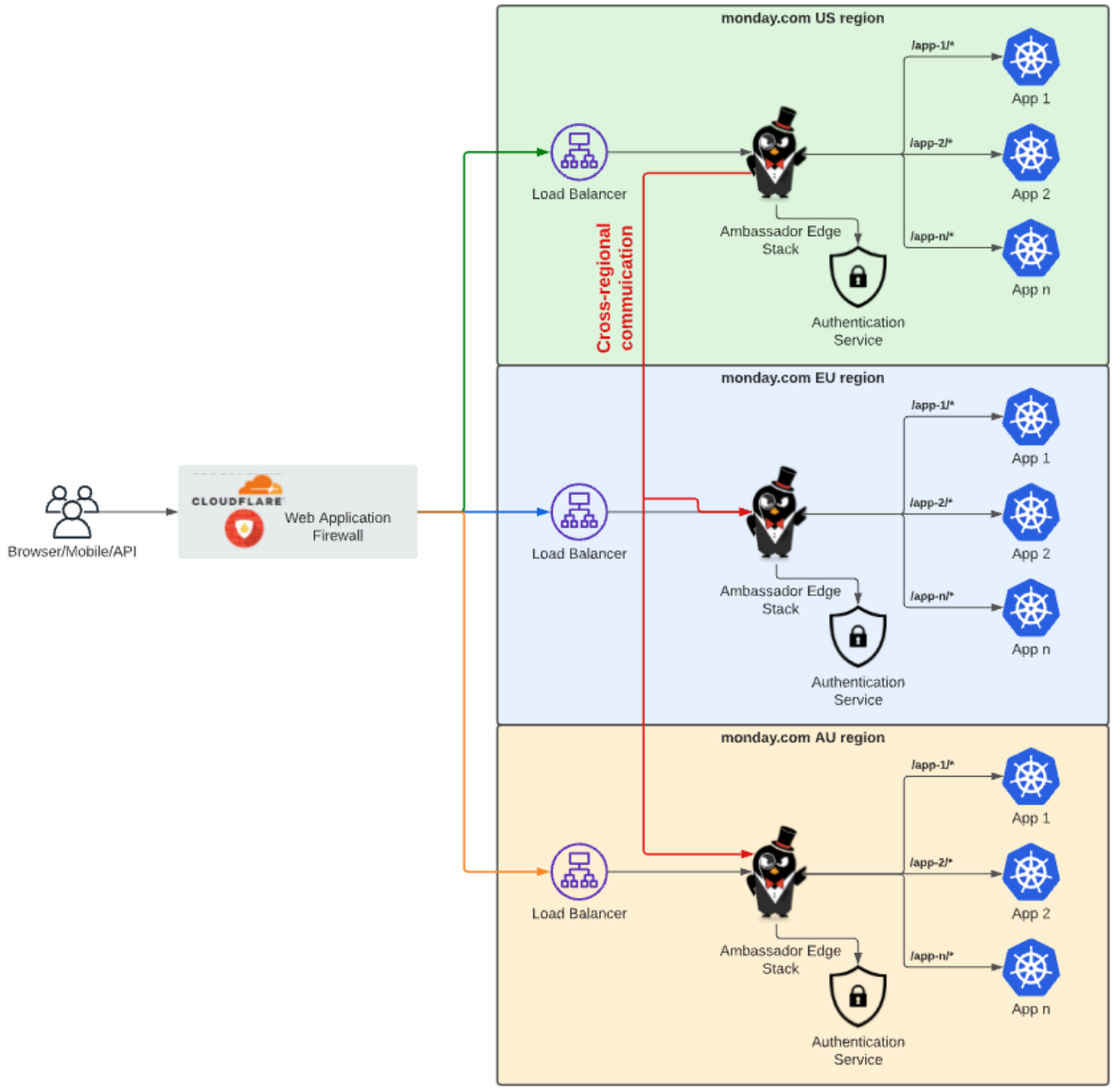
To achieve high availability and resiliency, our service is hosted on Amazon Web Services (AWS) which is a best in class secure infrastructure, hosted in multiple regions, monday.com data may be hosted in the US Data Region, the EU Data Region, or the APAC Data Region. Data is hosted across several Availability Zones, with dedicated disaster recovery (DR) deployments established in different regions. Customer accounts are bound to a single region. For more information on AWS security, please visit https://aws.amazon.com/security

In the AWS Shared Responsibility Model, AWS manages the cloud computing infrastructure, while monday.com manages the security of the software and data residing on the cloud computing infrastructure.

Network architecture

- monday.com's network architecture is built according to AWS best practices, including separating public and private subnets.
- monday.com uses industry leading Content Delivery Network (CDN) providers to prevent DDoS attacks and brute-force attacks. Rate limiting is configured at both the edge and at the application level.
- Load balancers reside in the public subnet and are accessible through our CDN ip ranges only, while internal network components such as the web application servers and databases reside in the private subnet, and have no public IPs assigned to them.
- A Web Application Firewall (WAF) is in place for content-based dynamic attack blocking.
- Firewalls are used throughout the network to enforce IP whitelisting and access through permitted ports only to network resources. Security Groups rules are configured to allow access only from required ports.
- Network Intrusion Detection System (NIDS) sensors are used in tandem with native AWS security services which are enabled for all production assets.

The following represents the highlights of the monday.com's network diagram, both in the US data region, the EU data region and APAC data Region:[1]



Infrastructure-as-Code is used extensively to ensure that configuration changes are tracked and audited. monday.com's Infrastructure Team conducts a thorough review of the perimeter network configuration on a quarterly basis and makes any changes deemed necessary to maintain or increase security.

[1] A high-level grid network diagram is available at https://trust.monday.com/.

AWS Advanced Technology Partner

monday.com is an AWS Advanced Technology Partner, which attests that AWS itself has rigorously vetted our organization in terms of infrastructure, information security, best-practice design, and more.

Network Security

As monday.com is a purely cloud-based solution, we have the advantage of using modern, cloud-oriented controls to get an accurate view of our network perimeter. We collect and monitor network logs using a NIDS and traffic logs from edge locations, and review relevant alarms through our Security Information and Event Management (SIEM) system. We use security monitoring tools which frequently retrieve our Security Groups and Network Access Control Lists (NACLs) configuration from the cloud provider, and construct a full overview of our network.

monday.com's Infrastructure Team conducts a thorough review of the perimeter network configuration on a quarterly basis and makes any changes deemed necessary to maintain or increase security. Access to production

Access to production assets is granted based on role and in accordance with the need-to-know and least privileges principles. Administrative privileges are provided only to our R&D or Infrastructure Team personnel (a small and limited team of adept engineers) through Just In Time Access (JIT) and Just enough, which needs to be approved by a system admin, each time access is requested and minimal permissions for what is required for specific resources. All access to the monday.com servers requires the use of our Virtual Private Network (VPN), which is authenticated against our Enterprise Identity Provider (IdP), fully audited, and enforces password strength and Multi-Factor Authentication (MFA).

Access to production clusters by our developers is done using an infrastructure privileged access management tool.

Hardening

Servers are hardened in alignment with CIS (Center for Internet Security) standards.

EKS clusters use AWS Bottlerocket AMIs, which are Linux based, open source operating systems which includes only essential software that requires running containers while ensuring that the underlying software is always secured.

Databases

Databases used by monday.com include MySQL, Elasticsearch, Redis, Postgres, Cassandra and Dynamodb.

File storage

File storage is hosted on Simple Storage Service (S3) by AWS, which stores attachments and database backups stored in snapshots. Attachments contain any files uploaded by a customer to the monday.com service.

In addition, we have a blacklist containing a list of forbidden file extensions. The file extension blacklist contains file types that may be considered dangerous, such as executables.. By blocking these file types (including checking for MIME types which attempt to bypass the name check) we reduce the risk of malware infection significantly.
For more information on accepted file types, please see this support article.

Multi-region

Due to the identical infrastructure principles in the US region, monday.com customers in the EU and APAC can enjoy the monday.com experience with the same level of security measures and controls, and with confidence that the CIA triad (Confidentiality, Integrity, and Availability) principles are observed.
Highlights of the monday.com network diagram are depicted above.

Encryption and key management

Encryption in transit

Data in transit across open networks is encrypted using TLS 1.3 (at minimum, TLS 1.2).

Encryption at rest

Data at rest is encrypted using AES-256. Encryption keys are stored using AWS Key Management Service (KMS). An annually rotated customer master key (CMK) is currently used to encrypt all customer data submitted to the monday.com service and processed on their behalf.
We also offer Bring Your Own Key (BYOK) and Tenant Level Encryption (TLE) as part of our Guardian add-on, see https://support.monday.com/hc/en-us/articles/25276756886674-Guardian-add-on to learn more

Tenant separation

Our environment is multi-tenant with logical separation between customers. Customer data is segregated at the application level using unique IDs that are the result of a combination of several parameters.

Backup

monday.com is responsible for backing up its customers' data. Our solution is continuously monitored by a managed SOC team. We continuously backup user data and full backups are performed daily, they can be restored in 24 hours.
In addition, we distribute the encrypted backups across multiple AWS Availability Zones, they are retained for 25 days in the same region and 7 days remote. All data at rest, including backups, are encrypted using AES-256. We have also established a DR site in a separate AWS region. Backups and restoration procedures are tested at least annually.

Scalability and reliability

Microservices architecture is utilized to ensure minimal impact on system health in the case of failure of one or more components. The monday.com service is fully containerized, with Kubernetes used for orchestration; this provides for highly scalable infrastructure, suitable for dealing with increasing customer demand while providing a quality experience for end-users.

Infrastructure-as-code is widely used via Terraform to facilitate resource provisioning and maintainability of infrastructure resources.

monday.com continuously monitors performance metrics for all of its infrastructure components and builds its infrastructure for scale. Furthermore, we hold quarterly scale reviews with both infrastructure engineers and management to ensure that our roadmap provides quality service to an ever-growing number of customers and product features.

Service-level agreement (SLA)

Our service's availability can be monitored through our Status Page. System downtime for maintenance is seldom required. When necessary and as practicable, it is scheduled during weekends, on low-activity hours.

Notifications regarding downtime are available immediately through the Status Page, where customers may subscribe to notifications regarding availability and our team's mitigation efforts via email or text message.

Enterprise Plan customers receive 99.9% uptime commitment.

---

3. Security features and functionality

Authentication
monday.com supports the following authentication methods:

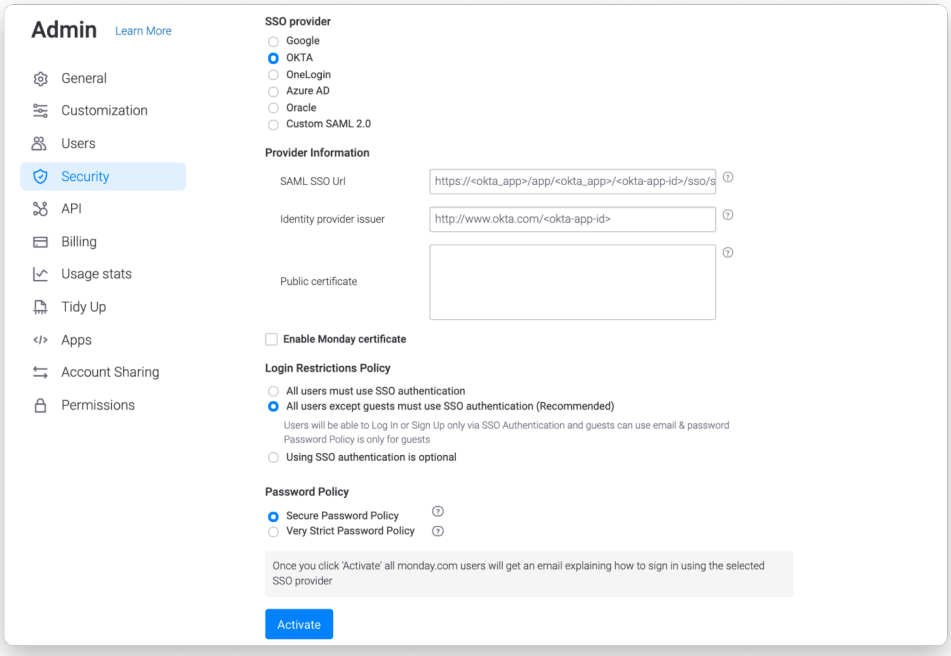
Credentials
If you choose to authenticate your account users using credentials, we provide administrators with a choice of two passwords strength settings for their accounts:

1. 8 characters minimum with no repeating or consecutive characters allowed, or
2. 8 characters minimum with no repeating or consecutive characters allowed and an inclusion of at least one digit (1, 2, 3), one lowercase letter (a, b, c), and one uppercase letter (A, B, C).

Identity provider (IdP)
monday.com currently supports five main identity providers:

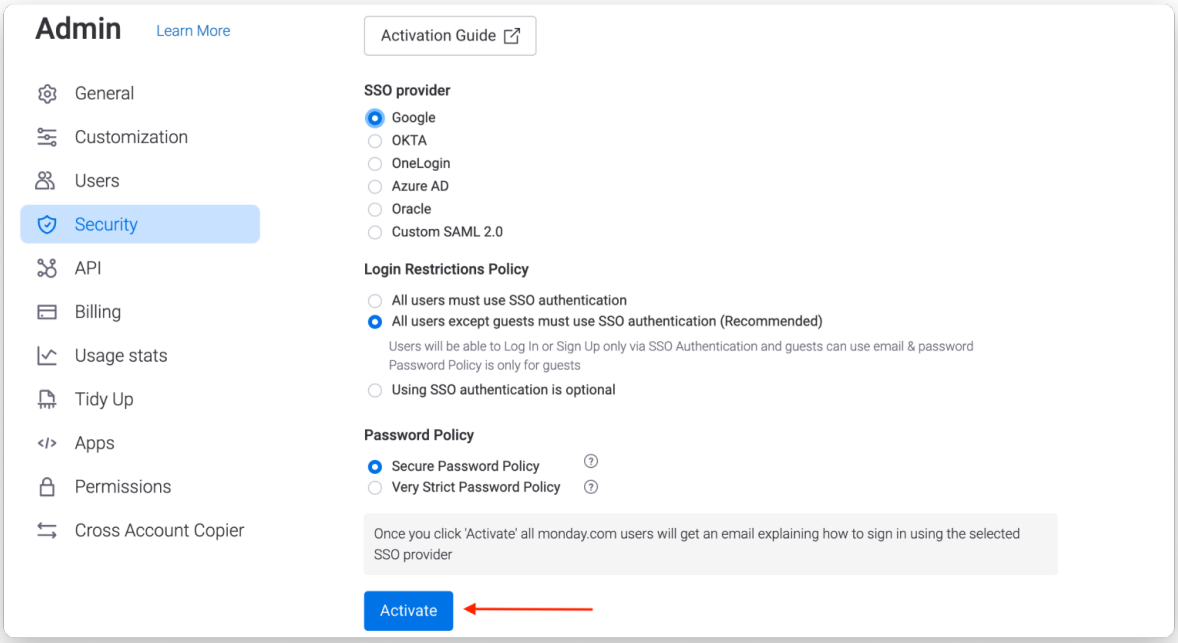
1. Google
2. OKTA
3. Entra ID (previously known as Azure AD)
4. OneLogin
5. Oracle

Furthermore, customers have the option to use their own provider using Custom Security Assertion Markup Language (SAML 2.0).
Please note: This feature is only available for Enterprise Plan customers.



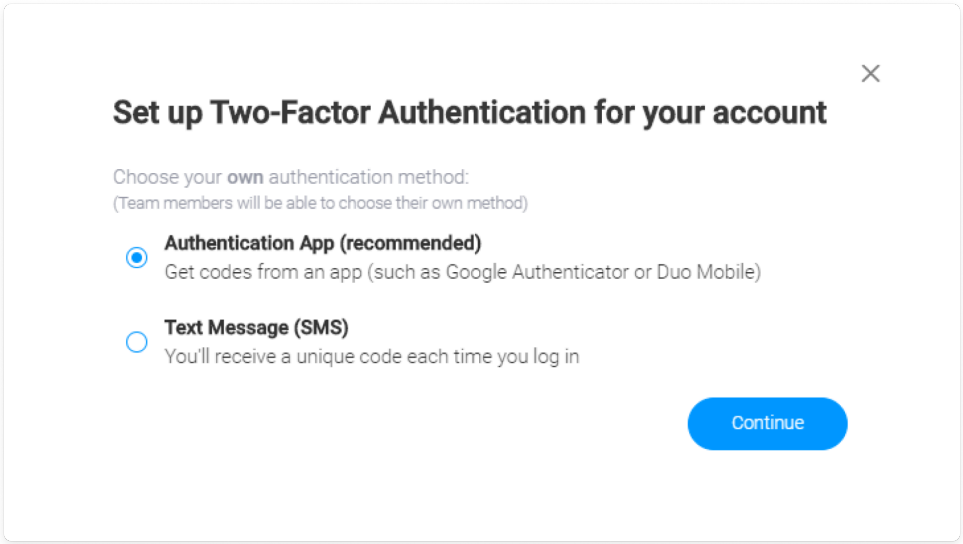
Google single sign-on (SSO)

Google SSO is a secure authentication system that reduces the burden of remembering multiple passwords by enabling users to sign in to the monday.com service using their Google account.
Please note: This feature is available for Pro and Enterprise plans only.



Two-factor authentication (2FA)

In addition to the above authentication methods, admin(s) can configure an extra layer of security and enable 2FA via a text message (SMS) or through an authenticator app.
Please note that if you choose to integrate with your IdP, 2FA must be enabled on your end.



Authorization

SCIM provisioning

System for Cross-domain Identity Management (SCIM) is a protocol for user management across multiple applications, which allows you to easily provision (add), de-provision (deactivate), and update user and team data across multiple applications at once. monday.com supports three ways to set up SCIM provisioning:

1. Existing monday.com SCIM applications:
    a. OKTA
    b. Entra ID (previously known as Azure AD)
    c. OneLogin
2. Custom SCIM integration with your choice of identity providers
3. SCIM provisioning using API

The following table presents all **user** attributes supported in monday.com's SCIM integration:

monday.com attribute	SCIM API attribute(s)	Description
Name (required)	name, displayName	The user's display name.
Email Address (required)	userName, email	The email address used by the user to log into the monday.com service.
Active (required)	active	When creating a user, this field must be set to 'true'. Changing a user's 'active' value to 'false' will deactivate them in the monday.com service.
Position	title	The user's position in the organization.
Timezone	timezone	The user's timezone (all dates in the platform will be according to this timezone).
Locale	locale	monday.com will display a localized version for different locales.
Phone Number	phoneNumbers	The user's phone numbers (only the one marked as 'primary' will be displayed).
Home Address	addresses	The user's address (only the one marked as 'primary' will be displayed).
User Type	userType	The level of each user within the account. The possible values are: admin, member, viewer, or guest or account customer role (the default value is "member").

The following table presents all **team** attributes supported in monday.com's SCIM integration:

monday.com attribute	SCIM API attribute(s)	Description
Name (required)	displayName	The team's displayed name.
Users	members	List of users assigned to the team.

Please note: This feature is only available for Enterprise Plan customers.

Permissions

monday.com helps you control who can do what on your account. We offer several types of permissions for you to customize to restrict the viewing or editing of data, including:

1. **Board permissions**
    a. Types: “Main,” “Shareable,” and “Private” boards
    b. Restrictions: “Edit everything,” “Edit content,” "Edit by assignee," "View by assignee" and “View only”
2. **Column permissions**: “Restrict column edit” and “Restrict column view”
3. **Dashboard permissions**
    a. Types: “Main” and “Private” dashboards
    b. Restrictions: only dashboard owners are able to edit the dashboard, as well as the apps and widgets within it
4. **Workspace permissions**
    a. Types: “Open” and “Closed” workspaces
    b. Restrictions: “No one,” “Only admin,” “Workspace owners,” and “Anyone”
    c. WS owners can set restrictions on the following features per the Workspace role:
        i. Create main boards
        ii. Create private boards
        iii. Create shareable boards
        iv. Create Main docs
        v. Create Private Docs
        vi. Create Shareable Docs
        vii. Create integrations/ automations
        viii. Delete self created items
        ix. Delete items created by others
        x. Move groups/items between boards
        xi. Board owners can mute board notifications for all users
5. **Account permissions:** admins can set restrictions (admin, team member, member, viewer, subscriber, board owner, guest and custom roles) on the following features:
    a. Create main boards
    b. Create private boards
    c. Create shareable boards
    d. Broadcast Boards on the web using public link
    e. Export data to excel
    f. Delete self created items
    g. Delete items created by others
    h. Move groups/items between boards
    i. Create main dashboards
    j. Create Main docs
    k. Create Private Docs
    l. Create Shareable Docs
    m. Broadcast docs on the web using public link
    n. Upload files across the system
    o. Create workspaces
    p. @mention or subscribe all users on the account to an update or board
    q. Generate API tokens
    r. Create Automations / Integrations

s. Create Integrations
t. Create teams
u. Delete teams
v. Edit team name and image
w. Add/remove members from teams
x. View the teams page and teams card
y. Upload Profile Picture
z. Board Owners can mute board notifications for all users.
aa. Create board views
bb. Delete self-created views
cc. Delete views created by other users
dd. Create docs on items
ee. Delete files
ff. Create private dashboard v2
gg. Invite users from non-authorized domains
hh. Invite guests
ii. View automation usage page
jj. Assign users to schedules
kk. Edit self-owned item updates and doc comments
ll. Delete self-owned item updates and doc comments
mm. Access the User management section
nn. Access the Security section
oo. Access the Billing section
pp. Access the Content Directory section
qq. Access the Apps section

Please note that some of the above features may not be available on all plans.

Roles within monday.com

For a full overview of roles within monday.com please see here.
The following are the main roles within the platform:

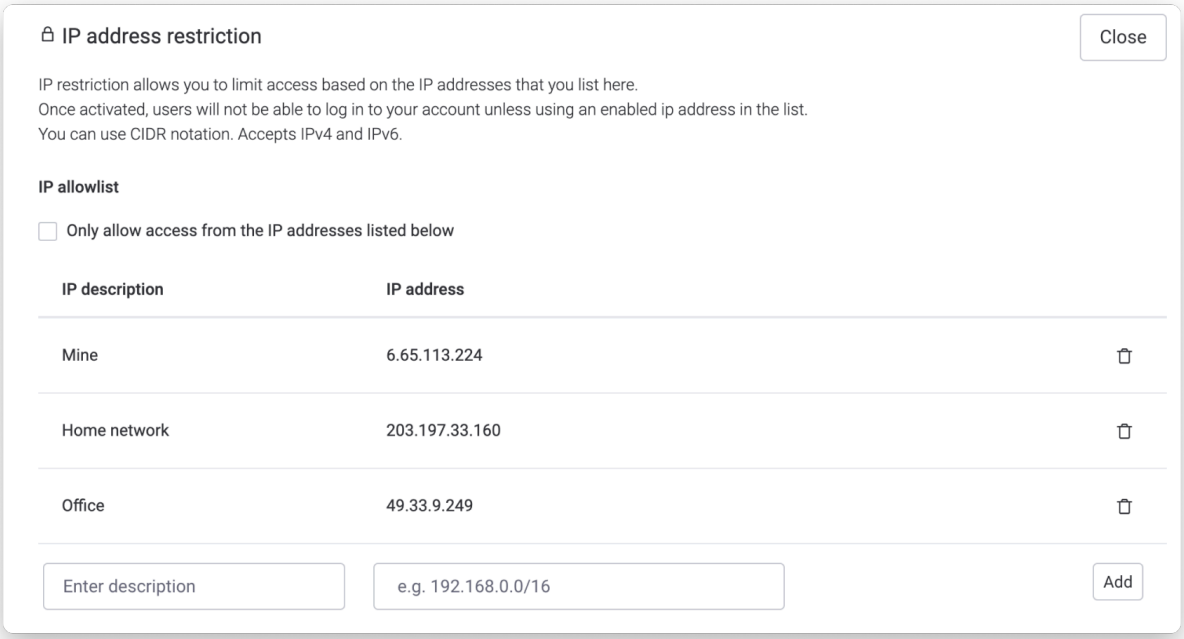
Role	Description	Can	Cannot
Administrator	A team member (or more if you choose) who manages its team	• Oversee the entire account • Manage everything, from users and boards to security and billing (as described in the "Admin Panel" section below)	
Member	Has editing access (The number of members you can invite depends on your plan)	• Create and edit boards, items and folders • Invite other members inside a board and item • View all main boards • Be invited to shareable or private boards • Edit their profile	• Access the User Management section • Access the Security section • Access the Billing section • Access the Content Directory section

		• Communicate and add attachments	
Viewer	Only able to view boards, with no editing rights whatsoever (You can invite an unlimited number of viewers regardless of the plan you have purchased)	• Optional: Export Data to Excel • View the Teams page and team cards • Optional: upload profile picture	• Create main boards • Create private boards • Create shareable boards • Broadcast boards • Delete Self Created Items • Delete Items created by others • Move groups / items between boards • Create main dashboards • Create main docs • Create Private docs • Broadcast docs • Upload files across the system • Create workspaces • @Mention/Subscribe everyone in the account • Generate API tokens • Create automations / integrations • Create integrations • Create team • Delete team • Edit team name and image • Add / Remove members from teams • Board owners can mute board notification to all users • Access the User Management section • Access the Security section • Access the Billing section • Access the Content Directory section
Guest	External to your organization, such as a vendor, client, freelancer or outside consultant	• Export Data to Excel • Delete Self Created Items • Delete Items created by others • Move groups / items between boards • Upload files across the system • Create automations / integrations • Create integrations	• Create main boards • Create private boards • Create shareable boards • Broadcast boards • Create main dashboards • Create main docs • Create Private docs • Broadcast docs • Create workspaces • @Mention/Subscribe everyone in the account • Generate API tokens

		• View the teams page and team cards • Upload profile picture	• • Create team • Delete team • Edit team name and image • Add / Remove members from teams • Board owners can mute board notification to all users • Access the User Management section • Access the Security section • Access the Billing section • Access the Content Directory section
Custom Roles (For Enterprise customers)	In addition, Enterprise admins can create unique, account-level roles and assign specific permissions for that role. This feature was built with the goal of simplifying effective governance of an account, while giving the proper amount of freedom to employees within their domain.	For more information please see here.	

IP address restrictions

Admin(s) have the ability to pre-define a set of allowed IP addresses which will be able to access your account. This allows you to restrict account access to users in specific contexts, like those joining from a specific location (i.e. from the office) or using a certain VPN. Any user attempting to log in with an IP address that does not match an address on the allowed list will receive an error message and will not be able to proceed.
Please note: This feature is only available for Enterprise Plan customers.



Tenant Level Restrictions

Tenant-Level Restrictions allows an organization to restrict access only to specific monday.com accounts from their network. In the Tenant-Level Restrictions feature, network administrators for an organization can specify which monday.com accounts can be accessed through that network - and attempts to access any other account while on that network would be blocked.

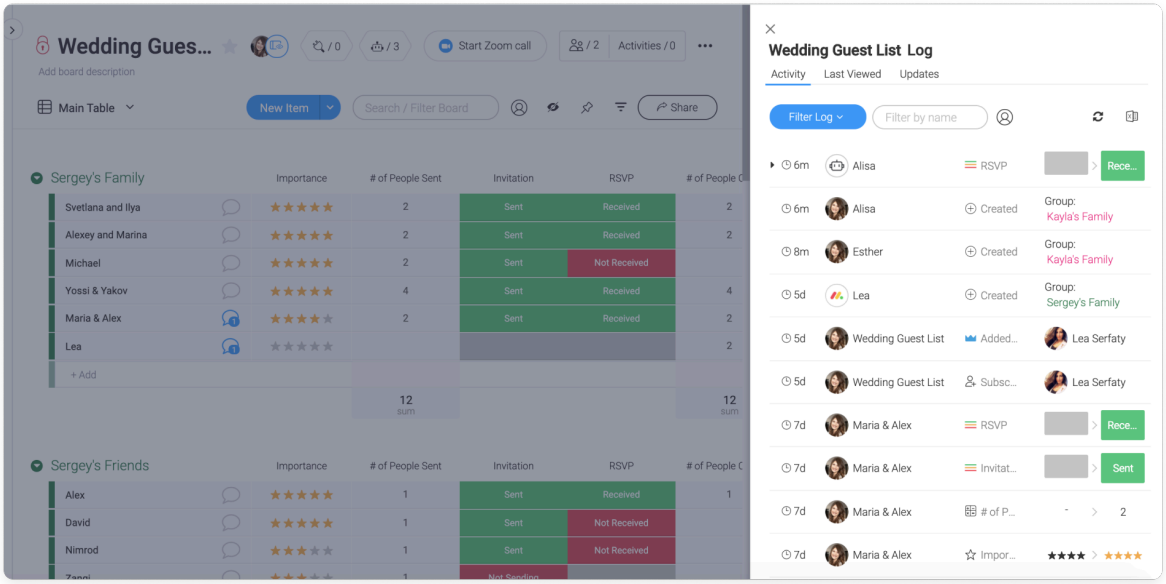
Tenant-Level Restrictions can work as a complementary feature for an account's IP restrictions: for example, given an organization with a monday.com account, the account admins can allow access to it only from specific IP ranges. Then, through tenant-level restrictions, network administrators belonging to that organization can ensure that no other monday.com account be accessed from that IP range - thus guaranteeing that sensitive information can only be accessed in one way, and cannot be easily moved to other monday.com accounts.

Logs

Activity Log

There are two types of Activity Logs:

1. **The Board Activity Log** shows all of a board's past activity in one list, including changed dates, statuses, movement between groups, automations, and permissions. The information displayed on the Board Activity Log varies according to your tier: the Basic Plan holds the activity from the past week only; the Standard Plan holds activity data for 6 months; while the Pro plans hold it for 1 year, and Enterprise plans hold it 5 years.



2. **The Item Activity Log** tracks all updates made to an individual item. In the Item Activity Log you can see a full history of that item's updates and exactly when they occurred. All of the updates are organized from newest to oldest. You can set an Alert Reminder on any update.

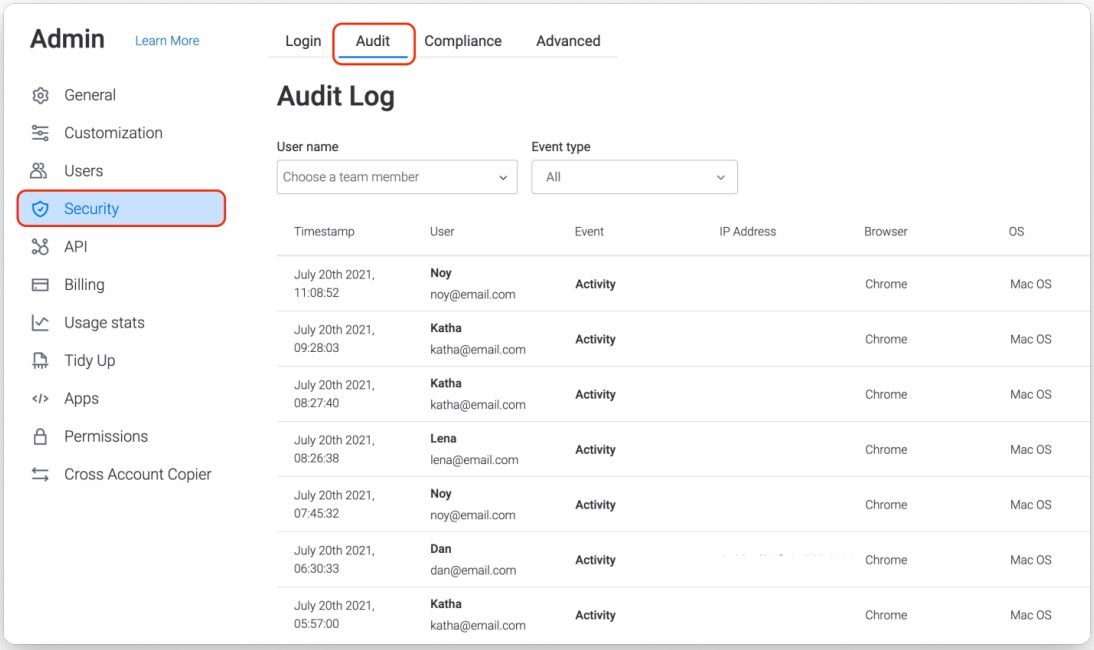
You can easily export your Item Activity Log or Board Activity Log to Excel in the click of a button.

Audit Log

The Audit Log provides account admin(s) a detailed report of all account security-related activity. In this section, you can see when users last logged in and out of the account, from which device, and their IP address for the session. This way, you can monitor any suspicious activities and activate the Panic Mode if needed.

The log also displays potentially vulnerable events such as failed logins, downloaded attachments, and exported board data. Please note: This feature is only available for Enterprise Plan customers.

The Audit log records are accessible also by an API, or as an add-on for Splunk SIEM. Please note: This feature is only available for Enterprise Plan customers.



Interoperability and portability

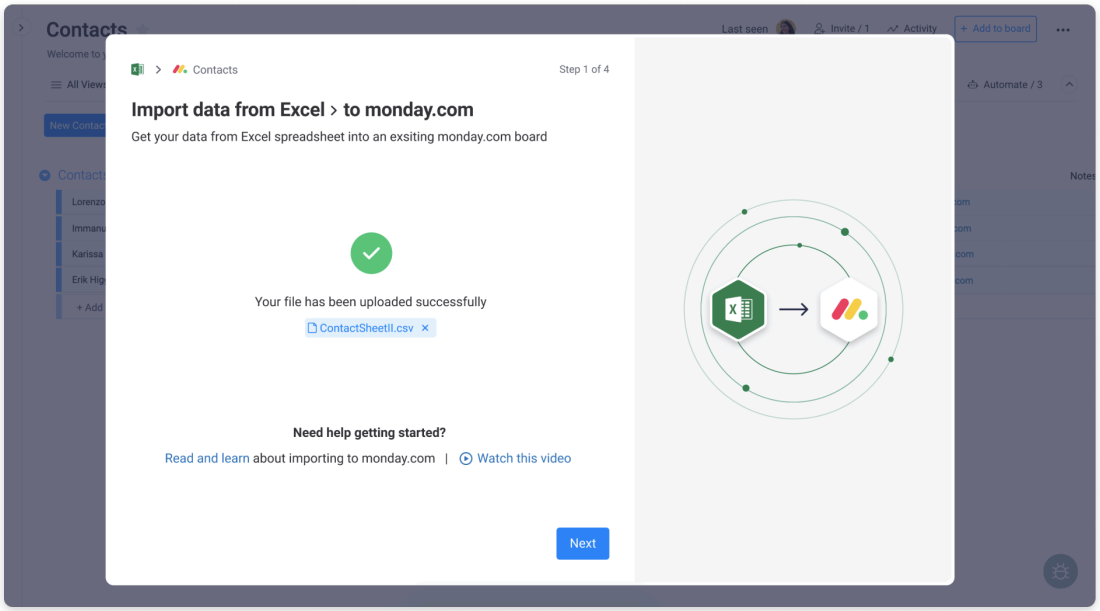
Integrations

monday.com supports integrations with various other software solutions to create customized workflows. You can connect monday.com with the tools you already use to manage all your team's work in one place.
Integrations are optional and can be disabled through the Admin Panel.

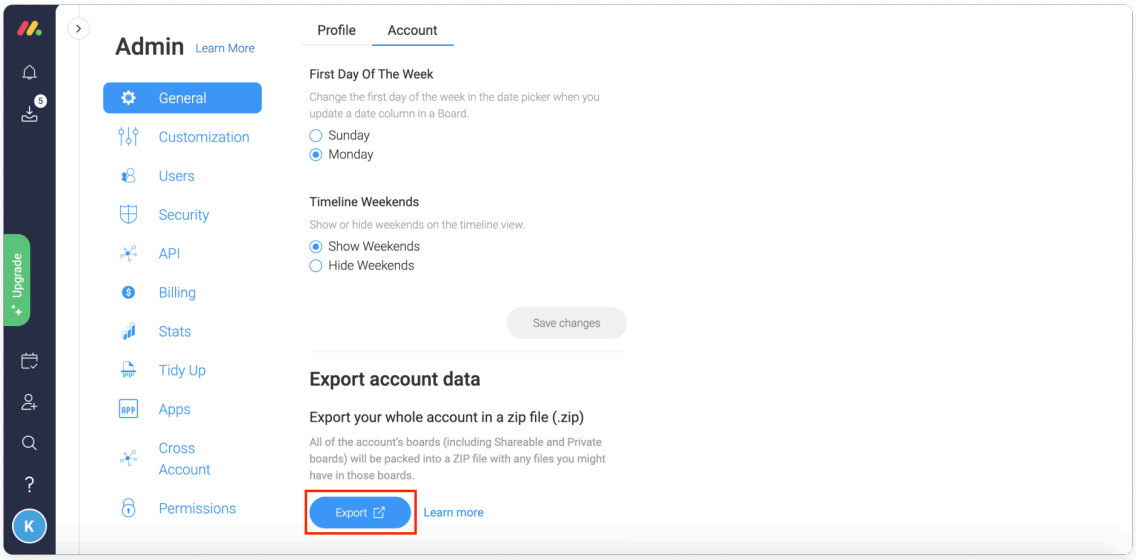
Excel import and export

monday.com provides customers two data management capabilities:

1. Transform data from an Excel spreadsheet into a monday.com board (new or existing).



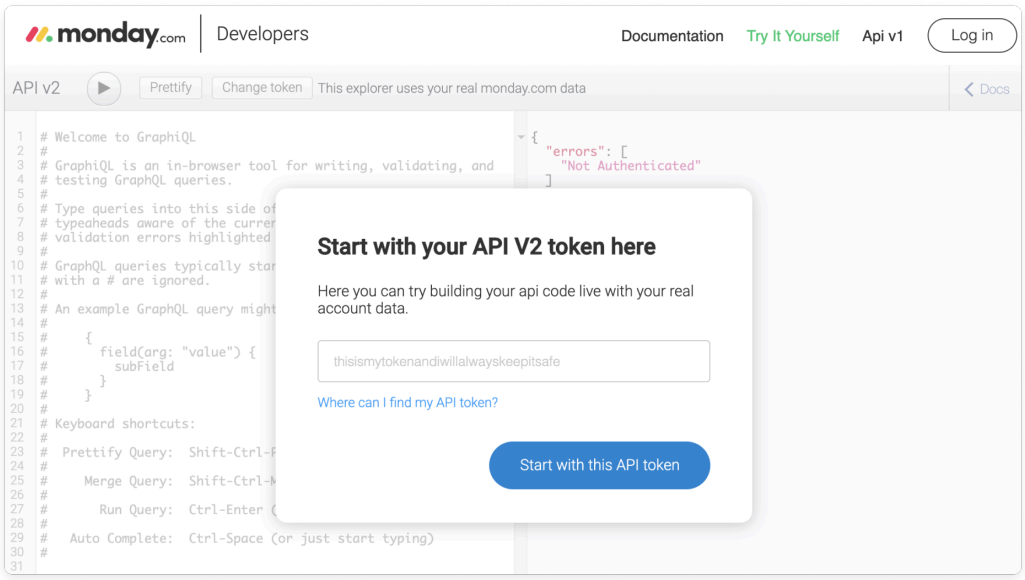
2. Export data from monday.com:
    a. Export boards to Excel.
    b. Export the entire account's data through the administrator panel. It will export as a zip archive containing excel sheets and the files uploaded to the account.



API

monday.com offers a GraphQL API. This is part of the monday apps framework and allows developers to programmatically access and update data inside their monday.com accounts.
Use cases for the API include:

- Accessing board data to render a custom report inside a monday.com dashboard
- Creating a new item on a board when a record is created on another system
- Importing data from another source programmatically



The Admin Panel

In the Admin Panel the admins(s) of your account can manage anything, including security settings, users on the account, account customization, billing, and more.

Authorized domain

Administrators can choose from two settings:

1. Only admins can invite Members and Viewers to the account from any email domain.
2. Admins determine one email domain from which users can sign up to the account.

Email domain blocking

Admins can prevent users from creating new monday.com accounts from certain email domains. This feature is useful to avoid redundant monday.com accounts in the same organization, especially ones that own multiple corporate domains, which can have implications for maintaining compliance to corporate data governance rules.
To block the creation of new accounts, email domains can be submitted to the monday.com service to be reviewed and verify ownership. They will be directed to the account admin(s) to be onboarded to the main organization's account.
Please note: This feature is only available for Enterprise Plan customers. Additionally, admins are able to control from which email domains guests are able to be invited to the account.

Panic Mode

By activating the Panic Mode, you will temporarily block your account. No one will be able to access it until the admin of the account sends a request to our Customer Success team. This feature is crucial if one of your team members' login credentials have been compromised.
Please note: This feature is only available for Enterprise Plan customers.

Session management

In the security section of the Admin Panel, admins can click on the sessions tab to view all users' session data, and control and reset any session. Admins can also set no activity timeout, and a session expiry.
Please note: This feature is only available for Enterprise Plan customers.

Generation of API tokens

Only admins may grant permissions to generate personal GraphQL API tokens in their account (either to everyone, only admin(s), or no one). This prevents users from generating API tokens and mistakenly sharing them with third party tools, or even making them public by pushing them to the public repository and exposing sensitive data of the account. A user who may not generate tokens will be presented with a warning.
Please note: This feature is only available for Enterprise Plan customers.

Content directory

In the content directory you'll find an overview of all the Workspaces, Boards, Dashboards, and Workdocs located in the account. Additionally, for each of these features, you'll be able to see its owners, subscribers, creation date, last updated date and whether it's publicly available to the rest of the account members or not.

* Please note that this white paper does not contain the complete list of the features which are managed via the Admin Panel. Additional information can be found in our support articles.
Additional features managed by the account admin(s) may be covered in various chapters of this document, such as login, two-factor authentication, SCIM provisioning, permissions, IP address restriction, monday apps, Audit Log, API tokens, and HIPAA compliance configuration.

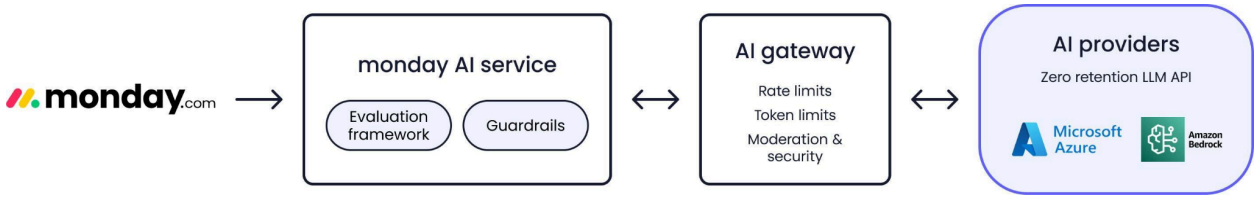
monday AI

Overview

We put powerful AI capabilities in everyone's hands with an intuitive, no-code approach that lowers barriers to AI adoption across multiple industries and use cases. You can start with simple, out-of-the-box AI features and gradually introduce more advanced capabilities to your workflows over time. We're committed to making AI accessible for everyone. Regardless of technical skills, we're empowering everyone to harness powerful intelligent capabilities at work, while ensuring secure, transparent, and ethical AI across our platform and product suite.Our AI capabilities follow the existing permissions within your monday.com account. If a team member

doesn't have access to specific boards or columns, AI won't retrieve or display any data from them.

Architecture diagram



AI Terms

monday AI requires admins and users to review additional terms and conditions that must be accepted on top of the platform's standard terms of service. Use of monday AI must comply with our AI Terms and Conditions, monday.com's Acceptable Use Policy, and our AI model providers policies, including OpenAI's Usage Policy, Sharing and Publication Policy, and Anthropic's Acceptable Use Policy.

Security of monday AI

monday AI leverages trusted third party models equipped with measures for accuracy and bias mitigation. At monday.com, we are dedicated to implementing responsible AI measures, including by using tools provided by our third party models providers and employing measures to monitor and track performance and behavior trends, allowing us to detect anomalies and make adjustments as needed. This combined approach enables us to offer a fair, ethical, and balanced AI experience for all users. We also involve an internal "red team" tasked with simulating edge cases, attempting to disrupt the feature, and uncovering weaknesses. This ensures our AI capabilities are resilient, secure, and aligned with real world needs. Following internal testing, we roll out features gradually to monitor stability and gather feedback, allowing us to refine and improve the feature.

Customer Data and monday AI

monday.com does not use your customer data or content to train its AI models, and we do not allow others to do so. While we may temporarily access your data (for up to 60 days) to monitor and improve our services, it is never shared with third parties or used for model training.

Guardian add-on

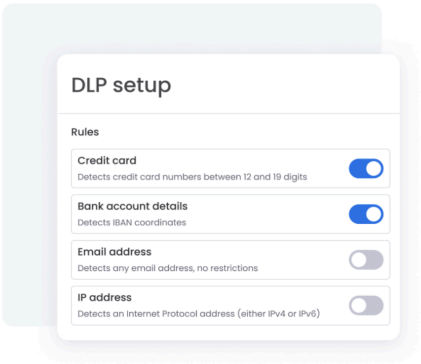
The Guardian add-on can be added to your monday.com account as an extra layer to enhance data protection and governance, streamline organization-wide access, and adhere to compliance requirements with an extra layer of protection. Additional information can be found here: https://support.monday.com/hc/en-us/articles/25276756886674-Guardian-add-on
Get in touch with your consultant to learn more about pricing and capabilities.

Bring Your Own Key (BYOK) and Tenant Level Encryption

BYOK- Gain full control over your data by bringing your own encryption key. Manage your key's lifecycle, grant and revoke access at any point, and maintain total data governance and privacy.
TLE- Segregate and safeguard your data with a dedicated encryption key for your account, further isolating any sensitive data from unauthorized access.

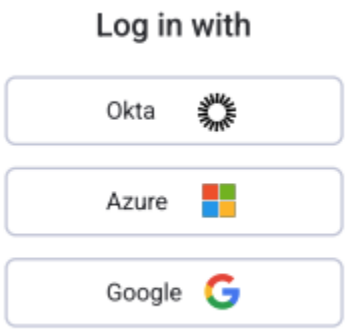
Data Leak Prevention

Our Data Leak Prevention (DLP) helps to manage data risks and identify data leaks early with DLP capabilities providing centralized monitoring and scanning of files and updates across your account.



Multiple SSO

Implement multiple SSO vendors seamlessly to simplify secured access to monday.com across the organization.


Log in with
Okta
Azure
Google

4. Application security

Secure software development life cycle (S-SDLC)

- monday.com uses OWASP Top 10 methodology to build in security for our secure software development life cycle (S-SDLC).
- All code is statically analyzed (SAST) and peer reviewed as part of the CI/CD process to ensure code quality before its deployment to production.
- Dynamic application security testing (DAST) is performed regularly.
- We put special emphasis on writing dedicated tests for new features that are released, while older features have been battle tested for several years.
- We continuously evaluate and monitor our application for vulnerabilities during and after deployment.
- All server side third-party libraries are automatically checked for publicly disclosed vulnerabilities using a software composition analysis (SCA) tool.

Vulnerability management

Vulnerabilities are centralized in a development backlog and are classified based on our evaluation of their impact on the confidentiality, integrity, and availability of the service and of customer data. Our R&D department then carries out remediation within predefined, severity-based timeframes according to our internal Patch Management Policy.

Penetration testing

Application penetration testing is performed on an annual basis, each year by an independent third party, which include manual and automatic testing methods.

In addition, our internal Application Security Team regularly performs security audits and penetration testing for various features which require deep understanding of our internal security mechanisms and architecture.

As part of our external and internal penetration testing, network scanning tools are used against our production servers. Our most recent report is available on our Trust Center at https://trust.monday.com/.

Bug bounty program

monday.com maintains an internally-managed private bug bounty program on HackerOne.

---

5. IT security

Endpoint security

All employee workstations are protected with a centrally-managed Endpoint Detection and Response (EDR) solution for detection and quarantine of malware. Our EDR solution is continuously monitored by a managed 24/7/365 SOC team. All workstations are encrypted using FileVault/BitLocker, password-protected, and set to 10 minutes screen timeout. Additionally, we can apply patches and remotely wipe a machine via a device manager.

Password policy

Our internal password policy dictates that passwords must be at minimum 12 characters long and contain the following:

1. Uppercase letter
2. Lowercase letter
3. Number
4. Symbol

An enterprise password management solution is used, default passwords are changed regularly, password reuse and common passwords are technically disallowed, and passwords expire after 90 days.

Identity and access management

Access to systems is granted by our IT Team based on role through our enterprise identity provider (IdP) solution, as dictated by HR and in accordance with the need-to-know and least privilege principles. All workstations have certificate based attestation as managed devices leveraging biometric authentication.
User access is modified within up to 24 hours following change in employment or termination. Additionally, quarterly user access reviews are conducted to ensure the appropriateness of access privileges. Any access that is no longer required is removed and documented.

Email protection

monday.com uses Google Workspace as our email provider, which is protected using third-party mail relay. DMARC and SPF are in place. Employees have continuously been instructed regarding phishing avoidance best practices and testing is conducted regularly.

Wireless access points

monday.com uses industry-standard technologies to ensure that wireless communications at our headquarters are secure. We use WPA2 Enterprise with certificate authentication that integrates with our IdP to ensure timely deprovisioning and nonrepudiation across the network in addition to other tools such as rogue AP monitoring, etc.

---

6. Operational security

Access to customer data
monday.com treats all data that customers submit to the monday.com service, which is processed by us solely on customer's behalf, as a "black box". This means that customer data is generally not accessed for the performance of the monday.com service, and that we treat all submitted customer data with the highest level of sensitivity and confidentiality.
Access to customer data by monday.com is limited in accordance with our Terms of Service or respective agreement with the customer, on a case-by-case basis. Access to the monday.com servers requires the use of our ZTNA / VPN, which is authenticated against our Enterprise Identity Provider (IdP), fully audited, and enforces password strength and Multi-Factor Authentication (MFA).

Human Resources
Background checks
monday.com carries out comprehensive screening of all its personnel in accordance with industry standards and in alignment with applicable laws and regulations, prior to initiation of employment.

Employment agreement
All monday.com's employment agreements contain confidentiality provisions and provisions allowing for immediate termination upon breach of certain duties and undertakings.
Additionally, monday.com maintains an HR security policy which defines the required security activities and responsibilities during the employment period, from recruitment until departure.

Acceptable use
monday.com maintains an acceptable use policy that is reviewed on an annual basis by our Security Team and wider Security Forum. Our employees are required to sign the policy during onboarding or a material change of the policy.

Training and awareness
As part of their initial onboarding process and at least once a year afterwards, monday.com employees receive mandatory training regarding the information security and privacy obligations they must fulfill. Training includes tutorials as well as written tasks, and are monitored by the Security Team.
Quarterly Security and Privacy Weeks are conducted to further increase awareness amongst employees.
In addition, dedicated training sessions are conducted as necessary (e.g. developers undergo secure coding training).

Termination of employment
User access is modified within up to 24 hours following change in employment or termination of employment, with the return of company equipment. Quarterly user access reviews are conducted to ensure the appropriateness of access privileges.

Red team assessments

Twice a year, we conduct red team assessments on our defensive posture that include internal penetration tests, infrastructure attacks, and assume breach simulation. The red team assessments are performed by leading offensive and defensive third-party security consulting companies, which use high-end sophisticated attack techniques that provide unique visibility into our potential security risks and vulnerabilities.

Governance and risk management

monday.com maintains an ongoing risk management process intended to proactively identify vulnerabilities within monday.com's systems and assess new and emerging threats to the company's operations. monday.com undergoes a risk assessment as part of the ISO 27001 certification, conducted annually.

Incident response and management

monday.com's incident response plan (IRP) sets forth guidelines for detecting security and privacy incidents, escalating them to the relevant personnel, communication (internal and external), mitigation, and post-mortem analysis in a formalized process.
monday.com's Incident Response Team (IRT) comprises representatives from Security, R&D, Legal, representatives from other teams on a case-by-case basis, and if needed, a third-party incident response firm.

Notification

In accordance with the terms of section 7 of our Data Processing Addendum ("Data Incident Management and Notification") after becoming aware of a Data Incident, monday.com will notify affected customers without undue delay .
Affected customers will be informed of the nature of the breach, the harmful effects of which monday.com is aware, actions monday.com has taken, and plans to remediate or mitigate the incident at the time of the notification.

Disaster recovery and business continuity

monday.com maintains a business continuity plan in alignment with ISO 27001 for dealing with disasters affecting our physical office (where no part of our production infrastructure is retained).
In addition, we maintain a Disaster Recovery Plan (DRP) for dealing with disasters affecting our production environment, which includes the restoration of the service's core functionality from our dedicated DR location. Testing is conducted at least twice a year. monday.com's DR test may be in the form of a walk-through, mock disaster, or component testing.

Data retention and disposal

Data retention

monday.com will retain your information that monday.com controls for the period necessary to fulfill the purposes outlined in our Privacy Policy. Data that monday.com processes on behalf of our customers will be retained in accordance with our Terms of Service, our Data Processing Addendum and other commercial agreements with such customers.

Data deletion

monday.com customers retain full control of their submitted data, and may modify, export, or delete it at all times using the means available through the service's user interface.

Upon termination or expiration of their subscription, customers are able to request deletion of their data as part of the account closure procedure. Customer data will then be deleted within 90 days of the request, which includes a 30-day period to allow for rollback and an additional 60 days to proceed with the deletion process.
Alternatively, customers may opt to keep the account's data in the platform, in which case we may continue to retain it, but may also delete it at any time at our discretion.

Data destruction
Our service is hosted on AWS, which implements proprietary data distribution and deletion strategies to allow for safe storage of sensitive data in a multi-tenant environment. Storage media decommissioning is performed by the aforementioned provider using the techniques detailed in NIST 800-88.

Monitoring and logs

monday.com collects and monitors network logs using a cloud intrusion detection system , traffic logs from edge locations, application-level logging for tracing and auditing events, and system-level logging for auditing access and high-privilege operations. Logs are streamed into our security information and event management (SIEM) solution, where they are continuously (24/7/365) monitored by a SOC team.

Supply chain management

Sub-processors
monday.com holds its sub-processors to industry standards with respect to data security and privacy, and considers both areas as critical in its sub-processors selection process. Among other measures, we have ensured that Data Processing Addendums and other relevant documentation and safeguards are in place with all of our sub-processors, and we perform privacy, legal, and information security assessments as well as questionnaire-based audits, all in accordance with industry standards and regulatory requirements. Assessments of our sub-processors are conducted at least on an annual basis.

Vendor management
monday.com maintains a central repository asset management program for both the services and software we utilize. The repository asset is maintained on an ongoing basis by our Security, Legal, Privacy, and Procurement teams, and the approval process is communicated to all employees.
Upon the beginning of usage and renewal of the services or software, the various teams categorize the vendors we work with according to the highest data-sensitivity level they have access to, in order to determine their appropriate risk level and review them in accordance with industry standards and regulatory requirements.

Physical security

monday.com offices
Physical IT assets in the monday.com offices are limited to laptops and office network devices. Office network devices are protected in a password locked, 24/7/365, CCTV-monitored, environmentally-controlled server room. Physical access to the offices is access controlled. Visitors are logged upon entering our offices, and are required to be escorted in sensitive areas at

all times by a monday.com employee during their stay in the office. All employees are to report suspicious activity, unauthorized access to premises, and theft or lost object incidents.

Data center security

monday.com relies on AWS world-class physical and environmental security measures, which results in highly resilient infrastructure. For more information about these security practices, please visit the following link:
https://aws.amazon.com/security/,

---

7. Compliance, privacy, and certifications

Audit assurance and compliance
Audits are performed annually by an independent third party. monday.com has developed its security and privacy programs in compliance and according to several industry-standard compliance programs, as well as leading privacy and data protection regulations in the territories where our service is offered:

ISO 27001, 27017, 27018, 27032, and 27701
monday.com follows the international standards of ISO (International Organization for Standardization) and manages its information security, cloud service, and privacy in accordance. We are audited by an independent third party on an annual basis and maintain 5 ISO certificates:

- **ISO/IEC 27001:2022** is the most rigorous global security standard for Information Security Management Systems (ISMS).
- **ISO/IEC 27018:2014** establishes commonly accepted control objectives, controls, and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.
- **ISO/IEC 27017:2015** provides controls and implementation guidance for both cloud service providers and cloud service customers. It gives guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls.
- **ISO/IEC 27032:2023** provides guidance for improving the state of cybersecurity, drawing out the unique aspects of cybersecurity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP).
- **ISO/IEC 27701:2019** specifies requirements and provides guidance for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS).

All of our certifications can be found here.

SOC 1, SOC 2, and SOC 3
monday.com has achieved Service and Organization Controls:

- **SOC 1 Type II audit**, which examines controls that may be relevant to the financial reporting of customers.
- **SOC 2 Type II audit**, which demonstrates our commitment to meeting the most rigorous security, availability, and confidentiality standards in the industry. It verifies that monday.com's security controls are in accordance with the AICPA (The American Institute of Certified Public Accountants) trust services principles and criteria and HIPAA security requirements.

- **SOC 3 Report**, which is a shorter version of our SOC 2 Type II report and is publicly available.

Cloud Security Alliance (CSA)

Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing."

monday.com takes part in the voluntary CSA Security, Trust, Assurance, and Risk Registry (STAR) Self-Assessment to document our compliance with CSA-published best practices. Our completed CSA Consensus Assessments Initiative Questionnaire (CAIQ) is free and publicly available on the CSA website.

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is designed to help protect healthcare data. Organizations such as hospitals, doctors' offices, health plans, or companies dealing with protected health information (PHI) are required to be HIPAA compliant. This may also extend to companies that work with these businesses and come into contact with PHI on their behalf.

monday.com offers its customers on the Enterprise plan HIPAA-compliant account configuration so that such customers can submit their sensitive healthcare information. Our HIPAA customers need to enter our Business Associate Agreement (BAA) to ensure the protection and proper processing of PHI on their behalf prior to their submission of HIPAA data.

monday.com and the GDPR

Our global Privacy Program is based on the most comprehensive and advanced data protection regulations in the world, with the EU and UK General Data Protection Regulation (GDPR) serving as our "north star."

Among other things, monday.com's Privacy Forum continuously monitors product and process developments across our organization, as well as the various activities involving the use of personal data to ensure that GDPR principles are upheld, such as the principles of Privacy-by-Design, data minimization and storage limitation, lawfulness and fairness in processing, and transparency into our activities and purposes.

monday.com and EU-US Data Privacy Framework (EU-US DPF)

monday.com Inc., our US subsidiary, complies with the EU-US Data Privacy Framework (EU-US DPF), the UK Extension to the EU-US DPF, and the Swiss-US Data Privacy Framework as set forth by the US Department of Commerce, and where appropriate, primarily relies on such certification for accepting transfers of data from the EEA, UK and Switzerland to our US entity (as applicable). You can review our certification on the DPF website here.

TX-RAMP

monday.com is certified through the Texas Risk and Authorization Management Program. These certified products have undergone a rigorous risk assessment and met strict security standards, ensuring they are suitable and secure for utilization by Texas State and local government entities.

Privacy Policy

monday.com's Privacy Policy, which describes our privacy and data processing practices in respect of personal data that we process for our own purposes as a data controller, can be found at the following link.

Data Processing Addendum (DPA)

monday.com's Terms of Service and customer agreements all contain a Data Processing Addendum to ensure the protection and proper processing of personal data on our customers' behalf. You can view and execute our Data Processing Addendum (DPA) online.

Cross-border transfers of personal data

monday.com is headquartered in Israel, with subsidiaries located in the US, UK, Australia, Japan, Singapore, Germany, France, Poland, and Brazil, and engages support teams in Philippines and Guatemala. We use sub-processors in various countries, as detailed on our sub-processors page.
monday.com ensures that any transfers of personal data originating from the EEA, UK or Switzerland, to a country that was not recognised by the European Commission, the UK Secretary of State or the Swiss Federal Data Protection and Information Commissioner (as applicable), as affording an "adequate" level of data protection to personal data, is governed by appropriate contractual safeguards. In such circumstances, we rely on, and build into our relevant agreements, the Standard Contractual Clauses (SCCs), which can be found here and here.
In addition to the protections provided by the SCCs, we supplement our contractual obligations with additional safeguards aimed at strengthening the rights and freedoms of data subjects beyond those granted by the SCCs, and have additional clauses in our contracts that aim to protect customer personal data from being transferred in the event of governmental requests to surveil or otherwise gain access to such data.

Controllers and processors

The GDPR defines and distinguishes between two primary roles when it comes to collecting and processing personal data: data controllers and data processors. A data controller determines the means and purposes of processing personal data, while a data processor is a party that processes data on behalf of the controller.

- monday.com is the data controller of personal data relating to its customers, users, and website visitors. This is further explained in our Privacy Policy.
- monday.com is the data processor of personal data that its customers and users submit to the platform (into the boards and items within their monday.com account), and processes this data on its customers' behalf. We do so in accordance with the Data Processing Addendum entered into with our customer. The third party service providers we use to help us process this data are our "sub-processors".

monday.com and the CCPA

As a "service provider," in relation to customer data submitted via the platform, monday.com complies with the applicable requirements of the California Consumer Privacy Act of 2018 (CCPA) and the regulations of the attorney general of California. Our Data Processing Addendum has been updated to reflect new requirements under the CCPA, ensuring we can continue offering our services to California consumers in compliance with the CCPA.
Additional information can be found here.

The Australian Privacy Act (APA) and Australian Privacy Principles (APP)

The Australian Privacy Act (APA) and Australian Privacy Principles (APP) establish a structured framework to collect, process, use, and share personal information, giving individuals greater control over the way their information is handled. monday.com is committed to complying with the requirements of the APA and APP.
Additional information can be found here.

Internal audits

Our Security, Privacy, Infrastructure, R&D, IT, Operations, and Legal teams conduct quarterly Security and Privacy Weeks, which include the performance of various auditing activities, including user access reviews, firewall configuration reviews, clean desk inspections, awareness training and activities, and more.

Disclosure to government authorities

monday.com does not permit government authorities unwarranted or unfettered access to any customers' data held with us. We rarely receive requests from authorities (in the US or otherwise) to disclose customer data. The few instances in which we have received such requests were limited in scope, and addressed very legitimate grounds for requesting such data (e.g. suspected illegal activity related to that particular account).
Where we are required, under law or a legal compulsion, to disclose customer data to government or law enforcement authorities, we follow a process of verifying that such requests are genuine, valid and warranted. Once a request has been reviewed by our Legal and Privacy teams to ensure its validity and that we have a legal duty to comply, any disclosure would be limited to data that is strictly necessary under law. We use our commercially reasonable efforts to notify our customers before we make such disclosure, unless we are prohibited from doing so..[2] We are also committed to taking commercially reasonable efforts to resist, subject to applicable laws, any

[2] Additional information can be found in section 4 ("Data Sharing") to our Privacy Policy.

request for bulk surveillance relating to the personal data protected under GDPR or the UK GDPR, including under section 702 of FISA.

PrivacyTeam and DPO

monday.com is protected by PrivacyTeam, global leading privacy consultants, and is working hard with PrivacyTeam to ensure that customer data and privacy are protected. Additional information can be found here.

monday.com has appointed privacy veteran Mr. Aner Rabinovitz of PrivacyTeam as our Data Protection Officer, for monitoring and advising on monday.com's ongoing privacy compliance, and serving as a point of contact on privacy matters for data subjects and supervisory authorities.

---

8. WorkCanvas

Hosting Provider

To achieve high availability and resiliency, WorkCanvas is hosted on Google Cloud Platform (GCP) which is a best in class secure infrastructure. Currently the hosting is only available in the US (East), but we are working on providing hosting from the EU for enterprise customers.
This data center employs leading physical and environmental security measures, resulting in highly resilient infrastructure. For more information about its security practices, see below:
GCP Physical Security

File Storage

File storage is hosted by Google storage bucket.

Databases

Databases used by WorkCanvas include Postgres and Redis provided by Google and deployed in high availability.

Backup and Disaster Recovery

Databases are backed up daily to a different region, disaster recovery plan is in place, and quarterly Database restoration tests are conducted.

Hardening

Hardening kubernetes nodes are based on googles Container optimized instances, Dockers are based on alpine.

SLA

Enterprise Plan customers receive 99% uptime commitment.

Admin Panel

To perform administrative actions such as managing users, you will be redirected to the Admin Panel of the connected monday.com account.

Compliance and Certifications

WorkCanvas has its own privacy and security certifications separate from monday.com

- **ISO/IEC 27001:2013** is the most rigorous global security standard for Information Security Management Systems (ISMS).

- **SOC 2 Type II audit**, which demonstrates our commitment to meeting the most rigorous security, availability, and confidentiality standards in the industry. It verifies that monday.com's security controls are in accordance with the AICPA (The American Institute of Certified Public Accountants) trust services principles and criteria.
- **SOC 3 Report**, which is a shorter version of our SOC 2 Type II report and is publicly available.

9. Epilogue

This white paper has provided a broad overview of the monday.com approach to security and privacy. Of course, given the complexity of those subjects you may have additional questions.
You can find further information at our Security Trust Center and Legal Portal.
For further clarification about monday.com's information security or privacy posture, you can also contact our teams via security.requests@monday.com or dpo@monday.com, in addition to the general support that is provided 24/7/365 through our support@monday.com.
Want to report a security concern or vulnerability? Email us at security@monday.com or report through our HackerOne form at https://monday.com/security/form/.