FICHA DE DATOS

Zero Trust Device Segmentation

Protección simplificada frente a amenazas laterales para redes de sucursales, fábricas y campus

Como parte integral de Zscaler Zero Trust Networking, la segmentación de dispositivos ayuda a los equipos de TI a reducir el riesgo, garantizar el cumplimiento y mejorar el tiempo de actividad empresarial eliminando las fuentes de movimiento lateral de amenazas en las redes empresariales.

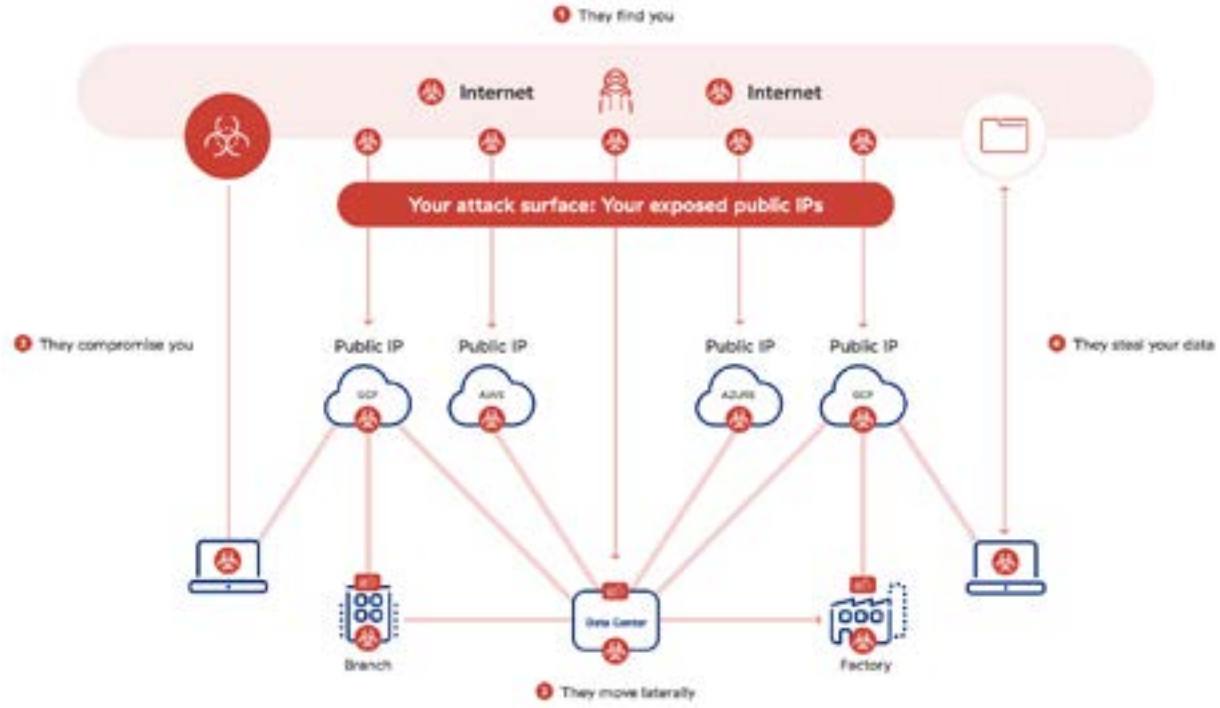
La evolución del panorama de las amenazas y el cumplimiento normativo

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 un aviso de advertencia a las organizaciones gubernamentales en relación con ciberatacantes preparados para desestabilizar las infraestructuras críticas, como los sistemas de transporte, los oleoductos y gasoductos de gas natural, las plantas de tratamiento de agua y las redes eléctricas. Esto complementa acciones similares emprendidas por la TSA para la seguridad de aeropuertos, operadores aéreos y ferroviarios, la reciente línea de base de ciberseguridad del DOE y la actualización casi definitiva del NERC al CIP-015-1.

Las tecnologías OT/IoT se diseñaron para ofrecer en primer lugar velocidad y eficacia en las transacciones, con la seguridad como objetivo secundario. Lamentablemente, OT/IoT es ahora un objetivo favorito de los ciberdelincuentes, con un aumento interanual del 400 % en los ataques, según el estudio 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 OT.

Zscaler Zero Trust Networking

Un medio más sencillo, seguro y rentable para la comunicación entre usuarios, dispositivos y cargas de trabajo



Cómo ocurren los ataques de ransomware

La EPA, la CISA y el FBI recomiendan encarecidamente a los operadores de sistemas que trabajen para cumplir la orden ejecutiva de la Oficina del Presidente de utilizar Zero Trust como directriz hacia una mejor ciberseguridad. Los puntos resaltados son áreas clave en estas recomendaciones donde Zscaler puede ayudar inmediatamente con nuestra solución de Segmentación de Dispositivos de Zero Trust.

- Reduzca la exposición a Internet de cara al público
- Reduzca la exposición a vulnerabilidades
- 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 un inventario de los activos OT/IT

Una arquitectura más segura para la segmentación de dispositivos

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

Panel de segmentación de dispositivos Zero Trust

Zscaler ha presentado Zero Trust Networking como una manera más sencilla, segura y rentable para que los usuarios, los dispositivos y las cargas de trabajo se comuniquen. La segmentación de dispositivos es fundamental en este enfoque como paso básico para establecer una visibilidad y un control granular para la red moderna.

Zscaler elimina la fricción de la segmentación intra-VLAN con una solución sin agente que frena todas las amenazas laterales aislando cada punto final IP, incluidos los sistemas heredados y sin supervisores, en un "segmento de red único". 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:

Segmentación interna de LAN
Extienda Extienda Zero Trust a la LAN imponiendo la segmentación en el tráfico este-oeste.Esto reduce su superficie de ataque interna y elimina la amenaza del movimiento lateral en redes OT/IoT críticas, sin necesidad de NAC ni de segmentación basada en firewalls.

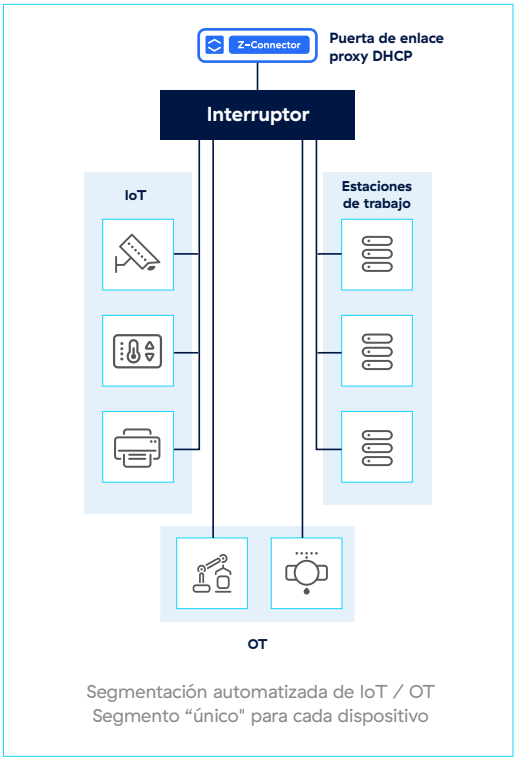
Para aplicar la segmentación Zero Trust en su red, simplemente:

- Aprovisione automáticamente cada dispositivo en un segmento único (/32).
- Agrupe automáticamente dispositivos, usuarios y aplicaciones mediante el análisis de sus patrones de tráfico, evitando que dispositivos no autorizados utilicen la suplantación de MAC para entrar en 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 Zscaler Zero Trust Device Segmentation actúa como un interruptor de desactivación de ransomware, inhabilitando la comunicación de dispositivos no esenciales para detener el movimiento lateral de las amenazas sin interrumpir las operaciones empresariales.Esta solución neutraliza amenazas avanzadas como ransomware en dispositivos IoT, sistemas OT y dispositivos sin capacidad de agente.

- Agrupe y aplique de manera autónoma la política para direcciones MAC conocidas en cualquier dispositivo (por ejemplo, denegación de acceso RDP a cámaras excepto para administradores)
- Aísle automáticamente las direcciones MAC desconocidas para limitar el radio de alcance en caso de que un dispositivo se vea comprometido
- Integración con sistemas de gestión de activos para políticas de control de acceso seguro



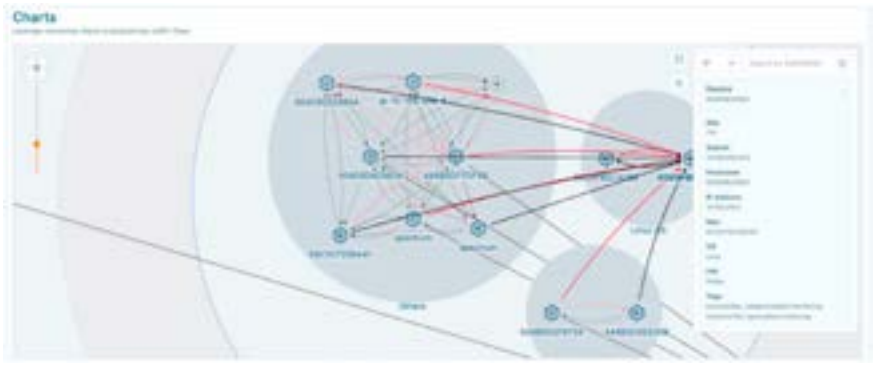
Segmentación automatizada de IoT / OT
Segmento “único" para cada dispositivo

Detección y clasificación automática de dispositivos

Dado que una parte significativa del tráfico OT/IoT permanece dentro de la red local, es importante disponer de 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 compleja gestión de inventario.

Para visibilidad de red y dispositivos:

- Descubra, clasifique y realice inventarios de los dispositivos OT/IoT sin necesidad de agentes de punto final
- Obtenga una referencia de los patrones de tráfico y los comportamientos de los dispositivos para determinar los accesos autorizados y no autorizados
- Obtenga información precisa sobre la red para la gestión del rendimiento y el mapeo de amenazas

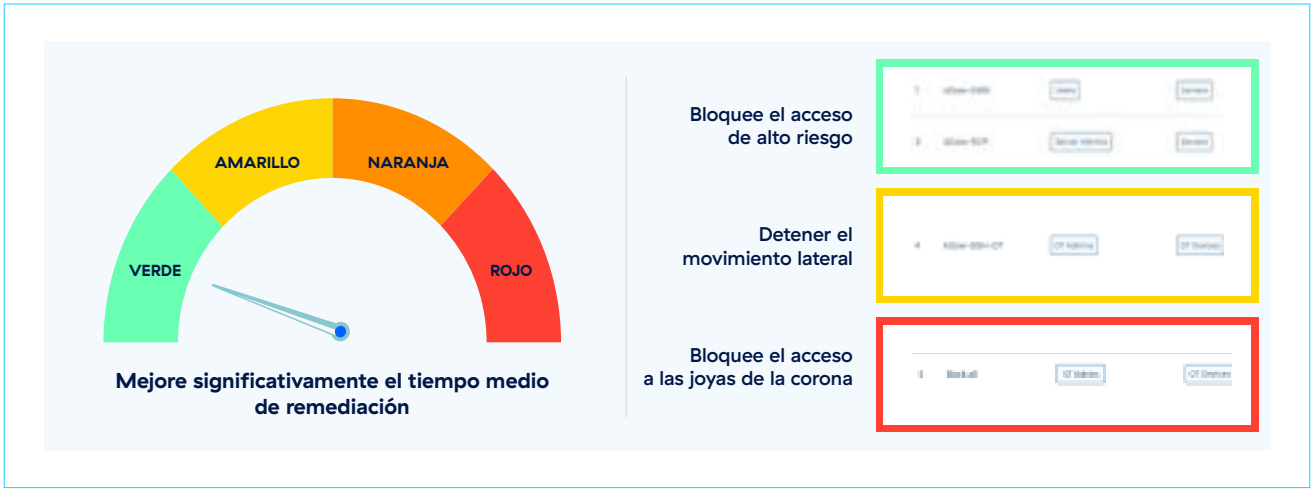


Panel de detección de dispositivos

Respuesta automatizada a incidentes

Presentamos Zscaler Ransomware Kill Switch. Reducción de la superficie de ataque con un solo clic totalmente integrada en nuestra solución Zero Trust Device Segmentation. Bloquee los protocolos y puertos vulnerables conocidos e incluso deshabilite instantáneamente el acceso a redes críticas como hospitales o plantas de fábrica enteras. Todo con niveles de gravedad preestablecidos para minimizar el tiempo de inactividad de la empresa.

Ransomware Kill Switch actúa como punto de aplicación de políticas multicapa, permitiendo niveles escalonados de respuesta a incidentes ante un compromiso activo, y el aumento de la inversión en herramientas de seguridad existentes. Cada nivel del Ransomware Kill Switch tiene una funcionalidad similar a los "fusibles virtuales" o niveles Defcon, con rutas de escalada predefinidas para bloquear todas las comunicaciones de red innecesarias hacia o desde cualquier punto final, negando la propagación lateral y reduciendo drásticamente la superficie de ataque.



Esta solución desactiva instantáneamente la comunicación no esencial de los dispositivos 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.

Zscaler ofrece un control completo del Ransomware Kill Switch a través de API. Mediante estas interfaces programables, las organizaciones de TI pueden habilitar las herramientas de orquestación de seguridad existentes, como la gestión de eventos e información de seguridad (SIEM), la orquestación y respuesta de seguridad (SOAR) o las soluciones EDR/XDR, para automatizar la respuesta a incidentes y poner inmediatamente en cuarentena los puntos finales comprometidos y contener el radio de alcance de la infección.

Esto proporciona a las organizaciones una protección de la inversión para su red existente y su infraestructura de seguridad, al tiempo que mejora inmediatamente la postura de seguridad de la empresa.

Ventajas

Contención granular para limitar la propagación lateral

Respuesta a incidentes automatizada y planificada previamente en el caos de una violación

Contención dura en capas fronterizas clave, como entre la TI corporativa y las redes centrales

Cierre ordenado de puertos y protocolos sospechosos para maximizar el tiempo de actividad empresarial

Elimine el movimiento lateral de amenazas a través de la LAN
Reduzca la superficie de ataque aislando cada uno en su propia “red única", eliminando la superficie de ataque y el riesgo de propagación de amenazas. Incluso los dispositivos comprometidos ya no pueden infectar a sus vecinos.

Reduzca la complejidad operativa y los costos asociados con las herramientas de segmentación heredadas
Segmente cada punto final de IP sin la complejidad de tecnologías de red antiguas y centradas en IP como NAC y firewalls este–oeste, o construcciones complejas como ACL y segmentación manual de VLAN.

Obtenga una mayor visibilidad del tráfico este–oeste
Obtenga una visibilidad lateral completa 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 cualquier dispositivo, incluso de aquellos que no pueden aceptar agentes.

Implemente sin interrumpir la red
Tecnología sin agente que se implementa rápidamente sin alterar la manera habitual de hacer negocios de los clientes y no requiere cambiar la arquitectura de la red ni redireccionar el IP de los dispositivos.

Cumplimiento más rápido
Los ciberestándares federales en todas las industrias ahora destacan la segmentación como piedra angular de Zero Trust. El enfoque sin agentes de Zscaler se implementa rápidamente y mejora al instante la postura de cumplimiento.

Características:

Aislamiento Airgap

- Aislamiento de dispositivos sin agentes
- Cuarentena de dispositivos con un solo clic
- Detección de violaciones por aislamiento Airgap
- Filtrado basado en direcciones MAC

Segmentación Zero Trust

- Segmentación basada en red

Segmentación basada en dispositivos

- Agrupamiento y política autónoma
- Control de políticas intraVLAN e interVLAN
- Política dinámica basada en etiquetas
- Política basada en la identidad del dispositivo y del usuario
- Política basada en el tiempo
- Política basada en zonas
- Marco de políticas jerárquico

Elaboración de perfiles y detección de activos

- Detección de puntos finales y redes
- Huella digital del dispositivo
- Categorización de dispositivos basada en perfiles
- Descodificación de protocolos ICS/ médicos

Alta disponibilidad

- Clúster de dos nodos con VRRP
- VRRP con sincronización de sesión
- Sincronización de configuración y estado
- Agregación de enlaces
- Supervisión de la actividad de la interfaz
- Actualizaciones de software sin problemas
- Reemplazo de hardware en servicio

Servicios de enrutamiento y red

- Enrutamiento dinámico: BGP, OSPF
- Rutina de multidifusión: IGMP, PIM
- Servidor DHCP, Relé/Proxy
- Enlace troncal de VLAN
- Traducción de direcciones de red
- Enrutamiento basado en políticas
- Ruta múltiple de igual costo (ECMP)
- VPN de sitio a sitio

Respuesta a incidentes

- Ransomware Kill Switch

Visibilidad y registro

- Mapa de tráfico con correlación de políticas
- Lago de datos elástico integrado
- Registros de inicio de sesión para todas las comunicaciones intra e intersegmentos
- Exportación de registros a SIEM/Colector de registros

Modos de implementación flexible

- Aprovisionamiento sin contacto de la puerta de enlace Airgap
- Plantillas y perfiles de sitios
- Implementación autónoma, en clúster de alta disponibilidad o multiclúster
- Puertas de enlace Airgap basadas en máquinas físicas o virtuales

Supervisión y resolución de problemas

- Consola de depuración remota
- CLI local en puertas de enlace Airgap
- Compatibilidad con SNMP

Gestión centralizada basada en la nube

- Inicio de sesión único (SSO) y MFA
- Registros de auditoría para eventos de inicio de sesión y cambios de configuración
- Control de acceso basado en roles
- Plataforma en la nube multiusuario
- Acceso basado en API

Integraciones de terceros

- Microsoft Active Directory
- Integración SIEM
- Proveedores de EDR: Crowdstrike, SentinelOne
- Gestión de activos—Armis
- SSE—Zscaler ZIA

Dimensionamiento del dispositivo de puerta de enlace Zscaler

A continuación se muestran varias estimaciones de tamaño para dispositivos de puerta de enlace Zscaler de hardware o virtualizados.

Especificaciones de hardware para implementaciones de puertas de enlace físicas						
	XS	S1	S2	M	L	XL
Disponibilidad	Junio de 2024	Junio de 2024	Ahora	Ahora	Ahora	1er trim. ej. 2025
Modelo de hardware	ZT400	ZT600	Dell VEP4600	Dell VEP4600	Dell VEP4600	Por confirmar
CPU	4C Atom	8C Atom	Procesador Xeon 4C	8C Xeon	16C Xeon	16C Xeon
Memoria	16 GB	16 GB	16 GB	32 GB	64 GB	64 GB
Almacenamiento	64 GB	64 GB	128 GB	256 GB	960 GB	256 GB
Puertos	4x 1 GbE	4x 1 GbE	6x 1 GbE 2x 1GbE (SFP)	4x 1 GbE 2x 10 GbE	4x 1 GbE 6x 10 GbE	4x 25 GbE
Factor de forma	Escritorio	Escritorio	1U	1U	1U	1U
Otras características	Sin ventilador		RPS	RPS	RPS	RPS
Rendimiento (HTTP de 64 KB)	4 Gbps	8 Gbps	10 Gbps	20 Gbps	40 Gbps	80 Gbps
Sesiones	250 mil	500 mil	500 mil	1M	2M	2M
# Puntos finales	200	500	1000	2000	4000	Por confirmar

Guía de dimensionamiento de dispositivos virtuales				
	XS	S1	S2	M
Disponibilidad	Ahora	Ahora	Ahora	Ahora
CPU	2 CPU virtuales	4 CPU virtuales	8 CPU virtuales	16 CPU virtuales
Memoria	8 GB	16 GB	32 GB	64 GB
Almacenamiento	256 GB	256 GB	256 GB	256 GB
Puertos	4x NIC virtuales	4x NIC virtuales	4x NIC virtuales	4x NIC virtuales
Rendimiento (HTTP de 64 KB)	5 Gbps	10 Gbps	20 Gbps	40 Gbps
Sesiones	250 mil	500 mil	1M	2M
# Puntos finales	200	500	2000	4000

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 SASE 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