Kaspersky and Waterfall Security solutions integration to secure industrial networks
Joint solution to secure industrial networks


Waterfall Security Solutions is the world’s leading producer of Unidirectional Gateway technologies and products, enabling safe IT/OT integration, enterprise-wide visibility into operations, and disciplined control. The company’s growing list of customers includes national infrastructures, power plants, nuclear plants, off-shore and on-shore oil and gas facilities, manufacturing plants, power, gas and water utilities, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases, and protocols in the market.

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky’s deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company’s comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 250,000 corporate clients protect what matters most to them.

Waterfall for Intrusion Detection Systems

Waterfall for Intrusion Detection Systems (IDS) enables network intrusion sensors to monitor operational technology (OT) and industrial control system (ICS) networks without risk to the monitored networks. Waterfall for IDS unidirectional hardware emulates OT mirror & SPAN ports to network intrusion sensors on IT networks. With Waterfall for IDS in place, industrial enterprises can confidently host OT sensors on IT networks where the sensors are easily managed and updated by central SOC analysts, without risk to physical operations.

Waterfall for IDS is a hardware-enforced, physical barrier that prevents remote attacks, malware, DOS attacks, ransomware, and human errors originating on IT networks from compromising or impairing physical operations, while enabling seamless interoperability with intrusion detection system platforms.

Waterfall for IDS appliance
Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) is an OT network monitoring and visibility solution, delivered as software or as a virtual appliance, passively connected to the ICS network.

KICS for Networks detects anomalies and intrusions inside ICS networks in their early stages and ensures the necessary actions are taken to prevent any negative impact on industrial processes. KICS for Networks technologies include asset discovery, inspection of industrial protocols (DPI), network integrity and command control, Intrusion detection system and others.

The KICS for Networks interface displays a live dashboard and a network map, allowing working with assets and security events.

KICS for Networks interface

Solution integration

The joint solution provides non-intrusive industrial network traffic inspection and deep packet inspection (DPI) to detect attacks, errors and anomalies, while providing industrial networks with hardware-enforced protection for safe and reliable operations. The Waterfall for IDS hardware is physically not able to pass any signal whatsoever back into an OT network from any external network.

The joint solution has been deployed, tested, and certified for compatibility and interoperability at Kaspersky’s laboratory in Jerusalem, Israel. A joint team of Waterfall and Kaspersky engineers carried out extensive compatibility verification tests on KICS for Networks and the Waterfall for Intrusion Detection Systems (Waterfall for IDS) products.
Sample solution architecture

Benefits

Proven, trusted and seamless integration provides many benefits - the joint solution:

- Safely extends the visibility of security and network operations centers into industrial control system networks,
- Enables safe, up-to-date analysis of industrial control system network traffic for anomalous and suspicious activities,
- Provides the confidence to connect industrial networks into monitoring, analysis and alerting infrastructures,
- Is fully passive, so as not to disrupt sensitive OT devices and networks,
- Enables safe and comprehensive cybersecurity monitoring designed for OT networks,
- Transparently protects OT networks from IT networks without disrupting OT systems,
- Enables a single IT/OT pane of glass to see and manage security and physical operations.

Kaspersky Industrial CyberSecurity is a portfolio of products and services designed to secure operational technology layers and elements of your organization - including SCADA servers, HMI’s, engineering workstations, PLC’s, network connections and even engineers - without impacting on operational continuity and the consistency of industrial process.

Learn more at www.kaspersky.com/ics