



# A network and infrastructure that provides real-time insights

Told by Ken Vanden Haesevelde, Securitas IT Infrastructure Lead, Belgium and Luxembourg in partnership with Wim Vancluysen, Kyndryl Customer Partner



## Securitas has been making the world a safer place for 90 years

With 57,000 security endpoints monitored in the Security Operations Center (SOC), the Belgian Securitas operations team processes more than 3 million alarms a year. In Belgium, the company safeguards people, enterprises, private residences, and critical environments including airports, banks, government and military sites, hospitals, nuclear sites, police zones, ports and NATO HQ. They step in to resolve more than 68,000 situations in customer locations, some triggering police or firefighter response.

Ken Vanden Haesevelde, the Securitas IT Infrastructure Lead for Belgium and Luxembourg, describes the Securitas Belgium Security Operations Centers (SOCs) as the “beating heart of their security services.” Always-on system availability in the SOCs is essential to guaranteeing communications with guards on the ground.

In addition to the critical SOC communications, essential business applications enable Securitas guards, operators and staff to access their operational data, anytime and anywhere. Securitas employees, including those working from home, can access timecards and orders for training, uniforms, badging and equipment, HR, payroll and more.

Ken knew that the Securitas aging Tier 2 datacenters were experiencing increasing latency. He had sleepless nights worrying if or when infrastructure performance might compromise the safety of guards in the field.

Any outage would put client trust at risk and threaten the reputation of Securitas. And business expansion plans hinged on upgrading to modern infrastructure that would ensure operations performed with high efficiency at scale.

## Advanced, scalable technology to ensure resilient systems

With datacenter performance challenges and the need to support future business, Ken saw an opportunity to address both with a single solution. Consulting with Wim Vancluysen, his Kyndryl partner, Ken envisioned a modernized infrastructure with:

- **A modern, advanced infrastructure** in a Tier 4 datacenter
- **Scalability on demand**, with plenty of room for business growth
- **Fit-for-purpose systems** designed for today and future-proofed for next-generation security technology

For years, Securitas relied on Kyndryl as a trusted managed services partner and saw the team as an extension of their own. So Kyndryl was a natural choice for collaborator on Securitas' infrastructure and network transformation.

Specially trained security officers with innovative data technology such as rugged phones with sensors that alert the SOC if a person is down, and AI capabilities, help provide fastest-possible responses. It's vital that communications are up 24/7 to comply with security and resilience industry standards.

Securitas SOC operators continually monitor customer sites with cameras and react when alarms go off, which may generate police or firefighter involvement. Incidents in the field need to be addressed within seconds.

## Migrating IT operations with zero downtime for operations and customers

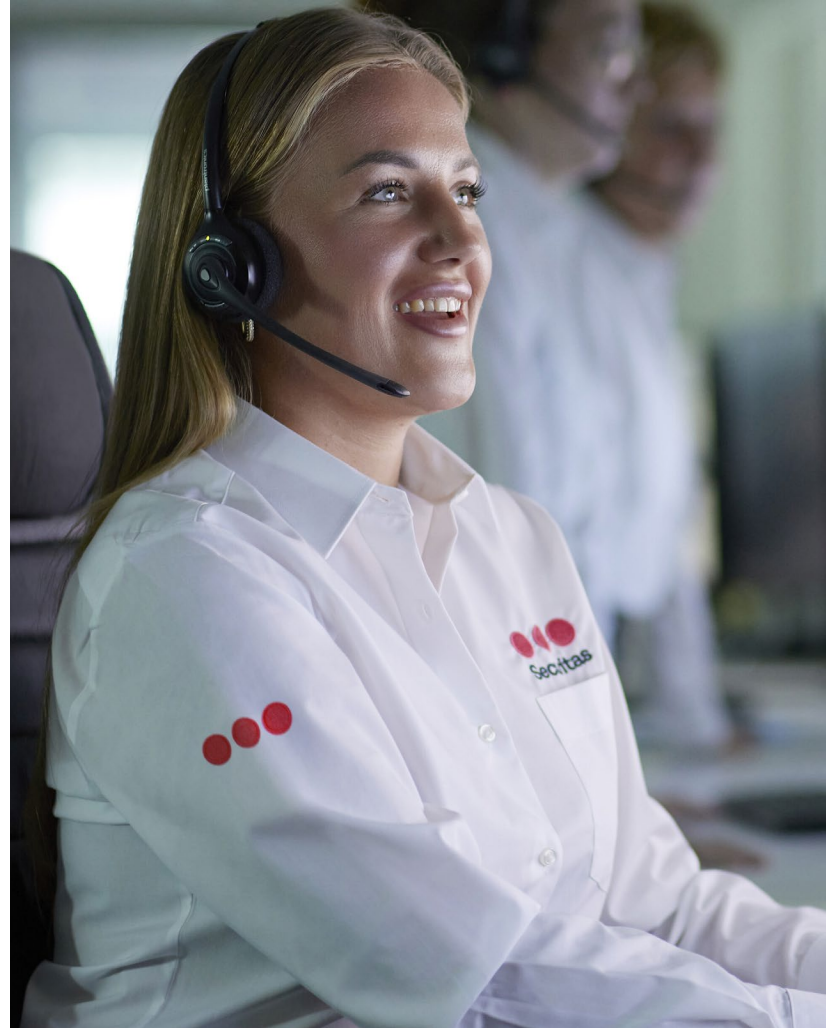
While maintaining business continuity in production, Kyndryl experts would work to introduce complex network services, monitoring for each Securitas customer, software support and a managed service desk, back-up and disaster recovery, and infrastructure management services.

Then, they'd need to install new hardware and networking systems and test the connections from the new data centers to client sites and the SOC—all ahead of planning the existing system migration. Working with Kyndryl as a single partner for both business as usual and the new solution helped Ken mitigate risks in coordinating the parallel efforts.

## High-availability infrastructure designed to keep thousands of customers safe

Together, the Securitas and Kyndryl team scoped, designed and implemented new server and network infrastructure. Using VMware® tools, they migrated existing systems and applications to the new Kyndryl datacenter in southern Belgium. Using redundant links and dedicated customer VPN tunnels, the network now connects all core applications with 24/7 availability and added security layers around firewalls and load balancers.

To maintain the same high service levels for new and existing clients, Kyndryl networking experts needed to deploy higher bandwidth connections. These would ensure low latency communications between core applications and across operations.



“We we needed a new solution, which encompassed new connectivity, new hardware, and new infrastructure to deliver services as we promise to our clients.”

- Ken Vanden Haesevelde, Securitas IT Infrastructure Lead, Belgium and Luxembourg



*Ken Vanden Haesevelde and Carolle Van Dijck, Securitas*

A disaster recovery solution at the new datacenter complex was implemented by Kyndryl. Redundant networking between Securitas service centers, offices and datacenter sites ensured critical applications were available throughout deployment. Examples of improvement results include:



**Recovery Time Objective (RTO) measured in minutes not days**, so in case of an outage critical applications have excellent RTOs



**More than 100 virtual machines migrated**, including multi-tier networks and the security layer, together with end-to-end connectivity for Securitas' customers



**Project completed in just 4 months**, without business interruptions

As part of new business as usual operations, Kyndryl enforces security parameters for each system, and keeps backup and recovery documents up to date for security compliance, easing the burden on Securitas.

**Kyndryl Bridge™** proactively recommends solutions for issues that have not yet occurred and automates issue resolution as permissions allow. Kyndryl Bridge AIOps extends ITSM efficiency by applying solutions to issues tracked over years in thousands of other customer engagements to the Securitas systems. The team expects up to 90% of issues to be automatically resolved as their ITSM evolves and critical applications and system resilience are boosted.

Fix once and resolve-for-all is achieved with IT Service Management (ITSM) software to track system and performance. As they resolve issues, the team creates and distributes **Red Hat® Ansible®** playbooks across all servers, for automated issues resolution, with 50 playbooks running in the Securitas infrastructure deployment. The team also uses RedHat Ansible for software updates and patches, important to applying compliant systems.

Ken cites Kyndryl's ongoing communication as a significant reason for the success of the operations and ongoing reassurance the Securitas clients are secure. The Securitas and Kyndryl operations team includes global experts working from more than five nations and in multiple languages. The team is far-flung but keeps in close contact, talking nearly every day.





“Over the years, Kyndryl has always been a Securitas trusted partner through various IT transformations, infrastructure changes and datacenter migrations. Kyndryl exceeds themselves every time with very thorough planning and speed to act all while upholding a superb level of professionalism in all levels of their organization.”

- Ken Vanden Haesevelde, Securitas IT Infrastructure Lead, Belgium and Luxembourg

The modernized infrastructure solution already has proven its business value in being able to accommodate company growth. In July 2022, Securitas announced the acquisition of Stanley Security, the Electronic Security Solutions business from Stanley Black & Decker Inc., growing their worldwide client base to more than 500,000 clients, and expanding their technology capabilities.

The Securitas leadership team extended its Kyndryl partnership with an expansion and approximately 100 new virtual machines to help support the **Stanley Security** acquisition. The project was completed at the end of February 2024.

### What progress looks like

A key success outcome is that the modernized high-availability network and infrastructure have eliminated latency issues for end-to-end, fail-proof communication between the SOC and guards. This helps ensure the security of the company’s thousands of customers.

The migration to Tier 4 datacenters took just 4 months—without interruptions, maintaining business continuity for thousands of customers. Disaster recovery initiation for critical applications takes minutes, not days. With 50 playbooks implemented to solve incident alerts automatically and eliminate false alerts, service helpdesk resolution time goals are consistently exceeded. The anticipated 90% standardized ITSM task automation will help free IT experts from routine tasks to work on higher value projects.

Above all, the low latency of the new solution gives Securitas the solid foundation the team needs to evolve services based on remote monitoring technologies, which is the company’s strategic business goal. Ken reports an additional key measure: being able to sleep better at night.



## About Securitas

Based in Stockholm, Sweden, Securitas is a world-leading safety and security solutions partner offering on-site and mobile guarding, aviation and electronic security, fire and safety services and enterprise risk management.

Securitas' Belgium employees monitor over 55,000 security endpoints, including residential customers, small organizations, and critical enterprise operations. More than 3.1 million alarms are processed annually, resulting in 53,200 effective interventions.

What's your next digital business challenge?

Let's tackle it together. →

## Meet the team



**Ken Vanden Haesevelde**  
Securitas IT Infrastructure Lead,  
Belgium & Luxembourg



**Carolle Van Dijck**  
Securitas Corporate  
Communications Manager



**Wim Vancluysen**  
Kyndryl Customer,  
Partner



**Marta Bawor**  
Kyndryl Delivery,  
Partner



# kyndryl.

© Copyright Kyndryl, Inc. March 2024

Kyndryl is a trademark or registered trademark of Kyndryl Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl Inc. or other companies. This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice.