Zscaler Zero Trust Segmentazione dei dispositivi per l'Industria 4.0

WHITE PAPER

Nell'era dell'Industria 4.0, in cui la produzione intelligente e i sistemi industriali interconnessi stanno diventando la norma, l'architettura zero trust si è affermata come un framework di sicurezza fondamentale. Gli approcci alla sicurezza tradizionali e basati sul perimetro non sono più sufficienti a proteggere il complesso ecosistema di dispositivi di tecnologia operativa (OT) e dei sistemi di controllo industriale. Il principio fondamentale dello zero trust, che si basa sulla verifica continua delle entità, elimina la fiducia implicita nella rete e garantisce un accesso sicuro e autenticato ai sistemi critici. Questo approccio è particolarmente cruciale negli ambienti industriali, in cui una violazione della sicurezza potrebbe comportare notevoli tempi di inattività, perdita di reputazione e ripercussioni normative.

Sicurezza informatica per la produzione

Le moderne reti di produzione si sono evolute in ecosistemi complessi, in cui le tecnologie operative (OT) e le tecnologie informatiche (IT) sono profondamente interconnesse. Questa convergenza ha consentito lo sviluppo di funzionalità avanzate, come la manutenzione predittiva, l'integrazione della catena di approvvigionamento e la gestione delle operazioni da remoto. Tuttavia, questa interconnettività crea anche nuove sfide per la sicurezza, in quanto le reti OT, che tradizionalmente erano isolate, diventano esposte a minacce legate all'IT. Ci sono due grandi aree su cui le organizzazioni si stanno concentrando:

- **Accesso sicuro alle risorse OT:** gli ambienti di produzione richiedono un controllo rigoroso su chi può accedere alle risorse tecnologiche operative come PLC, HMI e sistemi di controllo industriale. Zscaler Privileged Remote Access consente un accesso rapido, diretto e sicuro alle risorse tecnologiche operative (OT) sul campo, in fabbrica e in qualsiasi altro luogo, senza dover ricorrere a VPN o agenti. Ulteriori informazioni su Zscaler Privileged Remote Access: https://www.zscaler.com/it/resources/data-sheets/privileged-remote-access-for-ot-and-iiot.pdf

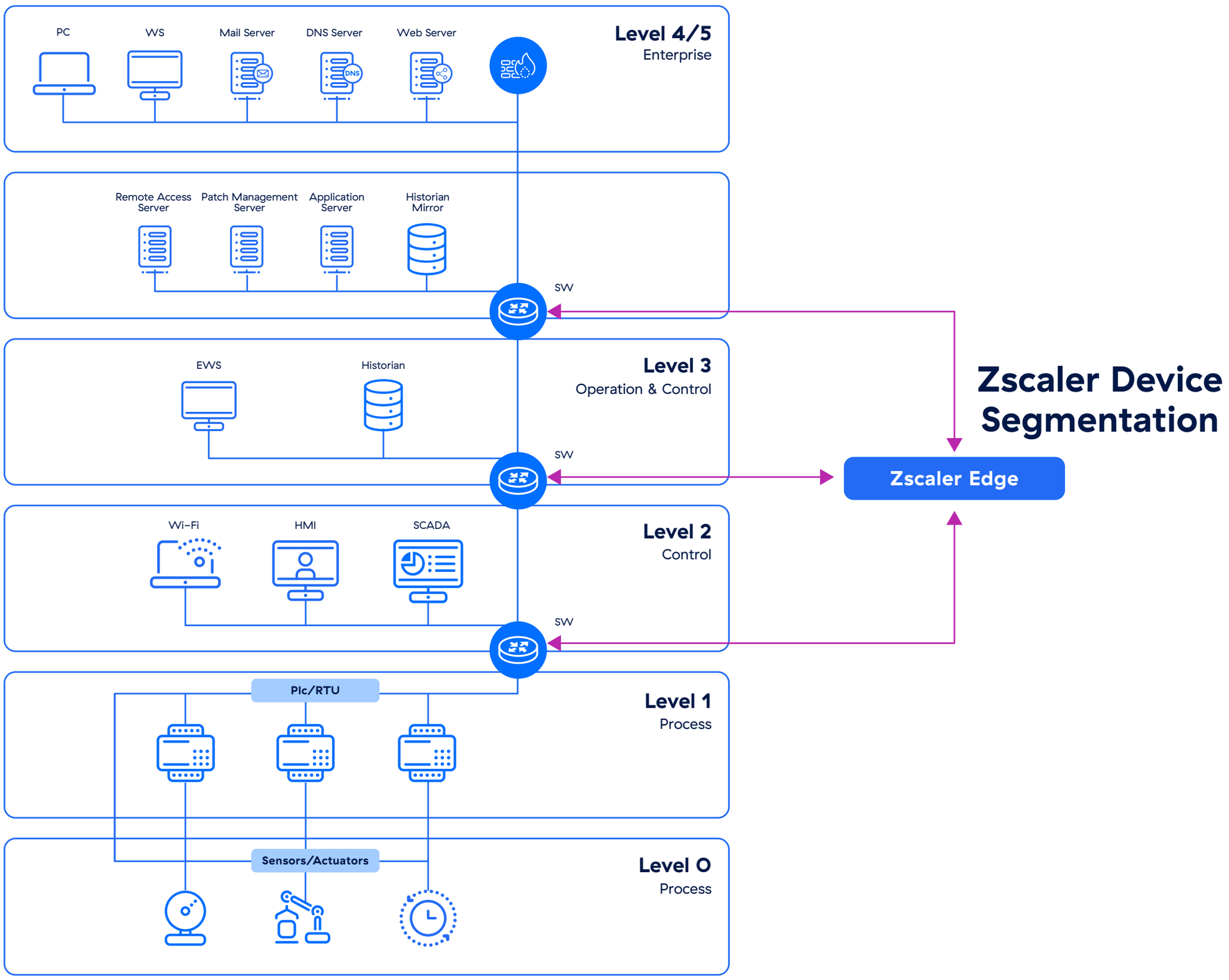
- **Segmentazione:** una preoccupazione critica per la sicurezza negli ambienti di produzione è la possibilità che le minacce si spostino lateralmente attraverso la rete. Questo è particolarmente pericoloso negli ambienti industriali, in cui

i sistemi legacy, spesso privi di moderne funzionalità di sicurezza, sono interconnessi con apparecchiature moderne. L'implementazione dei principi dello zero trust tramite la microsegmentazione aiuta a contenere le minacce applicando un rigoroso controllo degli accessi alla rete basato su policy, limitando di fatto la capacità di un aggressore di muoversi lateralmente anche in caso di violazione delle difese iniziali.

La combinazione di soluzioni zero trust per l'accesso privato con la segmentazione consente di stabilire un solido framework di sicurezza per le risorse OT nelle reti di produzione. Questa strategia di sicurezza completa garantisce che le attività di produzione rimangano protette sia da minacce esterne che da vulnerabilità interne, mantenendo al contempo la flessibilità necessaria per svolgere operazioni efficienti.

Segmentazione nel settore manifatturiero

Nelle tipiche reti di produzione o di controllo industriale ci sono vari tipi di dispositivi connessi alla rete. Secondo il modello Purdue, questi dispositivi possono essere classificati in livelli distinti.



Livello Purdue	Dispositivi	Descrizione	Rischio
Livello 3	Historian, Jump Server, Server per la gestione delle patch	Esegue sistemi operativi noti, ad esempio Windows Nonostante le opzioni EDR, rappresentano comunque un rischio per la sicurezza a causa delle minacce laterali	Da medio ad alto
Livello 2	HMI, SCADA	Eseguono il sistema operativo incorporato (ad esempio Windows CE, Windows XP). A causa della loro natura obsoleta, questi sistemi presentano gravi vulnerabilità e rischi significativi per la sicurezza.	Alto
Livello 1	PLC, RTU	Dispositivi headless di fascia bassa che richiedono strumenti speciali per la programmazione e la modifica delle impostazioni	Da basso a medio
Livello 0	Sensori, attuatori	Per lo più sistemi non basati su IP che eseguono funzioni molto specifiche	Basso

Questi vari tipi di dispositivi OT stabiliscono modelli di comunicazione complessi e dipendenze tra loro per mettere in atto processi di produzione senza interruzioni, mantenere la continuità operativa e assicurare una produzione affidabile in tutto lo stabilimento. Zscaler Zero Trust Device Segmentation (Zscaler ZTDS) fornisce misure di sicurezza complete per proteggere le operazioni di produzione implementando solidi controlli degli accessi e stabilendo chiari confini di comunicazione tra diverse tipologie di dispositivi industriali. Questa strategia di segmentazione avanzata aiuta a mantenere l'integrità e l'affidabilità dei processi di produzione, proteggendoli al contempo da potenziali minacce alla sicurezza e tentativi di accesso non autorizzati.

Caso d'uso 1

Comunicazioni Internet

Negli ambienti di produzione moderni, i sistemi OT richiedono sempre più la connettività Internet per diverse esigenze operative, tra cui aggiornamenti software, supporto dei fornitori e analisi basate su cloud. Tuttavia, questa esposizione a Internet amplia notevolmente la superficie di attacco delle reti industriali. I sistemi OT, che prima erano isolati, ora sono vulnerabili alle minacce informatiche più comuni, come malware, ransomware e minacce persistenti avanzate (APT). I rischi sono particolarmente significativi, perché molti dispositivi OT sono stati progettati senza funzionalità di sicurezza integrate e spesso utilizzano sistemi operativi obsoleti che non possono essere facilmente aggiornati o corretti.

Tutte le comunicazioni Internet sono protette da Zscaler ZIA, e le connessioni in uscita dalle risorse OT vengono instradate tramite questo servizio.

I VANTAGGI DI ZSCALER ZIA

- **Protezione avanzata dalle minacce:** Zscaler Internet Access (ZIA) fornisce una sicurezza completa contro malware, ransomware e minacce zero-day attraverso l'ispezione multilivello di tutto il traffico Internet proveniente dalle risorse OT

- **Filtraggio in uscita:** applica rigorosi controlli degli accessi limitando le comunicazioni dei dispositivi OT solo alle destinazioni autorizzate e bloccando siti web e contenuti potenzialmente dannosi

- **Intelligence sulle minacce in tempo reale:** usa l'intelligence globale del cloud per identificare e bloccare le minacce emergenti prima che possano avere un impatto sulle risorse OT

Caso d'uso 2

Comunicazioni tra OT e IT

La comunicazione tra OT e IT negli ambienti di produzione rappresenta un'intersezione critica in cui i sistemi OT devono interagire con l'infrastruttura IT. Questa integrazione consente funzioni essenziali come l'analisi dei dati, il monitoraggio da remoto e la pianificazione delle risorse aziendali. Tuttavia, queste comunicazioni creano anche notevoli vulnerabilità di sicurezza. Le reti IT, che in genere sono connesse a Internet e vengono regolarmente aggiornate, devono interfacciarsi con sistemi OT che spesso utilizzano software e protocolli obsoleti e non progettati per la sicurezza moderna.

Questa disparità nelle capacità di sicurezza crea potenziali punti d'ingresso per gli attacchi informatici.

I VANTAGGI DELLA SEGMENTAZIONE DEI DISPOSITIVI CON ZSCALER:

- In passato, le reti IT e OT venivano progettate come sistemi separati, ed erano tenuti isolati l'uno dall'altro tramite veri e propri air gap fisici. Tuttavia, con la modernizzazione, questi confini si stanno assottigliando. Zscaler Device Segmentation aiuta a mantenere la separazione tra reti IT e OT senza compromettere la produttività e i vantaggi offerti dalla modernizzazione.

- Nonostante abbiano VLAN separate, i sistemi IT e OT finiscono spesso per condividere la stessa rete a causa di configurazioni errate o rapidi cambiamenti aziendali. La tecnologia brevettata di Zscaler ZTDS identifica tutti i sistemi IT e OT nella rete condivisa (come le VLAN) e le separa logicamente senza richiedere la riconfigurazione delle VLAN, modifiche dell'IP o la riprogettazione della rete.

- Per proteggere le apparecchiature legacy e impedire l'accesso non autorizzato alle reti OT, Zscaler ZTDS aiuta a eliminare la fiducia implicita e limita l'accesso alla rete da un sistema specifico come JumpHosts, Zscaler ZPA e Zscaler PRA.

- Un sistema di gestione centralizzato e altamente scalabile basato sul cloud con un solido controllo degli accessi in base ai ruoli e capacità multi-tenancy semplifica le operazioni di rete IT e OT mantenendo al contempo compiti e controlli amministrativi separati.

Caso d'uso 3

Comunicazioni a livello operativo

Al livello 3, le comunicazioni a livello operativo comprendono le interazioni tra vari sistemi MES (Manufacturing Execution Systems, ovvero sistemi software che gestiscono e controllano e i processi di produzione), historian e altre applicazioni di gestione operativa. Questi sistemi in genere funzionano su reti standard TCP/IP, che spesso utilizzano protocolli come OPC UA, MQTT o REST API per lo scambio di dati. In questo caso, la segmentazione della rete è particolarmente importante, in quanto questi sistemi spesso colmano il divario tra le reti IT e OT, rendendole potenziali bersagli per gli attacchi informatici.

I VANTAGGI DELLA SEGMENTAZIONE DEI DISPOSITIVI CON ZSCALER:

- A differenza dei firewall tradizionali, Zscaler ZTDS funziona in modo indipendente dai dettagli della rete e consente il controllo dinamico delle policy indipendentemente dal modo in cui i sistemi del livello operativo si connettono alla rete. Un motore di policy adattivo centralizzato riduce significativamente la complessità operativa associata ai firewall tradizionali

- Una risposta efficace agli incidenti è fondamentale per ridurre l'impatto degli incidenti informatici negli ambienti mission-critical. Zscaler Ransomware Kill-Switch è un potente strumento di risposta agli incidenti che prepara le organizzazioni alla risposta di emergenza e blocca in modo mirato la propagazione delle minacce a livello di rete.

- L'architettura unica di Zscaler ZTDS centralizza tutta l'intelligence a livello di rete ed elimina le dipendenze da prodotti isolati e tecnologie complesse come VLAN, ACL, 802.1X, Firewall e routing L3.

Caso d'uso 4

Comunicazioni a livello di supervisione

Al livello 2, le comunicazioni a livello di supervisione implicano interazioni critiche tra HMI, sistemi SCADA e altri sistemi di controllo di supervisione su reti TCP/IP. Questi sistemi in genere comunicano utilizzando protocolli industriali come Modbus TCP, EtherNet/IP e OPC UA su porte di rete standard (502 per Modbus, 44818 per EtherNet/IP, 4840 per OPC UA). Sono responsabili del monitoraggio e del controllo dei processi industriali, della raccolta di dati in tempo reale e della fornitura di interfacce operatore. Data la natura obsoleta di molti sistemi di supervisione, l'uso di protocolli potenzialmente vulnerabili e il loro ruolo critico nelle operazioni, la protezione di queste comunicazioni è particolarmente importante e deve essere attuata attraverso un'adeguata segmentazione della rete e controlli di sicurezza specifici per protocollo. Le comunicazioni possono essere ulteriormente suddivise in:

1. **Comunicazioni tra livelli 2 (ad esempio, interazioni HMI–HMI)**
2. **Comunicazioni da livello 2 a livello 3 (ad esempio, trasferimento dati da HMI a Historian)**

I VANTAGGI DELLA SEGMENTAZIONE DEI DISPOSITIVI CON ZSCALER:

- La tecnologia brevettata di Zscaler ZTDS protegge in modo unico i sistemi di supervisione (come gli HMI) connessi al livello 2 del modello Purdue, creando confini di isolamento sicuri che riducono significativamente la superficie di attacco su questi sistemi legacy e vulnerabili.

- Zscaler ZTDS rileva e visualizza tutte le comunicazioni tra dispositivi a livello di supervisione e le interazioni con il livello 3 (livello operativo), indipendentemente dalla configurazione VLAN. Genera mappe del traffico di queste comunicazioni e mantiene i log delle transazioni nel SIEM integrato basato su Elastic.

- Basato sui principi dello zero trust, Zscaler ZTDS si integra con vari strumenti aziendali, tra cui CMDB ed EDR, per adattare automaticamente le policy di controllo degli accessi in base ai cambiamenti comportamentali. Un framework di policy gerarchico consente l'implementazione di policy in un singolo sito, in più gruppi di siti o in tutti i siti.

- Un framework di policy semplificato che utilizza attributi e tag dei dispositivi (tramite tagging automatico, inserimento manuale o importazione da terze parti) anziché indirizzi IP e MAC complessi

- Uno dei maggiori vantaggi di Zscaler ZTDS è che non richiede l'uso di agenti, interagisce con le apparecchiature di rete esistenti (indipendentemente dal fornitore, dal modello o dalla versione) e richiede modifiche minime alla configurazione di rete.

Caso d'uso 5

Comunicazione a livello di controllo

Al livello 1, i PLC e le RTU interagiscono tra loro per coordinare le operazioni dei dispositivi e il controllo dei processi. Questi dispositivi comunicano anche verso l'alto con sistemi di Livello 2 come HMI e sistemi SCADA per consentire il monitoraggio e il controllo dei processi industriali in tempo reale. Questo livello di comunicazione è fondamentale per

mantenere l'efficienza operativa, e richiede misure di sicurezza solide per la difesa da potenziali minacce informatiche garantendo al contempo una latenza minima e un'elevata affidabilità. Le comunicazioni possono essere ulteriormente suddivise in:

1. **Comunicazioni tra dispositivi del Livello 1 (ad esempio, comunicazioni PLC–PLC)**
2. **Comunicazioni tra dispositivi del Livello 1 e del Livello 2 (ad esempio, comunicazioni PLC–HMI)**

I VANTAGGI DELLA SEGMENTAZIONE DEI DISPOSITIVI CON ZSCALER:

- Grazie alla sua architettura unica, Zscaler ZTDS visualizza e analizza varie comunicazioni e offre la possibilità di rilevare le impronte digitali e di profilare i sistemi OT connessi. Analizza i vari protocolli, tra cui HTTP, ENIP, Modbus, SSL ecc., ed estrae informazioni sui metadati per identificare e taggare con precisione le risorse OT.

- Visualizza tutte le comunicazioni tra i dispositivi L1 (PLC, RTU) e i sistemi L2 (HMI, SCADA). Implementa controlli di accesso limitati per proteggere i dispositivi L1 sensibili (ad esempio PLC) da dispositivi L2 ad alto rischio potenzialmente vulnerabili (ad esempio HMI).

- Quando implementato in modalità di apprendimento, Zscaler ZTDS identifica accuratamente i modelli di comunicazione dai dispositivi L1 (PLC, RTU) a quelli L2 (HMI e altri). Questo aiuta a modellare le policy di segmentazione.

- I dispositivi al Livello 1 del modello Purdue sono progettati per funzioni specifiche e non implementano tutti i principi standard delle reti. Questo complica l'implementazione di Zscaler ZTDS Ringfence per questi dispositivi. Tuttavia, la mancanza di segmentazione o di separazione per dispositivo non compromette i controlli di sicurezza complessivi.

- Poiché le minacce provengono in genere da dispositivi di Livello 2 vulnerabili e ad alto rischio, ZTDS limita l'accesso dei dispositivi di Livello 1 solo ai dispositivi di Livello 2 richiesti per le operazioni aziendali.

- Invece della segmentazione per dispositivo, ZTDS implementa la segmentazione a livello macro (utilizzando la definizione di rete esistente) o la segmentazione a livello di gruppo (i dispositivi L1 possono essere raggruppati in piccoli segmenti utilizzando Airgap-Plus).

- Dato che la comunicazione tra dispositivi L1-L1 richiede una programmazione speciale, ZTDS riduce le modifiche non autorizzate o errate della programmazione limitando l'accesso in ingresso ai dispositivi L1.

- Tutte le altre funzionalità, tra cui l'individuazione e la profilazione delle risorse, la visualizzazione del traffico, il controllo adattivo delle policy e il kill switch anti-ransomware, restano pienamente applicabili ai dispositivi di Livello 1.

I dispositivi al Livello 0 del modello Purdue, o a livello di processo (ad esempio sensori e attuatori) non supportano TCP/IP e si collegano generalmente direttamente tra loro o ai dispositivi di Livello 1 tramite protocolli proprietari, bus seriali, ecc. Questi dispositivi sono al di fuori dell'ambito di Zscaler Devices Segmentation.

Riepilogo

In quanto componente fondamentale della sicurezza zero trust, la soluzione Zscaler Zero Trust Device Segmentation svolge un ruolo cruciale nell'eliminazione della fiducia implicita creando confini logici tra diversi tipi di dispositivi e sistemi industriali. Implementando policy di segmentazione granulare, le organizzazioni possono isolare i sistemi di produzione critici dai dispositivi potenzialmente vulnerabili, contenere le violazioni della sicurezza e mantenere rigorosi controlli di accesso tra i diversi livelli.

	Caso d'uso 1 (Internet)	Caso d'uso 2 (IT e OT)	Caso d'uso 3 (L3 — Operazioni)	Caso d'uso 4 (L2 — Supervisione)	Caso d'uso 5 (L1 — Controllo)
Senza agente	✓	✓	✓	✓	✓
Indipendente dalla rete	✓	✓	✓	✓	✓
Rilevamento e profilazione delle risorse	✓	✓	✓	✓	✓
Visibilità sul traffico	✓	✓	✓	✓	Tra segmenti
Integrazione con terze parti	N/D	✓	✓	✓	✓
Controllo adattivo delle policy	✓	✓	✓	✓	Tra segmenti
Ransomware Kill Switch	N/D	✓	✓	✓	✓
Gestione centralizzata	✓	✓	✓	✓	✓

I progetti di segmentazione spesso non vengono completati perché le alternative attuali richiedono modifiche significative alla rete (come l'aggiornamento o la ristrutturazione delle apparecchiature), non offrono un controllo granulare o non riescono a coprire tutti i livelli delle reti di produzione. Zscaler ZTDS offre una soluzione unica che garantisce una copertura completa tramite una piattaforma senza agente, indipendente dalla rete e intuitiva. Zscaler ZTDS si implementa rapidamente e non richiede tempi di inattività operativa. Le aziende manifatturiere possono ora unirsi alle aziende Fortune 500 e utilizzare Zscaler Zero Trust Device Segmentation (ZTDS) per implementare rapidamente la segmentazione zero trust, proteggendo le loro reti di controllo industriale e di tecnologia operativa (OT) critiche.

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 **www.zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/it**

zscaler™

Zero Trust Everywhere