Zscaler Zero Trust Device Segmentation para OT/IoT

Impeça a movimentação lateral,
reduza a superfície de ataque
e melhore a segurança operacional

Resumo
da solução

O problema em questão

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 nas transações 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.

O que você pode fazer?

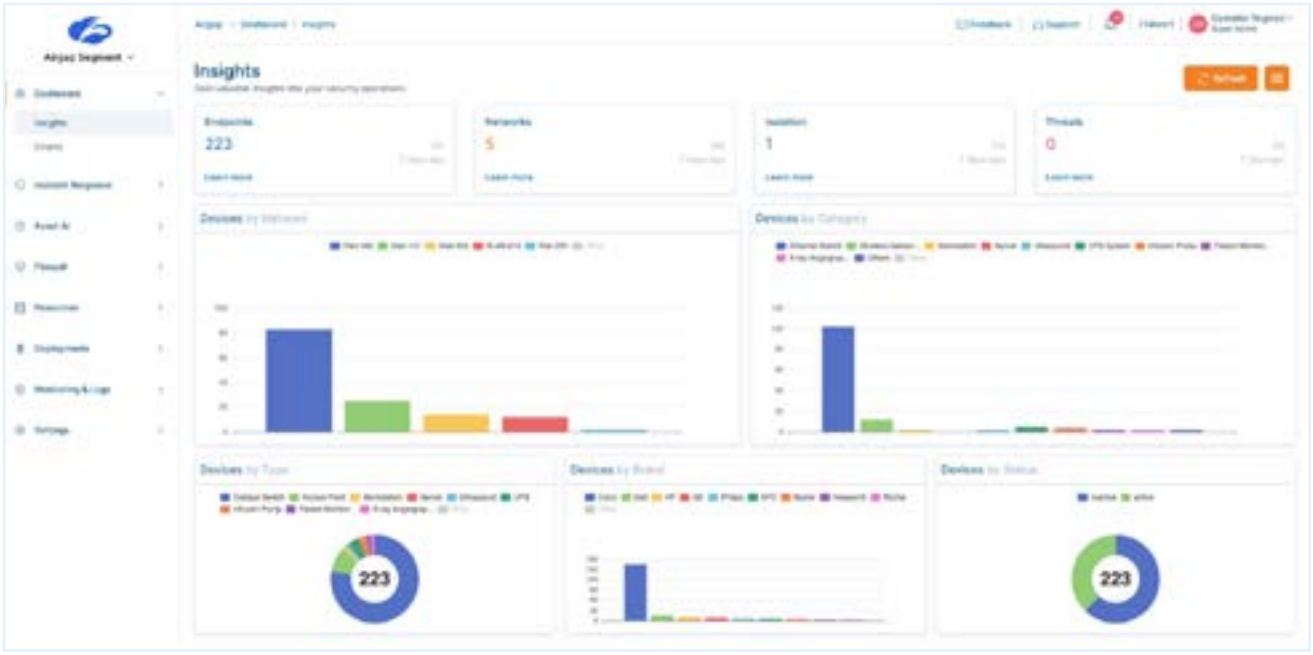
A EPA, a CISA e o FBI recomendam fortemente que os operadores de sistemas trabalhem de encontro à ordem executiva do Gabinete do Presidente para usar zero trust como uma diretriz para uma melhor segurança cibernética.

Os itens destacados são áreas-chave nessas 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
- Realizar um inventário de ativos de OT/IoT

Como fazer isso?

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 microssegmentação da 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 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 de um". Isso elimina a necessidade de ACLs complexas e não exige alterações na infraestrutura existente, ao mesmo tempo em que fornece a segmentação mais granular e eficaz disponível.

Casos de uso

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

Microssegmentação de LAN

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

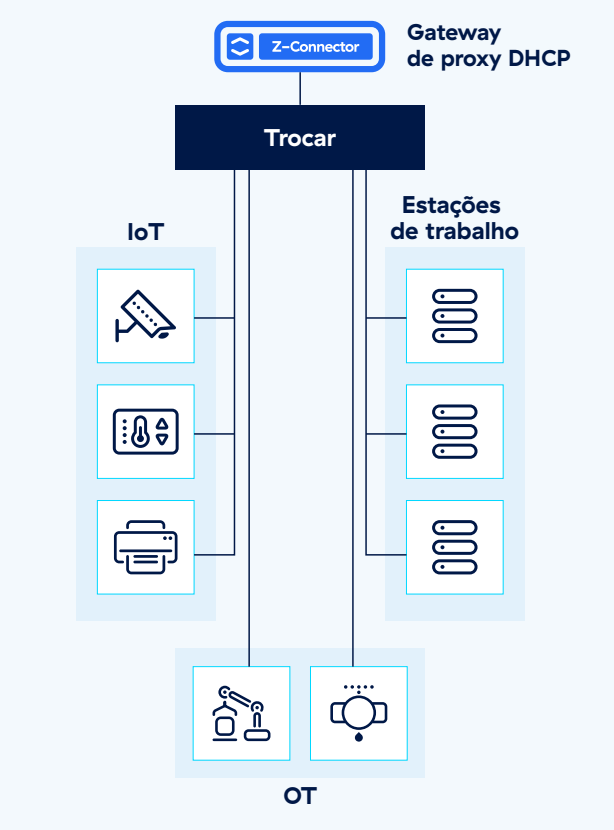
Para aplicar segmentação zero trust em sua rede:

- Provisione automaticamente cada dispositivo em um segmento de um (/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 IoT/OT

A tecnologia Zscaler Zero Trust Device Segmentaiton atua como um kill switch contra ransomware, desabilitando a comunicação não essencial de dispositivos para impedir 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.

- 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



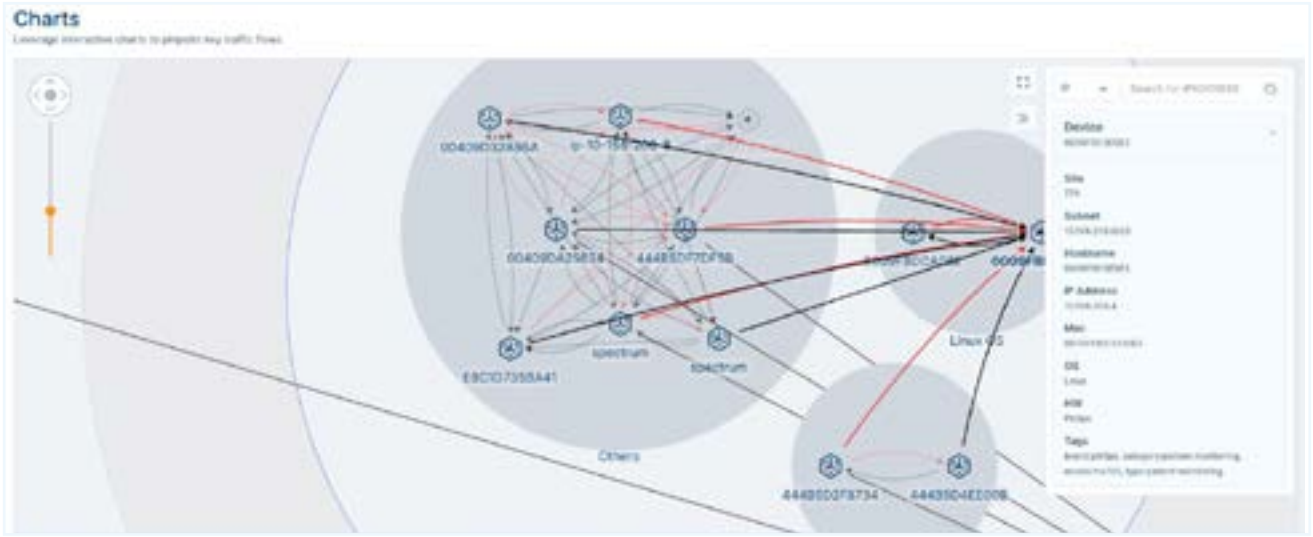
Segmentação automatizada de IoT/OT Segmento de "um" para cada dispositivo

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:

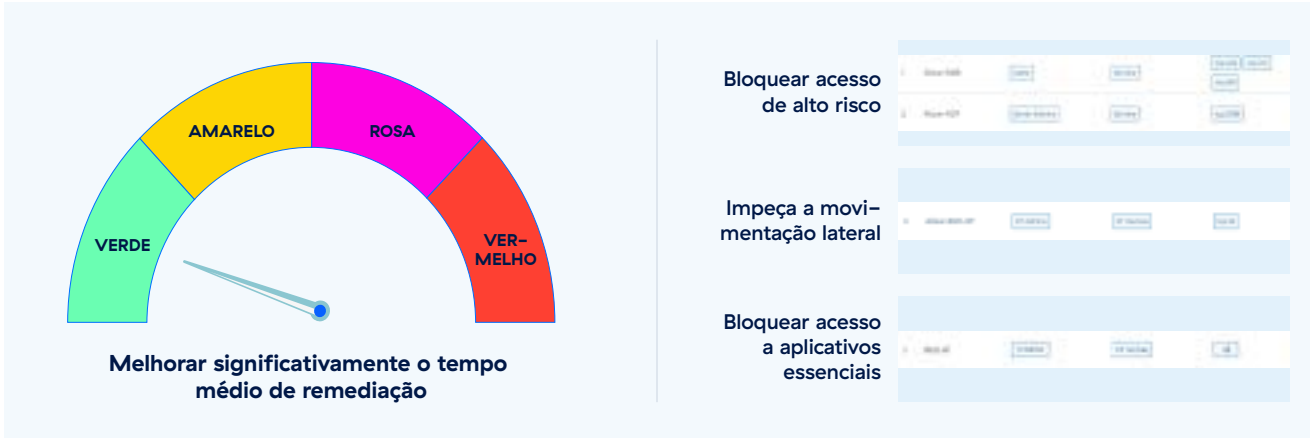
- Descubra, classifique e faça inventário dos dispositivos de OT/IoT sem a necessidade de agentes de terminais
- Obtenha uma base de referência de padrões de tráfego e comportamentos de dispositivos para determinar acessos autorizados e não autorizados
- Obtenha insights precisos da rede para gerenciamento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



Painel de descoberta de dispositivos

Resposta automatizada a incidentes

O Zscaler Ransomware Kill Switch oferece redução de superfície de ataque selecionável pelo usuário. Basta escolher um nível de gravidade predefinido para bloquear progressivamente protocolos e portas vulneráveis conhecidos e até mesmo desabilitar instantaneamente o acesso a redes inteiras, como linhas de manufatura e pisos hospitalares. Sem suposições no caos de uma violação: basta ajustar o mostrador para corresponder à ameaça e, ao mesmo tempo, manter a atividade dos negócios.



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 que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A solução Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SSE é a maior plataforma integrada de segurança 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