



KASPERSKY LAB:

EMPOWERING INDUSTRIAL

CYBER SECURITY



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

KASPERSKY LAB LEADERSHIP

KASPERSKY LAB: STRENGTH IN SECURITY, LEADERSHIP IN VISION.

The world's largest privately held cyber security company, Kaspersky Lab has over 300 million users in 200 countries and territories worldwide. Kaspersky Lab has a corporate client base of more than 250,000 companies located around the globe, ranging from small and medium-sized businesses all the way up to large governmental and commercial organizations. Over 300 million people worldwide are protected by Kaspersky Lab products and technologies.

Under the leadership of founder-CEO, recognized cyber security expert and visionary, Eugene Kaspersky, the company has earned a reputation for unparalleled insight into local and global threats, making many of the most significant and relevant discoveries in recent years, including Dark Hotel, Flame, Gauss, mini-flame, Red October, NetTraveler and The Mask, as well as recent industrial-specific attacks such as Crouching Yeti (Energetic Bear), Miancha and Black Energy 2.

LEADERSHIP IN THREAT INTELLIGENCE

While Kaspersky Security Network, our complex distributed infrastructure, builds on the real-time intelligence generated by over 60 million volunteer Kaspersky users globally, our elite Global Research and Analysis Team (GReAT) contributes a unique set of skills and expertise to Kaspersky Lab's threat research, developing solutions capable of combating increasingly complex and sophisticated malware code.

LEADERSHIP IN RESEARCH AND INNOVATION

Because it's privately owned, Kaspersky Lab is free to invest heavily in Research and Development outside short-term market constraints. Almost half of our 3000 employees globally work in our research and development labs, focusing on developing innovative technologies, investigating cyber-warfare, cyber-espionage and cyber-sabotage and all types of threats and techniques.

This focus on high-quality, internal R&D has led to Kaspersky Lab being recognised as an industry leader in cyber security technologies – with independent tests continuing to award more 'top scores' to Kaspersky Lab than any other vendor.

TRUSTED PARTNER OF GOVERNMENTS AND REGULATORS

Threat research has always been an integral part of Kaspersky Lab's strategy. With acknowledged industry-leading researchers and analysts around the world, the global cyber security community and respected international organizations, including INTERPOL, Europol, Microsoft Digital Crimes Unit, Cyber Security Agencies and numerous CERTs, ISA (International Society of Automatization) have all invited Kaspersky Lab to collaborate and consult with them on an ongoing basis. We are currently working closely with regulatory authorities from Russia to the United States to develop frameworks for industrial security and critical infrastructure protection.

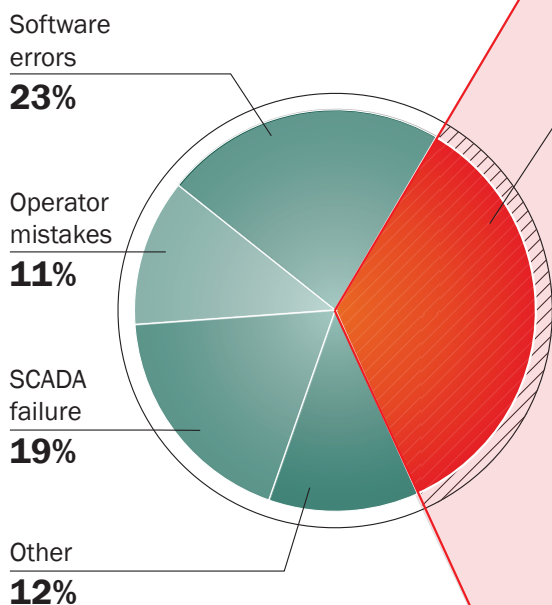
► KASPERSKY LAB'S VIEW OF THE STATE OF INDUSTRIAL SECURITY

THREATS: YOU DON'T HAVE TO BE A TARGET TO BECOME A VICTIM & WHY CURRENT INDUSTRIAL SECURITY APPROACHES DON'T WORK

Recent research by the SANS Institute has found that only 9 per cent of industrial sector IT pros said they were certain they had not been breached¹. Remarkably, 16 per cent said they had no process in place to detect vulnerabilities – partly out of a fear that they will attract unwanted attention to system vulnerabilities.

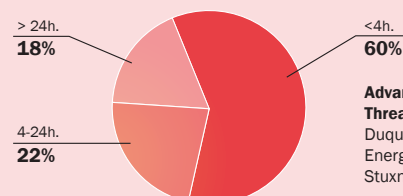
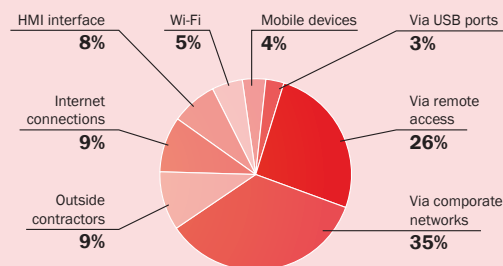
But you don't have to be a target to become a victim. In addition to industrial-specific Advanced Persistent Threats such as Citadel, Crouching Yeti/Havex, Miancha or Black Energy 2, many of the threats and vulnerabilities facing industrial systems today come from everyday threats in the business layer of their infrastructure.

THREATS: YOU DON'T HAVE TO BE A TARGET TO BECOME A VICTIM



Major reasons for industrial network malfunction incidents
securityincidents.net

Malware attacks 35%



Downtime of the industrial process due to malware incidents
securityincidents.net

Advanced Persistent Threats (APT)
 Duqu, Flame, Gauss Energetic Bear, Epic Turlia Stuxnet

Generic Malware
 Many ICS threats are unsophisticated but their impact is massive: Worms, Trojans, Blockers, Password theft, remote access, vandalism.

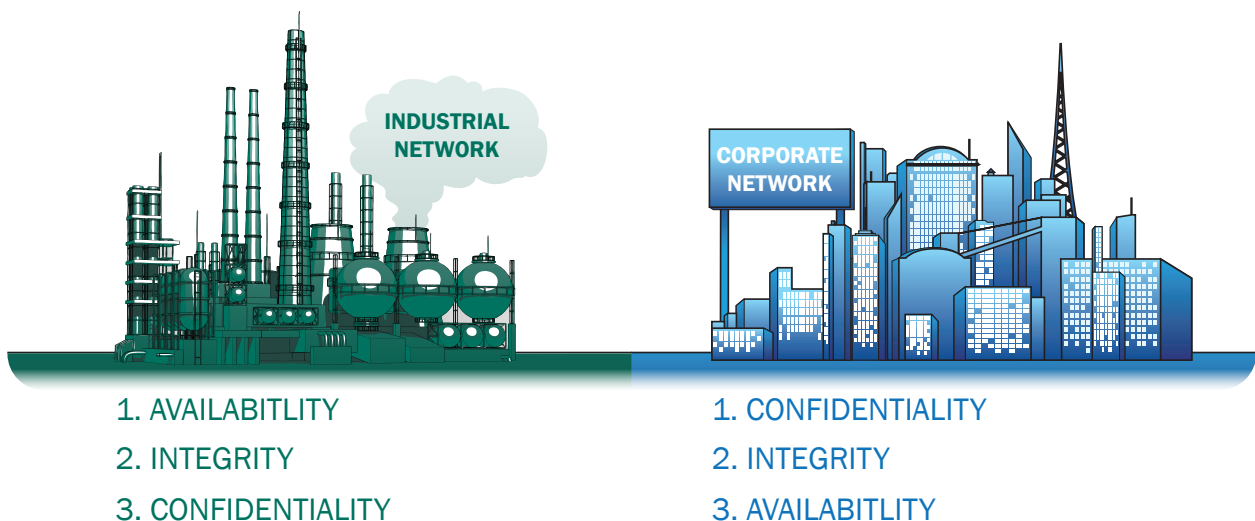
¹ SANS Institute: 2014 Control System Security Survey

Industrial-specific attacks use both the enterprise LAN and industrial control systems (ICS) to launch and propagate; Energetic Bear infected OPC server and ICS equipment software with a remote access Trojan, but also exploited known vulnerabilities in Adobe PDF software to launch spear-phishing attacks. The attack propagated from one system to another, stealing information from SCADA systems and damaging unhardened ICS by wiping PCs or overloading networks.

The Conficker worm, although not industrial-specific, has not only been found in critical medical equipment, but is suspected to have been a 'door kicker' for high-profile industrial attacks such as Stuxnet. Conficker is capable of completely overloading networks and bringing vital processes to a halt. Traditional industrial security techniques don't address these threats very well: 'air-gap' or 'security through obscurity' strategy doesn't address the reality that smart grid systems and web-based applications mean 'Industrial Control Systems look more and more like consumer PCs².'

INDUSTRIAL SECURITY IS DIFFERENT

There is an overlap in the threats, but the differences between industrial cyber security requirements and those of general business are significant. Many IT security strategies are focused on data protection and rely on the concept of C-I-A : confidentiality, integrity and availability of data. Industrial systems prioritise continuity above all else; their protection is not about "data", it's about "process" **availability, integrity and confidentiality**, in that order. This is what distinguishes industrial security needs; even the highest quality security solution is effectively useless if it puts the continuity of process at risk. Everyday security techniques such as anti-malware protection, patch management/software updates, and security configuration management can't be allowed to negatively impact on processes.



² EU Agency for Network and Information Security (ENISA): 'Can we learn from SCADA security incidents?'

THE RIGHT APPROACH TO INDUSTRIAL SECURITY

These different industrial security needs make working with the right vendor extremely important. Industrial cyber security solutions should include three key pillars: a process-based approach to security implementation, employee awareness/education and solutions created specifically for industrial environments.



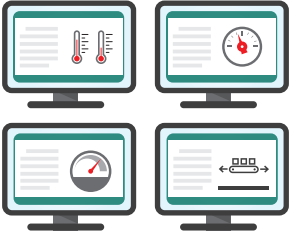
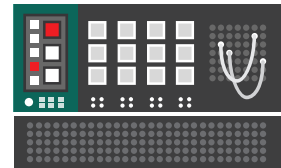


Kaspersky Lab's approach to industrial security is a holistic one that includes:

- The right attitude to industrial security – there is no silver-bullet, out-of-box solution – industrial security implementation is a process that begins with audit and other services before moving on to preparing people for change, before starting the gradual rollout of dedicated, non-disruptive solutions. This is the only way to enable seamless, fully functional protection. Because every minute of manufacturing process downtime carries significant costs, any product installation should be implemented under the guidance of professional experts, on duty 24x7.
- People play a key role in any security strategy. Empowering different stakeholders and teams through training and education, from C-level executives to IT managers and OT engineers. Our Kaspersky Industrial Protection Simulation (KIPS) role playing game, for example, enables even non-technical staff to gain an understanding of the importance of cyber security and the needs of their workplace.
- At a technology level, Kaspersky Lab offers solutions based on unique technologies, created specifically for industrial networks – extremely fault-tolerant, non-disruptive to technology processes and capable of working in air-gap conditions.

▶ KASPERSKY LAB SOLUTION

KASPERSKY LAB VALUE PROPOSITION

<p>LEVEL 4 Business planning and logistics</p>		<p>Managing end-to-end supply chain. Establishing the basic plant schedule – production, material use, delivery, and shipping.</p>	<p>Kaspersky Security for Business + Professional Services</p>
<p>LEVEL 3 Manufacturing Operations management</p>		<p>Work flow/recipe control to produce the desired end products. Maintaining records and optimizing the production process.</p>	
<p>LEVEL 2, 1 Batch Control. Continuous Control. Discrete Control.</p>		<p>Monitoring, supervisory control and automated control of the production process</p>	<p>Kaspersky Industrial Security + Professional Services</p>
<p>LEVEL 0 Physical</p>		<p>Sensing the production process, manipulating the production process</p>	

▶ CUSTOMER BENEFITS

3-EDGE PROTECTION

Kaspersky Lab's industrial security solution covers every aspect of cyber security for industrial customers, such as Energy providers:

- At every level, from the business-layer network down to the production site.
- Education and awareness for: C-level executives, IT, IT security and engineers.
- Securing business continuity through data protection and technological process protection.

SPECIALIZED, BESPOKE INDUSTRIAL SECURITY OPTIONS

Kaspersky Lab understands that each technology network has its specific features that, in most cases, are unique. Our industrial solution is fully customizable and works as a 'construction set' that can be tailored to specific customer needs and to fit unique challenges, demands and specific infrastructures.

Working with Kaspersky Lab, industrial clients have full access to over a decade's worth of cyber security intelligence and expertise; our consultants and engineers are a core component of our professional services team. Because every minute of manufacturing process downtime carries significant costs, any product installation should be implemented under the guidance of professional experts, on duty 24x7. In addition to maintenance support agreements, Kaspersky Lab experts are also available to perform in-depth investigations of security incidents as well as deliver regular intelligence reports on existing threats, including threat intelligence from our GReAT team of experts. Kaspersky Lab believes that the most effective industrial security is delivered through a combination of technology and integrated, expert services. Among the expert services Kaspersky Lab offers to industrial providers are:

- Cyber security audit, report and recommendation, followed by the development and implementation of policies and procedures – as well as the necessary technical support.
- Threat model development and mitigation recommendations
- Incident response: incident investigation, digital forensics (and malware analysis) and legal support.
- Training in ICS-specific and general cyber security
- Advice to state agencies and industrial regulators.

KASPERSKY LAB: THE FUTURE OF INDUSTRIAL SECURITY

Building on our expertise in bespoke industrial security technologies, Kaspersky Lab is actively developing solutions tailored to protect technology networks. Our long term strategy involves the development of a secure operating system, underlining our vision of providing the ultimate embedded security basement for a variety of PLC-like devices used in critical infrastructures, including industrial ones.

Already a trusted security provider and partner to leading industrial organizations, which have used our anti-virus protection for many years, Kaspersky Lab also collaborates with leading industrial automation vendors, including Emerson, Rockwell Automation, Siemens and others to establish specialized procedures and cyber-security co-operation frameworks to protect industrial environments from existing and emerging cyber-threats (including APTs) and ensure the compatibility of Kaspersky Lab solutions with customer operational technology. This demonstrates our ability to provide effective industrial security without impacting on operational continuity and consistency.

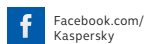
KASPERSKY LAB - SPECIALIZED INDUSTRIAL SECURITY EXPERTS

According to Forrester Research, threats to critical and industrial infrastructure can no longer be ignored, and those selecting security vendors should "Look for specialized industry expertise."³ The Forrester report goes on to identify Kaspersky Lab as one of the few vendors offering specialized industrial security solutions that actually delivers on their promises and has genuine experience and expertise in the sector.

As a recognized leader in cyber security and industrial protection, Kaspersky Lab is continually researching and developing solutions that do more to address the constantly evolving threats to industrial and critical infrastructures. From operations management to the SCADA level and beyond, into a future where a secure operating environments will be a reality, Kaspersky Lab is playing a leading role in helping industry, regulators and government agencies globally to anticipate changes in the threat landscape and defend against attacks.

Industrial security has consequences that reach far beyond business and reputational protection. In many instances, there are significant ecological, social and macro-economic considerations to consider when it comes to protecting industrial systems from cyber threats. As threats targeting critical industrial infrastructure increase, choosing the right advisor and technology partner to secure your systems has never been more important. Why not call Kaspersky Lab's experts and find out more about the future of industrial cyber security?

³ Forrester Research, *S&R Pros Can No Longer Ignore Threats to Critical Infrastructure*, by Rick Holland.



Kaspersky Lab
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

© 2015 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners. Mac and Mac OS are registered trademarks of Apple Inc. Cisco is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. IBM, Lotus, Notes and Domino are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, Windows Server and Forefront are registered trademarks of Microsoft Corporation in the United States and other countries. Android™ is a trademark of Google, Inc. The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

