DEEPINSPECT

DEEPINSPECT
OT CYBERSECURITY LIKE NEVER BEFORE

THE BUSINESS CHALLENGE

OT (Operational Technology) security poses a critical challenge for companies managing industrial and production infrastructures.

Protecting these systems and physical devices, which control essential processes in sectors like manufacturing, energy, and transportation, from cyberattacks is crucial. **OT environments frequently rely on legacy technologies not originally designed with cybersecurity in mind**, making them susceptible to **advanced threats**. The integration with IT (Information Technology) systems further compounds the risk, necessitating a **comprehensive security strategy** that covers both physical and digital aspects. Companies must navigate the delicate challenge of balancing innovation and digital transformation with the need to ensure operational continuity and robust security, all while managing limited resources and adhering to increasingly stringent regulations.

The stakes are high, as the growing sophistication of cyberattacks and the imperative to maintain uninterrupted operations mean that **any disruption could result in severe economic losses and public safety hazards**.

THE SOLUTION

DeepInspect simplifies complex OT cybersecurity challenges by providing methodology, hardware and software in a unified approach.

Our approach integrates **cybersecurity expertise**, focused on Operational Technology (OT), **with military insights** to enhance protection for critical infrastructures, particularly in the industrial sector. By combining these strengths, we streamline **Threat Detection and Asset Discovery processes**.

Leveraging its **asset identification capabilities**, DeepInspect swiftly identifies cybersecurity threats, detecting suspicious activities, anomalous behaviors and potential risks. The platform seamlessly integrates with third-party systems like SOC/SIEM or risk analysis tools.

DeepInspect is engineered for versatility, **operating effectively in air-gapped environments** without internet connectivity, ensuring maximum reliability and security without sacrificing performance.

The Italian engineered solution is patented and designed by cybersecurity experts with over 20 years of International experience included Government and Defence sector.

Application Areas

- Navy / Maritime
- Energy
- Transportation
- Oil and Gas
- Government and Critical Infrastructures
- Industry 4.0
- Healthcare
- Airports

Why Deepinspect

Patented solution

Type-approved hardware certified for energy, transportation and maritime application

Generate alerts using Anomaly Detection based on network segment communication patterns

Automated Asset Discovery in OT environments for improved network visibility

Ability to operate effectively even in air-gapped environments

Possibility of third-party system integration such as SOC/SIEM or risk analysis tools

DEEPINSPECT SOLUTION OVERVIEW

The DeepInspect solution is carefully designed to ensure comprehensive cybersecurity across the entire OT environment with each of its components fulfilling a distinctive role in defense against OT cyber threats. DeepInspect's architecture seamlessly integrates **physical devices**, **virtualized environments**, and **advanced management software**, all working together to deliver secure and uninterrupted operations.

This approach guarantees flexibility and scalability, enabling tailored solutions for various environments.
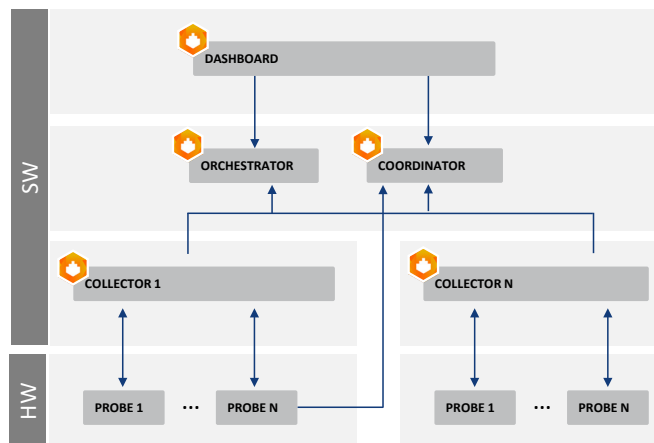
DEEPINSPECT SOFTWARE

The DeepInspect virtual devices are key components of the solution architecture, as they allow for **full visibility over the entire OT Environment** and provide complete governance of all involved probes, assets, devices and information.

DASHBOARD

The **DeepInspect Dashboard** offers a comprehensive overview of assets, communications, protocols, and anomalies, giving operators centralized access to analyze the OT environment and quickly identify potential threats.

Main functions:
- Displays processed data graphically.
- Allows for real-time monitoring and analysis.
- Offers customizable visualization.

ORCHESTRATOR

The **DeepInspect Orchestrator** centralizes the deployment, configuration, and management of the DeepInspect architecture, ensuring consistency and easy access to component status and version information. It also handles licensing and registration for probes connecting to the Collectors.

Main functions:
- Deploys all necessary microservices to the probes.
- Centralizes resource and service control.
- Ensures scalability and reliability.

COORDINATOR

The **DeepInspect Coordinator** streamlines network analysis by aggregating data from multiple collectors and probes. It optimizes security data management for clients with distributed infrastructure, enhancing efficiency and organization.

Main functions:
- Organizes data from multiple collectors hierarchically.
- Centralizes and aggregates data.
- Supports efficient information distribution.

COLLECTOR

The **DeepInspect Collector** deploys key services like protocol dissection, threat detection, and SIEM integration on DeepInspect probes. It enables detailed data analysis and clear aggregation for higher architecture levels.

Main functions:
- Collects data from multiple probes.
- Coordinates data aggregation and management.
- Facilitates data flow control.

DEEPINSPECT HARDWARE

The physical probe plays a crucial role in the DeepInspect architecture. It collects and processes network traffic, identifies assets and threats, and provides detailed data for analysis. Utilizing Type-Approved certified hardware, it ensures reliable performance and compliance with industry standards.

Main Functions:
- Collects and processes network traffic.
- Identifies assets and threats.
- Provides detailed data for analysis.
- Utilizes Type-Approved certified hardware.

MARITIME TYPE APPROVED DEVICES

Operating in maritime environments requires hardware that can withstand moisture, salt, and extreme weather conditions. DeepInspect's maritime devices are built to endure such challenges, ensuring continuous operation and security. We offer two types of devices to optimize resources based on specific operational needs.
The **DeepInspect Maritime Data Gatherer** is ideal for scenarios with limited space or lower processing requirements, allowing for efficient management of smaller network segments without overwhelming the system.

The **DeepInspect Maritime Probe** is designed to handle heavier data traffic and more complex processing tasks, or to be used where extensive network management is required. Both devices are **wired, completely air-gapped and DNV** (Det Norske Veritas) **certified**, capable of withstanding wide temperature variations, high humidity, and constant vibrations. The Maritime Data Gatherer connects to the Maritime Probe, which is specifically designed to manage Maritime Data Gatherer by collecting and storing a substantial volume of data.

MARITIME DATA GATHERER

MARITIME PROBE

ENERGY&TRANSPORTATION PROBE

In applications such as transportation, railway, energy or where the presence of high voltage electricity is involved, it is necessary to ensure device safety and compatibility with harsh conditions and regulatory requirements. The **DeepInspect Energy&Transportation Probe,** with EN 50121-4 certification, ensures reliable and secure data management. Available in Base and Advanced versions, it offers scalable networking, memory, and storage to adapt to evolving operational needs.

OIL&GAS PROBE

In applications such as oil and gas, where **hazardous environments** and **explosive atmospheres** are common, **device safety and compliance with stringent regulatory standards are crucial**. The **DeepInspect Oil&Gas Probe**, certified with Class 1, Division 2, ATEX Zone 2, and IECEx, ensures resilience and safety. It is designed to withstand electromagnetic interference, temperature fluctuations, and physical strain, and equipped with **antennas** to enhance its capabilities in **monitoring and data collection** in remote and challenging environments.

ENERGY&TRANSPORTATION PROBE

OIL&GAS PROBE

THE HIERARCHY MATRIX APPROACH

The Hierarchy Matrix feature is an advanced technique for generating real-time alerts based on the analysis of traffic patterns within OT systems.

The feature works by examining and exploring traffic patterns within OT systems giving clients the ability to promptly generate and monitor DeepInspect alerts. **These alerts are generated using a hierarchy matrix based on matching rules** (custom and fixed), that represent the communication between assets.

This approach allows for **rapid detection and response** to any deviations from the norm, ensuring the **security and integrity of the OT system**.

The process involves mapping permitted traffic in a matrix based on Protocol/Port specifications, serving as a foundational reference for expected communication pathways in the OT system. Once established, the system dynamically analyzes relationships within the matrix, scrutinizing the interplay between Sources (S), Destinations (D), and Protocol/Port (P) combinations to detect potential security threats or irregularities. Upon identifying a non-conforming combination of S + D + P in relation to the predefined Value (X), the system generates a focused alarm.

Protocol/ Port (P)

Source (S)

Destination (D)

APPROACH

If Source (S) + Destination (D) + Protocol/Port (P) ≠ Value (X) the near real-time alarm is created

HOW IT WORKS

1. **Map allowed traffic in a matrix**
2. **Analyze relationships found in the matrix**
3. **Generate alarm**

OUR SERVICES
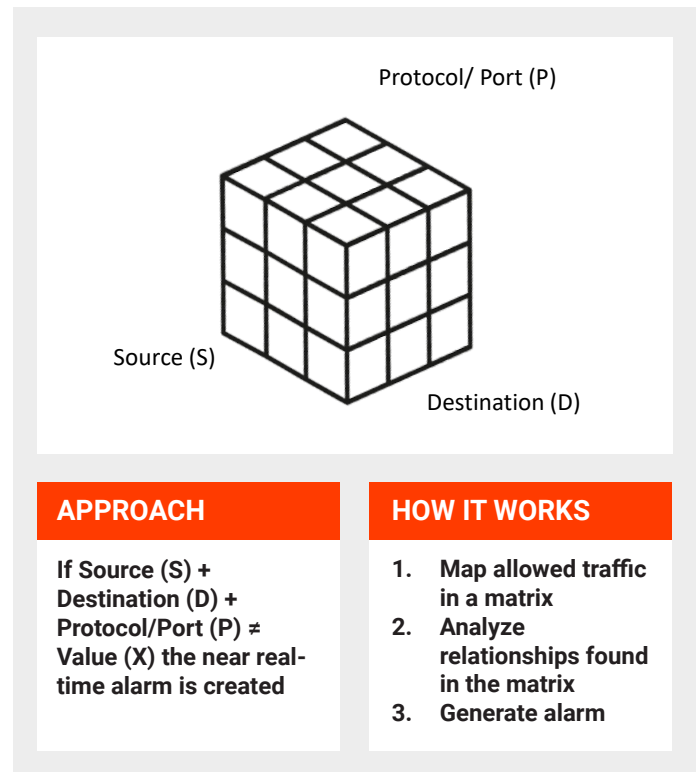
Professional Services

- Consulting and Training
- Senior Trust Advisory
- Security Assessment and Governance
- Security by Design
- Risk and Compliance
- Training and Human Factor
- 24/7 Support
- Custom Solutions

ABOUT DEEPINSPECT

DeepInspect is an Italian startup specializing in OT engineering. Drawing inspiration from military and governmental backgrounds, our mission is to provide innovative solutions through our proprietary technology, blending technical, organizational, and methodological expertise in the OT market.

Our expert team at Deepinspect holds unique capabilities in engineering, patents, sales, and marketing. With a strong foundation in the cybersecurity industry, we leverage cross-selling strategies to capitalize on our existing customer base.

As a 100% Italian company, we are thrilled to extend our reach globally and establish a formidable presence in the marketplace