

Zscaler für Fertigungsbetriebe

Stärken Sie das Purdue-Modell mit Zero Trust

LÖSUNGSPROFIL

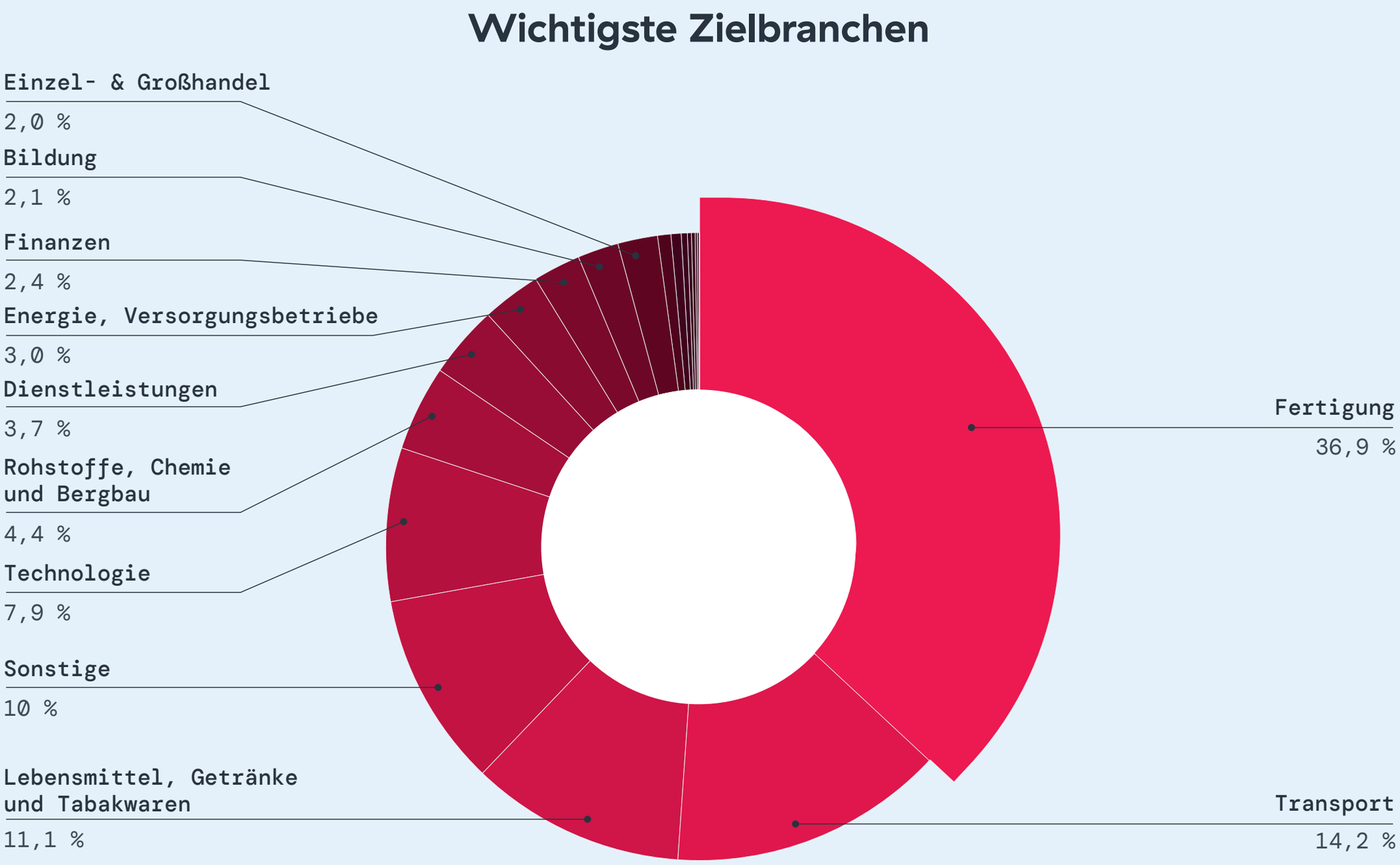
©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Fabriken brauchen einen neuen Ansatz zur Sicherung von OT-Systemen

Zur Optimierung ihrer Produktionsanlagen setzen globale Fertigungsunternehmen auf intelligente Roboter, IoT-Sensoren an jeder Maschine, Cloud-basierte Analysen und digitale Zwillinge der gesamten Fabrikhalle. Das Ziel liegt auf der Hand: höhere Leistung, geringere Ausfallzeiten und vorausschauende Wartung, damit die Anlagen rund um die Uhr in Betrieb bleiben.

Die Realität sieht jedoch oftmals ganz anders aus. Denn jede neue Verbindung erweitert die OT-Angriffsfläche. Und wenn die Angreifer erst einmal im System sind, erhöhen veraltete Betriebssysteme, instabile Netzwerke und eingeschränkte OT-Transparenz das Risiko. Um die Transformation der Fabriken fortzusetzen, muss die Sicherheitsarchitektur überdacht werden.

Der aktuelle IoT/OT-Report von Zscaler ThreatLabz ergab, dass die Fertigungsbranche mit 36 % der insgesamt beobachteten IoT-Malware-Blockaden am stärksten betroffen war.



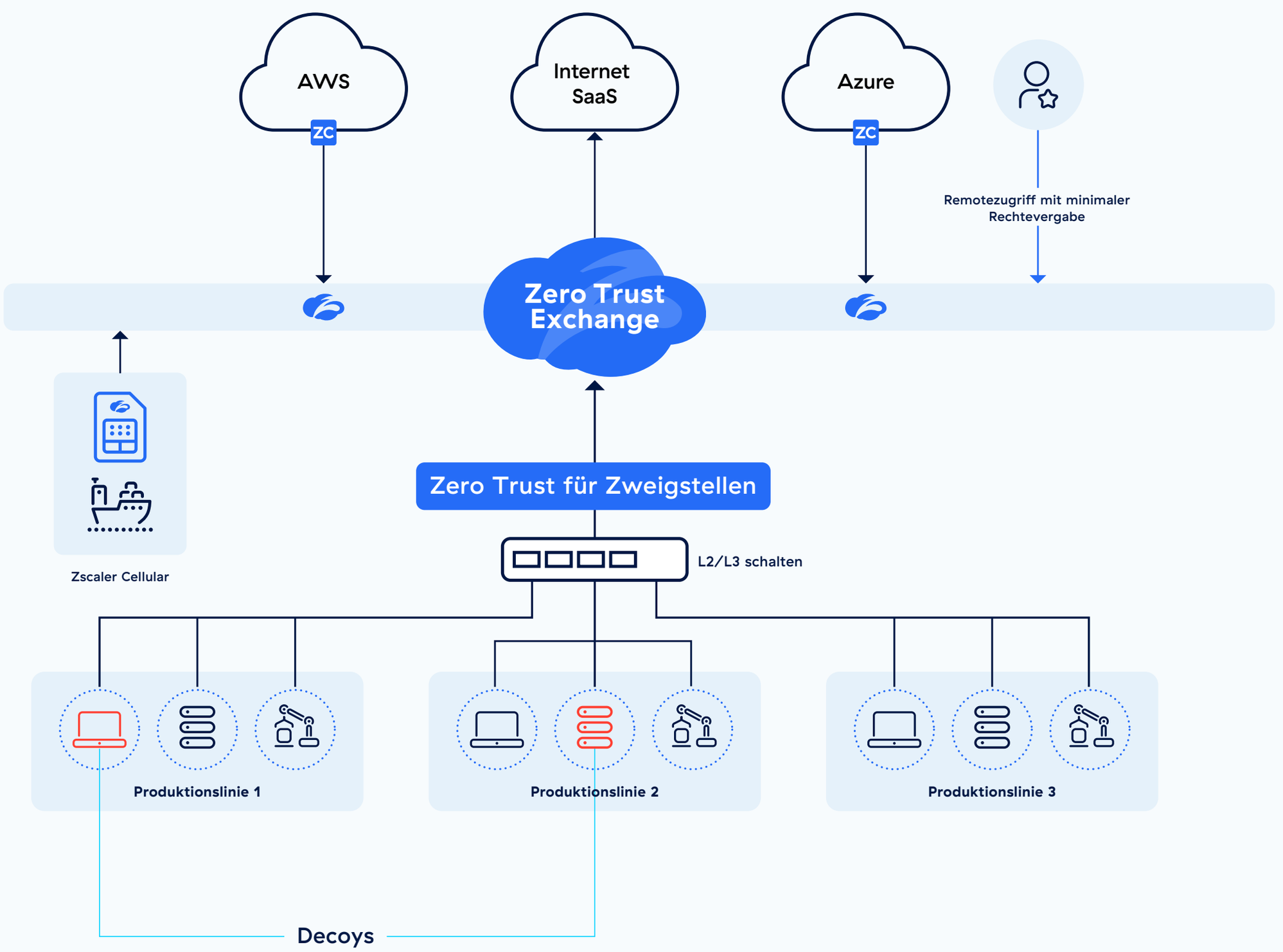
Verteilung der am häufigsten betroffenen Branchen

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Zuverlässiger Zero-Trust-Schutz für alle User und Geräte innerhalb und außerhalb Ihrer Fabriken

Um Fertigungs- und Industrieumgebungen zu sichern, müssen Sicherheitsverantwortliche sicherstellen, dass jede User- und Geräteinteraktion überprüft und das Prinzip der minimalen Rechtevergabe durchgesetzt wird. Unser Zero-Trust-Ansatz ist speziell zum Schutz von OT-Systemen konzipiert und ermöglicht sicheren Zugriff, Segmentierung und Konnektivität in allen Fertigungsabläufen.

- Gewähren Sie Technikern und Dritten Zugriff auf kritische OT-Systeme ohne VPNs
- Granulare Segmentierung, um die laterale Ausbreitung von Bedrohungen zu verhindern
- Sichere Verbindung von OT-Systemen mit der Cloud und dem Rechenzentrum für Analysen
- Profitieren Sie von zuverlässigem Zero-Trust-Schutz für OT-Systeme wie LKWs, Kioske und POS-Scanner
- Frühzeitige Erkennung von Angreifern, um die Rechteausweitung zu verhindern



Zero-Trust-Fabrik-Architektur

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Komponenten der Zscaler-Lösung

Remotezugriff mit minimaler Rechtevergabe

Ermöglichen Sie Drittusern und Remote-Technikern die sichere Verbindung zu RDP/SSH/VNC-Zielen über jeden Browser ohne Agents.

KERNFUNKTIONEN

Eingeschränkte Nutzung der Zwischenablage Schränken Sie Funktionen zum Kopieren und Einfügen basierend auf Zero-Trust-Richtlinien zum Schutz vertraulicher Daten ein.	**Audit- und Governance-Kontrollen** Reduzieren Sie Drittuser-Risiken durch Sitzungsaufzeichnung, Sitzungsfreigabe und begleiteten Zugriff.
Vaulting und Mapping von Zugangsdaten Speichern Sie Anmeldedaten für Zielsysteme in einem cloudbasierten Credential Vault und geben Sie den Zugriff über Zuordnungsrichtlinien frei.	**Zeitgebundener und bedarfsgerechter Zugriff:** Weisen Sie Wartungsfenster zu und stellen Sie bedarfsgerechten Zugriff für die Notfallwartung bereit.

Zero-Trust-Segmentierung

Mikrosegmentieren Sie OT-Systeme und setzen Sie Richtlinien durch, um sicherzustellen, dass nur autorisierte Kommunikation zwischen Ihren OT-Systemen und anderen Systemen erfolgt.

Granulare Mikrosegmentierung Isolieren Sie unterstützte OT-Systeme in Einzelsegmenten (mithilfe /32).	**Geräteerkennung und -klassifizierung:** Automatische Erkennung und Klassifizierung von OT-Geräten.
Ransomware-Killswitch Automatisieren Sie die Reaktion auf Vorfälle mit voreingestellten Richtlinien zur schrittweisen Sperrung von OT-Systemen.	**Durchsetzung von Richtlinien** Gruppieren Sie Geräte automatisch und setzen Sie Richtlinien für lateralen Traffic basierend auf Gerätetyp und Tags durch.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Sicherer OT-Zugriff

Ermöglichen Sie Kameras, Sensoren, Monitoren, Kiosken und anderen OT-Systemen eine sichere Verbindung zu Cloud-Anwendungen und dem Internet. Verhindern Sie die Kommunikation mit verdächtigen oder schädlichen Anwendungen und URLs.

Zero-Touch-Bereitstellung : Nutzen Sie die vollständig automatisierte Zero-Touch-Bereitstellung mit vordefinierten Vorlagen.	**Einheitliche Zero Trust-Richtlinien:** Prüfen und Durchsetzen von Richtlinien für IoT/OT zu privaten Unternehmensanwendungen und dem Internet.
Granulare Richtliniendurchsetzung Setzen Sie Richtlinien durch basierend auf User-/Geräte-Standort, aufgerufenen URLs, Vertraulichkeit von Daten usw.	**Zero Trust Cellular** Einfache Verbindung von Mobilfunkgeräten wie Lkw, Kiosken, Bohrinseln usw. mit Zero Trust

Zscaler Deception

Mithilfe von Decoys können OT-Bedrohungen erkannt werden, die vorhandene Abwehrmaßnahmen umgangen haben. Lokalisieren Sie kompromittierte User, stoppen Sie laterale Bewegungen und schützen Sie das Unternehmen vor Ransomware und böswilligen Insider.

Erkennung lateraler Bewegungen: Setzen Sie Decoy-SPS und -SCADA-Systeme ein, um Angreifer zu erkennen, die versuchen, sich lateral durchs Netzwerk zu bewegen.	**Früherkennung von Angriffen** Erhalten Sie präzise Warnmeldungen, wenn Bedrohungsakteure Ihre IT/OT-Umgebung vor einem Angriff auskundschaften.
Cloud-native Bereitstellung: Integriert mit Zscaler Private Access (ZPA) zum Erstellen, Hosten und Verteilen von Decoys.	**Keine Netzwerkkonfiguration erforderlich.** Die Umleitung des Traffics an Decoys funktioniert ohne VLAN-Trunking, SPAN-Ports und GRE-Tunnel.

©2025 Zscaler, Inc. Alle Rechte vorbehalten.

Alleinstellungsmerkmale von Zscaler

BESEITIGEN VON SICHERHEITSLÜCKEN

Setzen Sie konsistente Zero-Trust-Richtlinien in allen Umgebungen innerhalb und außerhalb Ihrer Fabriken durch.

REDUZIEREN SIE AUSFALLZEITEN

Setzen Sie die Zero-Trust-Segmentierung mit minimaler Unterbrechung Ihrer vorhandenen OT-Umgebung durch und verringern Sie so das Risiko von Ausfallzeiten aufgrund lateraler Bewegungen.

REDUZIERTE KOSTEN UND KOMPLEXITÄT

Reduzieren oder konsolidieren Sie Firewalls, NAC, VPNs, VDIs und Mikroseg-mentierungs-Tools mit einer einfacheren Sicherheitsarchitektur in Ihren Fabriken, die dem Purdue-Modell entspricht.

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**. Gerne können Sie uns auch auf X folgen **@zscaler**.

© 2025 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ sowie weitere unter **zscaler.com/de/legal/trademarks** aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

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

zscaler™

Zero Trust Everywhere