Zscaler Zero Trust Device Segmentation para OT/IoT

Detenga el movimiento lateral, reduzca la superficie de ataque y mejore la seguridad operativa

Resumen de la solución

El tema en cuestión

Recientemente, se ha producido un aumento de las alertas y advertencias sobre ciberataques de malintencionados patrocinados por Estados contra infraestructuras críticas estadounidenses. El 7 de febrero de 2024, la Oficina Federal de Investigación (FBI) y la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA), junto con la Agencia de Seguridad Nacional, emitieron un aviso de advertencia a las organizaciones gubernamentales en relación con ciberatacantes preparados para desestabilizar las infraestructuras críticas, como los sistemas de transporte, los oleoductos y gasoductos de gas natural, las plantas de tratamiento de agua y las redes eléctricas. Esto complementa acciones similares emprendidas por la TSA para la seguridad de aeropuertos, operadores aéreos y ferroviarios, la reciente línea de base de ciberseguridad del DOE y la actualización casi definitiva del NERC al CIP-015-1.

Las tecnologías de OT/IoT se diseñaron para ofrecer, en primer lugar, velocidad y eficacia en las transacciones, con la seguridad como objetivo secundario. Lamentablemente, OT/IoT es ahora un objetivo favorito de los ciberdelincuentes, con un aumento interanual del 400 % en los ataques, según el estudio de Zscaler ThreatLabz. El ransomware es la estrategia de ataque más popular, y el 61 % de todas las violaciones tuvieron como objetivo organizaciones conectadas a OT.

¿Qué puede hacer?

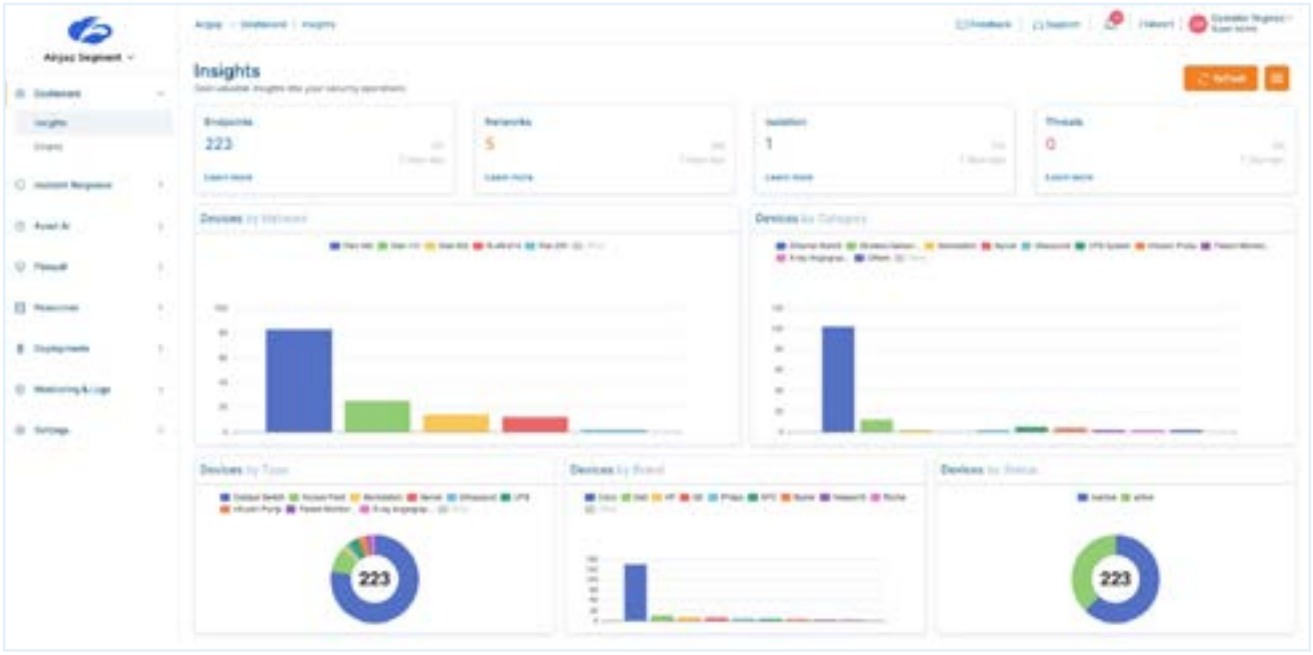
La EPA, la CISA y el FBI recomiendan encarecidamente a los operadores de sistemas que trabajen para cumplir la orden ejecutiva de la Oficina del Presidente de utilizar Zero Trust como directriz hacia una mejor ciberseguridad.

Los puntos resaltados son áreas clave en estas recomendaciones donde Zscaler puede ayudar inmediatamente con nuestra solución de Segmentación de Dispositivos de Zero Trust.

- Reduzca la exposición a Internet de cara al público
- Reduzca la exposición a vulnerabilidades
- Segmentación de la red
- Recopilación de registros
- Prohíba la conexión de usuarios no autorizados
- No permita servicios explotables en Internet
- Limite las conexiones OT/IoT a Internet
- Detección de amenazas relevantes
- Realice un inventario de los activos OT/IT

¿Cómo hacerlo?

La segmentación ha sido durante mucho tiempo un elemento básico en las redes, con herramientas como las listas de control de acceso (ACL) y los firewalls que gestionan el tráfico norte-sur (de cliente a servidor). Sin embargo, la microsegmentación OT desplaza la atención hacia el tráfico este-oeste, más vulnerable, que fluye lateralmente entre los dispositivos y las cargas de trabajo. En las VLAN compartidas, debido a la arquitectura de conmutación heredada, los dispositivos pueden ver y comunicarse con todos los demás, lo que crea un entorno propicio para la propagación del malware. Lamentablemente, las soluciones basadas en agentes, pioneras para las cargas de trabajo en la nube, no pueden segmentar las máquinas heredadas y sin supervisor que son tan comunes en OT, y los enfoques tradicionales basados en ACL siguen siendo excesivamente complicados.



Panel de segmentación de dispositivos Zero Trust

Zscaler elimina la fricción de la segmentación intra-VLAN con una solución sin agente que frena todas las amenazas laterales aislando cada punto final IP, incluidos los sistemas heredados y sin supervisores, en un "segmento de red único". Esto elimina la necesidad de ACL complejas y no requiere cambios en la infraestructura existente, al tiempo que proporciona la segmentación más granular y efectiva disponible.

Casos de uso

Algunos de los casos de uso más comunes para la segmentación de dispositivos sin agente incluyen:

Microsegmentación LAN

Extienda Zero Trust a la LAN imponiendo la segmentación en el tráfico este-oeste. Esto reduce su superficie de ataque interna y elimina la amenaza del movimiento lateral en redes OT/IoT críticas, sin necesidad de NAC ni de segmentación basada en firewalls.

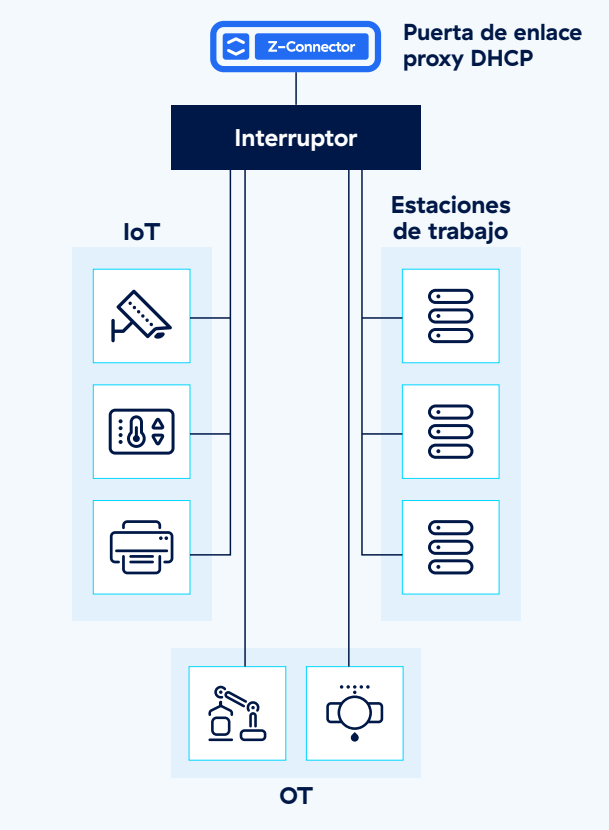
Para aplicar la segmentación Zero Trust en su red:

- Aprovisione automáticamente cada dispositivo en un segmento único (/32)
- Agrupe automáticamente dispositivos, usuarios y aplicaciones mediante el análisis de sus patrones de tráfico, evitando que dispositivos no autorizados utilicen la suplantación de MAC para entrar en la red.
- Aplique dinámicamente políticas para el tráfico este-oeste en función de la identidad y el contexto de los usuarios y dispositivos

Segmentación IT/OT

La tecnología Zscaler Zero Trust Device Segmentation actúa como un interruptor de desactivación de ransomware, inhabilitando la comunicación de dispositivos no esenciales para detener el movimiento lateral de las amenazas sin interrumpir las operaciones empresariales. Esta solución neutraliza amenazas avanzadas como ransomware en dispositivos IoT, sistemas OT y dispositivos sin capacidad de agente.

- Agrupe y aplique de manera autónoma la política para direcciones MAC conocidas en cualquier dispositivo (por ejemplo, denegación de acceso RDP a cámaras excepto para administradores)
- Aísle automáticamente las direcciones MAC desconocidas para limitar el radio de alcance en caso de que un dispositivo se vea comprometido
- Integración con sistemas de gestión de activos para políticas de control de acceso seguro



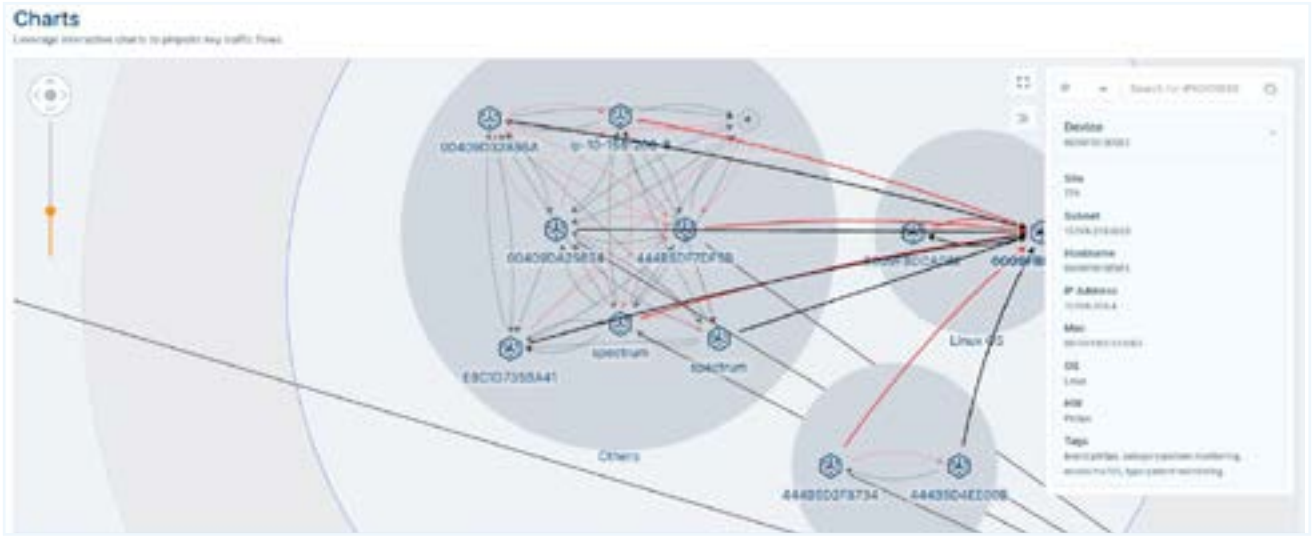
Segmentación automatizada de IoT / OT Segmento “único" para cada dispositivo

Descubrimiento y clasificación automática de dispositivos

Dado que una parte significativa del tráfico OT/IoT permanece dentro de la red local, es importante disponer de una visibilidad continua del tráfico este–oeste. Con la detección y clasificación automática de dispositivos, los administradores de red pueden gestionar mejor el rendimiento, el tiempo de actividad y la seguridad de los sistemas IoT/OT sin necesidad de una compleja gestión de inventario.

Para visibilidad de red y dispositivos:

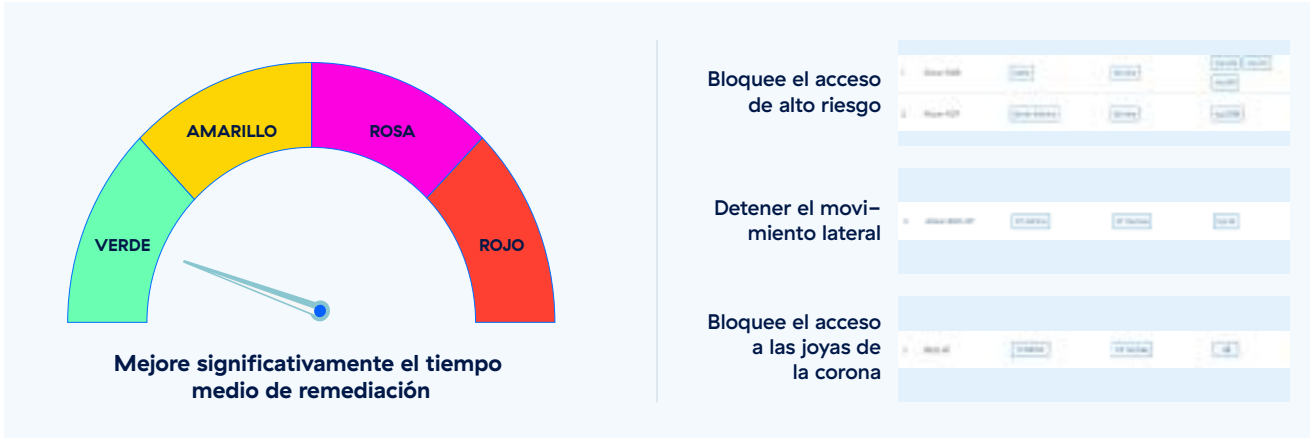
- Descubra, clasifique y realice inventarios de los dispositivos OT/IoT sin necesidad de agentes de punto final
- Obtenga una referencia de los patrones de tráfico y los comportamientos de los dispositivos para determinar los accesos autorizados y no autorizados
- Obtenga información precisa sobre la red para la gestión del rendimiento y el mapeo de amenazas



Panel de detección de dispositivos

Respuesta automatizada a incidentes

Zscaler Ransomware Kill Switch ofrece una reducción de la superficie de ataque seleccionable por el usuario. Solo tiene que elegir un nivel de gravedad preestablecido para bloquear progresivamente los protocolos y puertos vulnerables conocidos, e incluso inhabilitar al instante el acceso a redes enteras como líneas de fabricación y plantas de hospitales. Adiós a las suposiciones en medio del caos de una violación: solo tiene que girar el dial para adaptarlo a la amenaza y mantener al mismo tiempo la actividad empresarial.



Hable con un experto técnico

¿Quiere obtener más información sobre cómo Zscaler puede ayudar a proteger su organización de infraestructura crítica? Programe una cita para hablar con uno de nuestros expertos técnicos.

zscaler™ | Experience your world, secured.™

Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, fuertes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de ciberataques y pérdida de datos al conectar de manera segura usuarios, dispositivos y aplicaciones en cualquier ubicación. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basado en SSE es la plataforma de seguridad en la nube en línea más grande del mundo. Obtenga más información en **zscaler.com.mx** o síganos en Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (Oficinas centrales) • 120 Holger Way • San José, CA 95134