GoTo Resolve

Ficha informativa

Modelo de confianza cero: no se la juegue.

Proteja sus dispositivos con el control de acceso con modelo de confianza cero pionero del sector.

¿Qué es el modelo de confianza cero?

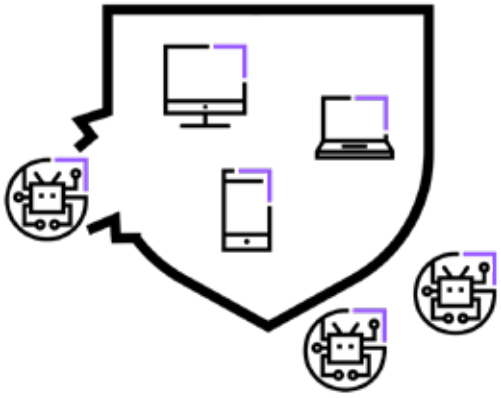
El modelo de confianza cero es un estricto protocolo de seguridad que adopta un enfoque "no confiar en nadie, verificar a todos" en un entorno de software o TI. Parte del supuesto de que en cada elemento de una infraestructura de TI o software existen varios puntos de entrada, no solo a través del inicio de sesión de usuario tradicional, sino potencialmente a través de puertas traseras de software y API (interfaces de programación de aplicaciones), entre otras. Por tanto, cualquier acción o información confidencial debería utilizar un punto de verificación adicional.

¿Qué implica el modelo de confianza cero en el software de gestión y monitoreo remotos (RMM)?

En el caso de despliegue de hosts mediante el software de gestión y monitoreo remotos (RMM), un enfoque de confianza cero asume que aunque un usuario esté protegido por el inicio de sesión, el sistema no debe confiar automáticamente en que debería estar allí.

En lugar de confiar automáticamente en el acceso y proporcionar a un usuario (o fragmento de código) la capacidad de realizar acciones en los hosts (como ejecutar automatizaciones de TI), el modelo de confianza cero exige que cualquier persona o código que intente conectarse a sus sistemas verifique su identidad antes de otorgar un nivel de acceso confidencial.

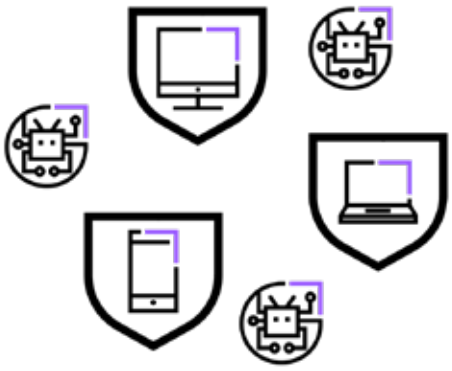
Seguridad tradicional



Permite el acceso ilimitado dentro de la zona de confianza. Una vez dentro, un agente malicioso puede causar estragos.

VS

Confianza cero



Elimina el concepto de confianza y traslada la zona de confianza a cada punto final.

¿Por qué es importante?

Dos transformaciones importantes hacen que el modelo de confianza cero sea más crítico que nunca:

1. Las organizaciones se han vuelto flexibles, ya no están centradas en la oficina física.

Los modelos de trabajo híbrido y teletrabajo han provocado cambios. Actualmente los equipos de TI deben garantizar una plantilla con plena movilidad. Con puntos finales en todas partes y en diferentes redes, las medidas de seguridad tradicionales en las instalaciones ya no ofrecen la mejor protección.

2. Los ciberataques no dejan de aumentar y cada vez son más sofisticados.

Los agentes maliciosos están más que dispuestos a aprovechar el modelo de trabajo flexible. Ciberataques como el phishing y el ransomware ponen en peligro los datos personales y empresariales; por su parte, los ataques a las cadenas de suministro pueden provocar resultados catastróficos para muchas empresas.

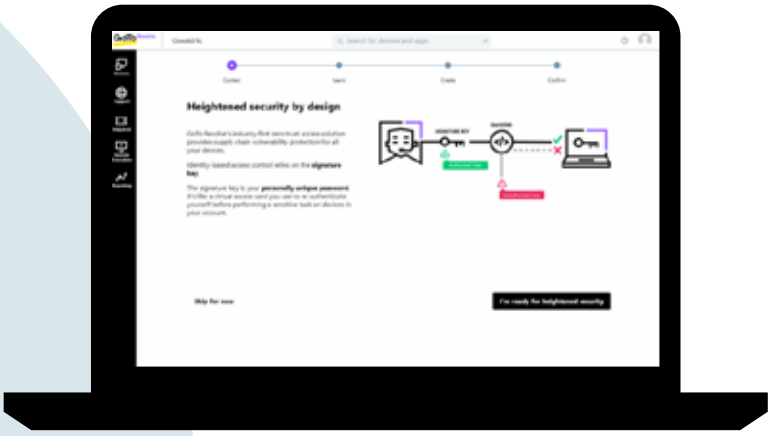
¿En qué se diferencia el enfoque de confianza cero de GoTo Resolve?

Como empresa pionera en soluciones SaaS (Software como servicio), GoTo aplica el modelo de confianza cero al control de acceso de RMM. GoTo Resolve está diseñado para proteger a las empresas y sus dispositivos gestionados frente a agentes maliciosos, además de proporcionar protección contra vulnerabilidades de las cadenas de suministro.

Funcionamiento:

El modelo de confianza cero protege el despliegue de acceso remoto y la ejecución remota a través de hosts desplegados.

- El applet en un dispositivo remoto **solo acepta comandos de los agentes autorizados.**
- Los agentes deben crear y utilizar una **clave de firma única** para volver a autenticar las tareas confidenciales.
- GoTo no conoce esta clave **(solo la conoce el agente),** y no se puede vulnerar en línea.
- Incluso si un agente malicioso hackea el back-end o suplanta las credenciales de inicio de sesión, **el atacante no puede cambiar ni crear nuevas automatizaciones** para puntos finales sin la clave de firma.
- Los puntos finales solo atienden sus **comandos firmados.**



Mejore su tranquilidad y protección contra los ciberataques en constante aumento.

Conseguir Resolve Free