SENETAS
Security without compromise

END-TO-END ENCRYPTION SOLUTIONS

SECURING CLOUD SERVICES

SOLUTION PAPER

CLOUD SERVICES

The rapid and pervasive adoption of cloud services is one of the cornerstones of digital transformation. As organizations across the world move more workloads to the cloud, they are realising significant improvements in workforce productivity, service availability and customer experience.

The way in which many organizations work has changed dramatically over the past decade. Improvements in technology, shifts in attitudes towards remote working and the diversity of communication channels available have all combined to affect a significant change in behaviour. In a global marketplace, work has become something you do, not somewhere you go.

Ubiquitous access to business critical data and applications is the key driver behind adoption. In 2020, a third of IT budgets were spent on cloud services, with the global market value

Public and private cloud

Current estimates show 90% of businesses using at least one cloud service, with 60% of workloads running in a hosted cloud environment.

Cloud is not an all-or-nothing proposition. Organizations can choose to leverage private cloud infrastructure, public cloud infrastructure or, in most cases, a hybrid of both.

Public cloud infrastructure has seen the most significant growth, with Amazon, Microsoft and Google dominating the IaaS and PaaS market. Organizations of all sizes are moving workloads to public cloud infrastructure as they benefit from its inherent scalability, availability and cost-efficiency.

For more sensitive or critical workloads, many businesses will prefer the security and control of their own private cloud infrastructure. Private cloud is also the infrastructure of choice for highly regulated industries, or those that require complete control over data sovereignty.

Hybrid cloud is positioned to become the default infrastructure of choice. 60% of businesses have already adopted a hybrid model that features elements of private cloud, public cloud and on-premises solutions.

The role of high-speed networks

The growing popularity of cloud services, and the amount of data flowing across these networks, means cloud services are heavily reliant on high-speed, low-latency data networks to deliver seamless user experience.

IDC predicts that, by 2025, 49% of the world's stored data will reside in public cloud environments[7], meaning the importance placed on fast and resilient networks is only becoming greater.

Threats to cloud services

The increasing volumes of data flowing across public and private cloud networks is attracting the attention of cyber criminals, who are using anything from simple 'blunt force' attacks to more elaborate techniques in order to breach these networks.

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

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

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

Network vulnerabilities

Network transmitted data, to/from cloud services, is not only exposed to the cyber-threats of bad actors, it is also exposed to network infrastructure vulnerabilities.

The frequency of network infrastructure (switches, routers, etc.) requiring software and security patches has never been greater - occupying technical staff and disrupting network services.

This patching adds significant hidden resourcing and business disruption costs to infrastructure management.

Only high-assurance end-to-end encryption can protect the network data against its exposure to public and private network vulnerabilities.

Similarly, only purpose-built, high-assurance encryptors provide maximum security. In comparison, multi-function network devices with embedded encryption, such as routers, do not provide high-assurance security and are exposed to vulnerabilities.

WHY ENCRYPT?

As increasing amounts of infrastructure and applications find their home in the cloud, the data transmitted between endpoints and the cloud is 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 trust and integrity of the data being transmitted, organisations must act to secure it against a wide range of threats.

For organisations that utilise private cloud, whereby they manage their own infrastructure, this solution will take the form of hardware encryption to protect the core network and virtualised encryption to protect the WAN.

For public cloud providers, this presents a great opportunity to provide encryption to customers 'as a service' – boosting security credentials and opening a new revenue stream.

The breach landscape

According to Gemalto's breach level index, over 14 billion data records were lost or stolen between 2013 and 2018 – equating to 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 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 it. 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 – especially for public cloud providers.

Emerging threats and popular trends

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

A LogicMonitor survey places digital transformation as the top trend driving public cloud engagement today, closely followed by IT agility as organisations look to leverage the benefits of cloud technologies while eliminating infrastructure management costs.

Increased mobility is another factor driving businesses to the cloud as it allows an increasingly geographically dispersed workforce to work together from anywhere thanks to hosted services such as CRM, box-style file sharing applications and UC tools.

Colocation allows organisations to benefit from the resilience of the cloud by hosting their own equipment in a data centre; a step many are taking along their digital transformation journey.

It is predicted that an increasing proportion of cloud services budgets will be spent on online backup and DR - signalling that organisations are becoming more security conscious and aware of the impact data loss could have.

The rapid growth in IoT devices, which will transmit data to and from the cloud, will also impact data security greatly.

As organisations that implement cloud services are introducing borderless infrastructure by default, they must be aware of the devices that lie at the network edge. If left unprotected, these devices provide hackers with opportunities to gain access to networks and mine sensitive information or input rogue data.

There has also been a notable rise in the theft of 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 AES encryption standards 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 10 years, meaning organisations need to introduce quantum-ready encryption now or risk the integrity of their data.

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

As increasing amounts of data flow across cloud networks, it is left vulnerable to breaches ranging from hack attacks to internal data misconfiguration or loss.

One such instance occurred in May of 2018 when a breach at LocalBox, a personal and business data search service, resulted in 48 million data records containing data from multiple sources – including scraped data from social media platforms – being leaked after a cloud storage repository was left publicly available.

A 2017 breach at Equifax, one of the world's largest credit rating agencies, saw data on 143 million US households stolen due to a misconfigured cloud storage system.

Transportation network company Uber had a similar experience in the same year, when a breach of its AWS account compromised the personal information of 57 million users worldwide. Instead of disclosing the breach, the company paid the hackers $100,000 to delete the data – resulting in a media storm and the resignation of the company's CEO.

In 2015 American health insurance company Anthem suffered a breach of their hybrid network. This resulted in over 37.5 million records with personally identifiable information being stolen after hackers gained access to an on-premise customer database after hacking a public-facing administrative website. The hackers also leveraged cloud storage to extract these records.

[12] The 2019 State of IT, Spiceworks

SECURING CLOUD SERVICES

By tapping into data in motion, 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 the cloud network – compromising the integrity of the data and the platform as a whole.

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

End-to-end encryption

Encryption is crucial to ensuring the security of cloud services. It should be deployed as an end-to-end solution across all layers of the network – including IoT devices – 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.

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 whether they are operating their own private cloud or providing a public cloud service to a customer base.

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

- Compromised high-speed network performance
- Hidden costs of lost effective bandwidth
- Adverse impact on business-critical applications
- Complex implementation and ongoing management technical impact
- Adverse impact on other network assets

Security as a service

As organisations and individuals become more security conscious, it is imperative for public cloud providers to offer encryption as a service to end-users as part of their wider security as a service offering.

Implementing encryption as a service allows providers to either apply it across the network or make it available to end users as an additional layer of security; something that can be leveraged as a service differentiator.

Cloud file sharing services

Sharing information as email attachments does not guarantee the security of the information being exchanged if it is intercepted.

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, without requiring lengthy processes to manage data exchange.

CHOOSING THE RIGHT ENCRYPTION SOLUTION

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.

Borderless infrastructure and edge computing sees data flowing from devices across the network, 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.

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, Senetas' SureDrop secure file sharing application
delivers a familiar box style functionality with high-assurance data protection.

SureDrop is also available to cloud managed service providers as a custom security add-on that can be offered to end users.

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.

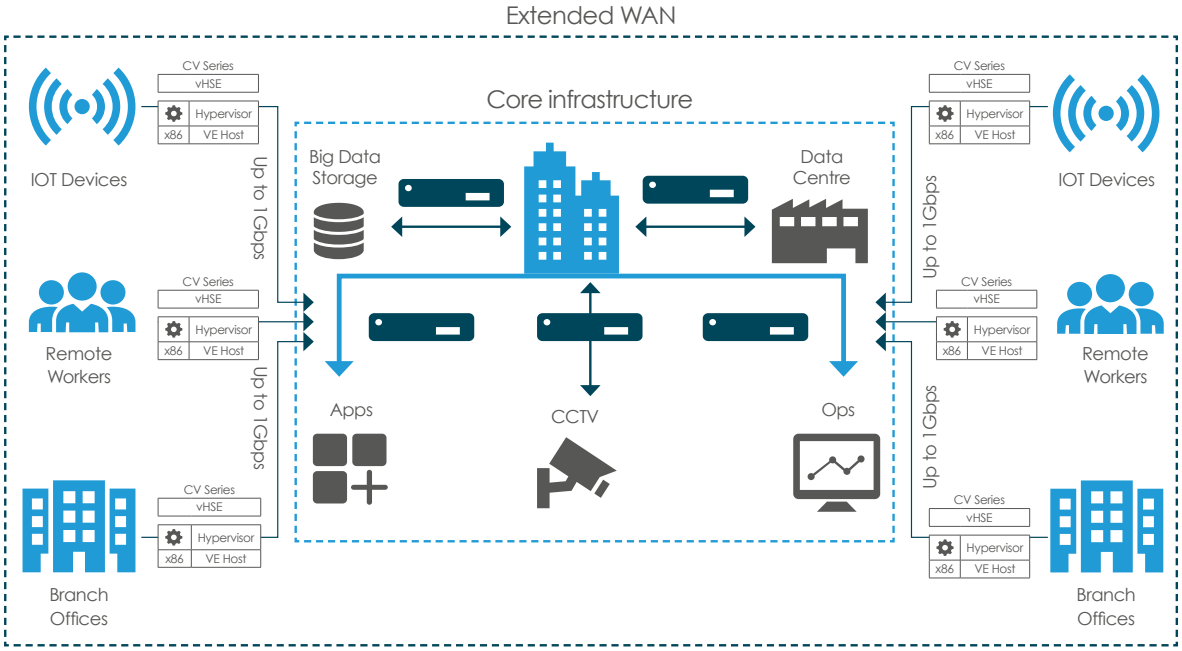
Mixed use cases

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 public and private cloud 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 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

USE CASE:
CLOUD SERVICES PLATFORM

Interoute, owner operator of Europe's largest cloud services platform, provides hosting services to Sterci's Software-as-a-Service (SaaS) product, GTSuite cloud Services, through Swiss data centres.

Sterci wanted to implement a secure data transmission platform for its customers' highly sensitive data.

Sterci chose Senetas high-assurance, certified CN encryptors. These were deployed by Ineroute across a high-availability network between data centres in Geneva and Zurich.

The partnership among Sterci, Interoute and Senetas allowed Sterci to match all the critical network transmitted data security requirements of Sterci's financial sector customers and meet SWIFT obligations.

Senetas encryptors are transparent to the network, ensuring 100% of the available bandwidth without packet expansion or loss and with latency fewer than 10 microseconds – all necessary for data centre interconnection.

Centralised network management tools, and features such as Link Loss Forwarding, ensure easy encryptor management and monitoring, as well as maximum network availability.

The simple installation and "set-and-forget" functionality minimises on-going maintenance costs, as well as the customer's total cost of ownership (TCO).

SENETAS CV1000
VIRTUALISED ENCRYPTION

The CV1000 is a Network Function Virtualisation (NFV) 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 NFV 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

*Subject to host appliance performance.

SUREDROP
ENCRYPTION 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 becomes 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.

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 ENCRYPTION 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 devices with encryption "embedded".

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.

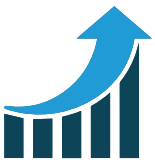
All Senetas encryptors feature automatic zero-touch key management. They also feature automatic network discovery and connection.

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 embedded encryption devices 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 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 as part of its CPL solutions portfolio.

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 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:** info@senetas-europe.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 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.

SCS-SP0121

SENETAS