Zscaler para manufatura

Implemente zero trust no modelo Purdue

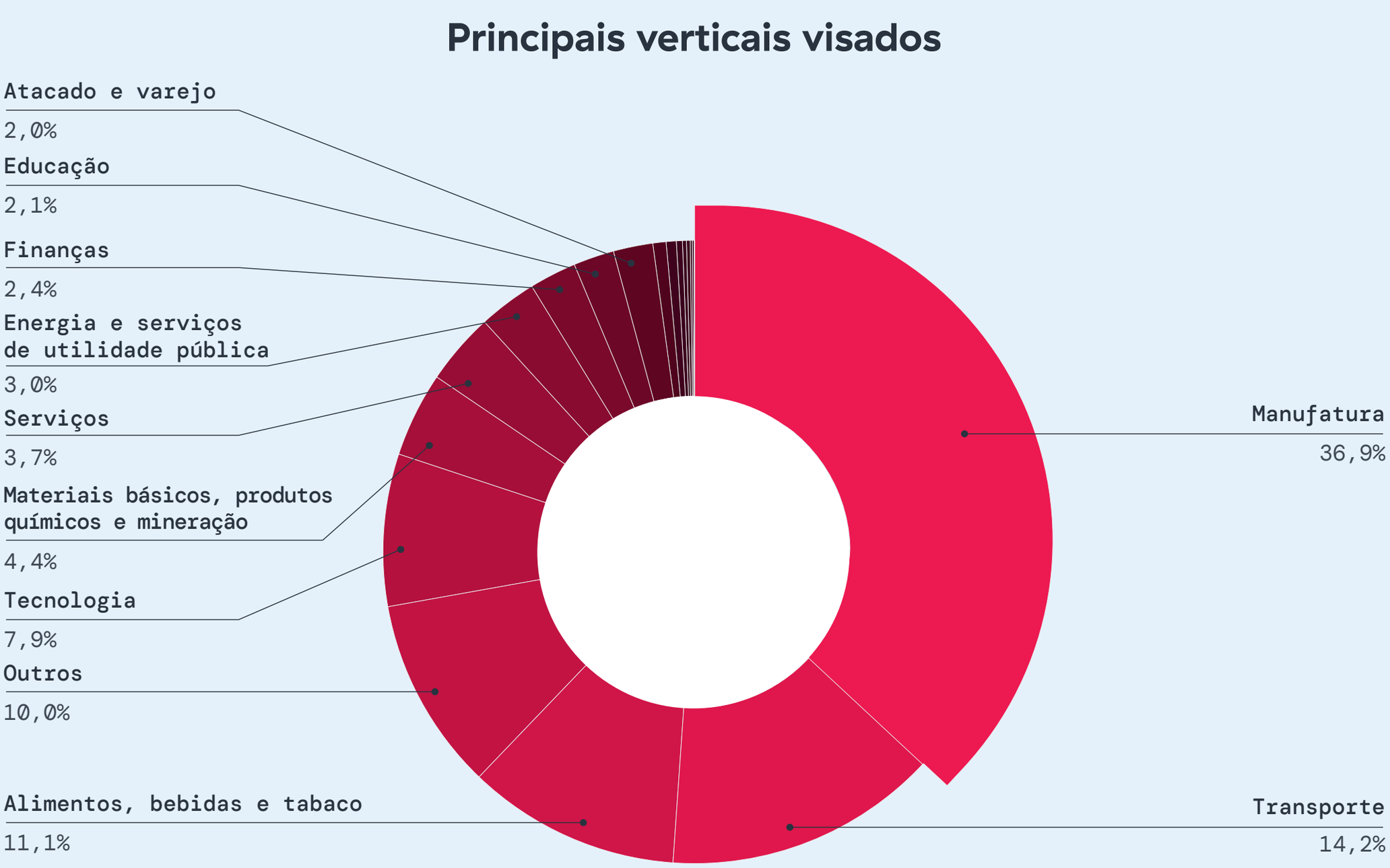
RESUMO DA SOLUÇÃO

As fábricas precisam de uma nova abordagem para proteger sistemas de OT

Organizações globais do setor manufatureiro têm se empenhado em aprimorar suas linhas de produção, adicionando robôs inteligentes, sensores de IoT em todas as máquinas, análises baseadas na nuvem e um gêmeo digital de toda a fábrica. O objetivo é simples: maior produção, menor tempo de inatividade e manutenção preditiva que ofereçam produção ininterrupta.

Mas muitas organizações reconheceram uma realidade diferente. Cada nova conexão expande a superfície de ataque da tecnologia operacional. E, uma vez que os atacantes conseguem entrar, o risco de impacto é muito maior devido a sistemas operacionais desatualizados, redes planas e visibilidade limitada da OT. Para dar continuidade à transformação das fábricas, é necessário que elas repensem sua arquitetura de segurança.

No relatório mais recente da Zscaler Threatlabz sobre IoT/OT, o setor de manufatura foi o mais afetado, representando 36% dos bloqueios de malware de IoT.

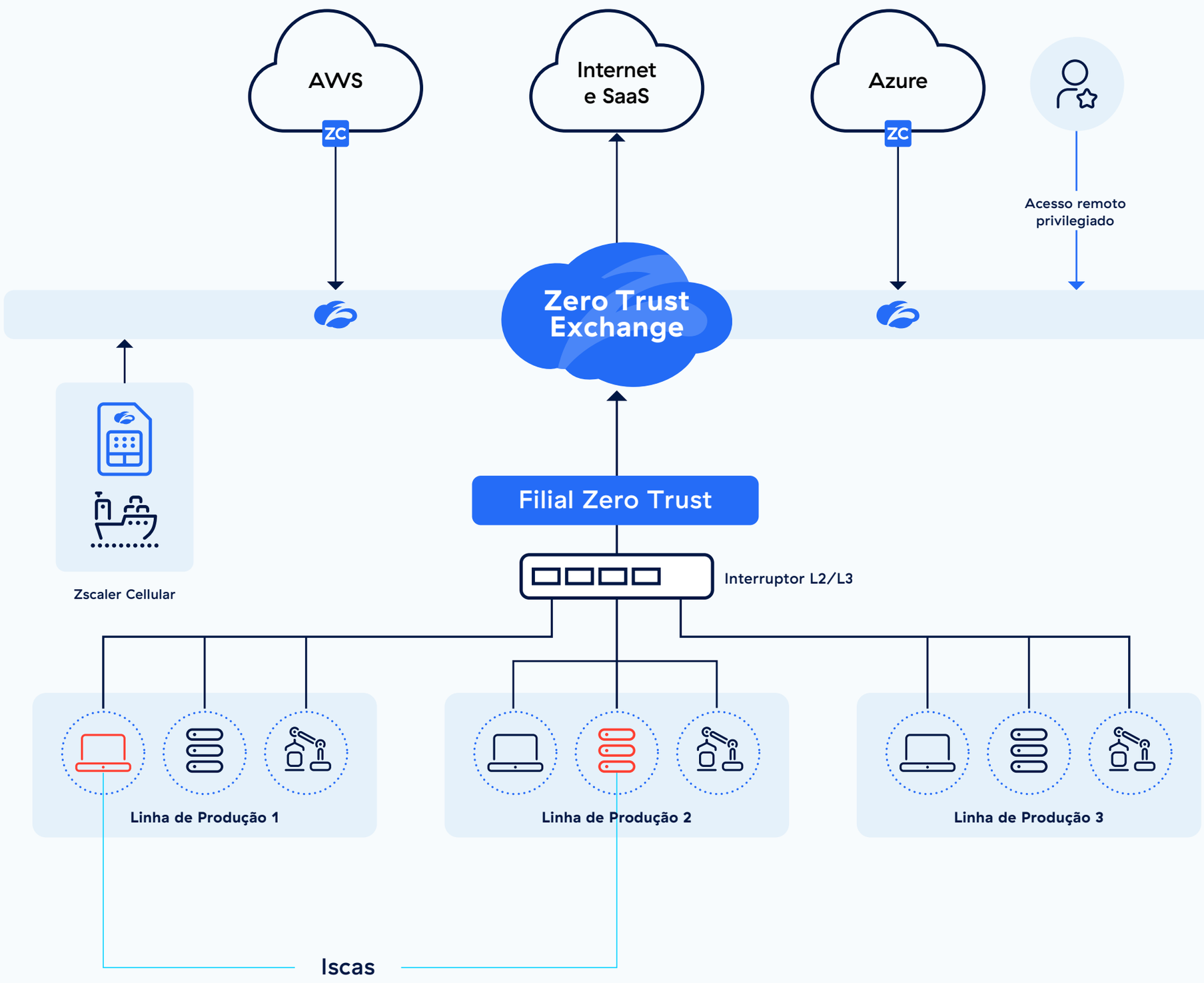


Distribuição das indústrias mais visadas

Estenda o zero trust a todos os usuários e dispositivos, dentro e fora de suas fábricas

Para proteger ambientes industriais e de manufatura, as equipes de segurança precisam garantir que cada interação entre usuários e dispositivos seja inspecionada e que as políticas de privilégio mínimo sejam aplicadas. Nossa abordagem zero trust foi desenvolvida especificamente para OT, oferecendo acesso seguro, segmentação e conectividade em todas as operações da sua fábrica.

- Permita que técnicos e terceiros acessem sistemas de OT críticos sem VPNs
- Aplique segmentação granular leste–oeste para evitar a movimentação lateral de ameaças
- Conecte com segurança os sistemas de OT à nuvem e ao data center para análise
- Estenda o zero trust para sistemas de OT móveis como caminhões, quiosques e scanners de POS
- Detecte invasores precocemente e evite que eles aumentem seus privilégios



Arquitetura zero trust de fábrica

Componentes da solução da Zscaler

Acesso remoto privilegiado

Permita que terceiros e técnicos remotos se conectem com segurança a destinos de RDP/SSH/VNC por meio de qualquer navegador, sem agentes.

PRINCIPAIS RECURSOS

Controles de área de transferência Limite recursos de área de transferência com base em políticas zero trust para proteger dados sigilosos.	**Controles de auditoria e governança** Reduza o risco de terceiros com gravação de sessões, compartilhamento de sessões e acesso controlado.
Cofre de credenciais e mapeamento Armazene credenciais para sistemas de destino em um cofre na nuvem e compartilhe o acesso por meio de políticas de mapeamento.	**Acesso com prazos definidos e sob demanda** Defina janelas de manutenção e forneça acesso just-in-time para manutenções emergenciais.

Segmentação zero trust

Microssegmente os sistemas de OT e aplique políticas para garantir apenas comunicações autorizadas entre seus sistemas de OT e outros sistemas de OT/TI

Microssegmentação granular Isole sistemas de OT compatíveis em um segmento individual (usando /32).	**Detecção e classificação de dispositivos** Descubra e classifique dispositivos de OT automaticamente.
Kill Switch contra ransomware Automatize a resposta a incidentes usando políticas predefinidas para bloquear progressivamente os sistemas de OT.	**Aplicação de políticas** Agrupe dispositivos automaticamente e aplique políticas para tráfego leste-oeste com base no tipo de dispositivo e em tags.

Proteja o acesso de OT

Permita que câmeras, sensores, monitores, quiosques e outros sistemas de tecnologia operacional se conectem com segurança a aplicativos na nuvem e à internet.
Impeça a comunicação com aplicativos e URLs de risco ou maliciosos.

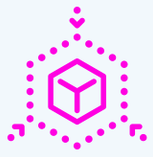
Provisionamento sem intervenção humana Aproveite a implantação totalmente automatizada e sem intervenção humana com modelos predefinidos.	**Políticas de zero trust unificadas** Inspecione e aplique políticas de IoT/OT para aplicativos privados e a internet.
Aplicação granular de políticas Aplique políticas com base na geolocalização de usuários/dispositivos, URLs acessados, dados sigilosos, etc.	**Zero trust móvel** Use zero trust para conectar facilmente dispositivos como caminhões, quiosques, plataformas de perfuração, etc.

Zscaler Deception

Use iscas para detectar ameaças de OT que contornaram as defesas existentes.
Identifique usuários comprometidos, impeça a movimentação lateral e defenda-se contra ransomware e agentes internos mal-intencionados.

Detecção de movimentação lateral Implante PLCs e sistemas SCADA falsos para detectar atacantes que tentam se mover lateralmente.	**Deteção pré-violação** Receba alertas precisos quando invasores estiverem examinando seu ambiente antes de um ataque.
Implantação nativa da nuvem Integra-se ao Zscaler Private Access (ZPA) para criar, hospedar e distribuir iscas.	**Sem configuração de rede** Diga adeus ao entroncamento de VLAN, portas SPAN e túneis GRE para rotear tráfego para redes de isca.

Diferenciais da Zscaler



ELIMINE AS BRECHAS DE SEGURANÇA

Aplique políticas de zero trust consistentes em todos os ambientes, dentro e fora de suas fábricas.

REDUÇÃO DO TEMPO DE INATIVIDADE

Aplique segmentação zero trust com o mínimo de interferência no seu ambiente de OT existente, reduzindo o risco de tempo de inatividade devido à movimentação lateral.

REDUZA O CUSTO E A COMPLEXIDADE

Reduza ou consolide firewalls, NAC, VPNs, VDIs e ferramentas de microssegmentação com uma arquitetura de segurança simplificada, baseada no modelo Purdue, dentro de suas fábricas.

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**.

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

zscaler™

Zero Trust Everywhere