



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

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.

© 2021 monday.com ltd. All rights reserved.

Jan 2023	1.5	Periodical review and revisions
Jan 2023	1.6	Minor update

Table of contents

1. Introduction	5
Our mission statement	5
Our teams	5
Useful Links	5
2. Infrastructure security	6
Hosting providers	6
Network architecture	6
AWS Advanced Technology Partner	7
Network Security	7
Access to production	8
Hardening	8
Databases	8
File storage	8
Multi-region	8
Encryption and key management	8
Encryption in transit	8
Encryption at rest	9
Tenant separation	9
Backup	9
Scalability and reliability	9
Service-level agreement (SLA)	9
3. Security features and functionalities	10
Authentication	10
Credentials	10
Google single sign-on (SSO)	10
Identity provider (IdP)	10
Two-factor authentication (2FA)	11
Authorization	11
SCIM provisioning	11
Permissions	12
Roles within monday.com	13

IP address restrictions	14
Logs	14
Activity Log	14
Audit Log	15
Interoperability and portability	16
Integrations	16
Excel import and export	16
API	18
The Admin Panel	18
Authorized domain	18
Email domain blocking	18
Panic Mode	19
Session management	19
Generation of API tokens	19
Content directory	19
4. Application security	20
Secure software development life cycle (S-SDLC)	20
Web application firewall (WAF)	20
Vulnerability management	20
Security champions	20
Penetration testing	20
Bug bounty program	21
5. IT security	22
Endpoint security	22
Password policy	22
Identity and access management	22
Email protection	22
Wireless access points	22
6. Operational security	23
Access to customer data	23
Human Resources	23
Red team assessments	23
Governance and risk management	24
Incident response and management	24
Notification	24

Disaster recovery and business continuity	24
Data retention and disposal	24
Data retention	24
Data deletion	24
Data destruction	25
Monitoring and logs	25
Supply chain management	25
Sub-processors	25
Vendor management	25
Physical security	25
monday.com offices	25
Data center security	25
7. Compliance, privacy, and certifications	25
Audit assurance and compliance	26
ISO 27001, 27017, 27018, 27032, and 27701	26
SOC 1, SOC 2, and SOC 3	26
Cloud Security Alliance (CSA)	27
The Health Insurance Portability and Accountability Act (HIPAA)	27
monday.com and the GDPR	27
Privacy Policy	27
Data Processing Addendum (DPA)	28
Cross-border transfers of personal data	28
Controllers and processors	28
monday.com and the CCPA	28
The Australian Privacy Act (APA) and Australian Privacy Principles (APP)	28
Internal audits	29
Disclosure to government authorities	29
PrivacyTeam and DPO	29
8. Epilogue	30

1. Introduction

monday.com Work OS manages the data of over 127,000 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.

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 and 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 DPO.

Useful Links

[monday.com Trust Center](#)

[monday.com Legal portal](#)

[monday.com's Status page](#)

[Sub-Processors, subsidiaries, and support](#)

[Security and Privacy at monday.com - FAQ](#)

[Report vulnerabilities](#)

[Support and Knowledge Base](#)

[Pricing and plans](#)

[monday.Engineering Blog](#)

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, primarily Northern Virginia (US) and Frankfurt (Germany),¹ 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 security of the cloud computing infrastructure, while monday.com manages the security of the software and data residing on the cloud computing infrastructure.

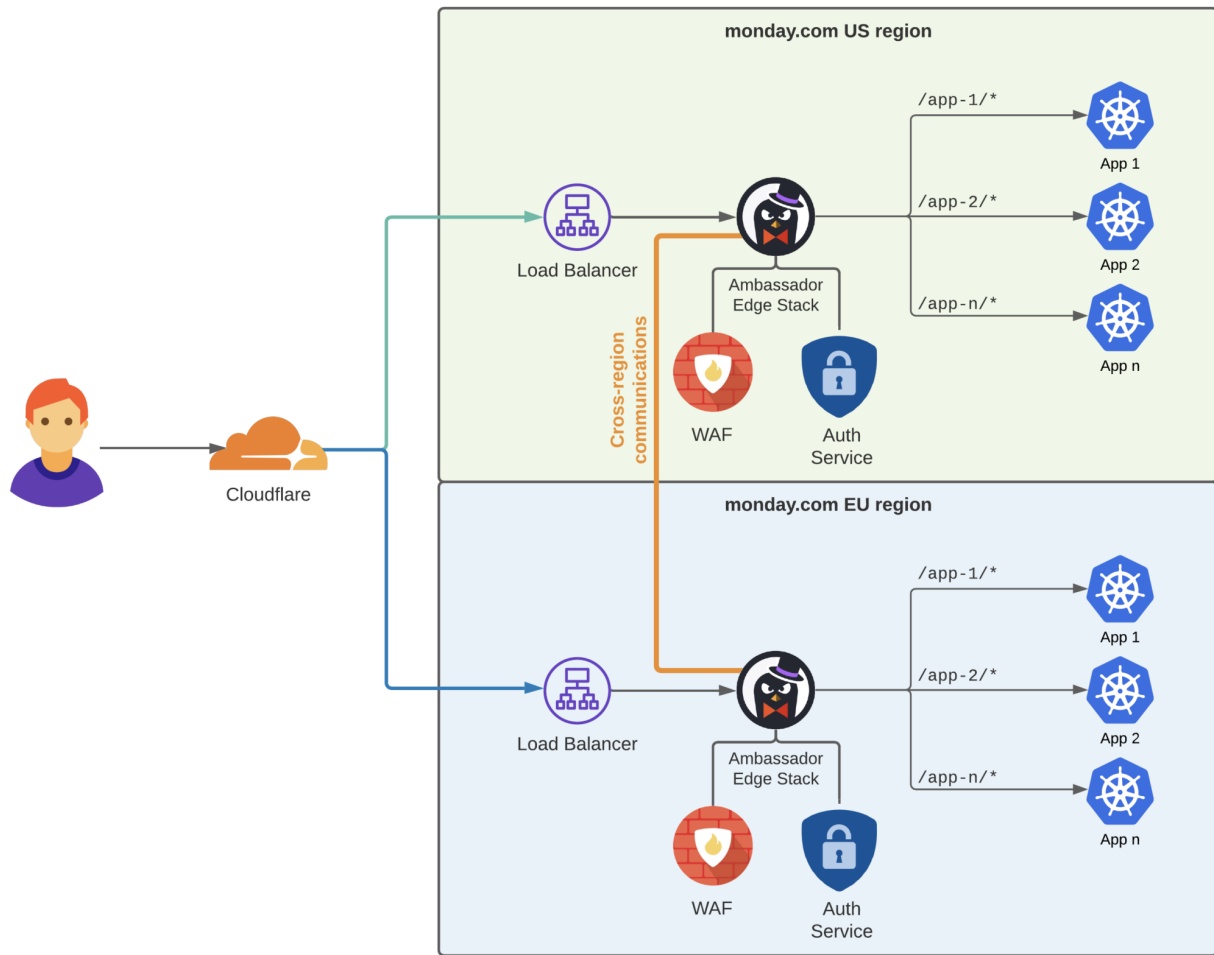
Network architecture

- monday.com's network architecture is built according to AWS best practices, including separating public and private subnets.
- monday.com uses multiple CDN providers, including Cloudflare and Fastly, 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, 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 and in the EU data region:²

¹ Enterprise plan customers can choose to host their data at our EU data center in Frankfurt, Germany.

² A high-level grid network diagram can be shared subject to demand and MNDAs signing.



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.

 AWS Advanced Technology Partner
 monday.com is also 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 ACLs 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. Furthermore, we engage with an independent auditor on an annual basis to review our network configuration.

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 Infrastructure Team personnel (a small and limited team of adept engineers). All access to the monday.com servers requires the use of our VPN, which is authenticated against our Enterprise Identity Provider (IdP), fully audited, and enforces password strength and Multi-Factor Authentication (MFA).

Access to production assets by our developers is done using Kubernetes port forwarding and is similarly authenticated against our IdP.

Hardening

Servers are based on the latest Ubuntu LTS version, 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 requires running containers while ensuring that the underlying software is always secured.

Databases

Databases used by monday.com include MySQL, Elasticsearch, and Redis. API keys to external systems, used by our Integrations features, are stored in a dedicated, self-replicating HashiCorp Vault cluster.

File storage

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

monday.com provides an automated malware detection service for files uploaded to the service by users, ensuring that foreign files uploaded to the service are not infected. 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 or HTML. By blocking these file types we reduce the risk of malware infection significantly.

Multi-region

As of January 2021, monday.com has expanded to its first European data region in Frankfurt, Germany (currently available to Enterprise plan customers).

Due to the identical infrastructure principles in the US region, monday.com customers in the EU 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.

In the future, we plan to open data centers in other regions.

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.

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 backs up its customers' data submitted to the monday.com service and processed on their behalf. We consistently backup user data every five minutes and distribute the encrypted backups across multiple AWS Availability Zones. We have also established DR sites in separate AWS regions for redundancy purposes.

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 ensure audibility 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:

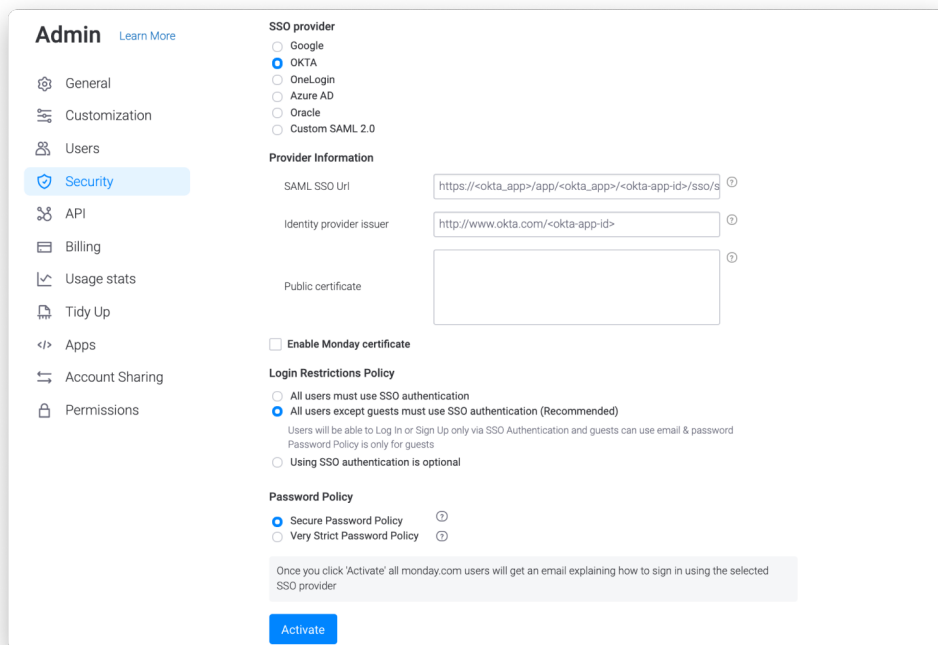
1. 8 characters minimum with no repeating or consecutive characters allowed, or
2. 8 characters minimum with no repeating or consecutive characters allowed and an inclusion of at least one digit (1, 2, 3), one lowercase letter (a, b, c), and one uppercase letter (A, B, C).

Identity provider (IdP)

monday.com currently supports four main [identity providers](#):

1. Google
2. OKTA
3. Azure AD
4. OneLogin

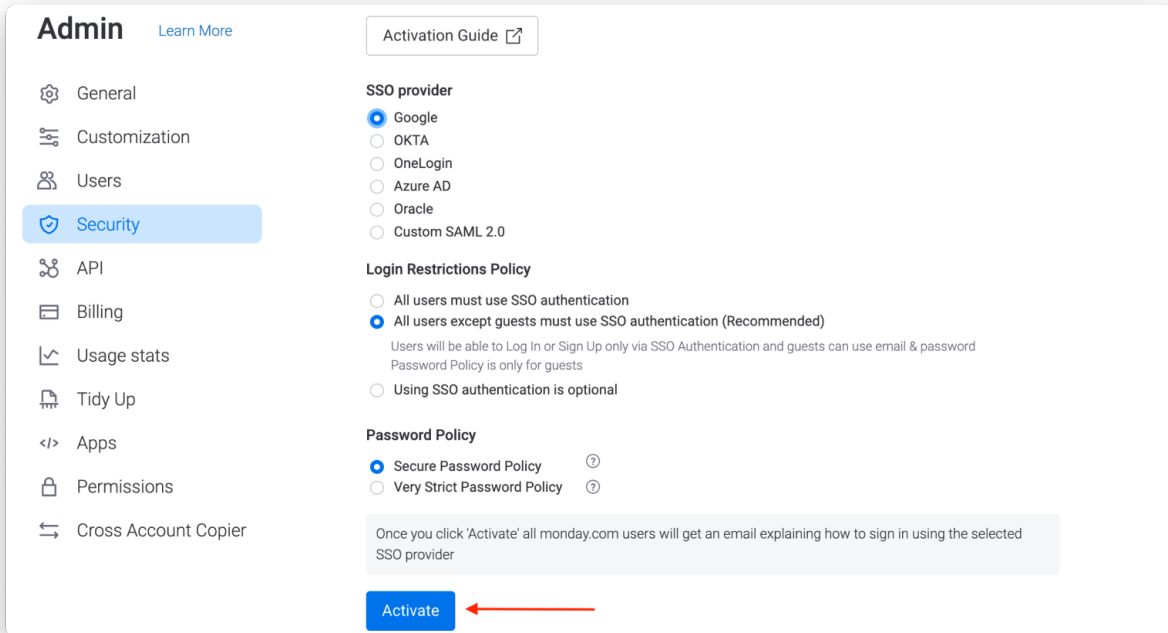
Furthermore, customers have the option to use their own provider using custom SAML 2.0. Please note: This feature is only available for Enterprise Plan customers.



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.

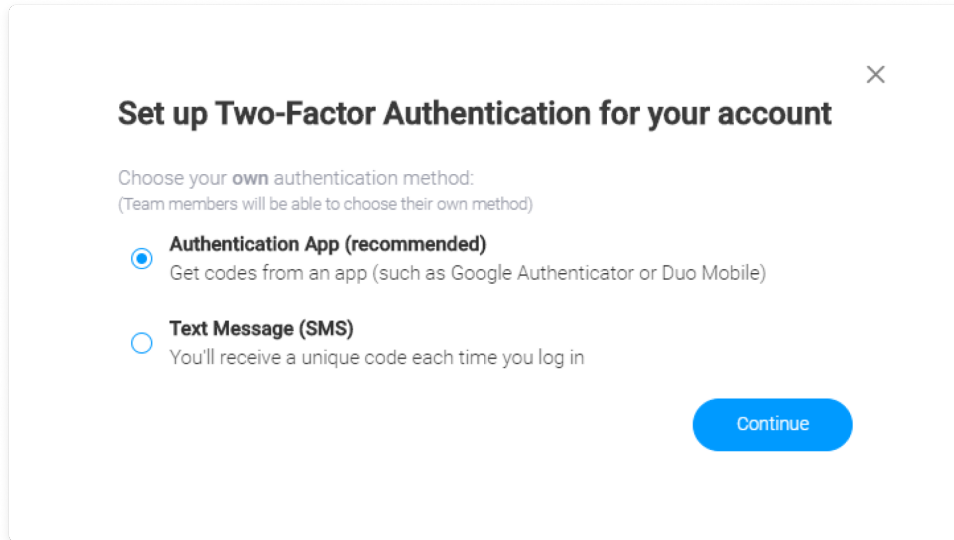
Please note: This feature is available for Pro and Enterprise plans only.



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. 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, member, viewer, 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.

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

Roles within monday.com

[Roles](#) within monday.com include:

Role	Description	Can	Cannot
Administrator	A team member (or more if you choose) who manages its team	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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 • Communicate and add attachments 	<ul style="list-style-type: none"> • Access the User Management section • Access the Security section • Access the Billing section • Access the Content Directory section
Viewer	Only able to view boards, with no editing rights whatsoever	<ul style="list-style-type: none"> • Optional: Export Data to Excel 	<ul style="list-style-type: none"> • Create main boards

	<p>(You can invite an unlimited number of viewers regardless of the plan you have purchased)</p>	<ul style="list-style-type: none"> • View the Teams page and team cards • Optional: upload profile picture 	<ul style="list-style-type: none"> • 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
<p>Guest</p>	<p>External to your organization, such as a vendor, client, freelancer or outside consultant</p>	<ul style="list-style-type: none"> • 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 • View the teams page and team cards • Upload profile picture 	<ul style="list-style-type: none"> • 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 • • Create team • Delete team

			<ul style="list-style-type: none"> ● 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.

IP address restriction Close

IP restriction allows you to limit access based on the IP addresses that you list here.
Once activated, users will not be able to log in to your account unless using an enabled ip address in the list.
You can use CIDR notation. Accepts IPv4 and IPv6.

IP allowlist

Only allow access from the IP addresses listed below

IP description	IP address	
Mine	6.65.113.224	🗑
Home network	203.197.33.160	🗑
Office	49.33.9.249	🗑

Enter description

e.g. 192.168.0.0/16

Add

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.

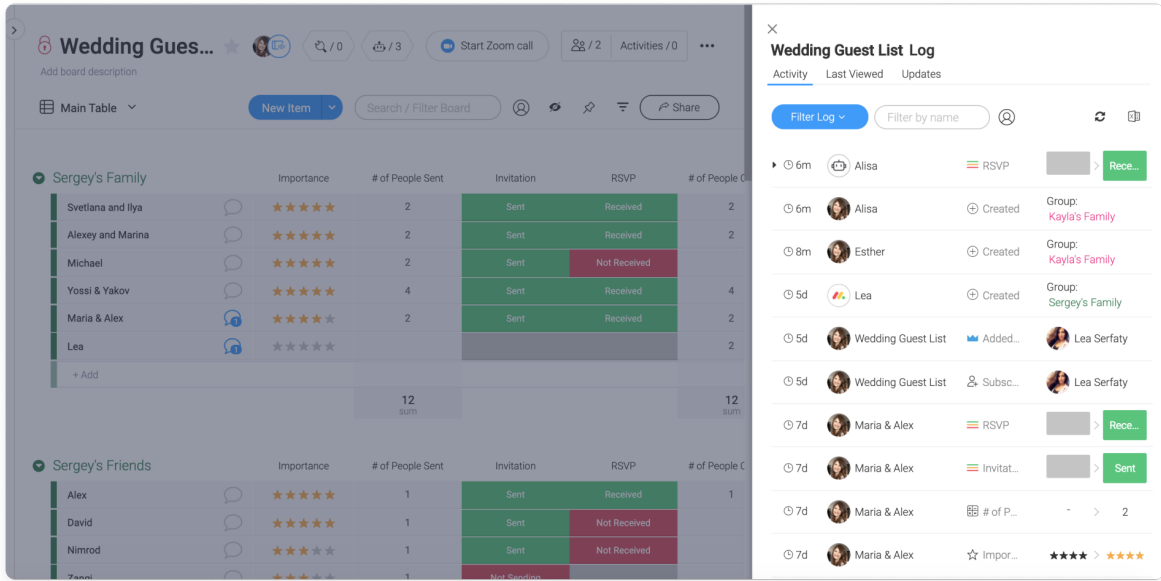
Logs

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 and Enterprise plans hold it up to 1 year.

•



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.

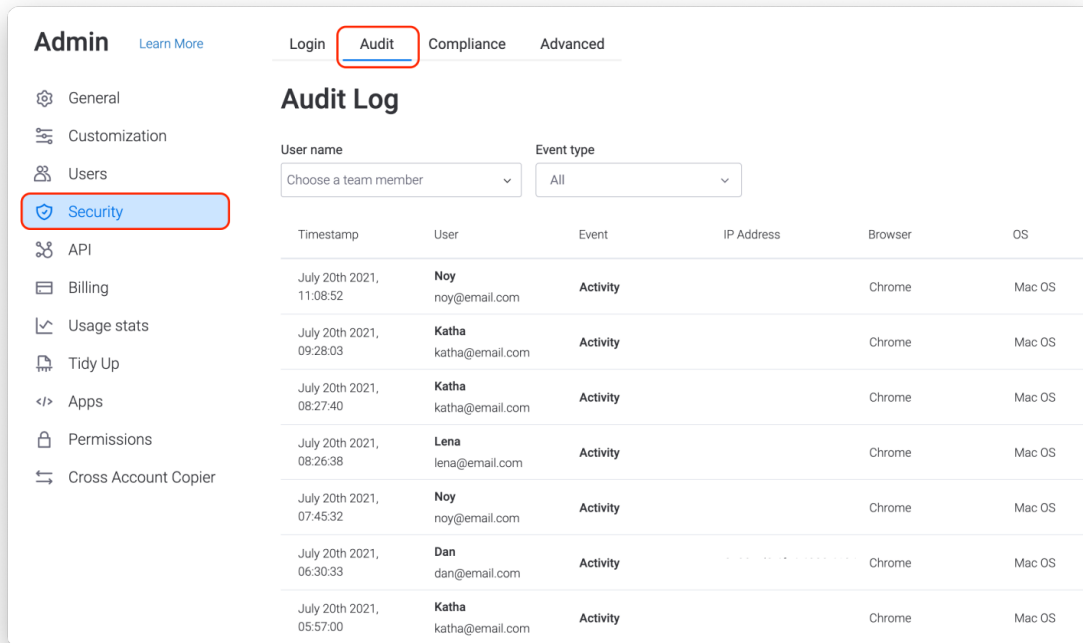
You can easily export your Item Activity Log or Board Activity Log to Excel in the click of a button.

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

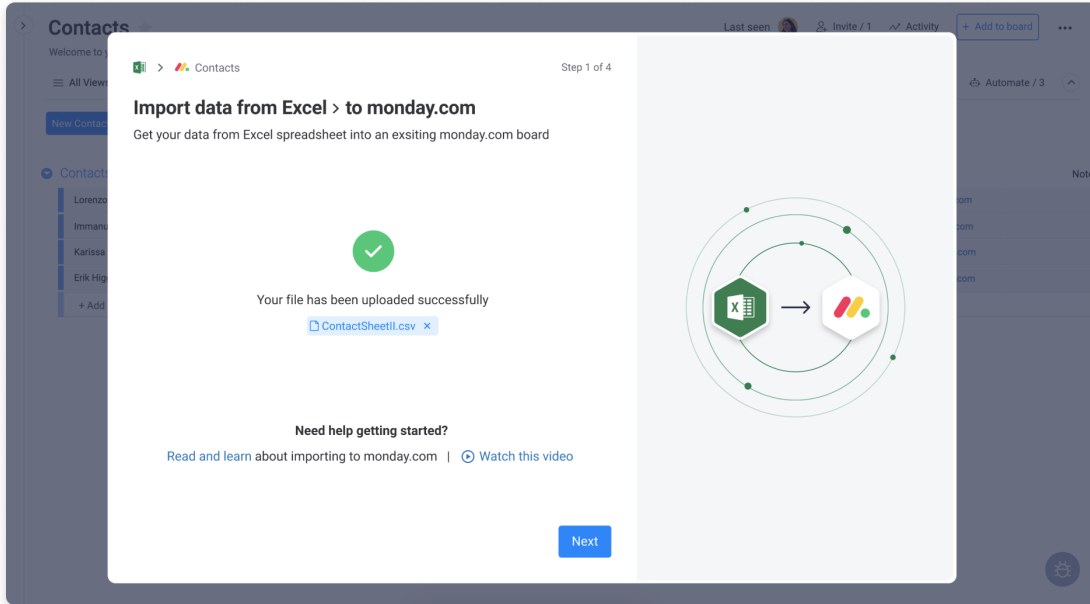
monday.com supports [integrations](#) with various other software solutions to create customized workflows. You can connect monday.com with the tools you already use to manage all your team's work in one place.

Integrations are optional and can be disabled through the Admin Panel.

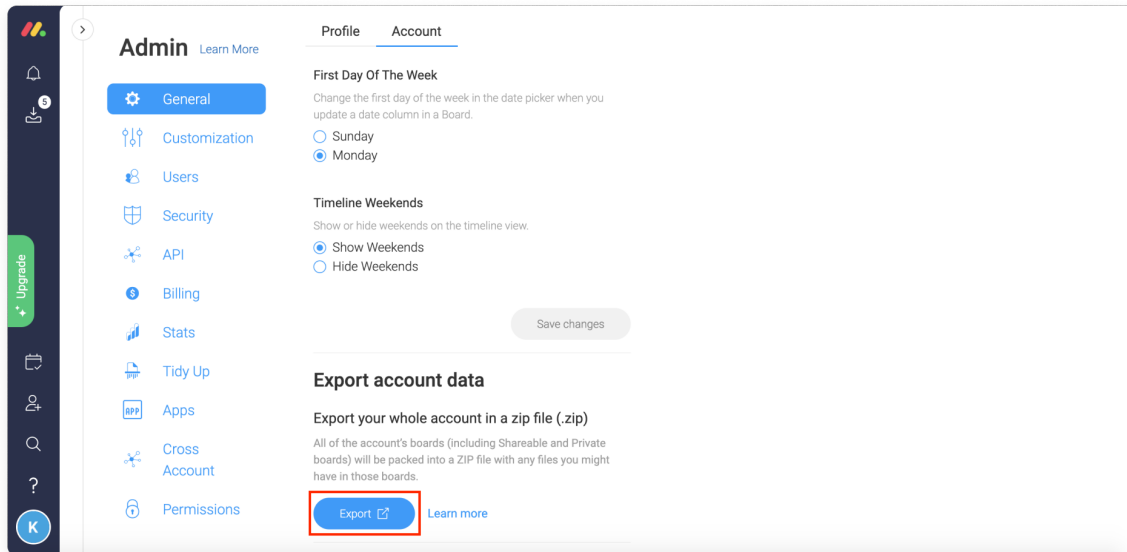
Excel import and export

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.

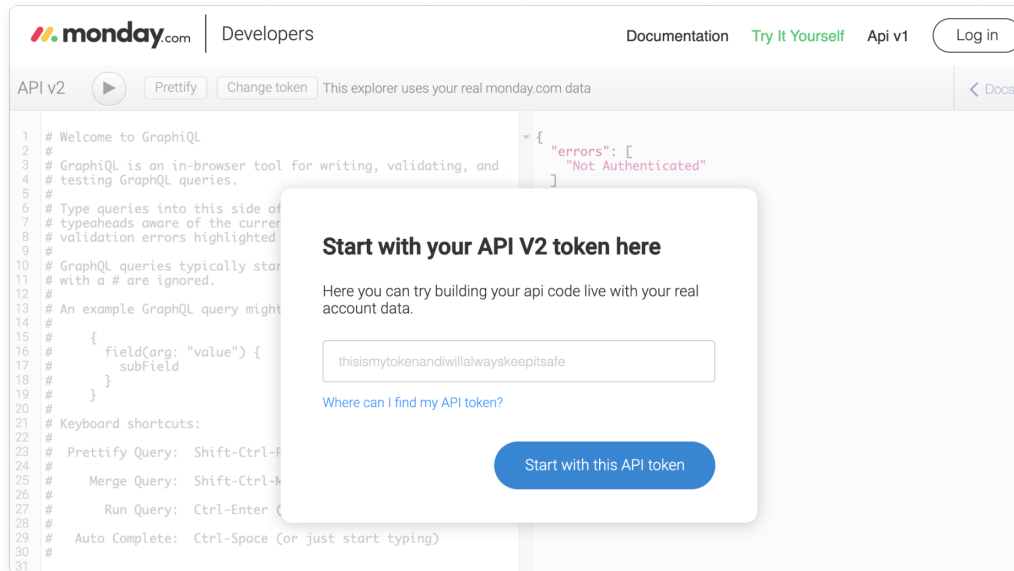


API

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.

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 on at least a weekly basis.
- 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.

Web application firewall (WAF)

A web application firewall (WAF) is in place for filtering, monitoring, and blocking application-level traffic to defend against known attacks.

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. The vulnerability's severity rating is determined by the Common Vulnerability Scoring System (CVSS). Our R&D department then carries out remediation within predefined, severity-based timeframes according to our internal Patch Management Policy.



Security champions

Our internal security champions community comprises developers from all R&D teams. Security champions receive advanced security training and are qualified to provide security guidance and conduct security code reviews whenever necessary.

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.



Bug bounty program

monday.com maintains an internally-managed private bug bounty program on [HackerOne](#), allowing security researchers from around the world to ethically and responsibly research and disclose security vulnerabilities to our Security Team. Certain features will receive special promotions on HackerOne in order to focus the security community research and efforts on these areas. As part of the program, we maintain a [hall of fame scoreboard](#) for hackers.

5. IT security

Endpoint security

All employee workstations are protected with a centrally-managed 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 120 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 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

Our headquarters are located in Israel, where background checks are not customary and are limited under law. The checks we conduct include work history and reference calls with previous direct managers.

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 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.

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 customer 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, with certain data backed up to GCP. Both cloud computing providers implement 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 providers using the techniques detailed in NIST 800-88.

Monitoring and logs

monday.com collects and monitors network logs using a network intrusion detection system (NIDS), 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 managed SOC team.

Supply chain management

Sub-processors

monday.com holds its [sub-processors](#) (both in the global data region and in the EU data region) 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 utilise. 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 controlled through biometric identification. Visitors are logged upon entering our offices, and are required to be escorted 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 and GCP's world-class physical and environmental security measures, which results in highly resilient infrastructure. For more information about these security practices, please visit the following links:

<https://aws.amazon.com/security/>, <https://cloud.google.com/security/>

7. Compliance, privacy, and certifications

Audit assurance and compliance

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 27001:2013** 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 27032:2012** 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.

Audits are performed annually by an independent third party and a report covering April through March is issued on an annual basis.

monday.com’s SOC reports can be found on the following links: [SOC 1](#), [SOC 2](#), and [SOC 3](#).



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.

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 in 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 and Brazil, and engages support teams in the Ukraine, and Guatemala. Our sub-processors are also registered in various countries, as detailed on our [sub-processors page](#).

When we transfer personal data from the EEA and the UK to other countries, we rely on the lawful transfer mechanisms afforded under the GDPR, such as the "adequacy decisions" made by the European Commission (e.g. the decisions deeming the UK and Israel as providing an adequate level of protection to personal data originating in the EU), and the EU Standard Contractual Clauses, which can be found [here](#) and [here](#).

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 for 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," monday.com is committed to complying with the applicable requirements of the California Consumer Privacy Act of 2018 (CCPA) and the regulations of the attorney general of California, in light of similar regulations worldwide (such as the GDPR) and evolving industry standards – to ensure that our customers may continue using monday.com without interruption and can process personal information of 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 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 in previous years were limited in scope, and addressed very legitimate grounds for requesting such data (e.g. suspected illegal activity related to that particular account).

After the request has been reviewed by our Legal and Privacy teams to ensure it is valid and warranted, 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 or are unable due to a potential risk.³ We are also committed to taking commercially reasonable efforts to resist, subject to applicable laws, any 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, the leading Privacy Consultancy in Israel, 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.

³ Additional information can be found in section 4 ("Data Sharing") to our [Privacy Policy](#).

8. 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@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/>.

