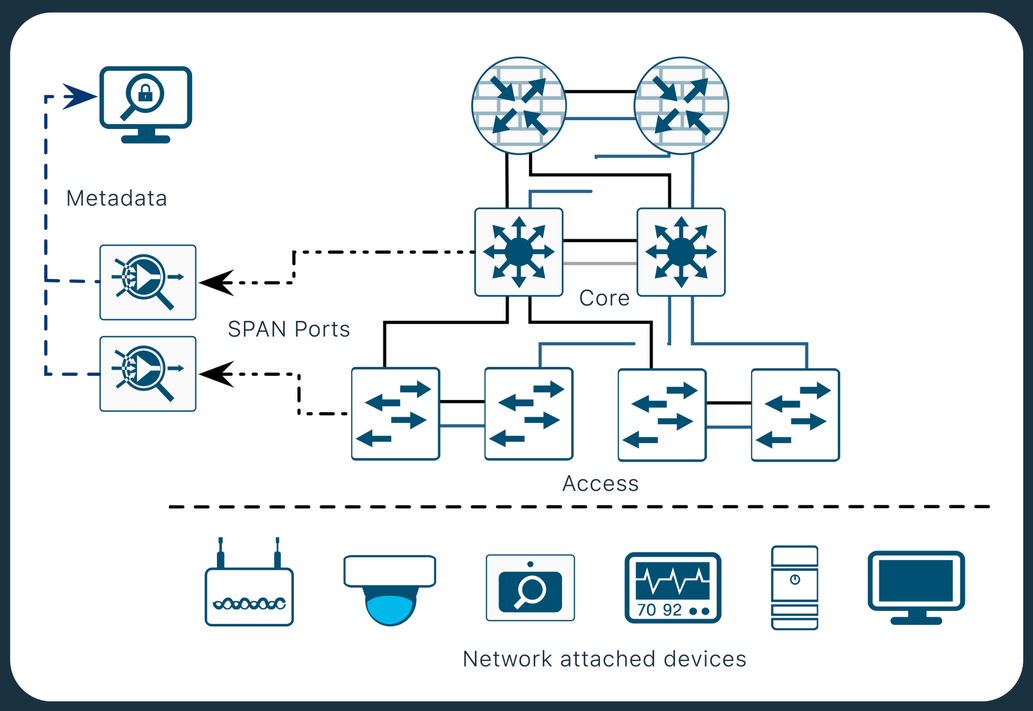
OMEGA NETWORKS

Network Attached Device Discovery

Complete visibility into every OT, IoT, and MIoT device on your network



Omega deploys compact sensors on SPAN ports at the core and access layer of your network, passively observing real traffic without sending a single packet. Because we analyse at the switch level, we see east-west traffic between devices on the same VLAN, not just north-south traffic through a gateway. Only connection metadata is transmitted to our analytics engine. No raw packet data ever leaves your premises.

The Challenge

Most organisations have no accurate picture of the OT, IoT, and medical devices on their network. Asset registers go stale within weeks, unmanaged devices accumulate, and security blind spots grow. Unpatched devices and rogue IoT create lateral movement paths for ransomware at the local switch level, often invisible to gateway-level monitoring. Visibility is a prerequisite for compliance frameworks such as HISO and NZISM.

Key Capabilities

Passive Discovery
Zero-impact traffic analysis. No packets sent, no disruption to clinical or OT systems.

East-West Visibility
SPAN port analysis at the switch level captures lateral device-to-device traffic that gateway monitoring misses.

Device Classification
Automatic identification of device type, manufacturer, OS, and role using protocol fingerprinting.

Risk Scoring
Per-device risk assessment with prioritised remediation recommendations.

Security Alerting
Known-bad signature detection and anomalous traffic pattern identification.

Managed Service
Sensors arrive pre-configured. Omega handles monitoring, firmware, and reporting remotely.

Highlights

- **Metadata only** leaves your premises. No raw packet captures transmitted.
- **NZ-hosted analytics** at Xtreme Datacentre, Wellington.
- **CISA-developed** technology for U.S. critical infrastructure protection.
- **14-day minimum** observation period per network.
- **Encrypted in transit** between sensor and analytics engine.
- **Passive and read-only** sensor. Cannot modify or inject traffic.

How it Works

1. **Deploy Sensor**
Compact sensor connects to a mirror/SPAN port on your core switch. No agents, no network changes.

2. **Passive Collection**
Sensor observes traffic for a minimum of 14 days, capturing connection metadata, protocols, and service fingerprints.

3. **Analysis & Enrichment**
Metadata is securely transmitted to our analytics engine where it is correlated, enriched, and scored for risk.

4. **Deliverable**
You receive a comprehensive discovery report with device register, communication map, service inventory, and risk assessment.

Service & Support

Sensors arrive pre-configured. Plug into your SPAN port and backhaul, and you're live. Omega monitors remotely. If a sensor goes offline, we notify you and guide troubleshooting. Faulty hardware replaced via advance shipment. Firmware updates, analytics improvements, and reporting enhancements included.

No raw packet data leaves site. Only connection metadata and security alerts transmitted.

Analytics hosted at Xtreme Datacentre, Wellington. Your data stays in New Zealand.

All metadata encrypted in transit. Sensor is passive and read-only.

Network Attached Device Discovery

OMEGA NETWORKS

Sensor Options

Choose the sensor tier that matches your environment. All sensors are deployed, managed, and maintained by Omega as part of the service.

Basic

Throughput	**Up to 850Mbps**
Uplink	**1GbE**
Backhaul	**WiFi**
Form Factor	**Compact SBC**

Small clinics, GP practices, remote sites

Advanced

Throughput	**Up to 2.3Gbps**
Uplink	**2.5GbE**
Backhaul	**Dedicated Ethernet**
Form Factor	**Mini PC**

Specialist centres, campuses, libraries

Enterprise

Throughput	**Up to 9.4Gbps**
Uplink	**10GbE**
Backhaul	**Dedicated Ethernet**
Form Factor	**Mini PC**

Hospitals, Data centres, Event centres

Need more than 10 Gbps? Custom sensor configurations available. Contact us to discuss your requirements.

Customer Deliverables

Deliverable	Description
Device Register	Every OT, IoT, and MIoT device observed, including hostname, MAC, IP, manufacturer, device role, protocols, and first/last seen timestamps.
Communication Map	Visual and tabular mapping of device-to-device communication with protocols, data volumes, and traffic direction.
Service Inventory	Detected services, applications, and OS fingerprints across your operational environment.
Security Alerts	Flagged anomalies, known-bad signatures, and unexpected traffic patterns.
Risk Assessment	Per-device risk scoring with prioritised recommendations for remediation.

Built For

Healthcare
Infusion pumps, patient monitors, imaging, telemetry, smart beds, and BMS.

Critical Infrastructure
OT/SCADA environments where active scanning is not an option.

Industrial
PLCs, HMIs, sensors, and industrial IoT across production lines.

Smart Buildings
BMS controllers, HVAC, access control, and connected building systems.

Ordering Information

Pricing assumes /23 or smaller subnets. Larger subnets may require additional sensors or custom pricing.

SKU	Description		
NDAS-VLAN	Per-VLAN Discovery Assessment	One-time	$2,250
NDAS-SITE-SM	Small Site Package (1-8 VLANs)	One-time	$18,000
NDAS-SITE-STD	Standard Site Package (9-20 VLANs)	One-time	$33,000
NDAS-SITE-LG	Large Site Package (21-30 VLANs)	One-time	$42,000
NDAS-VLAN-ADD	Additional VLAN (beyond 30)	One-time	$1,600
NDAS-SNS-BAS	Basic Sensor (850 Mbps)	Monthly	$250/mo
NDAS-SNS-ADV	Advanced Sensor (2.3Gbps)	Monthly	$450/mo
NDAS-SNS-ENT	Enterprise Sensor (10 Gbps)	Monthly	Contact us
NDAS-SNS-CST	Custom Sensor (>10 Gbps)	Monthly	Contact us
NDAS-RPT-RRW	Risk & Remediation Workshop (optional)	Per site	$2,250

Book a scoping call