safous By IIJ

OsecT

AT-A-GLANCE

# OsecT With Safous

## Unified Asset Visibility & Monitoring for Cyber-Physical Systems

Bring visibility, threat detection, and secure remote access for your Cyber-Physical Systems (CPS) together in one platform for safer, faster Operational Technology (OT) operations.

## Three Pillars

Industrial environments weren't designed with cloud connectivity and remote access in mind, so modern OT operators are inheriting new cybersecurity risks and challenges like:

**OT Network Visibility:**
Live inventory, topology/flows, change diffs

**Early Threat Detection:**
New/rogue devices, abnormal traffic, OT-aware alerts

**Secure Remote Access:**
MFA, approvals, least privilege, full audit & recording

## CPS Visibility & Monitoring Powered by OsecT

OsecT is provided by NTT DOCOMO BUSINESS, Inc.

- Available as an on-premises solution via the one appliance
- Central, multi-site portal for all assets, flows, and alerts
- Baseline and change diffs to see what changed, where, and when
- Early anomaly discovery for unknown/rogue devices, unsupported OS, etc
- Evidence and reporting, including exportable findings for reviews

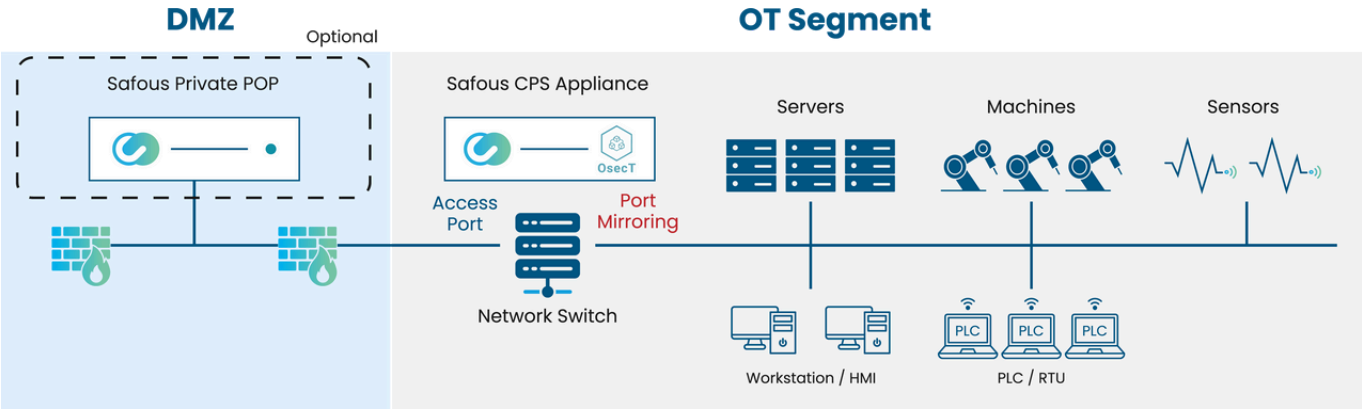

## Secure, Governed Access With Safous

Safous Privileged Remote Access is the foundation of governed connectivity within the Safous + OsecT architecture. It enhances OsecT by enabling approved, audited access to your CPS assets with governance, monitoring, and credential hygiene baked in.

- MFA and approvals with just-in-time, least-privilege sessions
- Agentless access via OT-DMZ/AppGateway, no broad network exposure
- Session recording and centralized logging
- Integrated credential governance (vaulting, SSO, no shared accounts)
- Unified policies and roll-up views let you scale across multiple plants

**From detection to governed action:**
Together, OsecT surfaces risks while Safous brokers approved, recorded access to your OT assets – all without exposing plant networks.

## How It Works




## Use Cases

**Real-Time Situational Awareness:** Visualize all asset communications in one interface. OsecT maps live network activity while Safous provides governed access for investigation and response.

**Change-Controlled Maintenance:** Use OsecT to baseline system behavior and detect anomalies. Safous gates all access with approval workflows and session audits.

**Secure IDS Portal Access & Evidence Linking:** Safous enables scoped access to OsecT analytics and ensures session logs directly link user actions to alert findings.

**Rogue/New Device Response:** OsecT detects unknown or unmanaged endpoints while Safous enables scoped, time-limited investigation and cleanup.

## Features

OsecT

**OsecT**

- Co-located on AppGateway hardware
- Asset discovery and traffic mapping
- Change diffs and baseline tracking
- Anomaly detection and alerts
- Multi-site roll-up views
- Exportable findings

safous

**Safous Privileged Remote Access**

- MFA, approvals, and least privilege access
- Session recording and logging
- Agentless access via AppGateway
- Credential vaulting and SSO
- Zero Trust based secure remote access

## Compliance & Governance

**Supports key OT security principles:** Strong authentication, encrypted sessions, centralized monitoring, and tamper-resistant audit evidence.

Ready for streamlined OT security in one easy-to-use appliance? Deploy OsecT and Safous Privileged Remote Access together on shared hardware – centrally managed on-premises.

**Request a joint demo** to see unified detection and access control in action.