MINDING THE GAP: INDUSTRIAL CYBERSECURITY WITH KASPERSKY LAB

A global leader in enterprise IT security, Kaspersky Lab is taking a leadership role in addressing the unique requirements of industrial cybersecurity.

Malicious attacks on industrial systems – including industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA) – have increased significantly in recent years.

As the Stuxnet and Black Energy attacks have shown, one infected USB drive or single spear-phishing email is all it takes for attackers to bridge the air gap and penetrate an isolated network. Traditional security is no longer enough to protect industrial environments from cyber threats.

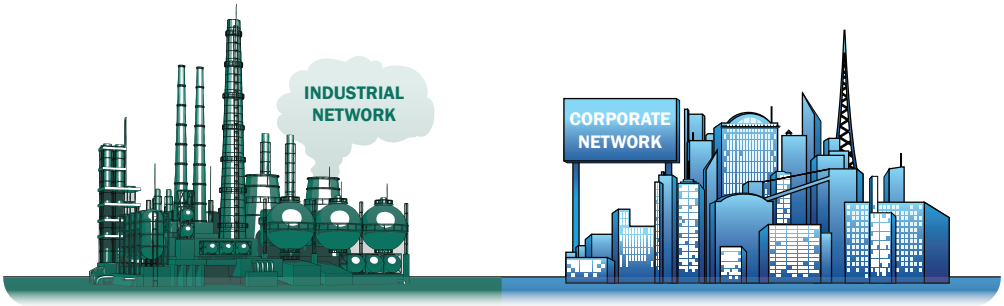
In a world where risk to supply chain and business continuity have ranked as the number one business risk concern globally for the past four years, it's hardly surprising that cyber risk is the number one emerging concern.[1]

For businesses operating industrial or critical infrastructure systems, the risks have never been greater.

Industrial CyberSecurity is different

There may be some overlap in the threats, but there are significant differences between the cyber security requirements of ICS environments and those of general business.

Corporate environments focus on safeguarding confidential data; when it comes to industrial systems, where every minute of downtime or error counts, uninterrupted operations are the ultimate priority. This is what distinguishes industrial cybersecurity from other businesses – and makes working with the right security vendor so important.



Industrial cybersecurity's priorities of availability, integrity and confidentiality are often the opposite of standard business priorities.

1 Allianz Risk Barometer 2016

INDUSTRIAL CYBERSECURITY SOLUTIONS SHOULD INCLUDE THREE KEY PILLARS:

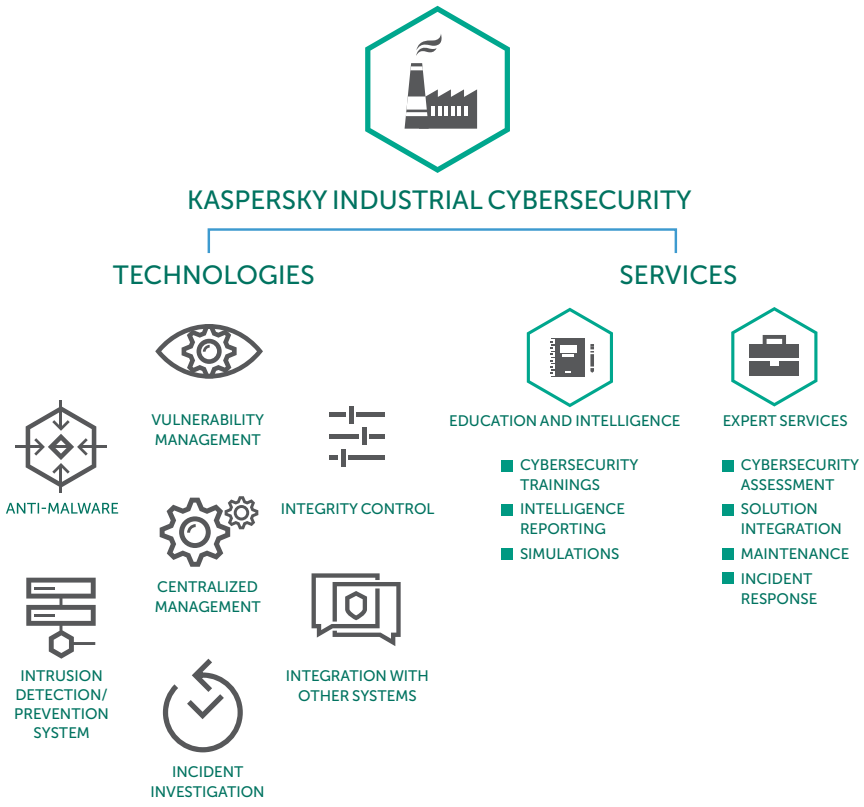
- A process-based approach to security implementation
- Employee awareness/education
- Technologies created specifically for industrial environments

KASPERSKY LAB'S INDUSTRIAL CYBERSECURITY APPROACH IS HOLISTIC:

- **Process:** There's no out-of-box solution for industrial cybersecurity. It's a process that begins with an audit, prepares people for change and moves through gradual roll-out with minimal disruption.
- **People:** Every employee – from business to factory floor – plays a role in cybersecurity. Training and education, such as Kaspersky Industrial Protection Simulation (KIPS) game, are vital.
- **Technology:** Kaspersky Lab has developed solutions based on unique technologies, designed specifically for industrial security needs. Fault-tolerant and non-disruptive, they can even work in air-gap conditions.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMI panels, engineering workstations, PLCs, network connections and people – without impacting on operational continuity and consistency of the technological process.



As threats targeting critical infrastructure increase, choosing the right advisor and technology partner to secure your systems has never been more important.

Talk to our experts today and learn more about the future of industrial cybersecurity.

www.kaspersky.com/ics

INTERPOL STRATEGIC PARTNER

IIC MEMBER industrial internet CONSORTIUM

MOST TESTED* MOST AWARDED* KASPERSKY LAB PROTECTION
*kaspersky.com/top3

KASPERSKY lab