CISCO
SECURE

Relatório de pesquisa de segurança

As empresas industriais ainda não têm visibilidade e preparo para se defender contra ataques cibernéticos de OT/ICS

Índice

Resumo executivo	3
Por que a visibilidade é a base da segurança industrial?	4
Status atual e metas	5
Desafios	8
Dentro de banda ou fora de banda: qual é a melhor opção para a sua empresa?	11
Conclusão	12
Metodologia	12

Resumo executivo

As empresas industriais estão preparadas para defender os ambientes de Tecnologia Operacional (OT) e Sistema de Controle Industrial (ICS) em caso de ataque cibernético?

Foi isso que a Cisco se propôs a responder em uma pesquisa do Q3 2022 (terceiro trimestre de 2022), juntamente com a Gartner Peer Insights and Takepoint Research, envolvendo 100 profissionais de TI, OT, engenharia e InfoSec em todo o mundo.

O que descobrimos foi surpreendente: 77% das empresas industriais ainda estão nos estágios iniciais da jornada de segurança de OT. E nenhum dos entrevistados ainda protegeu totalmente os ambientes de OT/ICS.

Isso é preocupante, considerando o mundo pós-pandemia em que nos encontramos hoje.

Muita coisa mudou nos últimos três anos. A pandemia acelerou significativamente a transformação digital da OT, o que levou a maioria das operações essenciais de uma empresa a serem integradas às tecnologias digitais. Por sua vez, os ataques cibernéticos, como os sofridos pelo Pipeline Colonial e pelo JBS em 2021, se tornaram mais comuns à medida que os agentes mal-intencionados detectavam as vulnerabilidades das redes de OT/ICS.

Atrás de portas fechadas, a pressão está aumentando na sala de reuniões, com preocupações com a continuidade dos negócios e diretrizes de segurança, como o Shields Up da CISA, sem dúvida contribuindo com isso. Nossas conversas com executivos de alto escalão revelam que a maioria das empresas reconhece que não está preparada para um ataque cibernético e que muitas estão apenas começando a priorizar a segurança de OT.

Olhando para o futuro, vemos a tempestade de segurança de OT perfeita vindo em nossa direção. Espera-se que a maioria das empresas industriais tenha funções de segurança convergentes em ambientes de TI e OT nos próximos três anos, o que expandirá consideravelmente as superfícies de ataque. E os ataques a ambientes de OT/ICS continuarão a se intensificar a ponto de causar danos ou perda de vidas, provavelmente na próxima década.

As empresas industriais devem acelerar seus esforços de segurança de OT agora para proteger a continuidade dos negócios.

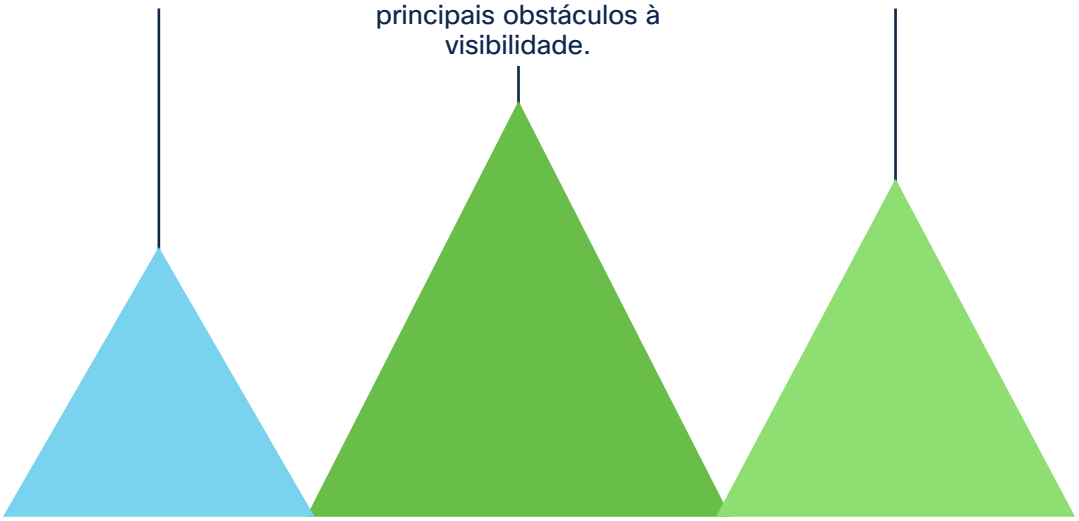
Principais descobertas

Nossa pesquisa revelou que a visibilidade abrangente dos dispositivos de OT e redes industriais é o principal objetivo – e o desafio – para proteger as operações industriais. Embora isso não seja uma surpresa, considerando o estágio em que a maioria das empresas se encontra nas jornadas de segurança cibernética de OT, é interessante observar as abordagens e os desafios para atingir esse objetivo.

58%
dos entrevistados dizem que ganhar visibilidade é o principal objetivo para proteger as operações industriais.

74%
dos entrevistados afirmam que o custo e a complexidade de criar uma rede SPAN fora de banda ou implantar TAPs de rede são os principais obstáculos à visibilidade.

65%
dos entrevistados pretendem obter visibilidade ao obter o inventário de recursos das equipes de engenharia de OT.



Por que a visibilidade é a base da segurança industrial?

Para entender o que é necessário para proteger ambientes de OT/ICS em um ambiente digital em constante mudança, basta olhar para a evolução da segurança de TI nos últimos 20 anos.

Antes, os esforços de segurança se concentravam no perímetro e nos sistemas confidenciais. A visibilidade da rede interna foi considerada sem importância porque se presumiu que qualquer pessoa com acesso era um agente legítimo. Tudo isso mudou com ataques de phishing e dia zero.

Agora, com abordagens de zero-trust e defesa em profundidade, o foco mudou para a manutenção de visibilidade total e segmentação de rede para limitar os efeitos de uma violação. Vemos isso na proliferação de sistemas de detecção e resposta de rede (NDR) e centros de operações de segurança (SOCs) ininterruptos.

A prevenção ainda é uma grande parte da segurança, assim como a contenção e a correção rápidas.

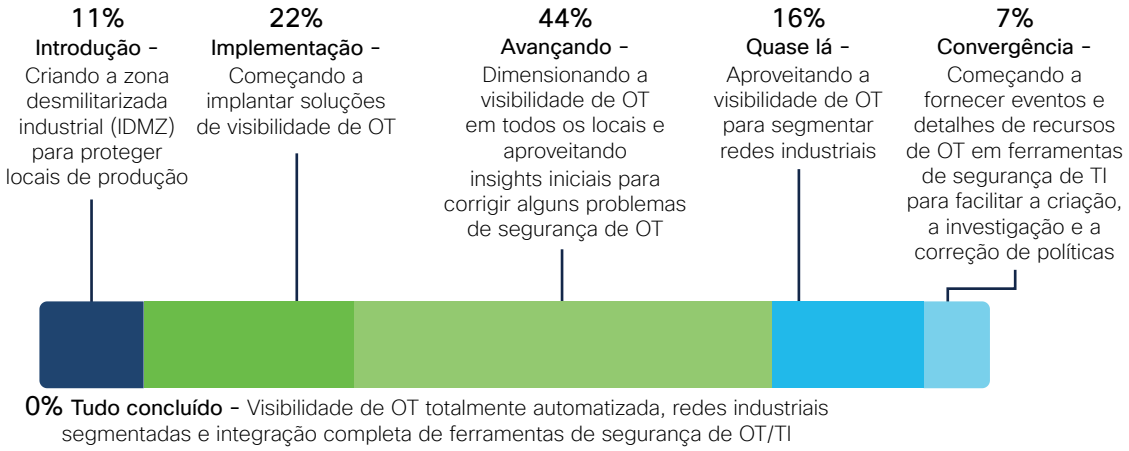
Quando se trata de proteger os ambientes de OT/ICS, muitas empresas seguiram o mesmo manual – bloquear a rede e isolar os sistemas essenciais – mas, como vimos, isso não vai funcionar por muito tempo.

As empresas simplesmente precisam estabelecer visibilidade total das redes de TI e OT antes que medidas corretivas ou preventivas possam ser tomadas.

Status atual e metas

A maioria das empresas está apenas começando a jornada de segurança de OT

Em qual estágio da jornada de segurança de Tecnologia Operacional (OT) você está agora?



Embora nenhuma empresa pesquisada ainda tenha atingido a maturidade de segurança de OT, a boa notícia é que os dados refletem um nível de autoconsciência e urgência em melhorar a situação.

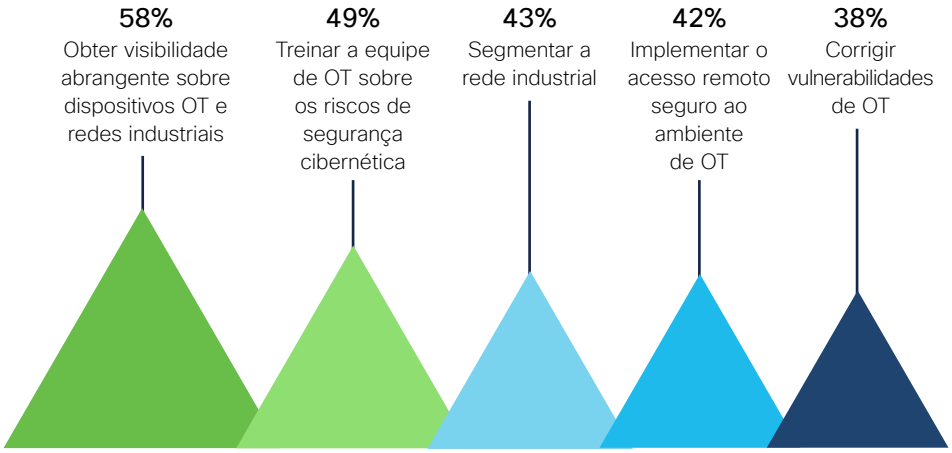
11% dos entrevistados começaram as jornadas com zonas desmilitarizadas industriais (IDMZ) para proteger locais de produção, 22% começaram a implementar soluções de visibilidade de OT e 44% estão dimensionando a visibilidade de OT em todos os locais e aproveitando os insights iniciais para corrigir alguns problemas de segurança de OT.

No entanto, apenas 23% dos entrevistados dimensionaram as implantações de visibilidade de OT e menos ainda estão aproveitando essas ferramentas em uma estratégia de segurança avançada: 16% segmentaram as redes industriais e apenas 7% começaram a fornecer eventos e detalhes de recursos de OT em ferramentas de segurança de TI para facilitar a criação, investigação e correção de políticas.

No geral, descobrimos que os líderes de segurança estão vendo os benefícios das soluções de visibilidade de OT e as veem como uma tecnologia madura a ser implantada em escala.

Visibilidade, treinamento e segmentação são as principais prioridades

Quais são seus principais objetivos para proteger as operações industriais nos próximos 12–24 meses?



Apresentar os manuais de resposta e correção de OT/TI **27%**,
Integrar os alertas de OT ao centro de operações de segurança (SOC) **25%**,
Implementar a detecção de invasão (IDS) na rede industrial **21%**,
Criar equipes funcionais de domínio cruzado (OT/TI) **6%**, Outro **0%**

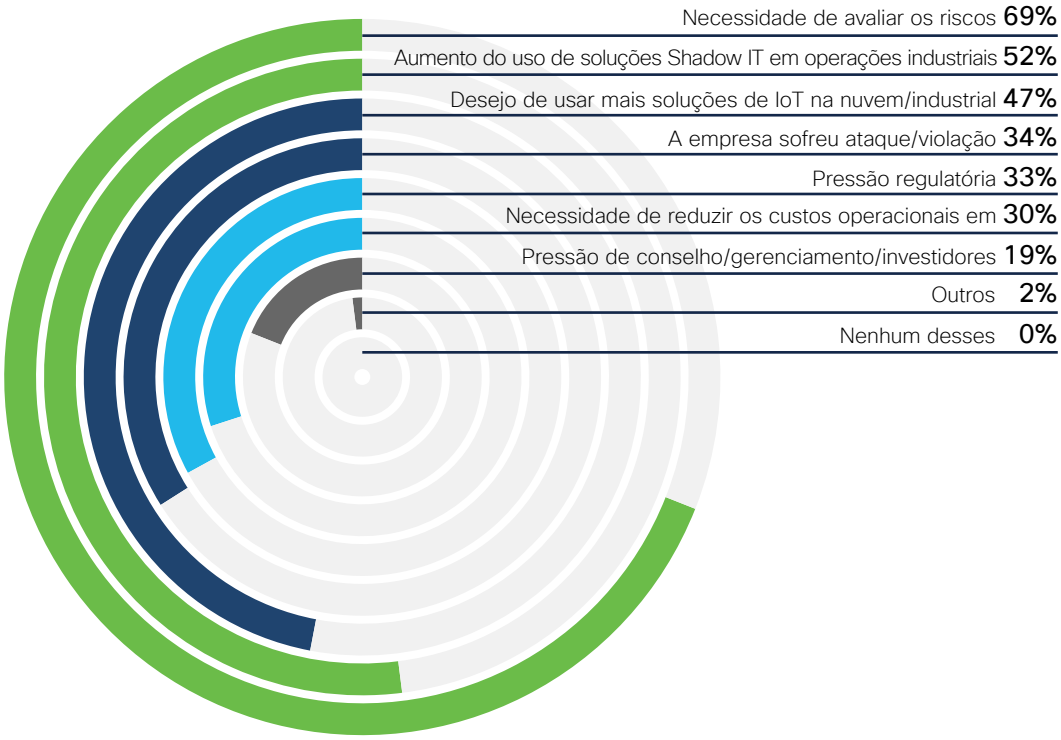
Quando se trata de metas, 58% dos entrevistados declaram que pretendem obter visibilidade abrangente da rede industrial em 24 meses e 49% indicaram que estão priorizando o treinamento de segurança cibernética, enquanto 43% pretendem segmentar a rede industrial.

Na segmentação, é importante observar que, embora os ambientes de OT tenham se tornado mais conectados ao longo do tempo, eles não foram otimizados para segurança. IDMZs, firewalls e gateways unidirecionais são medidas de segurança abrangentes que podem proteger o perímetro, mas não protegem o ambiente de OT contra invasores.

Muitas redes de OT ainda são simples e não segmentadas, e não é incomum que as empresas não tenham uma contabilização completa de toda a rede.

O gerenciamento de riscos e a Shadow IT estão gerando a necessidade de visibilidade

Quais são os principais fatores que impulsionam a necessidade de visibilidade da rede industrial e segurança cibernética na empresa?



É interessante observar que os dois principais impulsionadores para visibilidade de rede são a necessidade de avaliar os riscos (69%) e o aumento do uso de soluções de TI invisíveis em operações industriais (52%).

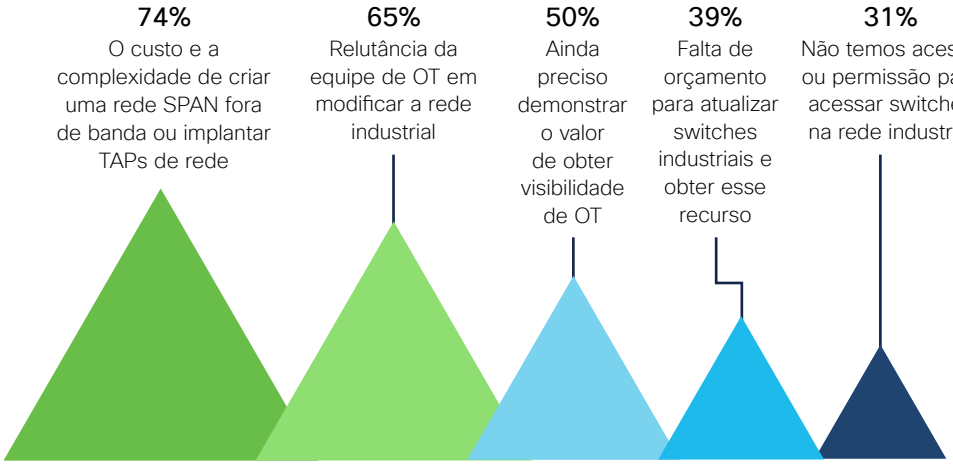
Isso reflete o fato de que os problemas de segurança de OT geralmente são muito mais sérios do que as empresas percebem e que, de forma anedótica, os líderes de segurança sabem que as empresas são vulneráveis. Por exemplo, não é incomum encontrar várias portas abertas ou sistemas operacionais implantados com credenciais padrão ou OEMs avaliando máquinas sem supervisão.

Essas vulnerabilidades podem ser expostas e abordadas apenas com visibilidade abrangente dos recursos conectados e das atividades de rede.

Desafios

As soluções convencionais são caras e complexas

Quais são os principais obstáculos para obter visibilidade abrangente em dispositivos OT e redes industriais?



Nenhum desses **2%**, outro **1%**

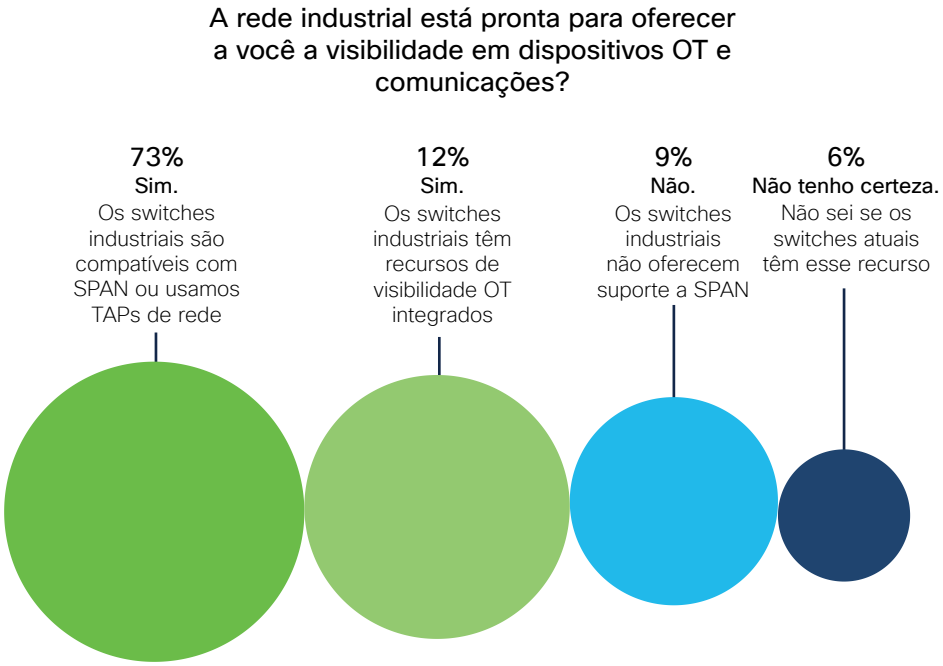
74% dos entrevistados dizem que o custo e a complexidade de criar uma rede de analisador de porta de switch (SPAN) para capturar e monitorar o tráfego de rede industrial é o principal bloqueador de visibilidade. Isso não é surpresa, considerando que isso envolveria a criação de uma rede de espelho, que simplesmente não é escalável.

65% dizem que as equipes de OT estão relutantes em modificar a rede. Novamente, isso não é surpresa, considerando a prioridade da OT em manter as luzes acesas. Com isso, 50% afirmam que é um desafio demonstrar o valor de obter visibilidade de OT.

Seguindo em frente, 39% dos entrevistados dizem que não têm orçamento para atualizar switches industriais, o que confirma ainda mais o fato de que o custo é a principal restrição. E 31% informam que não têm permissão para acessar switches na rede industrial.

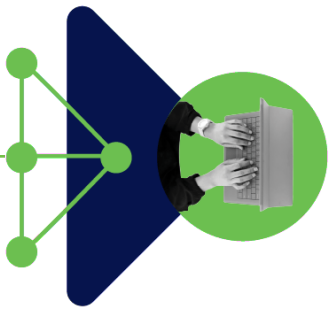
Em nossa experiência, a empresa só aumentará os investimentos em atualizações de rede quando a TI criar confiança com a OT e puder demonstrar o valor da visibilidade na melhoria da confiabilidade operacional. Até lá, a TI precisa contornar essas restrições.

A escalabilidade continua sendo um desafio

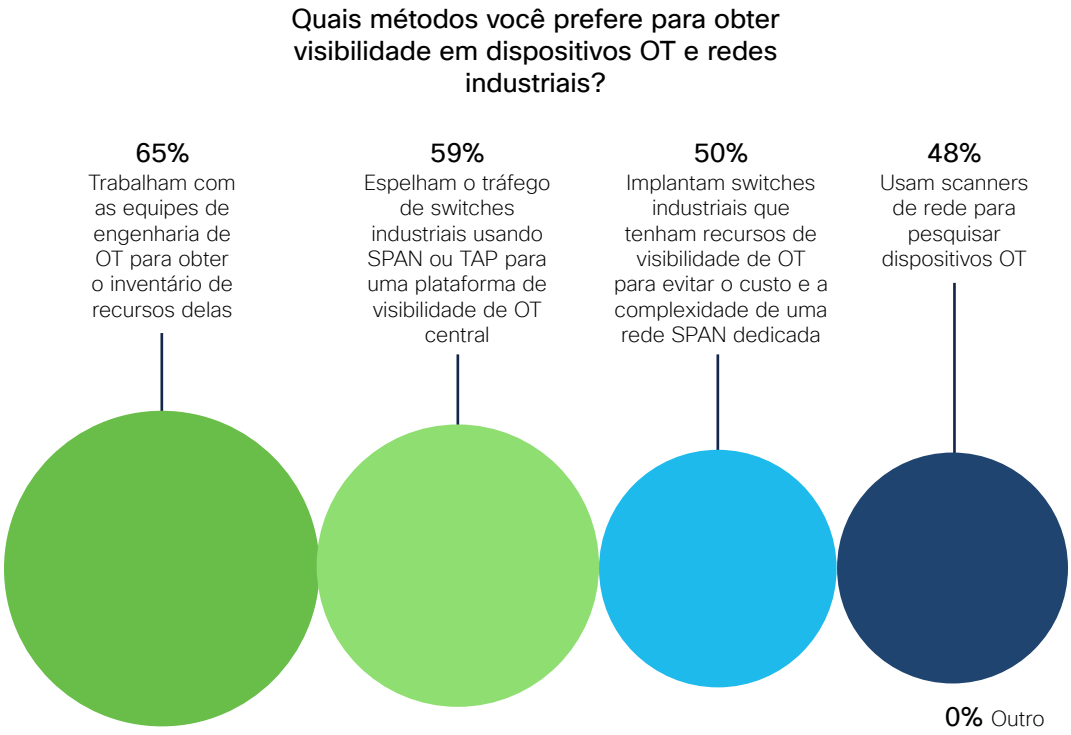


Quando questionados sobre a disponibilidade da rede para fornecer visibilidade, 73% dos entrevistados disseram que os switches estavam prontos para SPAN ou Traffic Access Point (TAP). Isso pode explicar a fixação em SPAN ou TAPs de rede como uma solução de monitoramento, mesmo que 74% dos entrevistados digam que essa implantação seria muito cara e complexa.

Também é revelador que a maioria dos entrevistados não está ciente de outros métodos mais econômicos de monitoramento de tráfego de rede, como o uso de switches industriais com descoberta de recursos integrada e recursos de inspeção detalhada de pacotes (DPI). Apenas 12% dizem que os switches industriais têm recursos de visibilidade de OT integrados.



As empresas devem repensar a visibilidade e a escalabilidade em OT



65% dos entrevistados dizem que trabalhariam com a engenharia de OT para obter um inventário, mas esse método não é confiável, pois os inventários de engenharia geralmente são incompletos e não são atualizados em tempo real. O principal problema é que esses inventários não oferecem visibilidade das atividades de comunicação reais e dos dispositivos mal-intencionados que se conectam à rede. Eles também não ajudam a detectar ameaças e resolver o problema da TI invisível.

59% preferem espelhar o tráfego usando um SPAN ou um TAP, provavelmente devido aos sucessos iniciais ou porque não conhecem alternativas. Isso será problemático em escala, pois os custos e a complexidade aumentam.

50% afirmam que usariam switches industriais com recursos de visibilidade OT. Das três opções, essa solução tem muito a seu favor. Não é necessário criar uma rede de coleta de dados separada, nem modificar a rede OT. Essa solução aborda os dois principais desafios discutidos anteriormente.

48% dizem que usariam scanners de rede. Mas essa opção, como obter um inventário da engenharia de OT, não oferece visibilidade em tempo real de recursos ou comunicações. Além disso, embora os scanners de rede sejam amplamente usados para detectar dispositivos de TI em redes corporativas, eles são inadequados em redes industriais. A maioria dos dispositivos de OT é antiga e vai esgotar rapidamente os recursos limitados de CPU e memória. Provavelmente, as varreduras de rede vão derrubá-los e interromper a produção. As soluções de visibilidade de OT capazes de consultar recursos usando tecnologias semânticas podem ser uma alternativa viável.

Esse desafio com scanners de rede é um bom exemplo do motivo pelo qual as empresas devem olhar além das melhores práticas de TI padrão para encontrar soluções, especialmente quando se trata de desafios de OT.

Dentro de banda ou fora de banda: qual é a melhor opção para a sua empresa?

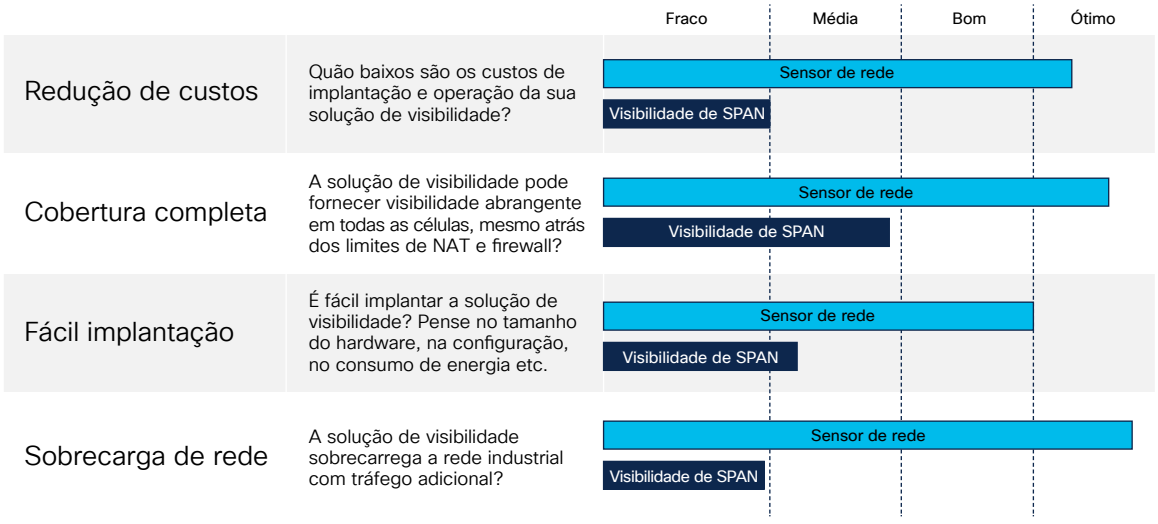
Vamos comparar as duas formas mais comuns de estabelecer visibilidade: criar uma rede SPAN (fora de banda) ou atualizar o equipamento de rede atual (dentro de banda) para dispositivos com recursos de DPI.

Em uma solução de SPAN, o tráfego de rede é coletado de switches industriais e enviado para um dispositivo de segurança dedicado em uma rede fora de banda para análise. Uma solução alternativa é usar equipamentos de rede que incorporam recursos de visibilidade, como DPI passivo e descoberta de recursos ativos.

Esses elementos de rede extrairão informações significativas e enviarão apenas metadados leves para uma plataforma de segurança de OT central para análise posterior. Como esses metadados normalmente representam 3% a 5% do tráfego original, eles podem ser transmitidos dentro de banda sem a necessidade de adicionar recursos de rede adicionais ao ambiente industrial.

As empresas devem considerar os seguintes fatores ao escolher uma solução:

- **Custo:** as soluções dentro de banda são relativamente econômicas porque não exigem hardware ou rede adicional. As soluções fora de banda exigem aquisição, instalação e manutenção de dispositivos dedicados, bem como uma rede totalmente nova, incluindo switches e cabeamento.
- **Escalabilidade:** as soluções dentro de banda aproveitam os recursos de rede atuais e podem ser implementadas rapidamente. Soluções fora de banda exigem tempo e esforço significativos para criar uma rede separada.
- **Visibilidade:** as soluções fora de banda têm um custo, forçando a maioria das empresas a monitorar o tráfego apenas de switches de agregação. Isso limita a visibilidade do tráfego norte-sul e restringe a capacidade de descobrir recursos atrás de firewalls industriais ou limites de conversão de endereço de rede (NAT). Com uma solução dentro de banda, a visibilidade é integrada em cada switch implantado no ambiente.
- **Complexidade:** as soluções dentro de banda não exigem repensar a topologia de rede, apenas configurações adicionais. Uma rede SPAN se torna mais complexa à medida que se torna maior.
- **Impacto na largura de banda:** as soluções dentro de banda enviam metadados leves. As soluções fora de banda duplicam o tráfego e geralmente exigem a criação de uma rede separada para evitar congestionamentos de loop de controle e instabilidade na rede industrial.



Para obter mais detalhes sobre como obter visibilidade usando uma arquitetura dentro ou fora de banda, consulte este resumo técnico.

Conclusão

Hoje, a vulnerabilidade dos ambientes de OT/ICS não pode ser exagerada. As empresas industriais devem acelerar seus esforços para aumentar a segurança de OT.

Embora a maioria das empresas esteja apenas começando a jornada de segurança de OT, é encorajador vê-las caminhando na direção certa. Elas têm uma abordagem de segurança bastante madura e entendem a importância da visibilidade para viabilizar medidas preventivas e corretivas.

Obviamente, a visibilidade é apenas uma parte da solução, mas é a etapa básica sobre a qual todo o resto é criado. Qualquer solução viável também deve ser capaz de segmentar as redes e ser dimensionada em vários locais de forma econômica.

Mais importante ainda, as empresas devem olhar além das melhores práticas de TI padrão para encontrar a melhor solução e melhorar a colaboração entre TI, OT e SecOps.

O Cisco Industrial Threat Defense utiliza a rede industrial como sensor e aplicador para ajudá-lo a obter visibilidade em escala e adotar uma abordagem passo a passo para implementar uma estratégia de segurança de OT abrangente. Para saber mais, acesse cisco.com/go/iotsecurity.

Metodologia

As descobertas neste relatório foram derivadas de uma pesquisa do setor do Q3 2022 projetada pela TP Research e conduzida pela Gartner Peer Insights envolvendo 100 profissionais de TI, OT, engenharia e InfoSec.

Os entrevistados vêm de diversas regiões, setores e empresas:

- 84% dos entrevistados estão na América do Norte e 16% na Europa, no Oriente Médio e na África (EMEA).
- 74% dos entrevistados estão no nível de diretoria e superior; 26% são gerentes.
- 50% dos entrevistados vêm de empresas com mais de 10.000 funcionários; 17% vêm de empresas com 5.000 a 10.000 funcionários; 33% vêm de empresas com pelo menos 1.000 funcionários.

C11-3411110-00 02/23