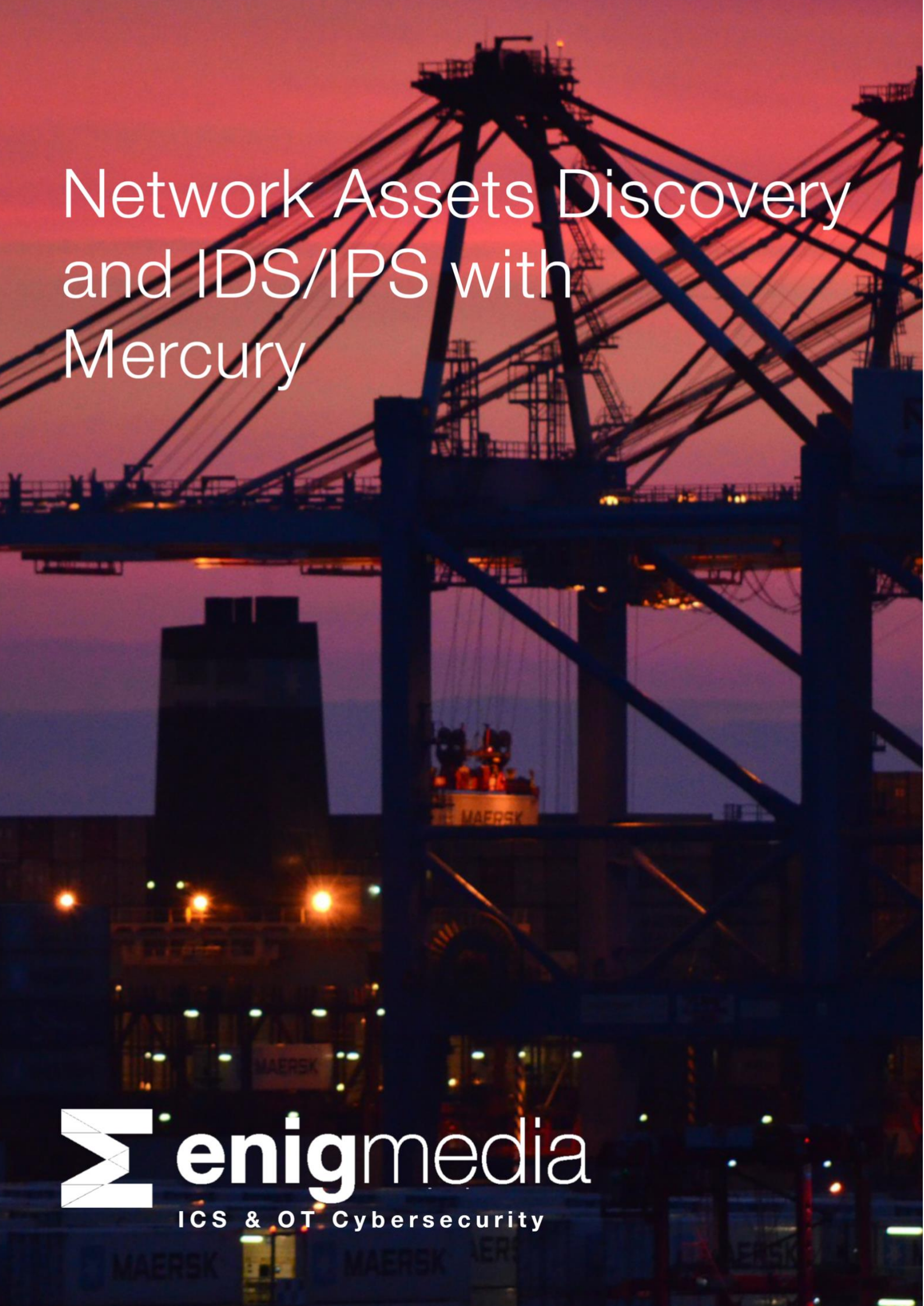


Network Assets Discovery and IDS/IPS with Mercury

enigmedia

ICS & OT Cybersecurity

Network Assets Discovery and IDS/IPS with Mercury

Nowadays, industrial companies and critical infrastructures are developing their digitisation strategies towards Industry 4.0, and cybersecurity is a prerequisite for digital transformation.

The roadmap for digitisation starts with the definition of the *Security Plan*, which includes an audit of the industrial control network in order to know existing infrastructure with identification of devices and their connections to assess potential system vulnerabilities enabling further plans and actions.

Companies facing this challenge are performing "Network Assets Discovery and Inventory", consisting on monitoring the ICS network traffic to:

- Identify network elements
- Discover communications between devices and protocols
- Categorize network elements

After knowing and understanding network traffic, companies can elaborate an Action Plan to implement security measures and mitigate cyber risks.

The most common technique to get *network knowledge* is to deploy appliances connected to network switches to capture traffic and analyze it.

This technique is called Port Mirroring or SPAN (Switched Port Analyzer) and it is done enabling port mirroring feature on the switch (or switches). Once enabled, the switch sends a copy of all network packets seen on the port to another port, where the packet can be managed (captured and analyzed or sent to be analyzed remotely).

Deploying these solutions requires installing dozens (when not hundreds) of network appliances along the industrial network. Based on current available solutions, this deployment represents a massive investment for the customer.

To solve this budget gap, Enigmedia proposes Mercury, the "all-in-one" industrial cybersecurity appliance designed to support industrial customers along their cybersecurity and digitisation journey.

Are you planning to start a "Network Discovery/Inventory and IDS/IPS" project? Contact Enigmedia to enjoy a cost-effective solution, improve your ROI, and get a future-proof solution with Mercury.

Save up to 70% in your Network Assets Discovery project with Mercury!

Mercury Box is an appliance that is deployed connected to network's switches to capture all network packets using Port Mirroring. Then, Mercury encrypts all traffic adding no-latency (less than 1ms!) and sends all packets to one unique central service for discovery, inventory, and IDS/IPS analysis, reducing exponentially the investment in appliances and licenses. Mercury offers LTE (3G/4G) connectivity, so network traffic and production data can be sent to any remote facility (or cloud) for IDS and data analytics.

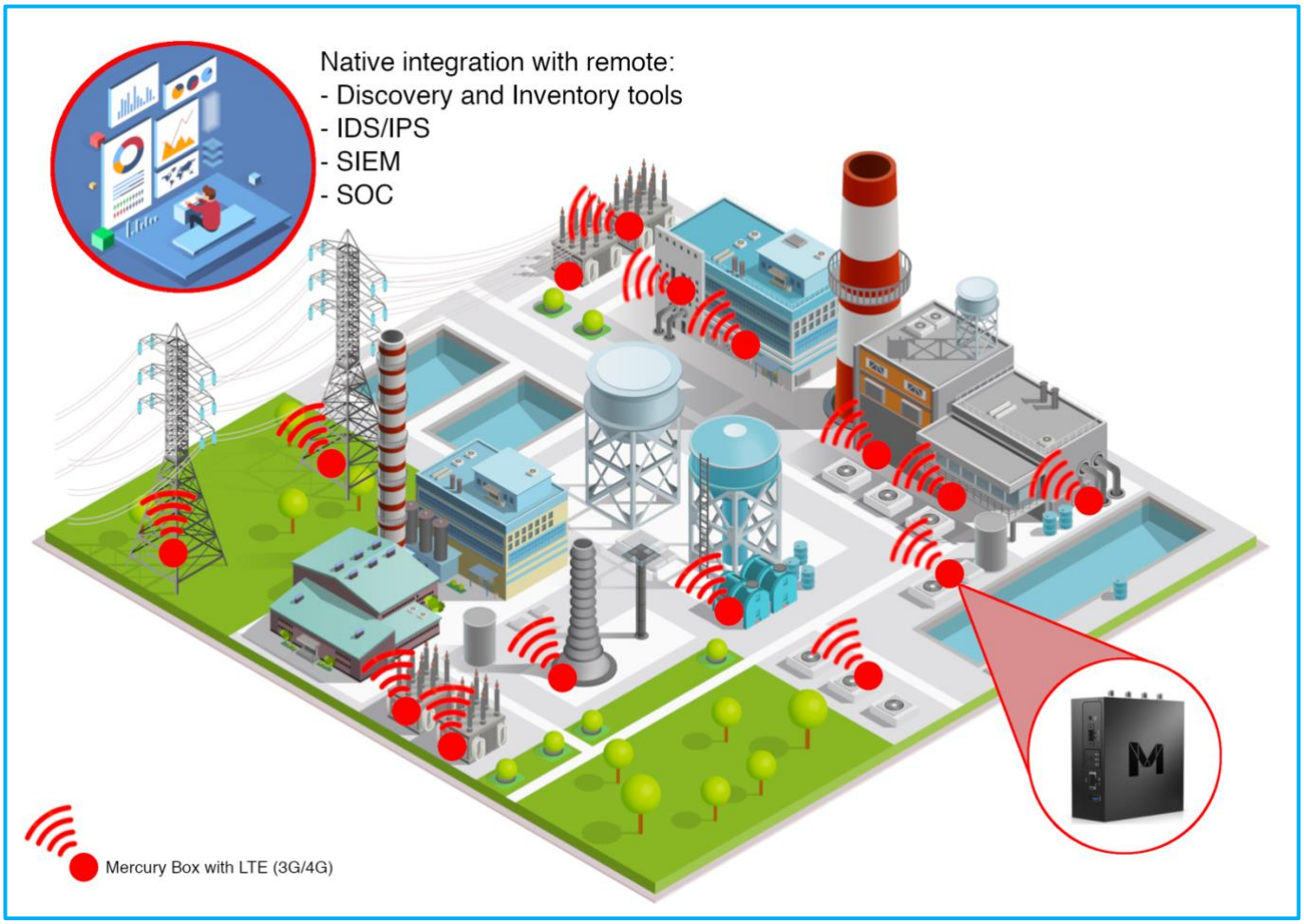
Mercury: Best ROI with future-proof solution

Mercury is compatible with all existing discovery and inventory solutions, so we propose to deploy Mercury Box appliance connected to network's switches to extract, encrypt, and send data.

Mercury Box offers:

- Data capture from switches by Port Mirroring
- Encryption of Captured Data and Communications
- Data-handling: data delivery to remote central discovery and inventory application via LTE (3G/4G)
- Integration with IDS/IPS solutions
- Integration with SIEM solutions
- Integration with SOC services

In addition, Mercury Box is much more than that. Mercury Box appliance is an "all-in-one" cybersecurity solution designed with CISOs and CIOS to secure industrial systems (ICS/OT/IoT).



Best ROI with future-proof solution

After discovery and inventory, industrial companies and critical infrastructures need more cybersecurity features to protect their networks. Following Best Practices and Standards (i.e. IEC-62443, ISO, NIST), customers shall implement more cybersecurity measures to enjoy a high-end secured network, including:

- Network Segmentation
- Firewall
- Conduits definition
- Devices Hardening
- Full Encryption

Mercury offers all these features in just one box!

Keep on securing your network with Mercury

Mercury Box, best-in-class "Plug&Protect" appliance, is the best tool for your industrial cybersecurity strategy.

After assets discovery and inventory, what else can be done with Mercury?

Once deployed, Mercury builds an encrypted network hiding all devices and protocols and avoiding cyberattacks. Attackers cannot get information from network elements, so they cannot exploit devices' vulnerabilities.

Mercury, Native Cybersecurity for Industrial Systems

Enigmedia builds native cybersecurity solutions to enable digitisation towards Industry 4.0. Enigmedia delivers essential building-blocks for secure digital transformation. Enigmedia follows IEC-62443 in its product strategy. For further information and to explore all our ICS Cybersecurity Portfolio, please contact us at:

contact@enigmediasecurity.com