

Datenblatt

Zero Trust: Gehen Sie kein Risiko ein.

Schützen Sie Ihre Geräte mit der branchenweit einzigartigen Zugriffskontrolle nach dem Zero-Trust-Prinzip.



Was versteht man unter „Zero Trust“?

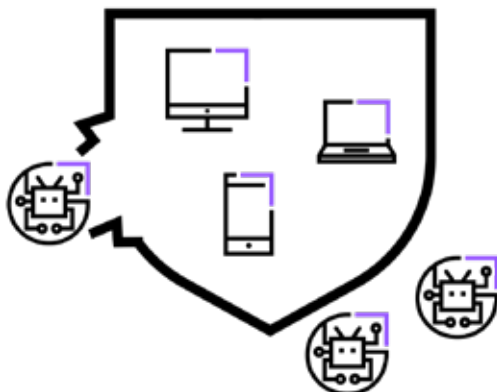
Zero Trust ist ein strenges Sicherheitsprotokoll, das nach dem Prinzip „vertraue niemandem, überprüfe jeden“ arbeitet, um Software oder IT-Umgebungen zu schützen. Dabei wird davon ausgegangen, dass es mehrere Zugangspunkte zu einer Software oder IT-Infrastruktur gibt – nicht nur die klassische Benutzeranmeldung, sondern auch potenzielle Hintertüren in Software, APIs (Anwendungsprogrammierschnittstellen) und vieles mehr. Von daher sollte bei allen sensiblen Aktionen oder Zugriffen auf vertrauliche Informationen eine zusätzliche Verifizierung stattfinden.

Was bedeutet Zero Trust im Kontext von Remote-Monitoring- und -Management-Software (RMM)?

In einem Szenario mit bereitgestellten Hosts durch eine Remote-Monitoring- und -Management-Software (RMM) geht ein Zero-Trust-Ansatz davon aus, dass das System selbst bei Benutzer:innen, die sich bereits erfolgreich angemeldet haben, nicht automatisch darauf vertraut, dass ihr Zugriff berechtigt ist.

Anstatt dem Zugriff automatisch zu vertrauen und einem/r Benutzer:in (oder einem Code) zu erlauben, Aktionen auf Hosts auszuführen (z. B. IT-Automatisierungen), erfordert das Zero-Trust-Prinzip von jedem, der versucht, eine Verbindung zu seinen Systemen herzustellen, die Verifizierung der Identität, bevor Zugriff auf vertraulicher Ebene gewährt wird.

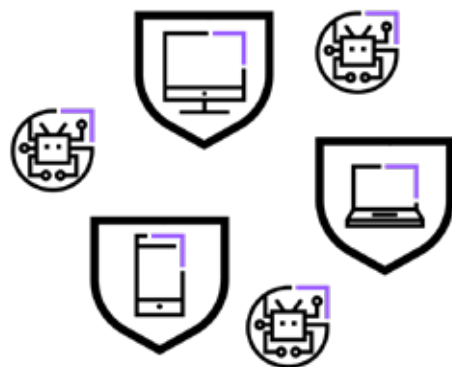
Herkömmliche Sicherheit



Erlaubt unbegrenzten Zugriff innerhalb der Vertrauenszone. Sobald ein Hacker sich einmal Zutritt verschafft hat, kann er nach Belieben schalten und walten und Unheil anrichten.

VS

Zero Trust



Das Konzept „Vertrauen“ gibt es nicht – die Vertrauenszone wird zu den einzelnen Endpunkten verlagert.

Warum ist das wichtig?

Zwei große Trends machen Zero Trust wichtiger denn je:



1. Bei Unternehmen steht Flexibilität an erster Stelle, nicht mehr das Arbeiten im Büro.

Hybrid- und Telearbeit haben die Spielregeln geändert. IT-Teams müssen jetzt für die Sicherheit einer ständig in Bewegung befindlichen Belegschaft sorgen. Da die Endpunkte von Unternehmen mittlerweile überall verstreut und in verschiedene Netzwerke eingebunden sind, bieten herkömmliche On-Premise-Sicherheitsmaßnahmen keinen ausreichenden Schutz mehr.



2. Cyberangriffe werden immer zahlreicher und raffinierter.

Hacker schlagen begierig Vorteile aus flexibler Arbeit. Cyberangriffe wie Phishing und Ransomware gefährden persönliche und geschäftliche Daten, während Angriffe auf die Lieferkette für viele Unternehmen katastrophale Folgen haben können.

Inwiefern ist der Zero-Trust-Ansatz von LogMeIn Resolve anders?

GoTo ist das erste Unternehmen, das das Zero-Trust-Prinzip in einer SaaS-Lösung (Software as a Service) für RMM-Zugriffskontrolle anbietet. Die Architektur von LogMeIn Resolve schützt Unternehmen und ihre verwalteten Geräte vor Hackerangriffen und bietet Schutz für Schwachstellen in Lieferketten.

Funktionsweise:

Zero Trust schützt Fernzugriffsinstallationen und die Ausführung von Remotebefehlen auf bereitgestellten Hosts.

- Das Applet auf einem Remotegerät akzeptiert **nur Befehle von autorisierten Techniker:innen**.
- Techniker:innen müssen einen **eindeutigen Signaturschlüssel** erstellen und verwenden, um sich für die Durchführung von Aktionen an vertraulichen Inhalten ein weiteres Mal zu authentifizieren.
- Dieser Schlüssel ist **nur den Techniker:innen bekannt**, nicht GoTo, und er kann online nicht kompromittiert werden.
- Selbst wenn sich ein böswilliger Akteur in das Back-End hackt oder Anmeldeinformationen per Phishing abgreift, **hat der Angreifer ohne den Signaturschlüssel keine Möglichkeit, Automatisierungen für Endpunkte zu ändern oder neue zu erstellen**.
- Endpunkte befolgen nur die entsprechend **signierten Befehle**.

