SCHEDA TECNICA

Zero Trust Device Segmentation

Protezione semplificata dalle minacce laterali per reti di filiali, stabilimenti e campus

La segmentazione dei dispositivi, una parte integrante di Zscaler Zero Trust Networking, aiuta i team IT a ridurre i rischi, raggiungere la conformità e aumentare i tempi di attività aziendali, eliminando il movimento laterale delle minacce nella rete.

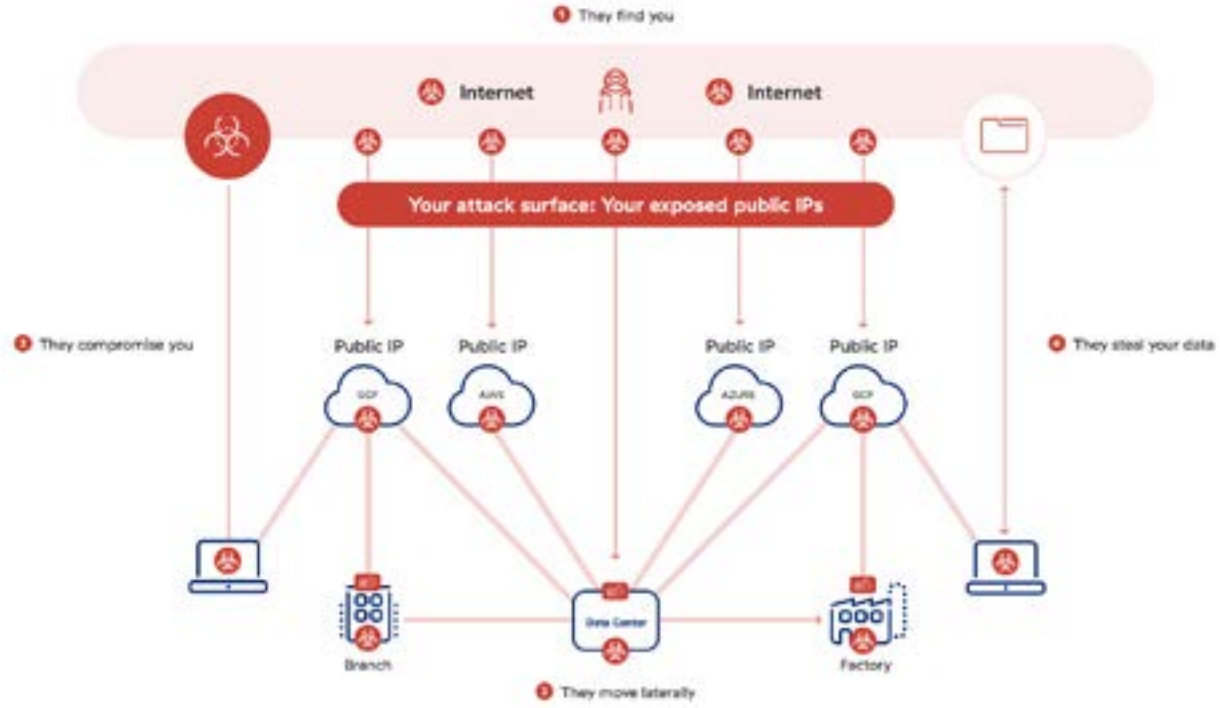
L'evoluzione del panorama delle minacce e della conformità

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; tuttavia, quello della sicurezza è stato un obiettivo secondario. Purtroppo, l'OT/IoT è ormai uno dei target prediletti dai criminali informatici: secondo la ricerca condotta da Zscaler ThreatLabz, i dispositivi OT/IoT hanno registrato un aumento del 400% del numero di attacchi subiti rispetto all'anno precedente. I ransomware sono la strategia di attacco più diffusa; il 61% di tutte le violazioni ha preso di mira organizzazioni con tecnologie OT connesse.

Zscaler Zero Trust Networking

Un mezzo più semplice, sicuro ed economico per la comunicazione tra utenti, dispositivi e workload



Come avvengono gli attacchi ransomware

EPA, CISA ed FBI raccomandano caldamente agli operatori di attenersi all'ordine esecutivo dell'Ufficio del Presidente, che indica l'utilizzo del 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 delle risorse OT/IT

Un'architettura più sicura per la segmentazione dei dispositivi

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 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, 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 ha introdotto Zero Trust Networking per offrire un mezzo più semplice, sicuro e conveniente per la comunicazione tra utenti, dispositivi e workload. La segmentazione dei dispositivi è fondamentale in questo approccio, in quanto stabilisce una visibilità e un controllo granulari per la rete moderna.

Zscaler elimina gli ostacoli della segmentazione intra-VLAN con una soluzione agentless in grado di bloccare tutte le minacce laterali, isolando gli endpoint con IP, inclusi i sistemi legacy e headless, in un "segmento di rete a elemento singolo". 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:

Segmentazione interna 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.

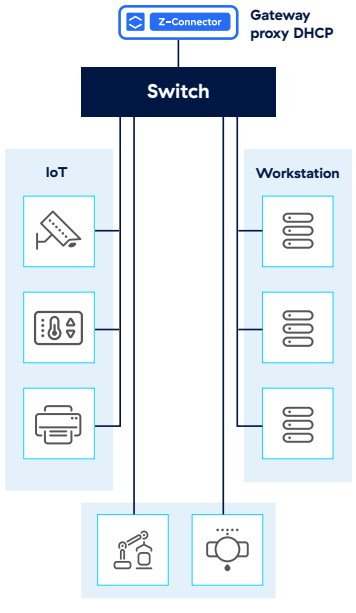
Per applicare la segmentazione zero trust alla rete è sufficiente:

- Assicurarsi che ogni singolo dispositivo sia associato a un segmento univoco (/32).
- Raggruppare in automatico dispositivi, utenti e app analizzandone i modelli di traffico e 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.



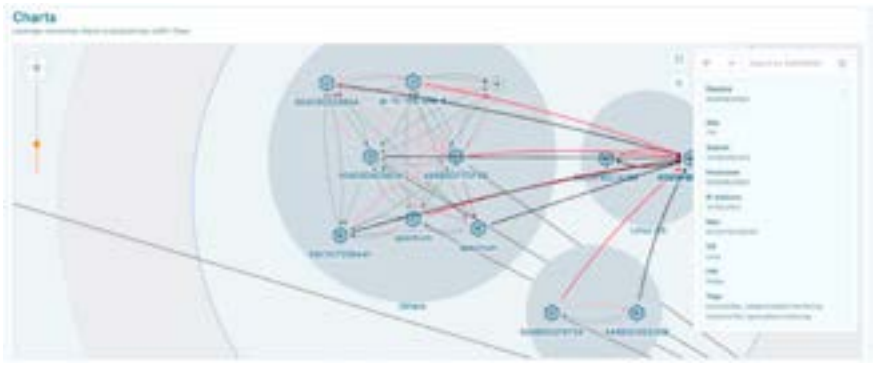
La segmentazione IoT/OT automatica prevede la creazione di un segmento "univoco" per ogni dispositivo

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

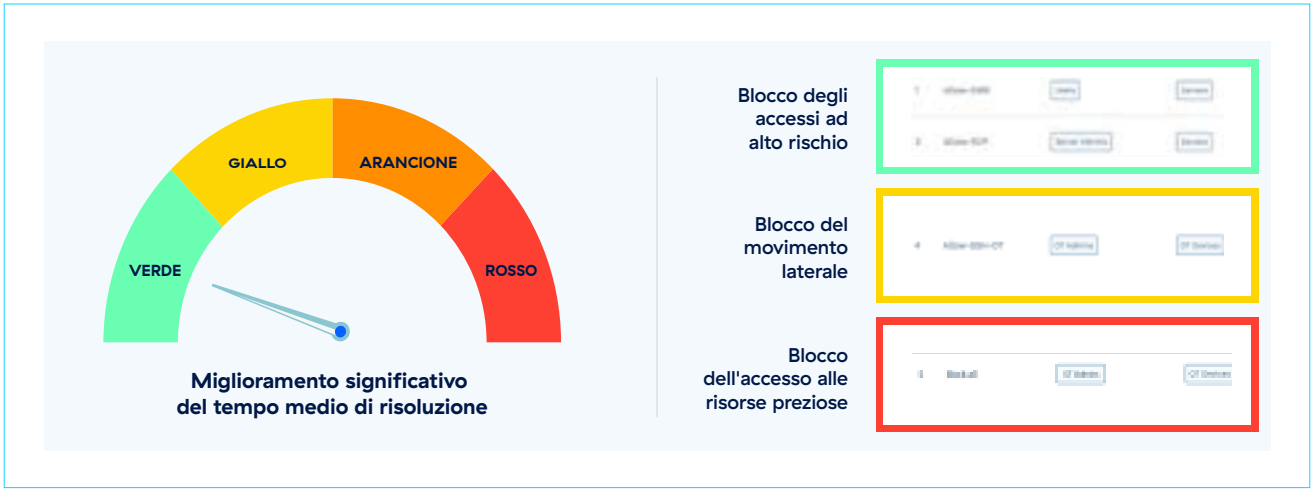


Dashboard di Device Discovery

Risposta automatica agli incidenti

Presentazione di Zscaler Ransomware Kill Switch. Funzionalità per la riduzione della superficie di attacco con un clic completamente integrata nella nostra soluzione Zero Trust Device Segmentation. Blocca i protocolli e le porte vulnerabili noti e disabilita istantaneamente l'accesso a reti critiche come interi ospedali o stabilimenti, il tutto con livelli di gravità preimpostati per ridurre al minimo i tempi di inattività aziendali.

Il Ransomware Kill Switch agisce come punto di applicazione delle policy su più livelli, consentendo risposte agli incidenti in base al livello in caso di una compromissione attiva e potenziando l'investimento negli strumenti di sicurezza esistenti. Ogni livello del Ransomware Kill Switch ha funzionalità simili a "fusibili virtuali" o livelli Defcon, con percorsi di escalation predefiniti che bloccano progressivamente tutte le comunicazioni di rete non necessarie da o verso qualsiasi endpoint, negando la propagazione laterale e riducendo drasticamente la superficie di attacco.



Questa soluzione disattiva istantaneamente le comunicazioni non essenziali tra i dispositivi, bloccando così il movimento laterale delle minacce senza interrompere le operazioni aziendali. Inoltre, neutralizza le minacce avanzate, come i ransomware, su dispositivi IoT, sistemi OT e dispositivi che non supportano l'uso degli agenti.

Zscaler offre il controllo completo del Ransomware Kill Switch tramite API. Utilizzando queste interfacce programmabili, le organizzazioni IT possono abilitare gli strumenti di organizzazione della sicurezza esistenti come il Security Information and Event Management (SIEM), il Security Orchestration and Response (SOAR) o le soluzioni EDR/XDR, in modo da automatizzare la risposta agli incidenti e mettere immediatamente in quarantena gli endpoint compromessi, contenendo il raggio di propagazione dell'infezione.

Tutto ciò garantisce alle organizzazioni la protezione degli investimenti per le loro infrastrutture di rete e di sicurezza e migliora immediatamente il profilo di sicurezza aziendale.

Vantaggi

Contenimento granulare per limitare la diffusione laterale

Risposta agli incidenti pianificata e automatizzata da applicare durante una violazione

Contenimento rigido nei livelli principali di confine, come tra l'IT aziendale e le reti core

Blocco graduale di porte e protocolli sospetti per massimizzare i tempi di attività aziendali

Elimina il movimento laterale delle minacce attraverso la LAN
Riduci la superficie di attacco isolando ogni elemento nella sua "rete di uno", eliminando la superficie di attacco e il rischio di propagazione delle minacce. Anche i dispositivi compromessi non possono più infettare i loro vicini.

Riduci la complessità operativa e i costi associati agli strumenti di segmentazione legacy
Segmenta ciascun endpoint IP senza ricorrere alle complesse e obsolete tecnologie di rete incentrate su IP, come NAC e firewall est–ovest, o a strutture complesse come ACL e segmentazione manuale delle VLAN.

Ottieni una visibilità migliore sul traffico est–ovest
Ottieni una visibilità laterale completa con il rilevamento e la classificazione automatica dei dispositivi; gli amministratori di rete possono gestire meglio le prestazioni, i tempi di attività e la sicurezza per qualsiasi dispositivo, anche quelli che non possono accettare agenti.

Distribuzione senza interruzione della rete
Ottieni una tecnologia agentless distribuibile rapidamente senza interrompere le modalità di gestione aziendale dei clienti e senza necessità di modificare l'architettura di rete o di ricorrere al reindirizzamento IP dei dispositivi.

Conformità più rapida
Gli standard federali di cybersecurity dei vari settori considerano la segmentazione un pilastro fondamentale del modello zero trust. L'approccio agentless di Zscaler è implementabile rapidamente e migliora immediatamente il livello di conformità.

Funzionalità

Isolamento airgap

- Isolamento del dispositivo agentless
- Quarantena del dispositivo con un clic
- Rilevamento delle violazioni dell'isolamento airgap
- Filtraggio basato sull'indirizzo MAC

Segmentazione zero trust

- Segmentazione basata sulla rete

Segmentazione basata sui dispositivi

- Raggruppamento autonomo e policy
- Controllo delle policy IntraVLAN e InterVLAN
- Policy dinamica basata su tag
- Policy basata sull'identità del dispositivo e dell'utente
- Policy basata sul tempo
- Policy basata su zone
- Framework della gerarchia delle policy

Rilevamento e profilazione delle risorse

- Rilevamento di endpoint e reti
- Creazione di impronte digitali
- Categorizzazione dei dispositivi basata sul profilo
- Decodifica dei protocolli ICS/medici

Alta disponibilità

- Cluster a due nodi con VRRP
- VRRP con sincronizzazione della sessione
- Sincronizzazione di configurazione e stato
- Aggregazione di link
- Monitoraggio della reattività dell'interfaccia
- Aggiornamenti software senza problemi
- Sostituzione hardware in-service

Servizi di routing e di rete

- Routing dinamico: BGP, OSPF
- Routine multicast: IGMP, PIM
- Server DHCP, Relay/Proxy
- Trunking VLAN
- Traduzione degli indirizzi di rete
- Routing basato su policy
- Percorso multiplo a costo uguale (ECMP)
- VPN da sito a sito

Risposta agli incidenti

- Ransomware Kill Switch

Visibilità e registrazione

- Mappa del traffico con correlazione delle policy
- Data lake flessibile integrato
- Registri di avvio sessione per tutte le comunicazioni tra segmenti e interne a essi
- Esportazione dei log verso SIEM/Raccoglitore di log

Modalità di distribuzione flessibili

- Provisioning del gateway airgap zero-touch
- Modelli e profili del sito
- Distribuzione autonoma, cluster ad alta disponibilità o multi-cluster
- Gateway airgap basati su macchine fisiche o virtuali

Monitoraggio e risoluzione dei problemi

- Console di debug remota
- CLI locale sui gateway Airgap
- Supporto SNMP

Gestione centralizzata basata sul cloud

- Single sign-on (SSO) e MFA
- Tracce di controllo per eventi di accesso e modifiche alla configurazione
- Controllo degli accessi basato sui ruoli
- Piattaforma cloud multi-tenant
- Accesso basato su API

Integrazioni con terze parti

- Active Directory di Microsoft
- Integrazione SIEM
- Fornitori EDR: Crowdstrike, SentinelOne
- Gestione delle risorse—Armis
- SSE—Zscaler ZIA

Dimensionamento dei dispositivi Zscaler Gateway

Di seguito sono riportate varie stime sulle dimensioni per dispositivi hardware o gateway Zscaler virtualizzati.

Specifiche hardware per distribuzioni di gateway fisici						
	XS	**S1**	**S2**	**M**	**L**	**XL**
Disponibilità	Giugno 2024	Giugno 2024	Ora	Ora	Ora	1QFY25
Modello hardware	ZT 400	ZT 600	Dell VEP4600	Dell VEP4600	Dell VEP4600	Da definire
CPU	4C Atom	8C Atom	4C Xeon	8C Xeon	16C Xeon	16C Xeon
Memoria	16 GB	16 GB	16 GB	32 GB	64 GB	64 GB
Archiviazione	64 GB	64 GB	128 GB	256 GB	960 GB	256 GB
Porte	4x 1GbE	4x 1GbE	6x 1GbE 2x 1GbE (SFP)	4x 1GbE 2x 10GbE	4x 1GbE 6x 10GbE	4x 25GbE
Caratteristiche	Desktop	Desktop	1U	1U	1U	1U
Altre caratteristiche	Senza ventola		RPS	RPS	RPS	RPS
Throughput (HTTP da 64 KB)	4 Gbps	8 Gbps	10 Gbps	20 Gbps	40 Gbps	80 Gbps
Sessioni	250.000	500 mila	500 mila	1M	2M	2M
# Endpoint	200	500	1000	2000	4000	Da definire

Guida al dimensionamento dei dispositivi virtuali				
	XS	**S1**	**S2**	**M**
Disponibilità	Ora	Ora	Ora	Ora
CPU	2 CPU virtuali	4 CPU virtuali	8 CPU virtuali	16 CPU virtuali
Memoria	8 GB	16 GB	32 GB	64 GB
Archiviazione	256 GB	256 GB	256 GB	256 GB
Porte	4x vNIC	4x vNIC	4x vNIC	4x vNIC
Throughput (HTTP da 64 KB)	5 Gbps	10 Gbps	20 Gbps	40 Gbps
Sessioni	250.000	500 mila	1M	2M
# Endpoint	200	500	2000	4000

Parla con un tecnico esperto

Vuoi saperne di più sul modo in cui 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 di 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 SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.com/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.com/it