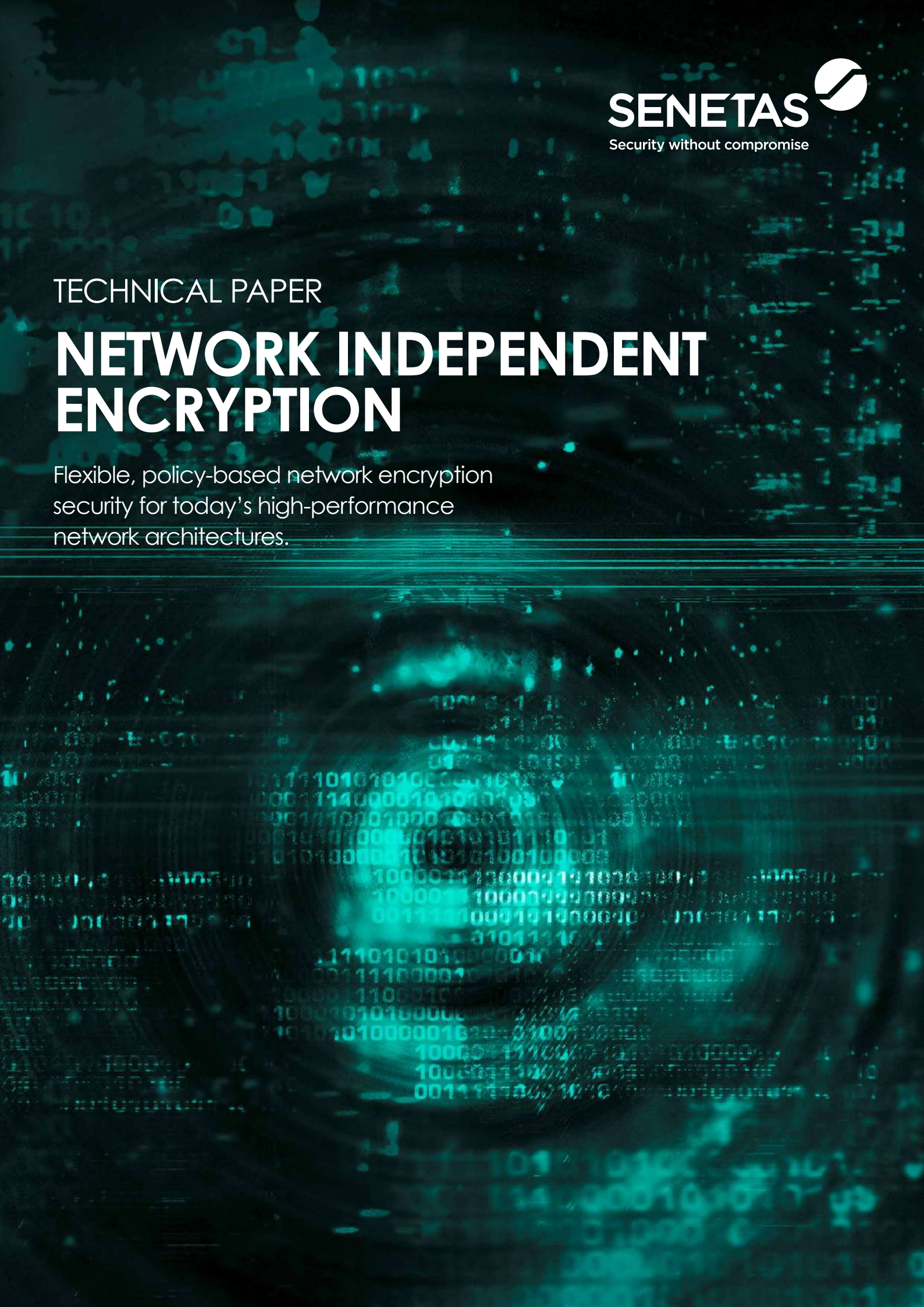
SENETAS
Security without compromise

TECHNICAL PAPER

NETWORK INDEPENDENT ENCRYPTION

Flexible, policy-based network encryption security for today's high-performance network architectures.



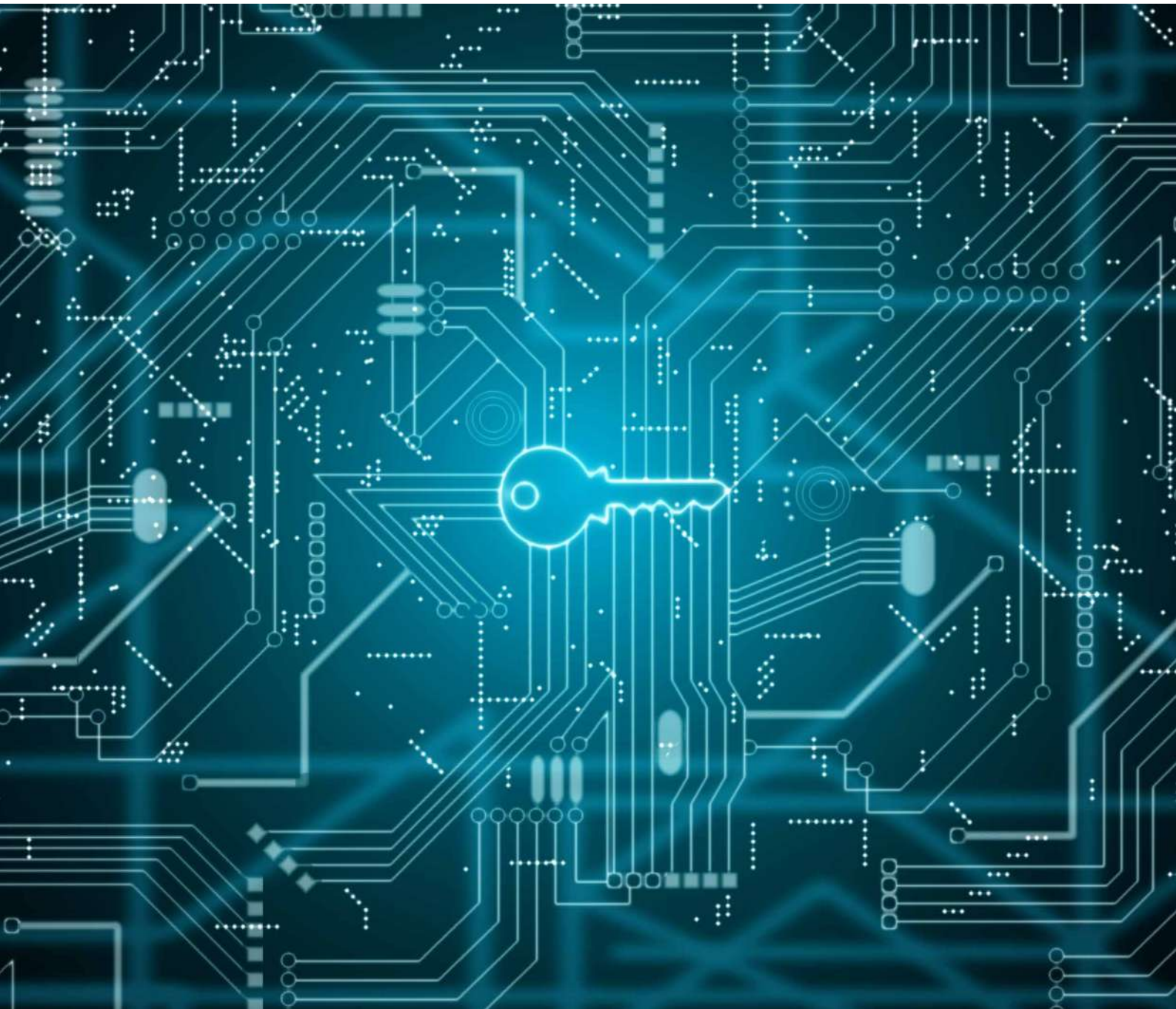
INTRODUCTION

First introduced to the CV Series virtualised encryption range in 2018, Senetas (Thales) Network Independent Encryption is now available for the CN Series of hardware encryption devices. It enables concurrent, policy-based multi-layer encryption for modern Ethernet and Internet protocol architecture

Developed specifically for today's multi-layer networks, Network Independent Encryption provides end-to-end encryption security without the typical performance and bandwidth costs associated with IPSec encryption solutions.

Historically, different network types have required different encryption solutions. As network architecture has evolved to comprise multiple transport layers, this has implications for network security, performance and cost.

In the case of Internet protocols, the most common encryption solution, IPSec, is over 20 years old. IPSec was not developed with wide area networking and cloud applications in mind; it incurs additional bandwidth costs and can impact significantly on network performance.



NETWORK INDEPENDENCE

The introduction of Network Independent Encryption to the CN Series hardware encryptors will help customers meet the increasing demand to protect data flows across multiple network types. The most common network protocols in use today are Ethernet (Layer 2) and Internet (Layer 3).

CN Series hardware encryptors have been used to protect Ethernet networks and their data for the past twenty years. The addition of Network Independent Encryption expands their use to protect Internet protocol networks.

Customers choose different network types for different data flows. With Network Independent Encryption, customers may choose a single, best-of-breed solution. One that provides high-assurance, end-to-end encryption across multiple network types, without compromising bandwidth and performance.

	DATA		LAYER	
HOST	DATA	7	APPLICATION	HTTP, FTP, RC, SSH DNS
HOST	DATA	6	PRESENTATION	SSL, SSH, IMAP, FTP, MPLG, JPLG
HOST	DATA	5	SESSION	API, SOCKETS, WINSOCK
	SEGMENTS	4	TRANSPORT	E2E CONNECTIONS, TCP, UDP
MEDIA	PACKETS	3	NETWORK	IP KMP, IPSEC, IGMP
MEDIA	FRAMES	2	DATA LINK	ETHERNET, PPP, WSITCH, BRIDGE
MEDIA	BITS	1	PHYSICAL	COAX, FIBRE, WIFI, HUBS, REPEATERS

Senetas encryption solutions

CUSTOMER SOLUTIONS

CN Series high-assurance hardware encryptors using firmware v5.01 or above feature Network Independent Encryption (Layer 2 and Layer 3).

- CN4000 10Mbps-1Gbps
- CN6000 1Gbps single and multi-port

CV Series virtualised encryption provides even greater flexibility for wide-area network architectures, supporting concurrent, policy-based encryption across Layers 2, 3 and 4.

Features & Benefits

Network Independent Encryption delivers flexibility through the use of a single solution to encrypt multiple data flows. Both CN Series hardware encryption and CV Series virtualised encryption provide policy-based, concurrent encryption across Ethernet and Internet network topologies.

Key benefits include:

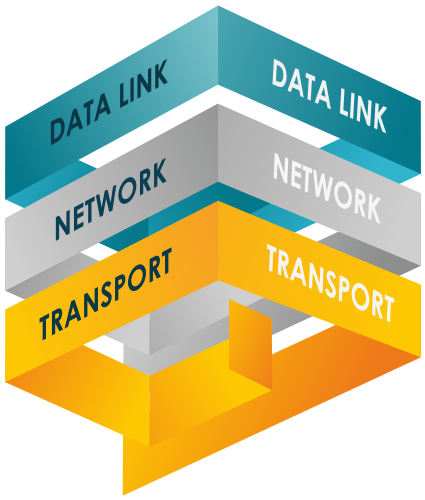
- High-performance, end-to-end encryption
- A single solution for both Ethernet and Internet networks
- Flexibility and ease of use, derived from independence from the underlying carrier network
- Destination and security policy-based encryption
- Tunnel-free, data flow encryption efficiencies
- Reduced management and bandwidth costs
- Near zero latency and data overheads

Policy-Based Concurrent Encryption

The cornerstone of Network Independent Encryption technology is policy-based, concurrent Encryption. This allows customers to define simple policies to concurrently encrypt different traffic flows at either Layer 2 or Layer 3, depending on the underlying network type and the assurance needs of the data.

The encryption of multiple network type data is concurrent IE. It occurs in conjunction with each other and having equal security protection while transported to pre-determined destinations.

Policy-based concurrent encryption matches the flexibility of security decisions with the flexibility of the network architecture employed.



The Case for Network Independence

Deployment of Senetas encryption solutions is not carrier network dependent. Where Ethernet and Internet protocol networks are in place, Senetas encryptors are easy to deploy, require very little management and provide uncompromising performance. In particular, the CN Series hardware encryptors offer:

- Near zero latency
- Minimal data overheads
- Predictable wire-speed performance

Proven ease of use and management have been a hallmark of Senetas solutions used across Ethernet network types. Now Internet protocol network traffic can be protected by the same solution.

Data-Flow Encryption

The most efficient approach to concurrent encryption of Ethernet and IP traffic is tunnel-free encryption. This approach minimises the encryption overhead and allows individual data flows to be natively encrypted at either Layer 2 or Layer 3.

A data-flow encryption approach ensures the optimal performance and security for transmitted data regardless of the underlying network type.

The performance and security benefits of Network Independent Encryption arise from:

- Lower data overheads – minimising the encryption overhead
- Minimises data exposure on the network by encrypting at the most secure layer possible
- Network transparency, does not require network changes – unlike many tunnelling approaches

Network Choices

When it comes to encrypting and transporting data across network infrastructure, organisations naturally choose the service that best meets their needs. For example, high-bandwidth point-to-point networks are ideal for Ethernet Fibre.

However, where multiple office sites require a fully meshed network, but require more modest bandwidth, then a routed Internet protocol network may be sufficient.

In other cases, a switched Ethernet network may be a simpler solution. Then, of course, there will be cost and availability considerations.

Fast-Moving Technologies

For the past 20 years IPSec has been the encryption security "hammer" applied to Internet protocol network data, but in an era of fast-moving technologies, a more appropriate tool is required.

As network dependent application technologies, such as SaaS and Cloud services, demand more intelligent and efficient data networks, encryption security requirements have also changed. Carriers have offered more network types, enabling the direct flow of data.

For example, SD-WAN network architectures allow data to be intelligently directed over the most appropriate transport network to meet the business intent e.g. direct to cloud or back to the corporate datacentre.

Network Independent Encryption security enables a single solution for any customer's multiple network security use case. It matches network architecture flexibility with encryption flexibility by providing a single security solution for organisations' chosen network architecture.

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.

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

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 or secure file sharing and collaboration 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 cybersecurity 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.

NETWORK DATA SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has a network independent encryption solution to suit. Our multi-certified high-assurance encryptors protect data across networks operating at speeds from modest 100Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 15Gbps. 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.

They are trusted to protect much of the world's most sensitive government, defence and commercial data.

SECURE COLLABORATION

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 Secure File Gateway extension.

DISARM MALICIOUS CONTENT

Votiro Secure File Gateway 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