

Segurança digital focada em OT

para manter a operação em funcionamento

Soluções desenvolvidas
especificamente para proteger
ambientes nos níveis de endpoint
e de rede.



Sobre as redes TXOne

Sistemas de controle industrial (ICS) são ecossistemas complexos onde dispositivos legados e de última geração operam juntos para manter os processos de produção em funcionamento no chão de fábrica. No entanto, essa infraestrutura complexa pode ser facilmente atacada. As vulnerabilidades em ICS estão sendo cada vez mais alvo, e ataques cibernéticos se espalham rapidamente—interrompendo a produção, podendo danificar ativos críticos e até mesmo colocar vidas em risco. A TXOne oferece soluções de segurança digital focadas em OT para proteger ambientes tanto no nível de endpoint quanto no nível de rede.

A TXOne implanta defesas em múltiplas camadas, nativas para OT, para a proteção de operações industriais contra ameaças conhecidas e desconhecidas.

Nossas soluções oferecem:



Visibilidade de ativos que se traduz em ações contra ameaças



Proteção de endpoint que suporta a maioria dos sistemas operacionais legados



Defesa de rede implantada além do gateway

Sem interrupção na operação de OT

A TXOne tem mais de 3.000 clientes e atende a vários segmentos industriais em todo o mundo:

- Semicondutores
- Automobilístico
- Manufatura
- Infraestruturas críticas
- Gás e petróleo
- Varejo
- Saúde
- Transporte
- Utilities
- Água e esgoto



Inspecção de Segurança Cibernética Série Portable Inspector

Garante a integridade dos ativos com varreduras rápidas de vírus e malware em dispositivos, sem nenhuma necessidade de instalação, permitindo a defesa de ambientes isolados (air-gapped), melhorando a segurança de supply chain e estendendo a visibilidade de seus ativos.



Proteção Endpoint Série Stellar

Proteção de ativos de ICS mesmo em condições extremas com segurança de endpoint para todos os cenários de uso, baseada em Zero Trust para OT, suportando a maioria dos sistemas operacionais legados.



Defesa de Rede Série Edge

Implementando-se além do gateway, minimiza o impacto de incidentes cibernéticos com segmentação de rede nativa para OT e cobre de forma definitiva vulnerabilidades em endpoints legados e não atualizados, blindando os ativos de ameaças no nível de rede.