



CASE STUDY

Gemalto Partners with AvaSys to Deliver High Speed Encryption for Integrated Healthcare System CCTV Data

An Integrated Healthcare system of hospitals needed a high speed encryption solution to protect their sensitive closed-circuit TV (CCTV) data, ensuring uninterrupted secure video feeds that comply with their privacy policies while resulting in near zero impact on their data network.

The Organization

AvaSure, a division of AvaSure Holdings, Inc., develops, markets and deploys technology and educational tools that support the nursing profession in improving its practice environment. They were able to provide their customer, an Integrated Healthcare system of hospitals, with a monitoring solution that met their requirements, but the sensitive CCTV data being observed by hospital administrators was not being protected from intrusion, manipulation, or capture.

Challenge

- > The end customer needed to encrypt its real time video data, ensuring secure patient monitoring with no feed disruption while still maintaining network performance.

Solution

- > By adding SafeNet Ethernet Encryptor CN4010 appliances onto the data network in a hub and spoke topology, an end to end encryption solution was enabled that secured data from each network camera all the way to the desktop monitoring system.

Benefit

- > The end customer can now ensure that all of their CCTV video data is encrypted with SafeNet Ethernet Encryptor CN4010 appliances from Gemalto, thus helping to ensure that they are protected from data intrusion, capture, or manipulation.

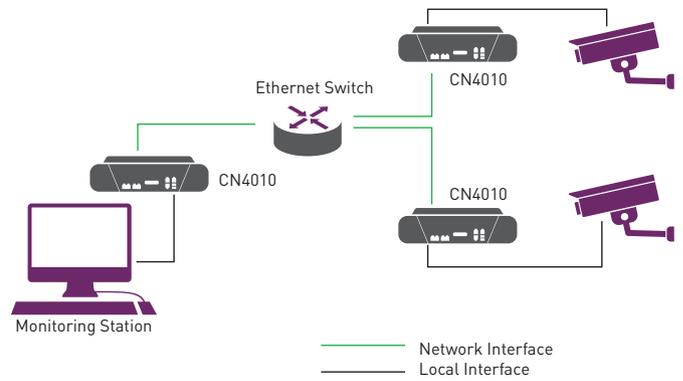
The Business Need

AvaSure's video monitoring platform, AvaSys, is an advanced closed-circuit television (CCTV) based patient observation and communications e-health initiative which benefits hospital patients through enhanced monitoring and care. This unique solution has been adopted by hospitals all across the U.S. The Federal Integrated Healthcare System of hospitals heavily relies on the AvaSys solution for continuous monitoring, and high quality, up-to-the second reliable feeds are required to ensure the well-being of their patients across the country. As their patient monitoring networks evolve, it is imperative that they protect against the vulnerabilities that CCTV data feeds can be exposed to:

- > **Patient privacy and data capture concerns.** Regulations such as HIPAA make it abundantly clear that any U.S. hospital has the responsibility of maintaining the privacy of its patients and their data. Hospitals must go to certain lengths to ensure that their patient confidentiality is kept secure, and defending against CCTV feed exposure, unauthorized access, capture, and manipulation is a large component of that defense.
- > **Higher bandwidth requirements vs. network performance.** With the advent of technology such as high-definition video capabilities, CCTV networks, now more than ever, are facing the ongoing tradeoff of improved video quality vs. increased network bandwidth due to the size of the video stream, which can introduce network latency. In an industry vertical such as healthcare, deploying an encryption solution that is designed to scale for additional bandwidth requirements removes the concern of latency and choppy, sluggish video feeds. A hospital administrator monitoring the video feed can recognize the signs of a potential catastrophic event in real-time and take preventative action.

The Solution

In a simple hub and spoke topology, SafeNet Ethernet Encryptor CN4010 appliances were wired to a camera in each room and then back to the core network switch. At the monitoring station, a SafeNet Ethernet Encryptor CN4010 was also placed between the monitoring station and the network switch.



The Benefits

Utilizing the SafeNet Ethernet Encryptor CN4010 appliances to encrypt the video feed of the AvaSys CCTV solution ensures that the hospital CCTV networks are being enabled with the optimal security, maximum network throughput, low latency, and flexibility for the future they need to meet their privacy objectives.

- > **Top rated security.** SafeNet High Speed Encryptors use the strongest publicly available cryptographic algorithms developed by NIST (the Advanced Encryption Standard AES-256). The appliances are crypto-agile, using field programmable gate array (FPGA) technology that allows them to be easily upgraded in the field to keep pace with the evolution of cryptographic advancements. The tamper-proof design appliances are certified to FIPS 140-2 Level 3 and Common Criteria, providing a top rated "security focused" encryption solution for sensitive data.
- > **Maximum network performance.** Gemalto's high speed Layer 2 encryption technology introduces zero protocol overhead so that maximum bandwidth is available for data – up to 50% more efficient than competing technologies. SafeNet High Speed Encryptors provide the fastest network encryption available, operating at true line speed with no impact on latency, ensuring the high quality of real-time applications such as VoIP and video. High availability features support architectures with over 99.99% uptime.
- > **Easy deployment.** The effort to add the SafeNet Ethernet Encryptor CN4010 units to the existing Layer 2 network was effortless due to the "bump in the wire" design aspects of the appliance. There's no need for network reconfiguration, so SafeNet Ethernet Encryptors can be set up in minutes. The unique features of SafeNet High Speed Encryptors enable them to be seamlessly overlaid onto any network topology.
- > **Scalability.** The "bump in the wire" drop-in design allows SafeNet High Speed Encryptors to support hundreds of concurrent encryption connections, securing all data on large networks. With flexible line speed license offerings, the customer can simply "pay as they grow", increasing their secure monitoring and bandwidth capabilities.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us

Follow Us: blog.gemalto.com/security

 GEMALTO.COM

gemalto
security to be free