GoTo Resolve

Fact Sheet

Zero Trust
Não se arrisque.

Proteja seus dispositivos com o controle de acesso Zero Trust pioneiro do mercado.

O que é o modelo Zero Trust?

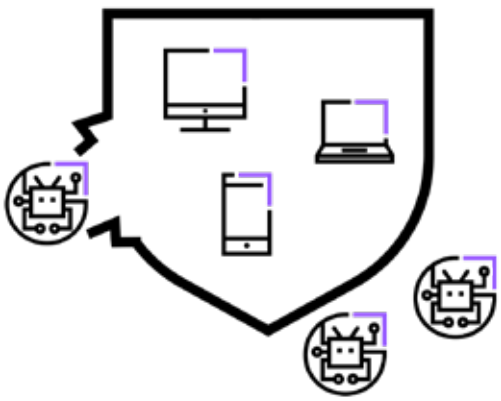
Zero Trust, ou Confiança Zero, é um rigoroso protocolo de segurança que segue a lógica "não confiar em ninguém, verificar todo mundo" em um software ou ambiente de TI. Nesse modelo, supõe-se que os softwares ou infraestrutura de TI têm diversos pontos de entrada, como backdoors de softwares, APIs e muitos outros componentes que vão além das credenciais tradicionais dos usuários. Portanto, qualquer ação ou informação sensível precisa passar por mais um ponto de verificação.

Como o modelo Zero Trust funciona em um software de monitoramento e gerenciamento remoto?

Em infraestruturas com hosts implementados por software de monitoramento e gerenciamento remotos, o modelo Zero Trust considera que, mesmo após o usuário informar suas credenciais de login, o sistema não deve acreditar automaticamente que é mesmo aquele usuário.

Em vez de conceder acesso automático para que o usuário (ou código) possa praticar ações nos hosts (como executar automações de TI), o modelo Zero Trust exige uma nova confirmação de identidade antes de conceder um nível sensível de acesso.

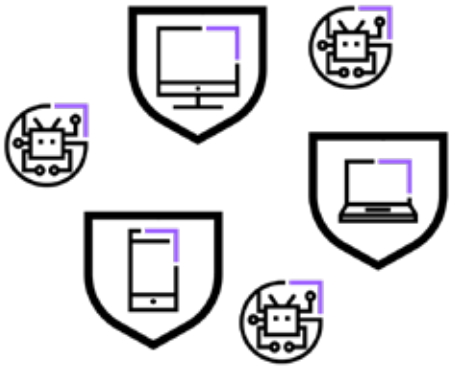
Segurança tradicional



Permite acesso ilimitado dentro da zona de confiança. Após conseguir entrar, a pessoa ou componente mal-intencionado pode fazer o que quiser.

x

Zero Trust



Acaba com o conceito de confiança, individualizando a zona de segurança de cada terminal.

Por que é importante saber disso?

Duas grandes tendências estão tornando o modelo Zero Trust mais importante do que nunca:

1. As empresas estão dando mais ênfase ao trabalho flexível, reduzindo a presença nos escritórios.

Os modelos de trabalho híbrido e remoto estão roubando a cena no mercado. Agora, as equipes de TI precisam proteger uma força de trabalho altamente fluida. Com terminais em todo lugar e usando diferentes redes, as medidas tradicionais de segurança local deixaram de oferecer a melhor proteção.

2. Os ataques cibernéticos estão cada vez mais frequentes e sofisticados.

Pessoas e componentes mal-intencionados estão se aproveitando das brechas do trabalho flexível. Ataques cibernéticos, como phishing e ransomware, colocam dados pessoais e empresariais em risco, enquanto ataques à cadeia de suprimento podem ser verdadeiras catástrofes para muitas empresas.

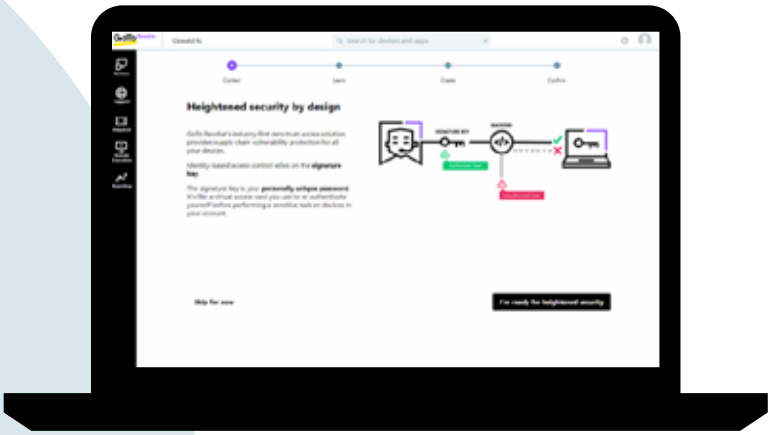
Qual é o diferencial do modelo Zero Trust no GoTo Resolve?

Por ser pioneira nas soluções de SaaS (Software como Serviço, na sigla em inglês), a GoTo adota o modelo Zero Trust no controle de acesso de monitoramento e gerenciamento remoto. A arquitetura do GoTo Resolve é projetada para proteger as empresas e seus dispositivos gerenciados contra pessoas e componentes mal-intencionados, bem como vulnerabilidades da cadeia de suprimentos.

Como funciona:

O modelo Zero Trust protege o acesso remoto e a execução remota em hosts.

- O applet instalado em um dispositivo remoto aceita **comandos apenas de agentes autorizados.**
- Os agentes precisam criar e usar uma **chave de assinatura exclusiva** para fazer uma nova autenticação em tarefas sensíveis.
- **Só o agente tem acesso** a essa chave, impossibilitando seu comprometimento online. É bom frisar que nem a GoTo tem acesso a ela.
- Mesmo que pessoas ou componentes mal-intencionados consigam invadir o backend ou roubar credenciais de login, **não será possível alterar nem criar novas automações** para os terminais sem a chave de assinatura.
- Os terminais obedecem apenas a **comando assinados.**



Trabalhe com tranquilidade e proteção em meio aos ataques cibernéticos cada vez mais frequentes.

Baixe o Resolve Free