FICHA DE DATOS

Zscaler 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, lograr el cumplimiento y mejorar el tiempo de actividad comercial al eliminar las fuentes de movimiento lateral de amenazas en las redes empresariales.

El panorama cambiante de las amenazas y el cumplimiento normativo

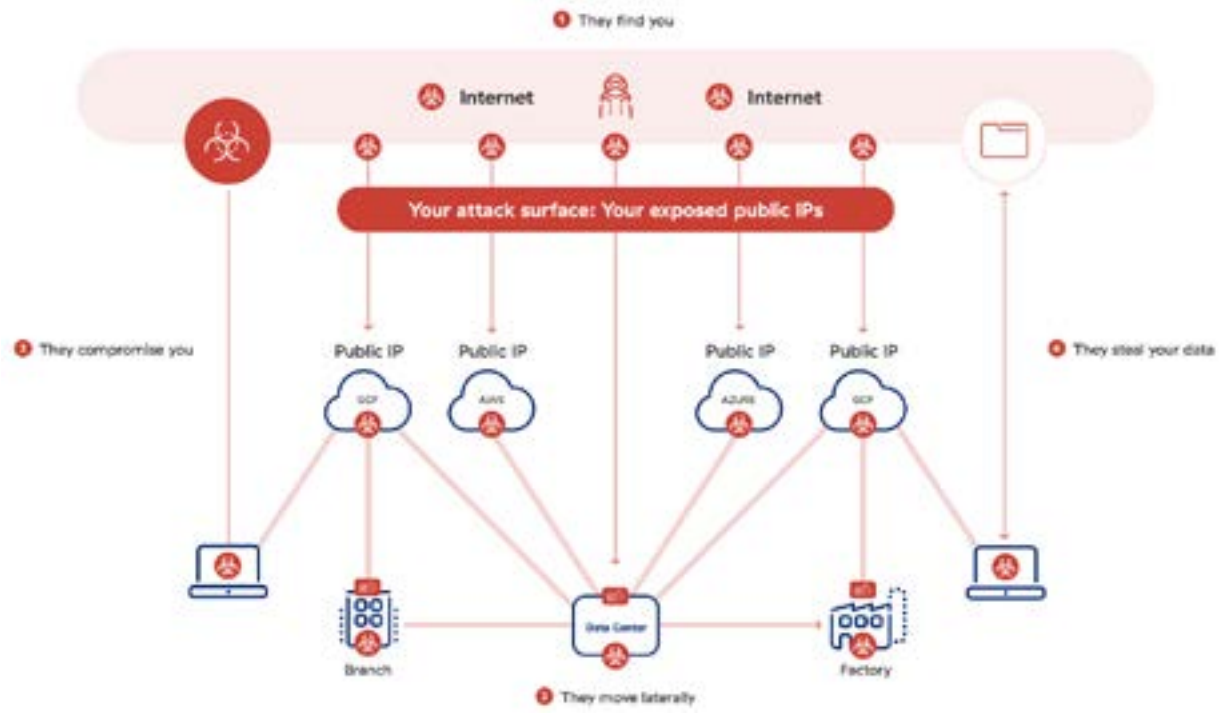
Recientemente, ha habido un aumento de alertas y advertencias sobre ciberataques de autores de amenazas patrocinados por estados a infraestructura crítica de Estados Unidos. El 7 de febrero de 2024, la Oficina Federal de Investigaciones (FBI) y la Agencia de Seguridad Cibernética y de Infraestructura (CISA), junto con la Agencia de Seguridad Nacional, emitieron una advertencia a las organizaciones gubernamentales sobre ciberdelincuentes preparados para interrumpir infraestructura crítica, como sistemas de transporte, oleoductos y gasoductos, plantas de tratamiento de agua y redes eléctricas. Esto complementa acciones similares adoptadas por la TSA para proteger aeropuertos, operadores de aeronaves y ferrocarriles, la reciente línea base de ciberseguridad del DOE y la actualización casi final del NERC a CIP-015-1.

Las tecnologías OT/IoT fueron diseñadas para brindar velocidad y eficiencia en las transacciones en primer lugar, con la seguridad como objetivo secundario. Desafortunadamente, OT/IoT es ahora un objetivo favorito de los ciberdelincuentes, con un aumento interanual del 400 % en los ataques, según la investigación de Zscaler ThreatLabz. El ransomware es la estrategia de ataque más popular y el 61 % de todas las infracciones tuvieron como objetivo organizaciones conectadas a OT.

Zscaler Zero Trust Networking

Un medio más sencillo, seguro y rentable para que los usuarios, los dispositivos y las cargas de trabajo se comuniquen

© 2024 Zscaler, Inc. Todos los derechos reservados.



Cómo se producen los ataques de ransomware

La EPA, la CISA y el FBI recomiendan encarecidamente que los operadores de sistemas trabajen según la orden ejecutiva de la Oficina del Presidente para utilizar zero trust como guía hacia una mejor ciberseguridad. Los elementos destacados son áreas clave en estas recomendaciones en las que Zscaler puede ayudar de inmediato con nuestra solución de segmentación de dispositivos Zero Trust:

- Reducir la exposición a Internet de cara al público
- Reducir la exposición a vulnerabilidades
- Segmentación de la red
- Recopilación de registros
- Prohibir la conexión de usuarios no autorizados
- No hay servicios explotables en Internet
- Límitar conexiones OT/IoT a Internet
- Detección de amenazas relevantes
- Realizar un inventario de 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 listas de control de acceso (ACL) y cortafuegos que administran el tráfico de norte a sur (de cliente a servidor). Sin embargo, la microsegmentación OT desplaza el foco hacia el tráfico este–oeste más vulnerable, que fluye lateralmente entre dispositivos y cargas de trabajo. En las VLAN compartidas, debido a la arquitectura de conmutación heredada, los dispositivos pueden verse y comunicarse con todos los demás, lo que crea un entorno propicio para la propagación del malware. Lamentablemente, las soluciones pioneras basadas en agentes para las cargas de trabajo en la nube no pueden segmentar las máquinas heredadas y sin cabeza tan comunes en OT, y los enfoques tradicionales basados en ACL siguen siendo demasiado complicados.

© 2024 Zscaler, Inc. Todos los derechos reservados.



Panel de segmentación de dispositivos Zero Trust

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

Zscaler elimina la fricción de segmentación intra-VLAN con una solución sin agente que detiene todas las amenazas laterales al aislar cada terminal de IP, incluidos los sistemas heredados y sin dirección, en un "segmento de red de uno". 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 la LAN
Extienda zero trust a la LAN al aplicar la segmentación en el tráfico este-oeste. Esto reduce la superficie de ataque interna y elimina la amenaza de movimiento lateral en redes OT/IoT críticas, sin necesidad de NAC o segmentación basada en cortafuegos.

Para aplicar la segmentación zero trust en su red, simplemente debe:

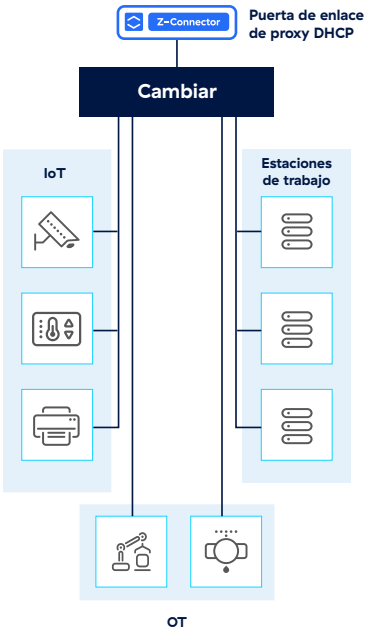
- Aprovisionar automáticamente cada dispositivo en un segmento de uno (/32).
- Agrupar automáticamente dispositivos, usuarios y aplicaciones analizando sus patrones de tráfico, lo que evita que dispositivos no autorizados utilicen la suplantación de MAC para acceder a la red.
- Aplicar dinámicamente políticas para el tráfico este-oeste en función de la identidad y el contexto de los usuarios y dispositivos.

© 2024 Zscaler, Inc. Todos los derechos reservados.

Segmentación TI/OT

La tecnología de segmentación de dispositivos Zero Trust de Zscaler actúa como un interruptor de seguridad contra ransomware, desactivando la comunicación no esencial del dispositivo 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.

- Agrupe y aplique políticas de forma autónoma para direcciones MAC conocidas en cualquier dispositivo (por ejemplo, acceso RDP a cámaras denegado excepto para administradores)
- Aísle automáticamente direcciones MAC desconocidas para limitar el radio de explosión en caso de que un dispositivo esté comprometido
- Integración con sistemas de gestión de activos para políticas de control de acceso seguro



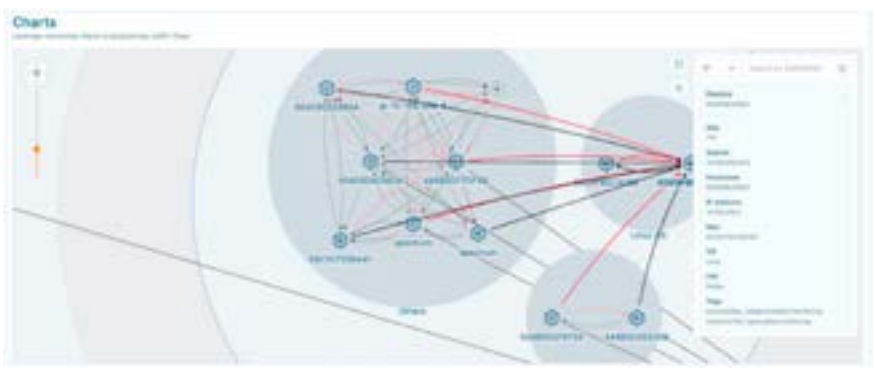
IoT automatizado / Segmentación OT
Segmento de 'uno' para cada dispositivo

Descubrimiento y clasificación automática de dispositivos

Porque una parte importante del tráfico OT/IoT permanece dentro de la red local, por lo que es importante tener una visibilidad continua del tráfico de este a oeste. Con el descubrimiento y la clasificación automáticos de dispositivos, los administradores de red pueden gestionar mejor el rendimiento, el tiempo de actividad y la seguridad de los sistemas IoT/OT sin gestión compleja de inventarios.

Para visibilidad de red y dispositivo:

- Descubra, clasifique y haga un inventario de dispositivos OT/IoT sin necesidad de agentes de punto final
- Obtenga una línea base de los patrones de tráfico y los comportamientos de los dispositivos para determinar el acceso autorizado y no autorizado
- Obtenga información precisa sobre la red para la gestión del rendimiento y la asignación de amenazas



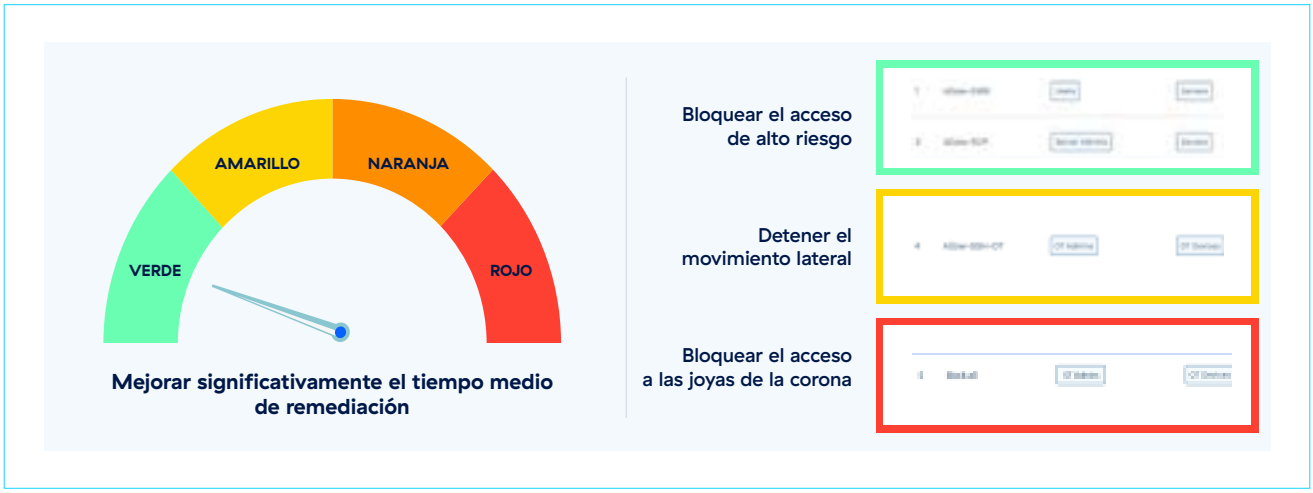
Panel de detección de dispositivos

© 2024 Zscaler, Inc. Todos los derechos reservados.

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 desactive instantáneamente el acceso a redes críticas como hospitales o plantas de fábrica completas. Todo con niveles de gravedad preestablecidos para minimizar el tiempo de inactividad de la empresa.

El interruptor de seguridad contra ransomware actúa como un punto de aplicación de políticas de múltiples capas, lo que permite 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 la de los "fusibles virtuales" o niveles Defcon, con rutas de escalada predefinidas para bloquear todas las comunicaciones de red innecesarias hacia o desde cualquier terminal, negando la propagación lateral y reduciendo drásticamente la superficie de ataque.



Esta solución desactiva instantáneamente la comunicación no esencial del dispositivo 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 control completo del interruptor de seguridad contra ransomware a través de API. Al utilizar estas interfaces programables, las organizaciones de TI pueden habilitar herramientas de orquestación de seguridad existentes, como Gestión de eventos e información de seguridad (SIEM), Orquestación y respuesta de seguridad (SOAR) o soluciones EDR/XDR para automatizar la respuesta a incidentes y poner en cuarentena inmediata los terminales comprometidos y contener el radio de expansión de la infección.

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

© 2024 Zscaler, Inc. Todos los derechos reservados.

Ventajas



Contención granular para limitar la propagación lateral



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



Contención estricta en capas límite clave, como entre la TI corporativa y las redes centrales



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

Elimine el movimiento lateral de amenazas a través de la LAN
Reduzca la superficie de ataque aislando cada dispositivo en su propia "red de uno", eliminando así 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 costes 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 cortafuegos este–oeste, o construcciones complejas como ACL y segmentación manual de VLAN.

Obtenga una mejor visibilidad del tráfico de este a oeste
Obtenga visibilidad lateral completa con la detección y la clasificación automáticos de dispositivos; los administradores de red pueden gestionar mejor el rendimiento, el tiempo de actividad y la seguridad de cualquier dispositivo, incluso aquellos que no pueden aceptar agentes.

Implementación sin interrupción de la red
Tecnología sin agente que se implementa rápidamente sin interrumpir la forma actual de hacer negocios de los clientes y no requiere cambiar la arquitectura de red ni cambiar la dirección IP de los dispositivos.

Cumplimiento más rápido
Los estándares federales de ciberseguridad en todos los sectores ahora consideran que la segmentación es una piedra angular de zero trust. El enfoque sin agente de Zscaler se implementa rápidamente y mejora instantáneamente la postura de cumplimiento.

Funcionalidades

Aislamiento del espacio de aire

- Aislamiento de dispositivos sin agente
- Cuarentena de dispositivos con un solo clic
- Detección de infracciones del aislamiento del espacio de aire
- Filtrado basado en direcciones MAC

Segmentación de confianza cero

- 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

© 2024 Zscaler, Inc. Todos los derechos reservados.

Detección y elaboración de perfiles de activos

- Detección de terminales y redes
- Huellas digitales de dispositivos
- Categorización de dispositivos basada en perfiles
- Descodificación de protocolo ICS/Médico

Alta disponibilidad

- Clúster de dos nodos con VRRP
- VRRP con sincronización de sesión
- Sincronización de configuración y estado
- Agregación de enlace
- 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 coste (ECMP)
- VPN de sitio a sitio

Respuesta a incidentes

- Interruptor de seguridad contra ransomware

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 flexibles

- Aprovisionamiento de Airgap Gateway sin intervención
- Plantillas y perfiles de sitios
- Implementación de clústeres independientes y de alta disponibilidad o de múltiples clústeres
- 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 entregada en la nube para múltiples inquilinos
- Acceso basado en API

Integraciones de 3 partes

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

© 2024 Zscaler, Inc. Todos los derechos reservados.

Dimensionamiento del dispositivo de puerta de enlace Zscaler

A continuación se presentan varias estimaciones de dimensionamiento para hardware o dispositivos de puerta de enlace Zscaler virtualizados.

Especificaciones de hardware para implementaciones de puertas de enlace físicas						
	XS	S1	S2	M	L	SG
Disponibilidad	Junio de 2024	Junio de 2024	Ahora	Ahora	Ahora	1QFY25
Modelo de hardware	ZT 400	ZT 600	Dell VEP4600	Dell VEP4600	Dell VEP4600	Por confirmar
CPU	Átomo 4C	Átomo 8C	Xeon 4C	Xeon 8C	Xeon 16C	Xeon 16C
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	4 x 1 GbE	4 x 1 GbE	6 x 1 GbE 2 x 1 GbE (SFP)	4 x 1 GbE 2 x 10 GbE	4 x 1 GbE 6 x 10 GbE	4 x 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 K	500 K	500 K	1 M	2 M	2 M
N° de terminales	200	500	1	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 K	500 K	1 M	2 M
N° de terminales	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 hora 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, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE, es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en **zscaler.com/es** o síganos en Twitter **@zscaler**.

©2024 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ y ZPA™ y otras marcas comerciales mencionadas en **zscaler.com/es/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/o en otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.