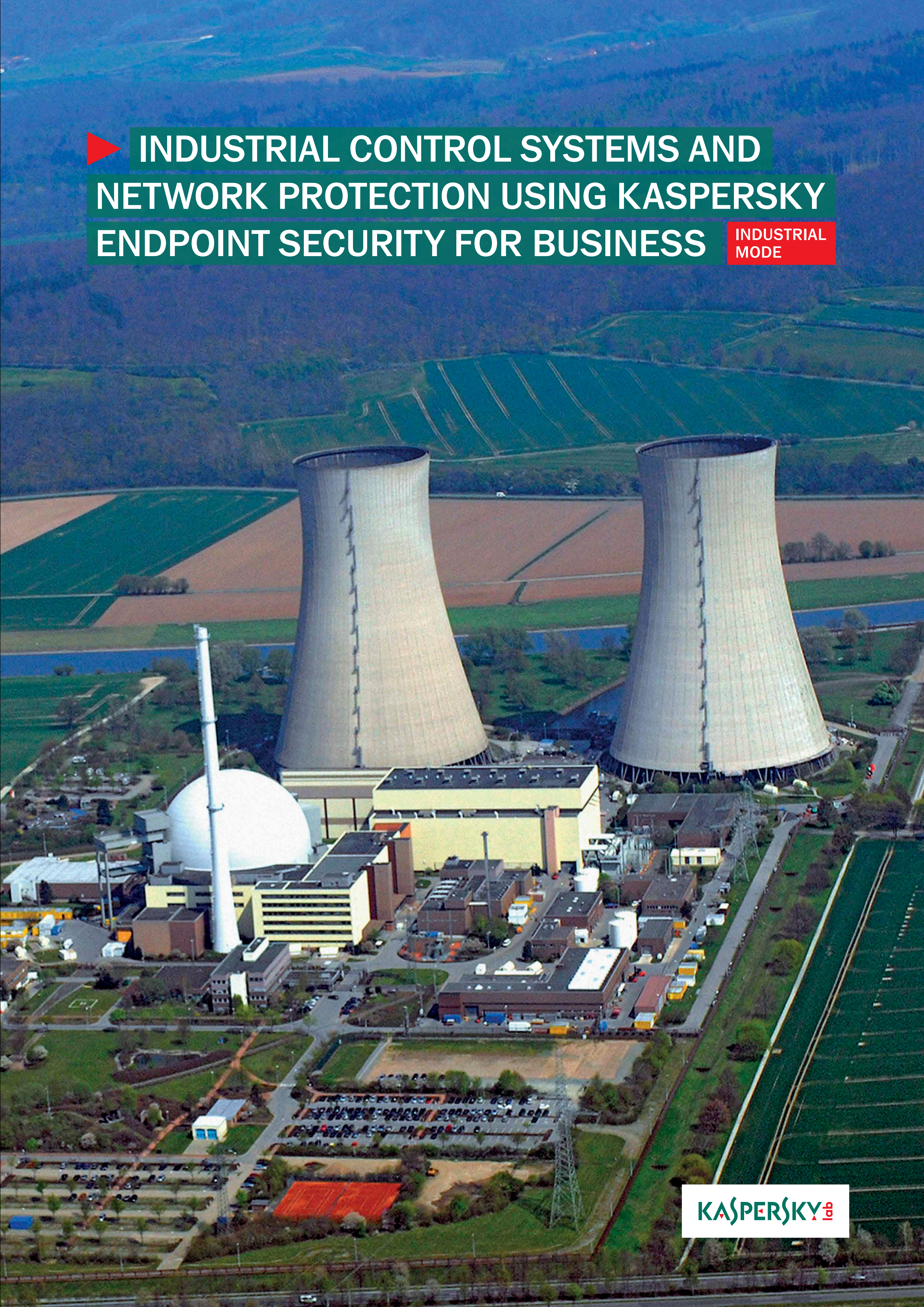
INDUSTRIAL CONTROL SYSTEMS AND NETWORK PROTECTION USING KASPERSKY ENDPOINT SECURITY FOR BUSINESS

INDUSTRIAL MODE



▶ INDUSTRIAL CONTROL SYSTEMS AND NETWORK PROTECTION USING KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Industrial Mode

Cyber threats to industrial networks are a real and fast-growing challenge. Kaspersky Lab's technologies and vision already provide an effective, defense-in-depth strategy to mitigate the growing risks posed by workstations and servers operating within industrial control systems. And that's just the beginning.

ATTACKS ON INDUSTRIAL SYSTEMS ARE ON THE INCREASE

In 2013, ICS-CERT responded to 256 cyber incidents, the majority of them first detected in the business networks of critical infrastructure organizations.[1] Fifty-nine per cent of these targeted the energy sector; critical manufacturing accounted for 20% of reported cyber incidents.

And these are just the attacks and threats we know about. 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 breached.[2] Forty per cent of those surveyed reported identified or suspected breaches — up from 28 per cent in 2013. Remarkably, sixteen per cent said they had no process in place to detect vulnerabilities. Many attacks go unreported — sometimes because the organization itself is incapable of recognizing an attack, but more often out of a fear that they will attract unwanted attention to system vulnerabilities.

COMMON NETWORK THREATS

Many of the network-based threats faced by conventional business infrastructures also affect ICS environments. In a world where smart grid systems and web-based applications mean 'Industrial Control Systems look more and more like consumer PCs'[3], it's no surprise that many industrial network breaches start with their connection to vulnerable, internet-connected workstations and servers in the enterprise layer. Stuxnet, for example, exploited three zero-day vulnerabilities in Windows to launch a worm-based attack; USB sticks were used to spread the attack and sabotage control systems. Search engines such as Shodan can be used to locate unsecured online devices and systems, from traffic lights to power grids; widespread use of default settings such as 'admin' and '1234' make it easy from criminals to connect using just a web browser. The U.S Department of Homeland Security suggests an average of 11 direct connections between the operations/processes network and the corporate network.[4] That's a lot of vulnerability.

Kaspersky Lab's internal research shows the key channels for threat penetration in industrial systems are:

- Software vulnerability exploits
- Vulnerable Windows PCs controlling ICS
- Connection with ERP/MES net and/or Internet
- Uncontrolled use of unauthorised/undesirable software applications
- Misuse of workstations by SCADA operators – i.e. 'recreational' Internet browsing
- Unauthorized connection of 3G modems/access points
- Uncontrolled use of USB drives
- Use of insecure contractor devices on site.

The reality is that many industrial PCs are already infected. Extensive research by Kaspersky Lab, using data from the Kaspersky Security Network (KSN) indicates that many industrial PCs are infected with the same malware afflicting business systems (IT), including (but not limited to) well-known culprits such as Trojans viruses, worms, potentially unwanted and dangerous programs (PUPs) and other exploits targeting vulnerabilities in the Windows operating system.[5]

	IT	SCADA
Trojan	65.45%	43.44%
PUPs	11.17%	37.03%
Worm	7.52%	13.43%
Virus	15.86%	6.10%

The potential impact of a successful attack reaches far beyond the bottom line; direct threats to operations can have life-threatening implications or lead to ecological catastrophe.

[1] ICS-CERT Monitor, October-December 2013
[2] SANS Institute: 2014 Control System Security Survey
[3] EU Agency for Network and Information Security (ENISA): 'Can we learn from SCADA security incidents?'
[4] Kaspersky Lab: Securing Critical Information Infrastructure: Trusted Computing Base, Securelist October 2012.
[5] Kaspersky Lab: IT Threat Evolution Q1 2013, Securelist May 16 2013

THE SAME, BUT DIFFERENT

There may be some overlap in the threats, but there are significant differences between the cyber-security requirements of industrial providers and those of general business. Only cyber-security vendors that understand these differences are able to deliver security solutions that meet the unique needs of industrial control systems and critical/industrial infrastructure owners.

While everyday business systems prioritise the defense-in-depth concept of confidentiality, integrity and availability[6] (in that order), industrial systems are the exact opposite: availability, integrity, confidentiality. In an industrial context, continuity and process have to take precedence — this is what distinguishes their security needs from the more general corporate approach. In other words, it's not acceptable to deliver high (even top-notch) security that puts continuity of the process at risk.

Industrial security approach

	INDUSTRIAL NETWORK	CORPORATE NETWORK
• Office IT Security is about Data protection	1. Availability	1. Confidentiality
• Industrial Security is about **Process** protection	2. Integrity	2. Integrity
• Process should be continuous and only then secure	3. Confidentiality	3. Availability

There are many shared threats, but the cyber-security security objectives of business and industrial providers are the exact opposite of each other

Industrial cyber security has some unique requirements, among them:

- zero impact on technology processes
- full compatibility with industrial software and hardware
- ability to function without user interaction for prolonged periods
- minimize reboots during lifecycle
- effectiveness against both common and SCADA network-specific threats.

ELIMINATING FALSE POSITIVES AND OPTIMIZING IT SECURITY PERFORMANCE

From an IT security point of view, process protection carries a heavy emphasis on false alarm prevention. Security is critical, but if industrial software is erroneously blocked or overloaded by an 'update storm' or extensive scanning process, it may as well not be there at all.

KESB is noted for its exceptionally low false positive rate[7], but, as will be seen in the "Application Startup Control — 'Default Deny' mode" section of this paper, it also delivers extensive functionalities that allow industrial organizations complete control over what software runs or is blocked on their systems.

In addition, KESB running in industrial mode can be optimized according to recommended settings for testing, deployment, rollout and updates in a pre-production environment, minimizing the potential for process disruption and highlighted any issues before they become real problems. KESB is streamlined to minimize system burden during scanning and antivirus operations. For added peace of mind, maintenance support agreement options are available[8] to industrial organizations that wish to avail of Kaspersky Lab's high level technical expertise in mission-critical environments.

KASPERSKY: TRUSTED INDUSTRIAL SECURITY PROVIDER

Kaspersky is already a trusted security provider and partner to leading industrial organisations, which have used our antivirus protection for many years. Working with leading industrial automation vendors, such as Emerson, Rockwell Automation and Siemens,, we have established many specialized procedures to ensure approval and compatibility of Kaspersky Endpoint Security for Business with customer operational technology. This enables us to guarantee effective protection without impacting on operational continuity and consistency. Kaspersky Endpoint Security for Business currently delivers effective 'industrial mode' protection, guarding ICS/SCADA endpoints from the threats and vulnerabilities that form the backdoor of choice for many criminals targeting critical systems.

Kaspersky Industrial Endpoint Security: Vendor Compatibility List

Kaspersky has established many specialized procedures to ensure approval and compatibility with leading industrial automation vendors, including:	• Rockwell Automation • Emerson • Siemens

How Kaspersky addresses top threats in ICS

Threat	Kaspersky Lab offering
Malware, Trojans, exploits, zero-day threats	Industry-leading anti-malware engine with signature-based, proactive and cloud detection techniques
Network attacks to industrial nodes	Network attack detection, firewall
Unauthorized run of software on HMI/engineering workstations	Application startup control with whitelisting ("default deny") policy support
Software vulnerabilities	Vulnerability assessment
Unauthorized connection of external devices	Device control that enables to allow connection of devices based on type/ID/family/bus
Industrial software blocking by a security solution (false alarm)	Internal procedure of pre-release updates testing Compatibility certification with industrial automation vendors Preliminary on-site update testing before roll-out to ICS network

Kaspersky Endpoint Security for Business @Industrial Mode already delivers effective protection — the above table highlights just some of the areas we protect

[6] http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

[7] AV-Comparatives, 'File Detection Test of Malicious Software — including false alarm test' September 2013. Kaspersky AV returned just 6 false positives out of a total scan of 136,610 files, with a detection rate of 99.2%; Kaspersky anti-spam achieved 99.75% detection rate with zero false positives in VB Spam Test, March 2014.

[8] Maintenance Support Agreements are available at an additional cost and only in certain countries.

INDUSTRIAL CONTROL SYSTEMS AND NETWORK PROTECTION USING KESB @ INDUSTRIAL MODE

Kaspersky Endpoint Security for Business @Industrial Mode already provides many global industrial organizations with an effective defense. Many of the features and technologies supplied already represent best practice for securing industrial systems — you just have to enable them. Let's take a look…

APPLICATION STARTUP CONTROL — "DEFAULT DENY" MODE

According to ICS-CERT, "The predictable and unchanging nature of control systems provides the ideal environment for whitelisting."[9] Kaspersky's 'Default Deny' approach is already a standard in a number of states worldwide, including governing bodies in the UK, USA, China and international standards such as ISA99/IEC 62443.

Kaspersky's Application start-up control enables easy software inventory and categorization (including for SCADA), with 'test mode' for fine-tuning rules. In addition to optimizing security, default deny mode significantly reduces resource strain — with strictly controlled application inventories, analysis and maintenance control requirements are lower, reducing impact on network performance.

DEVICE CONTROL — "DEFAULT DENY" MODE

USB drives have played a significant role in the spread of high-profile industrial attacks such as Stuxnet and Gauss. Researchers at Purdue University in the U.S. found that malicious software introduce via a mobile or other device can spread to 500,000 devices in just 100 seconds.[10] Taking into account that common networks are much smaller than 500,000 devices, one infected removable flash-drive can infect the whole network even faster than you can click a mouse.

Prevent unauthorized/unsecured USB devices from connecting to industrial endpoints, workstations and servers using Kaspersky Endpoint Security for Business. It enables a 'Default Deny' policy for devices, with configuration by ID, class, bus.

By centrally maintaining policies around the use of removable devices and media — USB, flash drives, CD/DVD, smart cards etc — you can significantly reduce risks to the industrial network. Kaspersky enables a flexible approach to managing device-related threats; granular controls allow you to set different rules for different devices, users and use cases. Apply policies for read only, block or read-and-write to different devices. Policies can be applied according to device serial numbers and integration with Active Directory facilitates easy enforcement.

VULNERABILITY SCANNING

Application vulnerabilities pose a significant threat to workstation and industrial endpoint security. Between 2012-2013, there was a 32 per cent increase in vulnerabilities, with 13,073 detected in 2013.[11] Just over sixteen per cent of all vulnerabilities in 2013 were rated 'Highly Critical.'

Kaspersky's vulnerability scanning, monitoring and assessment technology analyses threats by tracking and detecting known vulnerabilities in software applications, operating systems and third party applications such as Adobe, Microsoft Office and Java-based software.

Recognizing the primacy of process and low tolerance for latency, Kaspersky Endpoint Security for Business can be optimized for industrial settings and will run even without the patch management and automation features enabled. This allows you to keep fully up to date on the latest threats and vulnerabilities while managing the most effective, appropriate response for your setting.

ANTI-MALWARE PROTECTION

Kaspersky Endpoint Security for Business's anti-malware protection offers proactive defense from known and zero-day malware. Used in combination, our on access scanner, System Watcher and Automatic Exploit Prevention technologies between them use heuristic analysis to detect, block and alert users to malicious activity on industrial workstations and servers.

- **Automatic Exploit Prevention (AEP)** Prevents malicious code from executing on systems. Kaspersky Lab's AEP specifically targets malware that exploits software vulnerabilities — even if a user opens a malicious file designed to exploit a flaw in Windows, Office or Adobe software, AEP will prevent that malicious code from executing.

- **System Watcher**: Gathers information on applications running on workstations and servers, providing insight into vulnerabilities and suspicious activities using heuristic analysis. In combination with other proactive protection technologies in KESB, it enables not only malware blocking, but can also "track", malicious software activity and rollback, ensuring process continuity while providing continuous monitoring capability.

- **On access scanner (OAS)**: Best practice for the proactive protection on SCADA systems (including internet-facing ICS). Performs immediate anti-malware scan of files as soon as they are accessed or run.

[9] ICS-CERT Monitor, October-December 2013
[10] Yu Zhang and Bharat Bhargava, Fibonacci Modeling of Malware Propagation, Purdue University 2008.

FIREWALL

Secures and controls workstation and server use of network connections: local networks and internet, guarding against both network and application based attacks. Apply rules to all network connections and control resource usage by applications installed on the SCADA host, HMI panel or engineering workstation. Specific and granular protection settings can also be applied — for example, on a SCADA server certain types of connection (such as connection to upper levels of industrial network or to PLCs)can be allowed only for SCADA application, but not to other applications on the same host. The same can be set up for an HMI panel: it's possible to allow connection only to SCADA host for acquiring information in real-time, but block other connections from or to this host.

KESB firewall also supports multi-network connection installations. This is useful if a host is connected simultaneously to two sub-networks (such as a data acquisition/aggregation server that collects data from the lower level of the industrial network and provides data to upper level) or if the host is "roaming" between networks (like an engineering workstation used for connection to SCADA or PLC in different sub-networks in a segmented industrial network).In most cases technology network has segmentation.

NETWORK ATTACK BLOCKER

As part of a layered defense approach, network attack blocker guards against malicious activities that anti-virus alone can't always handle: buffer overrun attacks, port scanning, denial of service and other remote malicious actions.

The network attack blocker works in tandem with the other security features and technologies in Kaspersky Endpoint Security for Business, using signatures to block connections that match the descriptions of known network attacks. It delivers effective defense against memory-based attacks, preventing the spread of malicious code throughout the network by blocking all packets from an infected industrial workstation or server for a specified time.

STRENGTHENING INDUSTRIAL ENDPOINT SECURITY

ICS-CERT is clear about the potential for insecure workstations, servers and endpoints to become a springboard for attacks on industrial control environments.[12] The lateral movement of malware and other threats into control systems enables the exfiltration of sensitive data and surveillance activities upon which criminals (or prying nation states) can build new attacks or ways to penetrate deeper into control systems.

A strength-in-depth approach to workstation, server and endpoint security enables industrial organizations to take a proactive, more thorough cyber security stance. By significantly reducing server and workstation vulnerabilities, it is possible to decrease the available attack surface in a meaningful way, enhancing the security of ICS systems without generating latency or otherwise interfering with processes or performance.

▶ THINKING ABOUT TOMORROW TODAY

As a leader in cyber-security, Kaspersky Lab is continually developing Critical Infrastructure Protection and industrial security solutions that do more to meet the specific requirements of industrial control systems and the organisations that are tasked with keeping these systems running.

Kaspersky Endpoint Security for Business already provides a solution that delivers effective cyber-security in an industrial setting, from operations management to the SCADA level and beyond. But that's just part of the story: to further address the constantly evolving threats to critical and industrial infrastructures, our experts are developing solutions tailored to protect the lower levels of industrial networks. Kaspersky Lab's 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 devices used in critical infrastructures, including industrial ones.

By establishing close relationships with government organisations and law enforcement agencies globally, as well as helping to educate, advise and inform industrial operators, Kaspersky is playing a leading role in helping industry and regulators anticipate changes in the threat landscape and defend against attacks.

[12] https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf

Twitter.com/
Kaspersky

Facebook.com/
Kaspersky

Youtube.com/
Kaspersky

Kaspersky Lab ZAO, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

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