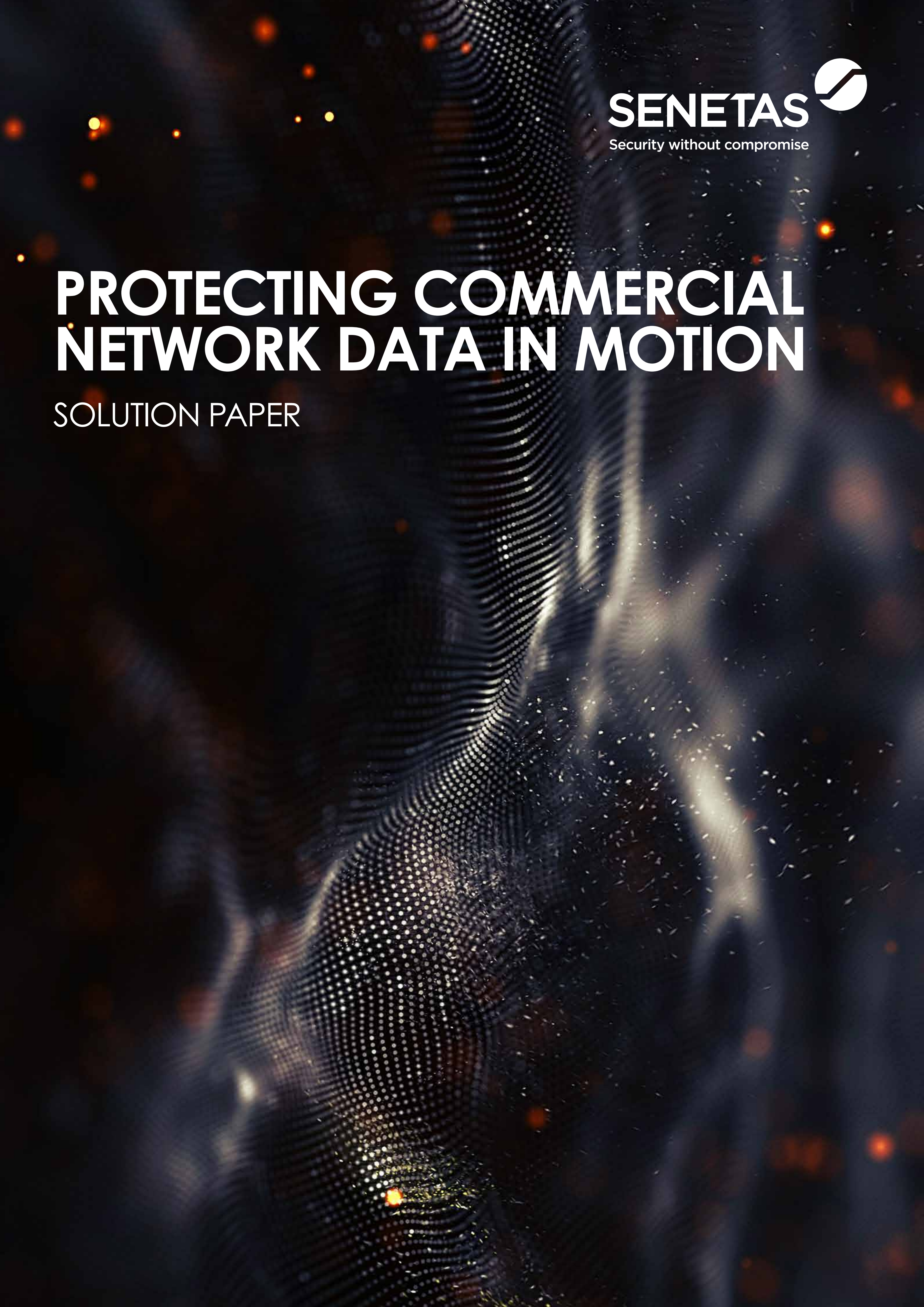


SENETAS

Security without compromise

PROTECTING COMMERCIAL NETWORK DATA IN MOTION

SOLUTION PAPER

PROTECTING HIGH-SPEED COMMERCIAL DATA NETWORKS

Modern organisations have become dependent upon the fixed, high-speed data networks that serve as their core network infrastructure; providing Big Data, Cloud, SaaS and other digital transformation technologies.

These critical technologies and applications generate huge volumes of data. Data that is often transmitted across wide and Metro Area Networks; exposing it to a variety of cyber-threats. Unfortunately, this "data in motion" is often over-looked when it comes to cyber-security planning.

Across the world, commercial organisations are required to comply with a wide variety of cyber-security regulations. Adherence to these standards, whether independent or sector specific, are often a prerequisite to operate within the sector.

However, private and public-sector organisations alike need to understand that managing cyber-security risks to network data goes well beyond essential privacy and compliance issues.

Some of the risks are serious enough that they can threaten the core of an organisation's operations; its value, intellectual property, business intelligence or physical assets.

Despite the high-profile stories of data breaches that have dominated the headlines since the beginning of the century, research repeatedly highlights that these risks are being underestimated; or worse still, ignored.

This is often because of a presumption that core network infrastructure, such as high-speed Ethernet networks, are safe. They are not.

Whether your network infrastructure is carrier-provided (public) or corporate-owned (private), it could be carrying large volumes of data, streamed at anything from 10Mbps to 100Gbps.

As a result, it is a high-value target for eavesdropping and all manner of cyber-attacks. As James Caplan from McKinsey and Company puts it "The larger the data volume, the greater the risk."

When it comes to securing core network infrastructure, the risk is even greater. The vulnerabilities present in major vendors' network devices (such as routers and switches) place an additional burden on infrastructure managers.

Interrupting day-to-day network operations to implement a long list of security software patches is nobody's idea of best practice.

Assuming they can stay up to date with the latest patches, IT professionals are still fighting a losing battle. High-speed networks are not inherently secure and breaches are inevitable.

As innovation and collaboration sit at the heart of modern infrastructure, potentially sensitive or valuable data is constantly in motion across core networks for a variety of reasons:

- Data centre network links for data storage with multiple redundancy for back-up and disaster recovery planning
- Sharing with collaborating partners, suppliers and customers across WAN and MAN links
- Big Data analytics used for research and development
- Cloud and SaaS applications for day-to- day operations

An evolving breach landscape

In a global economy, data has become the life-blood of commercial organisations of all sizes. Protecting this data should be priority.

The commercial sector is amongst the most cyber-security aware sectors in the world. As big data applications and the IoT have come to dominate day-to-day operations, they have focused the minds of cyber-security professionals.

Experts are predicting that cyber-security spend will exceed $1 trillion over the next five years.

The commercial sector's involvement in high-value innovation, science and technological development makes it a high priority target for cyber-attacks from a variety of vectors; including cyber-activists, organised crime syndicates, global competitors, even state-sponsored attacks.

As tighter regulations come into force and organisations are bound by mandatory breach notifications, the true scale of the problem is becoming apparent.

The breach landscape has been dominated by web-based vectors in recent years, as cyber-criminals seek to gain from identity theft, financial or account access.

No industry sector is safe, with high-profile breaches spanning healthcare, energy, telecommunications, banking, retail and technology companies.

The Yahoo breach in 2013 was the largest ever, with 3 billion users' account details compromised because of ineffective data security.

The cost of a data breach continues to rise. In its 2020 report, IBM puts the average cost of a data breach at $3.86 million.

Consider eavesdropping on core network infrastructure. How and when would an organisation know its data streams are the subject of eavesdropping?

When eavesdropping is discovered, what damage has already been done and what future damage may be done?

- What products have been compromised?
- What R&D investment has been lost?s
- Which customers will no longer buy your products?
- What will the downstream effect be – i.e. damage to reputation, trust and brand?

This downstream effect has become increasingly damaging, where manufacturers with unique product technologies discover their intellectual property has been stolen.

In the US, rogue state actors eavesdropped on the core network infrastructure of international advertising and marketing agencies used by global enterprises.

Concerns among agencies and their clients identified that business critical product development, pricing and other secrets had reached competitors in foreign states. The costs to the agencies and customers involved are being measured in hundreds of millions of dollars.

The business of cyber-crime

Cyber-crime is not limited to activities of common criminals and bored teenagers. It is now a key domain and skillset of terrorists and state-sponsored hackers.

Like any well-run business, cyber-criminals have plans based on objectives – whether to do serious harm, engage in espionage (industrial, defence or state), or just make money.

A recent Verizon Cyber Security Report states, "Cybercriminals care most about ROI (return on investment), so make yourself expensive to hack."

The report suggests where would-be hackers discover high-quality data protection, rather than a challenge to overcome, it acts as a deterrent and encourages them to "move on and attack organisations that are not so well protected".

Cyber-criminals have become more skilled and better equipped in recent years, but prevention technologies have struggled to keep pace.

Like most anti-crime measures, prevention is a process of catch up. This, in part, explains the shocking statistics published every year.

Prevention versus protection

When it comes to protecting network data in motion, a robust cyber-security strategy needs to include elements of both prevention and protection.

Prevention uses technologies designed to stop a data breach. Whether that breach occurs while data is in motion or not, breach prevention technologies are key components of any cyber-security strategy.

However, if there is one truth in data security, it's that it's not a matter of if a breach will occur, but when.

Protection is concerned with safeguarding data in the event of a breach. Only by encrypting your data can you ensure that when prevention fails, your data remains protected.

Not all encryption solutions offer the same level of security, as we look towards the future, encryption solutions must be crypto-agile and provide high-assurance data protection.

High-assurance encryption solutions provide long-term protection for data; well beyond its useful life. They also provide protection against the increased use of traffic flow analysis, where cyber-attackers seek to gain insights from analysing data flow patterns.

It may be surprising to know how much cyber-criminals can learn from core network infrastructure traffic flows.

Initially a defence force tactic used to infer intelligence about enemy troop movements, traffic flow analysis has also become an important cyber-security issue for commercial organisations. Targets are frequently oblivious to the eavesdropping and inferences made by the cyber-attacker.

The future holds greater uncertainty, as new technologies like Quantum Computing evolve.

Although a viable quantum-computer may still be 5-10 years away, its arrival will render much of the technology currently used to secure public key infrastructure redundant; unless your encryption solution has agility built-in.

What is high-assurance encryption?

The term is used to differentiate between encryption methodologies and features. Four critical components make up high-assurance network data encryption:

1. Secure and tamperproof hardware; 100% dedicated to encryption
2. End-to-end, authenticated encryption; ensuring no data is unencrypted when in motion
3. State-of-the-art, zero-touch encryption key management; ensuring only the customer can ever access the keys
4. Use of recognised, standards-based encryption algorithms; such as AES256

In addition to high-assurance criteria, robust encryption should also be officially certified by independent standards authorities as suitable for government and defence use.

Certification represents an independent validation of your chosen solution. The three key standards organisations are:

- Federal Information Processing Standard (FIPS) – United States
- Common Criteria (CC EAL) – International
- North Atlantic Treaty Organisation (NATO) – All Member States.

Since developing the first CN encryptor, Senetas has chosen to differentiate its products through certification. Multiple certifications form a key part of the 'certified high-assurance' Senetas proposition.

We refer to this commitment as 'Certifications In-Depth'. Having developed expertise in security standards and testing requirements, certification is a cornerstone of Senetas' hardware encryption design and development.

Critical risk factors

In recent years, four key factors have emerged as critical cyber-security risks within the commercial sector.

An increase in collaboration has led to the sharing of sensitive information outside of the data security safe-zone (with customers, employees, partners and suppliers).

The Internet of Things has broken down the borders of traditional infrastructure and exponentially increased the number of access points to the network.

Old-fashioned human or technical error, whilst on the decline, still accounts for almost 1 in 5 of all lost or stolen data records (2017 Gemalto Breach Level Index).

Security vulnerabilities discovered in core network infrastructure devices significantly add to the cyber-security risks of data in motion.

Examples include:

- Network devices discovered to have security weaknesses that may be exploited by cyber-criminals
- Inferior or poorly engineered devices that promise added encryption security, but use weak encryption processes

In one instance, PC World reported that over 840,000 Cisco networking devices from around the world were exposed to a vulnerability akin to one exploited by a hacking group.

Research by SEC Consult revealed further vulnerabilities in over 900 products; with poor encryption key-management processes used by routers and switches that promise "hybrid encryption".

This highlights three key issues for defence industry organisations that take data security seriously:

- The importance of certified encryption solutions and government evaluations
- Why encryption security must be a 100% dedicated and separated function
- That hybrid network and security products do not offer optimal data protection

> "Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting."
>
> Bruce Schneier.

The real cost of a breach

Cyber-security experts continue to warn that too many organisations underestimate and underinvest in protecting data in motion.

Whether all data in an organisation is sensitive per se, is not the point; nor is it a reason to avoid protecting it with encryption. Data has become the currency of modern business and the rewards for cyber-criminals, hackers and terrorists can be significant.

Beyond the potential for privacy breaches, and a failure to meet regulatory compliance obligations, the impact of a data breach can be catastrophic.

Loss or corruption of critical business data and management information can have a wide-ranging impact on day-to-day operations.

Even greater impact would come from the loss of intellectual property or "secret" information that provides any degree of competitive advantage.

Under new, stricter, data protection regulations, organisations found to be in breach of the rules could face significant financial penalties; especially if it is not a first offence.

The GDPR, though originating within the EU, will impact on just about every organisation and includes the potential for eye-watering penalties (up to 4% of global revenues) for repeat offenders.

Emerging regulations will also see individuals within organisations liable for financial penalties and even custodial sentences in the case of negligence.

This will place a greater responsibility and "duty of care" on both data owners and processors within the commercial sector.

Longer-term implications of a breach can also be derived from a loss of reputation or trust; jeopardising future revenues.

For example, US industrial software developer AMSC – a listed company – discovered that critical software intellectual property had been stolen and was being used by foreign competitors.

Despite swift action by AMSC (with the aid of the FBI), stock values fell from $370 per share to just $5 per share while the matter was being prosecuted.

COMBINING HARDWARE AND VIRTUALISED ENCRYPTION

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

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

Security versus performance and network link use

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

Network link use cases

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

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

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

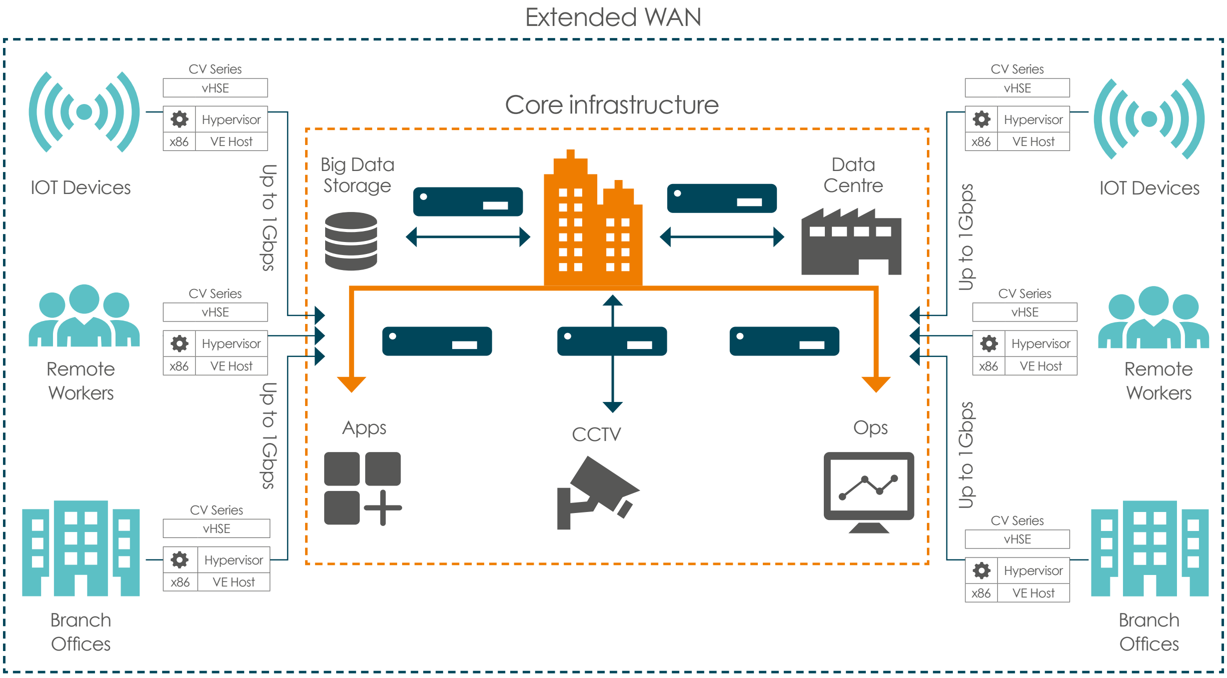
However, for extended WAN links and high-scale virtualised links that typically run at up to 5Gbps, a virtual encryptor is likely to be a more flexible and cost-effective solution.

Mixed use cases

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

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

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



CN SERIES HARDWARE ENCRYPTION

CN9000 Series

The CN9100 is the world's first commercially available certified high-assurance 100Gbps Ethernet network encryptor that supports all network topologies.

Like all Senetas CN encryptors, the CN9000 Series provides maximum high-assurance network data security, without compromising network and application performance. It boasts ultra-low latency of just 1.5 microseconds in customer testing.

Developed in collaboration with customers and service providers, Senetas CN9100 encryptors are designed to meet the exacting requirements of all 100Gbps use cases, making them an ideal application for securing public and private Cloud networks.

Senetas' CN and CV Series encryptors include integrated support for CypherTrust (Thales' centralised cryptographic key management solution) that provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

CN6000 Series

Senetas CN6000 Series encryptors provide highly secure, full line-rate transparent encryption for data moving across both dark fibre and metro/wide area Ethernet networks; in point-to-point, hub & spoke or meshed environments.

The CN6000 Series are rack-mounted, high-speed encryptors for business-critical applications; offering 1Gbps to 10Gbps bandwidth speeds. They are the optimal choice when you require:

- Efficient, investment-proof data encryption
- Multi-purpose, in-field upgradable and flexible hardware
- Choice of Common Criteria, and FIPS certifications
- Compact 1U form factor with advanced performance and power features

CN4000 Series

Network data security is a challenge to organisations of all shapes and sizes, to help address the encryption demands of smaller organisations and in-field operations, Sneetas developed the CN4000 series of compact encryptors.

Despite their small form-factor, Senetas CN4000 Series encryptors boast the same robust security credentials of their rack-mounted cousins.

The CN4000 series is the ideal low-cost, high-performance encryptor range for small to medium-sized enterprises (SME). They also provide a cost-effective "encrypt everywhere" solution for larger enterprises looking to secure remote or temporary locations connected via networks operating at up to 1Gbps.

Like all CN hardware encryptors, the CN4000 Series features standards-based encryption, secure key management and the peace of mind that comes from certification by the world's leading independent testing authorities.

WHAT MAKES CN SERIES ENCRYPTORS STAND OUT?

Performance

High Speed

Market-leading performance. Operating anywhere from 10Mbps or 100Gbps, Senetas encryptors consistently win competitive performance test.

Low Latency

Operating in full duplex mode, at full line speed, without packet loss. Latency is as low as 2 microseconds per unit at 100Gbps.

Zero Impact

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

Security

Certification

For over 20 years, Senetas R&D has remained committed to the principle of certification in depth. Senetas CN Series encryptors are certified by: FIPS, Common Criteria and NATO.

Key Management

All CN Series encryptors feature state-of-the-art encryption key management. Keys are securely stored and encrypted, and only accessible by you.

Solution Integrity

Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption.

Versatility

Crypto Agility

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

Topology Support

Senetas CN encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies.

Flexible Management

Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software.

Efficiency

Cost Effectiveness

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

Reliability

All carrier-grade Senetas encryptors are hot-swappable, feature dual redundancy and deliver 99.999% uptime.

Flexibility

Use of FPGA technology enables maximum operational flexibility, including use of custom encryption and in-field upgradability.

Secure, tamper-proof, dedicated hardware

Standards-based encryption algorithms

End-to-end, authenticated network encryption

Automatic ‘zero-touch’ encryption key management

High-Assurance Encryption

As recommended by leading data security and encryption analysts; for a network encryption solution to be truly robust, and provide long-term data protection (well beyond the useful life of the data), it must be a high-assurance solution.

Not all encryption solutions are created equal. So-called ‘hybrid’ encryption devices – such as network routers/ switches with embedded encryption or those using MACSec or similar standards (not originally intended for WAN and MAN security) provide low assurance data protection.

By contrast, Senetas CN Series encryption solutions are certified by the world’s leading independent testing authorities as suitable for government and defence applications. They are purpose-engineered for dedicated, high-assurance network data security.

Senetas CN Series encryptors’ security credentials include all four essential high-assurance features:

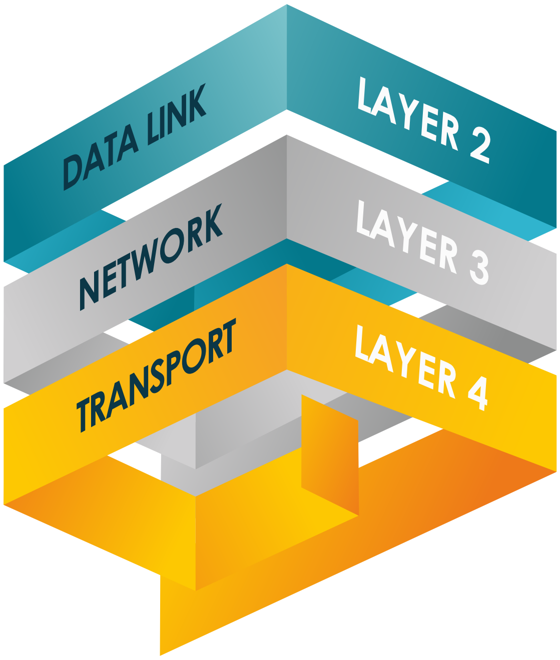
- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art, client-side, zero-touch encryption key management
- End-to-end, authenticated encryption
- Use of standards-based encryption algorithms

Network Independent Encryption

Many organisations utilise multiple data network Layer protocols (Layer 2, 3 and 4) to help deliver their business applications and communications services. Recognising this, Senetas has designed-in Network Independent Encryption.

This advanced, network Layer agnostic encryption technology enables destination policy-based, concurrent multi-Layer encryption.

Significantly, customers are still assured of strong, end-to-end encryption as the protected data traverses the various network Layers, for example: from Layer 2 Ethernet to Layer 3 IP network destination.



CV1000 VIRTUALISED ENCRYPTION

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

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

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

Integrated support for SafeNet KeySecure (Thales' centralised cryptographic key management solution) provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

Enhanced key security

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

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

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

DPDK acceleration - performance up to 15Gbps

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

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

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

Key benefits

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

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

SUREDROP ENCRYPTED FILE-SHARING

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

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

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

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

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

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

SureDrop + Votiro Disarmer

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

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

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

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

Key benefits

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

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its brand.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our **ANZ Partner Page** for full details.

© 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:** 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.

COMNDS-SP0820

SENETAS