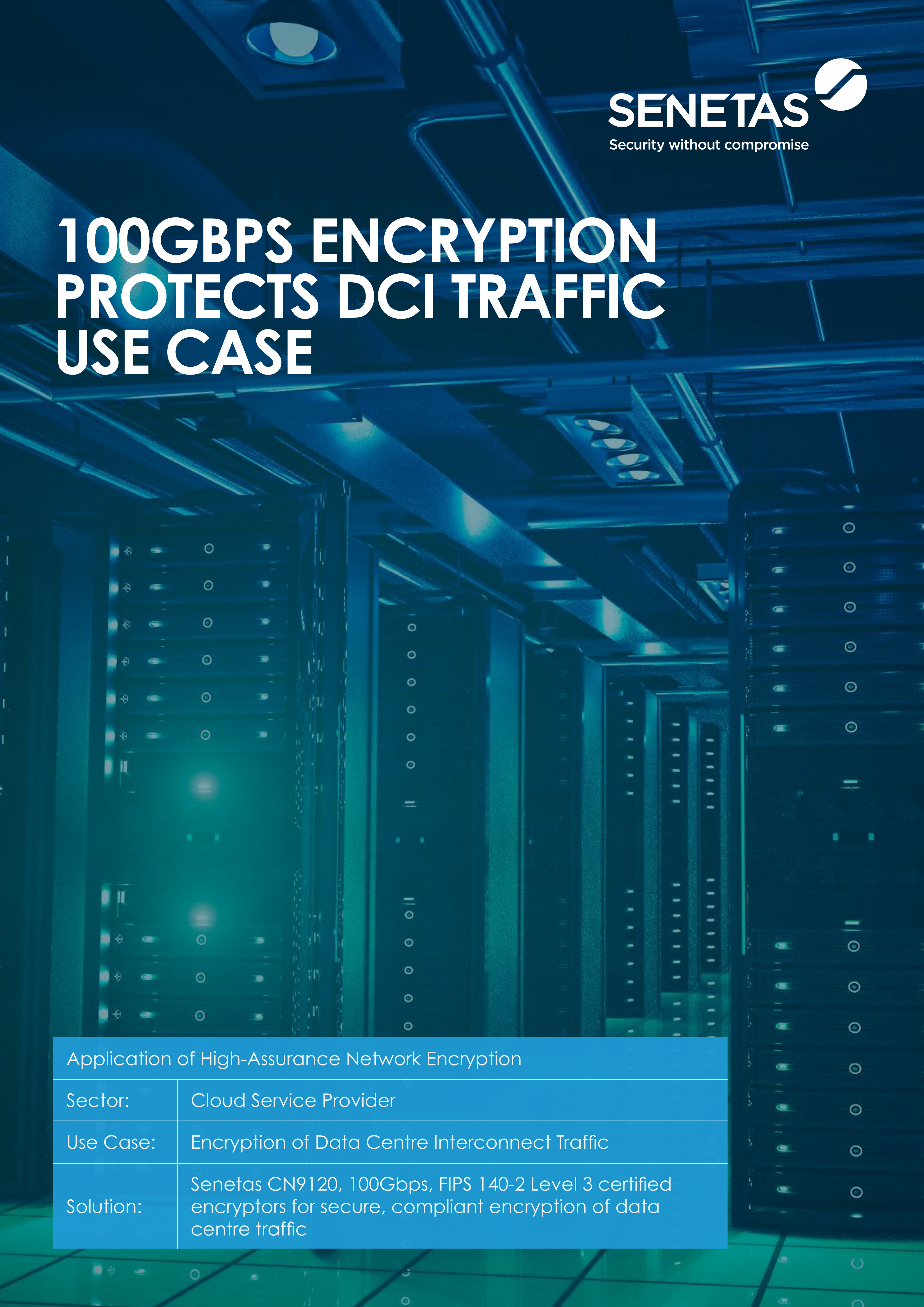

SENETAS

Security without compromise

100GBPS ENCRYPTION PROTECTS DCI TRAFFIC USE CASE

Application of High-Assurance Network Encryption	
Sector:	Cloud Service Provider
Use Case:	Encryption of Data Centre Interconnect Traffic
Solution:	Senetas CN9120, 100Gbps, FIPS 140-2 Level 3 certified encryptors for secure, compliant encryption of data centre traffic

Overview

Growing data volumes, driven by demand for video content and more capable mobile devices, are increasing the strain on network infrastructure, particularly on routes to, from and between data centres.

Data Centre Interconnect (DCI) technology enables the reliable transport of critical information between facilities - over short, medium, or long distances using modern optical transmission equipment at speeds up to several hundred gigabits per second.

Data centre connections form the critical backbone of cloud connectivity and must provide reliable, high-capacity and secure connections to ensure the transmission of critical information. Data sets from applications can be very large and may contain highly sensitive data, such as personal information, financial records, or intellectual property.

Ensuring the protection of such data at all times is essential to avoiding costly data breaches or potential data loss. Keeping data confidential as it leaves one data centre, and arrives at another, requires not only strong encryption but encryption that will not degrade network performance, especially for latency sensitive applications.

Challenge

A leading cloud service provider, running a large number of global data centres, required a solution to protect their customers' high-speed DCI traffic. As a secure cloud provider to government customers around the world, they required the use of FIPS 140-2 Level 3 validated cryptographic modules to meet their customers assurance and regulatory compliance needs*.

In addition to security compliance needs, the cloud provider mandated an encryption solution that would not degrade network bandwidth or latency between data centres.

Maintaining deterministic performance levels for a wide range of latency-sensitive traffic was a vital design objective. It was important that the deployed solution did not impact the Quality of Service (QoS) for any network services or add more than a few microseconds of end-to-end latency.

The provider's data centres were in diverse geographic locations, separated by a range of distances. To ensure reliable operation, all deployed equipment was required to support a variety of optical connections, including 100GBase-LR4, 100GBase-SR4 and Single Lambda modules.

Early in the design process, the decision was made to isolate the network and security components in the system architecture and to use a dedicated encryption appliance. Although security features such as encryption are often available in common network devices (such as switches or routers) many such integrated solutions have not completed any formal security assessment or have only done so at a low level.

Products with lower levels of security assessment (EG. below FIPS 140-2 Level 3) typically do not provide the security mechanisms that are mandated by many Federal and Defence customers, such as physical protection against tamper and probing attacks.

Using a dedicated encryption appliance also provides a 'Separation of Duties' security benefit and ensures that only those security team members with the requisite credentials can control the encryption policy across the network. This reduces the chance of accidental or malicious attempts to disable security in other network equipment.

A further consideration was that the cloud provider infrastructure team wanted the agility to modify the network equipment over time, without reducing the security of the network. Deploying a dedicated encryption appliance meant that other network equipment could be swapped out or optimised for reasons of efficiency, performance or cost without reducing security compliance.

*Note: All US federal government agencies are required to use hardware or software cryptographic systems that have been validated against the FIPS 140 standard to protect sensitive but unclassified information. FIPS 140-2 Level 3 is also recognised as a gold standard security certification by commercial, government and defence customers in many jurisdictions.

Solution

The cloud provider evaluated several possible solutions and chose Senetas CN9120 100Gbps encryptors to protect their fibre optic circuits.

Figure 1 - CN9120 100G Encryptor

The Senetas HSE platform is a family of fully interoperable hardware and software encryption solutions that has been independently tested and certified to FIPS 140-2 Level 3, Common Criteria EAL4+ and US DoDIN APL.

The certification level ensured that the cloud provider easily met the security requirements for both US Federal customers and for many other commercial and government requirements. The CN9120 uses NIST-approved encryption algorithms and provides strong physical protection with built-in tamper detection (operates with or without power) and anti-probing baffles.

The CN9120 encryptors are deployed in Point-to-Point configurations across the provider's global data centre infrastructure and provide a highly efficient, transparent encryption overlay that ensures the confidentiality and integrity of all transmitted data. The encryptors operate at full line speed and introduce a non-service impacting latency of approximately one microsecond per device.

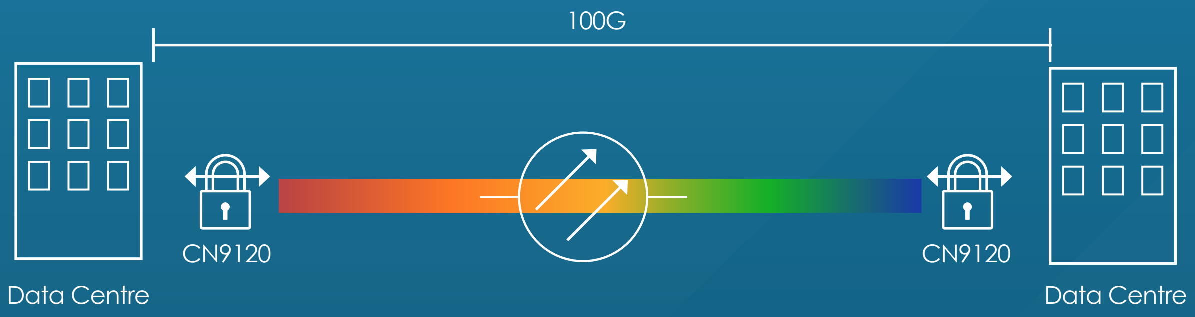

Figure 2 - DCI encryption

Even with the encryptors in circuit, it was noted that applications across the DCI traffic ran as well with encryption as they did without.

CN9120 encryptors are simple to deploy and require little or no ongoing maintenance. Encryption key updates occur automatically at frequent intervals (5 minutes) without impacting network performance. The devices are fully remotely manageable using the Senetas management application CM7, which runs on Linux or Windows.

Due to the flexible policy engine the encryptors can operate across any Layer 2 topology, including hub-spoke or fully meshed data centres. Senetas encryptors are designed to operate across any Layer 2 WAN circuit, including metro-Ethernet, Layer 2 MPLS (VPLS) or pseudo-wire connections and have field-tested proven interoperability across international Service Provider links.

The operational flexibility gives the provider the freedom to change their network topology in the future without requiring expensive equipment refreshes.

Benefits

The CN9120 is a FIPS 140-2 Level 3 certified encryption appliance that provides wire-speed encryption of data across point-to-point, hub & spoke and any-to-any and mesh network topologies. As such, it is the only wire-speed certified encryption appliance that has the versatility to operate in any network topology while meeting both the performance and security needs of the network.

The CN9120 provides efficient "bump-in-the-wire", tunnel free encryption at Layer 2 for all traffic types and is able to encrypt at line speed even with a constant packet flow of minimum-size 64-byte packets.   This means that performance levels are guaranteed for all data types, regardless of application mix or packet size.

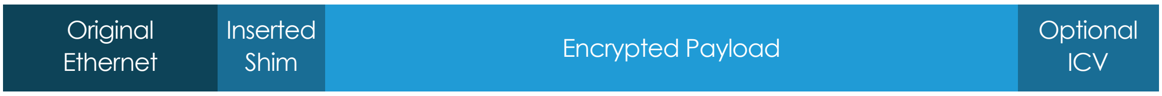

Figure 3 - Tunnel free encryption

The CN9120 supports a wide range of industry standard pluggable QSFP-28 transceivers, providing customers with extensive connectivity options for data centre networking, enterprise core aggregation and service provider transport applications.

The CN9120 is interoperable with the full suite of Senetas hardware and software encryption appliances. This designed-in versatility means that FIPS grade encryption can be deployed across the fastest commercially available Ethernet services to satisfy the strong demand for high bandwidth secure connectivity.

The encryptor is fully in-field upgradeable and has no hard-baked security logic. This crypto-agility means that the appliances can be easily upgraded in-situ to support new encryption algorithms as mandated by NIST, and also to meet the transition from Quantum vulnerable encryption to Quantum Safe security.

Senetas maintains an active FIPS certification schedule for all encryptors to ensure that the device firmware complies with the latest NIST encryption requirements.

The encryption modes provide defence-in-depth protection and support hybrid operation using both Classic and Post-Quantum public key signature and key establishment mechanisms, as well as support for the standardised ETSI Quantum Key Distribution interface.

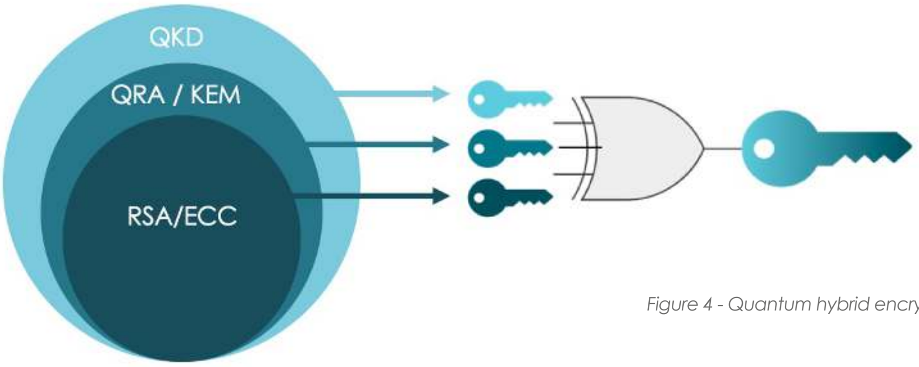

Figure 4 - Quantum hybrid encryption security

Summary

By standardising on the Senetas CN9120 platform to secure their data centre infrastructure, the cloud provider is able to offer customers the strongest possible protection of their data. At the same time, they can meet government and enterprise compliance requirements globally without impacting service or application performance.

The designed-in crypto-agility of the CN9120 ensures that the provider is well placed to evolve and grow their network whilst ensuring they can meet future security needs and adapt to new threats.

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales and within government & defence sectors by Thales Defense & Security Inc.

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 SafeNet brand.

THALES

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. For a current list, visit our **ANZ Partner Community Page**.

© 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 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 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 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.

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 File Gateway extension.

DISARM MALICIOUS CONTENT

Votiro 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.

XXX-XX-1121

SENETAS