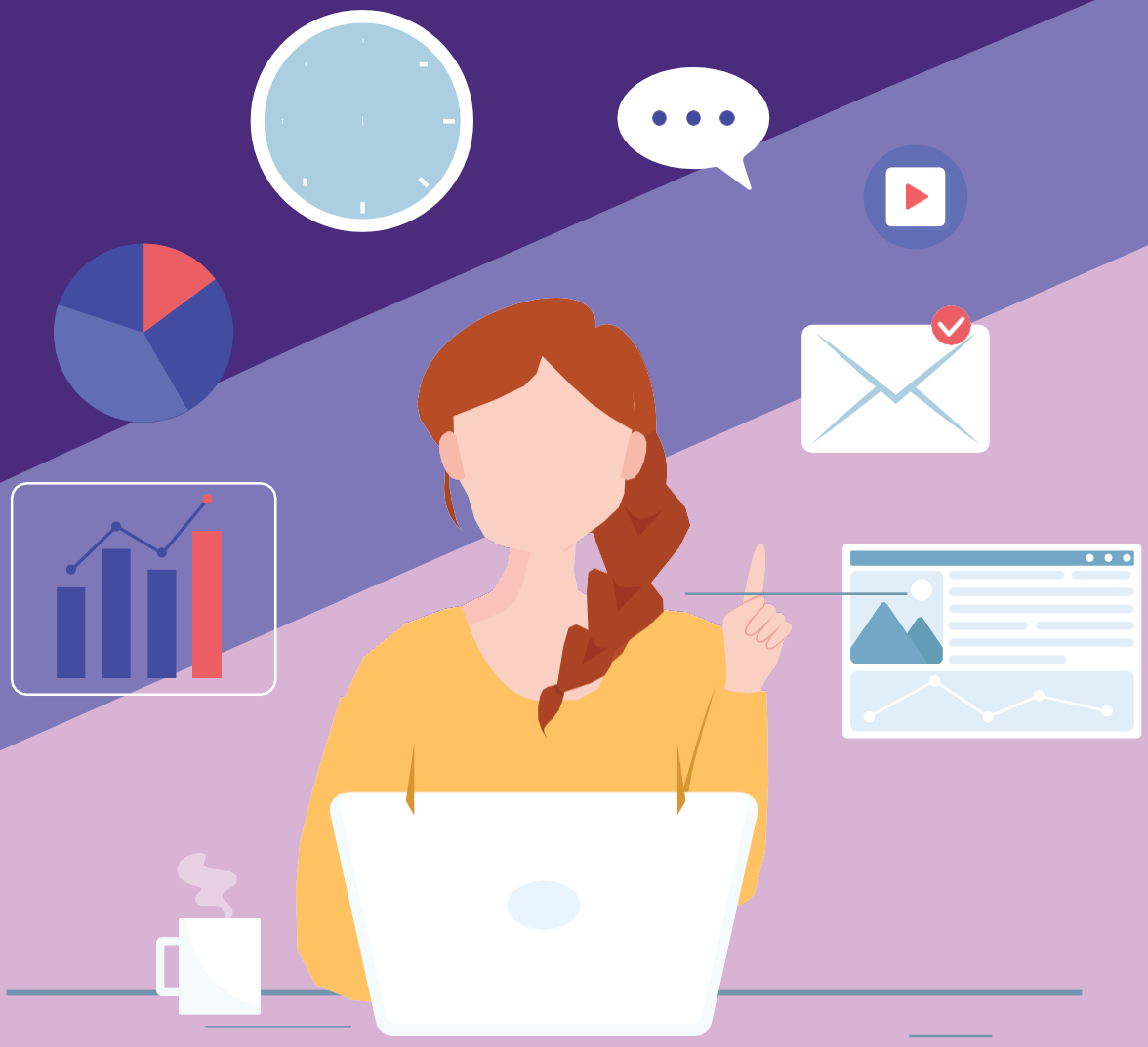
ManageEngine

# **Gerenciar** e **proteger** sua força de trabalho remota



Os funcionários remotos usam uma variedade de endpoints conectados à Internet para realizar seu trabalho, o que representa uma ameaça à postura geral de segurança de sua organização. Christopher Sherman, analista sênior da Forrester Research, diz: “Com grande parte da força de trabalho global passando a trabalhar remotamente, a segurança de endpoints nunca foi tão crítica.” Se os endpoints e os funcionários remotos não forem gerenciados de forma pertinente, sua organização estará em risco.

O gerenciamento e a segurança de endpoints moldarão o futuro do trabalho e estarão prontos para serem uma solução de longo prazo para o trabalho remoto. Dito isso, agora é o momento certo para verificar novamente os recursos de trabalho remoto e implementar algumas práticas recomendadas para impor o trabalho remoto adequado.

# Práticas recomendadas para proteger seus endpoints remotos

## Nem todas as vulnerabilidades precisam de patching imediato. Avalie-as!

Você pode estar inundado de vulnerabilidades, mas nem todas as vulnerabilidades requerem patching imediato. Automatize a avaliação de cada vulnerabilidade, configure a integridade de seus sistemas e implante patches quando for necessário.

## Teste cada patch antes de implantá-lo

É vital testar cada patch antes de deslocá-lo para máquinas, especialmente se for uma máquina instalada no servidor.

## Selecione uma lista de executáveis mal-intencionados e bloqueie-os completamente

Apesar de um sistema de segurança infalível, executáveis mal-intencionados ainda encontram seu caminho para as redes. Selecione uma lista de executáveis mal-intencionados e bloqueie-os completamente fornecendo o valor hash do executável.

## Agende e automatize atualizações do sistema operacional

Na maioria das vezes, os usuários tendem a ignorar as atualizações do SO. Os criminosos virtuais geralmente exploram vulnerabilidades conhecidas em SOs desatualizados para atacar o endpoint e usá-lo como um canal para atacar toda a rede. Sempre automatize as atualizações e programe a atualização para grupos específicos de usuários para evitar problemas de gargalo de banda.

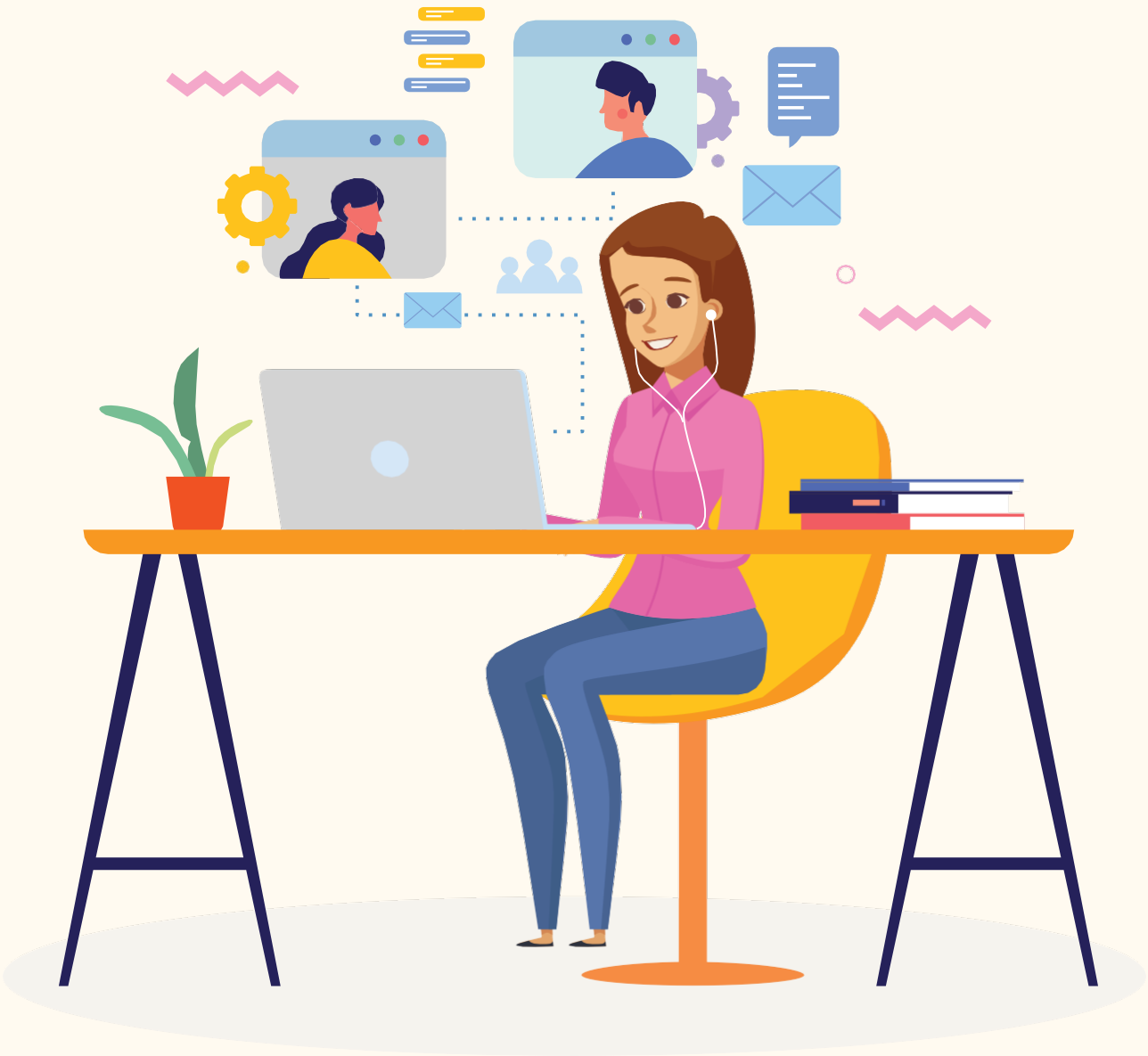
## Fazer auditoria de configurações incorretas de softwares e sistemas de alto risco

Procure a presença de softwares de alto risco, como software de fim de vida útil, ponto a ponto e de compartilhamento de área de trabalho remota. As configurações ignoradas e padrão abrem caminho para uma configuração incorreta que pode ser facilmente explorada. É fundamental auditar as configurações de maneira proativa para manter os ataques cibernéticos afastados.

## Configurar perfis para impor políticas rígidas em dispositivos móveis

Publique perfis para implementar políticas de Wi-Fi para impedir que dispositivos móveis ingressem automaticamente em redes Wi-Fi, definindo configurações de VPN para autenticar cada conexão com a rede corporativa e restringindo recursos do dispositivo, como Bluetooth e câmera.

# Práticas recomendadas para gerenciar seus usuários remotos



## Agrupe as configurações rudimentares como uma única coleção de configurações

Agrupe configurações de linha de base para proteger navegadores, USBs e firewalls; mapear drivers; gerenciar arquivos, pastas, permissões e energia; e padronização da exibição de monitores. Certifique-se de que todos os novos sistemas que ingressam no domínio tenham essas configurações em vigor.

## Adapte o processo de implantação de aplicações essenciais aos negócios

Certifique-se de que as versões recomendadas das aplicações de negócios estejam presentes em todos os endpoints. Personalize o processo de implantação de aplicações definindo atividades de pré-implementação, como verificar o espaço livre em disco e as versões instaladas anteriormente, e atividades pós-implantação, como criar um atalho.

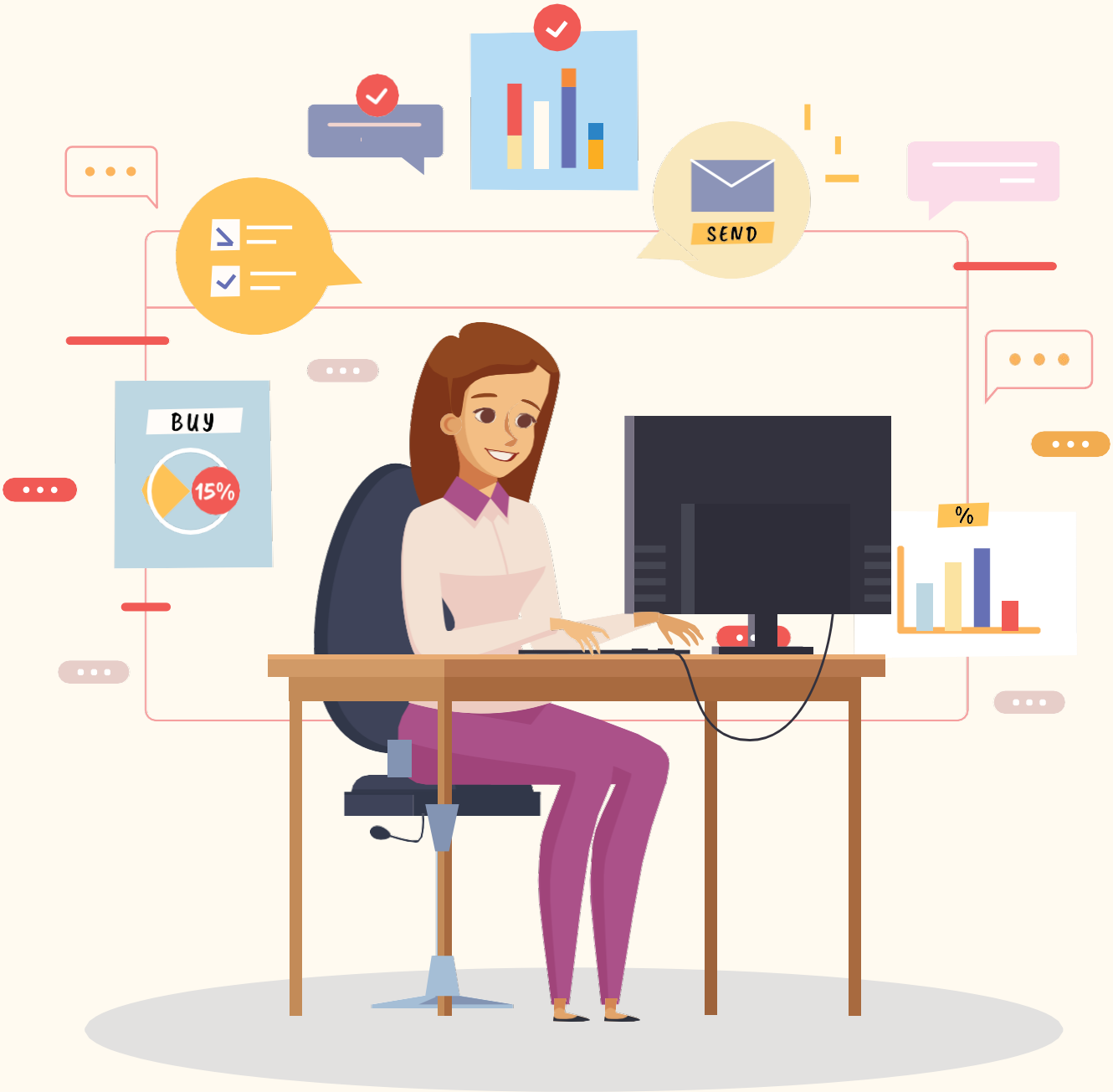
## Centralizar o gerenciamento dos complementos do navegador

Detecte a presença de complementos prejudiciais e desative extensões que usam permissões que podem levar à extração dos dados. Distribua extensões de um repositório central e identifique complementos desatualizados.

## Implantar políticas de delimitação geográfica apropriadas dependendo da localização dos dispositivos

Crie cercas virtuais e configure políticas de delimitação geográfica relevantes para determinar o grau de acesso aos dados corporativos, dependendo do local do endpoint remoto. Defina uma regra de conformidade e tome as medidas necessárias em dispositivos não compatíveis.

# **Práticas recomendadas** para garantir a produtividade



## Proibir o uso de aplicações na lista de bloqueios e desinstalá-las automaticamente

Compile uma lista de aplicações a serem incluídas na lista de bloqueios que dificultam a produtividade e instigam os problemas de conformidade durante o trabalho à distância. Desinstale-as automaticamente se forem detectadas e permita que os usuários façam uma solicitação se precisarem de acesso a qualquer aplicação específica.

## Capacitar os usuários para instalar ou desinstalar aplicações à sua disposição

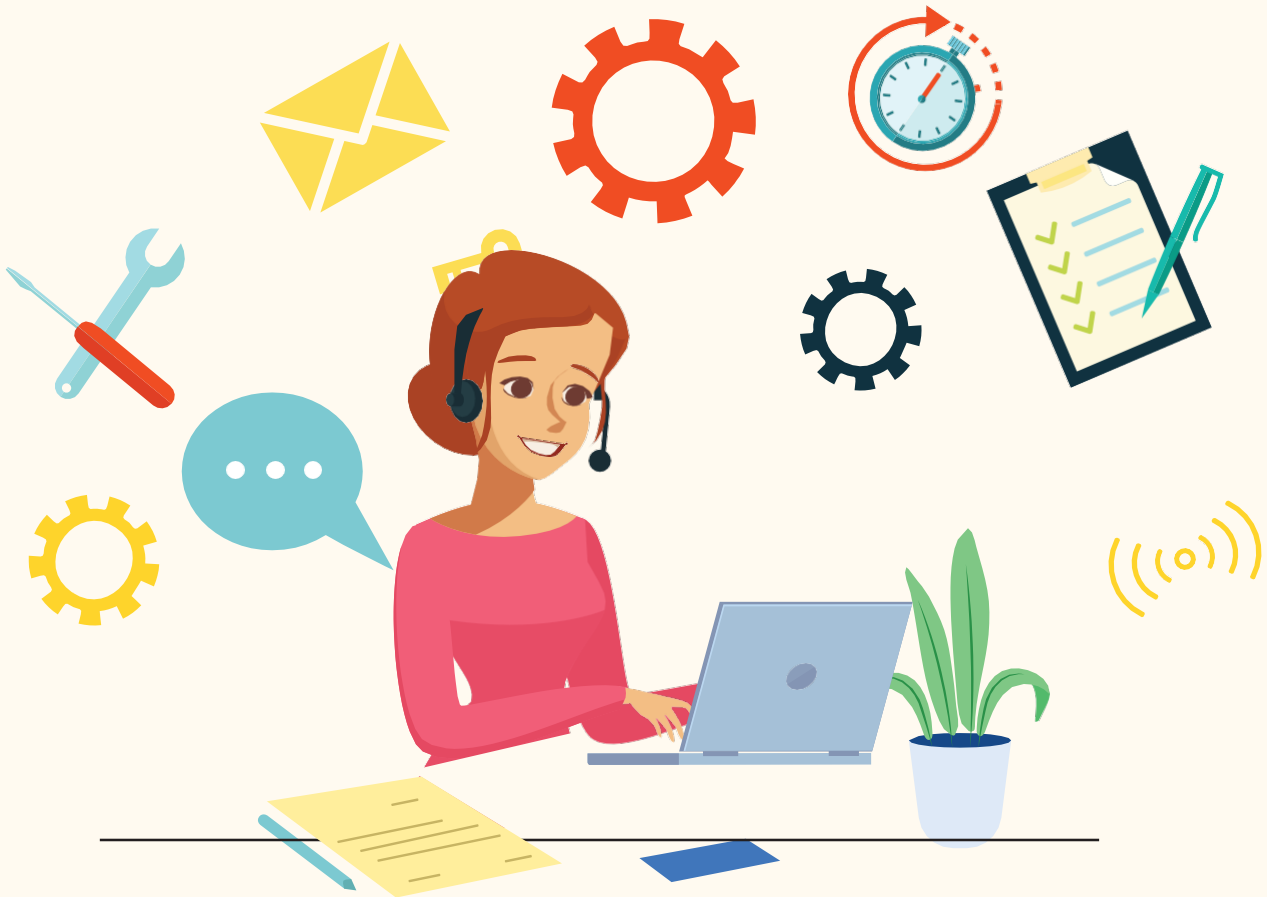
A instalação silenciosa de aplicações pode provar não ser uma dádiva durante o trabalho remoto, devido às bandas variáveis dos usuários. Em vez disso, publique software no portal de autoatendimento e capacite os usuários para instalar aplicações com base no que eles precisam e na banda disponível para eles.

## Monitorar a atividade na Web dos usuários e aplicar um filtro da Web para restringir o acesso

O uso da Internet é onipresente e tende a colocar os usuários fora de seu curso, onde eles podem começar a navegar em sites que não estão relacionados ao trabalho e podem ser mal-intencionados. Monitore a atividade na Web dos usuários e aplique um filtro da Web para restringir o acesso a sites improdutivos e mal-intencionados.

# Práticas recomendadas

## para resolução remota de problemas



## Transferir arquivos dependentes durante uma sessão ao vivo

Em vez de recorrer aos métodos tradicionais de transferência de arquivos, transfira os arquivos necessários para a máquina de destino durante a resolução de problemas. Você pode usar a ferramenta integrada de transferência de arquivos bidirecional para garantir que todos os arquivos dependentes estejam presentes na máquina de destino para uma resolução mais rápida.

## Procurar a orientação de técnicos especializados para uma resolução mais rápida

Muitas vezes, mais de um técnico trabalha em um ticket. Seus técnicos recomendados colaboram uns com os outros para obter as percepções necessárias. Além disso, você deve procurar a orientação de técnicos especializados para resolver problemas complexos mais rapidamente.

## Acompanhar os usuários iniciantes e intervir quando necessário

O trabalho remoto torna o treinamento um processo complicado. Você pode dar aos novos técnicos uma experiência prática enquanto os acompanha silenciosamente. Para fins de demonstração, você pode intervir e assumir o controle.

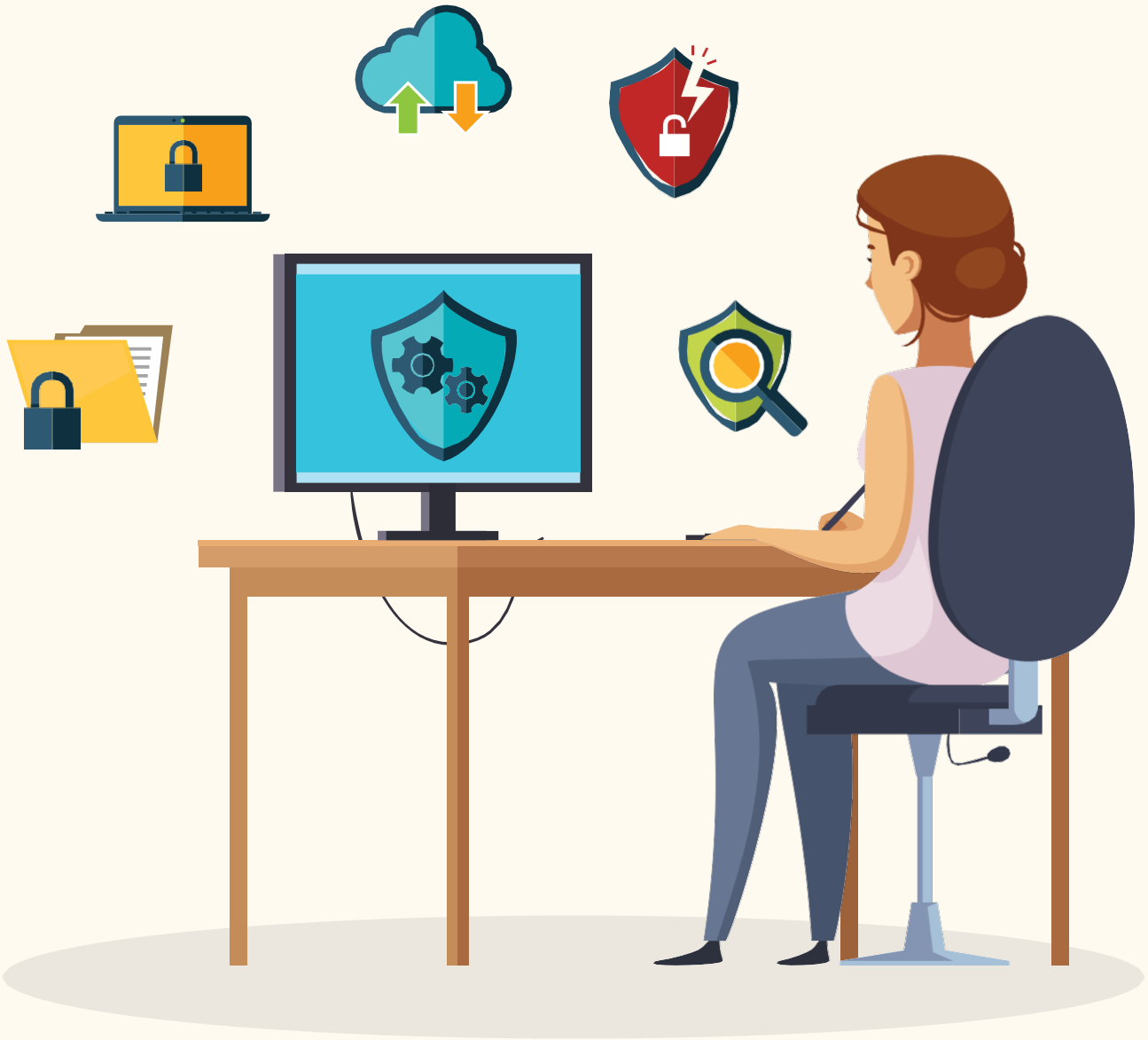
## Aproveitar os canais de comunicação integrados

Agilize seu processo de resolução de problemas aproveitando canais de comunicação integrados, como bate-papo baseado em texto e chamadas de voz e vídeo. Isso o ajudará a adquirir as informações necessárias dos usuários finais. Além disso, você pode manter os usuários finais informados sobre todas as ações realizadas em seus endpoints.

## Gravar sessões remotas e manter um histórico de scripts de bate-papo

Registre automaticamente sessões remotas para fins de auditoria e treinamento. Além disso, se a sua organização estiver atenta à conformidade, você poderá exportar os scripts de bate-papo e solicitar a aprovação do usuário sempre que iniciar uma sessão remota.

# Práticas recomendadas para proteger seus recursos corporativos



## Distribuir e gerenciar documentos corporativos com segurança

Crie um repositório de conteúdo e distribua os documentos corporativos necessários a partir desse repositório para manter guias sobre os recursos acessados. Impeça que os usuários compartilhem o conteúdo com outros dispositivos ou o copiem para outras aplicações para ajudar a evitar vazamento de dados.

## Distribuir seus certificados do repositório para gerenciar a expiração e a renovação

Distribua seus certificados a partir de um repositório central para simplificar o gerenciamento de expiração e renovação de certificados. Além disso, habilite a autenticação baseada em certificado para segurança de dados corporativos.

## Supervisionar os privilégios de administrador para manter os ataques de elevação no compartimento

Durante a instalação do software, é importante que as organizações concedam privilégios administrativos conforme e quando necessário. Não há limite para qual usuário requer que grau de acesso. Sempre mantenha guias sobre os privilégios de administrador concedidos e certifique-se de revogá-los quando não forem mais necessários.

## Isolar seus navegadores e renderizar sites improdutivos em um navegador virtual

Ao usar navegadores para o trabalho, os usuários tendem a ser desviados e navegar por sites que não estão relacionados ao trabalho. Coloque na lista de permissões todos os sites relacionados ao trabalho que serão renderizados em um navegador normal, enquanto qualquer item que se desvie dessa lista será renderizado em um navegador virtual para proteger a organização contra os riscos que sites não relacionados ao trabalho têm.

## Regule o uso de dispositivos externos para evitar a extração dos dados

Os dispositivos externos são parte integrante de todas as organizações, cuja utilização é inevitável. Implemente uma abordagem de Confiança Zero, na qual você bloqueia o uso da maioria dos dispositivos externos, sobretudo USBs, e permite que  o dispositivo seja apenas de um fornecedor confiável.

## Certificar-se de executar apenas aplicações aprovadas pela empresa em dispositivos móveis

As políticas de Traga seu próprio dispositivo (BYOD; Bring Your Own Device) eliminam a necessidade de provisionar dispositivos de trabalho remotos. Para garantir a segurança dos dados, é importante executar apenas aplicações aprovadas pela empresa nesses dispositivos. Distribua aplicações do repositório e armazene-as em um contêiner criptografado separado.

Outras práticas recomendadas que você deve seguir incluem a auditoria de logs de eventos para detectar anomalias de maneira proativa, automatizar a geração de relatórios predefinidos e exportar relatórios para analisar a estrutura atual e fazer as alterações necessárias.

A proliferação de endpoints e usuários torna difícil manter um controle dos eventos. É aqui que os alertas para o gerenciamento em tempo real são úteis. Quebre o gargalo da banda associando diferentes políticas de implantação para diferentes grupos de usuários que atendem suas circunstâncias.

Integre seu help desk com uma solução de gerenciamento de endpoints para equipar seus técnicos, para que eles possam oferecer resolução rápida de problemas diretamente da janela de tickets, pois uma das últimas coisas que qualquer técnico deseja é uma help desk inundada.

**Implemente essas práticas recomendadas imediatamente!**