CCTV NETWORK ENCRYPTION SOLUTIONS-PAPER

SENETAS
Security without compromise

CCTV'S ADVANCES AND INCREASED USE IN PUBLIC AND PRIVATE APPLICATIONS DEMAND RIGOROUS DATA PROTECTION. WHETHER CCTV NETWORK DATA PROTECTION IS REGULATED OR NOT, THE NETWORKS USED FACE INTEGRITY, SURVEILLANCE DISRUPTION AND THEFT RISKS.

OVERVIEW

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

These requirements not only demand dependable data protection, but also reliable high-performance and high-capacity data networks. Both are essential to real-time CCTV monitoring and ensuring timely responses to threatening events. Importantly, dependable data protection must not come at a cost of reduced network performance.

As CCTV technology rapidly advances, such as high definition video and instant face recognition, the need to protect the data increases.

In some countries CCTV footage is highly regulated – how CCTV can and cannot be used and how the data must be protected, backed-up and stored. In some circumstances CCTV surveillance is regulated under multiple laws.

The critical data protection issues involve:

> Data integrity – prevention of interference with CCTV footage

> Disruption to surveillance – ensuring uninterrupted coverage

> Privacy and compliance with regulations – prevention of data theft and data diversion.

Because the number of CCTV devices in a system – public or private – is typically large, protecting the data networks that transmit the CCTV data can be very complex.

Furthermore, protecting the CCTV network is typically a process of catch-up. It is not a matter of if the network will be breached, but when! That's why the most secure organisations also focus on protecting the data itself – by encrypting the data that is transmitted across the network.

When a successful network breach occurs, unauthorised parties are left with meaningless encrypted data.

Encryption is the optimal last line of defence for the protection of CCTV generated data. Encryption renders the data meaningless when in unauthorised hands. Encryption is the optimal solution by protecting the data itself.

Senetas certified encryptors provide that data protection – "defence-grade" high-speed encryption. Whether the information being transmitted is voice, video or data, Senetas encryptors performance and benefits are world-leading.

However, unlike other high-speed encryption solutions, only Senetas certified, defence-grade, high-speed encryptors provides maximum protection without compromising network performance.

CCTV monitoring systems depend upon maximum network performance as well as data protection. Only Senetas certified high-speed encryptors provide maximum security without compromising network performance. That's why the world's most secure organisations trust Senetas high-speed defence-grade encryptors.

Importantly Senetas encryptors meet the demanding requirements of typical 24/7/365 CCTV surveillance – 99.999% uptime and maximum network performance. And their performance is certified!

THREATS TO CCTV SYSTEMS

Due to its information content; the data volumes transmitted and organisations' inability to completely control and secure all the data networks they use; CCTV data is a significant and rich target for cyber criminals.

The Cloud Computing applications and the high-speed networks they use expose organisations to increasing risks of unauthorised high-speed network access through:

- Data "sniffing"
- Information theft
- Redirection of data streams
- Disruption to business operations
- Identity theft
- Damaging asset attacks

These risks are real and growing. The consequences can be catastrophic:

- Major financial loss
- Expensive litigation costs
- Loss of reputation
- Loss of stakeholder confidence
- Devastating impact on physical assets and business revenue
- Consequential losses from business disruption and asset damage.

Because Senetas defence-grade data encryption protects the data itself, it provides peace of mind that should a successful network breach occur, unauthorised parties would only obtain meaningless data.

Data encryption is the optimal solution. However, most data network encryption solutions have high impact on the network's performance and other network assets – they degrade the data network performance and can adversely affect delivery of CCTV monitoring.

Senetas high-speed network data encryption avoids those downsides. Our unique high-speed encryptors provide maximum data protection without compromising high-speed network performance. And that's certified – by the three leading international, independent testing authorities.

That's why Senetas encryptors are used by the most secure organisations around the world. No other products of their type offer those capabilities or the same assurance of testing authorities' certifications.

Senetas' proven encryption "security without compromise" maintains maximum network performance – and that's certified! It also assures you of uncompromised dependability, zero impact on network assets and ease of implementation and on-going management.

THE INTEGRITY AND CONTINUITY OF CCTV DATA

Whether your CCTV network application is law enforcement, public security or asset and facility monitoring, its performance and data integrity are paramount. Government and private CCTV networks require secure and dependable data streaming and data integrity. Senetas defence-grade high-speed encryption assures that protection without compromising network speed or performance.

These CCTV network performance requirements are becoming increasingly important as CCTV definition increases. At the same time, Senetas high-speed encryption customers are assured that their data protection is not adversely affecting network performance.

Around the world, the use of CCTV has grown rapidly and new CCTV technology enhancements have greatly increased the volume of the data generated. Likewise, the data network performance needs are similarly increasing at a rapid rate. Therefore, it's important that CCTV data encryption not add performance overheads that reduce network bandwidth and speed performance.

Because the use of CCTV is dominated by personal and public security applications, the enormous data volumes generated are typically sensitive. That sensitive data must be protected from tampering, redirection, theft and eavesdropping.

Particularly in the case of CCTV applications, encryption's focus on protecting the data itself, makes it the optimal last line of defence,

Senetas high-speed network data encryption provides that protection and does so without compromising network performance due to the specific technical features unique to Senetas encryptors. These features begin with proven, certified near-zero latency and zero impact on network assets.

The high volumes of sensitive CCTV data streaming from multiple locations benefit greatly from:

- Maximum data network performance
- The assurance of world-leading independent, international testing authorities' certifications
- The ease of "set and forget" implementation and management
- 99.999% up-time and dependability
- Flexible network integration
- More efficient network data transmission costs through superior performance
- Dependable consistent and near-zero latency
- Outstanding interoperability of encryptors

Senetas defence-grade encryptors provide the efficiencies and effectiveness of dedicated, specialist designed and engineered hardware encryptors – with long-term proven use in high sensitivity government, defence, military and major banking transaction environments.

DEDICATED DATA SECURITY WITHOUT COMPROMISE – DEFENCE-GRADE

Whatever network type or protocol you use for high-speed data transmission, it is at risk of interception by unauthorised third parties.

Increasingly* organisations that require high-performance data networks for the transmission of relatively large data volumes chose to use Layer 2 networks over the Layer 3 (IP type) networks. Layer 2 networks often provide more efficient transmission of data volumes and are simpler to manage.

When it comes to the best protection of data being transmitted through defence-grade encryption, customers prefer Senetas Layer 2 network encryption solutions because they do not compromise network performance and provide better data transmission efficiencies.

The typical use of Layer 3 data networks for the transmission of CCTV monitoring comes with built–in network performance impediments when encrypted – a bandwidth speed cost of 50% to 70%!

However, the use of Layer 2 networks with their inherently simpler and easier (lower cost) to manage characteristics and overall cost efficiencies enable the advantages of Senetas' certified, world-leading high-speed encryptors without network performance compromise!

Unlike other data encryption products, Senetas encryptors are defence-grade – dedicated high-speed encryptors. "Multi-function" devices that simply "include" encryption, do not match the performance or certification assurance of Senetas dedicated encryptors – ground-up designed, engineered and manufactured defence-grade encryptors.

Critically, CCTV data must be dependable therefor it must be protected. Senetas encryption technology was initially developed to solve high-speed network data encryption issues in federal law enforcement and defence applications. This experience and Senetas' R&D commitment to dedicated data security products have led to the certifications held.

In sensitive CCTV applications (regulated or not), you are provided with the assurance of certified optimal data protection and maximum network performance – security without compromise!

* Layer 2 markets take up trends.

THE ASSURANCE OF INDEPENDENT, INTERNATIONAL TESTING CERTIFICATIONS

Senetas unmatched data encryption – triple-certified!

Only Senetas' high-speed, dedicated data encryptors provide triple-certified network data protection without loss of network performance and the simplicity of "configure and forget" defence-grade encryption. Senetas encryptors ensure that data protection need not come at the significant cost of lost bandwidth and network performance – so critical in CCTV monitoring. And that performance is dependable. This is why governments, defence and military organisations around the world prefer Senetas encryptors. They demand no-compromise performance.

Senetas' high-speed encryptors – unlike any other high-speed encryptors of their type – hold certifications by the three leading international, independent government testing authorities:

> FIPS (US)

> CAPS (UK)

> Common Criteria (international and Australia)

These certifications are your assurance of security without compromise!

Because CCTV applications rely so heavily upon uninterrupted data flows and processing, organisations can be assured that protection of the data in transit comes with the dependability of 99.999% up-time availability.

Similarly, commercial and government organisations implementing secure dedicated, everywhere, anytime CCTV applications that generate huge data volumes, have peace of mind that Senetas encryptors are providing a defence-grade, last line of defence – without compromise. And because Senetas high-speed encryptors hold more product certifications than any other products of their type, they provide you with the highest level of performance assurance.

*Senetas Layer 2 encryption performance versus conventional encrypted Layer 3 network performance.

SENETAS CCTV CUSTOMER SOLUTIONS

Senetas encryptors have been selected to protect CCTV networks transmitting large volumes of data across high-speed networks by government and non-government organisations around the world.

While we cannot reveal much about our customers, we can tell you how we met their CCTV data security requirements.

In each case our customers ran their own extensive performance testing and benchmarking. Senetas encryptors excelled – the best performance and the most trusted certifications:

- The integrity of certifications by the three largest international, independent testing authorities in the world. The encryptors held the required testing authority certification/s required
- Near-zero latency and maximum network performance
- Consistent and dependable latency performance suitable for business-critical applications
- Maximum bandwidth performance
- Extensive interoperability and backward compatibility of Senetas encryptors
- Flexibility to tailor the devises to specific unique customer requirements
- Efficient "total cost of ownership"
- Zero impact on other network assets
- Ease of on-going encryptor management
- Best practice reliability (99.999% uptime)
- Multi-network protocol compatibility

SUGGESTED FURTHER READING

TOPIC	DESCRIPTION	LOCATION
Senetas CN Series encryptors	CN Series Brochures	View website
Senetas Encryptors at a Glance	Specifications of Senetas CN Series encryptors	Download PDF
White-paper "Batten Down The Hatches"	Assessing threats to your ethernet network – A guide to protecting data in motion	View website Download PDF