SecurOT

DADS Box (Digital Asset Discovery)

Find out rapidly what is operating on your network with minimal distruption and a clar actionable view of your critical assets.

This service empowers your organisation to gain immediate insights into your security posture, prioritise remediation efforts, and lay a robust foundation for future cybersecurity initiatives, such as continuous monitoring through an OT Security Operations Centre (SOC).

Regulatory Alignment

- Meet SOCI Act's requirement for thorough asset inventories, helping to demonstrate compliance and proactively reduce audit fatigue.

Operational Uptime

- Identify hidden or rogue devices and vulnerabilities before they cause outages or degrade production.

Cost-Effective Starting Point

- Gain immediate visibility with minimal disruption. No heavy forklift upgrades required to begin discovering and securing assets.

Scalable to Full OT SOC

- Seamlessly expand from asset visibility to a fully managed OT SOC service with 24×7 monitoring, threat detection, and incident response.

Book a Demo

Wavelink Communications
Unit 1/318 Auburn Rd,
Hawthorn VIC 3122

(03) 9832 4444
sales@wavelink.com.au
www.wavelink.com.au

wavelink
an Infinigate Group company

SecurOT

Why Digital Asset Discovery Matters

Many organisations operating critical infrastructure struggle with maintaining a clear, up-to-date inventory of their OT and critical assets. This lack of visibility leaves them vulnerable to unpatched systems and undiscovered threats. With the increasing integration of traditionally air-gapped OT systems into broader IT networks, the risk of cyber threats escalates, making comprehensive asset discovery a necessity for safeguarding your operations.

The Digital Asset Discovery service is designed for rapid deployment and minimal disruption, providing you with a clear and actionable view of your OT and critical assets. The approach is structured around three key phases:

Rapid Deployment

Comprehensive Identification

Detailed Reporting

Core Service Value and Key Benefits

Identification
The service scans the network to identify all OT devices, such as programmable logic controllers (PLCs), remote terminal units (RTUs) and other industrial control systems.

Non-Disruptive
The discovery process is non-intrusive, meaning it does not disrupt the normal operation of the OT devices.

Cataloguing
Once identified, the devices are catalogued with detailed information, including firmware versions, serial numbers and other relevant metadata.

Security Baseline
By providing a comprehensive inventory of OT assets, the service helps in implementing effective cybersecurity measures, change management and managing vulnerabilities.

Compliance
Ensures that the organisation meets regulatory and compliance requirements by maintaining an accurate and up-to-date asset inventory.

SecurOT

Adressing Customer Challenges

Incomplete Asset Visibility

OT/ICS environments often have decades-old equipment, shadow devices, and vendor systems. A lack of clarity on what's running in the environment creates blind spots and vulnerabilities.

Increased Regulatory Pressure

Australian SOCI Act obligations demand thorough asset inventories and risk assessments, but many organizations don't have a credible, continuous source of real-time asset data.

Limited Resources & Expertise

Teams often struggle to manage security on top of their day job (plant operations, maintenance, etc.). They need a turnkey solution that quickly identifies assets without significant internal overhead.

Cyber & Operational Risk

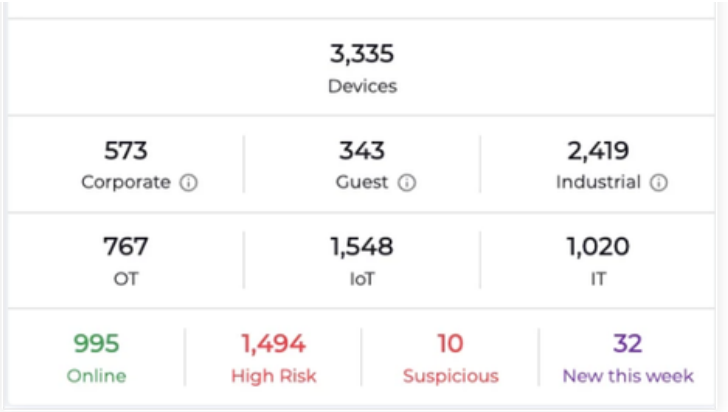
Without clear visibility, organisations risk undetected vulnerabilities and potential disruption to critical operations, leading to financial losses, reputational damage, and safety incidents.

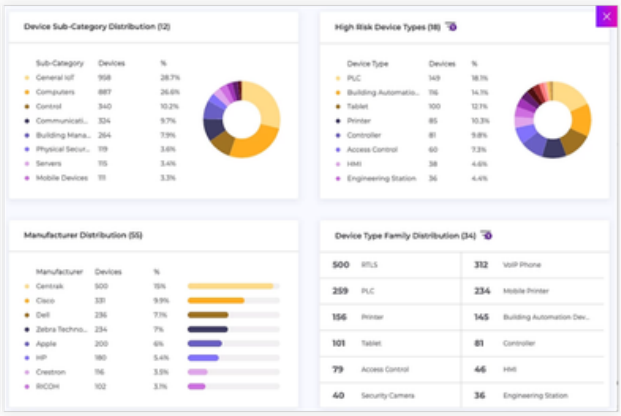
SecurOT

The Digital Asset Discovery Solution

Typically runs for 30 days with the following outputs:

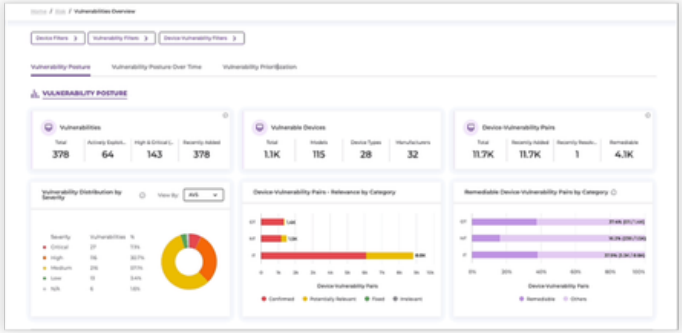
Automated Discovery & Classification
Deploy lightweight sensors (or agentless scanning) to map all connected devices, from PLCs, SCADA servers, and HMIs to IT network devices. Rapidly build a real-time asset inventory that classifies devices by make, model, firmware, and criticality.

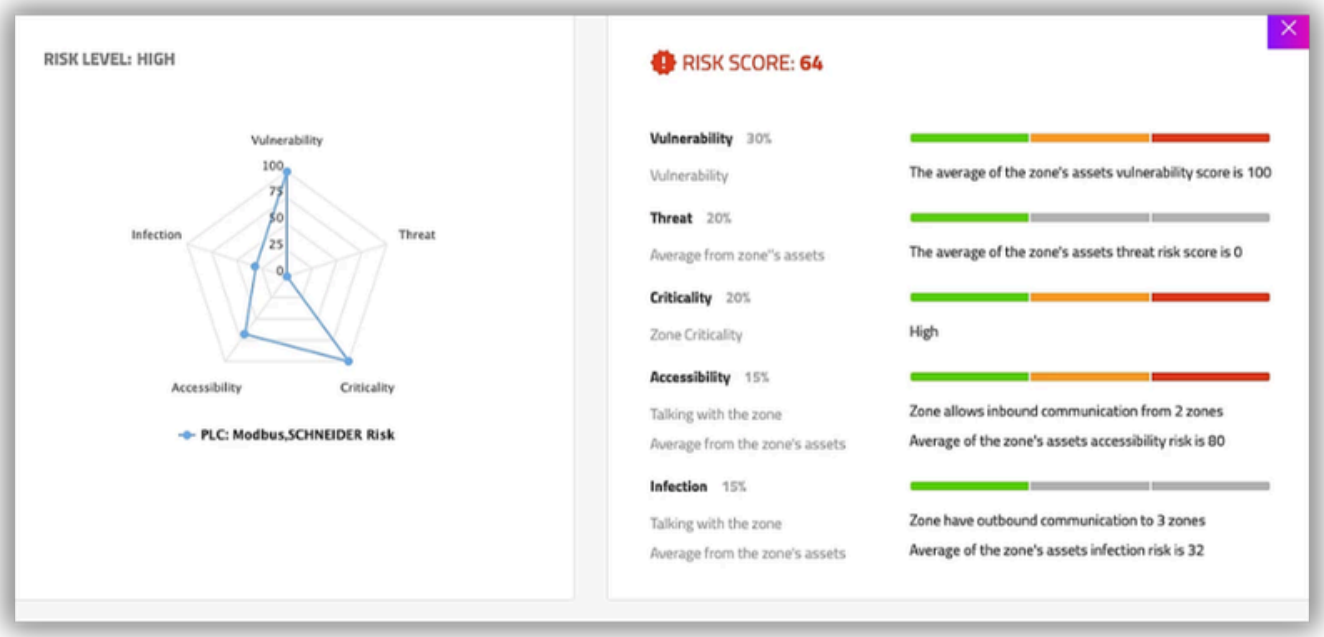




Continuous Monitoring & Alerts
Ongoing discovery ensures that any new or transient devices are captured. Receive alerts for unauthorized additions or changes (e.g., firmware updates, new vendor laptops).

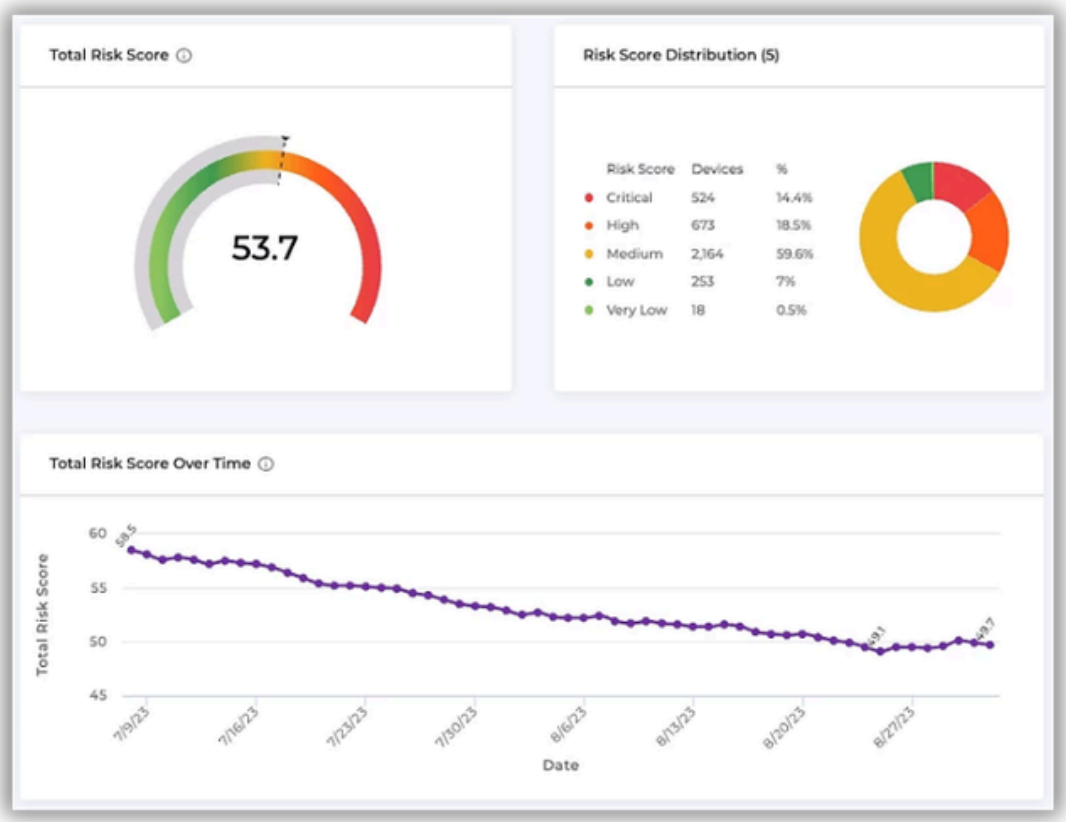
Actionable Reporting & Dashboards
Clear, executive-level dashboards and technical drilldowns. Prioritise remediation steps (e.g., patch updates, network segmentation needs) aligned with compliance frameworks.





Qualitative risk assessment

As part of the service offered, a Qualitative Risk Assessment that evaluates risks based on high level subjective criteria defined, rather than numerical values. This approach will help understand, at a high level, the potential impact of threats and vulnerabilities in a more descriptive and context-specific manner over the various assets.



SecurOT

What the DAD's Box Finds

Asset Attributes Captured

Depending on device type, DADs Box can provide visibility into, but not limited to:

- Asset type and classification
- Vendor, make and model
- Firmware and software versions
- IP and network information
- Communication protocols
- Asset criticality
- Location or network segment
- Operating system details
- Serial numbers and device identifiers
- Vulnerability exposure
- Configuration change indicators
- Asset ownership and responsibility
- Device relationships and dependencies
- Lifecycle and support status

Why This Matters to Different Stakeholders

CISO / Cyber Security Teams

Unknown assets create unknown risk.

- Find unmanaged and rogue devices
- Prioritise remediation based on risk
- Improve vulnerability management
- Establish a defensible OT security baseline

Risk & Compliance Teams

Show compliance without manual audits.

- Support SOCI obligations
- Accelerate audit preparation
- Maintain accurate asset inventories
- Produce evidence for regulatory reviews
- Executive Leadership

OT Managers & Operations Teams

Maintaining uptime.

- Understand what is connected to production environments
- Reduce operational blind spots
- Identify unsupported or outdated assets
- Improve change management

Engineering & Maintenance Teams

Limited visibility into device lifecycle.

- Track firmware versions
- Identify unsupported equipment
- Improve maintenance planning
- Reduce unplanned outages

SecurOT

Key Benefits

Enhanced Security Posture

- Gain Immediate insights to prioritise remediation and strengthen your overall cyber security defences
- Rapidly identify and mitigate potential threats in your operational technology environments

Immediate Decision Making

- Detailed findings on asset types, firmware/software versions, and high-risk exposures enable strategic security planning
- Effectively prioritise remediation efforts based on asset health scores and risk assessment
- Achieve a complete inventory of all OT and critical assets, including those previously unknown.

Compliance and Future Readiness

- Facilitate compliance with regulations like the Australian Security of Critical Infrastructure (SOCI) Framework
- Prepare for future security demands with a clear remediation roadmap
- Streamline compliance reporting and demonstrate adherence to regulations
- Roadmap for longer-term security initiatives, potentially feeding into an OT SOC or managed security programs.

Ordering SKU

ITEM	SKU
DADs Box - Digital Asset Discovery Service	WL-DADS-PACKAGE-01

Book a Demo

Wavelink Communications
Unit 1/318 Auburn Rd,
Hawthorn VIC 3122

(03) 9832 4444
sales@wavelink.com.au
www.wavelink.com.au

wavelink
an Infinigate Group company