Zscaler Zero Trust Segmentación de dispositivos para la Industria 4.0



©2025 Zscaler, Inc. Todos los derechos reservados.

DOCUMENTO TÉCNICO

En la era de la Industria 4.0, donde la fabricación inteligente y los sistemas industriales interconectados se están convirtiendo en la norma, la arquitectura de zero trust ha surgido como un marco de seguridad fundamental. Los enfoques de seguridad tradicionales basados en el perímetro ya no son suficientes para prTOeger el complejo ecosistema de dispositivos de tecnología operativa (TO) y sistemas de control industrial. El principio fundamental de Zero Trust, “nunca confíes, siempre verifica”, elimina la confianza implícita en la red y proporciona acceso seguro y autenticado a sistemas críticos. Este enfoque es particularmente importante en entornos industriales donde una brecha de seguridad podría provocar importantes tiempos de inactividad empresarial, pérdida de reputación y repercusiones regulatorias.

Ciberseguridad para la fabricación

Las redes de fabricación modernas han evolucionado hasta convertirse en ecosistemas complejos donde los sistemas de tecnología operativa (TO) y de tecnología de la información (TI) están profundamente interrelacionados. Esta convergencia permite capacidades avanzadas como el mantenimiento predictivo, la integración de la cadena de suministro y la gestión remTOa de operaciones. Sin embargo, esta interconectividad también genera nuevos desafíos de seguridad, ya que las redes TO tradicionalmente aisladas quedan expuestas a amenazas relacionadas con las TI. Las organizacones se centran en dos grandes áreas.

- **Acceso seguro a activos de tecnología operativa (TO):** los entornos de fabricación requieren un control estricto sobre quién puede acceder a los activos de tecnología operativa, como PLC, HMI y sistemas de control industrial. El acceso remoto privilegiado de Zscaler permite un acceso rápido, directo y seguro a los activos de TO en ubicaciones de campo, en la planta de producción o en cualquier lugar, sin necesidad de VPN ni agentes. Más información sobre el acceso remoto privilegiado de Zscaler – https://www.zscaler.com/es/resources/data-sheets/privileged-remote-access-for-ot-and-iiot.pdf

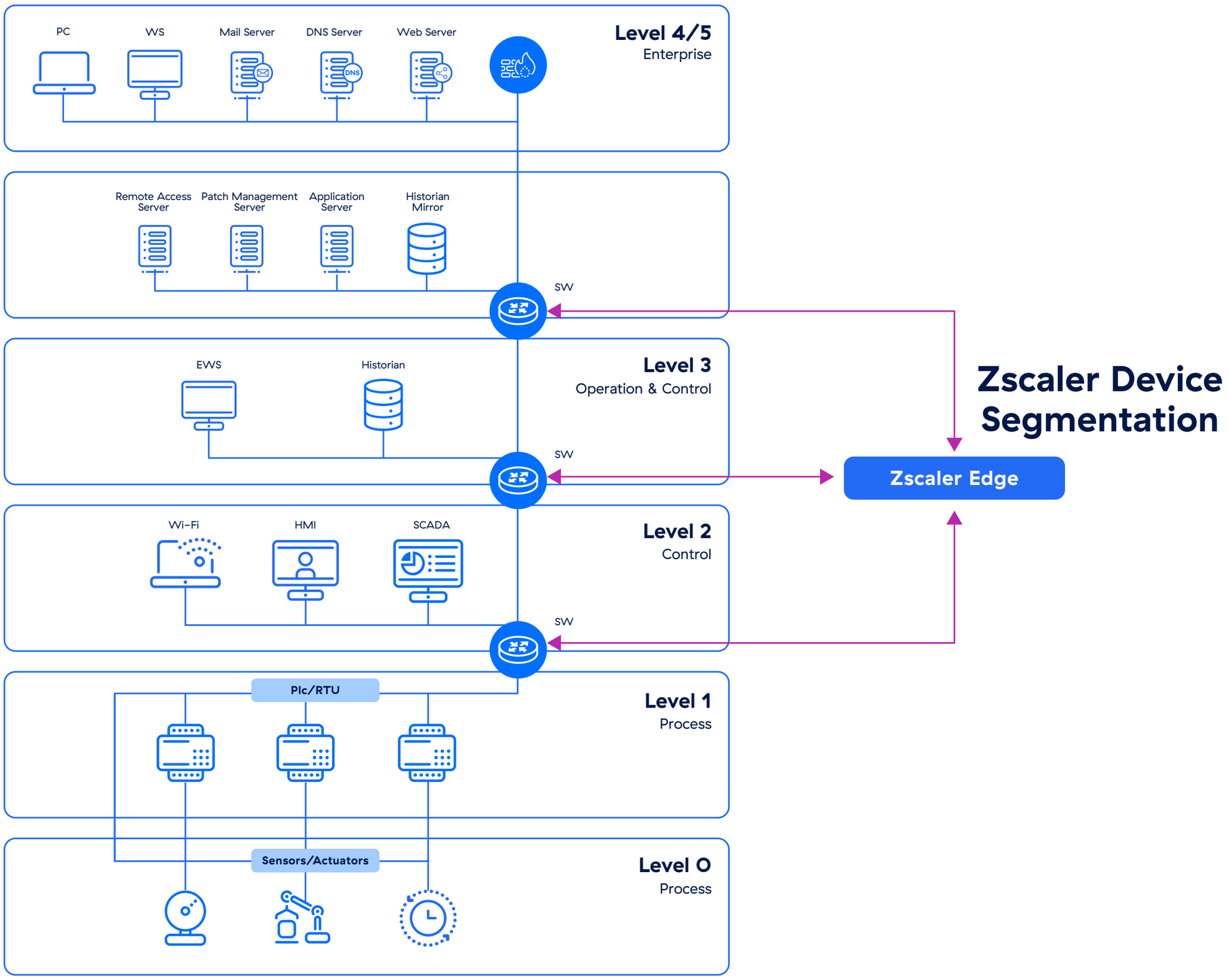
- **Segmentación:** Una preocupación crítica para la seguridad en entornos de fabricación es la posibilidad de que las amenazas se desplacen lateralmente a través de la red. Esto es particularmente peligroso en entornos industriales donde los sistemas heredados, que a menudo carecen de características de seguridad modernas, están interconectados con equipos modernos. La implementación de los principios Zero Trust a través de la microsegmentación ayuda a contener las amenazas al aplicar un estricto control de acceso a la red basado en políticas, lo que limita de manera efectiva la capacidad de un atacante de moverse lateralmente incluso si infringe las defensas iniciales.

En conjunto, el acceso privado de zero trust y la segmentación trabajan en tándem para establecer un marco de seguridad sólido para los activos de tecnología operativa (TO) en las redes de fabricación. Esta estrategia integral de seguridad garantiza que las operaciones de fabricación permanezcan prTOegidas tanto frente a amenazas externas como a vulnerabilidades internas, manteniendo al mismo tiempo la flexibilidad necesaria para un funcionamiento eficiente.

©2025 Zscaler, Inc. Todos los derechos reservados.

Segmentación en la fabricación

En las redes típicas de fabricación o control industrial hay diversos tipos de dispositivos conectados a la red. Según el modelo de Purdue, estos dispositivos se pueden clasificar en distintos niveles.



Nivel Purdue	Dispositivos	Descripción	Riesgo
Level 3	Historian, servidores de salto, servidores de parches	Ejecuta sistemas operativos conocidos, por ejemplo Windows. A pesar de contar con opciones de EDR, aún existen riesgos de seguridad de amenazas laterales	Medio a alto
Nivel dos	HMI, SCADA	Ejecutan sistema operativo integrado (p. ej. Windows CE, Windows XP). Debido a su naturaleza heredada, estos sistemas presentan graves vulnerabilidades y riesgos de seguridad significativos.	Alto
Nivel uno	PLC, RTU	Dispositivos sin pantalla de gama baja que requieren herramientas especiales para programar y modificar ajustes	De bajo a medio
Nivel O	Sensores, actuadores	Principalmente sistemas no basados en IP que realizan funciones muy específicas	Bajo

©2025 Zscaler, Inc. Todos los derechos reservados.

Estos diversos tipos de dispositivos TO establecen patrones de comunicación y dependencias complejas entre sí para lograr procesos de fabricación fluidos, mantener la continuidad operativa y garantizar una producción fiable en toda la planta de producción. La segmentación de dispositivos de zero trust de Zscaler (Zscaler ZTDS) proporciona medidas de seguridad integrales para prTOeger las operaciones de fabricación; a tal fin implementa controles de acceso robustos y establece límites de comunicación claros entre diferentes tipos de dispositivos industriales. Esta estrategia de segmentación avanzada ayuda a mantener la integridad y la fiabilidad de los procesos de fabricación, a la vez que prTOege frente a posibles amenazas a la seguridad e intentos de acceso no autorizados.

Caso de uso 1

Comunicaciones por Internet

En los entornos de fabricación modernos, los sistemas TO requieren cada vez más conectividad a Internet para diversas necesidades operativas, incluidas las actualizaciones de software, el soporte de los proveedores y el análisis basado en la nube. Sin embargo, esta exposición a Internet amplía significativamente la superficie de ataque de las redes industriales. Los sistemas TO, que antes estaban aislados, se vuelven vulnerables a ciberamenazas comunes como malware, ransomware y amenazas persistentes avanzadas (APT). Los riesgos son particularmente graves porque muchos dispositivos TO se diseñaron sin funciones de seguridad integradas y a menudo ejecutan sistemas operativos heredados que no se pueden actualizar ni parchear fácilmente.

Zscaler ZIA protege todas las comunicaciones por Internet y las conexiones salientes de los activos TO se enrutan a través de este servicio.

VALOR CLAVE ZSCALER ZIA

- **Protección avanzada frente a amenazas:** ZIA proporciona seguridad integral contra malware, ransomware y amenazas de día cero mediante la inspección multicapa de todo el tráfico de Internet procedente de los activos TO
- **Filtrado de salida:** aplica controles de acceso estrictos al limitar las comunicaciones de los dispositivos TO únicamente a destinos autorizados y bloquear sitios web y contenido potencialmente maliciosos
- **Inteligencia de amenazas en tiempo real:** aprovecha la inteligencia global en la nube para identificar y bloquear las amenazas emergentes antes de que puedan afectar a los activos de tecnología operativa (TO)

©2025 Zscaler, Inc. Todos los derechos reservados.

Caso de uso 2

Comunicaciones entre TO y TI

Las comunicaciones entre sistemas TO y TI en entornos de fabricación representan una intersección crítica donde los sistemas TO deben interactuar con la infraestructura TI. Esta integración permite funciones esenciales como el análisis de datos, la monitorización remota y la planificación de recursos empresariales. Sin embargo, estas comunicaciones también crean importantes vulnerabilidades de seguridad. Las redes de TI, que normalmente están conectadas a Internet y se actualizan con regularidad, deben interactuar con sistemas de TO que a menudo ejecutan software y protocolos heredados que no se diseñaron teniendo en cuenta la seguridad moderna.

Esta disparidad en las capacidades de seguridad genera posibles puntos de entrada para ciberataques.

VALOR CLAVE DE SEGMENTACIÓN DE DISPOSITIVOS ZSCALER:

- Tradicionalmente, las redes de TI y TO se construían por separado, con espacios físicos de aire entre ellas. Sin embargo, con la modernización, estos límites se están difuminando. La segmentación de dispositivos de Zscaler ayuda a mantener la separación entre las redes de TI y TO sin comprometer la productividad y el valor que la modernización aporta a las redes industriales.

- A pesar de tener VLAN separadas, los sistemas de TI y TO a menudo terminan compartiendo la misma red debido a errores de configuración o cambios rápidos en el negocio. La tecnología patentada Zscaler ZTDS identifica todos los sistemas de TI y TO en la red compartida (por ejemplo, las VLAN) y las separa lógicamente sin necesidad de reconfiguración de VLAN, cambios de IP o rediseño de la red.

- Para proteger los equipos heredados y evitar el acceso no autorizado a las redes TO, Zscaler ZTDS ayuda a eliminar la confianza implícita y restringe el acceso a la red desde un sistema específico como JumpHosts, Zscaler ZPA y Zscaler PRA.

- Un sistema de gestión en la nube centralizado y altamente escalable, con un sólido control de acceso basado en roles y capacidades multiinquilino simplifica las operaciones de red de TI y TO, manteniendo las funciones y los controles administrativos separados.

©2025 Zscaler, Inc. Todos los derechos reservados.

Caso de uso 3

Comunicaciones a nivel operativo

En el nivel 3, las comunicaciones a nivel operativo abarcan las interacciones entre varios sistemas de ejecución de fabricación (MES), sistemas de registro de datos históricos y otras aplicaciones de gestión operativa. Estos sistemas suelen funcionar con redes TCP/IP estándares, a menudo utilizando protocolos como OPC UA, MQTT o API REST para el intercambio de datos. La segmentación de la red es particularmente importante aquí, ya que estos sistemas a menudo sirven de puente entre las redes de TI y TO, convirtiéndolos en objetivos potenciales para ciberataques.

VALOR CLAVE DE SEGMENTACIÓN DE DISPOSITIVOS ZSCALER:

- A diferencia de los cortafuegos tradicionales, Zscaler ZTDS funciona independientemente de los detalles a nivel de red y permite un control dinámico de políticas independientemente de cómo se conecten a la red los sistemas a nivel operativo. Un motor de políticas adaptativo centralizado reduce significativamente la complejidad operativa asociada a los cortafuegos tradicionales.

- Es crucial una respuesta eficaz ante incidentes para reducir el impacto de los incidentes cibernéticos en entornos de misión crítica. Zscaler Ransomware Kill–Switch es una potente herramienta de respuesta a incidentes que prepara a las organizaciones para la respuesta ante emergencias y detiene rigurosamente la propagación de amenazas por la red.

- La arquitectura única de Zscaler ZTDS centraliza toda la inteligencia a nivel de red y elimina las dependencias de productos puntuales y tecnologías complejas como VLAN, ACL, 802.1X, Cortafuegos y enrutamiento L3.

Caso de uso 4

Comunicaciones a nivel de supervisión

En el nivel 2, las comunicaciones de nivel de supervisión implican interacciones críticas entre HMI, los sistemas SCADA y otros sistemas de control de supervisión de las redes TCP/IP. Estos sistemas suelen comunicarse mediante protocolos industriales como Modbus TCP, EtherNet/IP, y OPC UA, que funcionan en puertos de red estándar (502 para Modbus, 44818 para EtherNet/IP, 4840 para OPC UA). Son responsables de supervisar y controlar los procesos industriales, recopilar datos en tiempo real y proporcionar interfaces para los operadores. Debido a la naturaleza heredada de muchos sistemas de supervisión, su uso de protocolos potencialmente vulnerables y su papel crítico en las operaciones, proteger estas comunicaciones es particularmente importante. Se deben emplear una segmentación de red adecuada y controles de seguridad específicos del protocolo. Estas comunicaciones pueden subdividirse en:

©2025 Zscaler, Inc. Todos los derechos reservados.

1. **Comunicaciones de nivel 2 entre dispositivos (por ejemplo, interacciones HMI a HMI)**
2. **Comunicaciones de nivel 2 a nivel 3 (por ejemplo, transferencia de datos de HMI a Historian)**

VALOR CLAVE DE SEGMENTACIÓN DE DISPOSITIVOS ZSCALER:

- La tecnología patentada Zscaler ZTDS aísla de forma única los sistemas de supervisión (por ejemplo HMI) conectado en nivel 2 de Purdue, creando límites de aislamiento seguros que reducen significativamente la superficie de ataque en estos sistemas heredados y vulnerables.

- Zscaler ZTDS detecta y visualiza todas las comunicaciones de dispositivo a dispositivo en el nivel de supervisión y las interacciones con el nivel 3 (nivel de operación) independientemente de la configuración de VLAN. Crea mapas de tráfico de estas comunicaciones y mantiene registros de transacciones en el SIEM elástico integrado.

- Construido con principios de zero trust, Zscaler ZTDS se integra con diversas herramientas empresariales, incluidas CMDB y EDR, para ajustar automáticamente las políticas de control de acceso en función de los cambios de comportamiento. Un marco de políticas jerárquico permite la implementación de políticas en un solo sitio, en varios grupos de sitios o en todos los sitios.

- Marco de políticas simplificado que utiliza atributos y etiquetas de dispositivos (mediante etiquetado automático, entrada manual o importación de terceros) en lugar de direcciones IP y MAC complejas

- Una de las mayores ventajas de Zscaler ZTDS es que no requiere agentes, interopera con equipos de red existentes (independientemente del proveedor, modelo o versión) y requiere cambios mínimos en la configuración de la red.

Caso de uso 5

Comunicación a nivel de control

En el nivel 1, los PLC y las RTU interactúan entre sí para coordinar las operaciones de los dispositivos y el control de procesos. Estos dispositivos también se comunican con sistemas de nivel 2 como HMI y sistemas SCADA para permitir la supervisión y el control en tiempo real de los procesos industriales. Esta capa de comunicación es fundamental para

mantener la eficiencia operativa y requiere sólidas medidas de seguridad para evitar posibles ciberamenazas, garantizando al mismo tiempo una latencia mínima y una alta fiabilidad.
Estas comunicaciones pueden dividirse además en:

1. **Interconexión de nivel 1 (por ejemplo, comunicaciones de PLC a PLC)**
2. **Nivel 1 y nivel 2 (por ejemplo, comunicaciones de PLC a HMI)**

©2025 Zscaler, Inc. Todos los derechos reservados.

VALOR CLAVE DE SEGMENTACIÓN DE DISPOSITIVOS ZSCALER:

- Gracias a su arquitectura única, Zscaler ZTDS visualiza y analiza diversas comunicaciones y ofrece la capacidad de identificar y perfilar los sistemas TO conectados. Analiza los distintos protocolos, incluidos HTTP, ENIP, Modbus, SSL, etc., y extrae información de metadatos para identificar y etiquetar con precisión los activos TO.

- Visualiza todas las comunicaciones entre dispositivos L1 (PLC, RTU) y sistemas L2 (HMI, SCADA). Implementa controles de acceso restringido para proteger los dispositivos L1 sensibles (por ejemplo los PLC) de dispositivos L2 de alto riesgo potencialmente vulnerables (p. ej. los HMI).

- Cuando se implementa en modo de aprendizaje, Zscaler ZTDS identifica con precisión los patrones de comunicación desde los dispositivos L1 (PLC, RTU) a los dispositivos L2 (HMI, etc.). Esto ayuda a modelar las políticas de segmentación.

- Los dispositivos de nivel 1 de Purdue están diseñados para funciones específicas y no implementan todos los principios de red estándar. Esto dificulta la implementación de Zscaler ZTDS Ringfence para estos dispositivos. Sin embargo, la falta de segmentación o aislamiento por dispositivo no compromete los controles de seguridad generales.

- Dado que las amenazas suelen originarse en dispositivos de nivel 2 vulnerables y de alto riesgo, ZTDS restringe el acceso de los dispositivos de nivel 1 únicamente al mínimo necesario para el funcionamiento de las operaciones comerciales.

- En lugar de la segmentación por dispositivo, ZTDS implementa la segmentación a nivel macro (utilizando la definición de red existente) o la segmentación a nivel de grupo (los dispositivos L1 se pueden agrupar en segmentos pequeños utilizando Airgap-Plus).

- Debido a que la comunicación entre dispositivos L1 a L1 requiere una programación especial, ZTDS reduce los cambios de programación no autorizados o incorrectos al restringir el acceso entrante a los dispositivos L1.

- Todas las demás funcionalidades, incluidos el descubrimiento y la creación de perfiles de activos, la visualización del tráfico, el control de políticas adaptativo y el interruptor de apagado contra ransomware, siguen siendo totalmente aplicables a los dispositivos de capa 1.

Los dispositivos de nivel O o de nivel de proceso de Purdue (por ejemplo sensores, actuadores) no son compatibles conTCP/IP y normalmente se conectan directamente a cada uno de los dispositivos de nivel 1 utilizando los protocolos personalizados, bus serie, etc. Estos dispositivos quedan fuera del alcance de la segmentación de dispositivos de Zscaler.

©2025 Zscaler, Inc. Todos los derechos reservados.

Resumen

La segmentación de dispositivos Zero Trust de Zscaler, como componente clave de la seguridad zero trust, juega un papel vital en la eliminación de la confianza implícita mediante la creación de límites lógicos entre diferentes tipos de dispositivos y sistemas industriales. Al implementar políticas de segmentación granular, las organizaciones pueden aislar los sistemas de producción críticos de los dispositivos potencialmente vulnerables, contener posibles brechas de seguridad y mantener estrictos controles de acceso entre las diferentes capas.

	Caso de uso 1 (Internet)	Caso de uso 2 (TI y TO)	Caso de uso 3 (Nivel 3 – Operaciones)	Caso de uso 4 (Nivel 2 – Supervisión)	Caso de uso 5 (Nivel 1 – Control)
Sin agente	✓	✓	✓	✓	✓
Independiente de la red	✓	✓	✓	✓	✓
Detección y elaboración de perfiles de activos	✓	✓	✓	✓	✓
Visibilidad del tráfico	✓	✓	✓	✓	Segmento Intermedio
Integración de terceros	N/A	✓	✓	✓	✓
Control de políticas adaptativo	✓	✓	✓	✓	Segmento Intermedio
Interruptor de seguridad contra ransomware	N/A	✓	✓	✓	✓
Gestión centralizada	✓	✓	✓	✓	✓

Los proyectos de segmentación a menudo no se completan porque las alternativas actuales requieren cambios significativos en la red (como actualizaciones o renovaciones de equipos), carecen de un control granular o no cubren todas las capas de las redes de fabricación. Zscaler ZTDS ofrece una solución única, brindando una cobertura integral a través de una plataforma sin agentes, independiente de la red y fácil de usar. Zscaler ZTDS se implementa rápidamente y no requiere tiempo de inactividad operativa. Las organizaciones de producción ahora pueden unirse a las empresas Fortune 500 y utilizar Zscaler Zero Trust Device Segmentation (ZTDS) para implementar rápidamente la segmentación de zero trust, protegiendo así sus redes críticas de tecnología operativa (TO) y control industrial.

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 de la pérdida de datos gracias a la conexión segura de usuarios, dispositivos y aplicaciones ubicados en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo , Zero Trust Exchange™ basada en SSE es la mayor plataforma de seguridad en línea en la nube del mundo. Para obtener más información, visite **www.zscaler.com/es** o síganos en Twitter**@zscaler**.

© 2025 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales enumeradas en **zscaler.com/es/legal/trademarks** son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/u otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.

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

zscaler™

Zero Trust Everywhere