



# Zscaler per l'industria manifatturiera

Estendere lo zero trust  
al modello Purdue



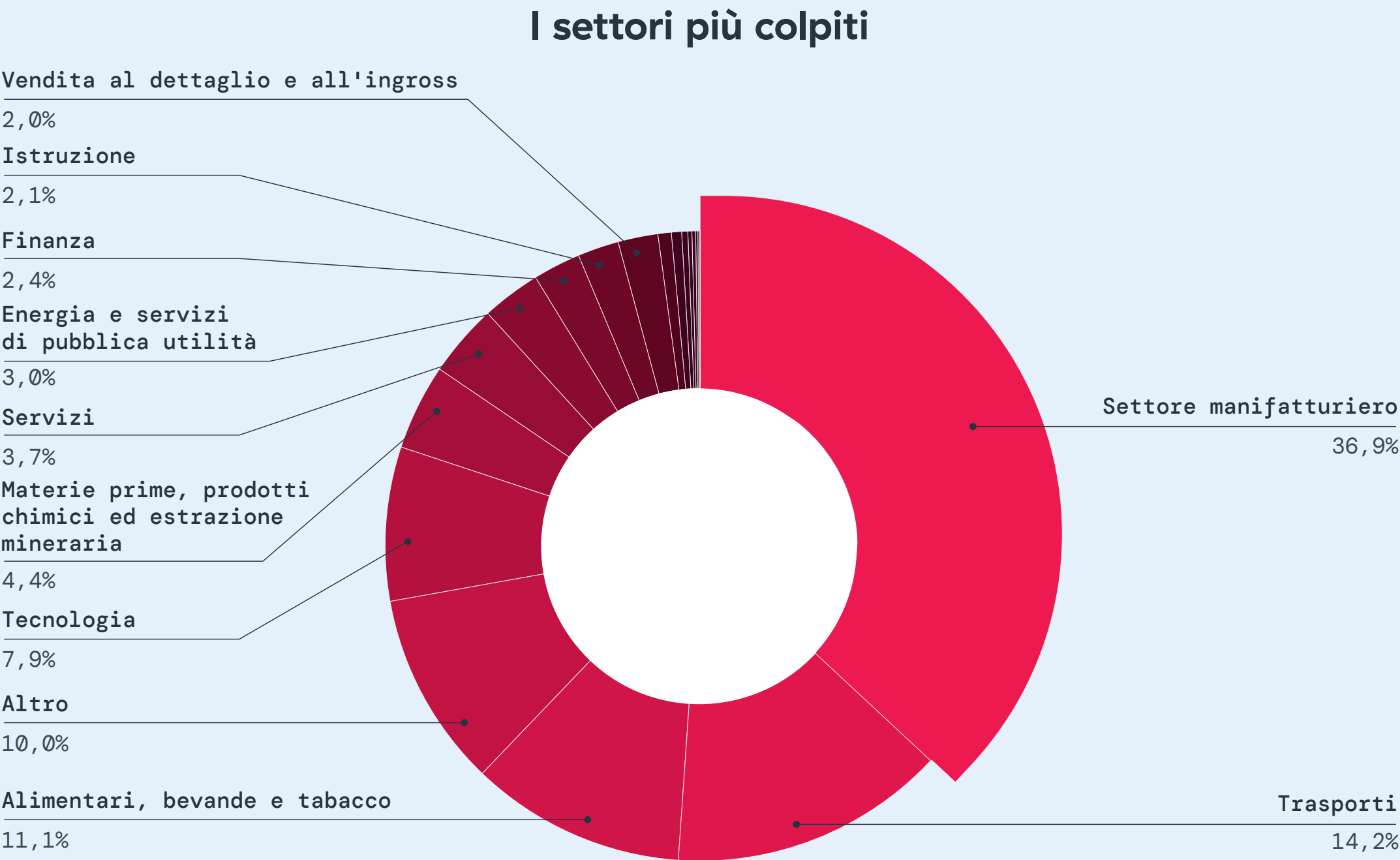


# Gli stabilimenti produttivi hanno bisogno di un nuovo approccio per proteggere i sistemi OT

Le aziende manifatturiere globali si stanno dando da fare per migliorare le proprie linee di produzione, aggiungendo robot intelligenti, sensori IoT su ogni macchinario, analisi basate su cloud e un gemello digitale dell'intero stabilimento. L'obiettivo è semplice: maggiore produttività, tempi di fermo ridotti e manutenzione predittiva che consentono una produzione 24 ore su 24, 7 giorni su 7.

Ma molte organizzazioni si sono rese conto che la realtà è ben diversa. Ogni nuova connessione estende infatti la superficie di attacco dell'OT e, una volta che gli aggressori riescono a entrare, il rischio subire un impatto dirompente si intensifica, questo a causa di sistemi operativi obsoleti, reti piatte e una visibilità limitata sulle risorse OT. Per proseguire nella trasformazione, l'architettura di sicurezza degli stabilimenti produttivi va ripensata.

Nell'ultimo report di Zscaler Threatlabz sulle risorse IoT/OT, il settore manifatturiero è risultato quello più colpito, con il 36% di malware bloccati diretti alle risorse IoT.



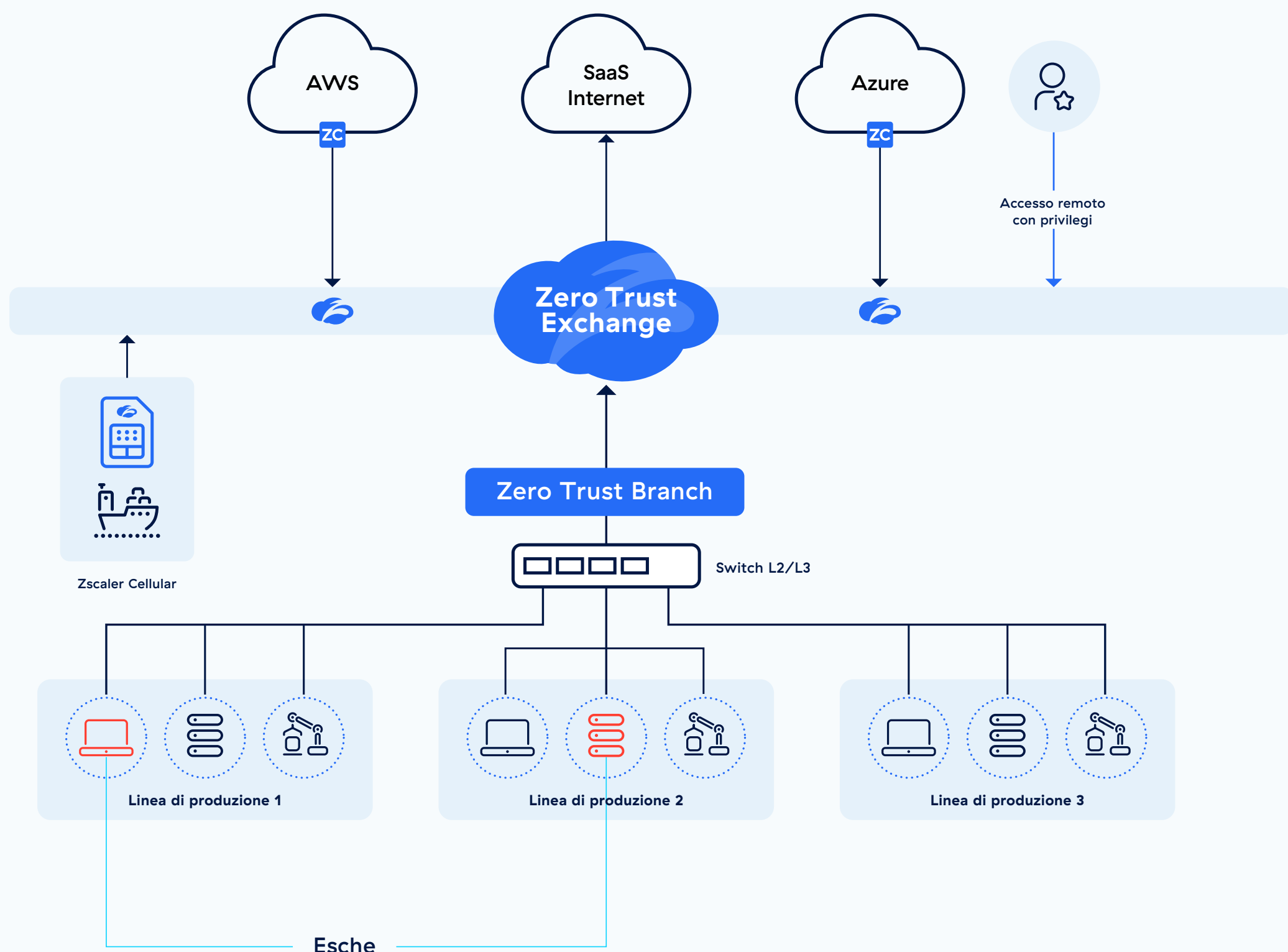
Distribuzione dei settori più colpiti



# Estendi lo zero trust a ogni utente e dispositivo, dentro e fuori dai tuoi stabilimenti produttivi

Per proteggere gli ambienti di produzione e industriali, i team di sicurezza devono garantire che ogni interazione tra utenti e dispositivi venga ispezionata e salvaguardata applicando policy basate sui privilegi minimi. Il nostro approccio allo zero trust è studiato appositamente per l'OT e offre accesso sicuro, segmentazione e connettività per supportare tutte le operazioni degli stabilimenti produttivi.

- Concedi a tecnici e terze parti un accesso ai sistemi OT critici senza VPN
- Implementa una segmentazione granulare est-ovest per impedire il movimento laterale delle minacce
- Connetti in modo sicuro i sistemi OT al cloud e ai data center per l'analisi
- Estendi lo zero trust ai sistemi OT basati su reti cellulari per abbracciare camion, chioschi digitali e scanner POS
- Rileva tempestivamente gli aggressori e impediscigli di accrescere i propri privilegi



**Architettura zero trust per le fabbriche**



# I componenti della soluzione di Zscaler

## Accesso remoto con privilegi

Consenti alle terze parti e ai tecnici in remoto di connettersi in modo sicuro a target RDP/SSH/VNC tramite qualsiasi browser e senza agenti.

### FUNZIONALITÀ PRINCIPALI

|   |   |
|---|---|
| <b>Controlli degli appunti</b><br>Limita le operazioni di copia/incolla con policy zero trust per proteggere i dati sensibili.  | <b>Controlli di audit e governance</b><br>Riduci i rischi associati alle terze parti con la registrazione e la condivisione delle sessioni e l'accesso assistito. |
| <b>Archivio e mappatura delle credenziali</b><br>Memorizza le credenziali dei sistemi target in un archivio cloud e condividi l'accesso seguendo la mappatura delle policy. | <b>Accesso a tempo e just-in-time</b><br>Stabilisci finestre di manutenzione e prevedi l'accesso JIT per la manutenzione di emergenza.                            |

## La segmentazione zero trust

Microsegmenta i sistemi OT e applica policy per garantire solo le comunicazioni autorizzate tra i tuoi sistemi OT e gli altri sistemi OT-IT.

|  |  |
|--|--|
| <b>Microsegmentazione granulare</b><br>Isola i sistemi OT supportati in un segmento univoco (utilizzando /32).   | <b>Rilevamento e classificazione dei dispositivi</b><br>Rileva e classifica in automatico i dispositivi OT.  |
| <b>Kill switch dei ransomware</b><br>Automatizza la risposta agli incidenti utilizzando policy preimpostate per isolare progressivamente i sistemi OT. | <b>Applicazione delle policy</b><br>Raggruppa in automatico i dispositivi e applica le policy al traffico est-ovest in base al tipo di dispositivo e ai tag. |



## Proteggi l'accesso all'OT

Consenti a telecamere, sensori, monitor, chioschi digitali e altri sistemi OT di connettersi in modo sicuro alle applicazioni cloud e a Internet, prevenendo la comunicazione con app e URL rischiosi o dannosi.

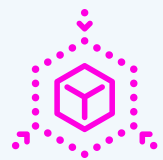
|   |  |
|---|--|
| <b>Provisioning zero touch</b><br>Sfrutta la distribuzione completamente automatizzata e senza intervento umano tramite modelli predefiniti.  | <b>Policy zero trust unificate</b><br>Ispeziona e applica le policy per IoT/OT, app private e Internet.  |
| <b>Applicazione granulare delle policy</b><br>Applica le policy in base a fattori quali geolocalizzazione di utente/dispositivo, posizione, URL a cui si accede, dati sensibili e altro ancora. | <b>Zero trust per le reti cellulari</b><br>Estendi facilmente lo zero trust ai dispositivi collegati tramite reti cellulari come camion, chioschi digitali, piattaforme ecc. |

## Zscaler Deception

Utilizza delle esche per rilevare le minacce OT che hanno aggirato le difese esistenti. Rileva gli utenti compromessi, blocca il movimento laterale e difenditi da ransomware e utenti interni malintenzionati.

|   |  |
|---|--|
| <b>Rilevamento del movimento laterale:</b><br>Distribuisci PLC e sistemi SCADA esca per rilevare gli aggressori che tentano di muoversi lateralmente. | <b>Rilevamento pre-violazione</b><br>Ricevi allerte attendibili che ti avvisano quando degli aggressori stanno esaminando il tuo ambiente prima di un attacco. |
| <b>Distribuzione nativa del cloud</b><br>Integrazione con Zscaler Private Access (ZPA) per creare, ospitare e distribuire esche.                      | <b>Zero configurazioni di rete</b><br>Dimenticati di trunking VLAN, porte SPAN e tunnel GRE per instradare il traffico verso le esche.                         |

# Cosa contraddistingue Zscaler



## ELIMINARE LE LACUNE NELLA SICUREZZA

Applica policy zero trust coerenti in tutti gli ambienti, all'interno e all'esterno delle tue fabbriche.



## RIDUCI IL DOWNTIME

Applica la segmentazione zero trust con un'alterazione minimale dell'ambiente OT esistente, riducendo il rischio di incorrere in periodi di fermo dovuti al movimento laterale.



## RIDUCI COSTI E COMPLESSITÀ

Riduci o consolida firewall, NAC, VPN, VDI e strumenti di microsegmentazione adottando nelle tue fabbriche un'architettura di sicurezza più semplice, basata sul modello Purdue.

### Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita [zscaler.com/it](https://zscaler.com/it) oppure seguici su X (precedentemente Twitter) @zscaler.

© 2025 Zscaler, Inc. Tutti i diritti riservati. Zscaler™ e gli altri marchi commerciali presenti su [zscaler.com/it/legal/trademarks](https://zscaler.com/it/legal/trademarks) sono (I) marchi commerciali o marchi di servizio registrati o (II) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi commerciali sono di proprietà dei rispettivi titolari.



**Zero Trust  
Everywhere**