SENETAS

Security without compromise

SECURE DATA CENTRE SERVICES

TECHNICAL PAPER

Best-practice data security

Ensuring the security of modern storage and data centre infrastructure is not without its challenges. The complex, multi-Layer structure of most networks places varying demands on IT professionals to ensure the secure transport of big data to and from data centres and SAN, especially for back-up and disaster recovery workflows.

The security, authenticity and integrity of data held in storage backbones is an essential element of business continuity. High-assurance encryption security should be considered the best, last line of defence for data, both at rest and in motion.

Although encryption is a mature technology, it can still pose significant challenges when used across high-performance, high-availability enterprise storage networks. The volumes of data stored and transported across modern infrastructure are resource intensive and, in the case of business-critical systems, cannot be impacted by the introduction of encryption security. Any encryption solutions introduced should be integrated transparently, so as to provide security without compromise.

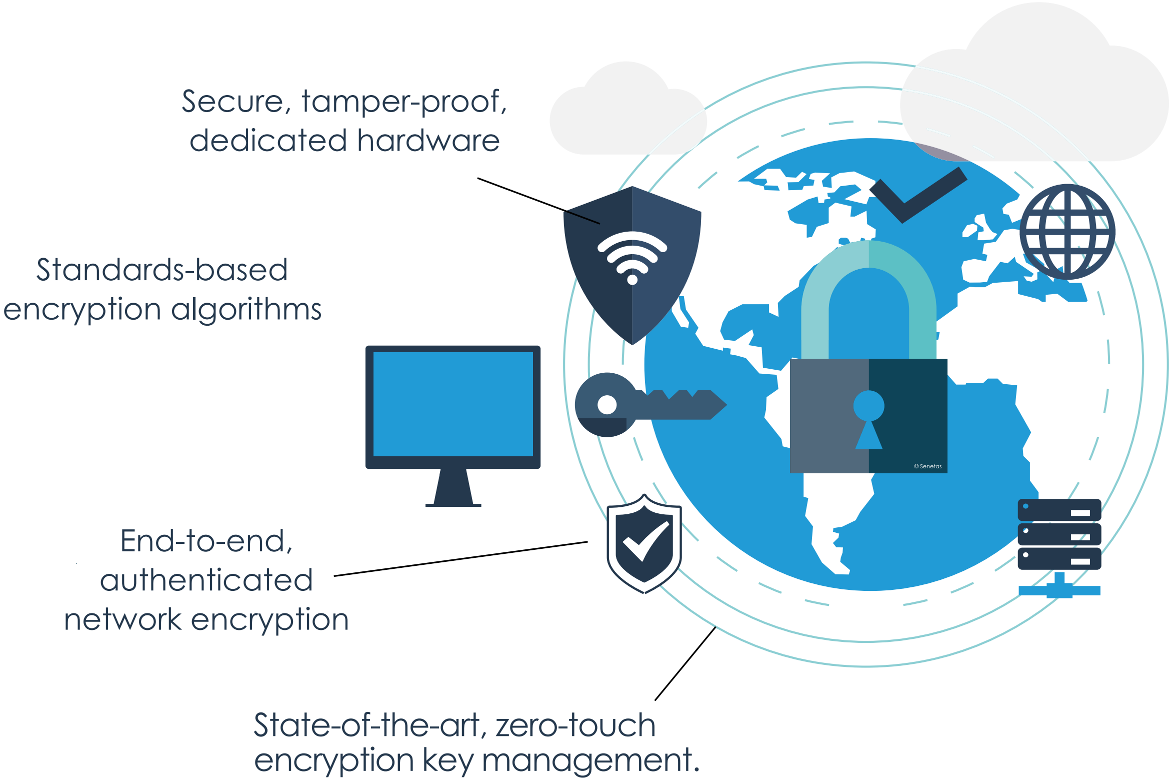
Best practice for all data centre and storage applications should be to leverage encryption solutions that have been through the stringent evaluation processes adopted by the world's leading independent certification authorities, such as FIPS and Common Criteria.

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. Multi-function 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 CypherNET Network Independent Encryption solutions are purpose-engineered for dedicated, high-assurance network data security. Their security credentials include all four essential high-assurance security features:


Secure, tamper-proof, dedicated hardware
Standards-based encryption algorithms
End-to-end, authenticated network encryption
State-of-the-art, zero-touch encryption key management.
© Senetas

QUANTUM RESISTANT 'HYBRID' ENCRYPTION

Senetas is the first cybersecurity developer to implement hybrid encryption, providing customers with both conventional and quantum resistant encryption algorithms in a single, high-performance, crypto-agile platform.

The huge global investment in quantum computing has seen development timelines contract significantly in recent years. Quantum assets are already being made available to cloud users and roadmaps from quantum tech companies indicate we are on the brink of the point of quantum advantage.

The impending arrival of quantum computers is widely acknowledged as the single largest threat to the public key infrastructure our digital universe depends upon. Conventional encryption relies on the concept of 'mathematical hardness' for security. Quantum computers are a game changer. Exponentially more powerful that the most sophisticated 'classical' computer, they are capable of solving mathematical problems that are virtually impossible (would require thousands of years for a classical computer to solve) in a matter of hours. This increase in computing power will render today's public key encryption infrastructure obsolete.

Much of today's sensitive data (EG intellectual property, government secrets, medical records, financial account access etc) is subject to long-term vulnerability, with an effective lifetime of 10-20 years or more. Not only does data need to be protected from today's conventional cyberattacks, but also from the harvest now, decrypt later threat posed by quantum computers. This 'backwards vulnerability' is why cybersecurity experts are advocating organizations to act now to secure tomorrow's data.

Post Quantum Cryptography

Transitioning to a new cryptographic infrastructure takes time. The National Institute of Standards and Technology (NIST) began the process of selecting new, quantum resistant algorithms in 2016. By 2019 it had shortlisted 26 candidate algorithms and expects to have finalised standards established by the end of 2023. In 2021 NIST published a report where it acknowledged that the implementation of the new standards could take anywhere between 5 and 15 years. If the rate of change currently experienced in the development of quantum computing continues, it will leave the cybersecurity industry exposed to a period of substantial threat.

"We cannot accurately predict when a quantum computer capable of executing Shor's algorithm will be available to adversaries, but we need to be prepared for it as many years in advance as is practical. As previously stated, when that day comes, all secret and private keys that are protected using the current public-key algorithms—and all available information protected under those keys—will be subject to exposure." Getting ready for post-quantum cryptography NIST, 2021.

With the introduction of hybrid encryption, Senetas customers are able to future-proof their data security; providing long-term data protection and facilitating the migration to quantum resistant cryptography - as advocated by both NIST and ANSI.

Storage Network Security

Senetas wire-speed encryption solutions are ideal for securing data on its way to the SAN. With minimal latency and a simple bump-in-the-wire configuration, CypherNET encryptors guarantee the confidentiality of data whilst remaining transparent to the user.

Senetas encryptors provide real-time data protection and are accredited to the global standards laid down by FIPS (140-2 Level 3), Common Criteria (EAL 4+) and NATO. They meet all the requirements set out by the Storage Network Industry Association for the protection of data in transit.

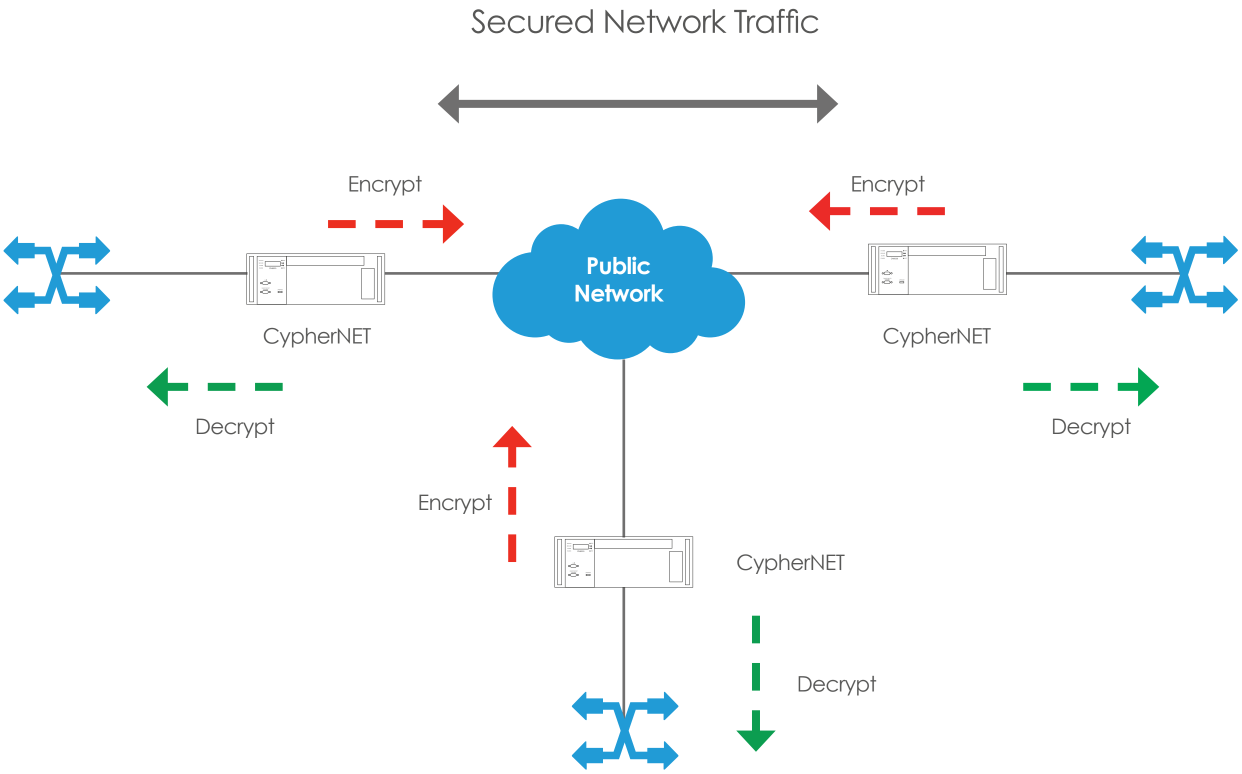
Multi-Layer Encryption

Senetas hardware has set the standard for secure Layer 2 encryption for many years. However, as networks have evolved to become increasingly borderless, there is greater demand to add encryption security at Layers 3 and 4.

The exponential growth in Cloud-enabled services and applications has seen organisations' data networks become increasingly multi-Layer, particularly in the use of Layers 2, 3 and 4 (Ethernet, Internet Protocol and Transport Layers).

Solution Benefits

- FIPS (140-2 Level 3), Common Criteria (EAL 4+) and NATO certified solution
- Encrypts traffic across all network topologies, from P2P to full mesh
- Full line speed with no packet expansion
- AES 256bit encryption
- GCM authentication mode
- Automatic 'zero-touch' key management
- Real-time availability of encrypted video, voice and data
- Near zero latency
- Nominal data overhead
- 100% interoperability across the CypherNET range
- 100% network device compatibility
- Compatible with external sources of entropy and custom curves
- Secure remote management with CypherManager (CM7)



Next gen data centre solutions

Senetas partners with service providers to deliver best-of-breed secure data centre and high-speed network services.

Senetas CypherNET encryptors have been used to protect commercial, defence and government network data around the world for over 20 years. Whether its core infrastructure, or WAN, data centre interconnect or cloud services, Senetas encryptors are the first choice for those seeking security without compromise.

Service partners provide a comprehensive range of data centre services, including high-density rack space, colocation, redundant back-up and disaster recovery.

Whatever the data centre solution, Senetas technologies provide private and public sector customers with high-performance, low-latency solutions to protect everything from citizen data to financial transactions, corporate IP to private medical records.

Secure key management

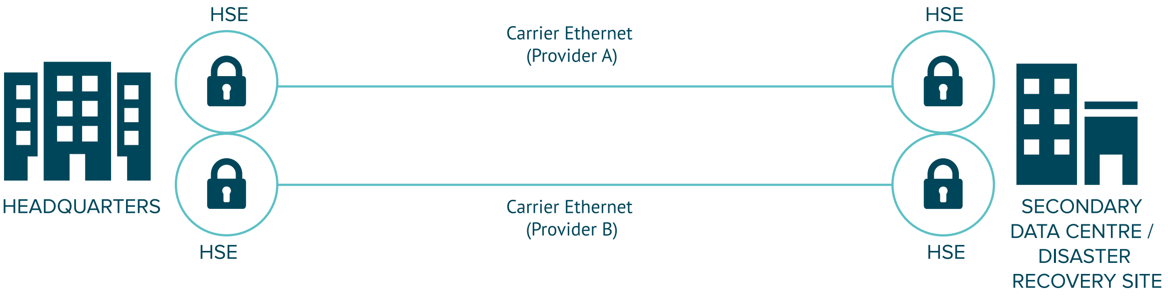
Senetas CypherNET encryptors leverage state-of-the-art, client-side only encryption key management (end-to-end encryption). This means the customer is the only entity with access to the encryption keys, neither Senetas nor the data centre service provider has access.

Encryption depends upon key management to provide and deliver the local information needed to encrypt and decrypt frames. In order to ensure any breached data is rendered meaningless in the hands of an unauthorised user, it is essential to restrict access to the encryption keys themselves.

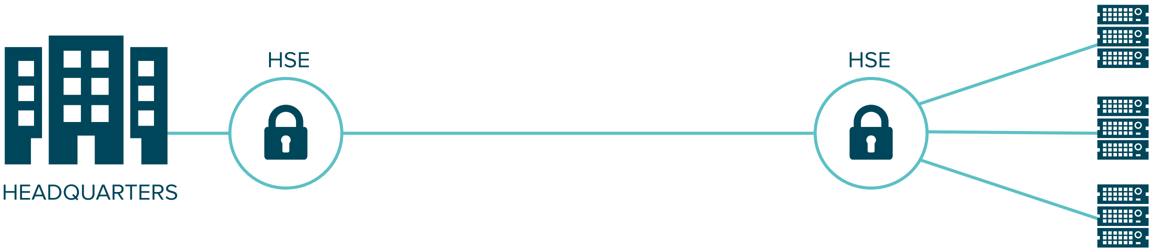
Effective encryption relies on key security at every stage. Secure keys require randomness and real randomness can only be delivered from a hardware source.

Keys are stored securely in a tamper-resistant enclosure, with any unauthorised access resulting in zeroization. Whilst in transit between encryptors, they keys themselves remain encrypted.

DATA CENTRE INTERCONNECT



CLOUD WAN



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:** infoemea@senetas.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 or secure file sharing and collaboration 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 cybersecurity 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.

NETWORK DATA SECURITY WITHOUT COMPROMISE

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

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 15Gbps. 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.

They are trusted to protect much of the world's most sensitive government, defence and commercial data.

SECURE COLLABORATION

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 Secure File Gateway extension.

DISARM MALICIOUS CONTENT

Votiro Secure File Gateway 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.

SENETAS