END-TO-END ENCRYPTION SOLUTIONS:

SECURING MULTI-LOCATION NETWORK LINKS

SENETAS

Security without compromise

Branch locations

Mid-size organisations and enterprises rarely have a single base of operations. Instead, they operate across multiple locations (either their own or supply chain businesses) both nationally and internationally.

The infrastructure that supports these organisations no longer runs out of a single location. The rise of Cloud computing, the IoT and Big Data sees services being run from multiple locations and shared among branches.

This flexibility also dictates how the workforce and the organisation itself operates. As business operations and supply chain communications become unified, they are fuelling growth into new markets and locations, all of which must be integrated into the main network.

The role of data networks

Multi-site organisations rely heavily on data networks to permit the exchange of data between locations and back to the head office or data centre.

Each branch and supply chain partner location will have a different requirement in terms of the volume of data being transferred and the speed at which this is conducted.

Over time, demands on these networks will change as branches grow and additional locations are added, making flexibility key.

Organisations will use a range of topologies to build their networks – from traditional Point-to-Point (P2P) to hub & spoke and fully meshed architectures.

Proven and trusted, Hub & Spoke networks will be the choice of many organisations, where individual locations make up the Spokes, connecting to a head office or data centre acting as the Hub.

Borderless infrastructure

With Mobility, Cloud Computing and Big Data applications driving digital transformation, organisations must come to terms with the reality of borderless infrastructure – where there is no longer a clear delineation between where one network ends and another begins.

The growth in popularity of IoT also adds billions of endpoints to the network. While this delivers innumerate advantages, it also poses a security challenge as normally closed networks become open, connected, and vulnerable to attack.

Threats to branch locations

The increasing volume of data flowing between branch locations has attracted the attention of cyber criminals, who are using anything from simple 'blunt force' attacks or eavesdropping to more elaborate techniques in order to breach these networks.

Once access is gained, these nefarious actors can either manipulate intercepted information, steal it for fraudulent use or insert malicious data.

The consequences of such a breach are widespread, with organisations suffering anything from loss of IP and customer data to financial loss and reputational damage.

In addition to existing threats, organisations must also be aware of emerging technologies, such as the impending age of quantum computing.

Branch location security

While inter-branch and supply chain connected communication brings a host of efficiencies, it also poses an inherent security risk if data is not encrypted end-to-end.

By encrypting data in motion across branch locations, it is possible to guarantee data integrity as, even if it is stolen, it will be unreadable and therefore rendered useless.

This Solution Paper analyses the threats that network connected branch locations face, explains why data in motion between these locations should be encrypted and offers guidance on choosing the right encryption solution.

Why encrypt?

Data networks are not safe. Cyber-security is not a network provider's responsibility so, as information is being transmitted between branch locations, it finds itself vulnerable to attack.

Prevention technologies such as firewalls ensure data is protected at rest, however data still remains exposed when in motion across public or private networks.

In order to guarantee the security, trust and integrity of the data being transmitted, organisations must act to secure it against a wide range of threats.

The breach landscape

According to Gemalto's breach level index, over 14 billion data records have been lost or stolen since 2013 – an average of six and a half million records per day.

Of those, a mere 4% were 'secure breaches' where encryption was used and the data was rendered useless.

Malicious outsiders and accidental loss account for 89% of breaches, with stolen data most commonly used for identity theft, account access and financial access.

While data breaches occur across all industries, they are most frequent in the health, technology, social media, retail and government sectors due to the quantity and detail of information exchanged.

It takes organisations an average of 197 days to identify a data breach and a further 69 days to contain. The consequences of these breaches include:

> Intellectual property theft

> Business disruption

> Compliance issues

> Loss of customer data

> Privacy breaches

> Financial loss

Alongside this, firms must address the loss of trust and reputation amongst stakeholders; something that is much more difficult to attribute a value to.

Emerging threats and popular trends

Alongside existing threats, organisations must be aware of technologies that are about to be introduced, as well as those gaining popularity.

The rapid growth in virtualisation and IoT devices being deployed at remote and branch locations is one such example.

Because virtualised CPE and IoT devices lie at the edge of the network, many organisations do not account for them when assessing their cyber security.

However, if left unprotected, these devices are providing hackers with countless opportunities to gain access to networks and farm sensitive information or input rogue data.

Organisations are utilising public, private and hybrid Cloud services to facilitate the collection, storage and analytics of data. Again, these networks are vulnerable if improperly protected.

There has also been a notable rise in hackers stealing meta data (data about data). Despite the common myth, this information is sensitive and can provide a wealth of exploitable information if not properly encrypted.

The coming age of Quantum computing also plays a growing part in cyber security. While the immense computing power of Quantum computers will have a transformative effect on computing, there is also a risk of the technology being used for harm.

Quantum computers will be able to break current Public Key encryption algorithms in a fraction of the time taken by traditional computing methods, threatening the protocols that underpin much of the world's data security.

While this seems like a distant concern, the reality is much closer. It is estimated that a Quantum computer capable of breaking today's cryptography will be available within the next 5 to 10 years, meaning organisations need to consider the shelf life of their encrypted data today as well as their ability to migrate to Quantum-safe encryption in the near future.

Protection vs 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 worldwide security standards.

Notable breaches

Because of the nature of the industry, retail is the subject of much of the media coverage around branch location security.

However, these security concerns are not limited to retail; affecting banking and finance, critical national infrastructure, logistics and indeed any organisation that operates out of multiple branches both nationally and internationally.

In 2018, US department stores Saks and Lord & Taylor had a reported five million records stolen after a known ring of cyber criminals implanted software into store cash registers, syphoning off payment card details.

2016 saw fast food chain Wendy's admit that 1,025 restaurant point-of-sale systems were infected with malware during a five-month data breach. In early 2019, the company reached a $50 million settlement with financial institutions.

In 2014, multinational delivery and supply chain management company UPS had five million records stolen via malware installed on card processing systems at 51 of its branches in 24 US states.

The same year saw home improvement chain Home Depot and office supply company Staples lose 56 million and 1.1 million records respectively due to unsecure payment systems at branches.

Securing branch locations

By tapping into data in motion among branch locations, hackers can bypass security systems in place around the data when it is at rest.

Upon accessing the network, cyber criminals can intercept and steal data as it flows between the point of origination and endpoint. By gaining unsolicited access, hackers can also inject rogue data into networks – compromising data integrity.

Network administrators must take steps to secure this data in motion, whilst ensuring that the performance of the network is not adversely affected.

In addition, they must be aware of the different data volume and speed requirements at each branch location. For example, implementing a solution designed for high-speed networks (>100Gbps) into a branch with moderate requirements will prove costly.

End-to-end encryption

Encryption is crucial to ensuring the security of data transmitted among branches as well as the wider network. It should be deployed as an end-to-end solution across the network and should secure metadata alongside main data packets.

In the event of a breach, encrypted data is unreadable by hackers and is therefore rendered useless. In addition, the forward secrecy provided by encryption solutions prevents rogue data being inputted into systems.

Encrypting data also benefits organisations from a compliance perspective, with data protection regulations such as GDPR treating 'secure breaches' differently to those that are not; potentially saving organisations from hefty fines as they demonstrate the importance of protecting the sensitive information they collect.

However, not all encryption solutions are the same. 'Embedded' solutions, such as MACsec used in network devices, may be low cost but they also have security, performance and overhead weaknesses. The optimal solution for maximum security, performance and near-zero overhead is a purpose-built, secure device providing true end-to-end encryption.

Network and application performance

Due to the volume of data transferred, it is crucial that an encryption solution does not impact network speed or performance.

Any increase in latency will result in a slow-down of key infrastructure; something organisations can ill afford.

Of equal concern is that some organisations opt for low-assurance data encryption technologies that appear to be effective, but come at a cost:

> Compromised network performance

> Hidden costs of lost effective bandwidth

> Adverse impact on business-critical applications

> Complex implementation and day-to-day management

> Adverse impact on other network assets

File sharing services

Similarly, sharing any type of information via email is unsecure. Sharing information as email attachments does not guarantee the security of the information being exchanged if it is intercepted. In a criminal's hands that information could have catastrophic business consequences.

Moreover, data protection regulations such as GDPR indicate that files containing personally identifiable information should be protected in transit – by password protecting files, for example. This approach is cumbersome and is subject to human error.

Implementing a secure encrypted file-sharing platform ensures that data remains secure when stored and shared among branches and the wider community, without requiring lengthy processes to manage data exchange.

Choosing the right encryption solution

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

Borderless infrastructure and edge computing sees data flowing across the network from multiple devices at multiple locations, meaning this data must be secured throughout its journey.

In the same way, data transmitted across metro area networks must be secured at all points as a single vulnerability will result in a failure across the network.

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 hardware 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 such as financial platforms and CCTV monitoring, 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 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.

To facilitate encrypted file sharing between branches, Senetas' SureDrop secure file-sharing application delivers a familiar box style functionality with high-assurance data protection and CDR technology.

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 (>1Gbps) 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 1Gbps, a virtual encryptor is likely to be a more flexible and cost-effective solution.

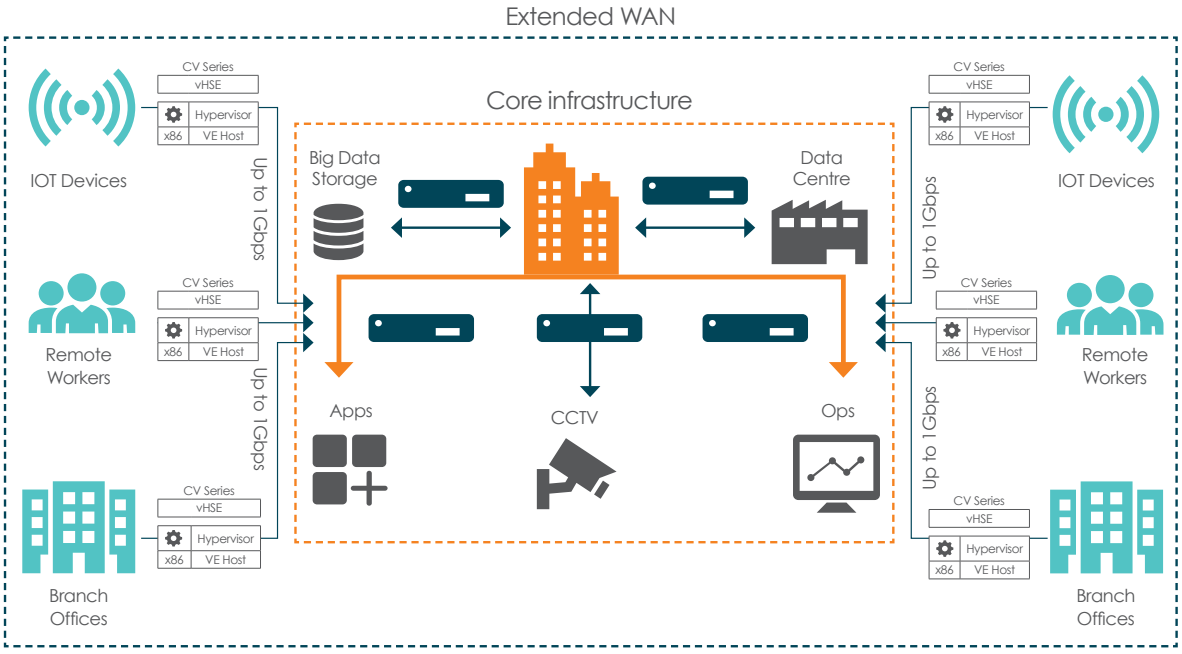
Mixed use cases

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.

Protecting the extended WAN to the 'virtual edge' (large-scale WAN deployments)



Senetas 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 (also known as SafeNet CN9100 Ethernet Encryptors) are designed to meet the exacting requirements of all 100Gbps use cases, making them an ideal application for securing high-speed networks.

Senetas' CN and CV Series encryptors include integrated support for SafeNet KeySecure (Gemalto's 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 (also known as SafeNet 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 P2P, Hub & Spoke or meshed environments.

The CN6000 Series are rack-mounted, high-speed encryptors for business-critical applications; offering 1Gbps to 10Gbps bandwidth speeds. Speeds can be rate-limited and changed on-demand, offering a flexible, cost-efficient solution for branch locations. 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

Versatile and scalable, the CN4000 Series provides secure, transparent encryption over Ethernet networks in P2P, Hub & Spoke or meshed environments (10Mbps to 1Gbps). They are an ideal solution for organisations with multiple branch locations and moderate data volumes and speeds.

Despite their low cost and small form-factor, CN4000 Series encryptors (also known as SafeNet CN4000 Ethernet Encryptors for SMB) have the same robust security credentials as the rack-mounted models.

Setting a new price/performance benchmark, the CN4000 Series is designed to meet more modest network requirements, but still delivers the same high-assurance encryption security that make Senetas encryptors stand out.

Key Senetas CN encryptor benefits including zero network impact, near-zero latency, ease of implementation and 100% interoperability are all a part of the CN4000 Series.

Use case: International banking branch encryption

A global bank was seeking to address its commitment to customer confidentiality, regulatory compliance and an increasing dependence upon real-time, big data applications.

The bank serviced an international clientele from a network of 30+ offices across 3 continents, all connected via an Ethernet WAN.

To meet its stated objectives, the bank needed to upgrade its network data encryption solution. Above all, it was looking for a high-performance solution that was easy to deploy and manage without "breaking the bank".

Out with the old, in with the new

Working in partnership with its multinational telecommunications service provider, the bank evaluated several solutions before choosing Senetas certified high-assurance encryptors.

Senetas provides a range of Layer 2 Ethernet encryptors, operating at line speeds from 10Mbps to 100Gbps.

Given the high-performance and security credentials demanded by the financial services industry, it was determined that the Senetas CN Series of hardware encryptors would be the best solution.

Deployment

Following a successful pilot project, the bank rolled out the encryption platform to their global WAN, incorporating over thirty branches on three continents.

Senetas CN Series encryptors were used for the Hub at the bank's head office; securing 10Gbps links.

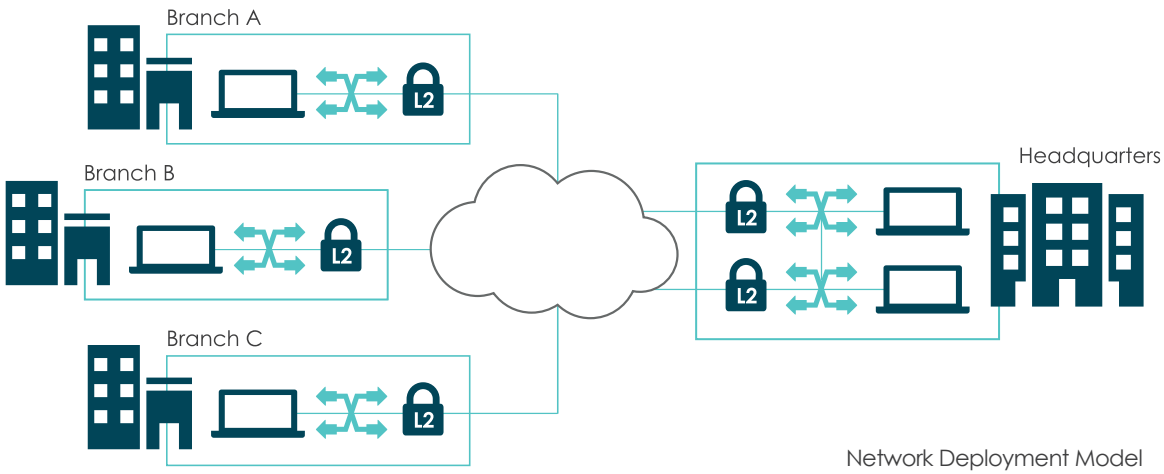
Other high-assurance CN Series encryptors were used to secure the endpoints in the WAN, depending on the bandwidth requirements and space available in the branch offices.

Initially, the branch locations opted for rate-limited encryptors, with bandwidths from 100Mbps to 1Gbps.

This enabled the bank to just pay for the bandwidth used, helping them to meet their CAPEX budget requirements.

However, it also provided the bank with the flexibility to upgrade the branches as bandwidth demands increase, without changing the hardware.

All Senetas CN Series encryptors are fully interoperable and share a common management platform.



Network Deployment Model

Senetas 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 (Gemalto's 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.

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

*Subject to host appliance performance.

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 Plus

SureDrop Plus features Votiro CDR content disarm and reconstruct (CDR) which adds a valuable layer of security through protection against malware, ransomware and zero-day 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

> Votiro Content Disarm & Reconstruction technology

> Available to telecommunications, Cloud and managed service providers as a custom security add-on to offer end-users

What makes Senetas CN Series encryptors stand out?

Best Performance

High-speed

The designed-in, market-leading performance capabilities of Senetas encryptors are what make them stand out from the crowd.

Whether operating at 10Mbps, 100Mbps, 1Gbps, 10Gbps or 100Gbps; time after time, they consistently win competitive performance tests.

Their encryption speeds, near-zero data overhead and near-zero latency make Senetas encryptors ideally suited to the most demanding network environments.

Ultra-low latency

Senetas high-speed encryptors operate in full duplex mode at full line speed 99.99% without loss of packets.

Latency is not affected by packet size (<2 microseconds per unit at 100Gbps) meaning maximum throughput with near zero protocol overhead.

Importantly, by using Field Programmable Gate Array (FPGA) technology, this outstanding performance is predictable and dependable.

Zero impact

The zero impact of Senetas encryptors is not limited to network bandwidth and latency; it extends to network operations and management.

They simply fit in within the user network. They don't require changes to other devices or network reorganisation; making them a favourite among network engineers.

High-Assurance

Certification in-depth

Because Senetas CN Series encryptors include the only multi-certified products of their types, they are trusted by governments and defence forces around the world.

Rigorous testing is carried out over many years and provides our government and commercial customers with maximum confidence. Senetas CN Series encryptors are certified by: FIPS, Common Criteria and NATO.

For 20 years, Senetas R&D has included a commitment to 'certification in depth'. Customers value the benefits of exhaustive and ongoing testing authorities' product evaluation.

Best encryption key management

All Senetas products adopt state-of-the-art encryption key management. Your encryption keys are only ever held by and accessible to you, on your premises; securely stored and encrypted.

Solution integrity

Senetas encryptors provide maximum solution integrity; unlike 'low assurance' solutions, such as router-based network data encryption or so called 'hybrid' encryptors.

Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption with standards-based (AES256) encryption algorithms.

Versatile & Simple

Crypto-agility

All Senetas encryptors are 'crypto-agile'; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

Selected Senetas encryptors also support Quantum Key Distribution (Quantum Cryptography) and Quantum Random Number Generation, for long-term data security.

Support for all protocols

The Senetas CN range of encryptors provides the widest feature-set. Able to operate at 10Mbps to 100Gbps, they are designed for Layer 2 Carrier Ethernet WAN and MAN networks and support all Layer 2 protocols: Ethernet, Fibre Channel; SONET/SDH and LINK.

Support for all topologies

Senetas CN encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies. Senetas CN9000 encryptors are the only 100Gbps encryptors that support multipoint-to-multipoint topologies.

Custom encryption

In addition to the standards-based AES256 and 128-bit algorithms, Senetas CN encryptors support the use of customer-requested algorithms, custom curves (BYOC) and entropy (BYOE).

Ease of use

Set and forget simplicity and network transparency are underlying Senetas design themes. They ensure ease of implementation, operation and management.

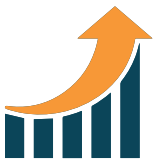
All Senetas encryptors feature automatic zero-touch key management. They also feature automatic network discovery and connection.

Interoperability

Senetas encryptors supporting the same Layer 2 network protocol are fully interoperable. All Senetas CN models are backward compatible.

Local or centralised management

Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software; which acts as the Certificate Authority in a network of encryptors by signing and distributing X.509 certificates.



Low Cost, High Efficiency

Suitability

All Senetas CN encryptors operate at full line speed; enable maximum network performance and deliver 'set and forget' management simplicity.

The business investment case out-performs even 'cheap and cheerful' low-assurance solutions that prove very costly over time.

It is not necessary, nor beneficial, to opt for low-cost, low-assurance solutions to meet the toughest business case and TCO requirements.

Cost-efficiency

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

Longevity, interoperability, backward compatibility, minimal installation and management costs and solution flexibility all contribute to a rapid ROI.

Other cost benefits include, low power consumption minimal rack space use and combined rack space/power utilisation efficiency.

Reliability

99.999% uptime and conforms to international requirements for safety and environment.

All carrier-grade, rack-mounted Senetas encryptors are hot-swappable and provide further network operations uptime benefits thanks to dual redundancy of encryptor consumables such as fans and power supplies.

Unlike hybrid encryptors and other low-assurance solutions, network uptime is not disrupted by Senetas encryptors.

Flexibility

Senetas encryptors' use of FPGA technology enables maximum operational flexibility.

They are better able to meet customers' specific requirements and provide an optimised high-speed data encryption solution.

This flexibility enables on-going operational simplicity, such as infield upgradability, as customers' requirements change; helping to protect their investment in technology.

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia & New Zealand) by Thales, within the US Federal Government by Thales Defense & Security Inc and across Australia and New Zealand by Senetas and its Partner Community.

THALES SENETAS

ANZ Partner Community

IBM dimension data VOCUS communications

DXC Data#3 DATACOM

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

Looking for a service provider to encrypt your high-speed network data? Contact us and we'll help you find the right one.

Senetas works with data network service providers across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers are free to 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 provide support for all network topologies.

Our virtual encryption solutions are used to secure virtual CPE asnd virtualized WAN operating at speeds of up to 5Gbps. They provide multi-Layer, end-to-end encryption across all network topologies.

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 security, SureDrop is also available with Votiro Disarmer and SafeNet KeySecure Extensions.

Votiro Disarmer leverages patented Content Disarm & Reconstruction 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.

SafeNet KeySecure is the industry's leading centralised key management platform. It provides simple and secure encryption key management across the entire lifecycle; including key generation, storage, distribution and deletion.

SCS-SP0419

SENETAS