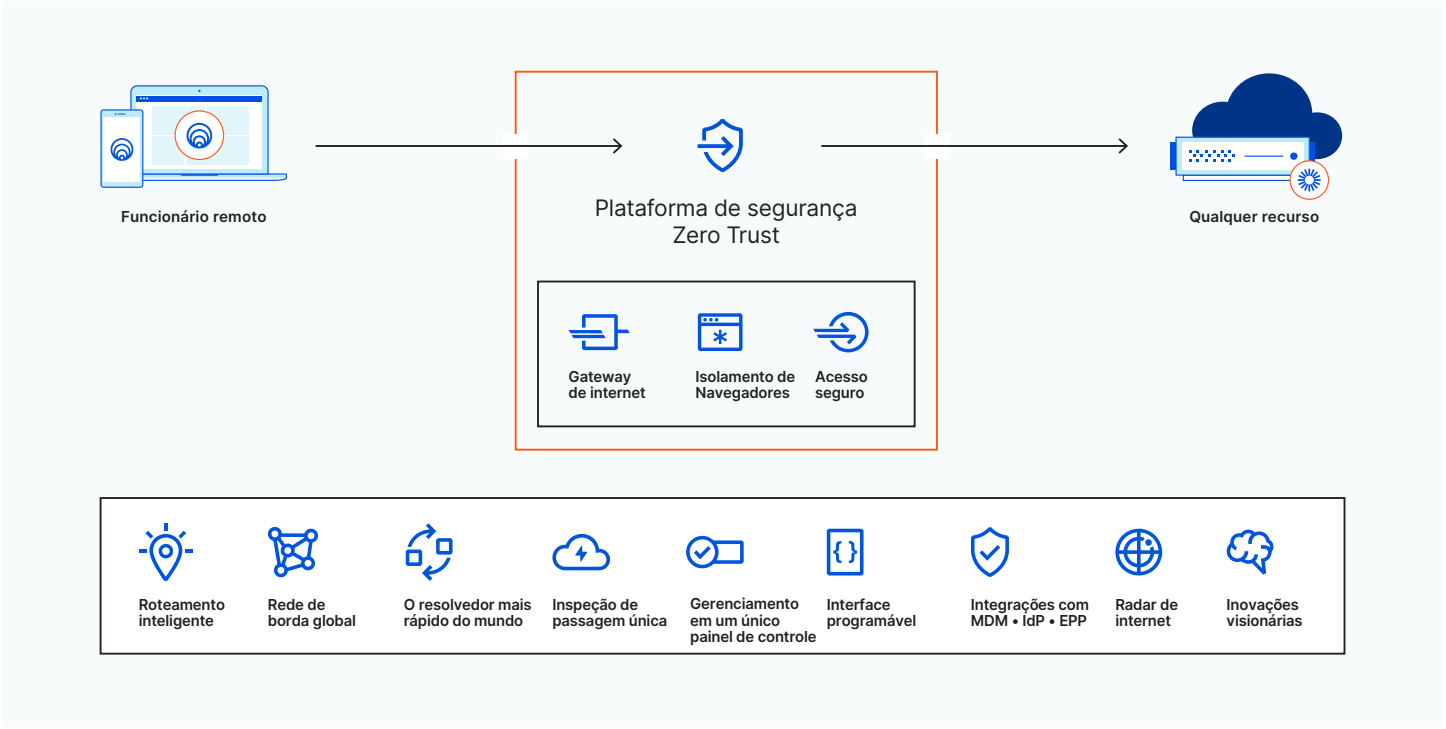
Proteja a conectividade do trabalhador remoto no longo prazo com a Cloudflare

A COVID-19 promoveu uma transição forçada para o trabalho remoto e as empresas se esforçaram para manter os funcionários conectados. Algumas soluções foram estratégicas, mas outras são recursos táticos, como intensificar os cuidados com VPNs lentas e pouco confiáveis, fazer o tunelamento dividido do tráfego da internet e usar hacks rápidos de acesso remoto. Agora é possível ver as brechas dessa abordagem, pois os desafios conhecidos de visibilidade, segurança e complexidade continuam.

Corrigir falhas de segurança no trabalho remoto não precisa levar meses ou semanas. Com a plataforma de segurança Zero Trust da Cloudflare, os administradores podem resolver mais de 20 casos urgentes de uso de segurança e conectividade da força de trabalho em apenas 30 minutos.

A solução: Cloudflare para Teams



A plataforma de segurança Zero Trust da Cloudflare aumenta a visibilidade, elimina a complexidade e reduz os riscos à medida que os trabalhadores remotos se conectam aos aplicativos e à internet. Ela é executada na rede de borda mais rápida do mundo, para implantar com mais rapidez e ter um desempenho melhor do que outros provedores.

Uma plataforma Zero Trust pode aumentar a segurança do trabalhador remoto de três maneiras

Reduz riscos

Depender de VPNs cria risco de failover e deixa brechas na infraestrutura corporativa que invasores podem explorar. Após obter acesso, o invasor se move lateralmente em diversos recursos para roubar dados. Mesmo com os melhores esforços para bloquear e solucionar ameaças, os pontos de terminação ainda ficam comprometidos por malware não descoberto.

As plataformas de segurança Zero Trust reduzem os riscos do trabalho remoto ao impor a autenticação de identidade baseada em contexto em todas as solicitações enviadas a seus aplicativos corporativos, o que deixa pouco espaço para a movimentação lateral. O isolamento de navegadores separa os pontos de terminação da atividade de navegação, mitigando ameaças conhecidas e desconhecidas.

Aumenta a visibilidade

Era simples manter os registros de atividade quando os usuários estavam no escritório. Manter uma trilha de auditoria é muito mais difícil quando os colaboradores estão distribuídos geograficamente e trabalham em novos dispositivos. Muitas vezes, o recurso de registro dos aplicativos SaaS são inconsistentes e os registros de VPN são difíceis de analisar.

Com as plataformas Zero Trust, é possível restaurar a visibilidade interceptando e registrando as solicitações de todos os dispositivos remotos, até os não gerenciados. Os administradores podem monitorar a atividade do trabalhador remoto em aplicativos SaaS hospedados internamente, com uma trilha de auditoria para investigar incidentes. Os registros são centralizados em um painel e enviados automaticamente para o SIEM de sua escolha.

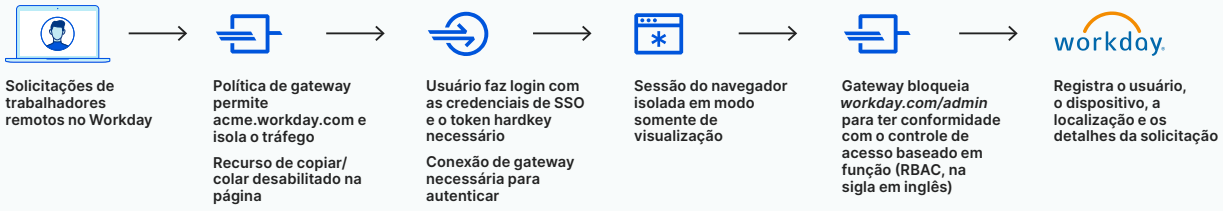
Elimina a complexidade

Soluções rápidas implementadas para conectar trabalhadores remotos estão se mostrando muito frágeis no longo prazo. Os administradores precisam gerenciar políticas de filtragem de tráfego em diversas ferramentas incompatíveis e os usuários ficam frustrados com o desempenho lento.

As plataformas Zero Trust simplificam a maneira como os usuários se conectam e facilitam o trabalho dos administradores. Com menos dependência de VPNs herdadas, os administradores podem usar controles de segurança padrão em todo o tráfego, independentemente de como a conexão é iniciada ou do local da pilha de rede em que ela reside. E todas as políticas podem ser gerenciadas em um painel.

Segurança Zero Trust na prática

Caso de uso: evitar a perda de dados em aplicativos SaaS



Em uma arquitetura de passagem única, o tráfego do trabalhador remoto é inspecionado, isolado, registrado e protegido contra ameaças da internet. E o desempenho nunca é afetado, pois os usuários se conectam a data centers próximos deles.

Seis problemas críticos do trabalho remoto resolvidos

Caso de uso	Como
Conectar trabalhadores remotos aos aplicativos corporativos	Rotear o tráfego (DNS, HTTP(S), RDP/SSH) por meio da rede da Cloudflare entre dispositivos e aplicativos, para melhorar o desempenho e confiabilidade de sua VPN.
Adotar a segurança Zero Trust para acessar aplicativos	Impor políticas de acesso a aplicativos com base na identidade, na postura do dispositivo e no contexto (geográfico) em vez de na localização de rede (IP).
Adotar a segurança Zero Trust para navegação na internet	Isolar a atividade de navegadores em dispositivos protegidos para impedir que malware e phishing comprometam os pontos de terminação.
Proteger dados contra acessos e carregamentos não autorizados	Exercer um controle mais refinado sobre os direitos de acesso do usuário e do dispositivo; evitar carregar/baixar arquivos, copiar/colar.
Proteger dispositivos contra conteúdo malicioso em um site	Todo conteúdo malicioso conhecido ou desconhecido é executado remotamente em contêineres seguros em toda a nossa rede, o que o impede de alcançar o navegador local do dispositivo.
Proteger os usuários contra sites de phishing	A inteligência contra ameaças nativas e de terceiros bloqueia tentativas de phishing antes que elas ocorram.

Principais resultados

80%↓

a menos do tempo consumido resolvendo chamados de suporte de TI e postura de segurança para trabalhadores remotos.

30 min

para concluir as duas primeiras etapas da segurança Zero Trust

91%↓

de redução na superfície de ataque ao colocar a Cloudflare na frente do acesso a aplicativos e da navegação na internet.

Próximas etapas

Assista à demonstração

Experimente o Teams, é gratuito para até 50 usuários

Solicite uma demonstração ao vivo com um especialista da Cloudflare