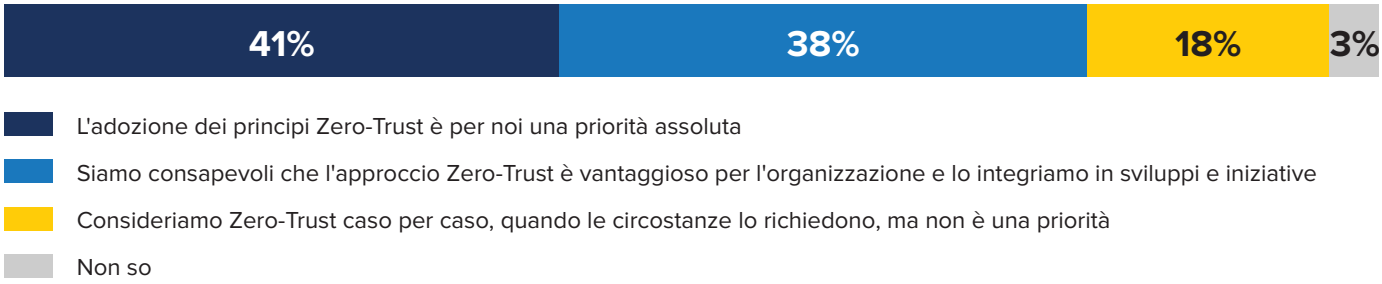
Come garantire la continuità delle operation estendendo i framework Zero-Trust agli ambienti OT

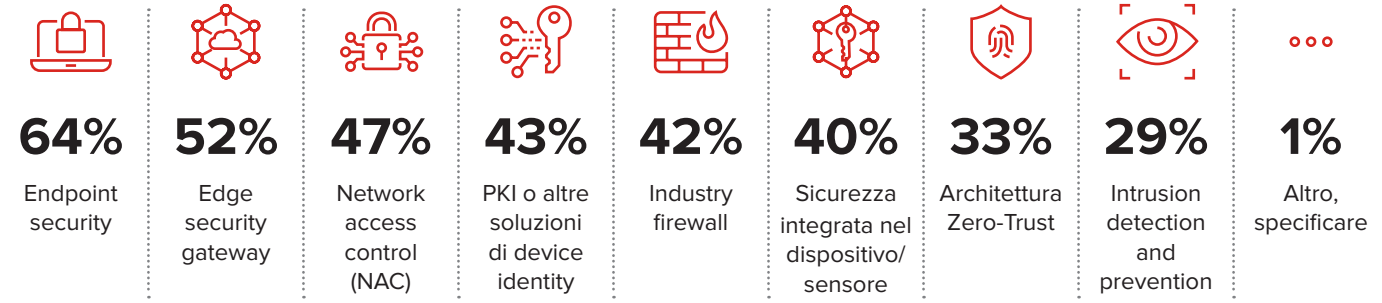
Gli asset OT connessi stanno aprendo le reti industriali a un vasto e avanzato, nonché redditizio, panorama di minacce informatiche che i cybercriminali possono sfruttare. L'estensione di framework Zero-Trust agli ambienti OT garantirà operation più sicure, resilienti e automatizzate.

Quale delle seguenti affermazioni relative all'approccio Zero-Trust è vera per la vostra organizzazione?



Fonte: IDC Security Survey 2022 (n = 700)

In che modo la vostra organizzazione protegge le implementazioni IIoT?



Fonte: IDC Security Survey 2022 (n = 233)

Zero-Trust è tra le priorità nell'agenda delle iniziative di sicurezza. Il 41% delle organizzazioni adotta principi Zero-Trust come una priorità assoluta, con strategia e obiettivi definiti e il supporto da parte del senior management per nuovi investimenti e iniziative. Ma Zero-Trust non è un prodotto, una soluzione o una rete specifica che può essere acquistata; si tratta di un approccio strategico alla sicurezza, che la rende un'architettura più difficile da implementare. Attualmente, solo un terzo delle organizzazioni sfrutta Zero-Trust per proteggere le proprie implementazioni IIoT.

Zero-Trust

L'architettura Zero-Trust si basa sul principio di negare l'accesso di default a qualsiasi richiesta di accesso alla rete. Ciò richiede il monitoraggio costante delle minacce per l'azienda, la manutenzione continua dell'ambiente e, poiché si tratta di un framework che va oltre la semplice soluzione tecnologica, richiede anche l'allineamento delle soluzioni ai requisiti di governance e conformità.

Zero-Trust è un'iniziativa di punta per la maggior parte delle organizzazioni, poiché i modelli di business cambiano e le aziende continuano ad andare avanti con le loro iniziative DX. Zero-Trust è una strategia a livello aziendale per ridurre il rischio complessivo per l'impresa. Con un numero crescente di applicazioni aziendali che passano al cloud e un numero maggiore di dispositivi che si connettono alla rete (risorse IoT e OT), il valore di una soluzione tradizionale di protezione dell'infrastruttura perimetrale diminuisce. Le organizzazioni trovano difficile far fronte a continue interruzioni e allo stesso tempo proteggere utenti, dispositivi, risorse e applicazioni. Ciò aumenta le inefficienze operative e il rischio di violazioni della sicurezza.

Estendete ora Zero-Trust all'OT: Consigli per iniziare

- Zero-Trust deve andare oltre le tradizionali definizioni di utenti e identità per includere tutti i dispositivi e le risorse.
- Assicurare una visibilità profonda sulla rete per identificare e monitorare ogni dispositivo (incluse le comunicazioni dei dati da/verso dove, da chi/cosa).
- Automatizzare l'applicazione delle policy, nonché il rilevamento e il blocco delle minacce.
- Segmentare la rete per applicare i principi Zero-Trust in tutti gli ambienti creando zone enterprise, IoT e OT, che potrebbero essere tenute separate.
- Contenere i dispositivi noti come vulnerabili, non sicuri o non brevettabili in zone più lontane per ridurre la superficie di attacco.

Che cosa significa per l'OT?

Nella sicurezza IT, la riservatezza è al primo posto della triade CIA (riservatezza, integrità, disponibilità). Negli ambienti OT, tuttavia, la disponibilità diventa l'aspetto più critico, il che richiede un cambiamento nelle strategie di gestione del rischio.

L'estensione di un framework Zero-Trust alle implementazioni OT può migliorare la sicurezza e ridurre i rischi, ma richiede una comprensione completa di tutte le risorse di rete, non solo dei tradizionali endpoint IT. Ciò consentirà alle organizzazioni di prendere decisioni di segmentazione per ridurre la superficie degli attacchi e i rischi complessivi senza influire sulla disponibilità.

Le risorse connesse possono diventare facilmente l'anello debole o il punto di ingresso in qualsiasi organizzazione. L'estensione di un framework Zero-Trust alle implementazioni OT può migliorare la sicurezza e ridurre i rischi, ma richiede una comprensione completa di tutte le risorse di rete, non solo dei tradizionali endpoint IT. Ciò consentirà alle organizzazioni di prendere decisioni di segmentazione per ridurre la superficie degli attacchi e i rischi complessivi senza influire sulla disponibilità.

Il punto di vista di IDC

La convergenza tra IT e OT è diventata una tendenza inarrestabile negli ultimi anni. Questa è un'opportunità per molte aziende per spostarsi verso attività decisionali e operation più resilienti per soddisfare i requisiti operativi futuri. Dall'essere due mondi diversi, IT e OT stanno comunicando e si stanno integrando sempre di più per migliorare le prestazioni operative delle organizzazioni e colmare il divario storico tra processi operativi e processi di business, aprendo però in questo modo l'OT a un vasto e avanzato panorama di minacce informatiche.

L'adozione di un approccio Zero-Trust, non solo per l'infrastruttura IT tradizionale, ma anche per gli ambienti OT con autorizzazioni di accesso granulari a livello di applicazione, aumenterà la sicurezza della connettività e l'interoperabilità tra IT e OT, riducendo al tempo stesso rischi e minacce per tutta l'area delle operation.

Messaggio dello sponsor:

L'approccio Zero-Trust OT di TXOne protegge le organizzazioni dagli attacchi informatici altamente efficaci che sono diventati una minaccia comune per il commercio. Applicazione semplificata di policy basate su Zero-Trust OT con **soluzioni ICS native**.