# Zscaler Zero Trust Device Segmentation für OT/IoT

Stoppen Sie laterale Bewegungen, minimieren Sie die Angriffsfläche und optimieren Sie die Betriebssicherheit



Lösungsprofil

## Ein dringendes Problem

In letzter Zeit ist es zu einem Anstieg der Warnmeldungen und Warnungen vor Cyberangriffen staatlich geförderter Bedrohungsakteure auf die kritische Infrastruktur der USA gekommen. Am 7. Februar 2024 veröffentlichten das Federal Bureau of Investigation (FBI) und die Cybersecurity and Infrastructure Security Agency (CISA) zusammen mit der National Security Agency eine Warnung an Regierungsbehörden, dass Cyber-Akteure im Begriff seien, kritische Infrastrukturen wie Transportsysteme, Öl- und Erdgaspipelines, Wasseraufbereitungsanlagen und Stromnetze zu stören. Dies ergänzt ähnliche Maßnahmen der TSA zur Sicherung von Flughäfen, Flugzeugbetreibern und Eisenbahnen, die jüngsten Cybersicherheits-Grundlinien des Energieministeriums und das nahezu endgültige NERC-Update zu CIP-015-1.

Bei der Entwicklung von OT/IoT-Technologien steht Geschwindigkeit und Transaktionseffizienz im Vordergrund, während Sicherheit nur eine Nebenrolle spielt. Leider ist OT/IoT mittlerweile ein beliebtes Ziel von Cyberkriminellen. Laut Untersuchungen von Zscaler ThreatLabz ist die Zahl der Angriffe dort im Vergleich zum Vorjahr um 400 % gestiegen. Ransomware ist die beliebteste Angriffsstrategie und 61 % aller Sicherheitsverletzungen zielten auf Organisationen mit vernetzter OT ab.

## Was können Sie tun?

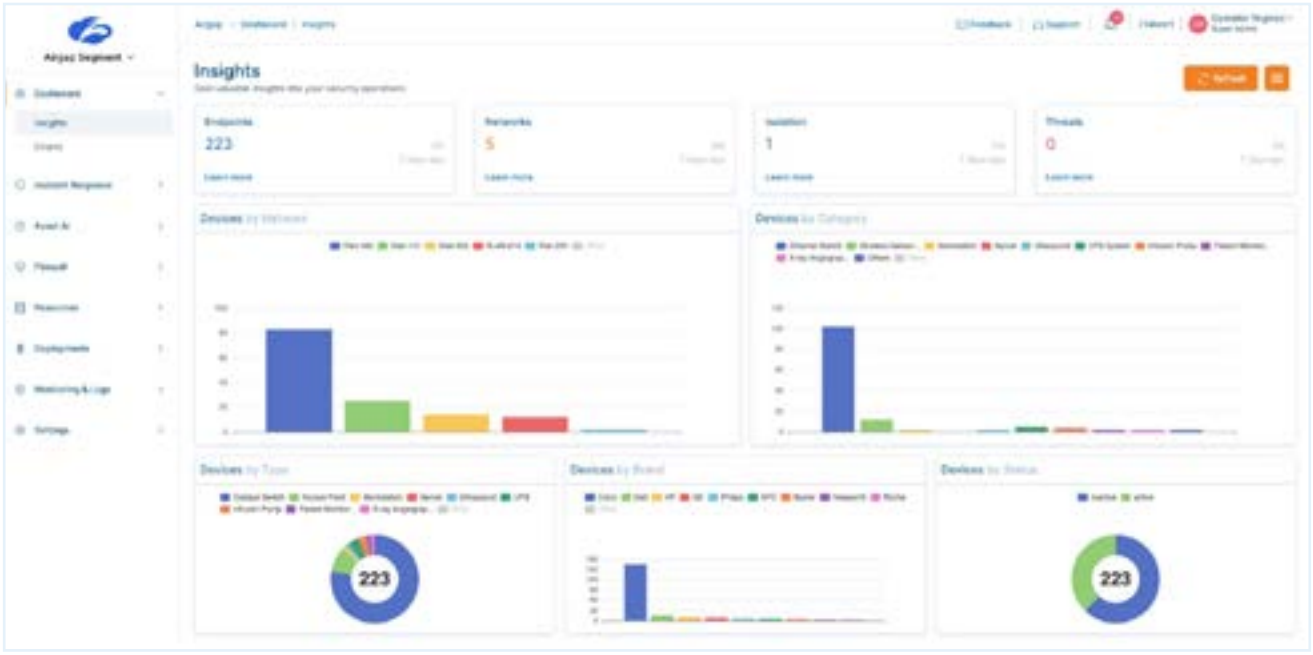
EPA, CISA und FBI empfehlen den Systembetreibern dringend, entsprechend der Durchführungsverordnung des Präsidenten auf Zero Trust als Richtlinie für eine bessere Cybersicherheit umzusteigen.

Die hervorgehobenen Elemente sind Schlüsselbereiche in diesen Empfehlungen, in denen Zscaler mit unserer Zero-Trust-basierten Lösung zur Gerätesegmentierung sofort helfen kann.

- Weniger Exposition gegenüber dem öffentlichen Internet
- Geringeres Risiko von Schwachstellen
- Netzwerksegmentierung
- Protokollierung
- Keine Verbindungen unbefugter User
- Keine ausnutzbaren Dienste im Internet
- Eingeschränkte OT/IoT-Verbindungen zum Internet
- Erkennen relevanter Bedrohungen
- Bestandsaufnahme von OT/IT-Assets

## Wie erreichen Sie das?

Segmentierung ist seit langem ein fester Bestandteil der Netzwerktechnik, wobei Tools wie Zugriffskontroll-listen (ACLs) und Firewalls den Traffic zwischen Client und Server verwalten. Die OT-Mikrosegmentierung verlagert den Fokus jedoch auf den anfälligeren lateralen Traffic zwischen Geräten und Workloads. Aufgrund der veralteten Switching-Architektur können Geräte in gemeinsam genutzten VLANs alle anderen Geräte sehen und mit ihnen kommunizieren. Dadurch entsteht eine Umgebung, in der sich Malware leicht verbreiten kann. Leider können agentenbasierte Lösungen, die für Cloud-Workloads entwickelt wurden, die in der OT so häufig vorkommenden Legacy- und Headless-Maschinen nicht segmentieren, und herkömmliche ACL-basierte Ansätze sind weiterhin mit hohem Aufwand verbunden.




Dashboard der Zero Trust Device Segmentation

Zscaler beseitigt Probleme bei der Segmentierung innerhalb des VLAN mit einer agentenlosen Lösung, die alle lateralen Bedrohungen stoppt, indem sie jeden IP-Endpunkt, einschließlich Legacy- und Headless-Systeme, als einzelnes Netzwerksegment isoliert.  Dadurch werden komplexe ACLs überflüssig und es sind keine Änderungen an der vorhandenen Infrastruktur erforderlich. Gleichzeitig wird eine hochgradig granulare und effektive Segmentierung bereitgestellt, die derzeit unübertroffen ist.

## Anwendungsfälle

Zu den häufigsten Anwendungsfällen für die agentenlose Gerätesegmentierung gehören:

### LAN-Mikrosegmentierung

Erweitern Sie Zero Trust auf das LAN, indem Sie die Segmentierung des lateralen Traffics erzwingen. Dies verkleinert Ihre interne Angriffsfläche und eliminiert die Gefahr von lateralen Bewegungen in kritischen OT/IoT-Netzwerken, ohne dass eine NAC- oder Firewall-basierte Segmentierung erforderlich ist.

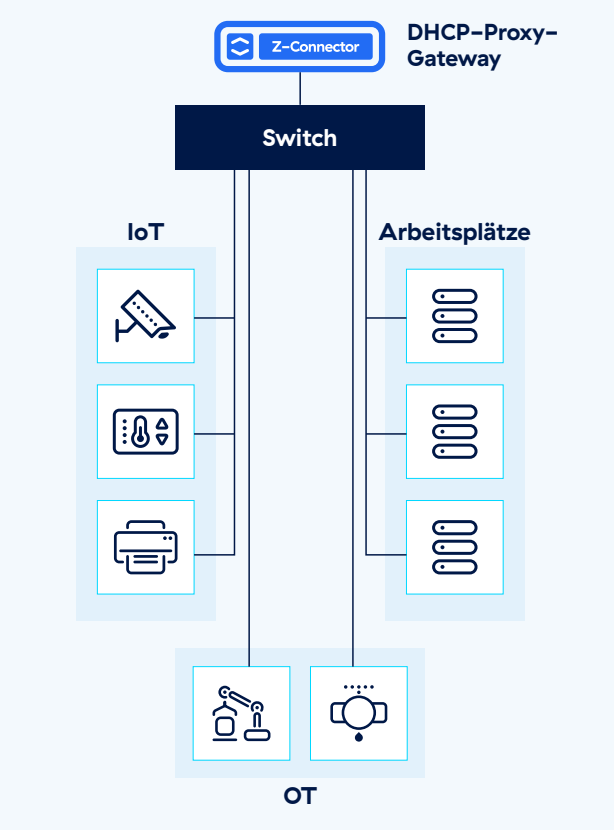
So setzen Sie Zero-Trust-Segmentierung in Ihrem Netzwerk durch:

- Automatische Isolierung jedes Geräts in einem Einzelsegment (/32)
- Gruppieren Sie Geräte, User und Apps automatisch, indem Sie ihre Trafficmuster analysieren. So verhindern Sie, dass betrügerische Geräte mithilfe von MAC-Spoofing in das Netzwerk gelangen.
- Dynamisches Durchsetzen von Richtlinien für lateralen Traffic basierend auf der Identität und dem Kontext von Usern und Geräten

### IT/OT-Segmentierung

Die Zscaler Zero Trust Device Segmentation fungiert als Kill Switch für Ransomware und deaktiviert nicht unbedingt erforderliche Gerätekommunikation, um die laterale Ausbreitung von Bedrohungen zu stoppen, ohne den Geschäftsbetrieb zu unterbrechen. Diese Lösung neutralisiert fortgeschrittene Bedrohungen wie Ransomware auf IoT-Geräten, OT-Systemen und agentenlosen Geräten.

- Gruppieren Sie bekannte MAC-Adressen auf allen Geräten autonom und setzen Sie entsprechende Richtlinien durch (z. B. wird der RDP-Zugriff auf Kameras außer für Administratoren verweigert).
- Automatische Isolierung unbekannter MAC-Adressen, um das Schadenspotenzial im Falle eines kompromittierten Geräts zu begrenzen
- Integration mit Asset-Management-Systemen für sichere Zugriffskontrollrichtlinien



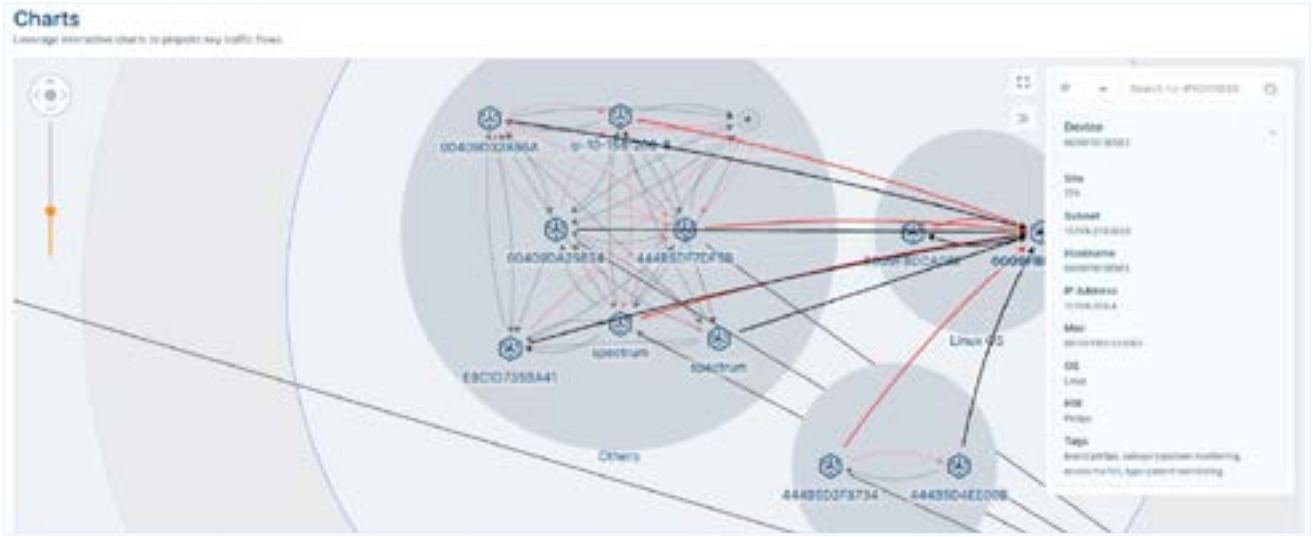

Automatische Isolierung von IoT/OT-Geräten in Einzelsegmenten

### Automatische Geräteerkennung und -klassifizierung

Da ein erheblicher Anteil des OT/IoT-Traffic innerhalb des lokalen Netzwerks bleibt, ist eine kontinuierliche Sichtbarkeit des lateralen Traffics wichtig. Durch die automatische Geräteerkennung und -klassifizierung können Netzwerkadministratoren Leistung, Verfügbarkeit und Sicherheit für IoT/OT-Systeme ohne komplexe Bestandsverwaltung besser verwalten.

Für Netzwerk- und Gerätesichtbarkeit:

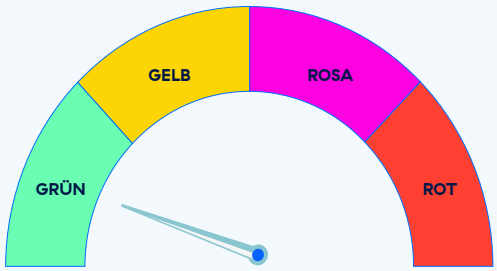
- Entdecken, klassifizieren und inventarisieren Sie OT/IoT-Geräte ohne Installation von Endgerät-Agenten
- Erhalten Sie eine Baseline der Trafficmuster und des Geräteverhaltens, um befugte und nicht befugte Zugriffe zu ermitteln
- Gewinnen Sie präzise Netzwerkeinblicke für das Leistungsmanagement und die Bedrohungsverfolgung




Dashboard Device Discovery

### Automatisierte Reaktion auf Vorfälle

Zscaler Ransomware Kill Switch bietet eine vom User wählbare Reduzierung der Angriffsfläche. Wählen Sie einfach einen voreingestellten Schweregrad aus, um bekannte anfällige Protokolle und Ports schrittweise zu sperren oder sogar den Zugriff auf ganze Netzwerke wie Fertigungsstraßen und Krankenhausetagen sofort zu deaktivieren. Kein Rätselraten im Chaos einer Sicherheitsverletzung — aktivieren Sie einfach die Kill Switch, um der Bedrohung zu begegnen und gleichzeitig die Betriebszeit Ihres Unternehmens aufrechtzuerhalten.




**Deutliche Verbesserung der durchschnittlichen Zeit bis zur Behebung**

**Hochrisikozugriff blockieren**

**Schutz vor lateraler Ausbreitung**

**Blockieren Sie den Zugriff auf geschäfts-kritische Assets**

**Sprechen Sie mit einem technischen Experten.**
Möchten Sie mehr darüber erfahren, wie Zscaler Ihnen beim Schutz Ihrer kritischen Infrastruktur helfen kann? Vereinbaren Sie einen Termin für ein Gespräch mit einem unserer technischen Experten.

zscaler™ | Experience your world, secured.™

**Über Zscaler**
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, zuverlässiger und sicherer arbeiten können. Die Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an beliebigen Standorten vor Cyberangriffen und Datenverlust. Die SSE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.



+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de