# NTT DATA Industrial MSSP powered by Claroty

OT Security di livello enterprise, resa accessibile attraverso un servizio gestito

NTT DATA

**Industrial MSSP**
managed OT cyber relience services
powered by CLAROTY

## 1 Mercato e opportunità

La necessità di proteggere gli ambienti OT cresce più velocemente della capacità delle aziende industriali di gestirla.

**Digitalizzazione e convergenza IT/OT**
Impianti sempre più connessi e digitalizzati aumentano la superficie di esposizione cyber.

**Continuità operativa**
OT Security è collegata a resilienza operativa, continuità produttiva e protezione del valore industriale.

**Pressione normativa**
NIS2 e altri requisiti stanno accelerando la governance, visibilità e gestione del rischio cyber.

**Carenza di competenze specialistiche**
Molte aziende industriali non dispongono di team e competenze OT Security dedicate.

## 3 La nostra offerta e il valore per il cliente

**NTT DATA rende accessibili capacità OT Security di livello enterprise a una fascia di clienti che difficilmente potrebbe adottarle attraverso un modello tradizionale dedicato.**

Un ambiente multi-tenant e segregato per cliente consente di superare la barriera dimensionale del modello tradizionale, **combinando tecnologia best-in-class e servizi specialistici NTT DATA.**

## 5 Il servizio: un percorso verso una OT Security più resiliente

**Visibilità**
Inventario aggiornato degli asset OT, IoT.

**Comprensione**
Visibilità su vulnerabilità, rischio, comunicazioni e dipendenze di rete.

**Priorità**
Contestualizzazione delle vulnerabilità e azioni rilevanti.

**Monitoraggio**
Rilevazione di alert, anomalie e minacce sugli ambienti OT.

**Miglioramento**
Reporting, governance periodica e raccomandazioni specialistiche.

## DALL'ESIGENZA ALLA CAPACITÀ ENTERPRISE

**Esigenza OT Security**

**Modello MSSP**

**Capacità di livello enterprise**

## 2 Cliente target

Aziende industriali di fascia media con esigenze concrete di OT Security, ma strutture e perimetri più contenuti.

**Cliente ideale**
Aziende industriali di fascia media che:

- hanno un ambiente OT significativo
- dispongono di uno o pochi siti produttivi
- stanno aumentando la maturità in ambito OT Security
- non dispongono di competenze OT Security dedicate
- necessitano di maggiore visibilità e gestione del rischio
- non hanno necessità tali da giustificare un tenant Claroty dedicato

Perimetro OT tipico: **250 – 1.000 asset**

Settori prioritari: **Manufacturing, Energy, Utilities e altri settori con infrastrutture critiche ed ambienti OT rilevanti.**

## 4 Superare la barriera di ingresso

**Modello tradizionale**
Tenant dedicato

- Soglia minima di licensing
- Competenze specialistiche necessarie
- Gestione continuativa della piattaforma

**Spesso sovradimensionato per aziende industriali mid-market**

**Modello NTT DATA Industrial MSSP**
Ambiente Claroty xDome MSSP

- Capacità tecnologica condivisa
- Sub-tenant segregato per ciascun cliente
- Servizi gestiti da NTT DATA

**Capacità enterprise rese accessibili anche a perimetri più contenuti**

## 6 Tecnologia best-in-class + servizi specialistici

**CLAROTY xDOME**
**Piattaforma OT Security**

- Asset Discovery & Inventory
- Vulnerability & Risk Management
- Network Visibility
- Threat Detection
- Reporting & Compliance

+

**NTT DATA OT SECURITY**
**Servizi specialistici gestiti**

- Onboarding e configurazione
- Discovery iniziale e tuning
- Monitoraggio e gestione continuativa
- Analisi, raccomandazioni e reporting
- Supporto alla compliance
- Accesso a competenze OT Security