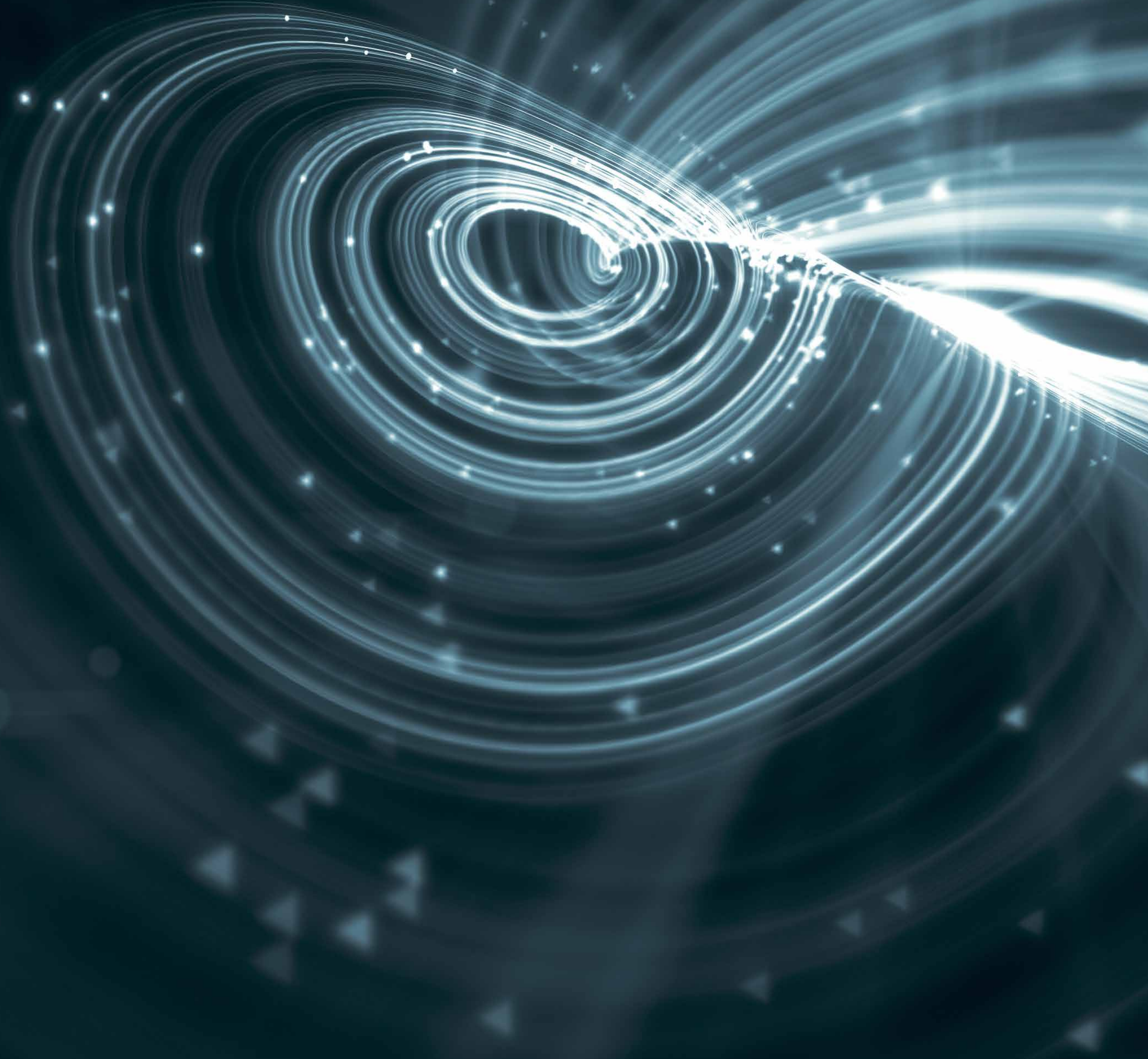
SENETAS

Security without compromise

SECURING REAL-TIME CCTV NETWORK DATA

SOLUTION PAPER



The high-speed networks used to transmit CCTV traffic require robust data protection, as they are sensitive to feed disruption and vulnerable to unauthorised access.

Closed Circuit TV (CCTV) has become a ubiquitous part of everyday life. Whatever its purpose – personal safety, asset protection or general environment monitoring – the sensitivity and integrity of the data collected is critical; as too is uninterrupted surveillance.

These requirements not only demand dependable data protection, but also reliable high-performance data networks. Both are essential to real-time high resolution CCTV monitoring and ensuring timely responses to threatening events.

Importantly, dependable data protection must not come at a cost of reduced network performance.

In recent years, CCTV technology has undergone some significant changes; not least of which have been the introduction of high-definition video, real-time streaming, face recognition and motion tracking.

As these features emerge, they generate larger volumes of data and increase the demand for high speed, high performance data encryption.

In many countries, the application of CCTV footage is tightly regulated, with compliance obligations established for the capture, streaming, storage, backup and sharing of video files.

The primary data protection considerations for CCTV are:

- Integrity – preventing interference with recorded video
- Disruption – ensuring uninterrupted, real-time coverage
- Privacy – regulatory compliance and theft prevention

The scale of modern CCTV networks, both private and public, means a typical network comprises multiple devices. As the number of devices increases, so does the complexity of the system and the number of points of potential weakness.

CCTV networks, like their IT infrastructure cousins, are not inherently secure. For most, it is not a case of if they will be breached, but when.

The most secure organisations focus on protecting the data itself, by encrypting it as it is transmitted across the network. So, when a network breach occurs, unauthorised parties are left with meaningless, encrypted data.

High-Assurance Encryption

Encryption provides the optimal, last line of defence for the protection of CCTV generated data.

CCTV networks typically have modest bandwidth (100Mbps - 1Gbps) and, because the video streams frequently need to be high-definition and real-time, they are sensitive to encryption latency and overhead.

Unlike other high-speed encryption solutions, Senetas high-assurance encryptors provide maximum data protection without compromising network performance.

The near-zero latency and data overhead of Senetas encryptors ensures optimal, real-time video streaming and 100% HD CCTV image quality. Time after time, tests prove that Senetas CN Series encryptors provide maximum image quality and real-time network performance.

Senetas high-assurance encryptors are certified by the world's leading independent testing authorities (FIPS, CAPS, Common Criteria and NATO) as being suitable for government and defence applications.

However, the high-assurance promise goes well beyond third party validation to include a range of industry-leading security features:

- Dedicated, secure and tamper-proof hardware
- State-of-the-art, client side key management
- Gapless, authenticated, end-to-end encryption
- Standards-based (AES-256) encryption algorithms

Threats to CCTV Systems

The nature and volume of the data transmitted across CCTV networks, combined with the inability to completely control and secure the network itself, makes CCTV data an attractive target for cyber-criminals.

The prevalence of high-speed networks, rapid Cloud computing adoption and the rise of the Internet of Things (IoT) exposes CCTV networks to an increased risk of unauthorised access. Data sniffing, injection, redirection or simple theft expose organisations to a wide range of potentially damaging consequences. Including:

- Financial Loss/Penalties
- Business Continuity
- Identity Theft
- Compliance Breaches
- Loss of Intellectual Property
- Damage to Reputation

Whether your CCTV network application is law enforcement, public safety or asset monitoring, its performance and data integrity are paramount.

Senetas CCTV Experience

Around the world, the adoption of high-definition CCTV applications has grown rapidly and new CCTV technology enhancements have greatly increased the volume of the data generated.

The increase in data volume and sensitivity has placed greater demands on data networks in terms of performance, security and reliability.

Senetas high-assurance encryptors have been selected to secure high-definition CCTV networks transmitting sensitive data across private networks for a wide range of government, healthcare, financial, law enforcement and commercial organisations:

Common CCTV Applications:

- Border Control
- Port & Airport Security
- Casinos & Gaming Venues
- Public Buildings & Spaces
- Military Installations
- Oil & Gas Facilities
- Critical Infrastructure
- Traffic Monitoring
- Public Transport Systems
- Patient Monitoring

Use Case 1: International Border Control

Our customer is a government agency responsible for providing integrated control and monitoring of international border security.

Having implemented an extensive CCTV network to monitor a number of major transport hubs, they opted for Senetas CN Series encryptors to ensure maximum network performance at 100Mbps.

Use Case 2: Patient Monitoring System

Our customer has developed an HD CCTV patient monitoring system, designed to increase the productivity of nursing staff at the same time as quality of care.

Senetas CN encryptors are used to provide real-time monitoring whilst protecting the CCTV network from disruption or the input of rogue data. The Senetas solution complies with FIPS 140-2 L3 security standards and strict US healthcare regulations.

Use Case 3: Secure Multicast Transmission

Our customer is a specialist provider of secure surveillance solutions, working with government and commercial partners in the most complex and critical HD CCTV environments.

Challenged to secure a nationwide video distribution infrastructure with over 100 end-points across Northern Europe, Senetas CN Series encryptors were used to deliver 100% encrypted throughput at speeds of up to 10Gbps – with no additional frame overhead.

CN SERIES HARDWARE ENCRYPTION

CN9000 Series

The CN9100 is the world's first commercially available certified high-assurance 100Gbps Ethernet network encryptor that supports all network topologies.

Like all Senetas CN encryptors, the CN9000 Series provides maximum high-assurance network data security, without compromising network and application performance. It boasts ultra-low latency of just 1.5 microseconds in customer testing.

Developed in collaboration with customers and service providers, Senetas CN9100 encryptors are designed to meet the exacting requirements of all 100Gbps use cases, making them an ideal application for securing public and private Cloud networks.

Senetas' CN and CV Series encryptors include integrated support for CypherTrust (Thales' centralised cryptographic key management solution) that provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

CN6000 Series

Senetas CN6000 Series encryptors provide highly secure, full line-rate transparent encryption for data moving across both dark fibre and metro/wide area Ethernet networks; in point-to-point, hub & spoke or meshed environments.

The CN6000 Series are rack-mounted, high-speed encryptors for business-critical applications; offering 1Gbps to 10Gbps bandwidth speeds. They are the optimal choice when you require:

- Efficient, investment-proof data encryption
- Multi-purpose, in-field upgradable and flexible hardware
- Choice of Common Criteria, and FIPS certifications
- Compact 1U form factor with advanced performance and power features

CN4000 Series

Network data security is a challenge to organisations of all shapes and sizes, to help address the encryption demands of smaller organisations and in-field operations, Sneetas developed the CN4000 series of compact encryptors.

Despite their small form-factor, Senetas CN4000 Series encryptors boast the same robust security credentials of their rack-mounted cousins.

The CN4000 series is the ideal low-cost, high-performance encryptor range for small to medium-sized enterprises (SME). They also provide a cost-effective "encrypt everywhere" solution for larger enterprises looking to secure remote or temporary locations connected via networks operating at up to 1Gbps.

Like all CN hardware encryptors, the CN4000 Series features standards-based encryption, secure key management and the peace of mind that comes from certification by the world's leading independent testing authorities.

WHAT MAKES CN SERIES ENCRYPTORS STAND OUT?

Performance

High Speed

Market-leading performance. Operating anywhere from 10Mbps or 100Gbps, Senetas encryptors consistently win competitive performance test.

Low Latency

Operating in full duplex mode, at full line speed, without packet loss. Latency is as low as 2 microseconds per unit at 100Gbps.

Zero Impact

The zero impact of Senetas encryptors is not limited to network bandwidth and latency; it extends to network operations and management.

Versatility

Crypto Agility

All Senetas encryptors are 'crypto-agile'; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

Topology Support

Senetas CN encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies.

Flexible Management

Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software.

Security

Certification

For over 20 years, Senetas R&D has remained committed to the principle of certification in depth. Senetas CN Series encryptors are certified by: FIPS, Common Criteria and NATO.

Key Management

All CN Series encryptors feature state-of-the-art encryption key management. Keys are securely stored and encrypted, and only accessible by you.

Solution Integrity

Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption.

Efficiency

Cost Effectiveness

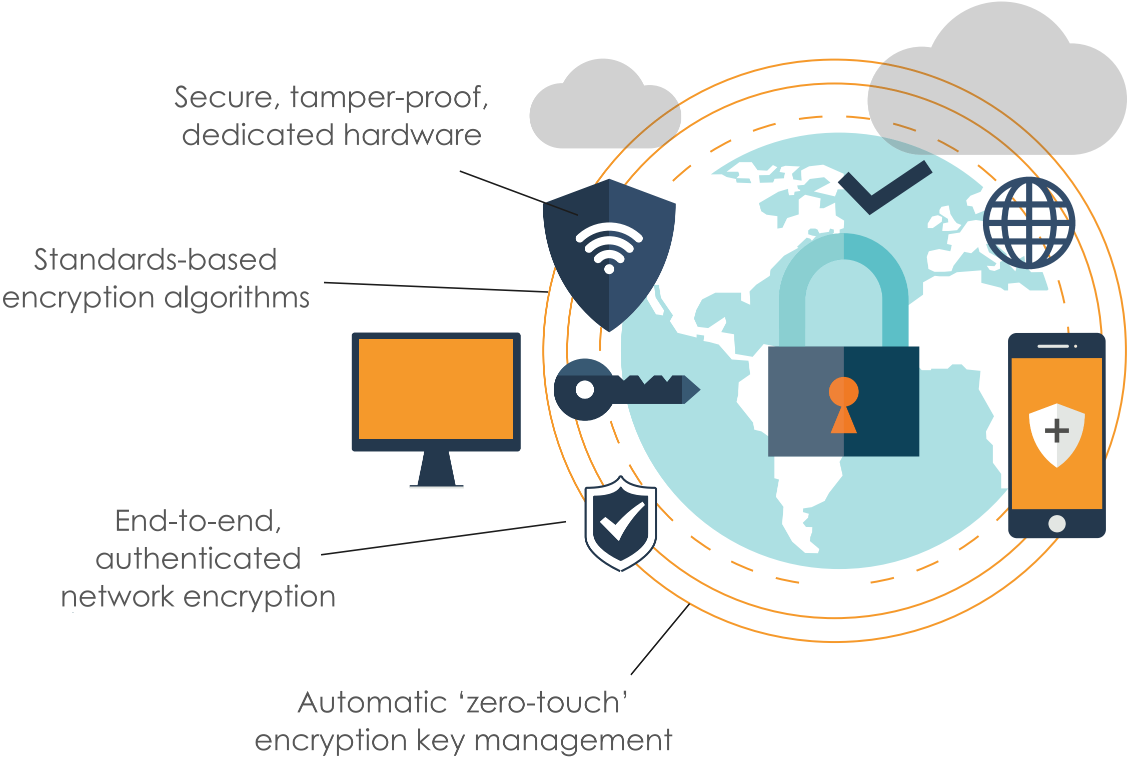
Senetas encryptors provide excellent TCO through a mix of network bandwidth savings, ease of management and longevity.

Reliability

All carrier-grade Senetas encryptors are hot-swappable, feature dual redundancy and deliver 99.999% uptime.

Flexibility

Use of FPGA technology enables maximum operational flexibility, including use of custom encryption and in-field upgradability.


Secure, tamper-proof, dedicated hardware
Standards-based encryption algorithms
End-to-end, authenticated network encryption
Automatic ‘zero-touch’ encryption key management

High-Assurance Encryption

As recommended by leading data security and encryption analysts; for a network encryption solution to be truly robust, and provide long-term data protection (well beyond the useful life of the data), it must be a high-assurance solution.

Not all encryption solutions are created equal. So-called ‘hybrid’ encryption devices – such as network routers/switches with embedded encryption or those using MACSec or similar standards (not originally intended for WAN and MAN security) provide low assurance data protection.

By contrast, Senetas CN Series encryption solutions are certified by the world’s leading independent testing authorities as suitable for government and defence applications. They are purpose-engineered for dedicated, high-assurance network data security.

Senetas CN Series encryptors’ security credentials include all four essential high-assurance features:

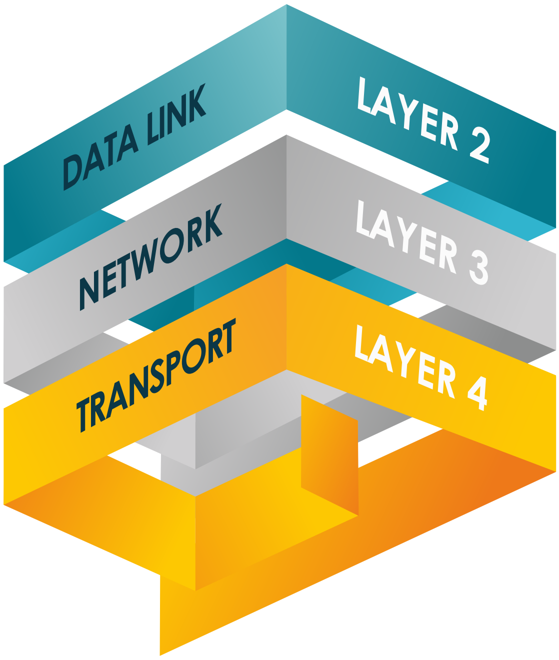
- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art, client-side, zero-touch encryption key management
- End-to-end, authenticated encryption
- Use of standards-based encryption algorithms

Network Independent Encryption

Many organisations utilise multiple data network Layer protocols (Layer 2, 3 and 4) to help deliver their business applications and communications services. Recognising this, Senetas has designed-in Network Independent Encryption.

This advanced, network Layer agnostic encryption technology enables destination policy-based, concurrent multi-Layer encryption.

Significantly, customers are still assured of strong, end-to-end encryption as the protected data traverses the various network Layers, for example: from Layer 2 Ethernet to Layer 3 IP network destination.



GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its brand.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our **ANZ Partner Page** for full details.

© SENETAS CORPORATION LIMITED

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file-sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** info@senetas-europe.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has an encryption solution to suit. Our certified high-assurance encryptors protect data across networks operating at speeds from modest 10Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 5Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

SECURE FILE SHARING

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

CCTVNS-SP0920

SENETAS