



See every bit, byte, and packet®

Achieving Network Visibility in Your ICS/OT Environment

January 19, 2022, 1:30 PM London Time



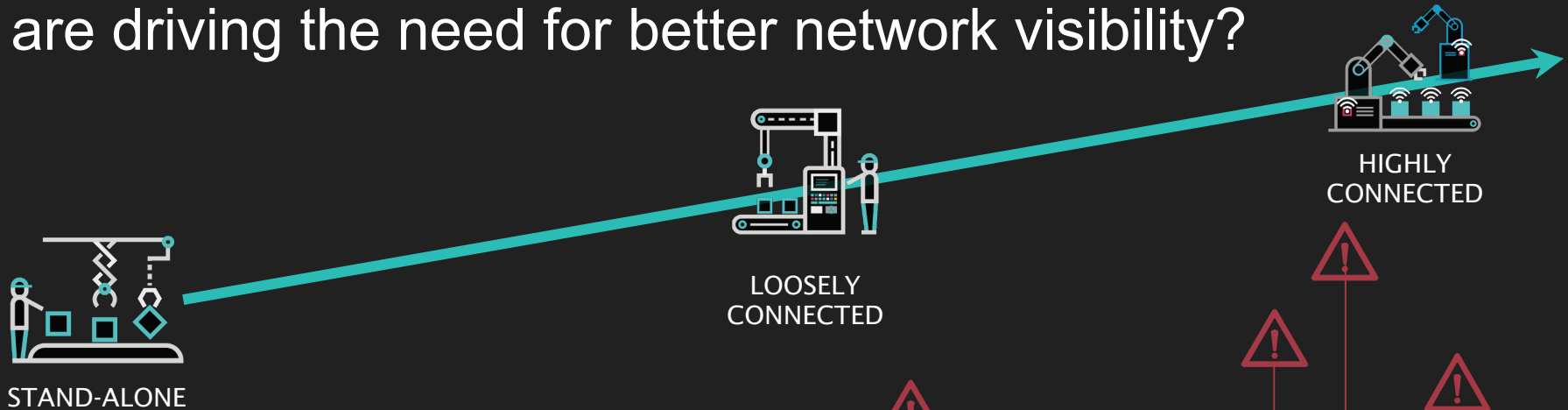


Dragos has a global mission: to safeguard civilization from those try to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience. Dragos codifies the knowledge of cybersecurity experts into an integrated software platform that provides customers **critical visibility into ICS and OT networks** so that threats are identified and can be addressed before they become significant events.



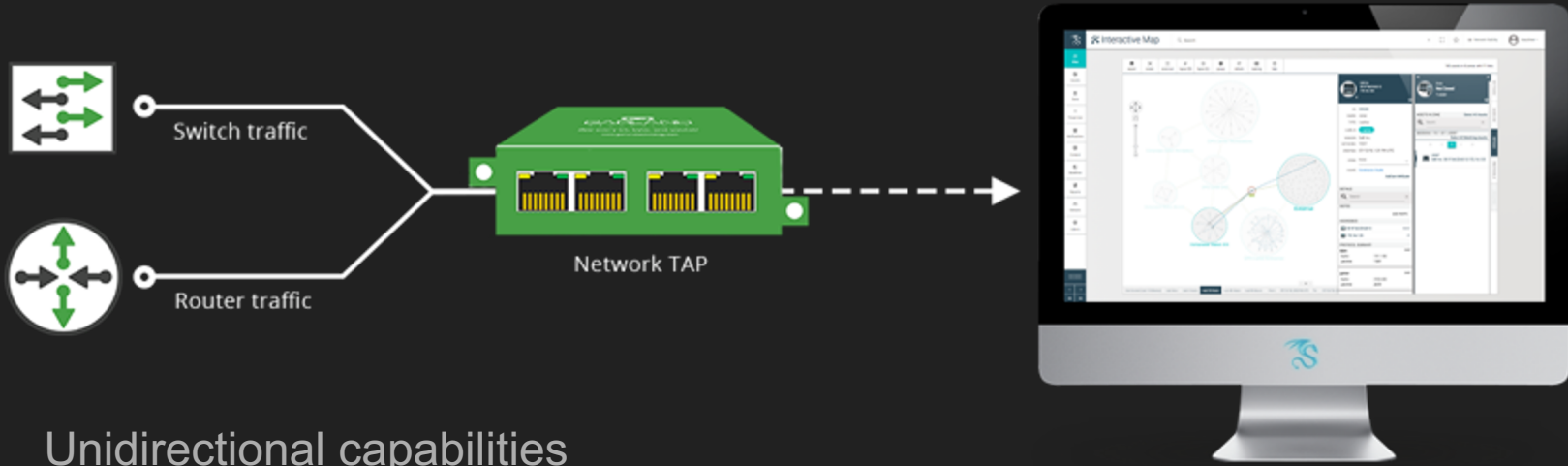
Garland Technology is an industry leader of **IT and OT network solutions** for enterprise, critical infrastructures and government agencies worldwide. Since 2011, Garland Technology has been engineering and manufacturing simple, reliable and affordable Network TAPs and Network Packet Brokers.

What changes are we seeing in ICS/OT environments that are driving the need for better network visibility?



- Digital Transformation
- Increased integration of IT and OT environments
- Greater adoption of intelligent/edge compute devices deeper in the facility
- Increase in remote access/remote operation capabilities

Explain the benefits of leveraging a network TAP fabric in industrial environments to provide visibility.

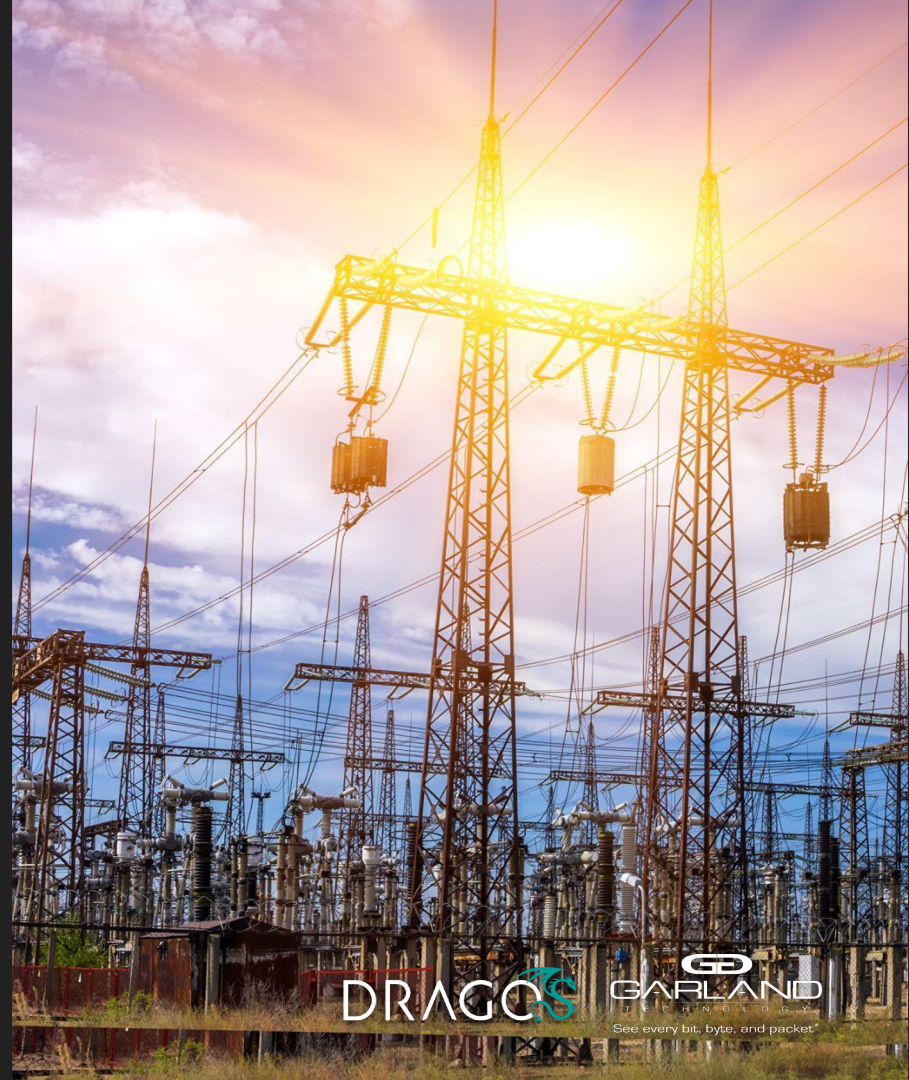


The Dragos Platform

- Unidirectional capabilities
- Provide packet visibility to multiple solutions
- No need to upgrade switching fabric
- Cost efficiencies

Describe how an organisation can **use this visibility to improve** both their operations and cyber security programs.

- Asset inventory
- Validation of defensible architectures
- Capacity planning
- Behaviour monitoring
- 360° visibility





Explain how organisations can **accelerate the maturing** of their ICS/OT cybersecurity program.

- Consolidation of security stack
- Maximisation of investment


DRAGO 


GARLAND
TECHNOLOGY
See every bit, byte, and packet[®]

Supply chain attacks are a growing form of cyber security threats. What makes **supply chain attacks** so challenging to find and identify?

- Attack vs vulnerabilities
 - Solarwinds
 - Log4J
 - WindRiver
 - OEM whitelabel
- Unknown vendor quantities





What are the consequences of doing nothing?

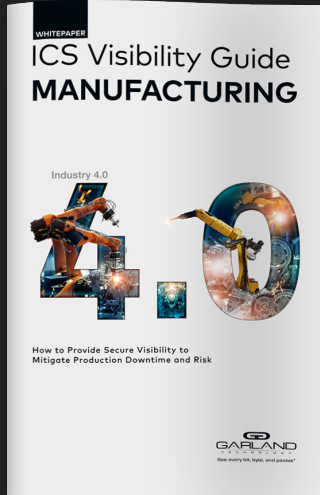
- Business impacts
- Downtime costs money
- Slows down the manufacturing or production process
- Uncertainty whether it is an IT or OT issue without visibility

In Review: Dragos and Garland Technology

- Minimise risks to the ICS/OT environment
- Maintain optimal device utilisation
- Reduce network downtime and monitoring solution deployment time
- Comprehensive asset visibility enabling detection of ICS/OT security threats
- Ensure network infrastructure reliability is maintained and implementation costs for monitoring solutions are minimized



Free Resources



Industrial Control Systems Visibility Guide: Manufacturing

[DOWNLOAD NOW](#)



See every bit, byte, and packet®



10 Ways Asset Visibility Builds the Foundation for OT Cybersecurity

[DOWNLOAD NOW](#)



Enhanced Security and Visibility Against ICS/OT Threats

The changing cyber threat landscape is impacting the management of ICS/OT environments, making the need for **passive, real-time monitoring** more urgent than ever.

See how Dragos and Garland Technologies provide advanced protection for your operations.

[LEARN MORE](#)



DRAGO
SAFEGUARDING CIVILIZATION

GD
GARLAND
TECHNOLOGY
See every bit, byte, and packet®

Thank You



Josh Carlson
Senior Business
Development Manager
jcarlson@dragos.com



Jason Farmer
Solutions Architect
jfarmer@dragos.com



Neil Wilkins
EMEA Technical Manager
neil.wilkins@garlandtechnology.com

