
SENETAS
Security without compromise
SECURING HIGH-TECH INDUSTRY NETWORK DATA
SOLUTION PAPER

# CYBERSECURITY CONSIDERATIONS FOR HIGH-TECH INDUSTRIES

We all understand the negative impact of data loss, so why is it that so many organisations seem to be failing in their duty of care to protect sensitive personal and commercial data?

Failure may sound harsh, but shareholders, suppliers, customers and employees have a right to expect their data to be protected. They shouldn't expect to suffer harm (loss of share capital, business disruption, stolen IP, privacy breaches and financial penalties) as a result of inadequate cybersecurity.

High-tech industries have become a target of choice for "bad actors" because of the potentially rich rewards resulting from a successful hack.

## The global technology market

The global technology market has continued to see strong growth in recent years. According to the 2019 Global 2000, Forbes' annual ranking of the world's largest public companies, technology companies account for more than $9 trillion in market value.

Moreover, a record 184 technology companies claimed a spot on this list; an increase of more than 40% on the previous report. The United States is home to almost half these organisations, with China taking second place, closely followed by Taiwan and Japan respectively.

These high-tech organisations, as well as those that fall outside the Global 2000 list, come from a diverse range of sub-industries – from electronics manufacturing and software development to digital media and aerospace.

All of these companies share a common trait: they operate at the leading edge of their respective industries, where IP and network security play a vital role in ensuring competitive advantage.

The very nature of these high-tech industries means that large volumes of data are generated; much of which will be sensitive in nature. This data is an attractive target for cyber-criminals.

## The threat landscape

The treats facing organisations that operate within high-tech industry verticals are many and varied; ranging from IP theft and eavesdropping to rogue data injection.

The impact of a successful data breach could range from financial to existential losses which, according to the 2019 Cost of a Data Breach Report by IBM Security and Ponemon Institute, can be felt for years to come.

The report shows that, while an average 67% of breach costs come in year one, 22% occur in the second year and 11% more than two years after the event.

Thankfully, effective cybersecurity prevention and protection technologies are readily available, and more cost-effective than ever. For example, the use of end-to-end encryption solutions (both for data at rest and in transit) is considered mandatory by many cybersecurity experts.

Encryption should be considered an everyday part of doing business; especially in high-value and high-tech industries.

## The role of the high-tech industry

Ironically, high-tech organisations themselves could play a vital role in shaping the cybersecurity landscape of the future.

Organisations operating at the forefront of technological development will not only unveil countless opportunities for innovation, but also their associated threats as the two come hand-in-hand.

One such example is the space industry where, as we move towards the age of the quantum computer, professionals are turning to satellite technology for the answer to tomorrow's cryptographic technologies.

Quantum Key Distribution is a technology that sits at the heart of future quantum communications networks. A network of communications satellites could hold the answer to a cost-effective, global QKD platform.

# IF YOUR DATA'S WORTH ANYTHING, IT'S WORTH ENCRYPTING

## An unsettled outlook

If cybersecurity is tough today, it will be much tougher tomorrow. Emerging business technologies promise greater security challenges as the Internet of Things (IoT), borderless infrastructure and ubiquitous cloud applications lead to a further explosion in high-speed, high-performance data networks and transmitted data volumes.

High-tech industries' use of emerging IoT and AI technologies, and their collaborative use of public and private cloud infrastructure, introduce new vulnerabilities.

Whilst identity theft and financial account access are major motivators for cyber-criminals, state-sponsored cyber-attacks and hacktivism pose a larger threat to society as a whole. Nuisance hacks are becoming less prevalent, but we are seeing the emergence of cyber-terrorism as an existential threat.

Thales' breach level index reports that over 14 billion data records have been lost or stolen in the past 5 years. Worryingly, less than 4% of this data was protected with encryption.

The EU's General Data Protection Regulation (GDPR) was introduced in 2018. In it, a qualifying breach is deemed to be one in which "…data is not protected by strong encryption…".

As the gold standard of data security regulations, the GDPR introduces unprecedented data breach notification requirements and the potential for severe financial penalties in the event of successful breaches of unencrypted data.

The GDPR is important to the global high-tech industry because it doesn't just apply to organisations within the EU, but anyone who trades or collaborates with EU member states.

While regulation is being introduced to encourage standards and ensure sensitive data is kept secure, responsibility for adhering to these standards remains with the organisation.

An example of this occurred in 2017 when, despite Australian data privacy regulations and federal government defence supplier data security requirements, it was revealed that a breach of a defence Industry contractor's data lead to the theft of 10 gigabytes of sensitive data. None of this data was encrypted.

Rather than meeting standards as the 'bare minimum', high-tech organisations must look to go beyond them.

## Looking beyond losses

Cybersecurity is not simply about protection against data loss or privacy breaches. Of increasing concern is the risk of data manipulation, access control, injection of rogue data and even interference with industrial and other asset control systems (i.e. criticalnational infrastructure).

The impact of a data breach or cyber-attack in some commercial markets can range from minor inconvenience to financial hardship; from the temporary shut-down of an application long-term reputational damage.

For critical infrastructure and high-tech sectors, the stakes could be much higher. A successful hack of an unencrypted network could enable a bad actor to seize control of critical systems, disrupt services and impact the day-to-day lives of millions of people. Strong encryption protects against these acts of cyber-terrorism.

**In the words of cybersecurity expert and cryptographer, Bruce Schneier, "Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting."**

## Traps for the trusting

US author and consultant Denis Waitley said, "Life is inherently risky. There is only one big risk you should avoid at all costs, and that is the risk of doing nothing."

His words are all the more poignant in a world where the technologies that help drive business opportunities also open doors to cybersecurity threats that will undermine them.

The adoption of new business technologies and collaboration (local and global) among high-tech organisations (partners, customers, suppliers) using Cloud, SaaS, multi-Cloud, IaaS and hybrid-Cloud technologies continues to accelerate.

Significantly, they require more complex and high-performance data networks than ever before to enable them and transmit record volumes of proprietary and control systems data.

The world we know has become dependent upon high-speed data networks. From the outset, these data networks are not inherently secure; and networking devices such as routers and switches often add security vulnerabilities.

A reliance on basic infrastructure to secure network data in motion is effectively "a trap for the trusting".

# PREVENTION AND PROTECTION - CAVEAT EMPTOR

There are two key components to data security: prevention and protection.

Prevention technologies (e.g. firewalls) attempt to stop cyber-attacks and data breaches from occurring. They are essential components of a good cybersecurity strategy but cannot work alone. If there is one truth in data security, it's that it's not a matter of if a data breach will occur, but when.

Protection technologies (e.g. encryption) secure the data in the event of a breach. Only encryption ensures that when prevention security fails, the breached data is rendered useless in the hands of unauthorised parties.

Remember, not all encryption solutions are created equal. Your choice of encryption technology should be fit-for-purpose. If you want to ensure long-term protection beyond the useful life of the data, it needs to be purpose-built, dedicated hardware with the agility to adapt to future quantum cryptographic technologies.

## Encrypt everything

Three main factors have added to cybersecurity risks in recent years; vulnerable network devices (routers and switches), email sharing of unencrypted documents with third parties (customers, partners and suppliers), and innocent human and technical errors.

Whether all data in an organisation is sensitive is not the point. As Schneier emphasises, nor is it a reason not to encrypt. Data has become the currency of modern business and the rewards for cyber-criminals, rogue-states and industrial-spies are significant.

High-tech organisations should not only encrypt all their data in motion; it should be encrypted end-to-end as it flows between network endpoint, be this core infrastructure or equipment at the virtual edge.

Should organisations choose not to do this, resultant eavesdropping and IP theft could have catastrophic implications for the organisation, its shareholders and customers alike.

One such example occurred when US industrial software developer AMSC – a listed company – discovered that critical software IP was stolen and used by foreign competitors. Despite swift action and with FBI help, AMSC's stock value fell from $370.00 per share to just $5 per share while the matter was being prosecuted.

# 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 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, the SureDrop secure file-sharing application delivers a familiar box style functionality with high-assurance data protection technology.

For those seeking an additional layer of security, SureDrop + Votiro Disarmer leverages Votiro's patented Content Disarm & Reconstruction (CDR) technology to protect organisations against known and zero-day malware attacks.

# 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.

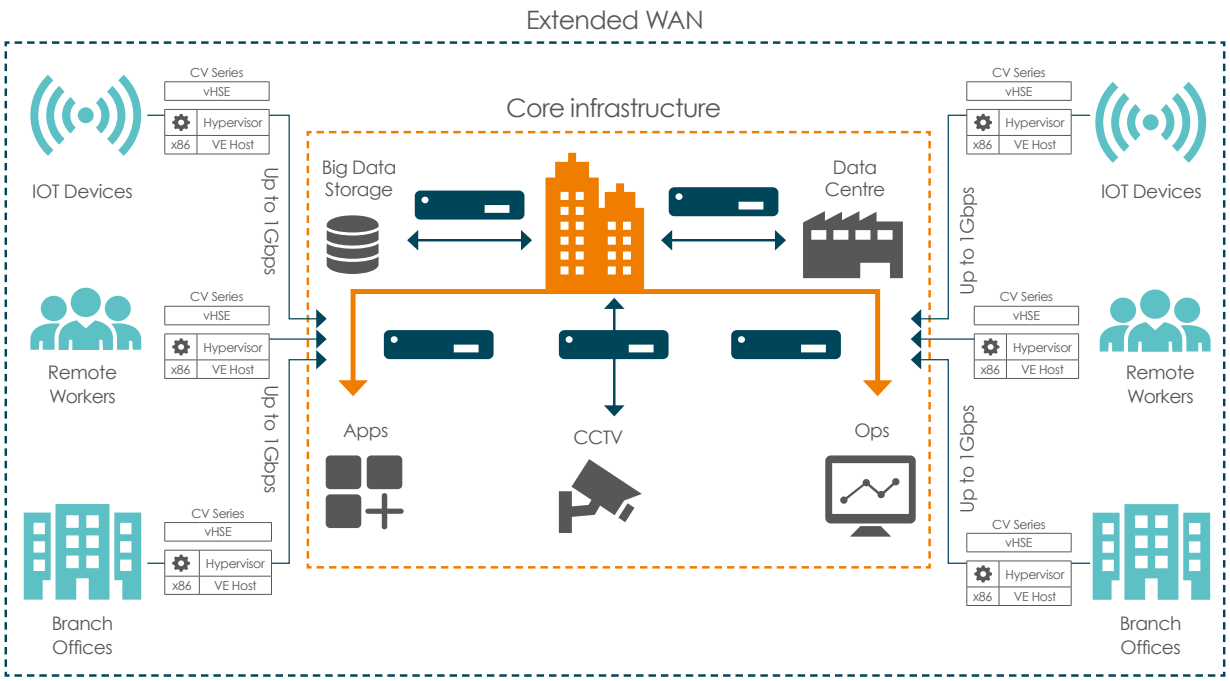
However, for extended WAN links and high-scale virtualised links that typically run at up to 5Gbps, a virtual encryptor is likely to be a more flexible and cost-effective solution.

## 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.

## 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.

## 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.

## Efficiency

### Cost Effectiveness

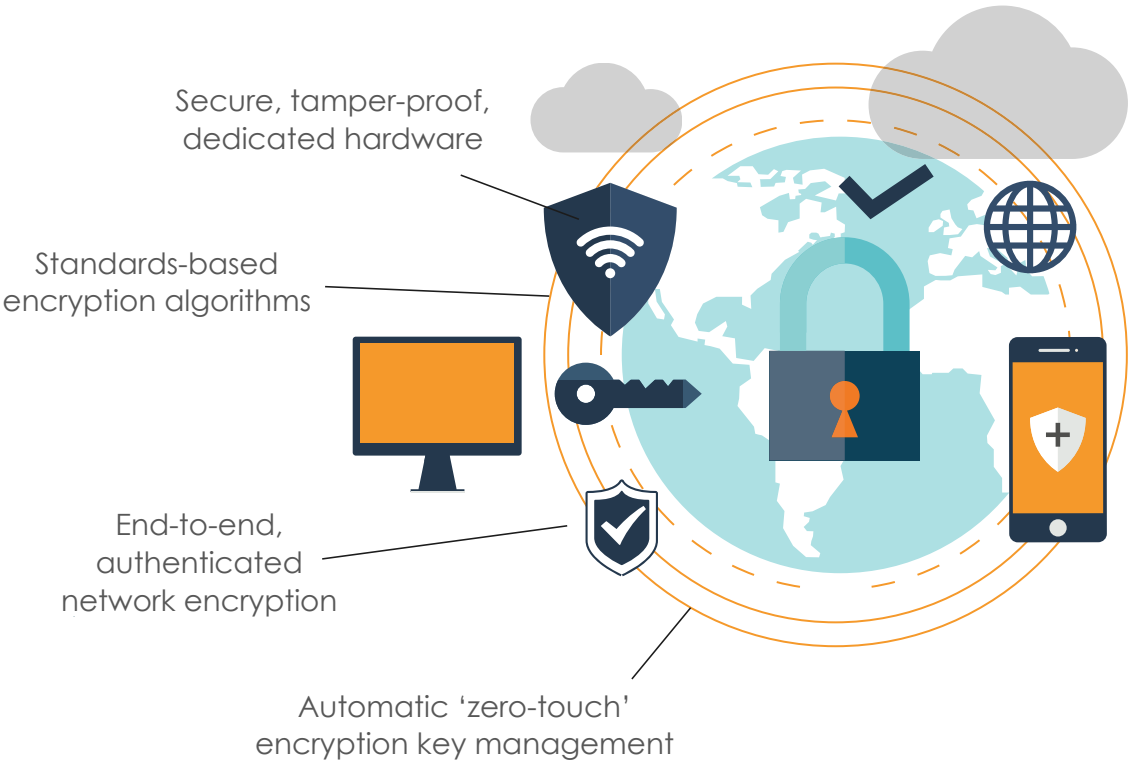
Senetas encryptors provide excellent TCO through a mix of network bandwidth savings, ease of management and longevity.

### 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.




## 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:

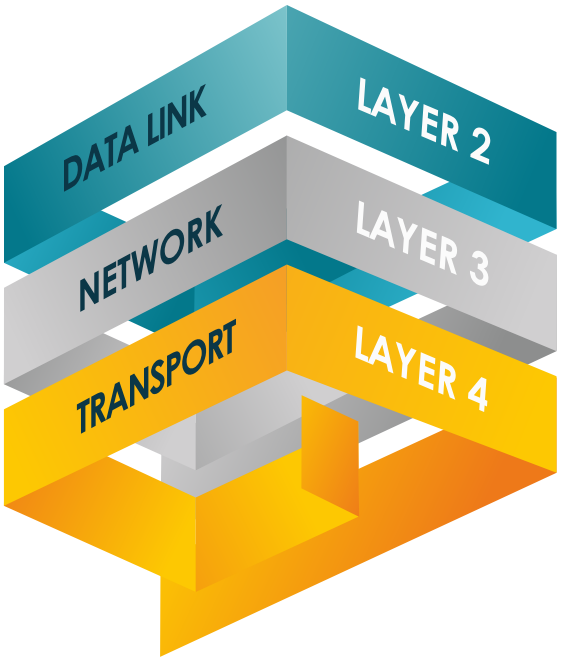
- Secure, tamper-proof hardware; dedicated to network data encryption
- State-of-the-art, client-side, zero-touch encryption key management
- End-to-end, authenticated encryption
- Use of standards-based encryption algorithms

## 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.



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.

SUM-DG0820

SENETAS