CCTV NETWORK HIGH ASSURANCE ENCRYPTION SECURITY

SOLUTIONS PAPER

SENETAS

Security without compromise

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.

SENETAS
Security without compromise

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
Security without compromise

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 Layer 2 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 Layer 2 Ethernet 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.

SENETAS
Security without compromise

SECURITY WITHOUT COMPROMISE

CCTV applications rely heavily upon uninterrupted data flows. Consequently, network performance is a key consideration when choosing an encryption solution.

The use of Layer 2 networks, with their inherent simplicity and ease of management, enables organisations to take advantage of the high-assurance benefits of Senetas encryptors, without impacting on the performance of the network or the applications running on it.

Layer 3 alternatives, or multi-function devices with "encryption included", simply cannot match the security and performance characteristics of dedicated encryption hardware:

> Maximum data network performance

> Maximum bandwidth availability

> The assurance of independent certification

> Simple, set and forget implementation

> Reliable, 99.999% availability

> Flexible network integration

> Transparent to all network devices

> Interoperability with all CN encryptors

> Near zero latency and network overhead

> Backwards compatible for long-term ROI

> Support for custom curves and algorithms

> Remote, centralised encryptor management

> Support for all Layer 2 protocols and topologies

> Integration with QKD for long-term data security

> Low total cost of ownership

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 around the world; including systems integrators, networks providers, cloud and data centre service providers, telecommunications companies and network security specialists.

For more information click here.

TALK TO SENETAS OR OUR PARTNERS

Senetas and Gemalto also work with customers' existing data network service providers, systems integrators and information security specialists to specify the optimal high-assurance encryption solution for their needs.

Wherever you are, simply contact Gemalto or Senetas to discuss your needs. Or, if you prefer, your service provider may contact Gemalto or Senetas on your behalf.

HIGH-ASSURANCE NETWORK ENCRYPTION

Whatever your Layer 2 Ethernet network security needs, Senetas has a high-assurance solution to suit. They support modest 10Mbps to high-speed 10Gbps links and multi-port 10x10Gbps links.

Scalable, agile and easy to use; Senetas high-assurance encryptors provide maximum security without compromising network performance.

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com

CCTVNS-SP0117