DEEPINSPECT.

NETWITNESS®

NetWitness & DeepInspect

Creating OT and IT cybersecurity innovation

The Business Challenge

In the context of cybersecurity, IT and OT integration represents the convergence of administrative network operations with the operational processes directly controlling physical devices and industrial operations. Historically, these two systems operated independently, with IT focusing on data and information management while OT managed industrial control systems and processes. However, **the increasing interconnectedness necessitates robust cybersecurity measures that bridge both domains effectively**.

The integration of IT and OT brings several benefits, including **streamlined operations, enhanced data exchange**, and **improved efficiency**. However, it also introduces **complexity in managing security risks**. The interconnected systems **increase the attack surface**, making both IT and OT vulnerable to a broader range of threats. **An integrated approach to cybersecurity is essential** to address these challenges, ensuring that threats are managed consistently across all networks.

The Solution

As industries evolve and the boundaries between IT and OT blur, the need for integrated security solutions becomes increasingly critical.

The integration between DeepInspect and NetWitness addresses current security demands and anticipates future challenges, ensuring businesses can operate safely and efficiently in an interconnected world.

By integrating DeepInspect with NetWitness, the platform's capabilities are significantly enhanced, resulting in a **robust and comprehensive security system**. This unified solution combines the cutting-edge technology of DeepInspect with the extensive features of NetWitness including **advanced log and event collection**, **state-of-the-art analytics**, and a **powerful threat intelligence engine**.

Together, DeepInspect and NetWitness deliver a superior security solution that meets the evolving needs of modern industries.

Application Areas

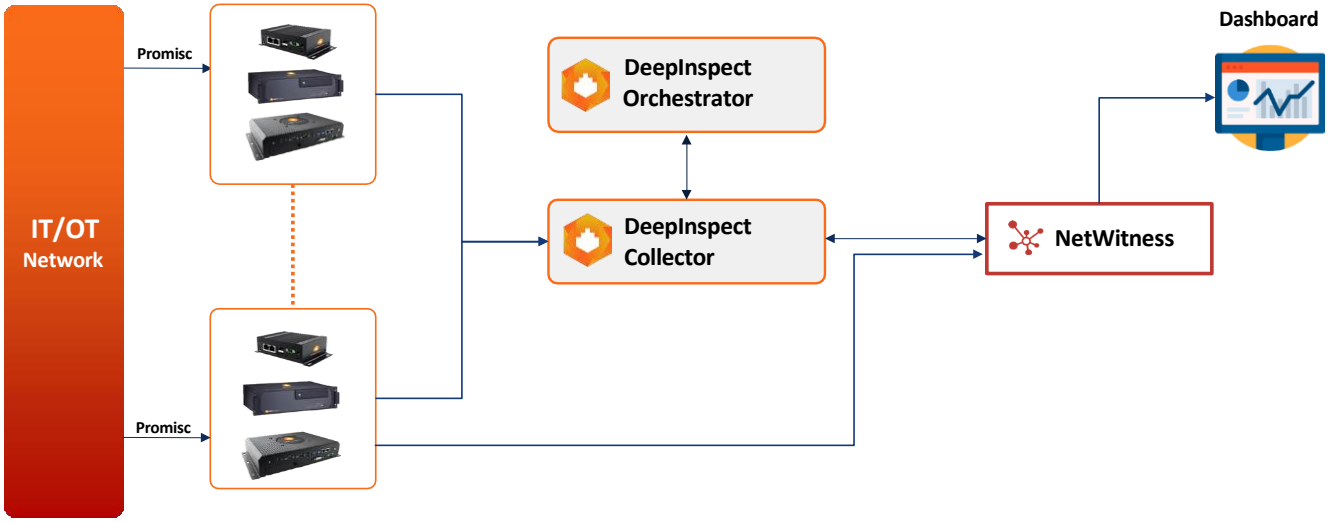
- Navy / Maritime
- Oil and Gas
- Energy
- Government and Critical Infrastructures
- Transportation
- Industry 4.0
- Healthcare
- Airports

Benefits

The combined motion integrates multiple technologies representing most of the five crucial steps of the NIST Cybersecurity Framework:

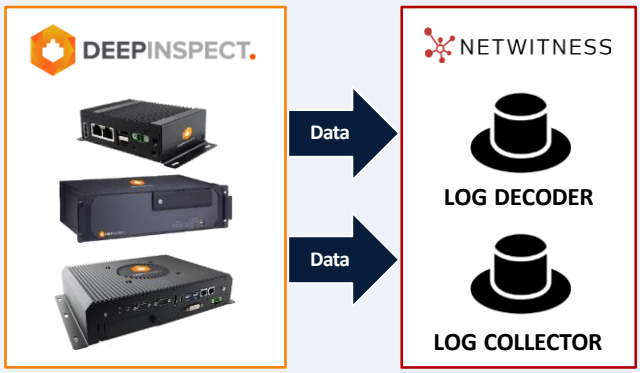
- **Identify:** Pinpoint potential vulnerabilities and threats across your network.
- **Detect:** Rapidly detect anomalies and security breaches.
- **Protect:** Implement robust security measures to safeguard your assets.
- **Respond:** React swiftly and effectively to mitigate any security incidents.
- **Recover:** Bounce back stronger with improved security post-incident.

DeepInspect + NetWitness Native Integration



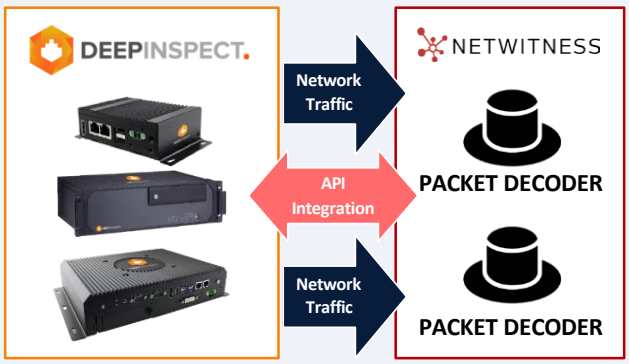
IT/OT Data Forwarding

- Field IT/OT protocols data forwarding to NetWitness XDR Log Collector
- Store and forward data in case of network communication issues with NW Collector



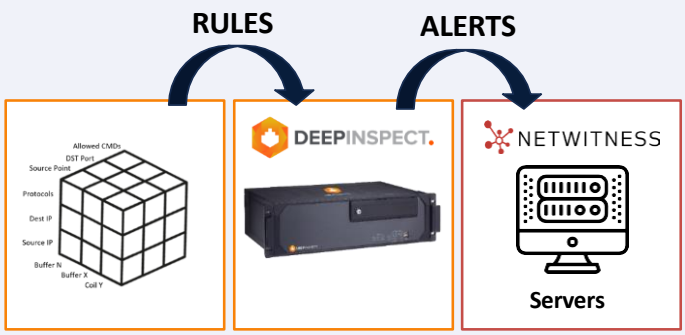
IT/OT Network Packet Forwarding

- Field IT/OT raw traffic forwarding to NetWitness XDR Packet Decoder
- Filtering of forwarded network traffic according to NetWitness XDR configuration
- Network traffic filtering



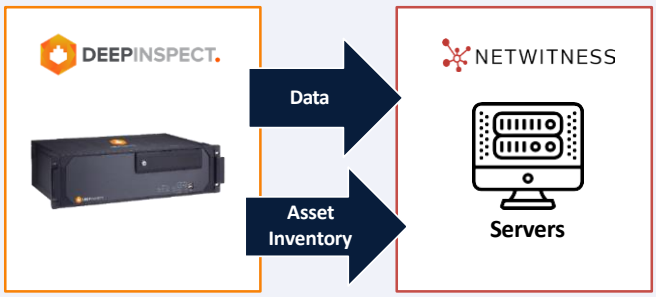
IT/OT Alerting

- Alerts Matrix (comm. anomaly detection)
- Baseline anomaly detection



IT/OT Enrichment

- Protocols dissection
- Asset Discovery
- Data extraction



DeepInspect + NetWitness Native Integration

Integrating IT and OT systems offers a comprehensive approach to security management, providing numerous benefits that enhance threat detection, incident response, visibility, and compliance. By leveraging both platforms, organizations can achieve:

- **Unified Threat Detection:** Integrating IT and OT systems within a single framework enables centralized threat detection from any source. This cohesive approach enhances the ability to quickly and effectively identify and respond to security threats.
- **Consolidated Incident Response:** Operating IT and OT under one security protocol allows for more coordinated and efficient incident response. Automated alerts and responses can be managed across both systems, significantly reducing response times and minimizing potential damage.
- **Enhanced Visibility and Control:** The integration provides a comprehensive view of both IT and OT networks, enabling security teams to monitor all systems from a single dashboard. This enhanced visibility is essential for detecting anomalies and ensuring network security.
- **Streamlined Compliance:** Integration simplifies the management of compliance requirements by offering unified reporting and control across IT and OT. This alignment with regulatory standards reduces administrative complexity and overhead.

Together is Better

MERGE OT & IT

Native integration with IT so you can correlate events and get a 360 view of the entire network

THREAT DETECTION

Alerts of suspicious activity based on signature, rules, flexible and dynamic correlation in the OT network with native NDR

NATIVE SIEM

The solution has native SIEM capabilities which allows for a unique correlation between IT and OT

FORENSICS

Unique storage space through which you can perform very accurate forensic analysis on metadata and raw data

TYPE-APPROVED

Certified hardware for specific industry with industrial grade DC power supply and designed natively for air gapped environments

CUSTOM DISSECTION

On-demand proprietary protocol dissection, encrypted traffic analysis and agent for syslog analysis

ABOUT THE PARTNERSHIP

DeepInspect and NetWitness are set to redefine the best practices of OT and IT network integration and protection. The native integrated solution incorporates the cutting-edge technology of the DeepInspect platform, with the NetWitness comprehensive suite of features. This includes advanced log and event collection, state-of-the-art analytics, a robust asset
discovery and anomaly detection engine, perfectly complementing DeepInspect capabilities. The NetWitness and DeepInspect integrated solution represents a new era of IT and OT SIEM correlation within networks.

INFORMATION

174 Middlesex Turnpike, Bedford, MA 01730

+1 888 480 0707

https://www.netwitness.com/

info@netwitness.com

NETWITNESS

DEEPINSPECT.