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 problema en cuestión

Recientemente, ha habido un aumento de alertas y advertencias sobre ciberataques de autores de amenazas patrocinados por estados a infraestructura crítica de Estados Unidos. El 7 de febrero de 2024, la Oficina Federal de Investigaciones (FBI) y la Agencia de Seguridad Cibernética y de Infraestructura (CISA), junto con la Agencia de Seguridad Nacional, emitieron una advertencia a las organizaciones gubernamentales sobre ciberdelincuentes preparados para interrumpir infraestructura crítica, como sistemas de transporte, oleoductos y gasoductos, plantas de tratamiento de agua y redes eléctricas. Esto complementa acciones similares adoptadas por la TSA para proteger aeropuertos, operadores de aeronaves y ferrocarriles, la reciente línea base de ciberseguridad del DOE y la actualización casi final del NERC a CIP-015-1.

Las tecnologías OT/IoT fueron diseñadas para brindar velocidad y eficiencia en las transacciones primero, con la seguridad como objetivo secundario. Desafortunadamente, OT/IoT es ahora un objetivo favorito de los ciberdelincuentes, con un aumento interanual del 400 % en los ataques, según la investigación de Zscaler ThreatLabz. El ransomware es la estrategia de ataque más popular y el 61 % de todas las infracciones tuvieron como objetivo organizaciones conectadas a OT.

¿Qué puede hacer?

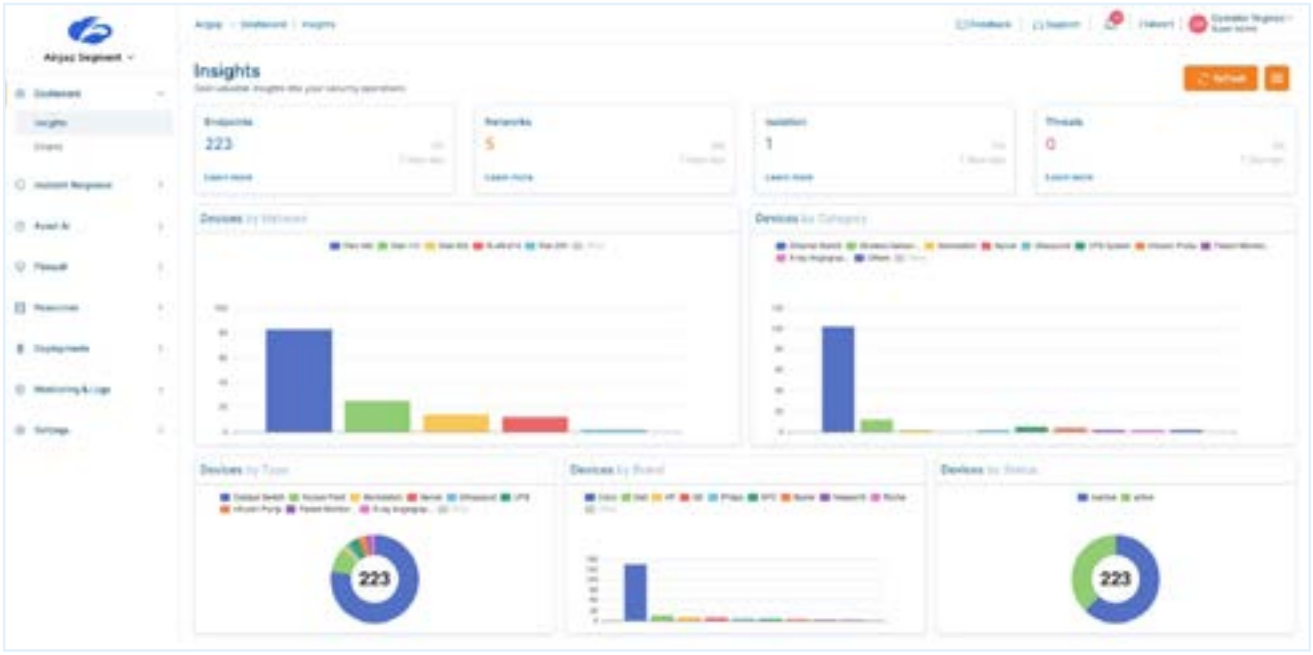
La EPA, la CISA y el FBI recomiendan encarecidamente que los operadores de sistemas trabajen según la orden ejecutiva de la Oficina del Presidente para utilizar zero trust como guía hacia una mejor ciberseguridad.

Los elementos destacados son áreas clave en estas recomendaciones en las que Zscaler puede ayudar de inmediato con nuestra solución de segmentación de dispositivos Zero Trust.

- Reducir la exposición a Internet de cara al público
- Reducir la exposición a vulnerabilidades
- Segmentación de la red
- Recopilación de registros
- Prohibir la conexión de usuarios no autorizados
- No hay servicios explotables en Internet
- Límitar conexiones OT/IoT a internet
- Detección de amenazas relevantes
- Realizar un inventario de activos OT/IT

¿Cómo puede hacerlo?

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



Panel de segmentación de dispositivos Zero Trust

Zscaler elimina la fricción de segmentación intra-VLAN con una solución sin agente que detiene todas las amenazas laterales al aislar cada terminal de IP, incluidos los sistemas heredados y sin dirección, en un "segmento de red de uno". 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 de LAN

Amplíe zero trust a la LAN imponiendo la segmentación en el tráfico este-oeste. Esto reduce su superficie de ataque interna y elimina la amenaza de movimiento lateral en redes OT/IoT críticas, sin necesidad de NAC o segmentación basada en cortafuegos.

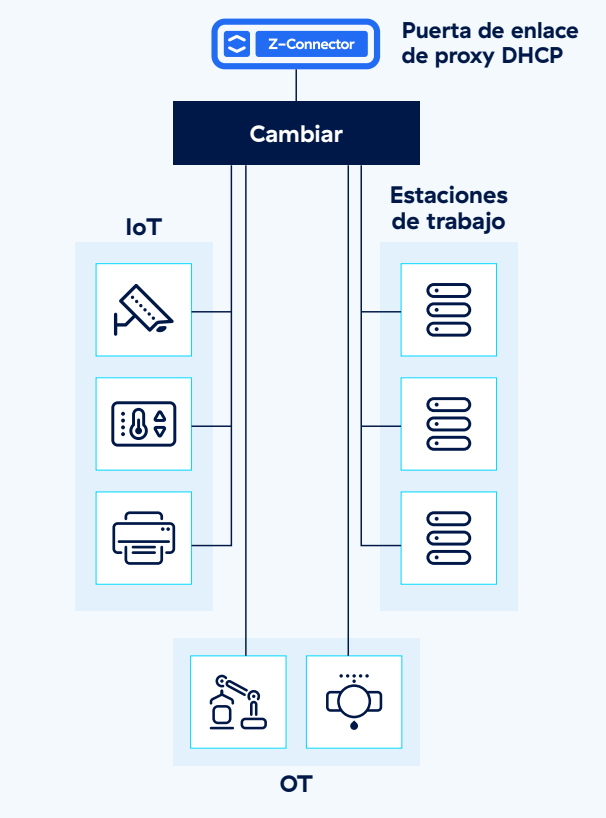
Para aplicar la segmentación zero trust en su red:

- Aprovisione automáticamente cada dispositivo en un segmento de uno (/32)
- Agrupe automáticamente dispositivos, usuarios y aplicaciones analizando sus patrones de tráfico, lo que evita que dispositivos no autorizados utilicen la suplantación de MAC para acceder a 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 de Zscaler Zero Trust Device Segmentation actúa como un interruptor de seguridad contra ransomware, desactivando la comunicación no esencial del dispositivo para detener el movimiento lateral de amenazas sin interrumpir las operaciones comerciales. Esta solución neutraliza amenazas avanzadas como ransomware en dispositivos IoT, sistemas OT y dispositivos sin capacidad de agente.

- Agrupe y aplique políticas de forma autónoma para direcciones MAC conocidas en cualquier dispositivo (por ejemplo, acceso RDP a cámaras denegado excepto para administradores)
- Aísle automáticamente direcciones MAC desconocidas para limitar el radio de explosión en caso de que un dispositivo esté comprometido
- Integración con sistemas de gestión de activos para políticas de control de acceso seguro



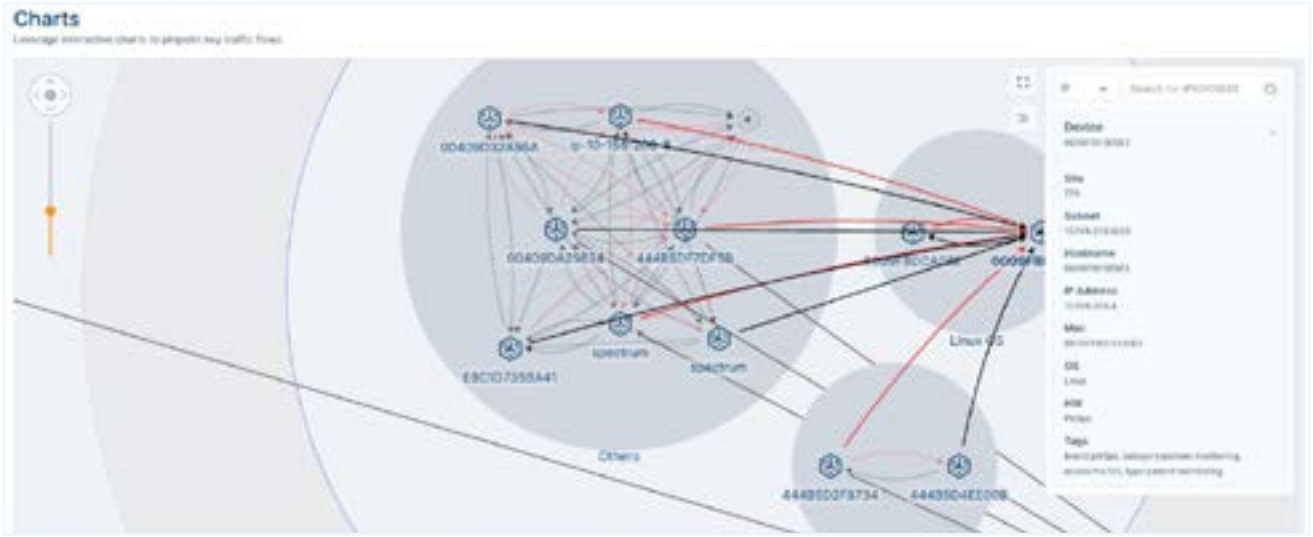
IoT automatizado / Segmentación OT Segmento de 'uno' para cada dispositivo

Descubrimiento y clasificación automática de dispositivos

Porque una parte importante del tráfico OT/IoT permanece dentro de la red local, por lo que es importante tener una visibilidad continua del tráfico de este a oeste. Con el descubrimiento y la clasificación automáticos de dispositivos, los administradores de red pueden gestionar mejor el rendimiento, el tiempo de actividad y la seguridad de los sistemas IoT/OT sin gestión compleja de inventarios.

Para visibilidad de red y dispositivo:

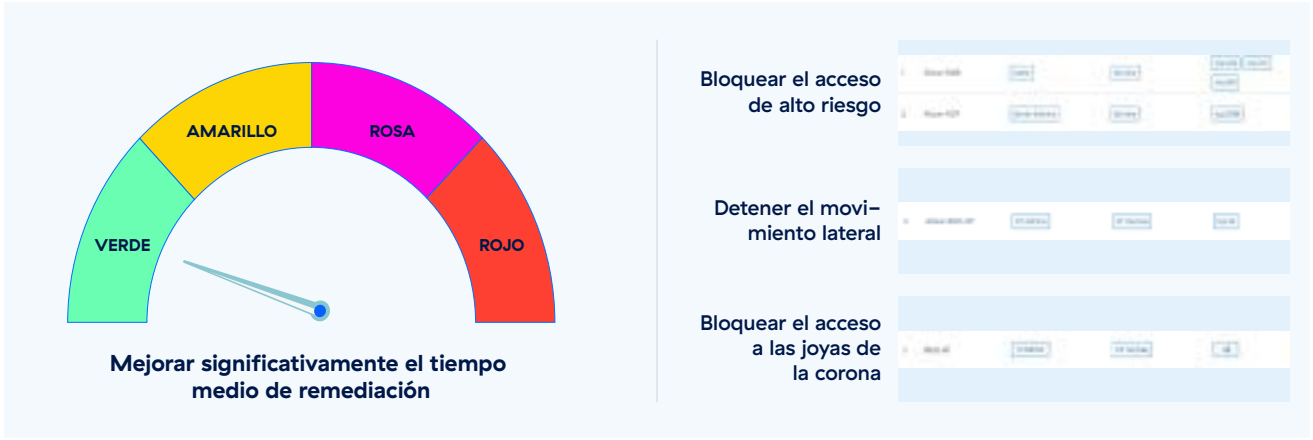
- Descubra, clasifique y haga un inventario de dispositivos OT/IoT sin necesidad de agentes de punto final
- Obtenga una línea base de los patrones de tráfico y los comportamientos de los dispositivos para determinar el acceso autorizado y no autorizado
- Obtenga información precisa sobre la red para la gestión del rendimiento y la asignación de amenazas



Panel de detección de dispositivos

Respuesta automatizada a incidentes

Zscaler Ransomware Kill Switch proporciona una reducción de la superficie de ataque seleccionable por el usuario. Sólo tiene que elegir un nivel de gravedad preestablecido para bloquear progresivamente protocolos y puertos vulnerables conocidos, e incluso deshabilitar instantáneamente el acceso a redes enteras, como líneas de fabricación y pisos de hospitales. No es necesario hacer conjeturas en el caos de una infracción: simplemente gire el dial para que coincida con la amenaza y, al mismo tiempo, mantenga el tiempo de actividad de la empresa.



Hable con un experto técnico

¿Quiere obtener más información sobre cómo Zscaler puede ayudar a proteger la infraestructura crítica de su organización? 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, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuido en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SSE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.es** o síganos en Twitter **@zscaler**.

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