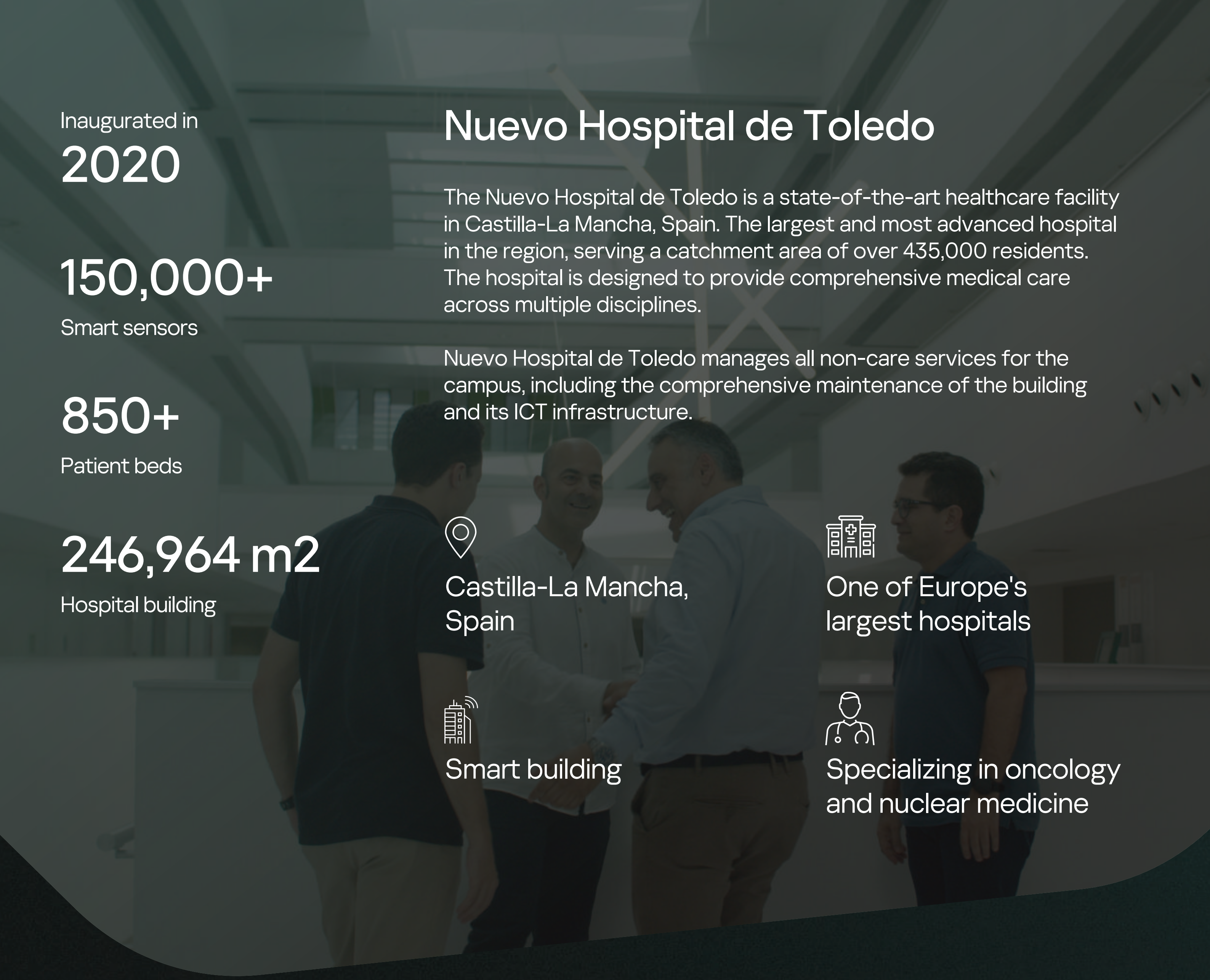
Cybersecurity of Operational Technology

at Nuevo Hospital de Toledo

kaspersky BRING ON THE FUTURE



Inaugurated in
2020

150,000+
Smart sensors

850+
Patient beds

246,964 m2
Hospital building

Nuevo Hospital de Toledo

The Nuevo Hospital de Toledo is a state-of-the-art healthcare facility in Castilla-La Mancha, Spain. The largest and most advanced hospital in the region, serving a catchment area of over 435,000 residents. The hospital is designed to provide comprehensive medical care across multiple disciplines.

Nuevo Hospital de Toledo manages all non-care services for the campus, including the comprehensive maintenance of the building and its ICT infrastructure.

Castilla-La Mancha, Spain

One of Europe's largest hospitals

Smart building

Specializing in oncology and nuclear medicine

Cybersecurity partner

Nuevo Hospital de Toledo has committed to a long-term partnership with Kaspersky to collaborate on cybersecurity with an intention to expand.

The Challenge

The Nuevo Hospital de Toledo was concerned with an overall lack of visibility and governance of their IT infrastructure and maintenance of their non-healthcare services like gas & lighting control systems, and air conditioning – the building's integral maintenance. The hospital was brand new and the transition from the construction phase of the building to the operational phase highlighted some gaps in asset management, cybersecurity, and compliance. The hospital recognized that it faced vulnerabilities in both IT and OT networks that needed to be addressed.

These issues highlighted the need for a full audit to assess the status quo and a robust solution to secure and manage the hospital's IT and OT environments.

Kaspersky Industrial CyberSecurity

Kaspersky Endpoint Detection and Response Optimum

Why Kaspersky?

The hospital needed a partner that offered a wide range of products and services. They evaluated several suppliers and selected Kaspersky because of the quality and fit of the products, the professionalism of the team, the clarity of the pre-sales process, and the performance of the products during the proof of concept phase.

The Kaspersky solution

To meet the challenges that Nuevo Hospital de Toledo faced, the Kaspersky team first deployed Kaspersky Endpoint Detection and Response. This rapidly provided powerful security with comprehensive visibility across all endpoints on the corporate network.

Even more so than the IT network though, this project was about securing the hospital's vital OT network. To that end, there was a deployment of Kaspersky Industrial CyberSecurity (KICS), which consists of two interconnected elements: Kaspersky Industrial CyberSecurity for Nodes, designed to protect industrial operator panels, workstations, and servers; and Kaspersky Industrial CyberSecurity for Networks, which monitors the security of industrial networks.

Kaspersky Industrial CyberSecurity (KICS) is a native Extended Detection and Response (XDR) Platform for industrial enterprises, designed and certified to protect critical OT equipment, assets, and networks from cyber-initiated threats.

The Nuevo Hospital de Toledo needed a solution that provided:

- ✓ Full audit of IT and OT infrastructure
- Secure the OT network
- Regulatory Compliance
- Visibility and Governance

José Carlos Fernández

IT Manager and CISO,
Nuevo Hospital de Toledo.

> We chose Kaspersky because we needed a provider offering not just products, but a full range of services. What truly set them apart, however, was their commitment to clarity and hands-on support. The tools did exactly what they promised, and the confidence that came from this transparency and reliability made Kaspersky the right choice.

Advantages

- Asset Inventory
- Vulnerability and Risk Assessment
- Comprehensive Security and Compliance Audit
- Non-Intrusive Modular Deployment

Outcomes

The successful completion of the project has led to several positive outcomes for Nuevo Hospital de Toledo. Firstly, the IT teams now have full visibility and control of their systems, allowing the hospital to manage their IT and OT systems with improved governance and oversight. This has resulted in a substantial reduction of security vulnerabilities and meant that the hospital can gain compliance certification for the National Security Scheme in Spain.

Operationally, the hospital optimized server load and network performance by detecting and resolving OT device configuration issues, freeing up resources for other technical priorities.

Financially, the project brought strategic cost savings by consolidating suppliers and reducing training requirements and support costs.

The partnership also established a solid foundation for ongoing collaboration, with the potential for deploying further security solutions like SIEM in the near future.

Kaspersky Industrial CyberSecurity

Learn more

www.kaspersky.com

@kaspersky
#bringonthefuture