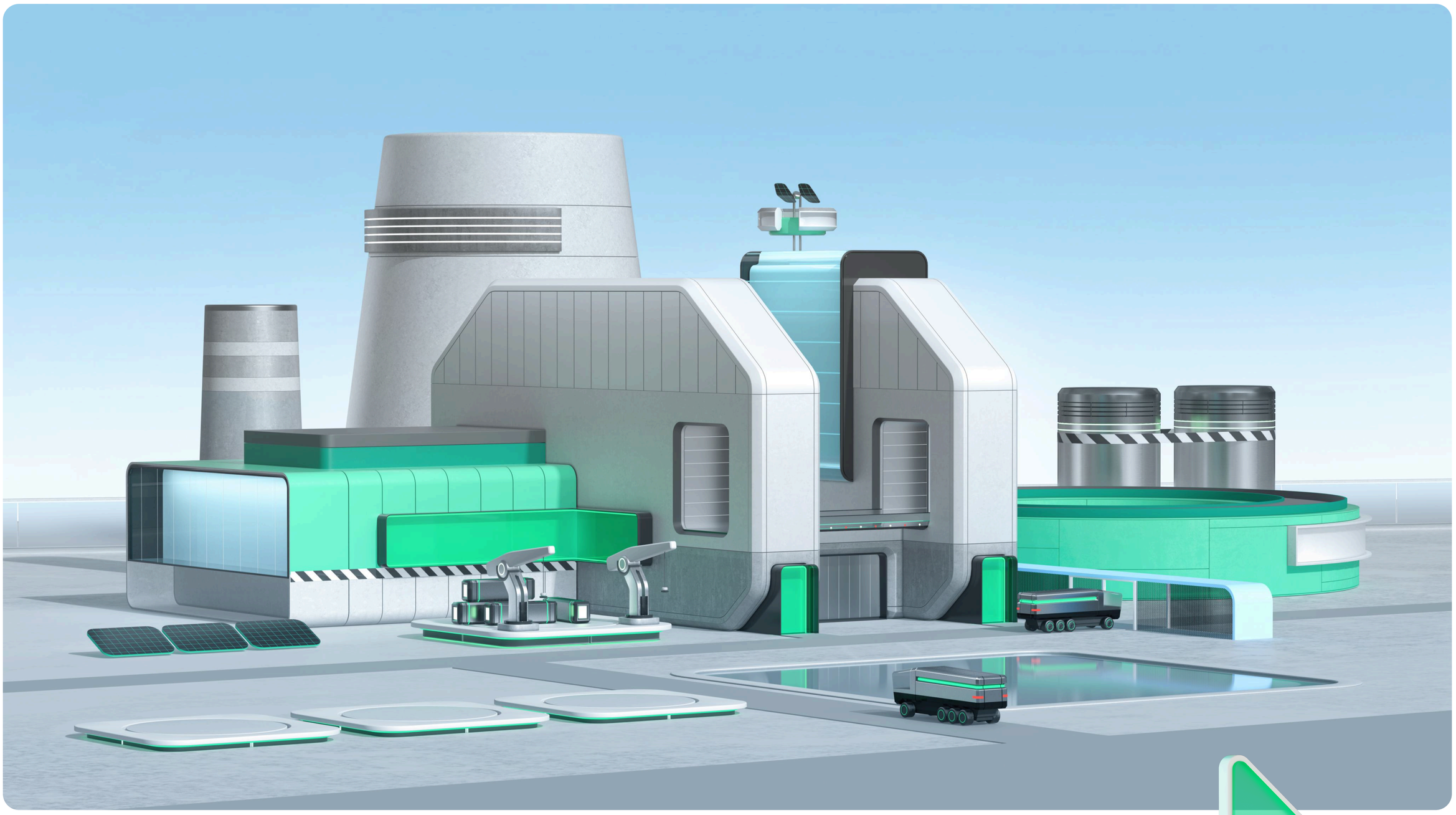
Container environment protection in the energy sector with Kaspersky Container Security

A major Russian energy company chose Kaspersky Container Security for the centralized protection of its container infrastructure

kaspersky



Background

Choosing a solution

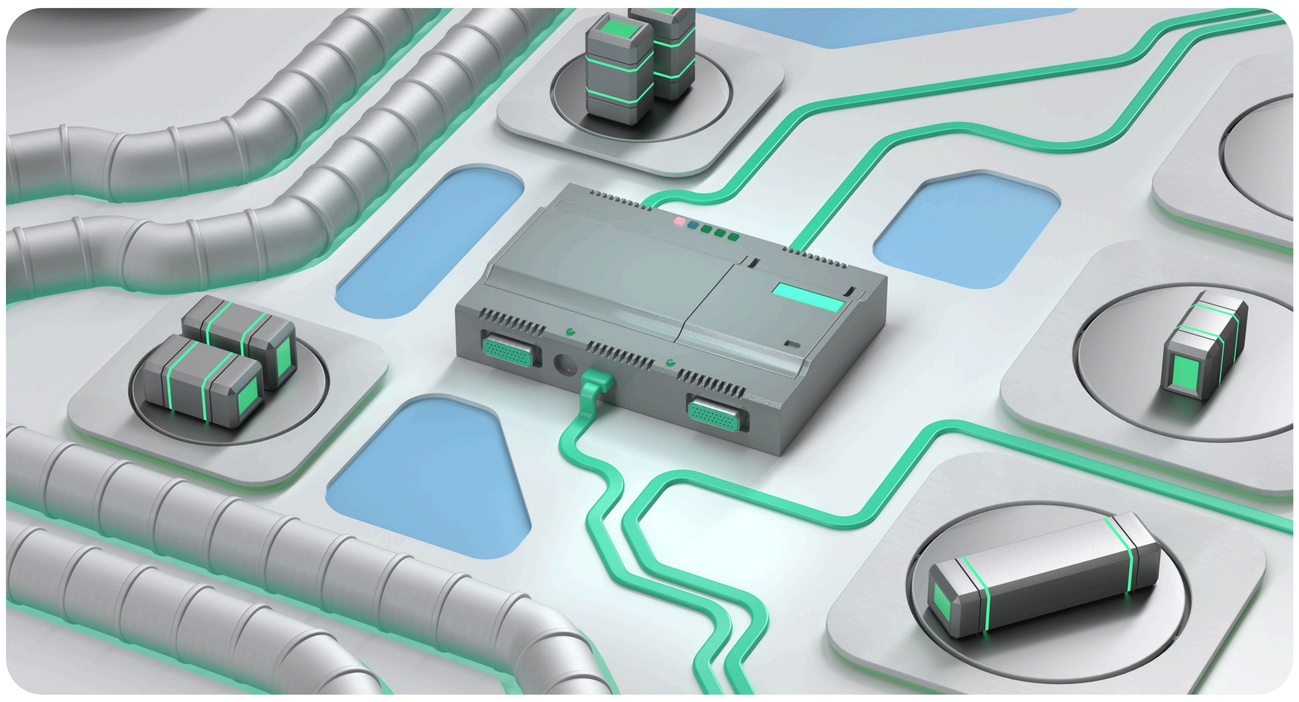
As the company's container infrastructure evolved and security requirements increased, the need arose to migrate from an open-source solution to a more reliable and user-friendly domestic product. The key drivers were a need for timely updates, professional technical support, and greater control over security processes.

The energy company also prioritized **analyzing the security of newly implemented systems and monitoring the emergence of zero-day vulnerabilities in existing services**. In the energy sector, any failure can have critical consequences, so the continuity of internal services is imperative.

This case is from one of Russia's largest energy companies providing high-quality heat and power supplies throughout the country. In the energy industry, demands for IT infrastructure security are especially high because internal services must always remain operational.

Information security in the company was already at a high level of maturity with an in-house information security department with deep expertise, 24/7 SOC, and a dedicated DevSecOps team.

The company's container infrastructure is deployed on the Russian **Deckhouse** platform and used to create and maintain internal services. The platform includes test and production environments, which require reliable protection at all stages of the application lifecycle.



Kaspersky Container Security

Solution

Kaspersky Container Security (KCS) is a specialized security solution for all key elements of container environments and containerized applications at all stages of the lifecycle, from development to operation.

Benefits of Kaspersky Container Security

- **Specialized solution** from a reliable international vendor based on best global practices
- **Designed for the architecture** and specific risks of container environments
- All-in-one solution to protect the orchestration environment, registries, images, container applications, and microservice development pipelines
- **Proprietary developments** (Policy Engine, Admission Controller, and eBPF) for flexibility and independence from open-source and third-party tools
- **Information on exploits** for identified vulnerabilities
- Enterprise-class solution **with 24/7 support**

Containerization is a more lightweight alternative to virtual machines. It's used to run isolated applications (microservices) on a host operating system with a shared OS kernel. Application code is bundled into a container along with all the dependencies required for its launch and operation.

This technology accelerates the process of creating and delivering applications. However, the architecture of container environments (for example, the lack of a separate guest operating system and their highly dynamic nature) make effective protection by traditional endpoint protection solutions impossible.

Kaspersky Container Security (KCS) is a specialized security solution for all key elements of container environments and containerized applications across all lifecycle stages, from development to operation. KCS protects business processes and helps organizations comply with industry standards and security regulations, as well as implement secure software development (DevSecOps).

Kaspersky Container Security launched on the global market in autumn 2023 and is developing rapidly thanks in part to close collaboration with users and their feedback.

Key features:

Integration into the development process

- Integration with image registries and CI/CD platforms
- Integration with security and notification systems
- Open API for easy integration with environments

Automatic inventory of cluster resources

- Informative dashboards and widgets
- Visualization of cluster resources, network interactions, associated risks, and policy execution directly on the graph

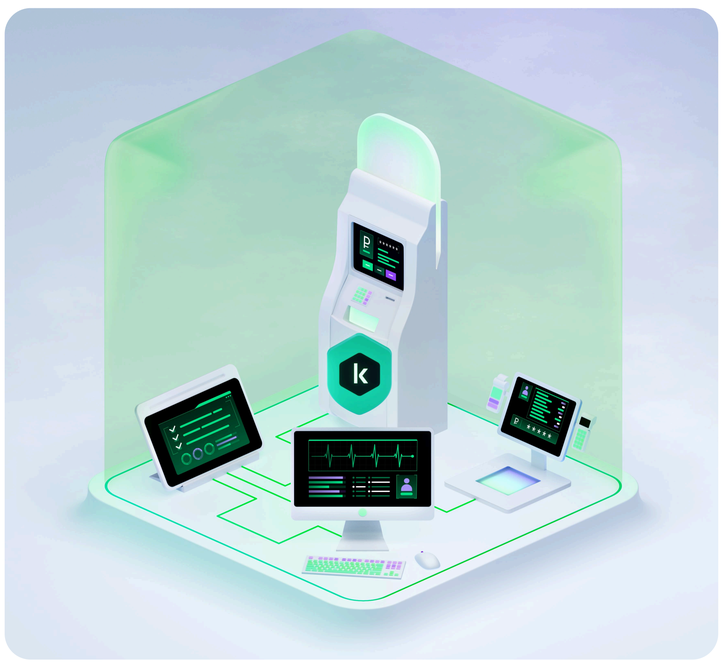
Runtime container protection

- Integration with orchestration platforms
- Container behavioral analysis based on a variety of criteria
- Modes to block and audit illegitimate activities

Regulatory compliance audit

- Checks the compliance of images and the orchestration environment with information security standards and best practices
- Uses 30+ vulnerability databases, including Data Security Threats Database from Kaspersky, and NIST
- Automation of routine checks and actions

KCS vs. Open-source



Open-source solutions are widely used for container environment protection. But it requires support, fine-tuning, and integration for multiple independent open-source tools, often with the use of custom components. This increases demands on the information security team and its level of expertise.

Plus, there are no guarantees that open-source components are free of vulnerabilities and bugs, have regular functional updates, or use relevant threat databases.

Benefits of Kaspersky Container Security compared to open-source solutions

- **Comprehensive protection for all** container infrastructure elements and application security at all stages of their lifecycle. This translates into significant savings in resources and time compared to developing a custom solution based on multiple open-source tools
- KCS **doesn't increase or impose new requirements** on the number and qualifications of employees
- **A single console** for configuration and management instead of multiple interfaces
- **30+ vulnerability databases**, including Kaspersky's own, NIST, and Kaspersky Open Source Software Threats Data Feed to identify vulnerabilities and threats in open-source components
- **Regular updates** of threat databases and information on exploits and their exploitability
- **Regular software updates**, bug fixes, and expanded functionality
- **Kaspersky's proven expertise** in cybersecurity, secure development, and antivirus solutions
- **24/7 customer support** — one of the most essential features of Enterprise-class solutions

Results

Implementation resulted in a significant increase in security service efficiency:

- Faster security assessments of container applications
- Quick integration with third-party services using the API reduced deployment time
- New user-friendly interface for comprehensive security assessments of images and clusters
- Lower labor costs for runtime protection and security analysis
- Centralized formation of security expertise instead of across disparate systems

The company made their decision based on **Kaspersky's reputation** as a global leader in cybersecurity trusted by major companies across a range of industries, as well as the product's **technical advantages: support for a wide range of tools, a focus on security** built into the solution at the development stage, and extensive **API integration capabilities**.

Other key considerations included **integration with common image registries** and CI systems, risk management, and an open API for interacting with the company's internal systems.

Implementation was a success despite the need to adapt to Deckhouse-powered Russian infrastructure, Astra Linux operating systems, and other domestic solutions. During integration, changes were made to boot priorities to ensure proper operation at runtime in the Cilium network environment. The pilot project lasted almost a year but never faced any major issues—Kaspersky experts helped resolve all problems promptly.

A notable achievement was the integration of KCS with the corporate information security portal, allowing for the centralization of container application security assessment processes.

"Migrating to Kaspersky Container Security significantly increased the protection of our critical container infrastructure. Centralized security management and integration with our internal processes has proven to be particularly valuable. In the energy industry, where system uptime is critical, comprehensive protection and control on this high a level is essential."

Aleksey Timonin
Information Security Expert

"Kaspersky Container Security integrated into our existing SDLC process and simplified the Shift-Left approach to container environment security. I see the key advantages of KCS in the ability of its unique architecture to simplify scalability, and its extensive functionality for the flexible implementation of established security policies."

Alexander Dyachenko
Information Security Expert