

Seguridad de zero trust para infraestructuras críticas

Respuesta a las vulnerabilidades de ciberseguridad en los sistemas de agua potable y de distribución eléctrica

© 2024 Zscaler, Inc. Todos los derechos reservados.

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 una advertencia a las organizaciones gubernamentales en relación con los ciberactores que podrían perturbar las infraestructuras críticas, como las plantas de tratamiento de agua, las redes eléctricas, los oleoductos y gasoductos y los sistemas de transporte.

Las tecnologías de OT/IoT se diseñaron para ofrecer, en primer lugar, velocidad y eficacia en las transacciones, con la seguridad como objetivo secundario. Desafortunadamente, OT/IoT es ahora el objetivo favorito de los ciberdelincuentes con un aumento del 400 % año tras año según la investigación 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 la tecnología operativa (OT). A través de extensas auditorías de la EPA, han encontrado que más del 70 % de los sistemas inspeccionados desde septiembre de 2023 están en violación de los requisitos básicos SDWA 1433 incluyendo la falta de secciones específicas de la RRA y ERP.

¿Qué puede hacer?

La EPA, la CISA y el FBI recomiendan encarecidamente a los operadores de sistemas que tomen las medidas descritas en “Acciones principales” para asegurar los sistemas de agua. Además, el DOE ha publicado la base de referencia sobre ciberseguridad y el NERC casi ha finalizado la actualización del CIP-015-1. Ambas directrices sugieren trabajar en pro de la orden ejecutiva de la oficina del Presidente para emplear la zero trust como directriz hacia una mejor ciberseguridad.

Los elementos resaltados son áreas clave donde Zscaler puede ayudarle rápidamente con nuestra solución Zero Trust Device Segmentation.

- Reduzca la exposición a Internet de cara al público
- Desarrolle y ponga en práctica planes de respuesta y recuperación ante incidentes de ciberseguridad
- Reduzca la exposición a vulnerabilidades
- Copia de seguridad de los sistemas OT/TI
- Imparta formación sobre ciberseguridad
- 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 evaluaciones periódicas de ciberseguridad
- Cambie las contraseñas predeterminadas inmediatamente
- Realice un inventario de los activos OT/TI

¿Cómo hacerlo?

Con Zscaler, ampliamos aún más Zero Trust Segmentation para ofrecer visibilidad y segmentación para el tráfico este-oeste en redes LAN, incluidos los entornos OT críticos. Esto se puede lograr de varias maneras:

Reemplazo de cortafuegos este-oeste

Extienda Zero Trust a la LAN imponiendo la segmentación en el tráfico este-oeste. Esto reduce las superficies de ataque internas y elimina la amenaza del movimiento lateral en las redes OT/IoT de los servicios públicos. No es necesaria ninguna segmentación basada en NAC o cortafuegos.

©2024 Zscaler, Inc. Todos los derechos reservados.

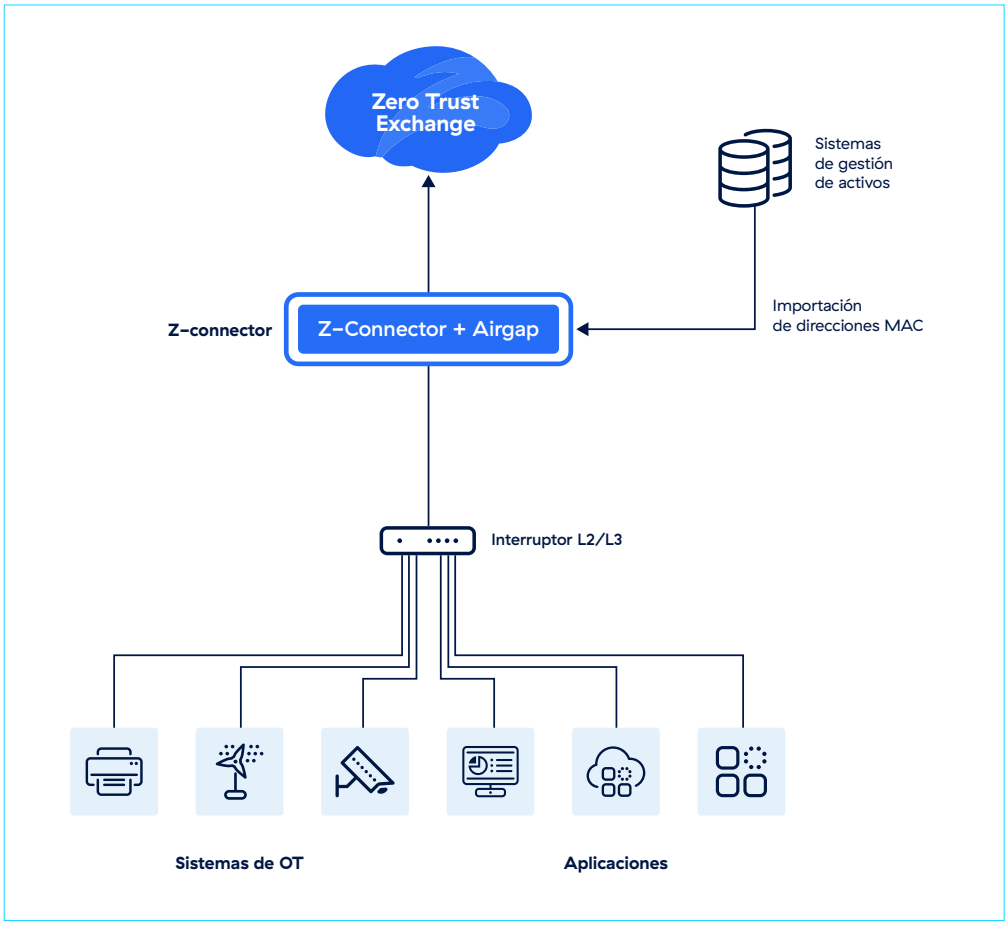
Para aplicar la segmentación Zero Trust en su red:

- Aprovisione automáticamente cada dispositivo en un segmento único (/32)
- Agrupación automsática de dispositivos, usuarios y aplicaciones mediante el análisis de los patrones de tráfico, lo que evita que los dispositivos fraudulentos utilicen la suplantación de MAC para entrar en la red.
- Aplique dinámicamente políticas de tráfico este-oeste basadas en la identidad y el contexto de usuarios y dispositivos

Segmentación IT/OT

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

- Agrupe y aplique de forma autónoma políticas para direcciones MAC conocidas en cualquier dispositivo; ej. Acceso RDP a las cámaras denegado excepto para los administradores
- Aísle automáticamente las direcciones MAC desconocidas para limitar el radio de alcance en caso de que un dispositivo se vea comprometido
- Integre con sistemas de gestión de activos para políticas de control de acceso seguro



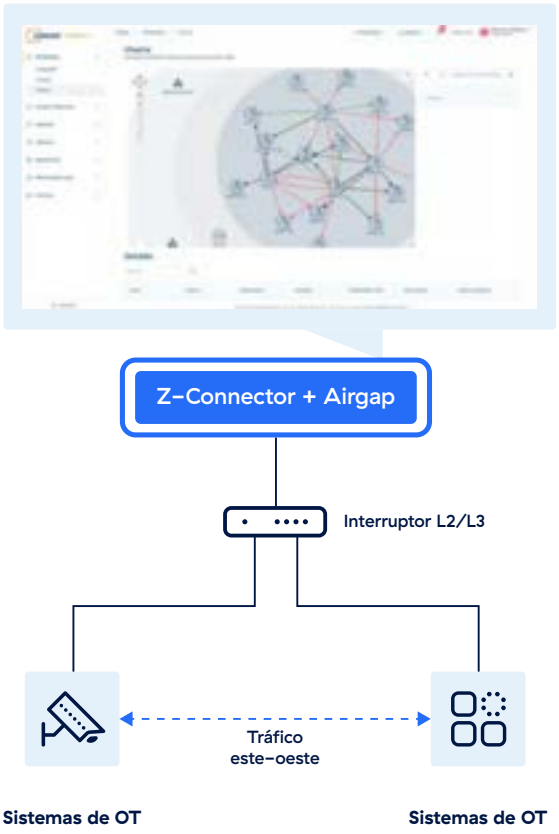
©2024 Zscaler, Inc. Todos los derechos reservados.

Detección y clasificación automática de dispositivos

Una parte significativa del tráfico IT/OT permanece dentro de la empresa de suministro de agua o electricidad, por lo que es importante tener 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 gestión de inventario compleja.

Para visibilidad de red y dispositivos:

- Descubra, clasifique e inventarié dispositivos IoT/OT sin necesidad de agentes de punto final
- Obtenga una línea de base de los patrones de tráfico y los comportamientos de los dispositivos para determinar los accesos autorizados y no autorizados
- Obtenga información sobre la red basada en IA para la gestión del rendimiento y el mapeo de amenazas



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, resilientes 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**.

© 2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ y otras marcas registradas listadas en **zscaler.com/mx/legal/trademarks** son (i) marcas comerciales o marcas de servicio registradas o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y otros países. Cualquier otra marca comercial pertenece a sus respectivos propietarios.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San José, CA 95134 zscaler.com/mx