GoTo Resolve



Fact Sheet

Zero Trust: Take No Chances

Protect your devices with the industry's first-of-its-kind, zero trust access control

What is zero trust?

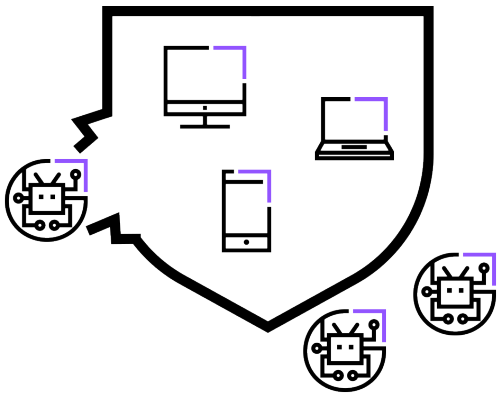
Zero trust is a strict security protocol that takes a "trust no one, verify everyone" approach within software or an IT environment. It goes by the assumption that there are multiple entry points into a piece of software or an IT infrastructure — not just a traditional user login, but potentially through software backdoors, APIs (Application Program Interfaces), and more. As such, any sensitive actions or information should invoke an additional verification point.

What is zero trust within RMM software?

Where there are hosts deployed by remote monitoring & management (RMM) software, a zero trust approach would assume that even if a user is behind the login wall, the system should not automatically trust they should be there.

Instead of automatically trusting access and giving a user (or piece of code) the ability to take actions on hosts (such as running IT automations), zero trust requires that anyone and everything trying to connect to its systems verify identity before granting a sensitive level of access.

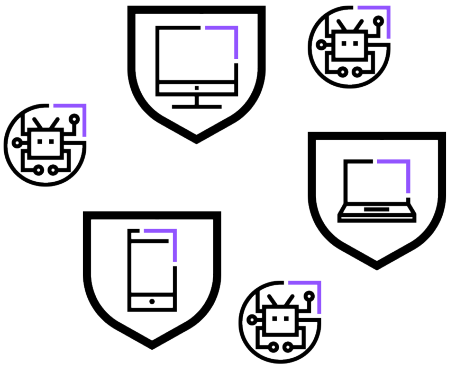
Traditional Security



Allows unlimited access within the trust zone. Once inside, a malicious actor can wreak havoc.

VS

Zero Trust



Eliminates the concept of trust, moving the trust zone to each endpoint.

Why does it matter?

Two major movements make zero trust more critical than ever:

1. Organizations are flexible-first, not office-centric.

Hybrid and remote work have changed the game. IT teams must now secure a highly fluid workforce. With endpoints everywhere and on different networks, traditional, on-premises security measures no longer offer the best protection.

2. Cyberattacks are on the rise and getting more sophisticated.

Malicious actors are eagerly taking advantage of flexible work. Cyberattacks like phishing and ransomware put personal and business data at risk, while supply chain attacks can cause catastrophic results for many companies.

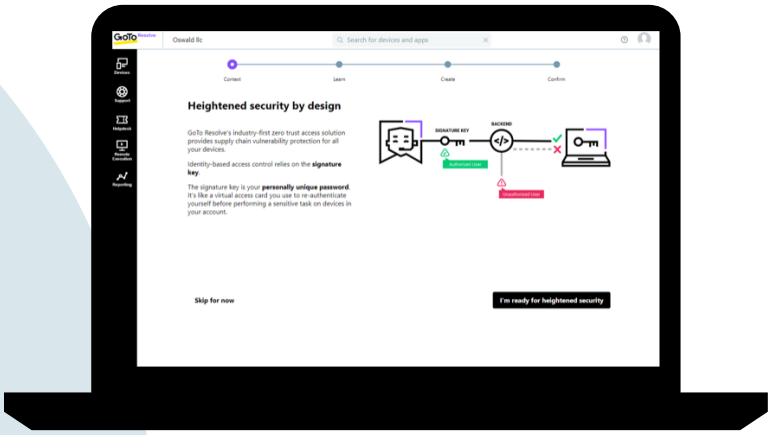
How is GoTo Resolve's approach to zero trust different?

As a first for SaaS (Software as a Service) solutions, GoTo is applying zero trust to RMM access control. GoTo Resolve is architected to protect businesses and their managed devices from malicious actors and provide supply chain vulnerability protection.

How it works:

Zero trust secures remote access deployment and remote execution across deployed hosts.

- The applet on a remote device accepts **commands from authorized agents only.**
- Agents must create and use a **unique signature key** to reauthenticate sensitive tasks.
- This key is **only known to the agent**, not to GoTo, and cannot be compromised online.
- Even if a malicious actor hacks into the backend or phishes login credentials, **the attacker cannot change or create new automations** for endpoints without the signature key.
- Endpoints obey only their **signed commands.**



©2023 GoTo. All rights reserved.