5 Pilares para Asegurar su Red Industrial

Su red industrial tiene puntos ciegos.

El 78% de las plantas industriales experimentaron al menos un incidente de ciberseguridad que impactó sus operaciones en los últimos 24 meses.

- **Manufactura**
- **CPG**
- **Retail**
- **Energy & Utilities**
- **Natural Resources**

La pregunta no es si su organización será un objetivo.
Es si estará lista cuando llegue el momento.

400%

aumento esperado en activos OT industriales conectados

15B

activos industriales con conectividad 5G para 2026

70%

de activos ICS/SCADA tienen conexiones externas

1K+

CVEs en sistemas de control industrial

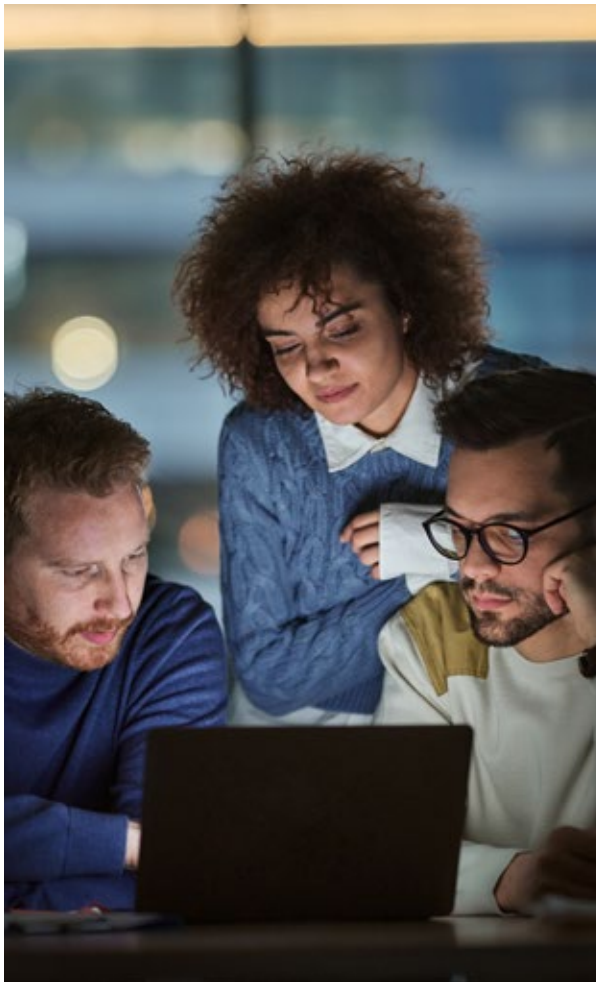
+80%

vulnerabilidades en los cuatro principales vendors OT

Desafíos y soluciones ciberseguridad industrial

Desafíos del C-Level Hoy

- Falta de visibilidad completa de activos industriales (OT/IoT)
- Convergencia IT/OT creando nuevos vectores de ataque
- Cumplimiento regulatorio cada vez más estricto
- Amenazas sofisticadas dirigidas a infraestructura crítica
- Arquitecturas complejas no enfocadas en industrias específicas



1 Framework de Visibilidad de Activos Industriales

Descubrimiento automático de PLCs, HMIs, SCADA e IoT sin agentes ni interrupciones. Inventario autorizado y siempre actualizado.

PA IoT/OT Security

2 Estrategias de Segmentación de Red OT

Segmentación inteligente basada en perfil de dispositivo. Contiene el movimiento lateral entre IT y OT. Cumplimiento IEC 62443.

PA NGFW + IoT Security

3 Monitoreo Continuo y Detección de Amenazas

Detección de anomalías en tráfico OT/IT con IA/ML en tiempo real. Correlación con Unit 42 threat intelligence de Palo Alto.

PA Cortex XDR + MXDR NTT

4 Arquitectura Avanzada y Simplificada

Zero Trust para entornos industriales: verificación continua de identidad, mínimo privilegio, sin rediseñar la red existente.

Prisma SASE + NGTS

Por qué NTT DATA & Palo Alto

PA IoT/OT Security

Visibilidad y segmentación automática de activos industriales. Sin agentes.

PA NGFW

Inspección de tráfico IT/OT. Políticas Zero Trust por zona de red.

Prisma SASE

Acceso remoto seguro a sistemas OT desde cualquier lugar.

NGTS

Gobierno de certificados integrado. Sin outages, sin hojas de cálculo.

MXDR (NTT DATA)

SOC gestionado 24/7 con Unit 42 threat intelligence. MTTD en minutos.

Converse con nuestro equipo.

Agende una Conversación con Nuestro Equipo

Contacta con nuestro equipo para solicitar una demostración o una evaluación gratuita y obtener más información sobre las capacidades de seguridad de los dispositivos OT.

→ Demo de la plataforma PA IoT/OT Security

→ Assessment gratuito de su postura OT/IT

→ Sesión estratégica con especialista NTT + PA

→ Propuesta de arquitectura personalizada

Agendar una llamada


NTT DATA