



SecurOT

Centre of Excellence

Updated CYQ3 2026



Contents

03	OT Security
04	Why OT Infrastructure Availability Matters
05	A Structured Approach for ANZ
06	Core Pillars of OT Security
07	Examples of a five-stage implementation
08	The SecurOT Centre Of Excellence
09	How do we help you win with the CoE?
10	The Customer OT Security Journey
11	Bespoke training with Wavelink
12	OT Services Portfolio
14	Vendor Matrix
15	Vendor Solutions
23	Next Steps and Engagement

OT Security: Secure your automation systems

OT security, or Operational Technology security, refers to the practices and technologies used to protect industrial automation and control systems (ICS), as well as other critical infrastructure, from cyber threats.

Unlike IT security, which focuses on networks, applications, and data, OT security is concerned with safeguarding physical systems such as machines, plants, and industrial processes. Many of these systems were originally designed without internet connectivity and often run on legacy operating systems (such as Microsoft Windows XP or Windows 7), making them more susceptible to cyber attacks.



OT is highly prevalent in industry

Manufacturing

OT automates and controls production, monitors equipment, and ensures consistent quality while improving efficiency and reducing downtime.

Energy & Utilities

OT manages power generation, transmission, and distribution, helping deliver reliable and safe energy across infrastructure.

Water & Wastewater

OT controls treatment plants, pumping systems, and networks to ensure clean water supply and effective wastewater management.

Transport & Infrastructure

OT supports traffic systems, rail, airports, and logistics to keep people and goods moving safely and efficiently.

Healthcare & Public Services

OT manages medical devices and hospital systems, helping deliver safe, reliable care and improved patient outcomes.



Why OT Infrastructure Availability Matters

1. **Operational and financial impact**
Disruptions or downtime in OT systems can result in significant financial losses, including lost revenue, repair costs, and reputational damage.
2. **Safety risks**
Failures in OT systems can threaten the safety of employees, the public, and the environment, particularly in critical infrastructure settings.
3. **Cyber and data risks**
Cyberattacks on OT systems can lead to data theft, process manipulation, and long-term operational and competitive disadvantages.

Reliable OT infrastructure is critical for organisations across Australia and New Zealand, particularly as regulatory and compliance expectations continue to evolve globally and locally. While international frameworks such as the NIS2 Directive and the Cyber Resilience Act (CRA) are shaping global best practices, similar principles are reflected in ANZ through frameworks like the **Australian Cyber Security Centre (ACSC) Essential Eight, the Security of Critical Infrastructure (SOCI) Act, and NZISM/NCSC guidance** in New Zealand.

These standards emphasise strong risk management, secure supply chains, and resilient operations, all of which extend directly to OT environments.

Questions
about SOCI,
ACSC or
NCSC?

Contact us for
assistance!



OT Security:

A Structured Approach for ANZ

In ANZ, organisations are increasingly adopting [ISA/IEC 62443](#) as a proven framework for securing industrial automation and control systems. It provides clear, practical guidance to design, implement, and manage OT security across the lifecycle.

ISA/IEC 62443 is a global standard for securing industrial control systems, providing practical guidance to design, implement, and manage OT security.

The framework aligns with ANZ requirements such as the SOCI Act, ACSC Essential Eight, and NZISM, supporting stronger security across critical industries.

A structured, risk-based model helps identify vulnerabilities, prioritise controls, and continuously monitor environments to improve resilience and security.

It also supports alignment with international regulations like NIS2 and the CRA, helping organisations meet both local and global standards.

IEC 62443 Functional Requirements

FR	Description
FR1	Identification & Authentication Control
FR2	Use Control
FR3	System Integrity
FR4	Data Confidentiality
FR5	Restricted Data Flow
FR6	Timely Response to Events
FR7	Resource Availability

OT Security Use Cases:

Core Pillars of OT Security

A comprehensive OT security strategy requires a coordinated set of controls across people, processes, and technology. Built on a defence-in-depth approach, multiple layers of protection work together to reduce the risk of cyber threats impacting critical operations.

This approach combines physical, technical, and operational safeguards to create a resilient and secure OT environment.

Risk management Risk assessments, evaluations, and ongoing reviews	Asset visibility IT/OT asset discovery, inventory, and management	Threat detection Monitoring systems to identify and respond to threats	Endpoint security Antivirus, EDR, and device protection controls
Monitoring & intelligence Continuous monitoring and threat intelligence	Identity & access control User access governance and privilege management	Secure remote access Controlled, secure connectivity into OT environments	Network security Segmentation and secure IT/OT architecture
Vulnerability management Patching, configuration hygiene, and remediation	Resilience planning Backups, incident response, and business continuity	Supply chain security Managing risk across vendors, OEMs, and software (SBOM)	People & awareness Training and security awareness programs
Governance & assurance Policies, audits, penetration testing, and improvement			



Examples of a five-stage implementation of OT security principles

Asset Inventory & Visibility

1.

- Maintain a comprehensive and up-to-date inventory of all OT/ICS assets to understand what needs protection.
- Asset visibility is foundational for effective OT security and risk management.
- Even partial visibility is a starting point, but completeness and accuracy should be continuously improved.

Network Architecture & Segmentation (IT/OT)

2.

- Establish clear separation between IT and OT networks using an IT/OT DMZ, typically enforced with layered firewalls.
- Restrict data flows wherever possible. Ideally from OT to IT only, minimising inbound exposure.
- Apply further zone-based segmentation within OT environments (aligned to IEC 62443 zones/conduits) to limit lateral movement.

Incident Response Planning

3.

- Develop and maintain an OT-specific incident response plan to ensure structured, rapid response.
- Key considerations include:
 - Protection of personnel and physical safety
 - Defined internal and external escalation paths (including regulators where required)
 - Rapid restoration of critical control systems (e.g., PLCs)
 - Minimising operational downtime and restoring production safely

Backup & Recovery

4.

- Implement secure, regularly tested backups of OT systems and configurations.
- Ensure backups are complete, stored securely (offline where possible), and aligned to recovery priorities.
- Maintain documented recovery procedures and routinely validate recovery capability.

Continuous Vulnerability Management

5.

- Apply an OT-specific approach to vulnerability management, recognising operational constraints.
- Key activities include:
 - Identifying vulnerabilities across OT assets
 - Reviewing vendor risk ratings and advisories
 - Assessing real-world impact on safety and operations before remediation



The SecurOT Centre Of Excellence

OT capability is fragmented across siloed partners. The OT Centre of Excellence is a control tower that orchestrates governance, architecture and the partner ecosystem to deliver OT outcomes safely and at scale. The CoE is the neutral layer that unites them around the customer outcome.

What the CoE does. Four pillars

01

Governance & Assurance

Policy, controls, compliance and audit readiness. Risk prioritised by operational impact, not generic scoring.

02

Architecture & Security Patterns

Approved reference architectures and resilience patterns that turn one-off complexity into reusable capability.

03

Ecosystem & Partner Program

Partner segmentation, qualification, joint roadmaps and co-delivery models — everyone clear on their role.

04

Vendor Portfolio: Building Blocks

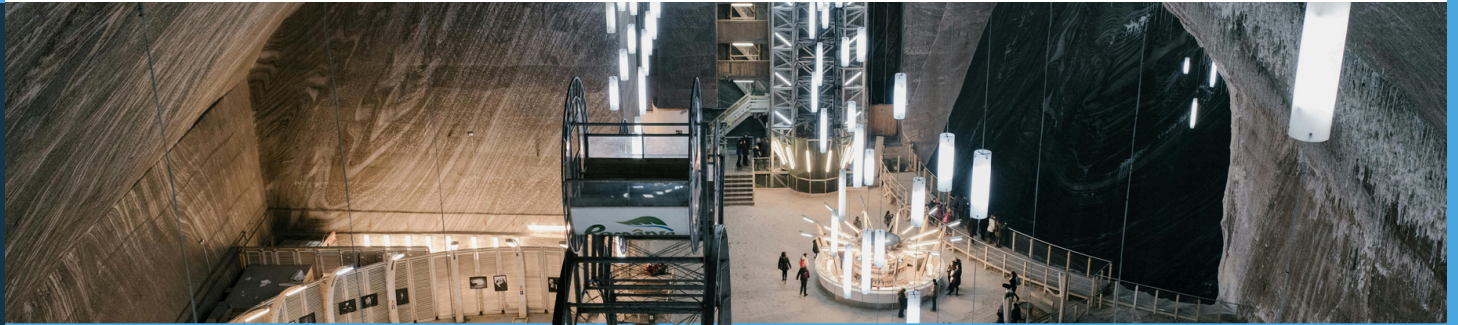
Technology on-ramped deliberately, by use case and positioned by role, to prevent platform sprawl.

WHAT THE CoE IS

- A governance, safety and scale mechanism
- An outcome referee, not a delivery team
- A way to de-risk OT engagements
- A way to make multi-partner delivery repeatable

WHAT THE CoE IS NOT

- A permanent delivery layer
- A replacement for partners
- A single vendor control function
- A bottle neck as maturity grows



How do we help you win with the CoE?

In OT, customers don't buy products, they buy uptime, safety and resilience. We help you lead that conversation and turn operational risk into qualified pipeline.

WIN THE OT CONVERSATION

Lead the customer journey

Engage on outcomes, not products.

- **Outcomes first** — anchor every conversation in operational risk reduction, not features.
- **Availability & safety win** — legacy systems and low downtime tolerance make OT a different discipline to IT.
- **Reframe the question** — move from “What tools do you need?” to “What risk must be reduced, and why?”
- **Get in early** — lead with the asset owner; people and process before product; anchor in a use case (compliance, asset discovery, segmentation, secure access).

WIN WITH THE CoE

One coherent OT story

Your orchestration control tower.

The OT Centre of Excellence orchestrates governance, architecture and the partner ecosystem so outcomes are delivered safely, consistently and at scale.

- **Reference architectures** — proven, patterns instead of one-off designs.
- **Use-case-led sales plays** — repeatable plays mapped to real OT outcomes.
- **Partner capability alignment** — the right roles, sequenced; vendors positioned by role.
- **Engagement governance** — a consistent, trusted model across every partner.

How the CoE works alongside you:

Three modes of involvement

Step-In

HIGHEST TOUCH

We stabilise, de-risk and set the rules of engagement in early, high-risk, low-maturity environments.

Step-Along

SHARED

We orchestrate use cases and build repeatability as you scale. Outcomes delivered side by side.

Step-Back

LOWEST TOUCH

You run independently and the CoE governs by exception. Less visible as success grows.



The Customer OT Security Journey

- 1. Discover — Asset visibility & risk baseline**
Build a full OT asset inventory and risk profile first. You can't protect what you can't see.
- 2. Protect — Segmentation & secure access**
Apply IEC 62443 zones and conduits, harden remote and vendor access, and separate OT from IT.
- 3. Detect — OT-aware threat monitoring**
Continuous monitoring tuned to OT protocols surfaces anomalies without disrupting operations.
- 4. Respond — Incident readiness & recovery**
Playbooks, backups and tested recovery so an incident never becomes downtime or a safety event.
- 5. Govern — Continuous compliance & maturity**
Ongoing assurance against SOCI and IEC 62443, with maturity uplift and board-ready reporting.

OT Security:

Compliance Crosswalk

Requirement Area	SOCI Act	Essential Eight	IEC 62443	SecurOT Capability
Asset Visibility	✓	Partial	✓	Asset Discovery
Network Segmentation	✓	Partial	✓	Network Security
Identity Management	✓	✓	✓	PAM & Zero Trust
Threat Monitoring	✓	Partial	✓	OT Detection
Incident Response	✓	Partial	✓	IR Planning
Backup & Recovery	✓	✓	✓	Resilience Planning
Vulnerability Management	✓	✓	✓	Exposure Management
Supply Chain Security	✓	Partial	✓	Vendor Risk

Want to become self sufficient? Bespoke training with Wavelink

SecurOT Sales Bootcamp

This workshop is designed for sales professionals who want to strengthen their ability to sell into Operational Technology (OT) environments.

Whether you are new to OT or looking to refine your approach, the session will give you the knowledge and practical skills needed to differentiate OT from IT, position the right solutions, and connect OT security directly to business value.

Find out more!



SecurOT Visibility Foundations

Find out more!



The OT Asset Visibility workshop is designed to educate participants on the challenges of achieving complete visibility in Operational Technology environments and why it is foundational for industrial cybersecurity.

Using our vendor portfolio, this session provides an in-depth understanding into utilising industry-leading platforms and visibility solutions to deliver secure, resilient operations.

OT Services Portfolio

Technical Services



Pre-Sales Consultation

Our experts will be glad to answer your technical or architectural questions and support you right at your customer's premises.



End Customer Support

Our experts will be glad to answer your technical or architectural questions and support you right at your customer's premises.



Demo/PoC Support

We can provide the necessary test devices/licences for demo and evaluation purposes. If desired, we also support longer periods (PoC).



Installation

We offer support to ensure installation and configuration of new solutions goes smoothly, or we can take on these tasks entirely



Post-sales support

We are able to relieve your technical department by providing fast support for solutions purchased from us for the majority of our portfolio.



Config review

You are using security solutions from Wavelink. Our specialists will help you check the configuration and further optimise it.

Training Services



Certification training

We can train you employees the necessary certifications so you can benefit from partner programmes.



Technical workshops

If practical knowledge is more important to you than certifications, our technical workshops offer the perfect format for your technicians to develop their knowledge.



Sales Training

In addition to technical training, we regularly organise sales training courses and webinars on the latest IT/OT security topics.

Sales and Marketing



Lead Generation

We can assist in generating end customer leads for you on a campaign-related basis or offer support with customer acquisition for events



Renewal Support

With our renewal tracking system, we can ensure that you never miss an upcoming service renewal for your end customers



Marketing campaigns

We will help define and implement a lead to cash process tailored to your needs.



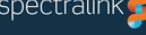
Events

We support your marketing team in organising and coordinating the manufacturers involved.



We cover the **entire** attack surface.

As a leading value-added distributor, Wavelink supports OT security by taking a holistic approach and providing the appropriate services.

	Network Segmentation	IoT/OT Asset Discovery	Endpoint Protection	Network Monitoring	Secure Remote Access	Rugged Hardware	Incident Response	Identity Management	Supply Chain Security	Fault Tolerance	Data Integrity	Threat Intelligence	Network Architecture	Post Quantum Crypto
 censys		✓		✓			✓	✓	✓			✓		
 CLAROTY	✓	✓	✓	✓	✓	✓		✓	✓					
 FORTINET	✓	✓	✓	✓	✓	✓	✓	✓	✓					
 GARLAND TECHNOLOGY				✓		✓								
 Honeywell						✓								
 imprivata							✓							
 PENGUIN SOLUTIONS						✓			✓					
 SOTI			✓			✓	✓	✓						
 spectralink						✓								
 FRENOS		✓		✓	✓									
 Trellix			✓	✓				✓						
 tributech								✓		✓				
 CYBLE						✓		✓						
 acromove						✓			✓					
 GXC												✓		
 CERTES													✓	
 Quintessence Labs													✓	

Asset Visibility and Threat Detection



Unmatched Asset Visibility

OT-centric security suite for asset discovery, vulnerability management, and threat detection. Distinguished by deep protocol inspection and out-of-band monitoring.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



OT Digital Twin

OT security posture platform detecting adverse behaviour, protecting industrial control systems. Agentic AI for legacy OT, delivering detection without disruption.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



Continuous Penetration Testing as a Service

CREST-certified Pentest-as-a-service platform and automation with expert manual testing. Continuous testing delivers recurring risk prioritisation.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

Network Protection & Segmentation



The Unified Threat Protection Fabric

Industry-leading firewall and zero-trust platform securing network edges and VPN access. Unified Security Fabric that provides single-pane-of-glass management.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



Full Stack Visibility into Network Traffic

Passive taps and packet brokers delivering full-stack visibility into network traffic. With high-performance distributed architecture that avoids single point of failure.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

External Exposure and Threat Intelligence



Operational Threat Intelligence

Unified SOC delivering detection and response across endpoint, network, email and cloud. AI-driven correlation & global threat intelligence for faster response.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



Authoritative Global Internet Map

Internet-wide attack surface management for real-time asset discovery and risk assessment, using continuous scanning and a searchable global dataset.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



Dark Web Threat Intelligence

Dark web threat intelligence delivering real-time monitoring of exposed assets & credentials with AI-driven risk scoring and threat feed for proactive defense.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

Operational Platforms & Data Exchange



Healthcare Orchestration

Healthcare comms and alarm orchestration improving clinical response and workflows. Deep integration into hospital systems and IoMT ecosystems.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



Establish Trust in Every Data Point

Data notarization middleware that creates trust and integrity in every IOT/OT datapoint. Supports compliance initiatives for critical infrastructure (e.g. SOCI).

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

Rugged Devices and Handsets

Honeywell

Rugged Mobile Computing

Rugged mobile computing and barcode-scanning devices for frontline operations. Differentiated by MIL-STD-certified durability and multi-OS flexibility.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



Enterprise wireless handsets

Enterprise wireless handsets enabling secure, mobile communications in regulated environments. Certified for compliancy and purpose-built for rough handling.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

Operational Mobility and Connected Workforce

SOTI

Mobility Management made easy

Mobility management platform for securing and managing devices at scale. Differentiated by its single-agent architecture and support for diverse IoT.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

imprivata

Clinical IAM

Healthcare IAM and single-sign-on solution streamlining secure clinical workflows. Leveraging context-aware access and soft-token authentication.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

Industrial Connectivity & Edge Computing



Private Mesh Cellular Stack

Private LTE/5G networks for enterprise, industrial, and high-bandwidth operations. Fully integrated private mesh-based cellular stack without carrier dependencies.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



Fault Tolerant Edge Compute

Fault-tolerant industrial compute appliances guaranteeing nonstop uptime. Powered by active-active redundancy without any application changes.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



Data Centre on the move

Portable fly-away datacentre and edge-cloud kits with private 5G and high-resilience compute. Ultra-deployable, self-contained, operational in minutes.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

Data Security and Post Quantum Cryptography



Post-Quantum Resilience

Crypto-agile data protection securing organisations against current & post-quantum threats. Full-stack approach to signing, encryption, and key management.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7



**Quintessence
Labs**

Quantum Random Number Generator

High speed quantum random number generation that can be leveraged for Post-Quantum Cryptography (PQC) projects. Physics-based quantum key distribution.

IEC62443 Functional Requirement

FR1 | FR2 | FR3 | FR4 | FR5 | FR6 | FR7

How We Scale Together

Engaging with Wavelink

Your engagement path

- 1 Connect**
Align on target accounts and OT opportunities.
- 2 Assess**
Joint discovery on risk, compliance and maturity.
- 3 Plan**
Map use cases, partner roles and the sales motion.
- 4 Co-deliver**
Execute with OT CoE support to de-risk delivery.
- 5 Scale**
Repeat proven plays as your OT practice matures.

Take the next step

- **Bring us in** early on your next OT opportunity.
- **Book** a joint OT discovery session to scope outcomes.
- **Contact** your Wavelink OT team to get started.
- **Join** one of our public OT training sessions.

About Wavelink Communications

Wavelink, an Infinigate Group company, is a leading value-added distributor and trusted advisor across Cybersecurity, OT, Cloud, and Network Infrastructure in the ANZ region.

Backed by the global strength of the Infinigate Group, operating in over 100 countries and generating €2.3B in FY23–24. Wavelink combines local expertise with international scale to help partners accelerate growth and seize new market opportunities.

Our specialised focus on cybersecurity, secure networking, and secure cloud solutions for both SMB and enterprise organisations sets us apart. Through deep technical expertise, tailored local support, and access to Infinigate's robust global supply chain, we empower our partners, MSSPs, and vendors to deliver secure, high-value outcomes and drive long-term success.

Wavelink Communication Pty Ltd

1/318 Auburn Road, Hawthorn, 3121, Australia

sales@wavelink.com.au

www.wavelink.com.au

