CASE STUDY

<table>
<thead>
<tr>
<th>Application of High-Assurance Network Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sector: Government</td>
</tr>
<tr>
<td>Use Case: CCTV Network data security</td>
</tr>
<tr>
<td>Solution: Secure, multicast HD video transmission in real-time; across Layer 2 network architecture</td>
</tr>
</tbody>
</table>
Global CCTV network and surveillance service provider chooses Senetas high-assurance encoders to protect CCTV network transmitted data.

**CUSTOMER CHALLENGE**
**SECURING SENSITIVE CCTV NETWORK TRANSMITTED DATA**
Our client is a specialist in delivering secure surveillance information in challenging environments. They work with governments and multinational corporations on the most complex and critical surveillance challenges within the defence, law enforcement and critical infrastructure sectors.

Working with a law enforcement organisation in Northern Europe, the challenge was to design a secure video distribution infrastructure that would allow sensitive CCTV streams to be securely distributed across the whole country.

CCTV technology is commonly used to help protect high-profile, high-risk locations such as airports, public buildings, military bases, oil and gas facilities, sports arenas and public transport systems.

Demand for live video has led to a proliferation of network video traffic; much of which is sensitive and must be securely and efficiently transmitted across communication infrastructures.

Specifically, CCTV data requires protection against privacy breaches, input of rogue data and any unauthorised access that may adversely affect the CCTV data’s integrity.

Efficient video distribution (which typically involves very large volumes of data) uses multicast transmission protocols to ensure that data is only sent to devices that have requested it.

**LAYER 3 LIMITATIONS**
**IPSEC ENCRYPTION IMPACTS NETWORK PERFORMANCE**
Our client initially considered a solution based on a Layer 3 routed data network, with all traffic to be encrypted using the common IPsec security protocol.

IPSec is an industry standard for securing data across Layer 3 routed data network environments it is optimised for use on “best-effort” networks such as the Internet.

However, the IPSec protocol has several limitations, especially when high-performance delivery of the CCTV feeds is required (EG. maximum speed, low latency and minimum network overhead).

There are also issues of complexity that arise when encrypting at Layer 3. IPSec encryption solutions typically require customers to increase the network bandwidth at considerable cost to help overcome some of these limitations.

IPSec introduces a high additional per frame overhead that may generate significant additional network bandwidth and latency when compared to the unencrypted traffic.

Also, securing multicast encryption at Layer 3 is problematic because the underlying network requires additional routing protocols to support multicast traffic, such as the Protocol-Independent Multicast (PIM) routing family.
SENETAS SOLUTION
HIGH-ASSURANCE NETWORK DATA PROTECTION

With the disadvantages of transmitting encrypted multi-location CCTV data across Layer 3 network links clearly identified, an alternative network architecture was required.

The alternative network architecture proposed was based on a pure Layer 2 WAN service with high-speed encryption at the Ethernet layer.

Senetas CN high-speed encryptors would not add overheads to the network data; offered near-zero latency and have no impact on other network assets.

At Layer 2, Senetas encryptors provide far simpler ‘set and forget’ implementation and ongoing management; making the solution much more efficient, both technically and financially.

Because Layer 2 encryption occurs at the data link layer on Ethernet networks, the Ethernet payload is encrypted but the Ethernet header (including MAC addresses and VLAN identifiers) is unmodified; allowing transmission across service provider networks.

The Ethernet payload fully encapsulates the IP header and IP payloads (which are also encrypted), providing the additional security benefit of hiding all IP addresses in the transmitted data.

By taking advantage of the underlying Layer 2 network characteristics, encryption at Layer 2 may deliver 100% encrypted throughput, even at speeds up to 10Gbps, with little or no additional per frame overhead.

Senetas CN encryptors protect data transmitted from approximately one hundred end-points throughout northern Europe; from where video traffic is distributed.

By reducing latency and network overheads, and minimising technical complexities, Senetas CN encryptors maximise the available bandwidth. As a result, the customer is able to significantly reduce its bandwidth and network management requirements; generating significant cost savings.

BUSINESS BENEFITS
HIGH-PERFORMANCE, LOW-LATENCY CCTV NETWORK

Senetas CN series Ethernet encryptors provide certified information security; with full line rate encryption for all data transmitted across point-point, hub and spoke and fully meshed data network environments.

Network performance is maximised for delivery of multicast as well as unicast traffic. Simple, automatic ‘zero-touch’ key management ensures that encryption scales efficiently to the largest deployments.

The continuous and consistent near-zero latency performance is enabled by Senetas’s unique technology – purpose built hardware encryption devices that perform cut-through processing of network traffic at wire speed.

Their tamper resistant chassis provides protection to all encryption keys and user credentials at government certified levels.
Senetas CN encryptors hold certifications from all leading, independent testing authorities – FIPS, Common Criteria, CAPS and NATO.

To assist the ease of implementation and encryptor management, Senetas CM7 remote management software is provided to all customers.

Large numbers of encryptors are easily and securely managed using Senetas CM7. Using SNMPv3 this tool provides simple, secure remote management either (out-of-band or in-band) using the encrypted Ethernet port.

Other important benefits realised by our client include:

**>> FLEXIBILITY AND INTEROPERABILITY**
Senetas’s unique Field Programmable Gate Array enables customisation flexibility and all CN encryptors are interoperable, providing an efficient long term investment.

**>> ZERO IMPACT**
Senetas CN encryptors have no impact on other network assets and do not require any network changes during implementation.

**>> OUTSTANDING RELIABILITY**
Senetas encryptors provide 99.999% uptime in the most demanding 24/7 availability environments. Their defence-grade design and manufacture ensure peace of mind.

**>> FIELD UPGRADABILITY**
Among the various CN encryptors, many have field replaceable and upgradeable components.

**>> SCALABILITY**
Unlike other encryption solutions, Senetas CN series encryptors are scalable to as many as 300 connections.

GLOBAL SUPPORT AND DISTRIBUTION
Senetas CN series encryptors are supported and distributed globally by Gemalto under its SafeNet encryption brand. Gemalto also provides pre-sales technical support to hundreds of accredited partners globally: systems integrators, networks providers, cloud and data centre service providers, telecommunications companies and network security specialists.