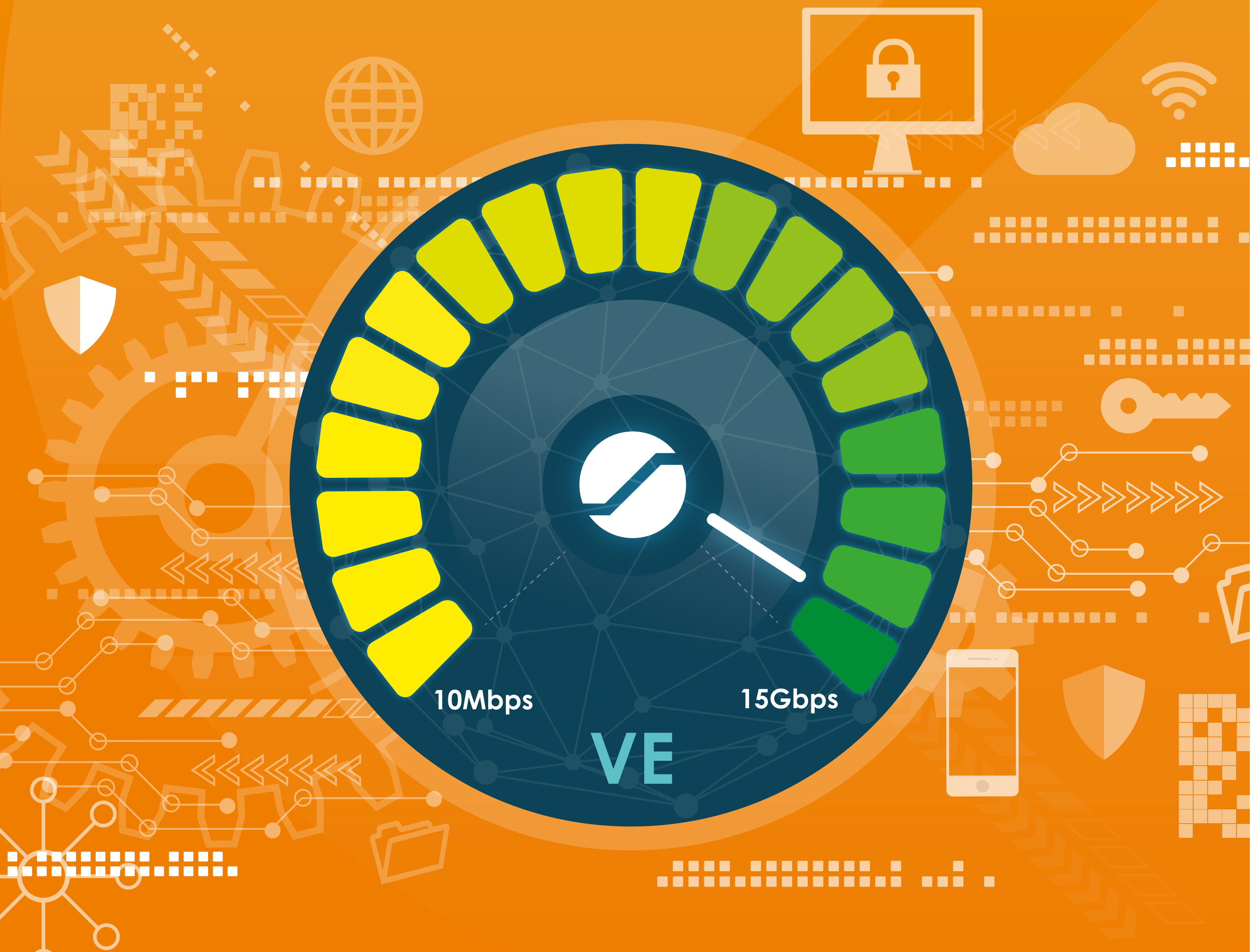
SENETAS
Security without compromise

SENETAS CV SERIES VIRTUALISED NETWORK ENCRYPTION

CV1000 VIRTUAL ENCRYPTOR

Virtualised Encryption, Real-World Security and Performance



Senetas CV1000 Virtual Appliance for virtual CPE and Virtualised WAN

The CV1000 virtual appliance provides strong and effective encryption for virtual customer premises equipment (CPE) and virtualised WAN environments. It delivers high performance (up to 15Gbps), Network Independent Encryption across large-scale virtualised and software-defined networks.

The evolution of network and server virtualisation continues to provide modern organisations with data networking simplicity, scalability and agility. While organisations prefer that data transmitted among core Ethernet network IT infrastructure be protected by certified high-assurance hardware encryption, virtualised encryption plays a key security role for virtual CPE and virtualised WAN.

As workforce mobility, ubiquitous connectivity and borderless infrastructure have come to dominate the IT landscape, the need for high-performance virtualised encryption security has grown.

The increased use of multi-Layer data networks is helping meet the demand for greater agility. IT is required to respond rapidly to changing business demands; driven by a significant increase in network scale and the need to rapidly deploy strong and effective encryption, all the way to the virtual network edge.

From Hardware Encryption to Virtualised Encryption

With enterprise, government, defence and global service provider customers in more than 35 countries, Senetas has a long-established reputation as a leader in the design, development and manufacture of certified, high-assurance encryption hardware for Layer 2 Ethernet networks.

The Senetas CN Series of high-speed hardware encryptors delivers certified high-assurance encryption security. Senetas CN Series encryptors are designed and built to protect core IT network infrastructure; offering predetermined performance and minimal impact on network and application performance.

The introduction of Senetas CV Series virtualised encryption leverages Senetas' expertise in both maximum network data encryption security and high-speed network performance. The CV Series is based on the same state-of-the-art encryption security and encryption key management as the CN Series.

Mobility and agility are key requirements in most organisations where high-speed data is transmitted beyond core Ethernet network infrastructures across large-scale networks. IDC has recently estimated that data networks are expanding at an annual compounding rate of 42% through to 2020. That same data network mobility and agility is now matched by Senetas CV1000 virtualised encryption.

The Senetas CV Series operates as a Virtual Network Function (VNF) that runs on industry-standard x86 appliance hosts and is compatible with virtualisation technologies such as VMware and Hyper-V (hypervisors).

The CV1000 is a software version of the CN Series encryptors. Whilst the CV1000 is optimised for performance, network and application performance is not predetermined. Rather, it is dependent upon the host x86 configuration and the customer environment and targets.

Why Virtualised Encryption?

The optimal application of the CV1000 is data protection across large-scale, virtualised WAN environments. Beyond the core IT infrastructure, these wide-area networks typically operate at speeds of 1Gbps or less; where customers prefer to protect without dedicated hardware solutions, but still require strong and effective data encryption security.

Senetas CN Series, 'certified high-assurance' encryptors are, by definition, secure hardware devices; dedicated to network data encryption. Their optimal use is in protecting core IT network infrastructure data.

Typically, core network infrastructure includes high-speed links (1Gbps, 10Gbps and higher) among key IT assets; such as those used for Big Data applications, data centre interconnections, data storage and redundant data centre back-up and disaster recovery.

Today's WANs often extend well beyond core infrastructure and include multi-Layer transport. However, the data transmitted to the edge of the network still requires strong and effective encryption protection; this is where virtualised encryption becomes an optimal solution.

Here, virtualised encryption provides the scalability, simplicity, flexibility and cost-efficiency demanded by IT and data networks managers.

Senetas CV1000 Virtualised Encryption

The CV1000 is a Virtualised Network Function (VNF) providing strong and effective data encryption security with designed-in crypto-agility. Designed for large-scale WANs, the CV1000 delivers Network Independent Encryption for high-speed networks at >15Gbps.

As an VNF 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 (the industry-leading 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.

How is the CV1000 Implemented?

The CV1000 is a guest virtual machine (VM) that runs on industry standard x86 hosts and hypervisors.

Large-scale WAN customers do not need to be operating network virtualisation to implement the CV1000 as a secure and efficient security solution.

Like any VM, the performance of the CV1000 is customer target specific and dependent upon the operating environment and platform. This means that implementation specifications are a guide only.

- Vendor agnostic x86 hardware
- Host configuration – minimum recommended:
    - Number of cores – three
    - RAM – 2GB
    - Virtual disk storage – 2GB
- DPDK Intel library packet acceleration support - enabling >1Gbps and up to 15Gbps bandwidth performance.

Platforms supported by the CV1000 include:

- VMware
- KVM/QEMU
- Microsoft Hyper-V

*Subject to host appliance performance

Other features and technologies supported by the CV1000 include:

- Interoperability with all Senetas CN Series hardware encryptors
- Network Independent Encryption - concurrent, policy-based encryption for Ethernet and Internet Protocol Networks (Layers 2, 3 and 4)
- Symmetric and asymmetric cryptography
- SafeNet KeySecure – for master key security and random number generation
- Sentinel – for simplified licencing
- Virtualised interfaces – 3x para-virtualised NICs

CV1000 - 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

Maximum Performance

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 15Gbps.

Consistent performance up to 5Gbps 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.

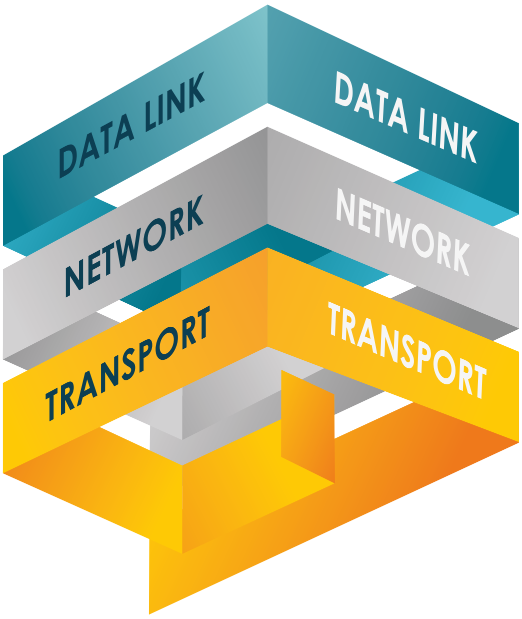
Network Independent Encryption

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, transport 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 destinations.

CONCURRENT, POLICY-BASED MULTI-LAYER ENCRYPTION



Enhanced Key Security

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

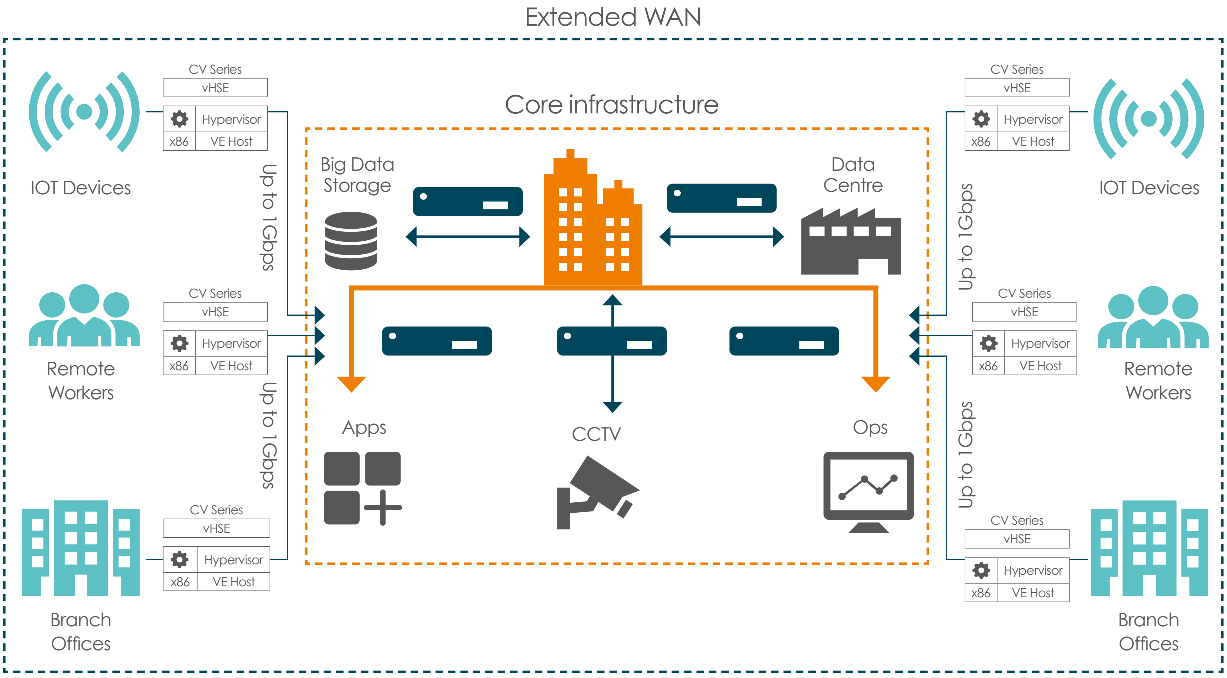
Available as a hardware appliance or a hardened virtual security appliance, SafeNet KeySecure provides support for multiple key types: symmetric, asymmetric, secret data and X.509 certificates.

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

Senetas CV1000 Use Case Examples

Following extensive network performance testing, and a broad range of customer and service provider Proof of Concept trials, the CV1000 proved its security and performance credentials in a variety of use-cases.

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



Your Questions Answered
Please refer to the CV1000 Frequently Asked Questions Customer Guide.

The most common use case for virtualised network data encryption is deployment across an extended WAN. The customer may or may not be adopting virtualisation of the network environment itself, but will be seeking several benefits:

- Efficient use of physical IT and network resources
- Increased responsiveness and flexibility
- Low encryption-cost-per-link
- Overcome the constraints of physical asset deployment across large-scale networks
- A transport Layer agnostic solution - multi-Layer (Layers 2, 3 and 4) network security

Having decided upon a virtualised network solution for its large-scale WAN, the security conscious customer is now considering encryption security solutions.

Just as the customer uses Layer 2 Ethernet network links among core infrastructure assets, it likely protects those links (as illustrated) with hardware encryptors. To protect data travelling across the wider network, a virtualised encryption security solution may be a better fit:

- Delivering the ability to scale rapidly
- Providing ease of deployment via a software implementation
- Enabling strong and effective security at a low cost-per-link

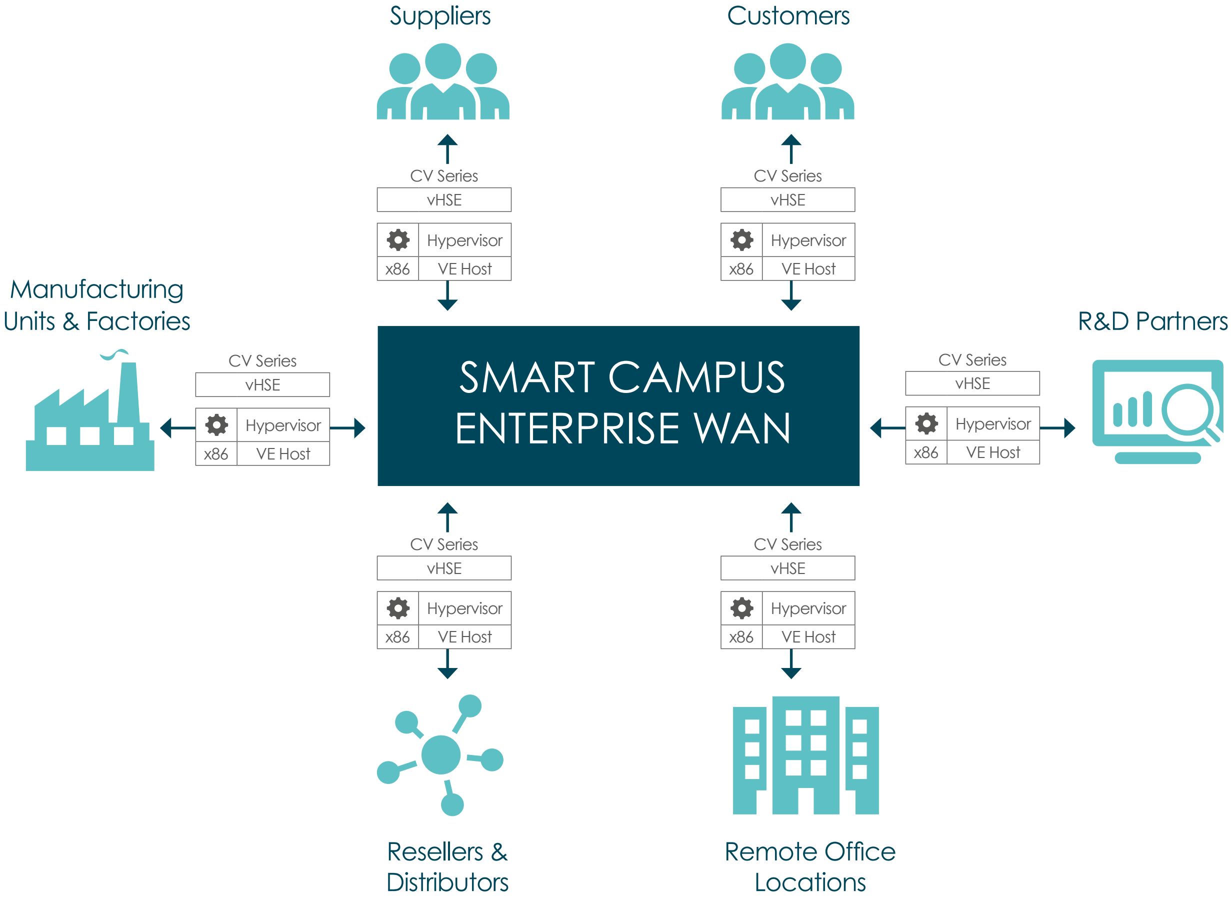
Because the CV1000 is transport Layer agnostic, it provides the flexibility of destination policy-based, concurrent multi-Layer (Layers 2, 3, and 4) encryption security.

Customers' environments may include:

- A high-performance, multi-core (minimum recommended is four cores) x86 host for the CV1000
- DPDK Intel library for packet acceleration
- Multi-Layer (Layers 2, 3 and 4) network links
- VMWare or similar virtualisation environment
- CN Series hardware encryptors used for core Ethernet network infrastructure – 100% interoperable with the CV1000

An important issue of business systems growth today is the infrastructure required to support it. Organisations are realising that what is necessary to enable that growth need not be physical. By virtualising some physical assets there are significant cost and utilisation advantages. One key example is the network.

Smart WAN transmitted data – secure virtualised network environments



This use case is referred to as the "Smart WAN" because it involves virtualising the Ethernet network resources, leading to network connectivity (Layer 2) that supports the network's increasing scale.

A "Smart WAN" often includes multiple network Layers (Layer 2, 3 and 4). Because the CV1000 is transport Layer agnostic, it provides destination policy-based, concurrent multi-Layer encryption security.

It may also reflect the customer organisation's preference to maximise virtualisation of what it considers to be underutilised IT physical assets, or overcomes the inconvenience of deploying physical hardware across the entire estate.

The benefits being sought are typically a mix of:

- Reduced WAN costs through more efficient use of the physical IT and network assets
- Significantly lower encryption costs beyond the core Ethernet network infrastructure, especially where bandwidths are often lower and the costs of deploying hardware are considered too high
- Increasing business performance through responsive and secure network expansion to the full reach of the organisation
- Enabling a more responsive and flexible network as business and application needs change.

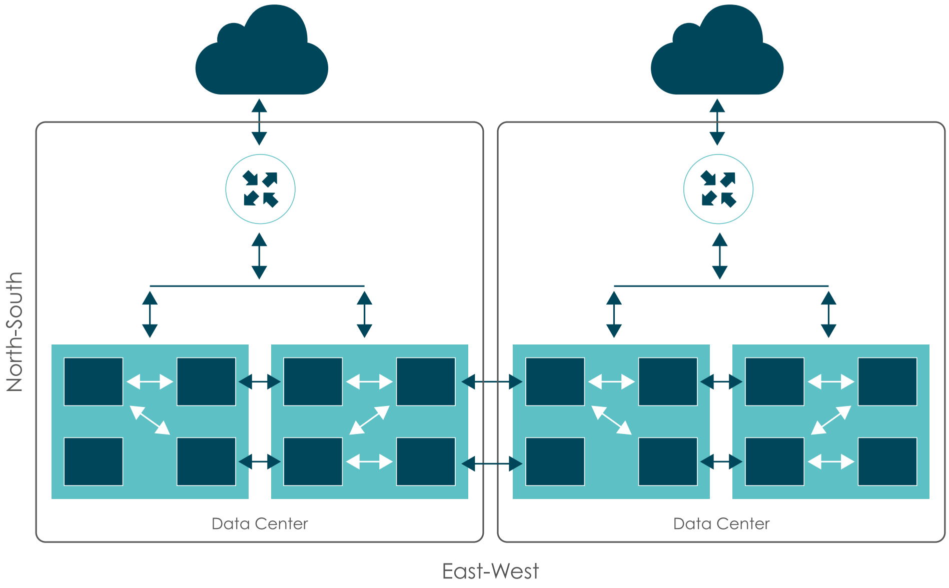
These benefits provide a strong business case for virtualisation in general, as well as the security initiative to protect network data cost-effectively.

Customers' environments may include:

- The multi-core x86 host/s for the CV1000
- DPDK Intel library for packet acceleration
- Virtualisation technologies such as Hyper-V or VMware
- Large-scale network links beyond the core Ethernet network infrastructure
- Customers may or may not already protect their core network infrastructure high-speed Ethernet links with CN Series hardware encryptors

As data centre and Cloud infrastructure matures through innovations in server technology, switch design and network and storage virtualisation, securing the applications and data in the data centre has become the top priority for many customers' IT managers.

Secure East-West Data Centre Traffic



Customer IT managers often require data centre service providers to not only secure traffic within the data centre (data centre container), but also demand separation of their East-West traffic from any other customers' traffic.

Traffic in data centres typically flows in three directions. Traffic entering or exiting from the data centre (from and to the customer) is called North-South traffic.

East-West traffic is network communications between servers and applications within the data centre.

Many enterprise and government organisations have traffic flowing among multiple private and/or public clouds.

Although data is often protected by encryption as it enters or exits the data centre, East-West traffic within a data centre is often unprotected. An IT manager may ask, "If the perimeter is protected, I don't have to worry about the data centre's internal security, right?" Wrong.

According to some research reports, up to half of the security breaches are caused by insiders, within the data centre itself. A compromised device may introduce vulnerabilities accessing the East-West data. Valuable data may be stolen. Also, it is possible that packaged application images may introduce vulnerabilities.

Surprisingly, these attacks may by-pass protections at the data centre entrance because these devices have no idea of what and how things are running within the data centre. It is for those reasons many security-aware organisations insist on their data being encrypted (and even separated) within the data centre as it moves East-West among assets within the overall data centre.

Virtualised encryption has become an excellent security solution for data centre managers as they adopt other hardware virtualisation.

Rather than implement hardware encryptors for each customer's separated East-West data, virtual encryptors provide flexibility, ease of management and lower costs, whilst adopting strong and effective encryption security.

Some key terms explained

Network Virtualisation (NV) – simply refers to the ability to create virtual or logical networks that are isolated from the underlying network hardware. Network virtualisation allows traffic to be separated into 'zones' to ensure it does not mix with other resources.

Network Function Virtualisation (NFV) – refers to the implementation of a network function such as a load balancer, firewall or encryptor in software rather than a traditional hardware implementation.

A specific function such as the Senetas CV1000 is called a Virtual Network Function or VNF. VNFs run on high-performance x86 hardware as virtual machines. Overall, VNFs deliver flexibility, scalability and responsiveness, (especially in high-scale network environments) and reduce capital expenditure requirements.

Software Defined Networking (SDN) – provides centralised control of the software processes that define the network, making the network programmable.

Virtualised Networks and Software Defined Networking

The move towards network resource management via software seeks to make increasingly complex and widespread networks more flexible and responsive to fast changing requirements.

Because SDNs are network Layer independent (Layers 2, 3 and 4) and protocol independent, they offer flexible networking. Being software-controlled, SDNs also enable greater flexibility and responsiveness in network architecture, as well as opportunities to expand the network scale quickly.

SDN technology is designed to make networks just as flexible as virtualised servers and storage. Virtualisation has become a common feature of data centre resources, making them an ideal use case for virtualised encryption; especially when the virtualised encryption solution does not compromise network performance.

The Senetas CV1000 was developed to match the key objectives and benefits of virtualised and software-defined network environments:

- Enabling network staff to respond quickly to changing business requirements for hardened encryption security
- Enable destination policy-based, concurrent multi-Layer encryption
- Simplified large-scale network traffic and encryption security management from a centralised point, without having to manage hardware such as switches
- Rapid expansion of encrypted network assets to meet business requirements for secure data-in-motion

Strong and Effective encryption security for a virtualised world

As the adoption of virtualisation grows, so does the demand for strong and effective encryption security. The emergence of virtualised and SDN architectures comes in response to the demand for greater control, agility and scalability; driven by big-data, high-bandwidth business applications.

Virtualised and software-defined networks do not come with any form of native data security. The CV1000 was built to match the flexibility, scalability and cost-efficiency of a virtualised environment and to provide strong and effective encryption security, without compromising network performance.

To further enhance its encryption security, the CV1000 integrates seamlessly with SafeNet KeySecure.

SENETAS CV1000 SPECIFICATIONS

SPECIFICATIONS & FEATURES	CV1000 (Software Version: v5.0.1)
Virtual Network Function (VNF) - Hosting Guide	
Network data encryptor type	Transport Layer agnostic VNF encryption (x86 hosted).
Network Independent Encryption	Concurrent, multi-Layer encryption (Layer 2, 3 and 4)
Bandwidth / performance[2]	>1Gbps.
Performance acceleration (optional)[2]	Supports DPDK Intel Library for up to 15Gbps performance.
Virtual appliance (min. recommended)	4x CPU, 4GB RAM (without DPDK) 2GB[3] virtual disk storage 3x CPU, 2GB RAM (with DPDK) 2GB[3] virtual disk storage
CV1000 (guest) operating system	Linux Debian distribution - v9 (stretch)
Functional Specifications	
Supported topologies	Point-to-Point, Point-to-Multipoint & Multipoint-to-Multipoint Layer 2 forwarding
Interoperability	Fully interoperable with all Senetas CN Series hardware encryptors
Maximum number of connections	500+
Encryption algorithms	Symmetric cryptography: - AES-128, AES-256, CFB or CTR modes Asymmetric cryptography: - ECC-512 - RSA-2048
Policy based encryption	- MAC address - VLAN ID
Crypto-agility	Support for custom curves, custom algorithms and BYO entropy
Authentication	Certificate based (X.509)
In-band/out-of-band management	- Console Command Line Interface (CLI) - SSH - TACACS+ - SNMPv3
Virtualised network interfaces	- Eth0 – Management port - Eth1 – Local port - Eth2 - Network port - Eth3 - Aux management port (optional)
Virtualised hosting environment	Supports: - KVM/QEMU - VMware - Microsoft Hyper-V
CV1000 management application	Senetas CM7 - Included
Centralised key server support	Optional support for SafeNet KeySecure - centralised cryptographic key lifecycle management solution[4]
Certificate-based software licensing model	Flexible model choice: - Perpetual - Subscription[5] Excludes host hardware and hypervisor

[1] For virtual (Ethernet) transport
[2] Customer environment, hardware platform and x86 host configuration dependent (DPDK optional)
[3] Subject to image storage requirements
[4] KeySecure provides additional customer benefits. See SafeNet KeySecure website for details
[5] Payable monthly, dependent upon number of instances

GLOBAL SUPPORT

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

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

THALES

ANZ Partner Community

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers; including:

ADVA™ Optical Networking	AUCLOUD	Data#3
DATACOM	dimension data	DXC
IBM	macquarie GOVERNMENT	VOCUS communications

© 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 35 countries.

From certified high-assurance hardware and virtualised encryption, to secure file sharing with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

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.

SENETAS