GoTo Resolve

Fiche technique

Zero Trust : ne prenez pas de risques inutiles.

Protégez vos appareils avec le contrôle d'accès Zero Trust unique en son genre.

Qu'est-ce que Zero Trust ?

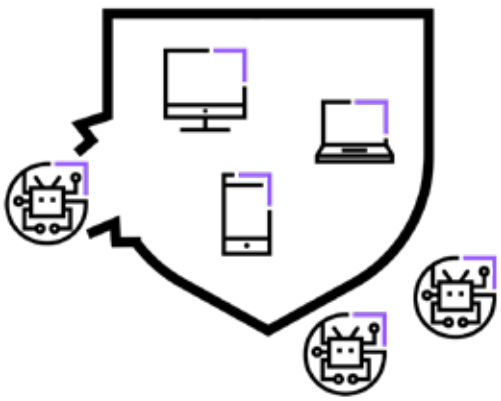
Zero Trust est un protocole de sécurité strict basé sur une approche « ne faire confiance à personne, valider tout le monde » intégré à un logiciel ou un environnement informatique. Il part du principe que chaque logiciel ou infrastructure informatique offre plusieurs portes d'entrée, en plus du mécanisme de connexion de l'utilisateur, comme des portes dérobées ou des API (interfaces de programmation), parmi d'autres. Dès lors, toute action ou information sensible doit déclencher une vérification supplémentaire.

Qu'est-ce que Zero Trust dans le cadre d'un logiciel de surveillance et gestion à distance (RMM) ?

Lorsque des hôtes ont été déployés à distance par un logiciel RMM, l'approche Zero Trust part du principe que même si un utilisateur est bien connecté, le système ne doit pas automatiquement croire qu'il a le droit d'être là.

Au lieu de faire confiance automatiquement à l'utilisateur (ou à un bout de code) en lui permettant d'agir sur les hôtes (en exécutant des automatisations informatiques par exemple), Zero Trust exige que toute personne ou entité qui tente de se connecter au système valide son identité avant de pouvoir accéder à un niveau d'accès sensible.

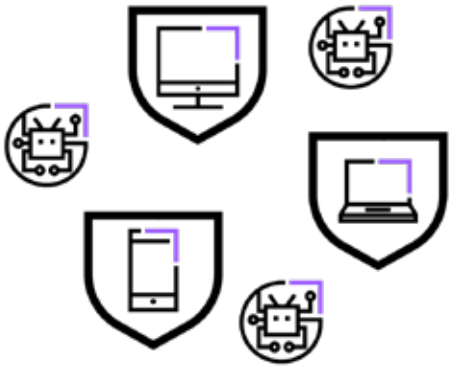
Sécurité traditionnelle



Offre un accès illimité dans la zone de confiance.
Une fois à l'intérieur, un acteur malveillant peut faire des ravages.

VS

Zero Trust



Élimine la notion de confiance, en déplaçant la zone de confiance vers chaque terminal.

Pourquoi est-ce important ?

Deux tendances de fond rendent l'approche Zero Trust plus essentielle que jamais :

1. Les organisations basculent du travail au bureau vers le travail nomade.

Le télétravail et le travail hybride ont changé la donne. Les équipes informatiques doivent désormais sécuriser un personnel particulièrement mouvant. Avec des terminaux partout sur différents réseaux, les mesures de sécurité traditionnelles sur site n'offrent plus la protection nécessaire.

2. Les cyberattaques augmentent en quantité et en sophistication.

Les acteurs malveillants profitent avec avidité du travail flexible. Les cyberattaques, comme le phishing ou hameçonnage ou les rançongiciels, mettent les données personnelles et professionnelles en danger, et peuvent avoir des conséquences dévastatrices pour de nombreuses entreprises.

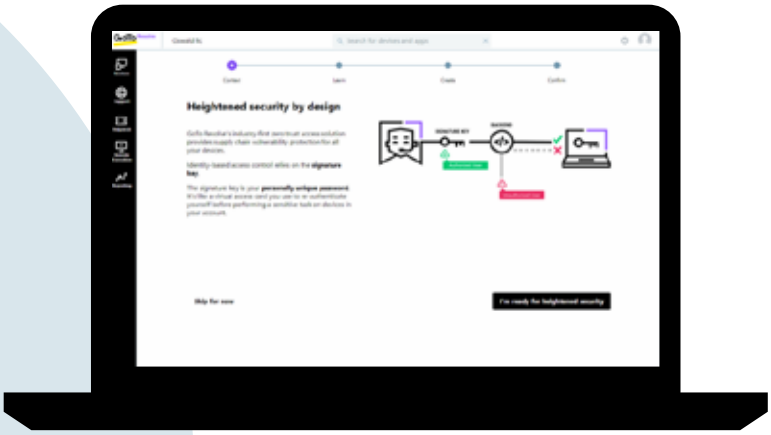
Qu'est-ce qui distingue l'approche Zero Trust de GoTo Resolve ?

GoTo applique l'approche Zero Trust au contrôle d'accès RMM, ce qui constitue une première pour un logiciel-service (SaaS). L'architecture même de GoTo Resolve protège les entreprises et leurs appareils gérés contre les acteurs malveillants, et contre les vulnérabilités de la chaîne logistique.

Fonctionnement :

Zero Trust sécurise le déploiement de l'accès à distance et l'exécution à distance sur tous les hôtes déployés.

- L'applet sur un appareil distant n'accepte que les **commandes provenant d'agents autorisés.**
- Les agents doivent créer et utiliser une **clé de signature unique** pour réauthentifier les tâches sensibles.
- Cette clé **n'est connue que de l'agent,** et pas par GoTo, et elle ne peut être piratée en ligne.
- Même si un acteur malveillant pénétrait le back-office ou obtenait des identifiants de connexion par hameçonnage, **il ne pourrait pas modifier ou créer des automatisations** sur les terminaux sans la clé de signature.
- Les terminaux n'obéissent qu'aux **commandes signées.**



Soyez plus serein en vous protégeant des cyberattaques en plein essor.

Obtenir Resolve Free