Zscaler para fabricación

Implementar la zero trust en el modelo de Purdue

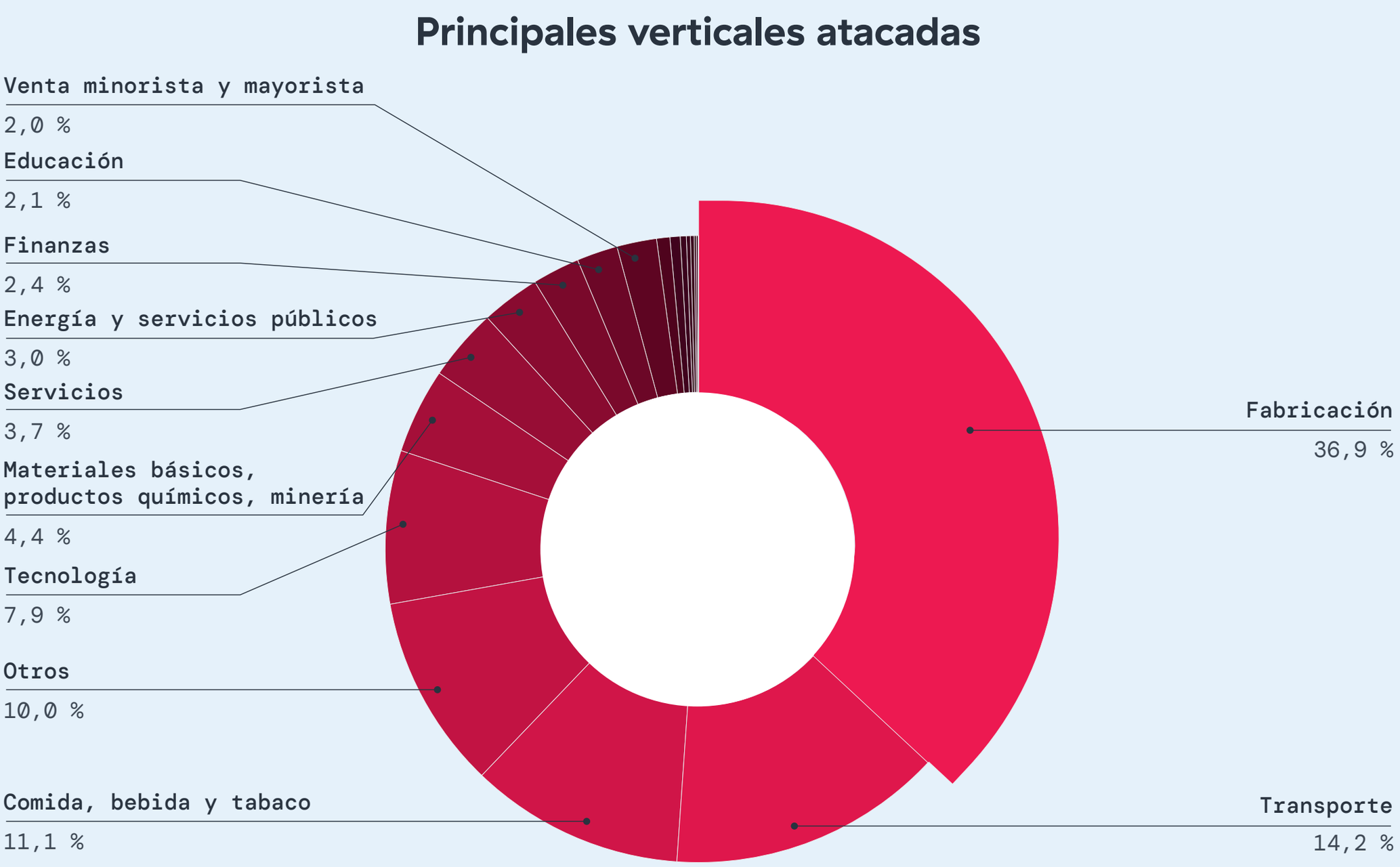
RESUMEN DE LA SOLUCIÓN

Las fábricas necesitan una nueva forma de proteger los sistemas OT

Las organizaciones manufactureras globales se han propuesto mejorar sus líneas de producción, agregando robots inteligentes, sensores de 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 permita ua producción 24/7.

Pero muchas organizaciones han se han encontrado con una realidad diferente. Cada nueva conexión amplía la superficie de ataque OT. Y, una vez que los atacantes logran entrar, el riesgo de impacto es mucho mayor debido al sistema operativo obsoleto, las redes planas y la visibilidad limitada de OT. Para continuar con la transformación de las fábricas, estas necesitan replantear su arquitectura de seguridad.

En la última versión del informe IoT/OT de Threatlabz de Zscaler , el sector manufacturero fue el más afectado, representando el 3 % de los bloqueos de malware de IoT.

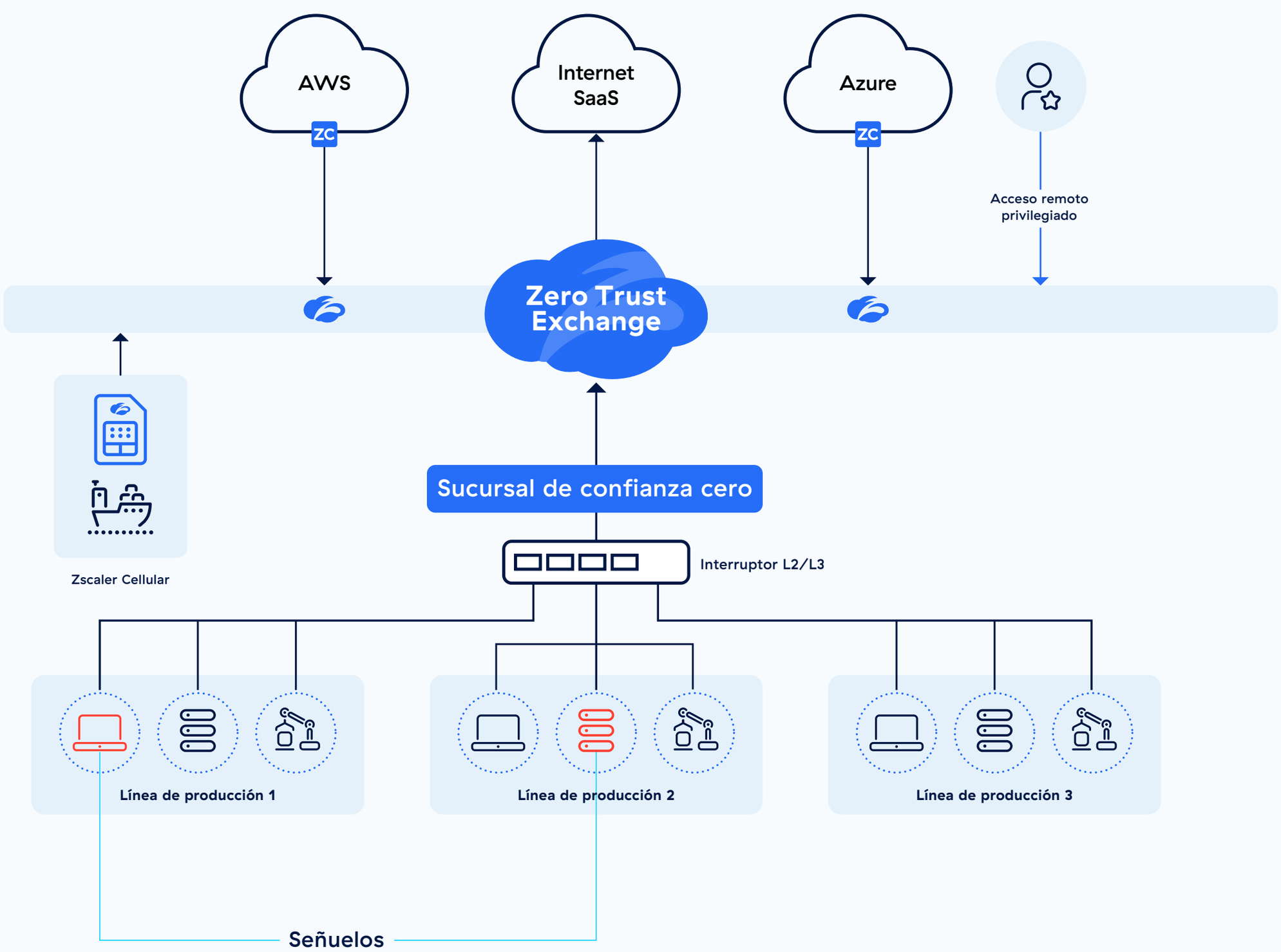


Distribución de los sectores más atacados

Extienda Zero Trust a todos los usuarios y dispositivos, dentro y fuera de las fábricas

Para proteger los entornos industriales y de fabricación, los equipos de seguridad deben garantizar que cada interacción entre usuarios y dispositivos se inspeccione y aplique de acuerdo con políticas de mínimo privilegio. Nuestro enfoque de Zero Trust está diseñado específicamente para OT y permite acceso seguro, segmentación y conectividad en todas las operaciones de su fábrica.

- Brinde a los técnicos y a terceros acceso a sistemas OT críticos sin VPN
- Aplique una segmentación granular de este a oeste para evitar 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 sistemas celulares como camiones, quioscos y escáneres POS
- Detecte a los atacantes de forma temprana y evite que aumenten los privilegios



Arquitectura de fábrica de zero trust

Componentes de la solución Zscaler

Acceso remoto privilegiado

Permita que terceros y técnicos remotos se conecten de forma segura a objetivos RDP/SSH/VNC a través de cualquier navegador.

CAPACIDADES CLAVE

Control del portapapeles Límite capacidades las capacidades de copiar y pegar basadas en políticas zero trust para proteger datos confidenciales.	**Controles de auditoría y gobernanza** Reduzca el riesgo procedente de terceros con la grabación de sesiones, el uso compartido de sesiones y el acceso guiado.
Mapeo y boveda de credenciales 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 proporcione acceso JIT para mantenimiento de emergencia.

Segmentación de confianza cero

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

Microsegmentación granular Aísle los sistemas OT compatibles en un segmento de uno (utilizando /32).	**Descubrimiento y clasificación de dispositivos** Descubra y clasifique automáticamente dispositivos OT.
Interruptor de ransomware Automatice la respuesta a incidentes mediante el uso de políticas preestablecidas para bloquear progresivamente los sistemas OT.	**Aplicación de políticas** Agrupe dispositivos automáticamente y aplique políticas para el tráfico de este a oeste según el tipo de dispositivo y las etiquetas.

Acceso seguro a OT

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

Aprovisionamiento sin intervención Aproveche la implementación sin intervención totalmente automatizada con plantillas predefinidas.	**Políticas unificadas de zero trust** Inspeccione y aplique políticas para IoT/OT a aplicaciones privadas e Internet.
Aplicación granular de políticas Aplique políticas basadas en localización geográfica, ubicación, URL accedidas, datos confidenciales, etc del usuario/dispositivo.	**Zero Trust Cellular** Aplique Zero Trust para conectar dispositivos celulares como camiones, quioscos, plataformas, etc.

Zscaler Deception

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

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

Diferenciadores de Zscaler

ELIMINAR LAS BRECHAS DE SEGURIDAD

Aplique políticas de zero trust consistentes en todos los entornos dentro y fuera de sus fábricas.

REDUZCA EL TIEMPO DE INACTIVIDAD

Aplique la segmentación de zero trust con una interrupción mínima en su entorno OT existente, lo que reduce el riesgo de tiempo de inactividad debido al movimiento lateral.

REDUCIR LOS COSTES Y LA COMPLEJIDAD

Reduzca o consolide cortafuegos, NAC, VPN, VDI y herramientas de microsegmentación con una arquitectura de seguridad del Modelo Purdue 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, 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**.

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

zscaler™

Zero Trust Everywhere