GoTo Resolve

Productoverzicht

Zero trust: neem geen risico's

Bescherm uw apparaten met de eerste, unieke zero-trust toegangscontrole

Wat is zero trust?

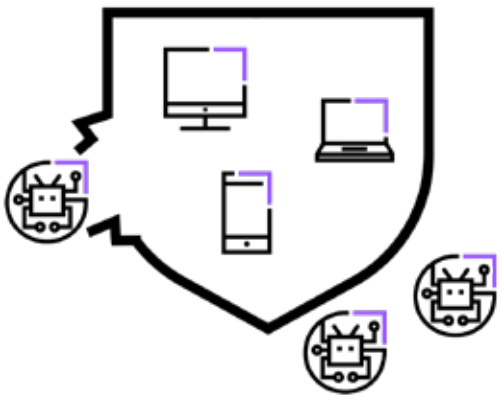
Zero trust staat voor een streng beveiligingsprotocol voor software- en IT-omgevingen. Het principe: "vertrouw niemand, en bevestig altijd de identiteit". Het uitgangspunt is dat software en IT-infrastructuur altijd meerdere toegangspunten bieden: mensen kunnen niet alleen binnenkomen via de traditionele aanmelding van de gebruiker, maar ook via backdoors in de software, API's en andere toegangspunten. Daarom moeten alle gevoelige acties of informatie eigenlijk een extra verificatie vereisen.

Wat wordt er bedoeld met zero trust als het gaat om software voor monitoring en beheer op afstand?

Als er hosts uitgerold zijn door software voor monitoring en beheer op afstand, gaat een benadering op basis van zero trust ervan uit dat het systeem gebruikers niet automatisch mag vertrouwen, zelfs niet als ze al aangemeld zijn.

De gebruiker (of een stukje code met deze rol) krijgt niet automatisch toegang en kan niet zomaar een actie uitvoeren op de hosts, bijvoorbeeld om een IT-automatisering te implementeren. In plaats daarvan vereist zero trust dat alle gebruikers en functies die proberen om verbinding te maken met de beveiligde systemen, eerst hun identiteit bevestigen. Pas dan geeft het systeem toegang tot gevoelige functies.

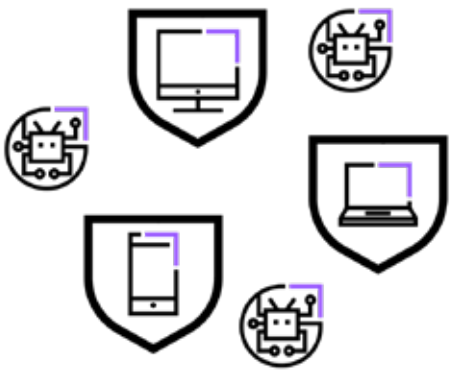
Traditionele beveiliging



Geeft onbeperkte toegang aan gebruikers binnen de vertrouwde zone. Kwaadwillenden die eenmaal binnen zijn, kunnen hierdoor ontzettend veel schade veroorzaken.

versus

Zero trust



Werkt zonder vertrouwde zone voor het gehele systeem: alle individuele endpoints krijgen hun eigen verdedigingslinie.

Waarom is dit zo waardevol?

Door twee wereldwijde ontwikkelingen is zero trust belangrijker dan ooit.

1. Organisaties werken inmiddels primair flexibel, en niet meer per definitie op kantoor.

Hybride werk en thuiswerken hebben de IT-beveiliging op zijn kop gezet. IT-teams moeten de beveiliging garanderen voor een extreem beweeglijk personeelsbestand. Endpoints zijn wijd verspreid en verbonden met verschillende netwerken. Traditionele on-premises beveiligingsmaatregelen bieden geen optimale bescherming meer.

2. Er zijn steeds meer cyberaanvallen, en ze worden steeds geavanceerder.

Cybercriminelen maken dankbaar gebruik van de opkomst van flexibel werk. Phishingaanvallen en ransomware vormen een risico voor persoonlijke informatie en gevoelige bedrijfsgegevens, en aanvallen op de leverketen kunnen voor veel bedrijven rampzalig uitpakken.

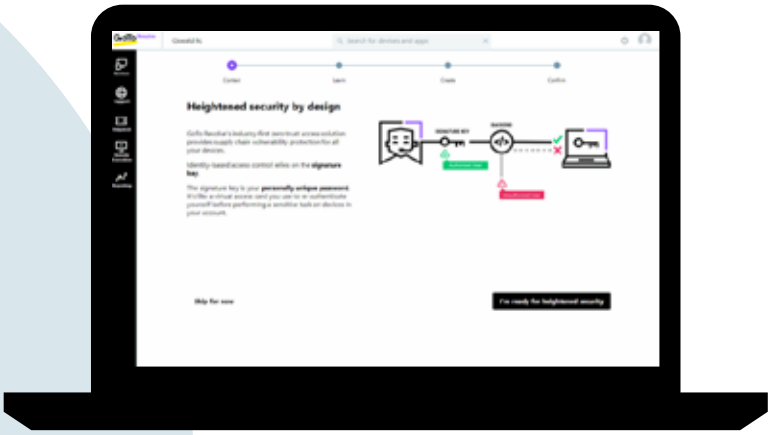
Wat maakt de zero trust-benadering van GoTo Resolve anders?

GoTo heeft een primeur voor SaaS-oplossingen: het past zero trust toe voor het toegangsbeheer voor externe toegang en beheer op afstand. De architectuur van GoTo Resolve beschermt bedrijven en beheerde apparaten tegen cybercriminelen en versterkt de beveiliging van kwetsbaarheden in de leverketen.

Hoe werkt het?

Zero trust beveiliging de toegang en uitvoering op afstand voor alle hosts in het netwerk.

- De applet op het externe apparaat accepteert **alleen opdrachten van geautoriseerde IT-medewerkers**.
- IT-medewerkers moeten een **unieke sleutel** aanmaken en gebruiken om hun identiteit bij gevoelige acties opnieuw te bevestigen.
- **Alleen de medewerker heeft deze sleutel** – GoTo niet. De sleutel is niet online toegankelijk.
- Zelfs als hackers toegang krijgen tot de backend of als ze aanmeldingsgegevens weten te verkrijgen met een phishingaanval, **kunnen ze zonder deze sleutel geen automatiseringen wijzigen of nieuwe scripts uitvoeren** op endpoints in het netwerk.
- Endpoints voeren alleen opdrachten uit die **ondertekend zijn met de sleutel.**



Kies voor gemoedsrust en bescherm uw organisatie tegen de vloed aan cyberaanvallen.

Download Resolve Free