monday.com Informe de Segurança e Privacidade

Data	Versão	Descrição da alteração
Novembro de 2021	1.0	Versão final

Índice

Este informe se destina a oferecer uma visão geral sobre as práticas de segurança e privacidade da monday.com em vigor na data da publicação deste documento, as quais estão sujeitas a alterações sem aviso prévio. A descrição de planos futuros está sujeita à alteração ou atraso, a exclusivo critério da monday.com. Este informe possui fins exclusivamente informativos e não constitui orientação jurídica e não deve ser interpretado como suplementar ou incorporado aos termos e condições de relações contratuais.

5

---

1. Introdução

O Work OS monday.com gerencia os dados de mais de 127 mil empresas ao redor do mundo, e, com essa responsabilidade, temos o compromisso de oferecer aos nossos clientes os mais altos padrões de segurança e proteção de dados. Conquistamos a confiança dos nossos clientes fazendo da segurança de dados a nossa prioridade.

Declaração da nossa missão
Oferecer tranquilidade aos nossos clientes na gestão de seus dados no Work OS monday.com.

Nossas equipes
Os esforços da monday.com na segurança da informação são orientados e monitorados pelo nosso CISO e equipe de segurança, além de um fórum de segurança composto por representantes das equipes de infraestrutura, P&D, operações e TI.
Os esforços da monday.com na área de privacidade são orientados e monitorados pelo nosso fórum de privacidade, que é composto por representantes das equipes jurídica, de privacidade e de segurança, lideradas pelo nosso DPO.

Links úteis
Central de confiança da monday.com
Portal jurídico da monday.com
Página de status da monday.com
Subprocessadores, subsidiárias e suporte
Segurança e privacidade na monday.com - FAQ
Relatar vulnerabilidades
Suporte e base de conhecimento
Preços e planos
Blog monday.Engineering

---

2. Segurança da infraestrutura

Provedores de hospedagem

Para alcançar alta disponibilidade e resiliência, nosso serviço é hospedado na infraestrutura da Amazon Web Services (AWS) em múltiplas regiões, principalmente na Virgínia do Norte (EUA) e Frankfurt (Alemanha)[1], em diversas zonas de disponibilidade, com implantações dedicadas à recuperação de desastres (DR) estabelecidas em diferentes regiões. As contas dos clientes são vinculadas a uma única região.

No modelo de responsabilidade compartilhada, a AWS gerencia a segurança da infraestrutura de computação na nuvem, enquanto a monday.com gerencia a segurança do software e dos dados que residem na infraestrutura de computação na nuvem.

Nosso recurso de log de atividades (conforme descrito abaixo, neste documento) faz o backup dos dados no Google Cloud Platform (GCP), nos EUA.

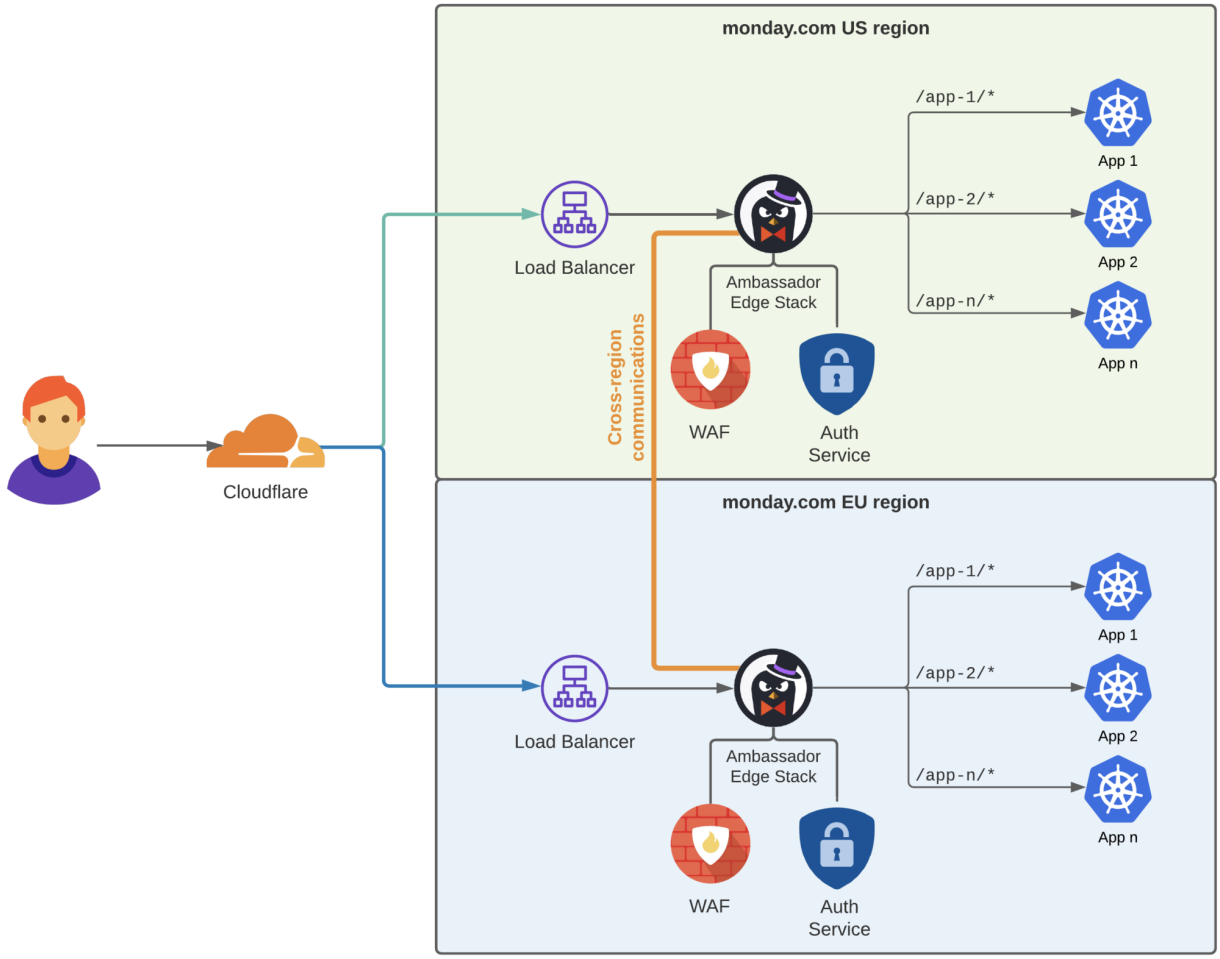
Arquitetura de rede

- A arquitetura de rede da monday.com é construída de acordo com as melhores práticas da AWS, incluindo a separação de sub-redes públicas e privadas.
- A monday.com usa múltiplos provedores de CDN, incluindo Cloudflare e Fastly, a fim de prevenir ataques DDoS e de força bruta. A taxa limite é configurada tanto na ponta quanto a nível de aplicação.
- Os balanceadores de carga residem na sub-rede pública, enquanto os componentes da rede interna, por exemplo, os serviços e bancos de dados da aplicação web, residem na sub-rede privada e não têm IPs públicos atribuídos a eles.
- Um firewall de aplicação web (WAF) é habilitado para bloqueio dinâmico de ataques, baseado no conteúdo.
- Os firewalls são usados ao longo da rede para reforçar as listas de permissão de IPs e o acesso dos recursos de rede somente através das portas permitidas. As regras de grupos de segurança são configuradas para permitir o acesso exclusivamente através das portas estabelecidas.
- Os sensores do sistema de detecção de intrusão de rede (NIDS) são usados em conjunto com os serviços de segurança da AWS, que são habilitados para todos os ativos de produção.

A seguir são mostrados os destaques do diagrama de rede da monday.com, tanto da região de dados dos EUA quanto da região de dados da UE:[2]

[1] Clientes do plano corporativo podem escolher hospedar seus dados em nosso centro de dados na UE, em Frankfurt, Alemanha.

[2] Um diagrama de alto nível da rede em grade por ser compartilhado mediante solicitação e assinatura de um MNDA.



A infraestrutura como código é extensamente usada para garantir que as alterações de configuração sejam registradas e auditadas. A equipe de infraestrutura da monday.com realiza uma revisão trimestral minuciosa da configuração da rede de perímetro e faz as alterações consideradas necessárias para manter ou aumentar a segurança.

aws partner network

Parceira de tecnologia avançada da AWS

A monday.com também é uma parceira de tecnologia avançada da AWS, o que atesta que a própria AWS examinou rigorosamente nossa organização em termos de infraestrutura, segurança da informação, design de melhores práticas e mais.

Segurança de rede

Visto que a monday.com é uma solução baseada puramente na nuvem, temos a vantagem de usar controles modernos e orientados à nuvem para obter uma visão precisa do nosso perímetro de rede. Coletamos e monitoramos logs de rede usando NIDS e logs de tráfego de locais de ponta, e

analisamos os alarmes relevantes através do nosso sistema de segurança da informação e gestão de eventos (SIEM). Usamos ferramentas de monitoramento de segurança, que frequentemente recuperam nossa configuração de grupos de segurança e ACLs de rede do provedor da nuvem, bem como construímos uma visão geral completa da nossa rede.

A equipe de infraestrutura da monday.com realiza uma análise trimestral minuciosa da configuração da rede de perímetro e faz as alterações consideradas necessárias para manter ou aumentar a segurança. Além disso, contratamos um auditor independente uma vez por ano para analisar nossa configuração de rede.

Acesso à produção
O acesso aos ativos de produção é concedido com base na função e de acordo com os princípios da necessidade de saber e menor privilégio. Os privilégios administrativos são oferecidos somente ao pessoal da nossa equipe de infraestrutura (uma equipe pequena e limitada de engenheiros peritos). Todo o acesso aos serviços da monday.com exige o uso da nossa VPN, que é autenticada com base em nosso provedor de identidade (IdP) corporativa, integralmente auditado, e reforça o nível de segurança da senha e autenticação multifator (MFA).
O acesso aos ativos de produção pelos nossos desenvolvedores é feito através de redirecionamento de porta Kubernetes e é autenticado de forma semelhante com base em nosso IdP.

Endurecimento
Os servidores são baseados na versão mais recente do Ubuntu LTS (20.04), endurecidos em alinhamento com os padrões do CIS (Center for Internet Security).

Bancos de dados
Os bancos de dados usados pela monday.com incluem MySQL, Elasticsearch e Redis. As chaves de API para sistemas externos, usadas pelos recursos das nossas integrações, são armazenadas em um cluster dedicado autorreplicante HashiCorp Vault.

Armazenamento de arquivos
O armazenamento de arquivos é hospedado no Simple Storage Service (S3) da AWS, que armazena os anexos e backups de bancos de dados. Os anexos contêm os arquivos enviados pelos clientes ao serviço monday.com.
A monday.com oferece um serviço automatizado de detecção de malwares para os arquivos enviados ao serviço pelos usuários, garantindo que arquivos externos enviados ao serviço não estejam infectados. Além disso, temos uma lista negra contendo as extensões de arquivo proibidas. A lista negra de extensões contém os tipos de arquivo que podem ser considerados perigosos, tais como executáveis ou HTML. Ao bloquear esses tipos de arquivos, reduzimos significativamente o risco de infecção por malwares.

Multirregião
Desde janeiro de 2021, a monday.com expandiu para sua primeira região de dados europeia em Frankfurt, Alemanha (disponível atualmente para clientes do plano Corporativo).
Em razão de princípios de infraestrutura idênticos aos da região dos EUA, os clientes da monday.com na UE podem desfrutar sua experiência com o mesmo nível de medidas e controles de segurança e com a confiança de que a tríade de princípios CIA (em português, confidencialidade, integridade e disponibilidade) é observada.

Os destaques do diagrama de rede da monday.com são retratados abaixo.
Futuramente, planejamos abrir centros de dados em outras regiões.

Criptografia e gestão de chaves

Criptografia em trânsito

Os dados em trânsito através de redes abertas são criptografados usando TLS 1.3 (no mínimo, TLS 1.2).

Criptografia em repouso

Os dados em repouso são protegidos por criptografia AES-256. As chaves de criptografia são armazenadas usando-se o Key Management Service (KMS) da AWS. Uma chave-mestra de cliente (CMK) com rotação anual é usada atualmente para criptografar todos os dados do cliente enviados para o serviço monday.com e processados em seu nome.

Separação de inquilinos

Nosso ambiente usa multitenancy com separação lógica entre os clientes. Os dados dos clientes são segregados a nível de aplicação usando IDs exclusivos resultantes de uma combinação de vários parâmetros.

Estamos trabalhando no momento para habilitar a criptografia a nível de inquilino (TLE) para nossos clientes. A TLE é uma camada que garante que os dados em repouso sejam criptografados com uma chave dedicada por conta e oferece proteção contra visualização de dados por sistemas ou pessoal não autorizados.

A TLE protege contra dois cenários principais:

1. **Invasores:** os dados nos campos dos bancos de dados são criptografados, portanto obter acesso ao banco de dados e extrair seus dados só fornecerá ao invasor os dados criptografados.
2. **Compartilhamento acidental:** os dados são criptografados por uma chave dedicada por conta, consequentemente, se os dados forem compartilhados acidentalmente entre as contas, eles nunca serão compartilhados como texto simples.

Planejamos oferecer aos clientes do plano Corporativo a opção de trazer suas próprias chaves de criptografia (BYOK: traga sua própria chave) num futuro próximo.

Backup

A monday.com faz backup dos dados enviados pelo cliente para o serviço monday.com e daqueles processados em seu nome. Fazemos backup dos dados dos usuários consistentemente a cada cinco minutos e distribuímos esses backups criptografados em múltiplas zonas de disponibilidade da AWS. Também estabelecemos locais de DR em distintas regiões da AWS para fins de redundância. O backup dos dados de logs de atividades é feito no GCP.

Escalabilidade e confiabilidade

A arquitetura de microsserviços é utilizada para garantir impacto mínimo na saúde do sistema, em caso de falha de um ou mais componentes. O serviço monday.com é completamente conteinerizado, com Kubernetes usados para orquestração. Isso oferece uma infraestrutura altamente escalável, adequada para lidar com a crescente demanda dos clientes, ao mesmo tempo em que proporciona uma experiência de qualidade para os usuários finais.

A infraestrutura como código é amplamente usada através do Terraform para garantir a audibilidade e manutenção dos recursos de infraestrutura.

A monday.com monitora continuamente as métricas de desempenho de todos os componentes de sua infraestrutura e a constrói para ser escalável. Além disso, realizamos revisões trimestrais de escala com engenheiros de infraestrutura e com a gerência para garantir que nosso roteiro ofereça serviços de qualidade para um número cada vez maior de clientes e recursos de produtos.

Acordo de nível de serviço (SLA)

A disponibilidade dos nossos serviços pode ser monitorada através da nossa página de status. Raramente é necessário que o sistema fique inativo para manutenção. Quando necessário e conforme praticável, agenda-se para os finais de semana, em horários de baixa atividade.

As notificações relativas ao tempo de inatividade são disponibilizadas imediatamente através da página de status, onde os clientes podem inscrever-se nas notificações por e-mail ou mensagem de texto relacionadas à disponibilidade e aos esforços de mitigação empregados por nossa equipe.

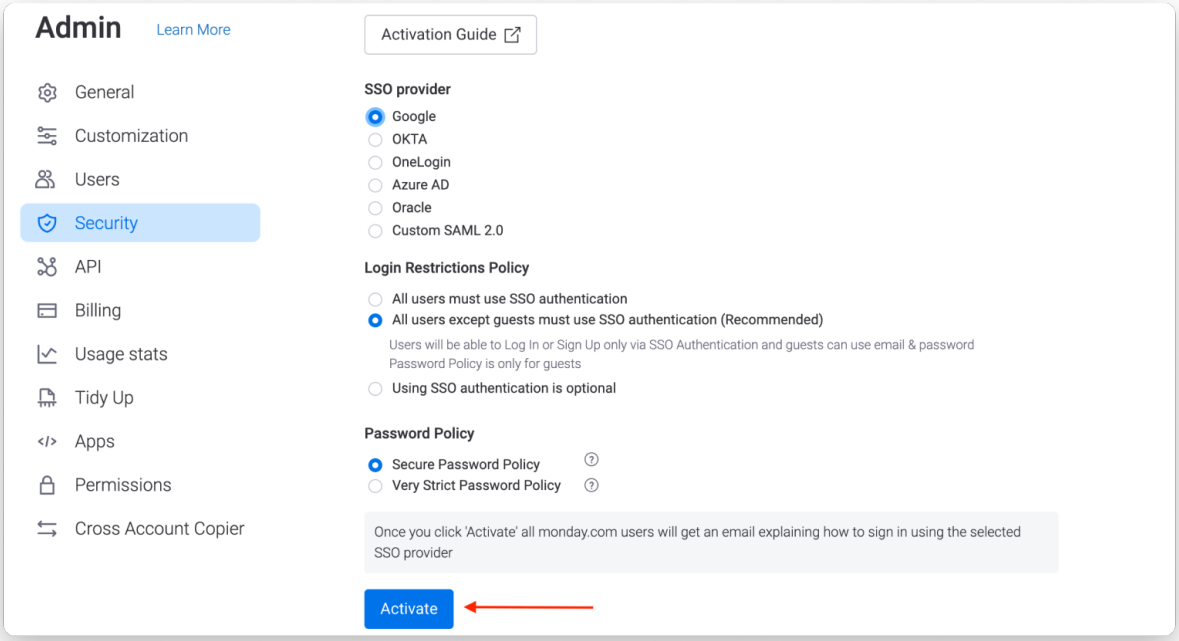
Clientes do plano Corporativo recebem o compromisso de 99,9% de tempo de atividade.

3. Recursos e funcionalidades de segurança

Autenticação
A monday.com é compatível com os seguintes métodos de autenticação:
Credenciais
Se você opta por autenticar os usuários de sua conta usando credenciais, oferecemos aos administradores duas opções de configuração de força da senha para suas contas:

1. Mínimo de 8 caracteres, não permitindo caracteres repetidos ou consecutivos, ou
2. Mínimo de 8 caracteres, não permitindo caracteres repetidos ou consecutivos, além da inclusão de, no mínimo, um dígito (1, 2, 3), uma letra minúscula (a, b, c) e uma letra maiúscula (A, B, C).

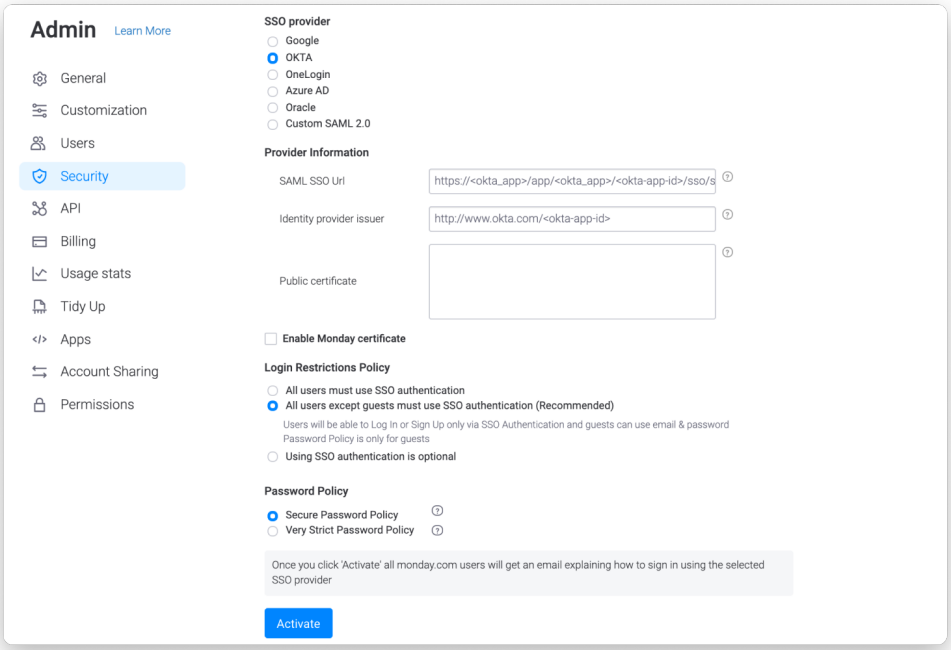
Logon único (SSO) do Google
O SSO do Google é um sistema de autenticação segura que reduz o fardo de se lembrar de múltiplas senhas ao permitir que os usuários iniciem sessão no serviço monday.com usando sua conta do Google.
Esse recurso está disponível apenas nos planos Profissional e Corporativo.



Provedor de identidade (IdP)
A monday.com atualmente é compatível com três dos principais provedores de identidade:

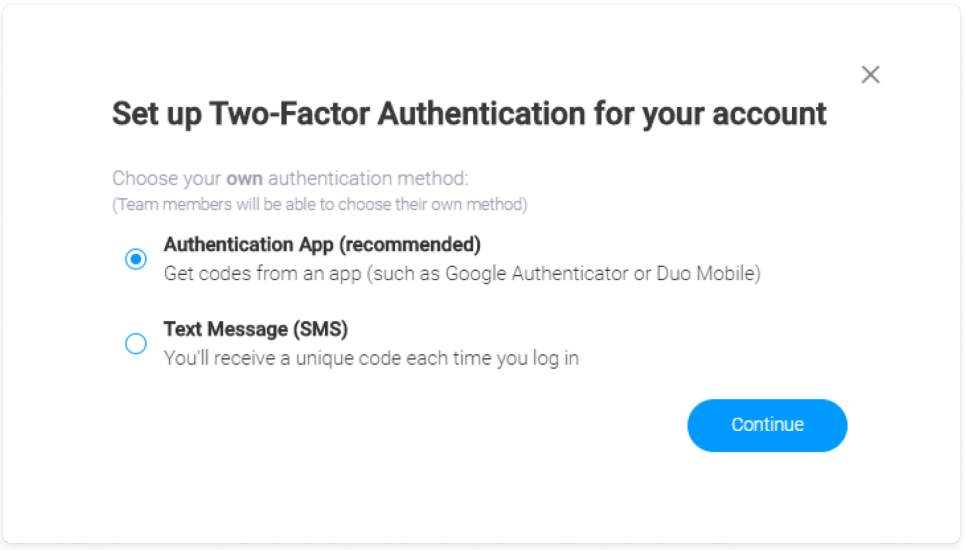
1. OKTA
2. Azure AD
3. OneLogin

Além disso, os clientes têm a opção de usar seu próprio provedor através de SAML 2.0 personalizada.
Esse recurso está disponível apenas para clientes do plano Corporativo.



Autenticação de dois fatores (2FA)

Além dos métodos de autenticação acima, os administradores podem configurar uma camada extra de segurança e habilitar o 2FA através de mensagem de texto (SMS) ou app autenticador. Observe que, se você optar por integrar seu IdP, o 2FA deverá ser habilitado do seu lado.



Autorização

Provisionamento SCIM

O sistema para gerenciamento de identidade entre domínios (SCIM) é um protocolo para a gestão de usuários entre múltiplas aplicações, que permite provisionar (adicionar), desprovisionar (desativar) e atualizar facilmente os dados de usuários e equipes entre múltiplas aplicações de uma vez. A monday.com é compatível com três formas de configurar o provisionamento SCIM:

1. Aplicações SCIM existentes na monday.com:
    a. OKTA
    b. Azure AD
    c. OneLogin
2. Integração SCIM personalizada com sua escolha de provedores de identidade
3. Provisionamento SCIM usando API

A tabela a seguir apresenta todos os atributos de **usuário** compatíveis com a integração SCIM na monday.com:

Atributo da monday.com	Atributo(s) de API SCIM	Descrição
Nome (obrigatório)	name, displayName	O nome de exibição do usuário.
Endereço de e-mail (obrigatório)	userName, email	O endereço de e-mail usado pelo usuário para efetuar login no serviço monday.com.
Ativo (obrigatório)	active	Ao criar um usuário, esse campo deve ser definido como "verdadeiro". Alterar o valor "ativo" do usuário para "falso" o desativará no serviço monday.com.
Posição	title	A posição do usuário na organização.
Fuso horário	timezone	O fuso horário do usuário (todas as datas na plataforma estarão de acordo com esse fuso horário).
Localidade	locale	A monday.com mostrará uma versão localizada para diferentes localidades.
Número de telefone	phoneNumbers	O número de telefone do usuário (somente aquele marcado como "principal" será exibido).
Endereço residencial	addresses	O endereço do usuário (somente aquele marcado como "principal" será exibido).
Tipo de usuário	userType	O nível de cada usuário dentro da conta. Os valores possíveis são: admin, member, viewer ou guest (o valor padrão é "member").

A tabela a seguir apresenta todos os atributos de **equipe** compatíveis com a integração SCIM na monday.com:

Atributo da monday.com	Atributo(s) de API SCIM	Descrição
Nome (obrigatório)	displayName	O nome de exibição da equipe.
Usuários	members	Lista de usuários atribuídos à equipe.

Esse recurso está disponível apenas para clientes do plano Corporativo.

Permissões

A monday.com ajuda você a controlar quem faz o que em sua conta. Oferecemos diversos tipos de permissões para personalizar e restringir a visualização ou edição de dados, incluindo:

1. **Permissões de quadro**
    a. Tipos: quadros "principal", "compartilhável" e "privado"
    b. Restrições: "editar tudo", "editar conteúdo", "editar por responsável" e "somente visualização"
2. **Permissões de coluna**: "restringir edição da coluna" e "restringir visualização da coluna"
3. **Permissões de painel**
    a. Tipos: painéis "principal" e "privado"
    b. Restrições: somente proprietários do painel podem editá-lo, bem como os apps e widgets dentro dele
4. **Permissões de área de trabalho**
    a. Tipos: áreas de trabalho "abertas" e "fechadas"
    b. Restrições: "ninguém", "apenas administradores", "proprietários da área de trabalho" e "todos"
5. **Permissões de conta:** administradores podem definir restrições ("ninguém", "apenas administradores" e "todos") nos seguintes recursos:
    a. Envio de arquivos
    b. Transmissão de quadros
    c. Criação de quadros principais
    d. Criação de quadros privados
    e. Criação de quadros compartilháveis
    f. Criação de integrações
    g. Criação de automações
    h. Criação de áreas de trabalho
    i. @mencionar ou inscrever todos os usuários da conta em uma atualização ou quadro
    j. Exportar para o Excel quadros, logs de atividades, resultados da busca e atualizações

Por favor, observe que alguns dos recursos acima podem não estar disponíveis em todos os planos.

Funções dentro da monday.com

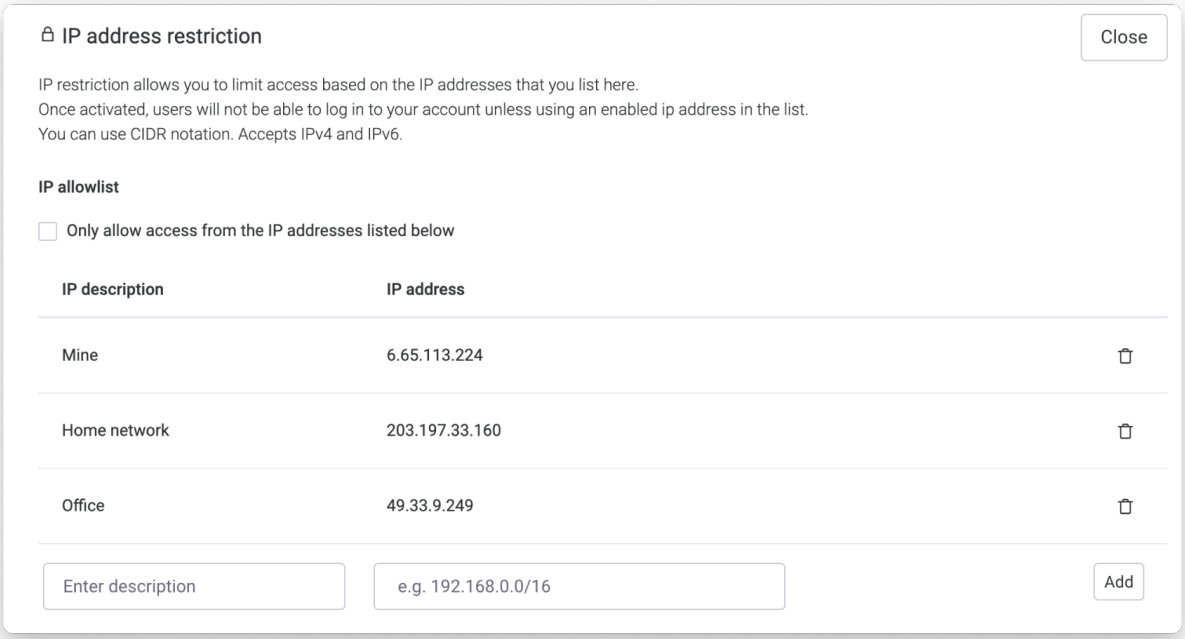
As funções na monday.com incluem:

Função	Descrição	Pode	Não pode
Administrador	Um membro da equipe (ou mais se você optar) que gerencia sua equipe	• Supervisionar a conta inteira • Gerenciar tudo, dos usuários e quadros à segurança e cobranças (conforme descrito na seção "painel do administrador", abaixo)	
Membro	Tem acesso à edição	• Criar e editar quadros, itens e pastas	

	(O número de membros que você pode convidar depende do seu plano)	• Convidar outros membros dentro de um quadro e item • Visualizar todos os quadros principais • Ser convidado para quadros compartilháveis ou privados • Editar o perfil • Comunicar e adicionar anexos	
Visualizador	Só pode visualizar quadros, sem nenhum direito de edição (Você pode convidar um número ilimitado de visualizadores, independentemente do plano adquirido)	• Ver todos os quadros na área de trabalho principal da conta • Abrir um item e ler as atualizações • Pesquisar ou filtrar dentro de um quadro • Ser convidado para quadros compartilháveis ou privados • Editar o perfil • Convidar novos visualizadores • Abrir as visualizações do quadro • Ser designado para um item • Ser adicionado a uma equipe • Exportar quadros para o Excel	• Criar ou excluir um novo quadro • Fazer alterações no conteúdo, estrutura ou configurações de um quadro • Adicionar atualizações a um item ou curtir uma atualização publicada por outra pessoa • Inscrever a si mesmo ou outras pessoas em um item/quadro • Ser designado como proprietário de um quadro • Convidar pessoas para um quadro compartilhável • Criar uma equipe
Convidado	Externo à sua organização, por exemplo, um fornecedor, cliente, freelancer ou consultor externo	• Ser convidado para quadros compartilháveis • Atuar como os membros	• Visualizar informações em quadros principais ou privados

Restrições de endereço IP

Os administradores podem predefinir um conjunto de endereços IP permitidos, que poderão acessar sua conta. Isso possibilita que você restrinja o acesso à conta para usuários em contextos específicos, como aqueles que participam a partir de uma localização específica (por exemplo, do escritório) ou usando uma VPN determinada. Todo usuário que tentar efetuar login com um endereço IP que não corresponda àqueles na lista de permissão receberá uma mensagem de erro e não poderá prosseguir.
Esse recurso está disponível apenas para clientes do plano Corporativo.

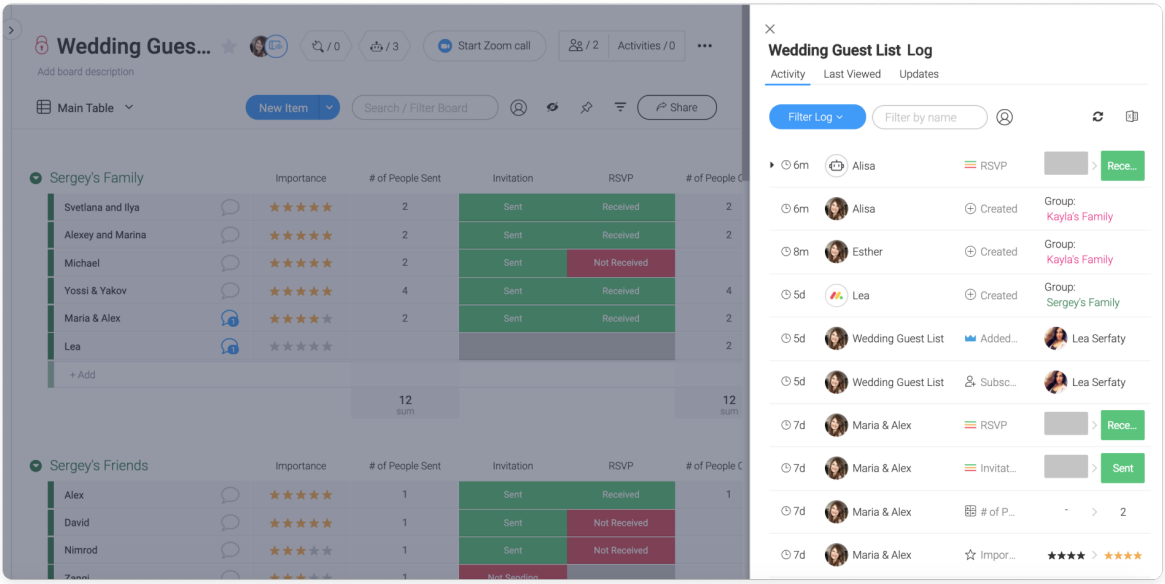


Logs

Log de atividades

Há dois tipos de log de atividades:

1. **O log de atividades do quadro** exibe todas as atividades prévias dele em uma lista, incluindo datas de alterações, status, movimentos entre grupos, automações e permissões. As informações exibidas no log de atividades do quadro variam de acordo com o seu nível: o plano Básico guarda somente as atividades da semana anterior; o plano Padrão guarda dados de atividades por 6 meses; enquanto os planos Profissional e Corporativo guardam por até 1 ano.

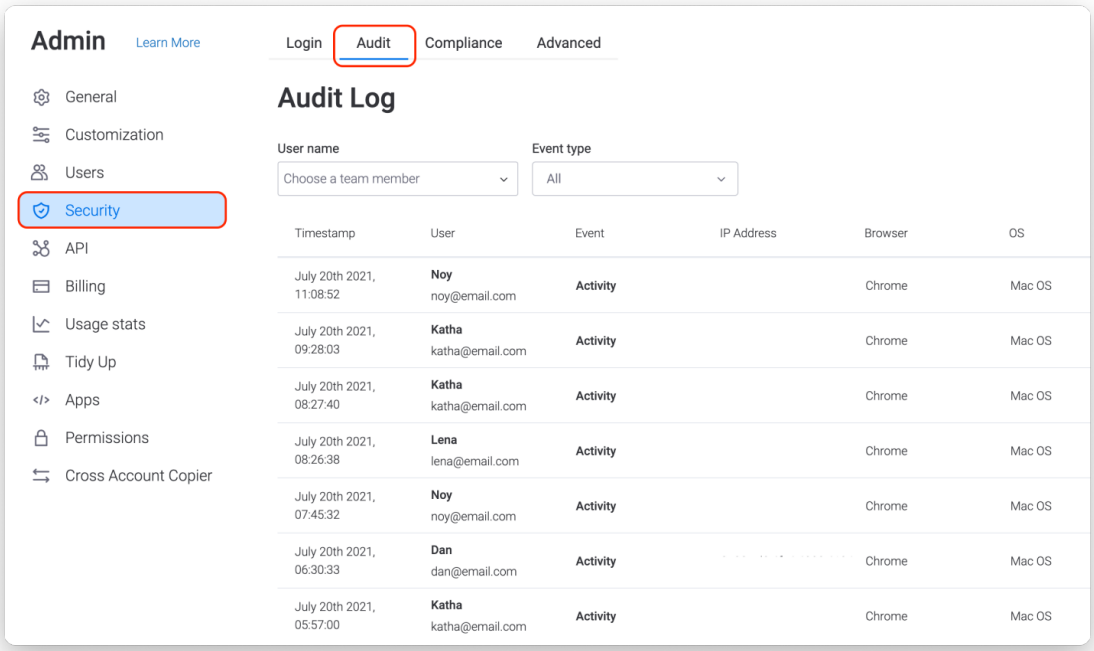


2. **O log de atividades do item** registra todas as atualizações feitas em um item individual. Nele você pode ver um histórico completo das atualizações do respectivo item e exatamente quando ocorreram. Todas as atualizações são organizadas das mais recentes às mais antigas. Você pode definir um lembrete de alerta em qualquer atualização.

É possível exportar facilmente seu log de atividades do item ou do quadro para o Excel com o simples clique em um botão.

Log de auditoria

O log de auditoria oferece aos administradores da conta um relatório detalhado de todas as atividades da conta relacionadas à segurança. Nessa seção, você pode ver quando os usuários efetuaram login e logout da conta pela última vez, de qual dispositivo e seu endereço IP na sessão. Assim, é possível monitorar qualquer atividade suspeita e ativar o modo pânico se necessário.
O log também exibe eventos potencialmente vulneráveis, como falhas de login, anexos baixados e dados de quadro exportados. Esse recurso está disponível somente para clientes do plano Corporativo.



Interoperabilidade e portabilidade

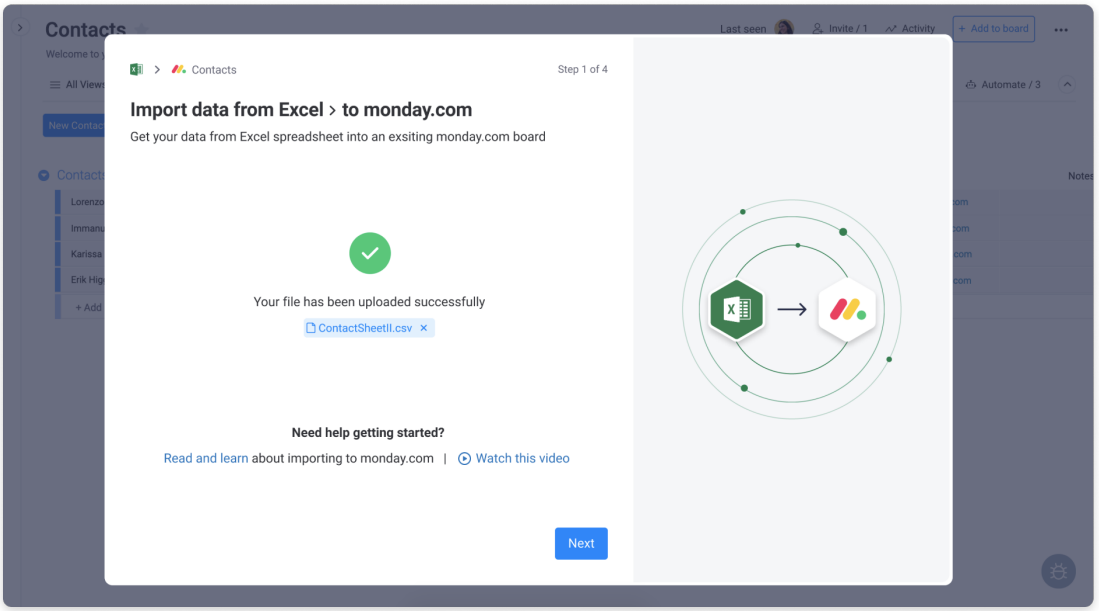
Integrações

A monday.com é compatível com integrações com várias outras soluções de software para criar fluxos de trabalho personalizados. Você pode conectar a monday.com às ferramentas que já utiliza para gerenciar todo o trabalho da sua equipe em um único lugar.
As integrações são opcionais e podem ser desativadas através do painel do administrador.

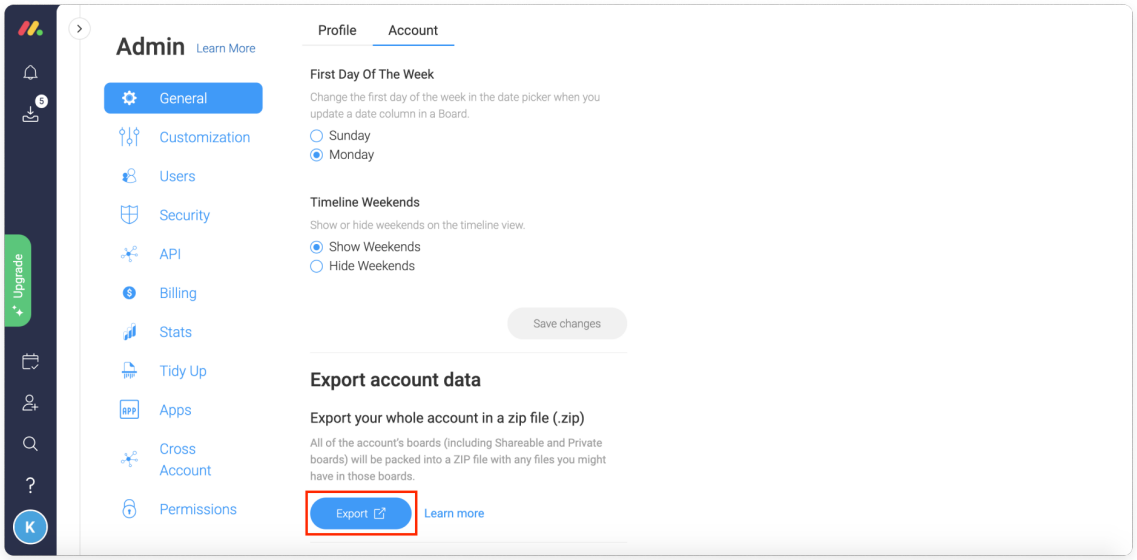
Importação e exportação para o Excel

A monday.com oferece aos clientes duas capacidades de gerenciamento de dados:

1. Transformar os dados de uma planilha do Excel em um quadro da monday.com (novo ou existente).



2. Exportar os dados da monday.com:
   a. Exportar quadros para o Excel
   b. Exportar todos os dados da conta através do painel do administrador. Isso exportará um arquivo zip contendo as planilhas do Excel e os arquivos enviados para a conta.

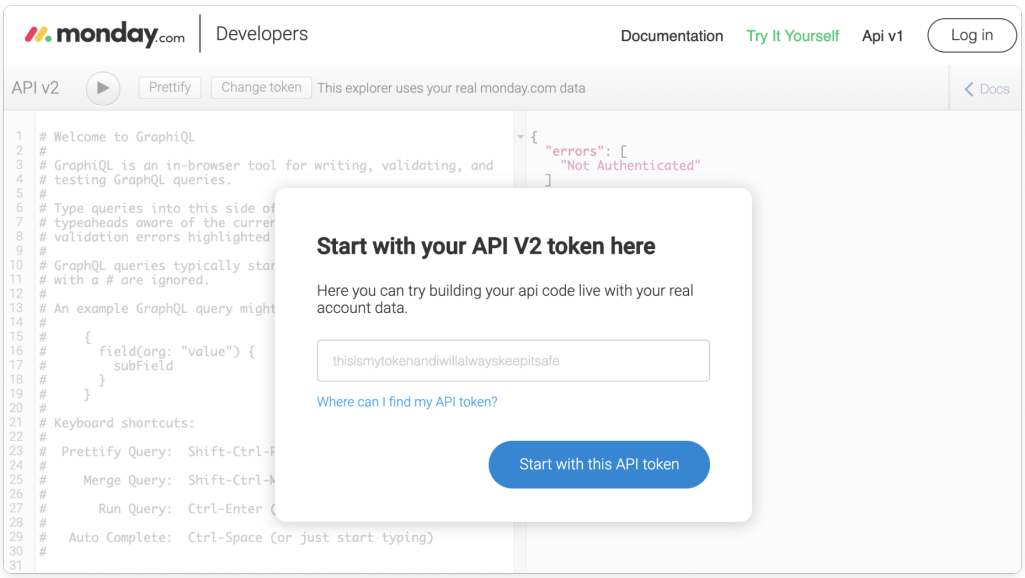


API

A monday.com oferece uma API GraphQL. Ela faz parte do framework de apps da monday e possibilita que os desenvolvedores acessem e atualizem programaticamente os dados de suas contas na monday.com.

Casos de uso da API:

- Acessar dados de quadros para renderizar um relatório personalizado dentro de um painel da monday.com
- Criar um item em um quadro quando um registro for criado em outro sistema
- Importar dados de outra fonte, programaticamente



O painel do administrador

No painel do administrador, os administradores da sua conta podem gerenciar tudo, incluindo configurações de segurança, usuários na conta, personalização da conta, cobrança e mais.

Domínio autorizado

Os administradores podem escolher entre duas configurações:

1. Somente administradores podem convidar membros e visualizadores para a conta, de qualquer domínio de e-mail.
2. Os administradores podem determinar um domínio de e-mail a partir do qual os usuários podem inscrever-se na conta.

Bloqueio de domínio de e-mail

Os administradores podem impedir os usuários de criarem contas na monday.com a partir de domínios de e-mail específicos. Esse recurso é útil para evitar contas redundantes na monday.com na mesma organização, especialmente aquelas que possuem múltiplos domínios corporativos, o que pode ter implicações na manutenção da conformidade às regras de governança de dados corporativos.

Para bloquear a criação de novas contas, os domínios de e-mail podem ser enviados ao serviço monday.com para análise e confirmação de propriedade. Eles serão encaminhados aos administradores da conta para integração na conta principal da organização.
Esse recurso está disponível apenas para clientes do plano Corporativo.

Modo pânico

Ao ativar o modo pânico, você bloqueará temporariamente a sua conta. Ninguém poderá acessá-la até que o administrador da conta envie uma solicitação à nossa equipe de sucesso do cliente. Esse recurso é crucial se as credenciais de login de um dos membros da sua equipe forem comprometidas.
Esse recurso está disponível apenas para clientes do plano Corporativo.

Gestão de sessão

Na seção de segurança do painel do administrador, os administradores podem clicar na aba de sessões para visualizar os dados de sessão de todos os usuários, a fim de controlar e redefinir qualquer delas.
Esse recurso está disponível apenas para clientes do plano Corporativo.

Geração de tokens de API

Somente os administradores podem conceder permissões para gerar tokens pessoais da API GraphQL em sua conta (para todos, somente administradores ou ninguém). Isso evita que os usuários gerem tokens da API e os compartilhem por engano com ferramentas terceirizadas, ou mesmo os publicizem ao enviá-los ao repositório público e exponham dados sigilosos da conta. O usuário que não puder gerar tokens receberá um aviso.
Esse recurso está disponível apenas para clientes do plano Corporativo.

Diretório de conteúdo

No diretório de conteúdo, você encontrará uma visão geral de todas as áreas de trabalho, quadros, painéis e documentos de trabalho localizados na conta. Além disso, para cada um desses recursos, você poderá ver seus proprietários, inscritos, dada de criação, data da última atualização e se está ou não disponível publicamente para o restante dos membros da conta.

* Por favor, observe que este informe não contém uma lista completa dos recursos gerenciados através do painel do administrador. É possível encontrar informações adicionais em nossos artigos de suporte.
Outros recursos gerenciados pelos administradores da conta podem ser cobertos em capítulos diversos neste documento, por exemplo, login, autenticação de dois fatores, provisionamento SCIM, permissões, restrição de endereço IP, logs de auditoria, tokens de API e configuração de conformidade HIPAA.

---

4. Segurança de aplicação

Ciclo de vida do desenvolvimento seguro de software (S-SDLC)

- A monday.com usa a metodologia OWASP Top 10 para aumentar a segurança em nosso ciclo de vida do desenvolvimento seguro de software (S-SDLC).
- Todos os códigos são analisados estaticamente (SAST) e revisados por pares como parte do processo de CI/CD para garantir a qualidade do código, antes de seu desenvolvimento para produção.
- Os testes dinâmicos de segurança da aplicação (DAST) são realizados, no mínimo, uma vez por semana.
- Colocamos ênfase especial em escrever testes dedicados a novos recursos lançados, enquanto recursos mais antigos vêm sendo postos à prova há muitos anos.
- Avaliamos e monitoramos continuamente nossa aplicação quanto a vulnerabilidades durante e após a implantação.
- Todas as bibliotecas de terceiros do lado do servidor são automaticamente verificadas quanto à divulgação pública de vulnerabilidades usando uma ferramenta de análise de composição de software (SCA).

Firewall de aplicação web (WAF)

Um firewall de aplicação web (WAF) se encontra habilitado para filtrar, monitorar e bloquear tráfego a nível de aplicativo, a fim de defender contra ataques conhecidos.

Gestão de vulnerabilidades

As vulnerabilidades são centralizadas em um backlog de desenvolvimento e são classificadas com base em nossa avaliação de seu impacto na confidencialidade, integridade e disponibilidade do serviço e dos dados do cliente. A classificação de gravidade da vulnerabilidade é determinada pelo sistema de pontuação de vulnerabilidades comuns (CVSS).

Security champions

Nossa comunidade interna de security champions inclui desenvolvedores de todas as equipes de P&D. Os security champions recebem treinamento avançado em segurança e são qualificados para oferecer orientação de segurança e realizar revisões de segurança em códigos, sempre que necessário.

Teste de penetração

O teste de penetração de aplicação é realizado anualmente, todo ano por terceirizada diferente e independente, incluindo métodos manuais e automáticos de teste.
Além disso, nossa equipe de segurança de aplicação interna realiza regularmente auditorias de segurança e testes de penetração em vários recursos, o que exige conhecimento profundo dos nossos mecanismos e arquitetura de segurança interna.
Como parte dos nossos testes externos e internos de penetração, são usadas ferramentas de varredura de rede em nossos servidores de produção.

Programa de caça aos bugs

A monday.com mantém um programa privado de caça aos bugs no HackerOne, gerenciado internamente, que permite a pesquisadores de segurança do mundo todo trabalhar de forma ética e responsável na busca e divulgação de vulnerabilidades de segurança para nossa equipe de segurança. Alguns recursos recebem destaques especiais no HackerOne para focar a pesquisa e esforços da comunidade de segurança nessas áreas.

Como parte do programa, mantemos um placar do hall da fama para os hackers.

---

5. Segurança de TI

Segurança de terminal

Todas as estações de trabalho dos funcionários são protegidas por uma solução EDR com gerenciamento centralizado para detecção e quarentena de malwares. Nossa solução EDR é monitorada continuamente por uma equipe gerenciada do SOC, 24 horas por dia, o ano todo.
Todas as estações de trabalho são criptografadas através de FileVault/BitLocker, protegidas por senha e com limite de tela ociosa definido em 10 minutos.
Além disso, podemos aplicar patches e limpar remotamente uma máquina através do gerenciador de dispositivos.

Política de senhas

Nossa política interna de senhas estabelece que elas devem ter, no mínimo, 12 caracteres e conter o seguinte:

1. Letra maiúscula
2. Letra minúscula
3. Número
4. Símbolo

Usa-se uma solução corporativa de gerenciamento de senhas, alteram-se regularmente as senhas padrão, não é tecnicamente permitido usar senhas comuns ou reusar as anteriores, e as senhas expiram após 120 dias.

Gestão de identidade e acesso

O acesso aos sistemas é concedido pela nossa equipe de TI com base na função, através da nossa solução de provedor de identidade (IdP) corporativa, conforme determinado pelo RH e de acordo com os princípios da necessidade de saber e do menor privilégio.
O acesso do usuário é modificado dentro de até 24 horas após alterações na relação de emprego ou rescisão contratual. Além disso, são realizadas revisões de acesso dos usuários trimestralmente para garantir a adequação dos privilégios de acesso. Todo acesso que não seja mais necessário é removido e documentado.

Proteção de e-mail

A monday.com usa o Google Workspace como nosso provedor de e-mail, que é protegido por retransmissão terceirizada das mensagens. DMARC e SPF estão habilitados. Os funcionários têm sido instruídos continuamente em relação às melhores práticas para evitar phishing e testes são realizados com regularidade.

Pontos de acesso sem fio

A monday.com usa tecnologias padrão da indústria para garantir que as comunicações sem fio em nossa sede sejam seguras. Usamos WPA2 Enterprise, dentre outras ferramentas, para assegurar o desprovisionamento oportuno e o não repúdio em toda a rede, além de termos habilitado o monitoramento de APs não autorizados.

6. Segurança operacional

Acesso aos dados dos clientes
A monday.com trata todos os dados enviados pelos clientes ao serviço monday.com, os quais são processados exclusivamente por nós em nome do cliente, como uma "caixa preta". Isso significa que, geralmente, os dados do cliente não são acessados para a prestação do serviço monday.com, e que tratamos todos os dados enviados pelo cliente com o mais alto nível de sensibilidade e confidencialidade.
O acesso aos dados do cliente pela monday.com é limitado de acordo com os nossos termos de serviço ou contrato respectivo com o cliente, caso a caso.

Recursos humanos
Verificação de antecedentes
Nossa sede é localizada em Israel, onde verificações de antecedentes não são habituais e são limitadas pela lei. As verificações que realizamos incluem histórico de trabalho e ligações para referências com gerentes diretos anteriores.

Contrato de emprego
Todos os contratos de emprego da monday.com contêm cláusulas de confidencialidade e previsões que permitem a rescisão imediata pela violação de alguns deveres ou por determinadas ações.
Além disso, a monday.com mantém uma política de segurança de RH que define as atividades e responsabilidades de segurança exigidas durante o período de emprego, do recrutamento à saída.

Uso aceitável
A monday.com mantém uma política de uso aceitável que é revisada anualmente pela nossa equipe de segurança e pelo fórum de segurança mais amplo. Nossos funcionários têm por obrigação assinar a política durante a integração ou em caso de uma alteração substancial da política.

Treinamento e conscientização
Como parte do processo de integração inicial e, no mínimo, uma vez ao ano depois disso, os funcionários da monday.com recebem treinamento relativo às obrigações de segurança da informação e de privacidade que devem cumprir. O treinamento inclui tutoriais, bem como tarefas escritas, e é monitorado pela equipe de segurança.
As semanas de segurança e privacidade trimestrais são promovidas para aumentar ainda mais a conscientização entre os funcionários.
Além disso, são realizadas sessões de treinamento dedicadas, conforme necessário (por exemplo, os desenvolvedores passam por treinamento de código seguro).

Rescisão do contrato de trabalho
O acesso do usuário é modificado dentro de até 24 horas após alterações na relação de emprego ou rescisão contratual, com a devolução dos equipamentos da empresa. São realizadas revisões de acesso do usuário trimestralmente para garantir a adequação dos privilégios de acesso.

Red team assessments
Duas vezes ao ano, realizamos red team assessments em nossa postura defensiva, incluindo testes internos de penetração, ataques à infraestrutura e simulação de violação em curso. Os red team assessments são realizados pelas principais empresas terceirizadas de consultoria em segurança ofensiva e defensiva, as quais usam técnicas de ataque de alta tecnologia e sofisticação, oferecendo visibilidade única dos nossos potenciais riscos e vulnerabilidades de segurança.

Governança e gestão de riscos
A monday.com mantém um processo contínuo de gestão de riscos destinado a identificar de forma proativa vulnerabilidades em seus sistemas e avaliar novas ameaças emergentes contra as operações da empresa. A monday.com passa por uma avaliação de risco como parte da certificação ISO 27001, realizada anualmente.

Respostas e gestão de incidentes
O plano de resposta a incidentes (IRP) da monday.com define as diretrizes para detectar incidentes de segurança e privacidade, encaminhando-os a níveis superiores para o pessoal pertinente, comunicação (interna e externa), mitigação e análise post-mortem.
A equipe de resposta a incidentes (IRT) da monday.com inclui representantes da segurança, P&D, jurídico, representantes de outras equipes caso a caso e, se necessário, uma empresa terceirizada de resposta a incidentes.

Notificação
De acordo com os termos da seção 7 do nosso adendo de processamento de dados ("gestão e notificação de incidente de dados"), depois de se tornar ciente de um incidente de dados, a monday.com notificará os clientes afetados sem atraso indevido.
Os clientes afetados serão informados da natureza da violação, dos efeitos prejudiciais dos quais a monday.com está ciente, das ações que tomou e dos planos para reparar ou mitigar o incidente no momento da notificação.

Recuperação de desastres e continuidade dos negócios
A monday.com mantém um plano de continuidade dos negócios alinhado à ISO 27001 para lidar com desastres que afetem nosso escritório físico (onde nenhuma parte da nossa infraestrutura de produção é mantida).
Além disso, mantemos um plano de recuperação de desastres (DRP) para lidar com os que afetem nosso ambiente de produção, o que inclui a restauração da funcionalidade básica do serviço a partir de nossa localização dedicada de DR. Os testes são realizados, no mínimo, duas vezes por ano. O teste de DR da monday.com pode dar-se na forma de um passo a passo, desastre simulado ou teste de componentes.

Retenção e descarte de dados
Retenção de dados
A monday.com reterá suas informações controladas por ela pelo período necessário ao cumprimento das finalidades descritas em nossa política de privacidade. Os dados que a monday.com processa em nome dos nossos clientes serão retidos de acordo com os nossos termos de serviço, nosso adendo de processamento de dados e outros contratos comerciais com os respectivos clientes.

Exclusão de dados

Os clientes da monday.com detêm controle total dos dados enviados e podem modificá-los, exportá-los ou excluí-los a qualquer momento usando os meios disponibilizados através da interface de usuário do serviço.
Após o cancelamento ou expiração de sua assinatura, os clientes podem solicitar a exclusão de seus dados como parte do procedimento de fechamento da conta. Os dados dos clientes serão então excluídos dentro de 90 dias da data da solicitação, o que inclui um período de 30 dias que permite a reversão e 60 dias adicionais para prosseguir com o processo de exclusão.
Alternativamente, os clientes podem optar por manter os dados da conta na plataforma, caso em que poderemos continuar retendo-os, mas também poderemos excluí-los a qualquer momento, a nosso critério.

Destruição de dados

Nossos serviços são hospedados na AWS, com o backup de alguns dados para o GCP. Ambos os provedores de computação na nuvem implementam estratégias proprietárias de distribuição e exclusão de dados para possibilitar o armazenamento seguro de dados sigilosos em um ambiente multi-tenant. O descomissionamento de mídias de armazenamento é realizado pelos provedores mencionados acima usando as técnicas detalhadas no NIST 800-88.

Monitoramento e logs

A monday.com coleta e monitora logs de rede usando um sistema de detecção de intrusão de rede (NIDS), logs de tráfegos oriundos de localizações de ponta, logs a nível de aplicação para rastrear e auditar eventos, além de logs a nível de sistema para auditar o acesso e operações de alto privilégio. Os logs são transmitidos dentro da nossa solução de segurança da informação e gestão de eventos (SIEM), onde são continuamente (24/7/365) monitorados pela equipe gerenciada do SOC.

Gestão de cadeia de suprimento

Subprocessadores

A monday.com exige que seus subprocessadores (tanto na região de dados global quanto na região de dados da UE) cumpram os padrões da indústria com relação à segurança e privacidade de dados, e considera ambas as áreas críticas no processo de seleção de seus subprocessadores. Entre outras medidas, asseguramos que os adendos de processamento de dados e outras documentações e salvaguardas relevantes estejam em vigor com todos os nossos subprocessadores. Também realizamos avaliações de privacidade, do aspecto jurídico e da informação, bem como auditorias baseadas em questionários, tudo de acordo com os padrões da indústria e requisitos regulatórios. As avaliações de nossos subprocessadores são realizadas, no mínimo, uma vez por ano.

Gestão de fornecedores

A monday.com mantém um programa central de gestão de ativos de repositório tanto para os serviços quanto para os softwares que utilizamos. O ativo de repositório é mantido continuamente pelas nossas equipes de segurança, jurídico, privacidade e aquisições, e o processo de aprovação é comunicado a todos os funcionários.
Com o início do uso e renovação dos serviços e softwares, as diversas equipes categorizam os fornecedores com quem trabalhamos de acordo com o nível mais alto de sensibilidade de dados a que têm acesso, a fim de determinar seu nível adequado de risco e revisá-lo de acordo com os padrões da indústria e requisitos regulatórios.

Segurança física

Escritórios da monday.com

Os ativos físicos de TI nos escritórios da monday.com se limitam a notebooks e dispositivos da rede do escritório. Os dispositivos da rede do escritório são protegidos em uma sala de servidor trancada por senha, monitorada ininterruptamente por CCTV em ambiente controlado. O acesso físico aos escritórios é controlado através de identificação biométrica. Os visitantes iniciam sessão ao entrar em nossos escritórios e precisam ser escoltados a todo momento por um funcionário da monday.com durante sua permanência no local. Todos os funcionários devem relatar atividades suspeitas, acesso não autorizado às instalações e incidentes de roubo ou perda de objetos.

Segurança dos centros de dados

A monday.com confia nas medidas de segurança de classe mundial da AWS e GCP em questão de segurança física e do ambiente, as quais resultam em uma infraestrutura altamente resiliente. Para mais informações sobre essas práticas de segurança, por favor, visite os links a seguir: https://aws.amazon.com/security/, https://cloud.google.com/security/

---

7. Conformidade, privacidade e certificações

Garantia e conformidade de auditoria

A monday.com desenvolveu seus programas de segurança e privacidade respeitando os diversos programas de conformidade padrão da indústria, além das principais regulações de proteção de privacidade e dados em territórios onde nosso serviço é oferecido:

ISO 27001, 27017, 27018, 27032 e 27701

A monday.com segue os padrões internacionais da ISO (Organização Internacional de Padronização) e gerencia sua segurança da informação, serviços na nuvem e privacidade em conformidade. Somos auditados anualmente por terceiros independentes e mantemos 5 certificações ISO:

- **A ISO/IEC 27001:2013** é o padrão de segurança mais rigoroso do mundo para sistemas de gestão de segurança da informação (ISMS).
- **A ISO/IEC 27018:2014** estabelece objetivos de controle, controles e diretrizes comumente aceitas na implementação de medidas para proteger informações de identificação pessoal (PII), de acordo com os princípios de privacidade no ISO/IEC 29100 para ambientes de computação na nuvem.
- **A ISO/IEC 27017:2015** oferece controles e orientação de implementação tanto para provedores quanto para clientes de serviços na nuvem. Ela oferece diretrizes para controles de segurança da informação aplicáveis à provisão e uso de serviços na nuvem ao oferecer orientação adicional para a implementação dos controles relevantes.
- **A ISO/IEC 27032:2012** oferece orientação para melhorar o estado da cibersegurança, destacando seus aspectos únicos e suas dependências em outros domínios da segurança, em particular: segurança da informação, segurança de rede, segurança da internet e proteção da infraestrutura de informações críticas (CIIP).
- **A ISO/IEC 27701:2019** especifica os requisitos e oferece orientação para estabelecer, implementar, manter e continuamente melhorar o sistema de gestão de informações de privacidade (PIMS).

Todas as nossas certificações podem ser encontradas aqui.

SOC 1, SOC 2 e SOC 3

A monday.com alcançou controles de organização e serviço:

- **Auditoria SOC 1 tipo II**, que examina os controles que podem ser relevantes para o relatório financeiro de clientes.
- **Auditoria SOC 2 tipo II**, que demonstra nosso compromisso em atender aos rigorosos padrões de segurança, disponibilidade e confidencialidade da indústria. Ela confirma que os controles de segurança da monday.com estão de acordo com os princípios e critérios de serviços de confiança do AICPA (Instituto Americano de Contadores Públicos Certificados) e requisitos de segurança da HIPAA.
- **Relatório SOC 3**, que é uma versão mais breve do nosso relatório SOC 2 tipo II e é disponibilizada ao público.

As auditorias são realizadas anualmente por terceiros independentes, com emissão anual de um relatório que cobre os meses de abril a março.
Os relatórios de SOC da monday.com podem ser encontrados nos links a seguir: SOC 1, SOC 2 e SOC 3.

Cloud Security Alliance (CSA)

A Cloud Security Alliance (CSA) é uma organização sem fins lucrativos com a missão de "promover o uso das melhores práticas no oferecimento de garantia de segurança dentro da computação na nuvem, além da educação sobre os usos da computação na nuvem para ajudar a proteger todas as outras formas de computação".
A monday.com participa na autoavaliação voluntária da CSA de registro de segurança, confiança, garantia e risco (STAR) para documentar nossa conformidade com as melhores práticas publicadas pela CSA. Nosso questionário da iniciativa de avaliação de consenso (CAIQ) da CSA é gratuito e está disponível ao público no site da CSA.

The Health Insurance Portability and Accountability Act (HIPAA)

A Health Insurance Portability and Accountability Act (HIPAA) foi concebida para ajudar a proteger dados de saúde. Organizações como hospitais, consultórios médicos, planos de saúde ou empresas que lidam com informações de saúde protegidas (PHI) são obrigadas a cumprir a HIPAA. Isso também pode estender-se para empresas que trabalham com esses negócios e entram em contato com PHIs em seu nome.
A monday.com oferece aos seus clientes do plano Corporativo uma configuração de conta em conformidade com a HIPAA, de modo que os clientes possam enviar suas informações de saúde sigilosas. Nossos clientes abrangidos pela HIPAA precisam assinar nosso acordo de associado comercial (BAA) para garantir a proteção e o processamento adequado de PHIs em seu nome, antes do envio de dados protegidos pela HIPAA.

monday.com e a LGPD

Nosso programa global de privacidade se baseia nas regulamentações de proteção de dados mais abrangentes e avançadas do mundo, tendo como "norte" a lei geral de proteção de dados (LGPD) da UE e UK.
Entre outras coisas, o fórum de privacidade da monday.com monitora continuamente os desenvolvimentos de produtos e processos em toda a nossa organização, bem como as diversas atividades que envolvem o uso de dados pessoais, a fim de assegurar que os princípios da LGPD sejam respeitados, por exemplo, os princípios de Privacy by Design, minimização de dados e limitação de armazenamento, legalidade e equidade no processamento, além de transparência em nossas atividades e finalidades.

Política de privacidade

A política de privacidade da monday.com pode ser encontrada aqui. Ela descreve nossas práticas de privacidade e processamento de dados em relação aos dados pessoais que processamos para nossas próprias finalidades como controladora de dados.

Adendo de processamento de dados (DPA)

Os termos de serviço da monday.com e os contratos com o cliente contêm um adendo de processamento de dados para garantir a proteção e processamento adequado dos dados pessoais em nome do nosso cliente. Você pode visualizar e assinar nosso adendo de processamento de dados (DPA) on-line.

Transferências transfronteiriças de dados pessoais

A monday.com tem sua sede em Israel, com subsidiárias localizadas nos Estados Unidos, Reino Unido, Austrália e Brasil, tendo equipes de suporte na Ucrânia e Guatemala. Nossos subprocessadores também estão registrados em diversos países, conforme detalhado em nossa página de subprocessadores.

Quando transferimos dados pessoais do EEE e Reino Unido para outros países, confiamos nos mecanismos lícitos de transferência oferecidos sob a LGPD, tais como as "decisões de adequação" tomadas pela Comissão Europeia (por exemplo, as decisões que consideram que o Reino Unido e Israel oferecem um nível adequado de proteção aos dados pessoais oriundos da União Europeia) e as cláusulas contratuais padrão da União Europeia, que podem ser encontradas aqui e aqui.

Controladores e processadores

A LGPD define e distingue entre duas funções principais em se tratando da coleta e processamento de dados pessoais: controlador de dados e processador de dados. O primeiro determina os meios e finalidades do processamento de dados pessoais, enquanto o segundo é a parte que processa os dados em nome do controlador.

- A monday.com é a controladora dos dados pessoais relacionados aos seus clientes, usuários e visitantes do site. Isso é explicado em mais detalhes em nossa política de privacidade.
- A monday.com é a processadora dos dados pessoais que seus clientes e usuários enviam à plataforma (em quadros e itens dentro de sua conta na monday.com), e processa esses dados em nome de seus clientes. Isso é feito de acordo com o adendo de processamento de dados celebrado com os nossos clientes. Os prestadores de serviços terceirizados que usamos para nos ajudar a processar esses dados são nossos "subprocessadores".

monday.com e a CCPA

Como "prestadora de serviços", a monday.com tem o compromisso de cumprir os requisitos aplicáveis estabelecidos pela California Consumer Privacy Act of 2018 (CCPA) e as regulamentações do procurador-geral da Califórnia, à luz de regulamentações mundiais semelhantes (como a LGPD) e padrões da indústria em evolução, a fim de garantir que nossos clientes possam continuar usando a monday.com sem interrupção e possamos processar informações pessoais de clientes da Califórnia em conformidade com a CCPA.

Mais informações podem ser encontradas aqui.

Australian Privacy Act (APA) e Australian Privacy Principles (APP)
Australian Privacy Act (APA) e Australian Privacy Principles (APP) estabelecem um framework estruturado para coletar, processar, usar e compartilhar informações pessoais, dando às pessoas maior controle sobre a forma como suas informações são tratadas. A monday.com tem o compromisso de cumprir os requisitos da APA e APP.
Mais informações podem ser encontradas aqui.

Auditorias internas
Nossas equipes de segurança, privacidade, infraestrutura, P&D, TI, operações e jurídico promovem trimestralmente as semanas de segurança e privacidade, que incluem a realização de diversas atividades de auditoria, incluindo revisões de acesso dos usuários, revisões de configuração de firewall, inspeções de mesa limpa, treinamento e atividades de conscientização e mais.

Divulgação para autoridades públicas

A monday.com não permite que as autoridades públicas acessem injustificadamente os dados que temos dos clientes. Raramente recebemos pedidos de autoridades (nos EUA ou em outros lugares) para divulgar dados dos clientes. As poucas ocasiões em que recebemos esses pedidos em anos anteriores foram limitadas em escopo e traziam fundamentos legítimos para requerer os respectivos dados (por exemplo, suspeita de atividade ilegal relacionada a uma conta em particular).
Após o pedido ser analisado pelas nossas equipes jurídica e de privacidade para garantir sua validade e justificação, a divulgação se limitaria aos dados estritamente necessários dentro da lei. Antes da divulgação, envidamos esforços comercialmente razoáveis para notificar nossos clientes, a menos que sejamos proibidos disso ou incapazes devido a um risco potencial.[3] Também temos o compromisso de empregar esforços comercialmente razoáveis para oferecer resistência, sujeito às leis aplicáveis, a qualquer pedido de vigilância em massa relacionada a dados pessoais protegidos pela LGPD da União Europeia ou do Reino Unido, incluindo as previsões da seção 702 da FISA.

PrivacyTeam e DPO

A monday.com é protegida pela PrivacyTeam, a principal consultoria em privacidade de Israel, e trabalha arduamente junto a ela para garantir que os dados e privacidade dos clientes estejam protegidos. Outras informações podem ser encontradas aqui.
A monday.com nomeou o Sr. Aner Rabinovitz – um veterano de privacidade da PrivacyTeam – como nosso diretor de proteção de dados, a fim de que monitore e oriente nossa constante conformidade de privacidade, além de atuar como ponto de contato para assuntos de privacidade perante sujeitos de dados e autoridades supervisoras.

---

[3] Outras informações podem ser encontradas na seção 4 (“compartilhamento de dados”) da nossa política de privacidade.

8. Conclusão

Este informe ofereceu uma visão ampla da abordagem de segurança e privacidade da monday.com. Naturalmente, dada a complexidade desses assuntos, é possível que você tenha outras perguntas.
Mais informações podem ser encontradas em nossa central de segurança e confiança e portal jurídico.
Para maiores esclarecimentos sobre a postura da monday.com quanto à segurança e privacidade, também é possível entrar em contato com nossas equipes através dos e-mails security@monday.com ou dpo@monday.com, além do suporte geral que é prestado 24 horas por dia, o ano todo, através do e-mail support@monday.com.
Deseja relatar uma preocupação ou vulnerabilidade de segurança? Fale conosco pelo e-mail security@monday.com ou relate através do nosso formulário HackerOne em https://monday.com/security/form/.

AVISO: Esta versão é uma tradução do original em inglês, fornecida apenas para fins de conveniência. O original em inglês é a versão oficial e juridicamente vinculante, e prevalecerá em caso de discrepância.