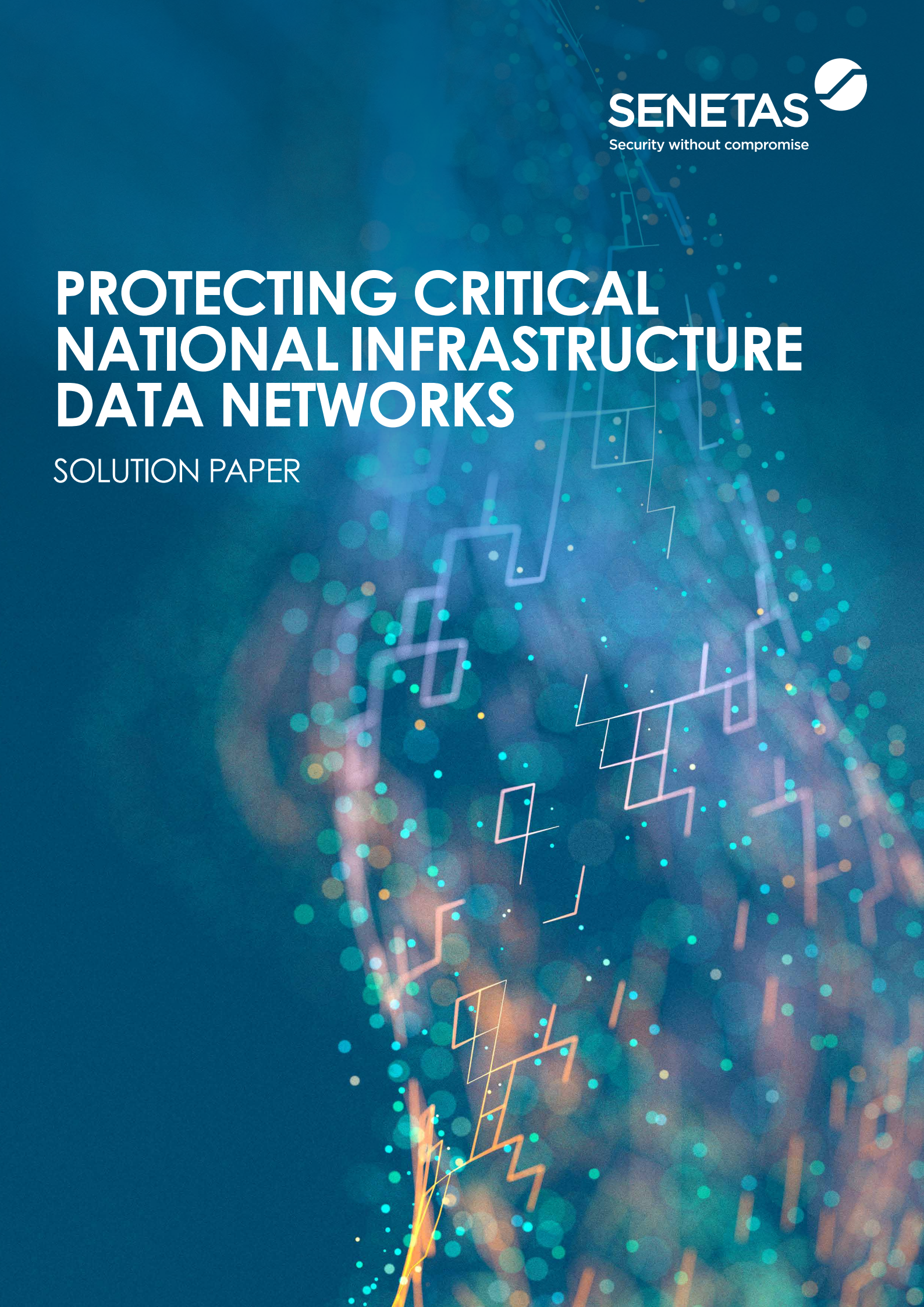
SENETAS
Security without compromise

PROTECTING CRITICAL NATIONAL INFRASTRUCTURE DATA NETWORKS

SOLUTION PAPER



CRITICAL NATIONAL INFRASTRUCTURE

Critical National Infrastructure may be defined as "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life depends".

National Infrastructure is typically divided into 9 categories: communications, emergency services, energy, financial services, food, government, health, transport and water. Assets within these categories are measured against a criticality scale and assigned a status based on the severity of impact.

The threat landscape is constantly evolving, with potential harm originating from terrorist attack, rogue states, hackers and organised crime, the implications of the growing threat to Critical National Infrastructure are wide ranging.

Loss or corruption of data would have an obvious negative impact on financial and operational performance for the organisation suffering the breach. However, of greater concern would be the potential impact on the security or supply of critical utilities and the broader implications for national security and public safety.

Supervisory Control and Data Acquisition (SCADA) Networks

Supervisory Control and Data Acquisition (SCADA) networks are used to carry command data that ensures the safe and reliable operation of a nation's critical infrastructure. Essential services such as electricity, natural gas, water, waste treatment and rail services all rely on SCADA networks.

Traditionally, SCADA networks have been isolated, and it has been high fences and barbed wire that has kept our critical infrastructure secure.

However, with the increased threat of cyber-attack, Governments and industry regulators around the world are focussing beyond physical perimeter protection to ensure the integrity of the systems used to control our critical infrastructure.

It is these controlling networks that represent the greatest vulnerability to utilities and infrastructure organisations, not only from the theft of sensitive data being transmitted across their networks, but also the consequences of disruption or manipulation of these data flows as part of a malicious attack.

Many SCADA systems are no longer isolated and are connected to public networks via the Internet.

Sometimes this is intentional, as a means of connecting to other systems, other times it can be an unintentional consequence of providing connectivity to remote locations or offices.

Globally, there are mandates from the highest levels of government requiring that SCADA networks and other critical infrastructures are secure.

In the UK, the Centre for the Protection of National Infrastructure (CPNI) provides advice on physical and cyber security, in the US, NERC (the organisation responsible for reliability standards for the nation's utility providers) has established a set of Critical Infrastructure Protection guidelines and in the EU, the European Programme for Critical Infrastructure Protection (ECPIP) provides a similar doctrine.

"Hackers are increasingly targeting electric, natural gas and other vital utilities; threatening a disaster of epic proportions that experts say firms are doing too little to guard against."

James W Sample, Ernst & Young

WHY ENCRYPT?

The rapid growth of virtualisation, data centre and cloud computing technologies mean we are becoming increasingly reliant on our high-speed/high-availability data networks to deliver information when and where we need it.

Cyber-crime in the form of hacking, corporate espionage and even cyber terrorism, is on the rise. Information security threats remain commonplace and there is an increasing emphasis on organisations of all types to ensure the integrity and security of their data, both at rest and in motion.

We cannot rely on the assumption that our data remains secure within the perimeter of the office environment. All organisations share systems and information that rely upon common network access and most modern businesses comprise multiple offices, some separated by a few yards, others by thousands of miles.

Fibre-optic cables are used to transport Petabytes of data across private and public networks every day. Although still considered the fastest and most reliable method of moving data, Fibre networks have become increasingly vulnerable as hacking technologies become more sophisticated, less expensive and more readily available.

Protection versus Prevention

There is a common misconception within many organisations that a robust firewall is enough to prevent unwanted access to their network. Unfortunately, this is not the case. Whilst the firewall can detect and eliminate a variety of penetration or denial of service attacks, it is no protection against a physical tap either inside or outside the firewall.

The only fail-safe solution to ensure that your data is secure as it travels across the network is encryption. Furthermore, your encryption solution should be de-coupled from any specific network architecture and accredited against recognised world-wide security standards.

Notable Breaches

As our critical infrastructure becomes more connected, it exposes legacy technologies to the outside world; leaving some vital systems open to exploitation.

In recent years, we have seen an increasing number of attacks on critical infrastructure. According to the Gemalto Breach Level Index, from 2017 to 2018, the industrial sector experienced the single largest increase in the number of breached data records.

In December 2015 the Ukraine fell victim to a spear phishing attack that compromised a SCADA system. This resulted in a massive power outage, affecting over 230,000 people.

In 2013 agents allegedly acting on behalf of a foreign state managed to access the command and control systems at the Rye Brook dam in New York state.

Throughout 2015 and 2016, a hacking group known as Lazarus targeted the SWIFT global bank messaging system and successfully stole millions of dollars from unsuspecting banks.

In 2017 a joint report from the FBI and Homeland Security in the US highlighted a number of cyber attacks on nuclear power stations across the country; including Wolf Creek in Kansas.

In another 2017 report, GCHQ in the UK announced that hackers were systematically targeting the UK energy sector.

In early 2018, the New York Times reported that a cyber-attack on a petrochemical plant in Saudi Arabia was intended to not only sabotage plant operations, but to cause an explosion that constituted a genuine threat to life.

SECURING THE IOT

The evolution of the Internet of Things (IoT) will see over 25 billion connected devices by 2020. From a cyber-criminal's perspective, this represents 25 billion possible system vulnerabilities.

Smart Grid Technology, where the SCADA network effectively extends all the way to the meter in the end-user's premises, is a case in point. A classic example of IoT in action, it poses some unique security challenges.

The Smart Grid is a sophisticated communications network where data is collected remotely, then collated and analysed centrally before control commands are issued.

If rogue data could be injected into the Smart Grid network and compromise the command and control systems, it could result in significant service disruption, economic damage or citizen harm.

End-to-End Encryption

Encryption is a key element in ensuring the security of SCADA networks. However, for encryption to be most effective it needs to deliver against four criteria: Speed, Scalability, Manageability and Affordability.

SCADA networks deal with real-time data, so any encryption technology needs to operate at full line speed and add minimal latency.

Scalability is essential as the nature of a SCADA network means that different bandwidths are in operation at different points in the network.

Encryption solutions should offer strong and effective data protection but should also be simple at the point of use. Centralised management allows users to configure and deploy new devices across the network.

Affordability is another key consideration when it comes to retrospectively securing SCADA networks. Encryption should be viewed in terms of TCO and ROI, not capital expenditure.

High-Assurance hardware encryption for core IT and communications infrastructure

With enterprise, government, defence and service provider customers in more than 35 countries, Senetas has a long-established reputation as a leader in the design, development and manufacture of certified, high-assurance encryption hardware for Layer 2 Ethernet networks.

The Senetas CN Series of high-speed hardware encryptors delivers certified high-assurance encryption security. Designed and built to protect core IT network infrastructure; CN Series encryptors deliver security without compromising on network and application performance.

Strong and effective virtualised encryption for extended & virtualised WAN

In a world dominated by distributed WAN, virtualisation and borderless infrastructure; the need for high-performance virtualised encryption security is growing.

These extended networks and virtualised environments, beyond the core Ethernet network infrastructure, typically operate at speeds of 1Gbps or less.

The Senetas CV Series of virtualised encryption appliances delivers strong and effective encryption security for data-in-motion across high-speed Carrier Ethernet WAN links at >1Gbps.

Instant scalability means the CV Series may be deployed rapidly across hundreds (thousands) of network links.

CHOOSING THE RIGHT ENCRYPTION SOLUTION

A lack of vendor compatibility within the network encryption marketplace means organisations looking to secure both core IT infrastructure and virtualised WAN need to think carefully about a choice of technology.

When it comes to choosing an encryption vendor, it's important to consider all the possible applications. Just as important is the realisation that all encryption solutions are not created equal.

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.

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 Layer 2 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 Ethernet network encryptors' security credentials include all four, essential high-assurance features:

- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art encryption key management; featuring secure, client-side key storage
- End-to-end, authenticated encryption
- Standards-based encryption algorithms

For real-time data applications, latency is a significant issue. Whilst adding a network encryption interface card to an existing switch may seem like an attractive option; it will result in higher latency and lower throughput performance than a dedicated Layer 2 device.

In some instances, using an NIC means the same vendor needs to be used throughout the network route and that data is decrypted and re-encrypted at each of the "hops".

This is both a security risk and a major key management issue. Dedicated appliances enable data to remain encrypted throughout the network route, irrespective of switch vendor.

If an NIC is used, the lifespan of the encryptor will be tied to the host network device and will need to be replaced when the switch is changed.

Most modern infrastructure comprises multiple network Layers; typically featuring Layer 2, 3 and 4 elements. So, organisations should look for a vendor that provides Layer agnostic encryption where possible.

Senetas CV Series virtual appliances provide concurrent, multi-Layer encryption and support DPDK for up to 5Gbps performance.

Like the CN Series hardware encryptors, our virtual appliances support all topologies, from P2P to Hub & Spoke and fully meshed networks.

COMBINING HARDWARE AND VIRTUALISED ENCRYPTION

A lack of vendor compatibility within the network encryption marketplace means organisations looking to secure both core IT infrastructure and virtualised WAN need to think carefully about a choice of technology.

The choice between hardware and virtualised encryption is based on an organisation's individual needs and preferences. Often, it is not a case of 'either/or' – but a blend of the two technologies together.

Security versus performance and network link use

Hardware encryptors deliver predetermined high-performance, not able to be matched by software/virtualised encryption. They also provide maximum data security through multi-certified, high-assurance credentials.

Network link use cases

High-speed links (>5Gbps) are more commonly used to connect IT infrastructure such as data centre interconnects, or Big Data feeds.

Encrypting data in motion between branch locations is of equal importance, though network speeds will vary between these locations.

These links ideally require both maximum data protection and best performance, only offered by hardware encryptors.

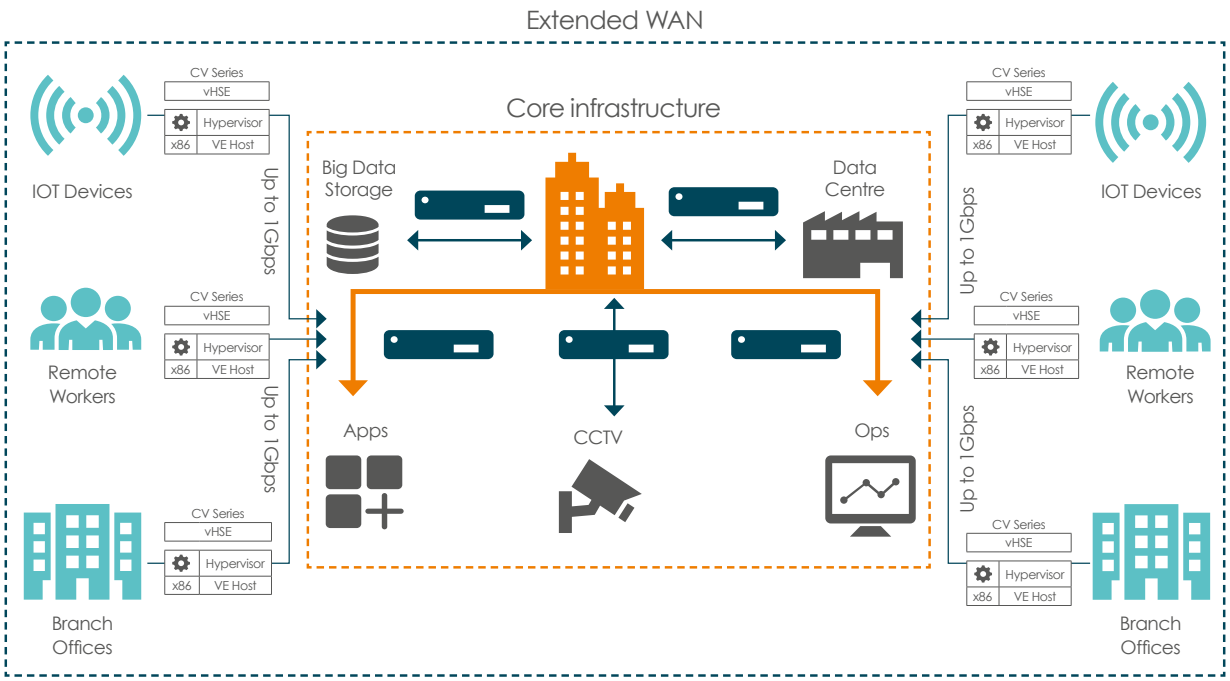
However, for extended WAN links and high-scale virtualised links that typically run at up to 5Gbps, a virtual encryptor is likely to be a more flexible and cost-effective solution.

Mixed use cases

Organisations often only deploy hardware encryption to protect core IT infrastructure data in motion. Many operate unprotected extended WAN links.

Virtualised encryption provides an opportunity to encrypt all data in motion through a single compatible technology.

Ultimately, organisations should utilise dedicated hardware encryption for their main feeds, interconnects and branch locations, while virtualised encryption is used to provide scalable, cost-effective encryption for devices at the network edge.



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

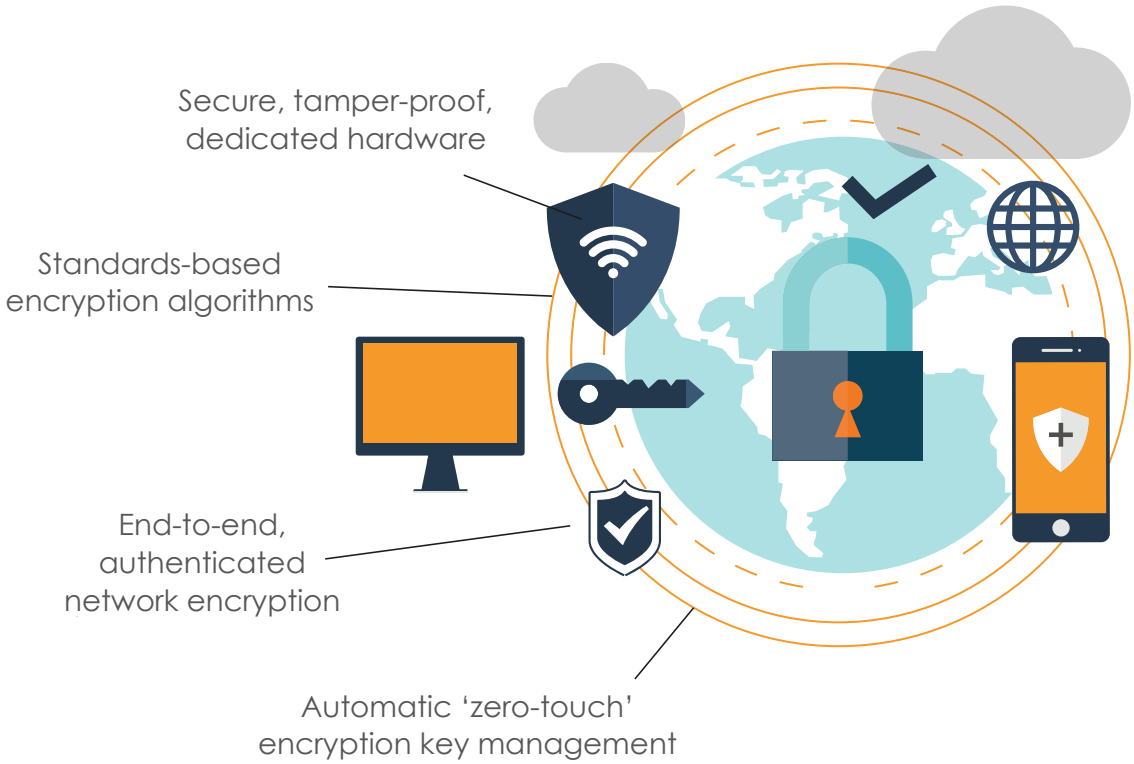
Senetas encryptors provide excellent TCO through a mix of network bandwidth savings, ease of management and longevity.

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.



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:

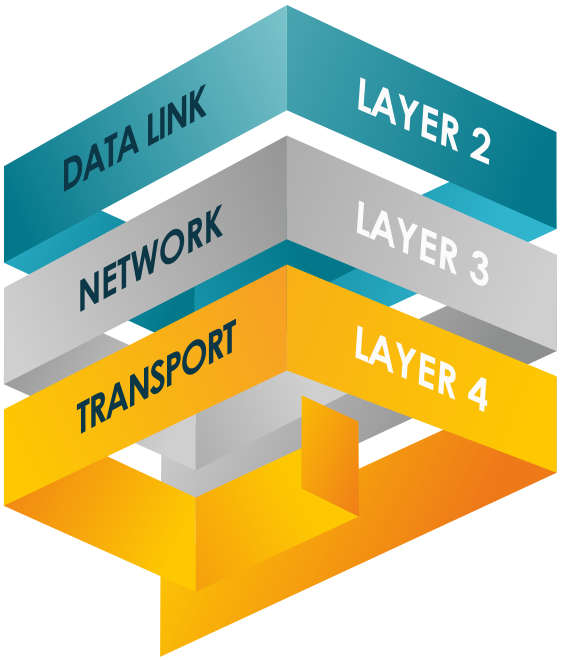
- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art, client-side, zero-touch encryption key management
- End-to-end, authenticated encryption
- Use of standards-based encryption algorithms

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.



CV1000 VIRTUALISED ENCRYPTION

The CV1000 is a Virtual Network Function (VNF) appliance providing strong and effective data encryption security with designed-in crypto-agility. Designed for virtual CPE, the CV1000 delivers transport-Layer agnostic encryption for high-speed networks at up to 5Gbps.

As an VNF appliance, the CV1000 stands out from the crowd. Instant scalability means it may be deployed rapidly across thousands of network links. It delivers the same flexibility and scalability as other virtualised network functions.

The CV1000 offers state-of-the-art encryption security and key management without impacting on network or application performance*. Unlike IPSec-type encryption solutions, the CV1000 is transparent to the network; making it ideal for securing your WAN, right to the virtual edge.

Integrated support for SafeNet KeySecure (Thales' centralised cryptographic key management solution) 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.

Enhanced key security

The CV1000 is fully compatible with SafeNet KeySecure; the industry's leading centralised key management platform.

Available as a hardware appliance or a hardened virtual security appliance, SafeNet KeySecure provides support for multiple key types: symmetric, asymmetric, secret data and X.509 certificates.

SafeNet KeySecure simplifies the management of encryption keys across the entire life-cycle; including key generation, storage, backup, distribution, deactivation and deletion.

DPDK acceleration - performance up to 15Gbps

DPDK Intel libraries enable x86 host device performance acceleration. If the host x86 device and DPDK are optimally configured, the CV1000 will deliver enhanced performance of >1Gbps up to 5Gbps.

Consistent performance up to 15Gbps is dependent upon host configuration and expertise in DPDK setup and configuration.

Environment and architecture factors may also play a role in virtualised encryption performance, as they do in virtualised networks.

Key benefits

Unmatched benefits of the CV1000 expressed by end-user customers and service providers include:

- The CV1000 enables adoption of a virtualised encryption solution that does not compromise on security or network and application performance
- Instant scalability to match the scale and flexibility of virtual and software-defined networks
- No requirement to deploy large numbers of hardware encryption devices to achieve high scale implementation of network encryption
- The CV1000 encryption security and key management model is optimised for strong and effective encryption security
- Through Transport Independent Mode, the CV1000 is suited to a multi-Layer network environment
- Competitively, the CV1000 delivers up to 30% network performance benefit over other solutions
- Ease of deployment with centralised, 'zero touch' provisioning
- 100% interoperability with Senetas CN Series encryptors
- As a software implementation of the Senetas high-assurance encryption platform, the CV1000 provides a flexible, cost-effective way to encrypt all the way to the virtual edge
- Data centre service providers identified the CV1000 as an optimal solution; providing strong and effective encryption security among devices within the data centre itself

SUREDROP ENCRYPTED FILE-SHARING

No matter where or how the people in your organisation work, there is always the need to share and sync files - both internally and externally.

While you want to enable collaboration, data security should always be the first priority. If it's not, the risk of non-compliance and data breaches become a serious problem.

Our customers have been telling us that their mobility and productivity initiatives are frustrated by insufficient levels of security delivered by existing box style file collaboration and sync and share solutions.

While many are user friendly, elegant and effective, they're simply not safe enough.

Senetas provides SureDrop to deliver state-of-the-art, standards-based encryption algorithms, key management and 100% file control security - without comprising your user experience.

In design, features and functionality, SureDrop solves the security issue of convenient file-sharing and synchronisation, to the highest standards required by governments and large enterprises.

SureDrop + Votiro Disarmer

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

Leveraging patented Content Disarm & Reconstruction (CDR) technology, Votiro Disarmer protects your files from the most advanced, persistent cyber-attacks.

By integrating Votiro with SureDrop, documents are not only secure through encryption, but safe to use.

If you've come to enjoy the familiarity of Dropbox, Box, OneDrive or Google Drive, you'll love the elegance, convenience and flexibility of SureDrop.

Key benefits

- Available on-premises or from the Cloud
- 100% control over data sovereignty
- Unlimited file size and types
- Standards-based encryption
- Effortless management and control

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.

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 35 countries.

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

Regional Contacts:

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

CNIDS-SP0820

SENETAS