Zscaler Zero Trust Gerätesegmentierung für Industrie 4.0

WHITEPAPER

Im Zeitalter von Industrie 4.0, in dem intelligente Fertigung und vernetzte industrielle Systeme zur Norm werden, hat sich die Zero-Trust-Architektur als zentrales Sicherheitskonzept etabliert. Klassische, perimeterbasierte Sicherheitsansätze reichen nicht mehr aus, um das komplexe Ökosystem aus OT-Geräten und industriellen Steuerungssystemen zu schützen. Das grundlegende Prinzip von Zero Trust — „niemals vertrauen, immer überprüfen“ — beseitigt implizites Vertrauen im Netzwerk und sorgt für sicheren, authentifizierten Zugriff auf kritische Systeme. Besonders in Industrieumgebungen ist dieser Ansatz entscheidend, da ein Sicherheitsvorfall zu erheblichen Produktionsausfällen, Reputationsverlust und regulatorischen Konsequenzen führen könnte.

Cybersicherheit für die Fertigung

Moderne Produktionsnetzwerke haben sich zu komplexen Ökosystemen entwickelt, in denen OT- und IT-Systeme eng miteinander verzahnt sind. Diese Konvergenz ermöglicht neue Funktionen wie vorausschauende Wartung, integrierte Lieferketten und das Remote-Management von Anlagen. Doch genau diese Vernetzung öffnet auch die Tür für neue Risiken. Was früher klar getrennt war, ist nun Angriffen ausgesetzt, die eigentlich aus der IT-Welt stammen. Entsprechend konzentrieren sich Unternehmen aktuell vor allem auf zwei zentrale Bereiche.

- **Sicherer Zugriff auf OT-Ressourcen:** In Fertigungsumgebungen muss genau kontrolliert werden, wer auf OT-Systeme wie SPSen (PLCs), HMIs oder industrielle Steuerungen zugreifen darf. Mit Zscaler Privileged Remote Access erhalten autorisierte User schnellen, direkten und sicheren Zugriff auf OT-Ressourcen — egal ob an Außenstandorten, auf dem Shopfloor oder an anderen Standorten. Das Ganze funktioniert komplett ohne VPN und ohne Agents. Weitere Informationen zu Zscaler Privileged Remote Access finden Sie hier: https://www.zscaler.com/de/resources/data-sheets/privileged-remote-access-for-ot-and-iiot.pdf

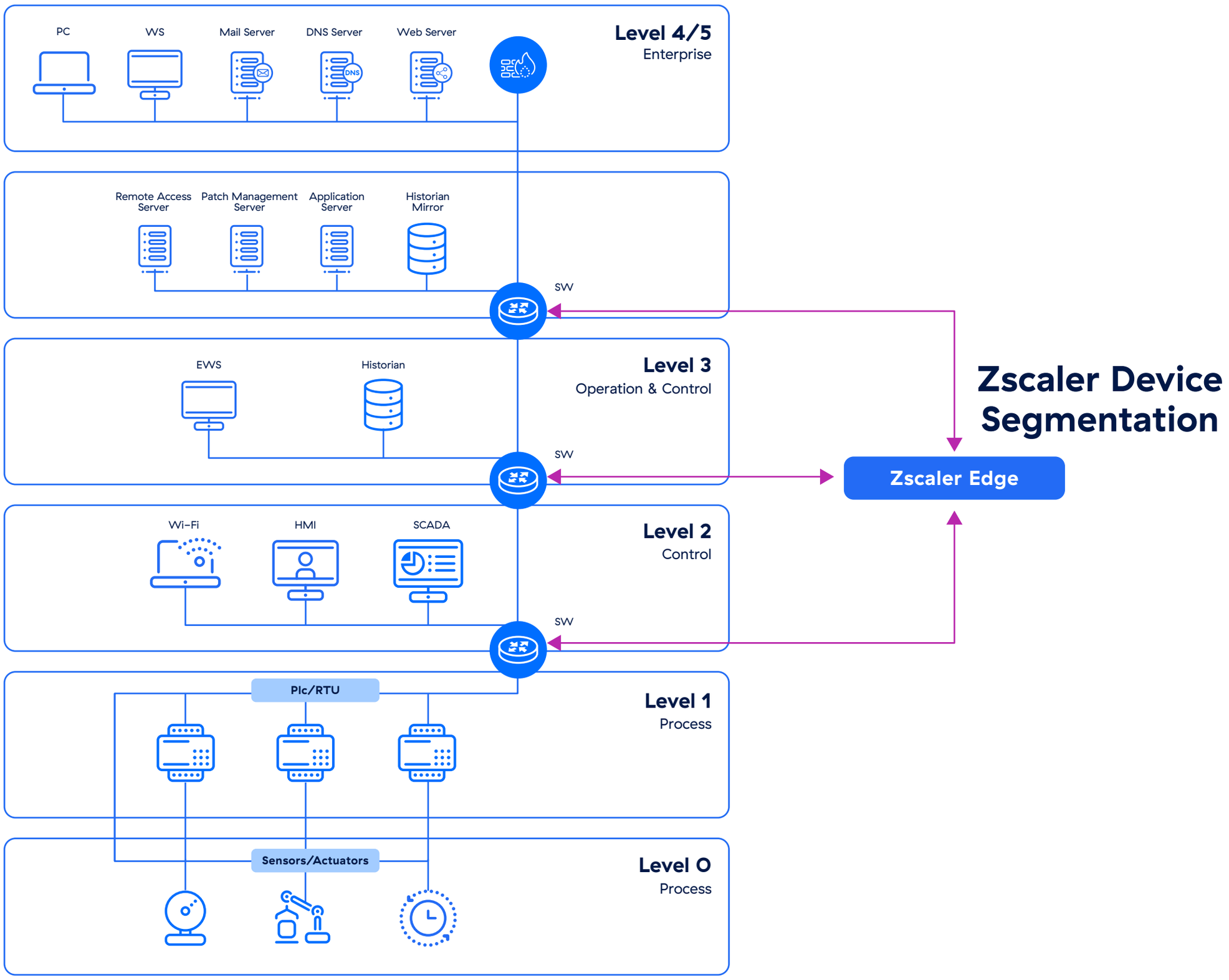
- **Segmentierung:** Ein kritisches Sicherheitsrisiko in Produktionsumgebungen ist die Möglichkeit, dass sich Bedrohungen lateral im Netzwerk ausbreiten. Dies ist besonders gefährlich in industriellen Umgebungen, in denen

Legacy-Systeme, denen es oft an zukunftsfähigen Sicherheitsfunktionen mangelt, mit Geräten auf dem aktuellen technischen Stand vernetzt sind. Die Implementierung von Zero-Trust-Prinzipien durch Mikrosegmentierung trägt zur Eindämmung von Bedrohungen bei, indem sie strenge richtlinienbasierte Netzwerkzugriffskontrollen durchsetzt und so die laterale Bewegungsfreiheit für Angreifer selbst nach erfolgreicher Erstkompromittierung effektiv einschränkt.

Zero Trust Private Access und Segmentation greifen ineinander und bilden zusammen ein robustes Sicherheitskonzept für OT-Ressourcen in der Fertigung. So bleiben Produktionsabläufe vor externen Bedrohungen und internen Risiken geschützt, ohne an Flexibilität und Effizienz zu verlieren.

Segmentierung in der Fertigung

In den meisten Fertigungs- oder industriellen Steuerungsnetzwerken sind unterschiedliche Geräte vernetzt. Laut Purdue-Modell können diese Geräte in klar abgegrenzte Ebenen bzw. Level unterteilt werden.



Purdue Level	Geräte	Beschreibung	Risiko
Level 3	Historian, Jump-Server, Patch-Server	Läuft mit bekannten Betriebssystemen, z. B. Windows. Auch wenn EDR-Lösungen vorhanden sind, bestehen weiterhin Sicherheitsrisiken durch laterale Bedrohungen.	Mittel bis hoch
Stufe 2	HMI, SCADA	Führen eingebettete Betriebssysteme aus (z. B. Windows CE, Windows XP). Aufgrund ihres veralteten Charakters weisen diese Systeme gravierende Schwachstellen und erhebliche Sicherheitsrisiken auf.	Hohe
Stufe 1	PLCs, RTUs	Einfache Headless-Geräte, die nur mit speziellen Tools programmiert und konfiguriert werden können.	Niedrig bis mittel
Level O	Sensoren, Aktoren	Überwiegend nicht IP-basierte Systeme, die sehr spezifische Funktionen ausführen.	niedrig

Die unterschiedlichen OT-Geräte bilden komplexe Kommunikationsmuster und Abhängigkeiten untereinander, um reibungslose Fertigungsprozesse, Betriebskontinuität und zuverlässige Produktionsergebnisse in der Fabrikhalle sicherzustellen. Mit Zscaler Zero Trust Device Segmentation (Zscaler ZTDS) werden Sicherheitskontrollen implementiert und klare Kommunikationsgrenzen zwischen Geräten gezogen. Dadurch wird die Integrität der Fertigungsprozesse gewahrt und Sicherheitsbedrohungen sowie unbefugter Zugriff verhindert.

Anwendungsfall 1

Internetkommunikation

In modernen Fertigungsumgebungen benötigen OT-Systeme immer häufiger eine Internetverbindung für verschiedene betriebliche Anforderungen, darunter Software-Updates, Hersteller-Support und cloudbasierte Analysen. Diese Internetanbindung vergrößert jedoch die Angriffsfläche industrieller Netzwerke erheblich. Bislang isolierte OT-Systeme werden anfällig für gängige Cyberbedrohungen wie Malware, Ransomware und Advanced Persistent Threats (APTs). Die Risiken sind besonders hoch, da viele OT-Geräte ohne integrierte Sicherheitsfunktionen entwickelt wurden und häufig mit älteren Betriebssystemen laufen, die nicht ohne Weiteres gepatcht oder aktualisiert werden können.

Die gesamte Internetkommunikation wird durch Zscaler ZIA geschützt, wobei ausgehende Verbindungen von OT-Ressourcen über diesen Service geleitet werden.

ZSCALER ZIA — ZENTRALE FUNKTIONEN

- **Erweiterter Bedrohungsschutz:** ZIA schützt OT-Ressourcen vor Malware, Ransomware und Zero-Day-Bedrohungen durch eine mehrschichtige Analyse des gesamten Internetverkehrs.

- **Filterung von ausgehendem Traffic:** Erzwingt strenge Zugriffskontrollen, indem die Kommunikation von OT-Geräten auf autorisierte Ziele beschränkt und potenziell schädliche Websites und Inhalte blockiert werden.

- **Threat Intelligence in Echtzeit:** Nutzt globale Cloud-Informationen, um neue Bedrohungen zu erkennen und zu blockieren, bevor sie sich auf OT-Ressourcen auswirken können.

Anwendungsfall 2

Kommunikation zwischen OT- und IT-Systemen

In Fertigungsumgebungen treffen OT- und IT-Kommunikation direkt aufeinander. Dort müssen OT-Systeme reibungslos mit der IT-Infrastruktur zusammenarbeiten. Das schafft die Grundlage für wichtige Funktionen wie Datenanalysen, Remote-Monitoring oder die Ressourcenplanung. Gleichzeitig entstehen dadurch neue Sicherheitsrisiken. IT-Netzwerke sind in der Regel mit dem Internet verbunden und werden häufig aktualisiert. OT-Systeme hingegen laufen oft mit älteren Anwendungen und Protokollen, die modernen Sicherheitsanforderungen nicht gewachsen sind.

Die Diskrepanz in den Sicherheitsfunktionen schafft potenzielle Angriffsvektoren für Cyberbedrohungen.

ZSCALER DEVICE SEGMENTATION — ZENTRALE FUNKTIONEN

- Traditionell wurden IT- und OT-Netzwerke getrennt aufgebaut — oft durch physische Air Gaps. Mit der Modernisierung verschwimmen diese Grenzen jedoch zunehmend. Zscaler Device Segmentation hilft Ihnen, die Trennung zwischen IT und OT aufrechtzuerhalten, ohne die Produktivität oder den Mehrwert moderner Industrieumgebungen zu beeinträchtigen.

- Selbst klar getrennte VLANs schützen IT und OT nicht immer voneinander. Fehlkonfigurationen oder schnelle Veränderungen im Unternehmen führen häufig dazu, dass beide Bereiche sich plötzlich ein Netzwerk teilen. Die patentierte Technologie der Zscaler Device Segmentation erkennt alle IT- und OT-Systeme in diesem geteilten Netzwerk (z. B. VLANs) und trennt sie logisch — ganz ohne VLAN-Änderungen, IP-Anpassungen oder ein Redesign des Netzwerks.

- Um Legacy-Geräte zu schützen und unbefugten Zugriff auf OT-Netzwerke zu verhindern, beseitigt Zscaler Device Segmentation implizites Vertrauen und beschränkt den Netzwerkzugriff auf klar definierte Systeme wie Jump Hosts, Zscaler ZPA oder Zscaler PRA.

- Eine zentrale, hochskalierbare Cloud-Plattform mit ausgeprägter rollenbasierter Zugriffskontrolle und Mehrmandantenfähigkeit macht den Betrieb von IT- und OT-Netzen erheblich einfacher. Gleichzeitig bleiben Zuständigkeiten und Berechtigungen sauber voneinander getrennt.

Anwendungsfall 3

Kommunikation auf Betriebsebene

Auf Level 3 umfasst die Kommunikation auf Betriebsebene den Austausch zwischen verschiedenen Manufacturing-Execution-Systemen (MES), Historian-Lösungen und weiteren Anwendungen für das operative Management. Diese Systeme arbeiten in der Regel über Standard-TCP/IP-Netzwerke und nutzen häufig Protokolle wie OPC UA, MQTT oder REST-APIs für den Datenaustausch. Eine klare Netzwerksegmentierung ist hier besonders wichtig, da diese Systeme die Brücke zwischen IT- und OT-Netzwerken schlagen und damit attraktive Ziele für Cyberangriffe darstellen.

ZSCALER DEVICE SEGMENTATION — ZENTRALE FUNKTIONEN

- Anders als herkömmliche Firewalls ist Zscaler Device Segmentation nicht an spezifische Netzwerkkonfigurationen gebunden. So lassen sich Richtlinien dynamisch durchsetzen — egal, wie sich Systeme auf Betriebsebene mit dem Netzwerk verbinden. Eine zentrale, adaptive Richtlinien-Engine reduziert die operative Komplexität herkömmlicher Firewall-Ansätze erheblich.

- In unternehmenskritischen Umgebungen zählt jede Sekunde: Eine wirkungsvolle Incident Response reduziert die Folgen von Cyberangriffen erheblich. Der Zscaler Ransomware Kill-Switch ist ein leistungsstarkes Tool zur Reaktion auf Vorfälle, das Unternehmen auf Notfallsituationen vorbereitet und die Ausbreitung von Bedrohungen auf Netzwerkebene gezielt stoppt.

- Die einzigartige Architektur von Zscaler ZTDS zentralisiert alle netzwerkbezogenen Informationen an einem Ort. Abhängigkeiten von Einzelprodukten oder komplexen Technologien wie VLANs, ACLs, 802.1X, Firewalls und L3-Routing gehören damit der Vergangenheit an.

Anwendungsfall 4

Kommunikation auf Überwachungsebene

Auf Level 2 umfasst die Kommunikation auf Überwachungsebene entscheidende Interaktionen zwischen HMIs, SCADA-Systemen und weiteren überwachenden Steuerungssystemen über TCP/IP-Netzwerke. Diese Systeme kommunizieren typischerweise über industrielle Protokolle wie Modbus TCP, EtherNet/IP oder OPC UA und nutzen Standard-Netzwerkports (502 für Modbus, 44818 für EtherNet/IP, 4840 für OPC UA). Sie überwachen und steuern industrielle Prozesse, erfassen Echtzeitdaten und stellen Bedienerschnittstellen bereit. Aufgrund des Legacy-Charakters vieler Überwachungssysteme, der Nutzung potenziell angreifbarer Protokolle und ihrer zentralen Rolle im Betrieb ist es besonders wichtig, diese Kommunikation durch angemessene Netzwerksegmentierung und protokollspezifische Sicherheitsmaßnahmen abzusichern. Diese Kommunikation lässt sich weiter unterteilen in:

1. **Kommunikation zwischen Level-2-Systemen (z. B. Interaktionen zwischen HMI und HMI)**
2. **Kommunikation zwischen Level 2 und Level 3 (z. B. Datenübertragung zwischen HMI und Historian)**

ZSCALER DEVICE SEGMENTATION — ZENTRALE FUNKTIONEN

- Die patentierte Zscaler ZTDS-Technologie schützt Überwachungssysteme (z. B. HMI), die auf Purdue Level 2 angebunden sind, durch einzigartige Ring-Fencing-Mechanismen. So entstehen klare Grenzen, die die Angriffsfläche dieser älteren, sensiblen Systeme erheblich verringern.

- Zscaler ZTDS erkennt und visualisiert jegliche Geräte-zu-Geräte-Kommunikation auf Überwachungsebene sowie deren Interaktionen mit Level 3 — unabhängig von der VLAN-Konfiguration. Dabei erstellt die Lösung Traffic-Übersichten dieser Kommunikation und protokolliert alle Transaktionen im integrierten Elastic SIEM.

- Auf Basis von Zero-Trust-Prinzipien lässt sich Zscaler ZTDS in verschiedene Enterprise-Tools wie CMDB und EDR integrieren und passt Zugriffsrichtlinien automatisch an verändertes Verhalten an. Ein hierarchisches Richtlinien-Framework ermöglicht die Umsetzung von Richtlinien für einen einzelnen Standort, für Standortgruppen oder für alle Standorte.

- Ein vereinfachtes Richtlinien-Framework, das Geräteattribute und Tags nutzt — über automatisches Tagging, manuelle Eingabe oder den Import von Drittanbietern — statt komplexer IP- und MAC-Adressen.

- Ein entscheidender Vorteil von Zscaler ZTDS: Die Lösung kommt ohne Agents aus, funktioniert reibungslos mit Ihrer vorhandenen Netzwerkausstattung — unabhängig von Hersteller, Modell oder Version — und benötigt nur sehr geringe Anpassungen der Netzwerkkonfiguration.

Anwendungsfall 5

Kommunikation auf Steuerungsebene

Auf Level 1 interagieren PLCs und RTUs miteinander, um Maschinenabläufe und Prozesssteuerungen zu koordinieren. Diese Geräte kommunizieren außerdem nach oben mit L2-Systemen wie HMIs und SCADA-Systemen, um die Echtzeitüberwachung und -steuerung industrieller Prozesse zu ermöglichen. Diese Kommunikationsebene ist entscheidend für

die Aufrechterhaltung der Betriebseffizienz und erfordert robuste Sicherheitsmaßnahmen, um potenzielle Cyberbedrohungen abzuwehren, ohne Latenz oder Zuverlässigkeit zu beeinträchtigen. Diese Kommunikation lässt sich weiter unterteilen in:

1. **Kommunikation zwischen Level-1-Systemen (z. B. Kommunikation zwischen PLC und PLC)**
2. **Kommunikation zwischen Level 1 und Level 2 (z. B. Kommunikation zwischen PLC und HMI)**

ZSCALER DEVICE SEGMENTATION — ZENTRALE FUNKTIONEN

- Dank seiner einzigartigen Architektur visualisiert und analysiert Zscaler ZTDS alle Kommunikationswege. Gleichzeitig erstellt die Lösung Fingerprints und Profile der angeschlossenen OT-Systeme. Dabei werden Protokolle wie HTTP, ENIP, Modbus oder SSL untersucht und Metadaten extrahiert, um OT-Ressourcen zuverlässig zu erkennen und automatisch zu taggen.

- Visualisiert alle Kommunikationsflüsse zwischen L1-Geräten (PLCs, RTUs) und L2-Systemen (HMIs, SCADA). Implementiert restriktive Zugriffskontrollen, um sensible L1-Geräte (z. B. PLCs) vor potenziell anfälligen, riskanten L2-Geräten (z. B. HMIs) zu schützen.

- Im Lernmodus analysiert Zscaler ZTDS genau, wie L1-Geräte (PLCs, RTUs) mit L2-Geräten (HMIs usw.) kommunizieren. So lassen sich Segmentierungsrichtlinien optimal planen und modellieren.

- Geräte auf Purdue Level 1 sind speziell für bestimmte Aufgaben konzipiert und folgen nicht allen Standard-Netzwerkprinzipien. Das macht die Umsetzung des Zscaler ZTDS Ringfence für diese Geräte komplex. Trotzdem bleibt die Gesamtsicherheit der Umgebung uneingeschränkt bestehen, auch ohne individuelle Segmentierung oder Ring-Fencing.

- Da Bedrohungen typischerweise von anfälligen und riskanten Level-2-Geräten ausgehen, beschränkt Zscaler ZTDS den Zugriff von Level-1-Geräten auf das absolute Minimum, das für den Geschäftsbetrieb erforderlich ist.

- Statt jedes Gerät einzeln zu segmentieren, nutzt Zscaler ZTDS eine Makrosegmentierung auf Basis der vorhandenen Netzwerkstruktur oder eine Gruppen-Segmentierung, bei der L1-Geräte mit Airgap-Plus in überschaubare Segmente eingeteilt werden.

- Da die Kommunikation zwischen L1-Geräten spezielles Programmieren erfordert, reduziert Zscaler ZTDS unbefugte oder fehlerhafte Programmänderungen, indem der eingehende Zugriff auf L1-Geräte eingeschränkt wird.

- Alle weiteren Funktionen — einschließlich Ressourcen-Erkennung und -Profiling, Traffic-Visualisierung, adaptiver Richtliniensteuerung und Ransomware Kill-Switch — bleiben für L1-Geräte uneingeschränkt anwendbar.

Geräte auf Purdue Level 0 (Prozessebene), wie Sensoren oder Aktoren, arbeiten ohne TCP/IP und verbinden sich meist direkt mit anderen Geräten oder Level-1-Systemen über proprietäre Protokolle oder serielle Bus-Systeme. Diese Geräte fallen nicht in den Anwendungsbereich von Zscaler Device Segmentation.

Zusammenfassung

Als Kernkomponente von Zscaler Zero Trust Branch sorgt Zscaler Device Segmentation dafür, dass implizites Vertrauen in industriellen Netzwerken der Vergangenheit angehört, indem logische Grenzen zwischen verschiedenen Arten industrieller Geräte und Systeme gezogen werden. Mit präzisen Segmentierungsrichtlinien lassen sich kritische Produktionssysteme von potenziell angreifbaren Geräten isolieren, Sicherheitsvorfälle gezielt eindämmen und strenge Zugriffskontrollen zwischen den verschiedenen Ebenen umsetzen.

	Anwen-dungsfall 1 (Internet)	Anwen-dungsfall 2 (IT & OT)	Anwendungsfall 3 (L3: Betrieb)	Anwendungsfall 4 (L2: Überwachung)	Anwendungsfall 5 (L1: Steuerung)
Agentlos	✓	✓	✓	✓	✓
Netzwerkunabhängig	✓	✓	✓	✓	✓
Erkennung und Profilerstellung von Ressourcen	✓	✓	✓	✓	✓
Traffic-Transparenz	✓	✓	✓	✓	Zwischen Segmenten
Drittanbieterintegra-tion	N/A	✓	✓	✓	✓
Adaptive Richtliniensteuerung	✓	✓	✓	✓	Zwischen Segmenten
Ransomware Kill-Switch	N/A	✓	✓	✓	✓
Zentrale Verwaltung	✓	✓	✓	✓	✓

Segmentierungsprojekte scheitern häufig, weil herkömmliche Lösungen umfangreiche Änderungen am Netzwerk erfordern (z. B. Geräte-Upgrades oder -Austausch), keine granulare Kontrolle bieten oder nicht alle Ebenen von Fertigungsnetzwerken abdecken. Zscaler ZTDS bietet eine einzigartige Lösung: eine agentlose, netzwerkunabhängige und benutzerfreundliche Plattform mit umfassender Abdeckung. Die Implementierung erfolgt schnell und ohne Betriebsunterbrechung. Fertigungsunternehmen können nun wie Fortune-500-Unternehmen Zscaler Zero Trust Device Segmentation (ZTDS) nutzen, um Zero-Trust-Segmentierung zügig umzusetzen und ihre kritischen OT- und Industrial-Control-Netzwerke zu schützen.

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **www.zscaler.com/de**. Auf X (ehemals Twitter) finden Sie uns unter **@zscaler**.

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

zscaler™

Zero Trust Everywhere