Zscaler para la fabricación

Aplique el modelo Zero Trust al modelo Purdue

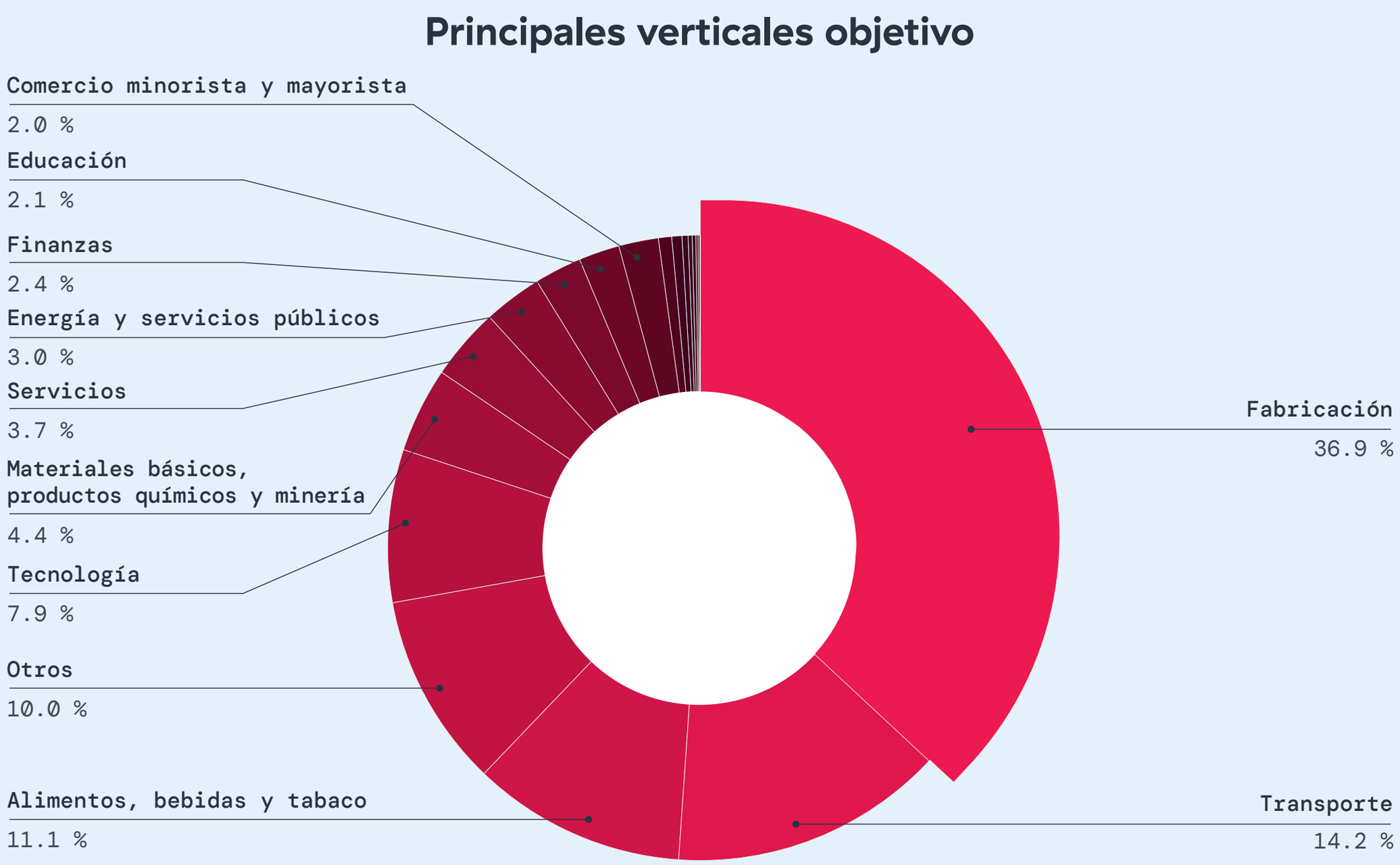
RESUMEN DE LA SOLUCIÓN

Las fábricas necesitan un enfoque nuevo para proteger los sistemas OT.

Las organizaciones globales del sector de la fabricación se han propuesto mejorar sus líneas de producción con la adición de robots inteligentes, sensores IoT en cada máquina, análisis basados en la nube y un gemelo digital de toda la planta. El objetivo es simple: mayor producción, menor tiempo de inactividad y mantenimiento predictivo que permitan una producción las 24 horas, todos los días.

Pero muchas organizaciones se han percatado de una realidad diferente. Cada conexión nueva amplía la superficie de ataque de OT. Y, una vez que los atacantes se infiltran, el riesgo de impacto es mucho mayor debido a los sistemas operativos obsoletos, las redes planas y la visibilidad limitada de OT. Para continuar la transformación de las fábricas, es necesario que replanteen su arquitectura de seguridad.

En la última versión del informe de IoT/OT de Threatlabz de Zscaler, el sector de la fabricación fue el más afectado, con el 36 % de los bloqueos de malware de IoT.

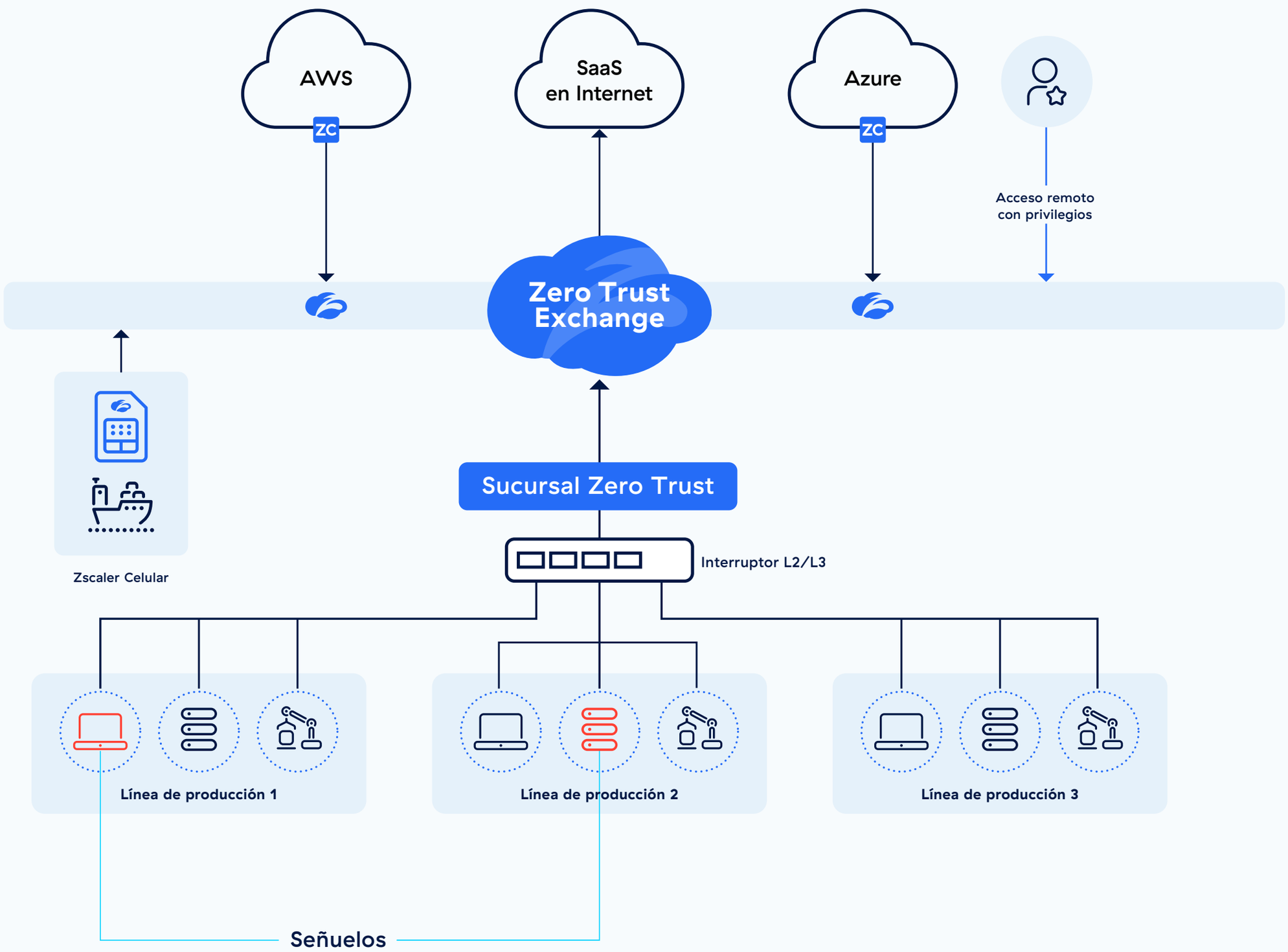


Distribución de los sectores más atacados

Extienda la zero trust a todos los usuarios y dispositivos, dentro y fuera de sus fábricas.

Para garantizar la seguridad en entornos industriales y de fabricación, los equipos de seguridad deben asegurarse de inspeccionar cada interacción de usuario y dispositivo y aplicar las políticas de privilegios mínimos. Nuestro enfoque Zero Trust está diseñado específicamente para OT, para permitir el acceso seguro, la segmentación y la conectividad en todas las operaciones de su fábrica.

- Dé acceso a técnicos y terceros a los sistemas OT críticos sin VPN.
- Aplique una segmentación granular este–oeste para impedir el movimiento lateral de las amenazas.
- Conecte de forma segura los sistemas OT a la nube y al centro de datos para realizar análisis
- Amplíe Zero Trust a los sistemas OT celulares como camiones, quioscos y escáneres de puntos de venta.
- Detecte a los atacantes en una fase temprana e impida que escalen privilegios



Arquitectura de fábrica Zero Trust

Componentes de la solución de Zscaler

Acceso remoto con privilegios

Permita que técnicos remotos y externos se conecten de manera segura a objetivos RDP/SSH/VNC a través de cualquier navegador sin agentes.

CAPACIDADES CLAVE

Controles de portapapeles Limite las funciones de copiar y pegar basándose en políticas Zero Trust para proteger los datos confidenciales.	**Controles de auditoría y gobernanza** Reduzca el riesgo de terceros mediante la grabación de sesiones, el uso compartido de sesiones y el acceso guiado.
Bóveda de credenciales y mapeo Almacene las credenciales de los sistemas de destino en una bóveda en la nube y comparta el acceso a través de políticas de mapeo.	**Acceso limitado en el tiempo y "justo a tiempo"** Asigne ventanas de mantenimiento y facilite el acceso JIT para el mantenimiento de emergencia.

Segmentación Zero Trust

Microsegmente los sistemas OT y aplique políticas para garantizar que solo haya comunicaciones autorizadas entre sus sistemas OT y los sistemas OT–IT.

Microsegmentación granular Aísle los sistemas OT compatibles en un segmento único (utilizando /32).	**Detección y clasificación de dispositivos:** Detecte y clasifique automáticamente los dispositivos OT.
Interruptor de seguridad contra ransomware Automatice la respuesta a incidentes mediante el uso de políticas preestablecidas para bloquear progresivamente los sistemas OT.	**Aplicación de políticas** Agrupe los dispositivos automáticamente y aplique políticas para el tráfico este–oeste basadas en el tipo de dispositivo/etiquetas.

Acceso seguro a OT

Habilite las cámaras, sensores, monitores, quioscos y otros sistemas OT para que se conecten de manera segura a las aplicaciones en la nube e Internet. Evite la comunicación con aplicaciones y URL riesgosas o maliciosas.

Aprovisionamiento sin contacto Aproveche la implementación totalmente automatizada sin intervención con plantillas predefinidas.	**Políticas Zero Trust unificadas** Inspeccione y aplique políticas para IoT/OT a aplicaciones privadas e internet.
Aplicación granular de políticas Aplique políticas basadas en la geolocalización del usuario/dispositivo, la ubicación de las URL a las que se accede, los datos confidenciales, etc.	**Conexión celular Zero Trust** Conecte fácilmente dispositivos celulares como camiones, quioscos, plataformas petrolíferas, etc.

Zscaler Deception

Utilice señuelos para detectar amenazas de OT que hayan eludido las defensas existentes. Detecte a los usuarios comprometidos, detenga el movimiento lateral y defiéndase contra el ransomware y los empleados maliciosos.

Detección de movimiento lateral Implemente PLC y sistemas SCADA señuelo para detectar a los atacantes que intenten moverse lateralmente.	**Detección previa a la violación** Reciba alertas precisas cuando los malintencionados estén explorando su entorno antes de un ataque.
Implementación nativa en la nube Se integra con Zscaler Private Access (ZPA) para crear, alojar y distribuir señuelos.	**Red de configuración cero** Diga adiós a los enlaces troncales VLAN, los puertos SPAN y los túneles GRE para enrutar el tráfico a señuelos.

Diferenciadores de Zscaler

ELIMINE LAS BRECHAS DE SEGURIDAD

Implemente políticas Zero Trust uniformes en todos los entornos, tanto dentro como fuera de sus fábricas.

REDUZCA EL TIEMPO DE INACTIVIDAD

Implemente la segmentación Zero Trust con una mínima interrupción de su entorno OT existente, lo que el riesgo de tiempo de inactividad debido al movimiento lateral.

REDUCIR LOS COSTOS Y LA COMPLEJIDAD

Reduzca o consolide las herramientas de firewall, NAC, VPN, VDI y microsegmentación con el modelo Purdue de arquitectura de seguridad más simple dentro de sus fábricas.

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 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 zscaler.com/mx

zscaler™

Zero Trust Everywhere