Healthcare Cybersecurity: Protecting Patient Data and Ensuring Continuity of Care

With Eye Security, SHG Groep gains continuous visibility into its IT environment, proactive threat detection, plus the confidence to protect patient data and ensure uninterrupted healthcare delivery.

The status quo

For SHG Groep, cybersecurity is a fundamental part of delivering safe and reliable care.

Digital systems underpin nearly every aspect of daily operations. When these systems fail, care delivery slows or stops entirely.

This risk became tangible when a system outage rendered one of SHG's pharmacies inoperable for three days. Staff were unable to access essential information, and services were interrupted.

The incident showed how deeply dependent healthcare delivery had become on stable and secure digital infrastructure.

Protecting digital infrastructure from within

At the same time, SHG's IT leadership recognised a deeper structural issue: there was no effective way to detect threats once attackers had breached the environment.

> "We had focused on keeping attackers out. But if someone did get in, we would not have immediate visibility."
>
> Guts Wissema, ICT Coordinator, SHG Groep

Implementing the solution: adopting an "assume breach" mindset

SHG's board recognised the urgency. Cybersecurity had become a strategic priority to ensure continuity of care and maintain patient trust.

To respond to this need, SHG sought a cybersecurity partner capable of providing continuous monitoring, threat detection, and strategic guidance. Eye Security stood out for its "assume breach" approach, the recognition that no organisation can prevent every intrusion but every organisation can detect and respond effectively.

Eye Security deployed 24/7 monitoring, vulnerability detection, and centralised visibility across SHG's infrastructure, supported by continuous analysis from its Security Operations Centre (SOC). Further, SHG received access to a centralised security portal that gave leadership clear, real-time insight into their security posture.

SHG gained a full overview: which devices are compliant, where vulnerabilities exist, and which risks require attention. The platform also provided proactive alerts about emerging threats, along with concrete recommendations to mitigate them. Regular strategic check-ins ensured ongoing alignment between SHG and Eye Security's experts.

During implementation, healthcare professionals could continue their work, without even noticing the security controls operating in the background.

Results, effectiveness, and benefits: peace of mind and operational stability

The most immediate benefit was visibility. SHG could now detect threats early, understand risks clearly, and act before incidents escalated.

Continuous monitoring ensures that suspicious activity such as compromised credentials or unusual system behaviour is identified and addressed promptly.

The greater impact

The impact extended beyond technical improvements. Healthcare professionals experienced greater confidence and stability in their daily work. They could rely on systems being available, secure, and resilient. Security now operates quietly in the background, protecting systems without interfering with clinical workflows.

SHG's leadership gained assurance that their environment is actively monitored and protected at all times. This allows executives and staff to focus fully on their primary mission: delivering high-quality patient care.

About the company

SHG Groep is a foundation with eight health centers and six pharmacies in the Haaglanden region of the Netherlands. The organisation provides comprehensive primary care services to tens of thousands of patients. Strengthening cybersecurity is a key component of its mission to deliver safe, trusted healthcare services.

www.shg.nl