

GUIDE · INTEGRATION

Complementing OT Visibility Platforms

How ConnexSight, ConnexGate and ConnexONE support Claroty, Dragos and Nozomi Networks deployments — the enforcement layer that OT visibility platforms depend on.

Contents

1

The enforcement gap visibility platforms cannot fill

3

2

The Connexite product suite

4

3

How the stack works together

6

4

Working with Claroty, Dragos and Nozomi Networks

8

–

Sources and references

10

OT visibility platforms such as Claroty, Dragos and Nozomi Networks detect and analyse — but they need a safe way to receive OT traffic, a safe way to move telemetry out of the OT zone, and something else to stop unwanted commands reaching field devices. This guide explains how the Connexite TAP, OT gateway and data diode provide those three things, and how to connect them to the monitoring platform you already run.

Products covered	ConnexSight (network TAP) · ConnexGate (OT gateway) · ConnexONE (data diode)
Visibility platforms	Claroty · Dragos · Nozomi Networks
Audience	Security architects and engineers planning or extending an OT monitoring deployment

1. The enforcement gap visibility platforms cannot fill

1.1 WHAT VISIBILITY PLATFORMS DO WELL

Claroty, Dragos and Nozomi Networks are leading OT visibility and detection platforms. They discover and classify assets, decode industrial protocols, baseline normal behaviour and raise alerts when something looks wrong. Dragos adds ICS-specific threat intelligence and incident response depth; Nozomi is known for AI-based baselining and multi-site management; Claroty for asset discovery breadth and exposure management. Most industrial deployments start with passive monitoring from TAP or SPAN traffic copies, so that operations are never put at risk.

1.2 WHAT THEY DEPEND ON

These platforms are readers, not enforcers. Their sensors need traffic delivered to them by a separate access layer, and their telemetry needs a controlled path out of the OT zone. They do not, on their own, decide what is allowed to cross a zone boundary. In every deployment, the same three needs appear:

- **Traffic access.** The sensor needs a complete copy of OT traffic. Without a purpose-built TAP, organisations default to switch SPAN ports, which can drop packets under load, add switch CPU overhead and cannot guarantee full capture.
- **Safe data export.** Sensor telemetry and alerts must travel from the OT/DMZ segment to the enterprise network where the management plane runs. Without a data diode, that channel is a bidirectional firewall rule that auditors scrutinise.
- **Field device protection.** A visibility platform can see a write command being sent to a PLC or RTU, but its job is to alert. Without a protocol-aware gateway enforcing read and write rules, field devices stay reachable from whatever is connected upstream.

Need	Visibility platform provides	Connexite provides
Traffic access	Sensor analyses the traffic it receives	ConnexSight: passive TAP with no IP or MAC address, selective filtering, device fingerprinting, local capture
Safe data export	Alerts and telemetry that must leave the OT zone	ConnexONE: hardware-enforced one-way transfer with any-to-any protocol translation
Command control	Detects and alerts on suspicious commands	ConnexGate: deep packet inspection to command level, read allowed and write blocked
Analytics and threat context	Asset inventory, anomaly detection, threat intelligence	Not Connexite's role — the customer chooses the platform

2. The Connexite product suite

Connexite makes three complementary products. Each can be deployed on its own; together they cover traffic access, command control and boundary enforcement.

ConnexSight

NETWORK TAP

connexite.co.uk/connexsight

The passive visibility foundation. It gives monitoring tools a complete copy of network traffic with no impact on the monitored network.

- **Zero footprint.** No IP or MAC address on the production side, so it cannot be discovered or targeted by traffic passing through it.
- **Fingerprinting.** Built-in device fingerprinting identifies endpoints from passive observation, without active scanning.
- **Selective filtering.** Delivers only relevant traffic to each downstream tool, protecting the capacity of costly analytics platforms.
- **Local packet capture.** Creates local capture files for immediate analysis, without waiting for access to the monitoring platform.
- **Physical bypass.** Selected models provide mechanical bypass so the monitored link stays live during power events.
- **Zero-touch deployment.** Plug-and-play operation with a modern single-page web interface.

ConnexGate

OT GATEWAY

connexite.co.uk/connexgate

A ruggedised, protocol-aware gateway that connects legacy field devices to modern IT and cloud applications without exposing them to unwanted commands.

- **Deep packet inspection.** Validates Modbus, Profinet, MQTT, OPC-UA, DNP3 and IEC 104 traffic down to individual command codes, not just port numbers.
- **Granular command filtering.** Rules such as “allow read operations on a register range, block all write and force-coil commands” prevent misconfiguration from the IT side reaching production devices.
- **Legacy integration.** Connects 10 to 20 year old RTUs, PLCs and sensors without replacing them.
- **Operational continuity.** Security enforcement is designed never to interfere with production availability.
- **SREL.** ConnexGate underpins Connexite’s Secure RTU Enforcement Layer for energy distribution networks, mapped to IEC 62443 Security Levels 2 and 3, NERC CIP and NIS2 requirements. See connexite.co.uk/srel.

ConnexONE

DATA DIODE

connexite.co.uk/connexone

Physically guaranteed one-way data transfer. There is no software configuration that can open a return path.

- **Any-to-any protocol translation.** Choose the source protocol on the OT side and the destination protocol the IT side expects; ConnexONE translates without extra middleware.
- **Guaranteed delivery.** Packet-level techniques ensure telemetry is not lost crossing the boundary, which matters for historian replication and audit trails.
- **Hardware range.** A modular hardware line-up for every deployment scenario, set out below.

Model	Throughput	Interfaces	Best for
NOVA 1G	Up to 1 Gbps	Multi-gigabit OT ports with 10G uplinks	Standard plant and factory deployments
ZENITH 10G	Up to 10 Gbps	High-density port aggregation	Data centre and large-site consolidation
COMET REMOTE	WAN-connected	xDSL, LTE/5G with encrypted tunnelling	Remote field edge, substations, pipelines

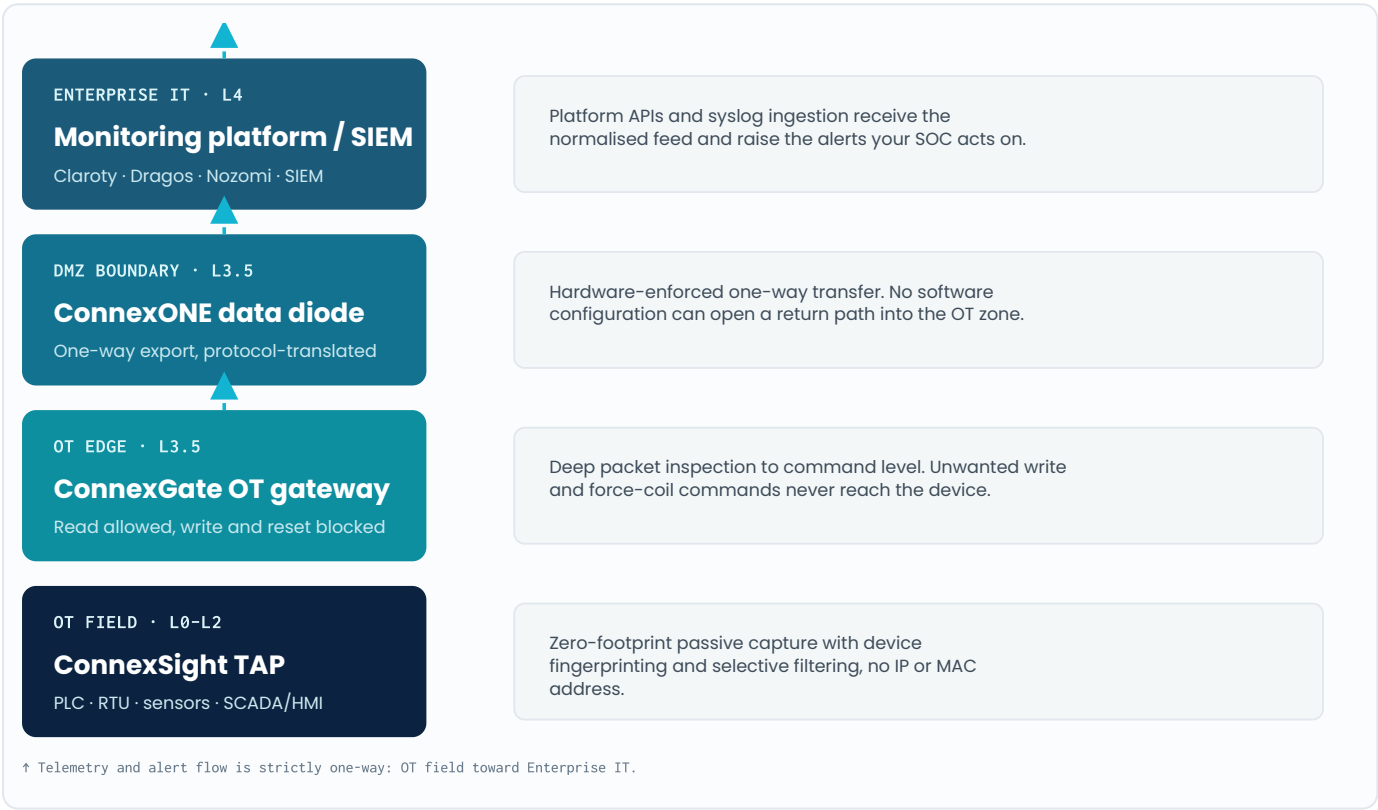
IN SHORT

ConnexSight sees everything on the wire without being seen itself. ConnexGate decides what commands are allowed to reach a field device. ConnexONE guarantees that nothing travels back the way telemetry came. Together, they are the access, control and export layer that a visibility platform is built to sit behind — not a replacement for it.

3. How the stack works together

The three products are deployed across the [Purdue reference model](#) zones, with Connexite hardware at the boundary between the OT field environment and the enterprise network.

Zone	Connexite product	Role	What flows
OT field (L0-L2)	ConnexSight TAP	Capture all traffic passively with zero footprint	Modbus, Profinet, DNP3, IEC 104, OPC-UA frames
OT edge (L3.5)	ConnexGate OT gateway	Protocol-aware command filtering for field devices	Allowed read commands pass; write and reset commands blocked
DMZ boundary (L3.5)	ConnexONE data diode	Hardware-enforced one-way export	Telemetry, historian data, syslog: outbound only, protocol-translated
Enterprise IT (L4)	Aggregator (partner-deployed)	Receives diode output and feeds platforms	Normalised telemetry to Claroty, Dragos, Nozomi and SIEM



Where Connexite sits across the Purdue model, from OT field devices to the monitoring platform

3.1 TYPICAL DEPLOYMENT SEQUENCE

For brownfield environments, sequence the deployment to minimise change risk in live production networks.

1 Deploy ConnexSight

Install the TAP on the critical ring segment or core switch. No network configuration changes are needed, and it immediately gives ground-truth visibility of what is on the network.

2 Baseline traffic

Use ConnexSight fingerprinting and local capture to produce an asset inventory and protocol baseline. This drives the ConnexGate and ConnexONE rules and seeds the monitoring platform.

3 Install ConnexGate at field device boundaries

Position it between RTU or PLC devices and the SCADA layer. Configure inspection rules from the baseline and start in monitoring-only mode before enabling active command filtering.

4 Install ConnexONE at the DMZ boundary

Configure protocol translation from OT-side sources to the IT-side aggregator. The aggregator becomes the feed point for whichever platform the customer selects.

5 Connect the monitoring platform

Feed the aggregator output, and the ConnexSight mirror where a sensor sits in the DMZ, to Claroty, Dragos, Nozomi or a SIEM.

3.2 PROTOCOL SUPPORT ACROSS THE STACK

Confirm protocol coverage per layer before finalising a bill of materials.

Protocol	ConnexSight TAP	ConnexGate inspection	ConnexONE translation	Typical use
Modbus TCP/RTU	Full capture	Command level	To HTTP or MQTT	PLC and RTU data
OPC-UA	Full capture	Session level	To REST/JSON	Historian, SCADA
IEC 104 / 101	Full capture	ASDU filtering	To syslog or HTTP	Energy, substations
DNP3	Full capture	Function code	To MQTT or syslog	Water, energy RTUs
Profinet	Full capture	Cyclic and acyclic	Protocol pass-through	Manufacturing PLCs
EtherNet/IP	Full capture	CIP service	Protocol pass-through	Allen-Bradley
MQTT	Full capture	Topic filtering	To HTTP or REST	IIoT edge devices
Syslog	Full capture	Port level	To syslog or REST	Logging, events

Protocol details are indicative. Confirm exact support and versions against current Connexite product documentation at docs.connexite.co.uk for each project.

4. Working with Clarity, Dragos and Nozomi Networks

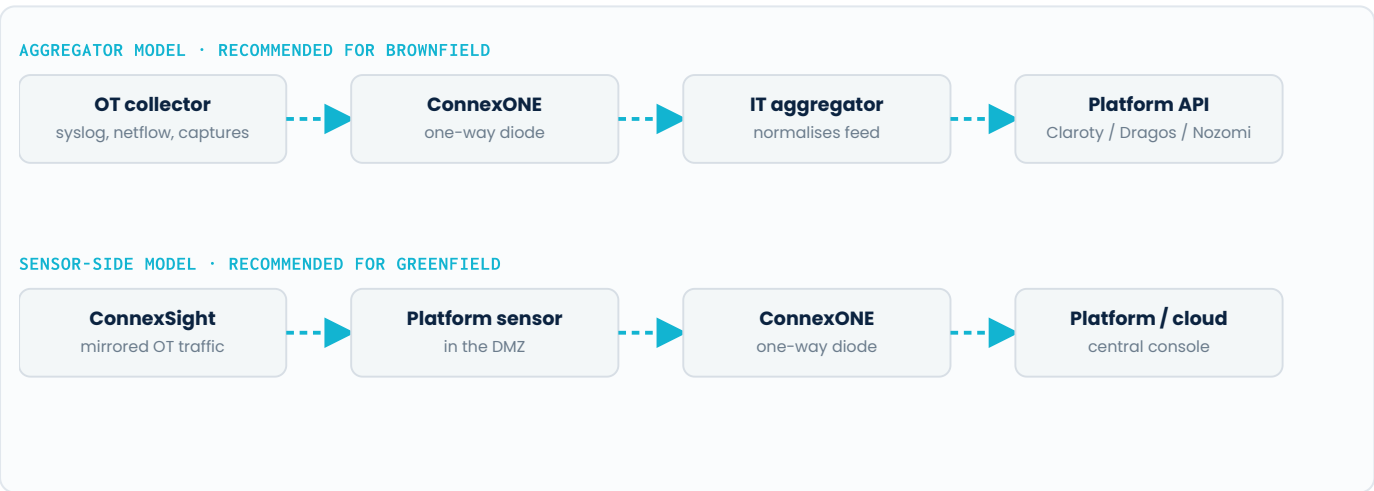
The Connexite layer is platform-agnostic. Any platform or SIEM that accepts syslog, REST or MQTT on the IT side can consume the aggregator output, and any sensor that accepts a mirrored feed can be connected to ConnexSight.

4.1 HOW EACH PLATFORM CONNECTS

Platform	Connects via	Typical model	What Connexite adds
Clarity	Management platform (xDome or on-premise CTD) pulls from the IT-side aggregator; a sensor in the DMZ is fed by the ConnexSight mirror	Aggregator model: sensor in DMZ, telemetry through ConnexONE to the management plane	Full-frame traffic for protocol parsing and asset discovery, with fingerprinting that helps seed the inventory
Dragos	A sensor in the DMZ receives the mirrored feed; exports cross the boundary through ConnexONE	Sensor-side model: Dragos sensor behind the diode, platform on the IT side	A controlled one-way path for air-gapped or near-air-gapped sites, with ICS threat intelligence layered on top
Nozomi	Guardian sensor fed by the ConnexSight mirror; Vantage or the central console receives data through ConnexONE	Vantage managed service: Guardian in DMZ, telemetry through ConnexONE to the cloud or central console	Selective filtering to protect sensor capacity, and a safe export path that supports partner-run managed services

Platform component names and supported ingestion paths evolve. Validate the exact connector and deployment model with the platform vendor for each project.

4.2 TWO REFERENCE DEPLOYMENT MODELS



Aggregator model (recommended for brownfield). A lightweight collector on the OT side bundles telemetry such as syslog, netflow, historian snapshots and protocol captures. ConnexONE forwards these as one-way streams to an IT-side aggregator. The monitoring platform connects to the aggregator over normal authenticated APIs. This avoids placing new probes in the OT segment and minimises change risk.

Sensor-side model (recommended for greenfield). The platform sensor sits in the DMZ and processes the ConnexSight mirror feed. Its telemetry is exported through ConnexONE to the platform on the IT side. The sensor sees raw frames, which gives the richest asset inventory and protocol analysis.

4.3 TECHNICAL INTEGRATION NOTES

ConnexONE, aggregator and monitoring platform

- Whitelist the UDP destination ports for the telemetry streams on the aggregator firewall.
- Synchronise NTP on both sides of the diode so alert timestamps and log correlation stay accurate.
- Align MTU between the OT-side agent and the diode (a typical safe value is 1400 bytes) to avoid fragmenting large OPC-UA or historian packets.
- Size the aggregator for the peak telemetry rate. ConnexSight selective filtering reduces the load by removing background traffic before it reaches the diode.

ConnexSight and sensor probes

- Configure ConnexSight selective filtering before connecting the probe, so irrelevant broadcast traffic does not overwhelm its analysis capacity.
- Use ConnexSight fingerprinting output to accelerate the platform's initial asset discovery.
- Physical bypass keeps the mirror and the monitored link running while the connected probe is maintained.

4.4 SINGLE PLATFORM OR SEVERAL

Many industrial sites run Claroty or Nozomi for broad asset visibility and add Dragos for ICS threat intelligence and response. With Connexite in place, all of them draw from the same enforcement layer: one TAP feed and one export path. That avoids duplicate collection points in the OT network, and the customer can add or change a platform later without redesigning the boundary.

Sources and references

Connexite. connexite.co.uk, including the ConnexONE, ConnexGate, ConnexSight, SREL and partner programme pages, and docs.connexite.co.uk for current protocol documentation.

Clarity. clarity.com — platform and integration documentation.

Dragos. dragos.com — platform and integration documentation.

Nozomi Networks. nozominetworks.com — Guardian and Vantage documentation.

IEC 62443. [Industrial automation and control systems security](https://www.iec.ch) — iec.ch.

Purdue Enterprise Reference Architecture. [The zone model referenced throughout this guide, via ISA](https://isa.org) — isa.org.

This guide reflects the Connexite product range and publicly available information about the named visibility platforms at the time of writing. Specific protocol support, connector names and ingestion paths should be confirmed against current vendor and Connexite documentation before deployment.

Talk to us about your deployment

Our engineering team can help you plan a brownfield or greenfield rollout alongside Clarity, Dragos, Nozomi or your SIEM of choice.

connexite.co.uk/contact

docs.connexite.co.uk