FICHA TÉCNICA

Zscaler Zero Trust Device Segmentation

Proteção simplificada contra ameaças laterais para redes de filiais, fábricas e campus

Parte integrante da Zscaler Zero Trust Networking, a segmentação de dispositivos ajuda as equipes de TI a reduzir riscos, obter conformidade e melhorar o tempo de atividade dos negócios, eliminando fontes de movimentação lateral de ameaças em redes corporativas.

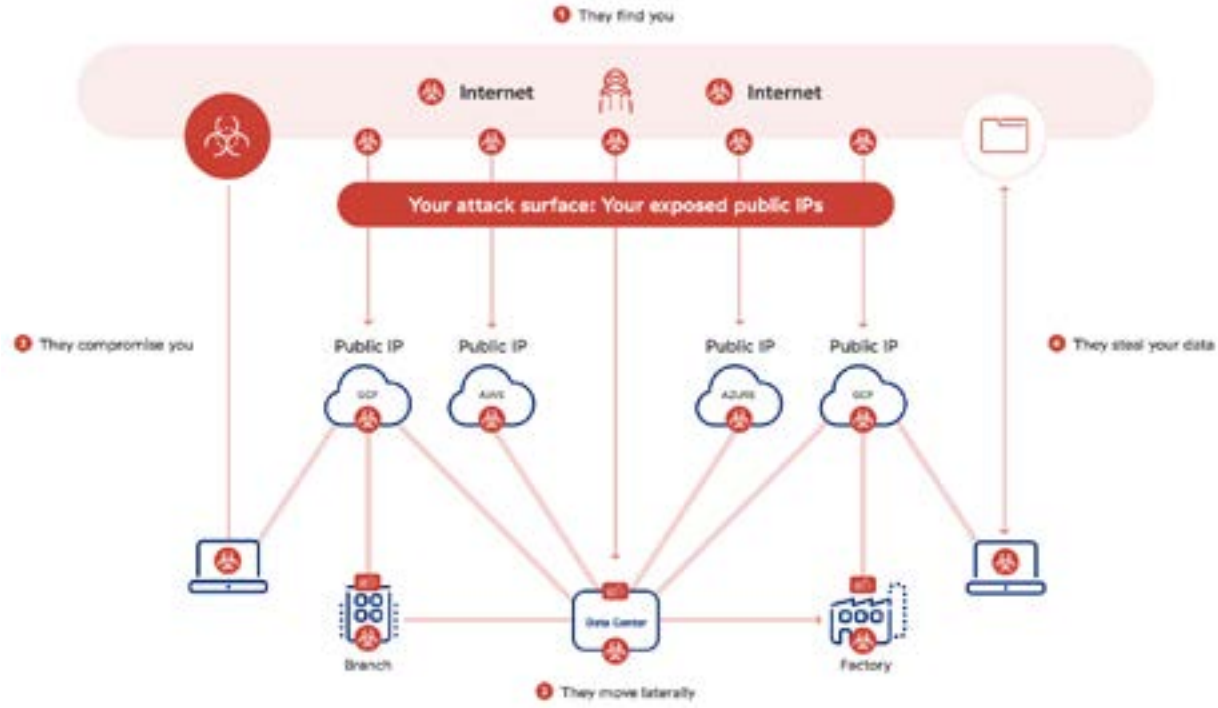
O cenário de ameaças e conformidade em evolução

Recentemente, houve um aumento nos alertas e avisos sobre ataques cibernéticos de criminosos patrocinados por governos contra infraestruturas críticas dos EUA. Em 7 de fevereiro de 2024, o Federal Bureau of Investigation (FBI) e a Cybersecurity and Infrastructure Security Agency (CISA), juntamente com a National Security Agency, emitiram um alerta consultivo para organizações governamentais sobre agentes cibernéticos prestes a interromper infraestruturas críticas, como sistemas de transporte, oleodutos e gasodutos, estações de tratamento de água e redes elétricas. Isso complementa ações semelhantes tomadas pela TSA para proteger aeroportos, operadores de aeronaves e ferrovias, a recente linha de base de segurança cibernética do DOE e a atualização quase final do NERC para o CIP-015-1.

As tecnologias de OT/IoT foram projetadas para oferecer velocidade e eficiência de transação em primeiro lugar, tendo a segurança como objetivo secundário. Infelizmente, a OT/IoT é agora um dos alvos favoritos dos cibercriminosos, com um aumento de 400% nos ataques ano a ano, de acordo com pesquisas da Zscaler ThreatLabz. O ransomware é a estratégia de ataque mais popular, e 61% de todas as violações tiveram como alvo organizações conectadas a OT.

Zscaler Zero Trust Networking

Um meio mais simples, seguro e econômico para usuários, dispositivos e cargas de trabalho se comunicarem



Como ocorrem os ataques de ransomware

A EPA, a CISA e o FBI recomendam fortemente que os operadores de sistemas trabalhem de encontro à ordem executiva do Gabinete do Presidente para usar zero trust como uma diretriz para uma melhor segurança cibernética. Os itens destacados são áreas-chave nestas recomendações onde a Zscaler pode ajudar imediatamente com nossa solução de segmentação de dispositivos zero trust:

- Reduzir a exposição à internet pública
- Reduzir a exposição a vulnerabilidades
- Segmentação de rede
- Coleta de logs
- Proibir a conexão de usuários não autorizados
- Nenhum serviço explorável na internet
- Limite de conexões de OT/IoT com a internet
- Detectar ameaças relevantes
- Realize um inventário de ativos de OT/IoT

Uma arquitetura mais segura para segmentação de dispositivos

A segmentação tem sido um elemento básico nas redes há muito tempo, com ferramentas como listas de controle de acesso (ACLs) e firewalls gerenciando o tráfego norte-sul (cliente para servidor). No entanto, a segmentação de OT muda o foco para o tráfego leste-oeste mais vulnerável, que flui lateralmente entre dispositivos e cargas de trabalho. Em VLANs compartilhadas, devido à arquitetura de comutação legada, os dispositivos podem ver e se comunicar com todos os outros, criando um ambiente propício para a propagação de malware. Infelizmente, as soluções baseadas em agentes desenvolvidas para cargas de trabalho na nuvem não conseguem segmentar as máquinas legadas e sem interface, tão comuns na OT, e as abordagens tradicionais baseadas em ACL continuam excessivamente complicadas.

Painel de segmentação de dispositivos zero trust

A Zscaler introduziu a rede zero trust como uma maneira mais simples, segura e econômica para usuários, dispositivos e cargas de trabalho se comunicarem. A segmentação de dispositivos é essencial para essa abordagem como etapa fundamental no estabelecimento de visibilidade e controle granulares para a rede moderna.

A Zscaler remove o atrito da segmentação dentro da VLAN com uma solução sem agentes que interrompe todas as ameaças laterais ao isolar cada terminal IP, incluindo sistemas legados e sem interface, em um "segmento de rede individual". Isso elimina a necessidade de ACLs complexas e não requer alterações na infraestrutura existente, proporcionando a segmentação mais granular e eficaz disponível.

Casos de uso

Alguns dos casos de uso mais comuns para segmentação de dispositivos sem agente incluem:

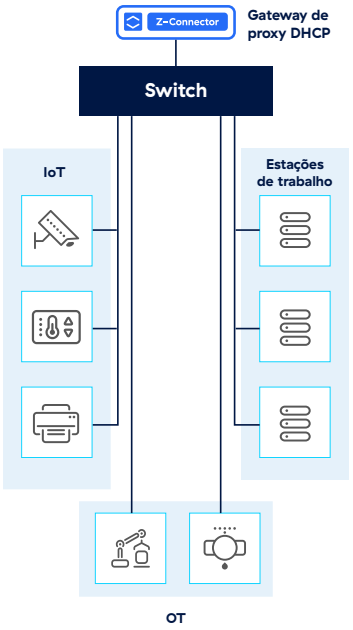
Segmentação interna da LAN Estenda o zero trust para a LAN aplicando a segmentação no tráfego leste–oeste. Isso reduz sua superfície de ataque interna e elimina a movimentação lateral de ameaças em redes críticas de OT/IoT, sem necessidade de segmentação baseada em NAC ou firewall.

Para aplicar a segmentação zero trust na sua rede, simplesmente:

- Provisione automaticamente cada dispositivo em um segmento individual (/32.)
- Agrupe automaticamente dispositivos, usuários e aplicativos analisando seus padrões de tráfego, evitando que dispositivos não autorizados usem falsificação de MAC para entrar na rede.
- Aplique dinamicamente políticas para tráfego leste–oeste com base na identidade e no contexto de usuários e dispositivos.

Segmentação de TI/OTA tecnologia de segmentação de dispositivo zero trust da Zscaler atua como um interruptor de ransomware, desativando a comunicação de dispositivos não essenciais para interromper a movimentação lateral de ameaças sem interromper as operações comerciais. Essa solução neutraliza ameaças avançadas, como ransomware em dispositivos de IoT, sistemas de OT e dispositivos incapazes de executar agentes.

- Agrupe e aplique políticas de forma autônoma para endereços MAC conhecidos em qualquer dispositivo (por exemplo, acesso RDP a câmeras negado, exceto para administradores)
- Isole automaticamente endereços MAC desconhecidos para limitar o raio de ação em caso de um dispositivo comprometido
- Integre-se com sistemas de gerenciamento de ativos para políticas de controle de acesso seguro



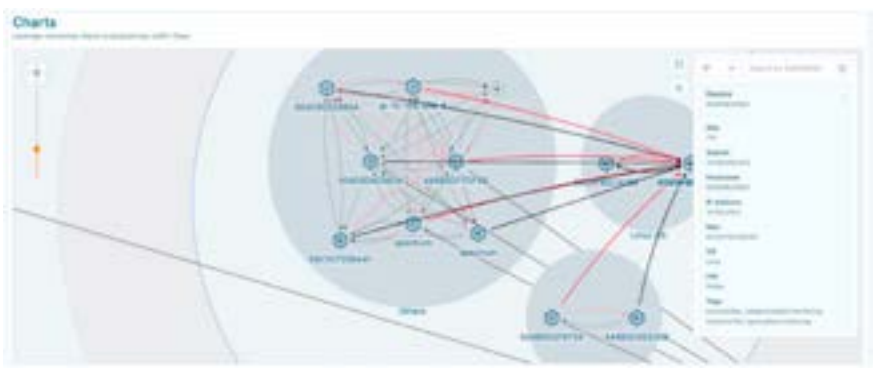
Segmentação automatizada de IoT/OT
Segmento de "um" para cada dispositivo

Descoberta e classificação automática de dispositivos

Como uma parcela significativa do tráfego de OT/IoT permanece dentro da rede local, é importante ter visibilidade contínua do tráfego leste-oeste. Com a descoberta e classificação automática de dispositivos, os administradores de rede podem gerenciar melhor o desempenho, o tempo de atividade e a segurança para sistemas de IoT/OT sem gerenciamento de estoque complexo.

Para visibilidade de rede e dispositivo:

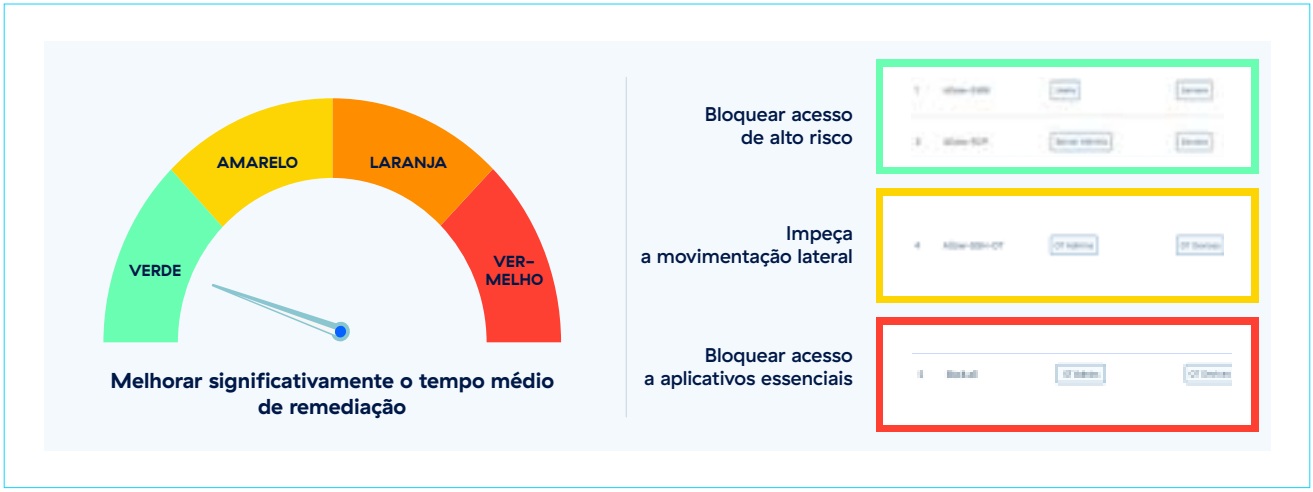
- Descubra, classifique e faça inventário dos dispositivos de OT/IoT sem a necessidade de agentes de terminais
- Obtenha uma base de referência de padrões de tráfego e comportamentos de dispositivos para determinar acessos autorizados e não autorizados
- Obtenha insights precisos da rede para gerenciamento de desempenho e mapeamento de ameaças



Painel de descoberta de dispositivos

Resposta automatizada a incidentes Apresentando o Zscaler Ransomware Kill Switch. Redução da superfície de ataque com um clique totalmente integrada à nossa solução de segmentação de dispositivos zero trust. Bloqueie protocolos e portas vulneráveis conhecidos e até mesmo desabilite instantaneamente o acesso a redes críticas, como hospitais inteiros ou andares de fábrica. Tudo com níveis de gravidade predefinidos para minimizar o tempo de inatividade dos negócios.

O Ransomware Kill Switch atua como um ponto de aplicação de políticas multicamadas, permitindo níveis diferenciados de resposta a incidentes a um comprometimento ativo e aumento do investimento em ferramentas de segurança existentes. Cada nível do Ransomware Kill Switch tem uma funcionalidade semelhante a “fusíveis virtuais” ou níveis Defcon, com rotas de escalonamento predefinidas para bloquear todas as comunicações de rede desnecessárias de ou para qualquer terminal, negando a propagação lateral e reduzindo drasticamente a superfície de ataque.



Essa solução desabilita instantaneamente a comunicação não essencial do dispositivo para interromper a movimentação lateral de ameaças sem interromper as operações comerciais. Essa solução neutraliza ameaças avançadas, como ransomware em dispositivos de IoT, sistemas de OT e dispositivos sem capacidade de agente.

A Zscaler oferece controle completo do Ransomware Kill Switch via APIs. Usando essas interfaces programáveis, as organizações de TI podem habilitar ferramentas de orquestração de segurança existentes, como gerenciamento de eventos e informações de segurança (SIEM), orquestração e resposta de segurança (SOAR) ou soluções de EDR/XDR para automatizar a resposta a incidentes e colocar imediatamente em quarentena terminais comprometidos e conter o raio de ação da infecção.

Isso fornece às organizações proteção de investimento para sua infraestrutura de rede e segurança existente, ao mesmo tempo em que melhora imediatamente a postura de segurança empresarial.

Benefícios

Contenção granular para limitar a propagação lateral

Resposta a incidentes pré-planejada e automatizada no caos de uma violação

Contenção rígida em camadas de limites importantes, como entre a TI corporativa e as redes principais

Desativação elegante de portas e protocolos suspeitos para maximizar o tempo de atividade dos negócios

Elimine a movimentação lateral de ameaças na LAN
Reduza a superfície de ataque isolando cada um em sua própria "rede individual", eliminando a superfície de ataque e o risco de propagação de ameaças. Mesmo dispositivos comprometidos não podem mais infectar seus vizinhos.

Reduza a complexidade operacional e o custo associado às ferramentas de segmentação legadas Segmente cada terminal IP sem a complexidade de tecnologias de rede antigas e centradas em IP, como NAC e firewalls leste-oeste, ou construções complexas como ACLs e segmentação manual de VLAN.

Obtenha maior visibilidade do tráfego leste-oeste Obtenha visibilidade lateral completa com descoberta e classificação automáticas de dispositivos. Os administradores de rede podem gerenciar melhor o desempenho, o tempo de atividade e a segurança de qualquer dispositivo, mesmo daqueles que não aceitam agentes.

Implante sem interromper a rede Tecnologia sem agentes que é implantada rapidamente sem interromper a maneira atual de fazer negócios dos clientes e não exige alteração da arquitetura de rede ou novo endereçamento IP dos dispositivos.

Conformidade mais rápida Os padrões cibernéticos federais em todos os setores agora chamam a segmentação como a base do zero trust. A abordagem sem agentes da Zscaler é implantada rapidamente e melhora instantaneamente a postura de conformidade.

Características

Isolamento com airgap

- Isolamento de dispositivo sem agentes
- Quarentena de dispositivo com um clique
- Detecção de violação de isolamento com airgap
- Filtragem baseada em endereço MAC

Segmentação zero trust

- Segmentação baseada em rede

Segmentação baseada em dispositivo

- Agrupamento e política autônomos
- Controle de política IntraVLAN e InterVLAN
- Política dinâmica baseada em tags
- Política baseada na identidade do dispositivo e do usuário
- Política baseada no horário
- Política baseada em zona
- Estrutura de política hierárquica

Descoberta e criação de perfil de ativos

- Descoberta de terminal e rede
- Identificação de dispositivo
- Categorização de dispositivos baseada em perfil
- ICS/Decodificação do protocolo médico

Alta disponibilidade

- Cluster de dois nós com VRRP
- VRRP com sincronização de sessão
- Configuração e sincronização de estado
- Agregação de links
- Monitoramento da vivacidade da interface
- Atualizações de software sem impacto
- Substituição de hardware em serviço

Serviços de roteamento e rede

- Roteamento dinâmico: BGP, OSPF
- Roteamento multicast: IGMP, PIM
- Servidor DHCP, Relay/Proxy
- Tronco de VLAN
- Tradução de endereços de rede
- Roteamento baseado em políticas
- Equal Cost Multi Path (ECMP)
- VPN site-to-site

Resposta a incidentes

- Ransomware Kill Switch

Visibilidade e registro

- Mapa de tráfego com correlação de políticas
- Data lake elástico integrado
- Logs de inicialização de sessão para todas as comunicações intra e intersegmentos
- Exportação de logs para SIEM/coletor de logs

Modelos de implantação flexíveis

- Provisionamento de gateway com airgap automático
- Modelos e perfis de sites
- Implantação autônoma de cluster de alta disponibilidade ou multicluster
- Gateways com airgap baseados em máquinas físicas ou virtuais

Monitoramento e solução de problemas

- Console de depuração remota
- CLI local em gateways com airgap
- Suporte SNMP

Gerenciamento centralizado baseado na nuvem

- Logon único (SSO) e MFA
- Trilhas de auditoria para eventos de login e alterações de configuração
- Controle de acesso baseado em função
- Plataforma na nuvem disponibilizada em multiusuário
- Acesso baseado em API

Integrações de terceiros

- Microsoft Active Directory
- Integração SIEM
- Fornecedores de EDR: Crowdstrike, SentinelOne
- Gestão de Ativos: Armis
- SSE: Zscaler ZIA

Dimensionamento do dispositivo de gateway da Zscaler

A seguir estão várias estimativas de dimensionamento para dispositivos de gateway da Zscaler de hardware ou virtualizados.

Especificações de hardware para implantações de gateway físico	XS	S1	S2	M	L	GG
Disponibilidade	Junho de 2024	Junho de 2024	Agora	Agora	Agora	1.º trimestre do ano fiscal de 2025
Modelo de hardware	ZT 400	ZT 600	Dell VEP4600	Dell VEP4600	Dell VEP4600	A ser determinado
CPU	4C Atom	8C Atom	4C Xeon	8C Xeon	16C Xeon	16C Xeon
Memória	16 GB	16 GB	16 GB	32 GB	64 GB	64 GB
Armazenamento	64 GB	64 GB	128 GB	256 GB	960 GB	256 GB
Portas	4x 1 GbE	4x 1 GbE	6x 1 GbE 2x 1 GbE (SFP)	4x 1 GbE 2x 10 GbE	4x 1 GbE 6x 10 GbE	4x 25 GbE
Formato	Desktop	Desktop	1U	1U	1U	1U
Outras características	Sem ventoinha		RPS	RPS	RPS	RPS
Taxa de transferência (HTTP de 64 KB)	4 Gbps	8 Gbps	10 Gbps	20 Gbps	40 Gbps	80 Gbps
Sessões	250 mil	500 mil	500 mil	1 milhão	2 milhão	2 milhão
N.º de terminais	200	500	1.000	2.000	4.000	A ser determinado

Guia de dimensionamento de dispositivos virtuais	XS	S1	S2	M
Disponibilidade	Agora	Agora	Agora	Agora
CPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU
Memória	8 GB	16 GB	32 GB	64 GB
Armazenamento	256 GB	256 GB	256 GB	256 GB
Portas	4x vNICs	4x vNICs	4x vNICs	4x vNICs
Taxa de transferência (HTTP de 64 KB)	5 Gbps	10 Gbps	20 Gbps	40 Gbps
Sessões	250 mil	500 mil	1 milhão	2 milhão
N.º de terminais	200	500	2.000	4.000

Fale com um especialista técnico

Quer saber mais sobre como a Zscaler pode ajudar a proteger sua organização de infraestrutura crítica? Agende um horário para falar com um de nossos especialistas técnicos.

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para proporcionar aos seus clientes mais agilidade, eficiência, resiliência e segurança. A Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados ao conectar com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers no mundo inteiro, a Zero Trust Exchange baseada em SASE é a maior plataforma de segurança integrada na nuvem do mundo. Saiba mais em **zscaler.com/br** ou siga-nos no Twitter **@zscaler**.

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