Zscaler Zero Trust Device Segmentation per OT/IoT

Blocca il movimento laterale,
riduci la superficie di attacco
e potenzia la sicurezza operativa

Panoramica sulla soluzione

Il problema da affrontare

Di recente, gli Stati Uniti hanno registrato un incremento di avvisi e allerte riguardanti attacchi informatici lanciati da aggressori che agiscono con il supporto di Stati nazionali per colpire infrastrutture critiche del Paese. Il 7 febbraio 2024, l'FBI (Federal Bureau of Investigation) e la CISA (Cybersecurity and Infrastructure Security Agency), insieme alla National Security Agency, hanno emesso un avviso rivolto alle organizzazioni governative per allertarle della presenza di hacker pronti a danneggiare infrastrutture critiche, come sistemi di trasporto, oleodotti e gasdotti, impianti di trattamento delle acque e reti elettriche. Questa comunicazione va ad aggiungersi ad azioni analoghe intraprese dalla TSA per proteggere aeroporti, operatori aerei e reti ferroviarie, come il recente standard del Dipartimento dell'Energia degli Stati Uniti (DOE) e la revisione quasi definitiva della normativa CIP-015-1 da parte della NERC.

Le tecnologie OT/IoT sono state progettate per garantire velocità ed efficienza nelle transazioni, mettendo però la sicurezza in secondo piano. Purtroppo, l'OT/IoT è ormai uno degli obiettivi prediletti dai criminali informatici; secondo la ricerca condotta da Zscaler ThreatLabz, i dispositivi OT/IoT hanno subito un aumento del 400% del numero di attacchi rispetto all'anno precedente. I ransomware sono la strategia di attacco più diffusa, e il 61% di tutte le violazioni ha preso di mira organizzazioni con tecnologie OT connesse.

Qual è la soluzione?

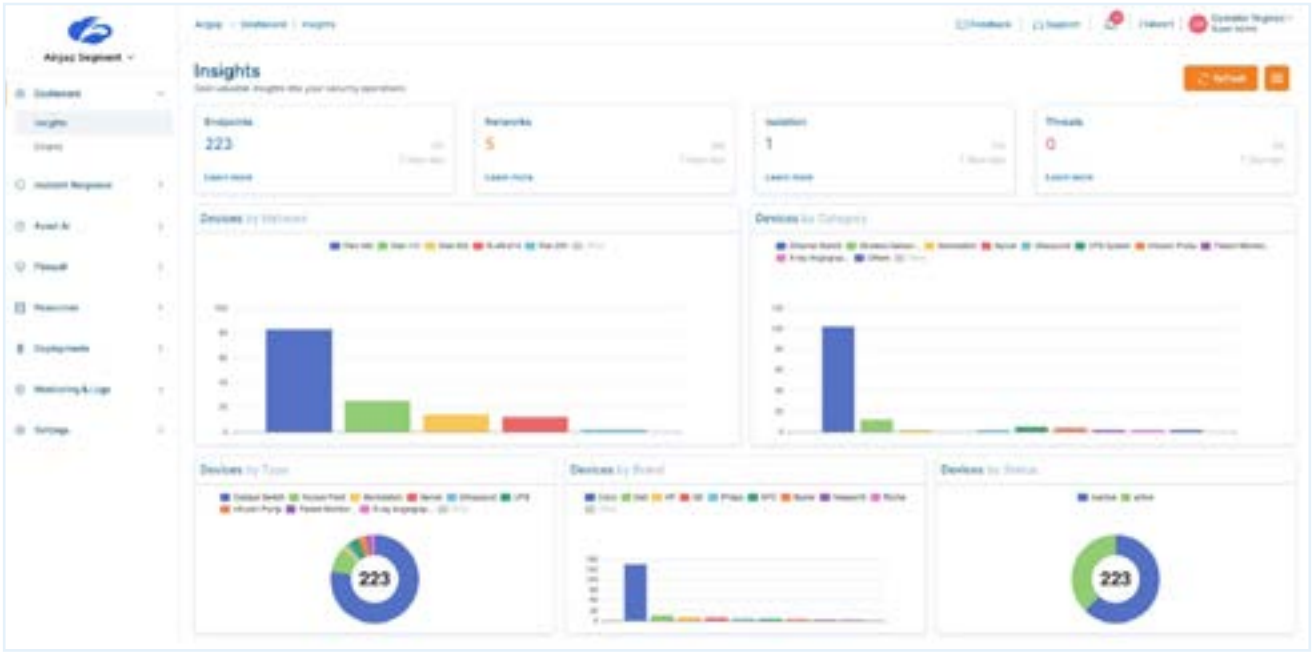
EPA, CISA ed FBI raccomandano caldamente agli operatori di sistemi di attenersi all'ordine esecutivo dell'Ufficio del Presidente, che indica di utilizzare il modello zero trust come linea guida per potenziare la sicurezza informatica.

Gli elementi evidenziati rappresentano le aree principali di queste raccomandazioni governative, in cui Zscaler può fornire un aiuto immediato e concreto grazie alla soluzione Zero Trust Device Segmentation.

- Riduzione dell'esposizione alla rete Internet pubblica
- Riduzione dell'esposizione alle vulnerabilità
- Segmentazione della rete
- Raccolta dei log
- Proibizione della connessione di utenti non autorizzati
- Eliminazione di servizi sfruttabili da Internet
- Limitazione delle connessioni OT/IoT rivolte a Internet
- Rilevamento delle minacce rilevanti
- Creazione di un inventario di risorse OT/IT

Come agire?

La segmentazione è da tempo un elemento fondamentale delle operazioni di rete, e il traffico nord-sud (client-server) viene gestito da strumenti come gli elenchi di controllo degli accessi (ACL) e i firewall. La micro-segmentazione OT sposta però l'attenzione sul traffico est-ovest, che risulta più vulnerabile e che consiste nel traffico che si muove lateralmente, quindi tra dispositivi e workload. Nelle VLAN condivise, a causa della presenza di architetture di switching legacy, tutti i dispositivi possono vedersi e comunicare tra loro, creando così un ambiente favorevole alla diffusione dei malware. Purtroppo, quando le soluzioni basate su agente vengono applicate ai workload cloud, esse risultano incapaci di segmentare i dispositivi legacy e headless comuni nell'OT, e gli approcci tradizionali basati su ACL sono eccessivamente complicati.



Dashboard di Zero Trust Device Segmentation

Zscaler elimina gli ostacoli della segmentazione intra-VLAN con una soluzione agentless in grado di bloccare tutte le minacce laterali, isolando tutti gli endpoint con IP, inclusi i sistemi legacy e headless, in un "segmento di rete univoco". In questo modo, si elimina la necessità di ricorrere ad ACL complesse e di effettuare modifiche all'infrastruttura esistente, garantendo al contempo una segmentazione molto più granulare ed efficace.

Casi d'uso

Ecco alcuni dei casi d'uso più comuni della segmentazione dei dispositivi agentless:

Microsegmentazione della LAN

Implementando la segmentazione sul traffico est-ovest, si estende il concetto di zero trust alla LAN. Oltre a ridurre la superficie di attacco interna, questo elimina la minaccia di movimento laterale nelle reti OT/IoT critiche, senza il bisogno di ricorrere a sistemi NAC o alla segmentazione basata su firewall.

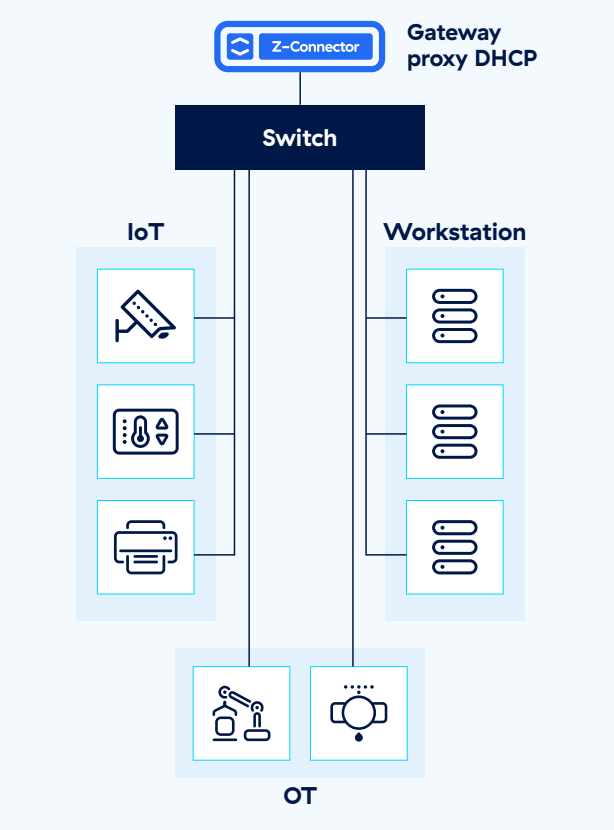
Per applicare la segmentazione zero trust alla rete è necessario:

- Assicurarsi che ogni singolo dispositivo sia associato a un segmento univoco (/32)
- Raggruppare in automatico dispositivi, utenti e app analizzandone i modelli di traffico ed impedendo ai dispositivi non autorizzati di utilizzare lo spoofing dei MAC per accedere alla rete
- Applicare dinamicamente le policy al traffico est-ovest in base all'identità e al contesto di utenti e dispositivi

Segmentazione IT/OT

La tecnologia di Zscaler Zero Trust Device Segmentation agisce come un kill switch anti-ransomware, disabilitando le comunicazioni non essenziali tra i dispositivi per bloccare il movimento laterale delle minacce senza interrompere le operazioni aziendali. Questa soluzione neutralizza le minacce avanzate, come i ransomware, su dispositivi IoT, sistemi OT e dispositivi che non supportano l'uso degli agenti.

- Raggruppa e applica policy autonomamente per gli indirizzi MAC noti su qualsiasi dispositivo (ad esempio, accesso RDP alle telecamere negato tranne che per gli amministratori)
- Isola automaticamente gli indirizzi MAC sconosciuti per limitare il raggio di azione in caso di compromissione di un dispositivo
- Esegui l'integrazione con i sistemi di gestione delle risorse al fine di ottenere policy sicure di controllo degli accessi.



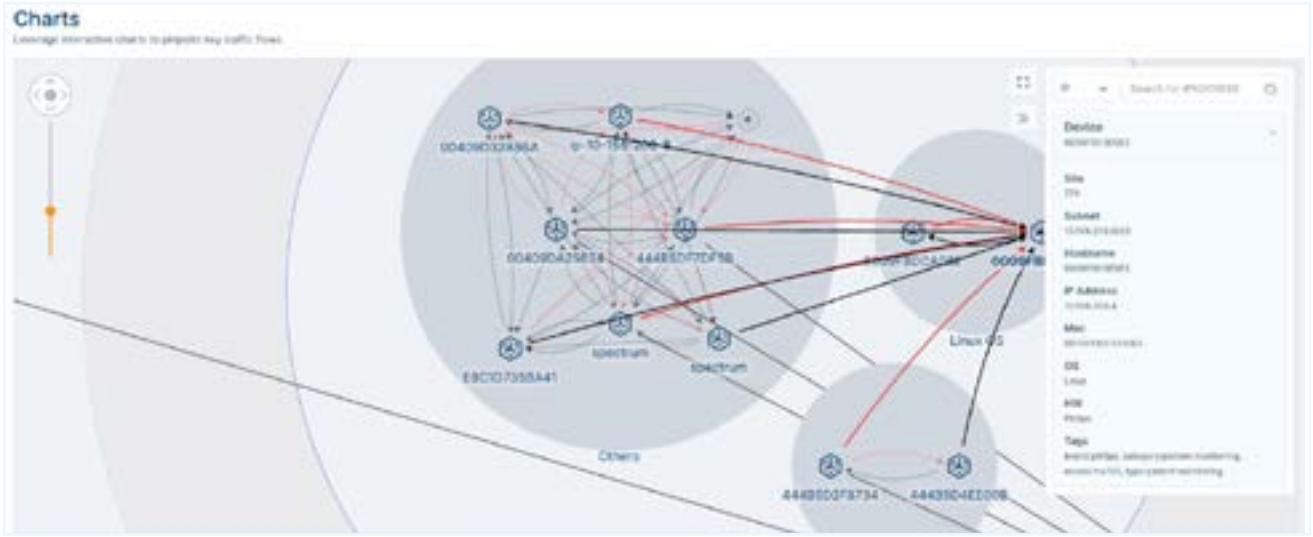
La segmentazione IoT/OT automatica prevede la creazione di un segmento "univoco" per ogni dispositivo

Rilevamento e classificazione automatica dei dispositivi

Dato che una parte significativa del traffico OT/IoT rimane all'interno della rete locale, è importante avere una visibilità continua sul traffico est-ovest. Grazie al rilevamento e alla classificazione automatica dei dispositivi, gli amministratori di rete possono gestire in modo ottimale le prestazioni, i tempi di attività e la sicurezza dei sistemi IoT/OT senza una gestione complessa dell'inventario.

Per la visibilità su rete e dispositivi:

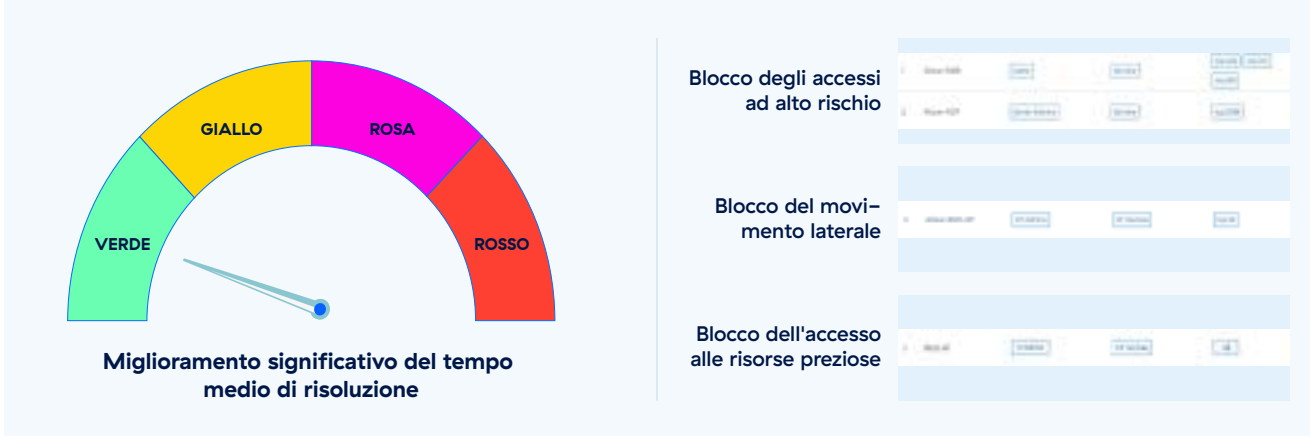
- Rileva, classifica i dispositivi OT/IoT ed eseguine l'inventario senza la necessità di agenti per gli endpoint
- Ottieni un modello di riferimento per i pattern del traffico e i comportamenti dei dispositivi per distinguere l'accesso autorizzato da quello non consentito
- Ricevi informazioni dettagliate sulla rete per la gestione delle prestazioni e la mappatura delle minacce



Dashboard di Device Discovery

Risposta automatica agli incidenti

Zscaler Ransomware Kill Switch fa in modo che la riduzione della superficie di attacco sia selezionabile da parte dell'utente. A quest'ultimo basterà infatti selezionare un livello di gravità preimpostato per bloccare progressivamente le porte e i protocolli vulnerabili noti e persino disabilitare istantaneamente l'accesso a intere reti, come ad esempio linee di produzione e reparti ospedalieri. Questo approccio consente di eliminare le incertezze durante una violazione, sfruttando parametri selezionabili e adattabili in base al tipo di minaccia ma preservando al contempo l'operatività aziendale.



Parla con una persona esperta

Vuoi saperne di più su come Zscaler può aiutarti a proteggere le infrastrutture critiche della tua organizzazione? Fissa un appuntamento per parlare con uno dei nostri tecnici esperti.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su X (precedentemente Twitter) sull'account **@zscaler**.

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