

# Segurança Zero Trust para Infraestrutura Crítica

## Abordagem a vulnerabilidades de cibersegurança em sistemas de água potável e de distribuição elétrica

© 2024 Zscaler, Inc. Todos os direitos reservados.

Resumo da solução

## O problema em questão

Recentemente, houve um aumento nos alertas e avisos sobre ciberataques de criminosos patrocinados por governos em infraestruturas críticas dos EUA. Em 7 de fevereiro de 2024, o Federal Bureau of Investigation (FBI) e a Cybersecurity and Infrastructure Security Agency (CISA), em conjunto com a National Security Agency (NSA), emitiram um alerta aos órgãos governamentais sobre agentes cibernéticos prontos para interromper infraestruturas críticas, como estações de tratamento de água, redes elétricas, oleodutos, gasodutos e sistemas de transporte.

As tecnologias de OT/IoT foram projetadas para oferecer velocidade e eficiência nas transações em primeiro lugar, tendo a segurança como objetivo secundário. Infelizmente, sistemas de OT/IoT agora são 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 tecnologia operacional (OT). Por meio de auditorias abrangentes realizadas pela EPA, foi descoberto que mais de 70% dos sistemas inspecionados desde setembro de 2023 violam os requisitos básicos do SDWA 1433, incluindo seções específicas ausentes do RRA e do ERP.

## O que você pode fazer?

A EPA, a CISA e o FBI recomendam fortemente que os operadores de sistemas tomem as medidas descritas em Top Actions for Securing Water Systemas (principais ações para proteger sistemas de água). Além disso, o DOE divulgou a base de referência de cibersegurança e o NERC quase finalizou a atualização do CIP-015-1. Ambas as diretrizes sugerem trabalhar em direção à ordem executiva do gabinete do presidente para usar zero trust como uma diretriz para uma melhor cibersegurança.

Os itens destacados são as principais áreas em que a Zscaler pode ajudar você rapidamente com nossa solução de segmentação de dispositivos zero trust.

- Reduzir a exposição à internet pública
- Desenvolva e implemente planos de resposta e recuperação de incidentes de cibersegurança
- Reduzir a exposição a vulnerabilidades
- Backup de sistemas de OT/TI
- Realize treinamento de conscientização sobre cibersegurança
- 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 avaliações frequentes de cibersegurança
- Alterar as senhas padrão imediatamente
- Realize um inventário de ativos de OT/IoT

## Como fazer isso?

Com a Zscaler, ampliamos ainda mais a segmentação zero trust para fornecer visibilidade e segmentação para tráfego leste-oeste em LANs, incluindo ambientes de OT críticos. Isso pode ser feito de várias maneiras:

### Substituição do firewall leste-oeste

Estenda a proteção zero trust para a LAN aplicando segmentação no tráfego leste-oeste. Isso reduz as superfícies de ataque internas e elimina a ameaça de movimentação lateral em redes de OT/IoT. Não há necessidade de segmentação baseada em NAC ou firewall.

© 2024 Zscaler, Inc. Todos os direitos reservados.

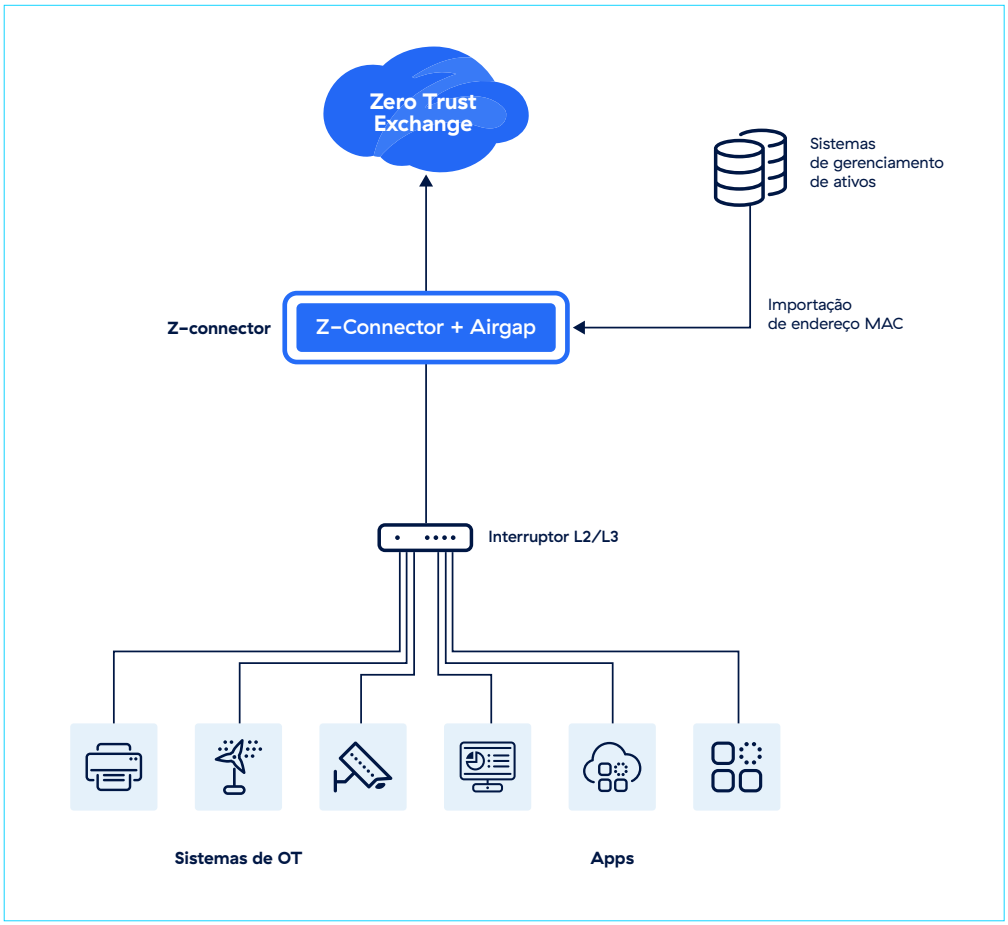
Para aplicar segmentação zero trust em sua rede:

- 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 de segmentação de dispositivos zero trust da Zscaler atua como um kill switch contra ransomware, desabilitando comunicações não essenciais 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 via RDP às câmeras negado, exceto para administradores
- Isole automaticamente endereços MAC desconhecidos para limitar o raio de ação em caso de um dispositivo comprometido
- Integração com sistemas de gerenciamento de ativos para políticas de controle de acesso seguro



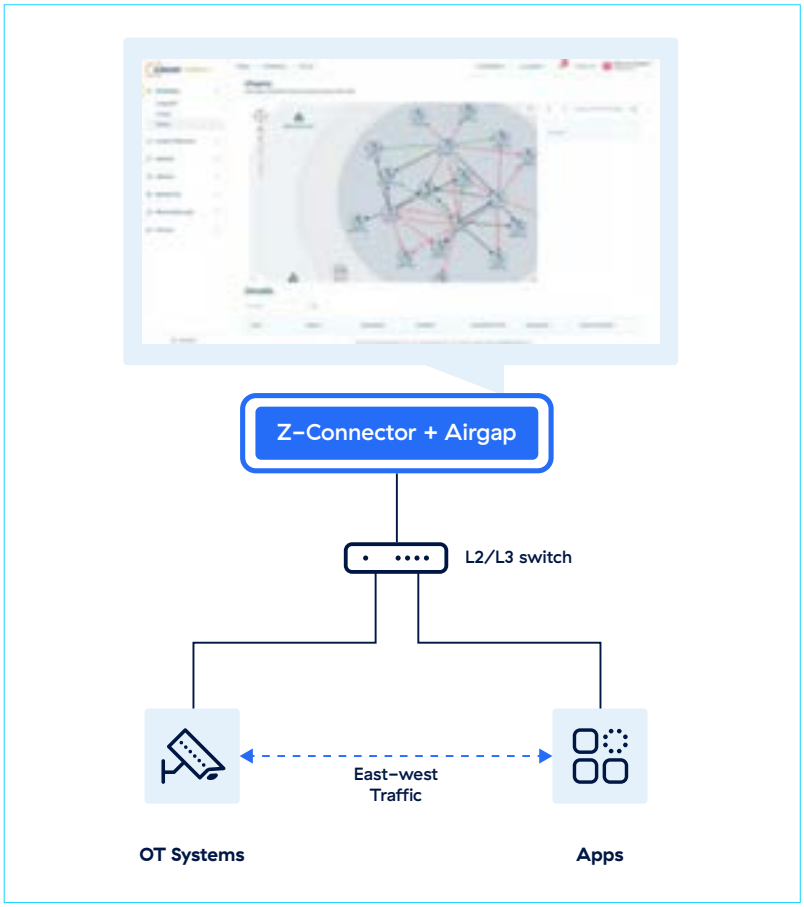

© 2024 Zscaler, Inc. Todos os direitos reservados.

## Descoberta e classificação automática de dispositivos

Uma parcela significativa do tráfego de IT/OT permanece dentro da rede de água ou elétrica, por isso 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 dos padrões de tráfego e comportamentos de dispositivos para determinar acessos autorizados e não autorizados
- Obtenha insights de rede baseados em IA para dar suporte ao gerenciamento de desempenho e ao mapeamento de ameaças




### 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 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**.

©2024 Zscaler, Inc. Todos os direitos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ e outras marcas registradas listadas em **zscaler.com/br/legal/trademarks** são (i) marcas registradas ou marcas de serviço ou (ii) marcas comerciais ou marcas de serviço da Zscaler, Inc. nos Estados Unidos e/ou em outros países. Quaisquer outras marcas registradas são de propriedade de seus respectivos detentores.

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