SENETAS

Security without compromise

HIGH SPEED ENCRYPTION PROTECTS GOVERNMENT VSAT & MICROWAVE LINKS

Application of High-Assurance Network Encryption	
Sector:	Government Defence Agency
Use Case:	Encryption of traffic across VSAT and Microwave links
Solution:	High-speed encryption of voice, video and data traffic across multiple network links.

SECURE GOVERNMENT VSAT & MICROWAVE LINKS

This government customer's network security requirements are centered around the need to secure VoIP (Layer 3 Internet Protocol) transmission of high-definition video and voice traffic using microwave and VSAT links.

Due to the sensitive nature of the data transmitted to and from multiple locations, the situation demands high-assurance encryption security without compromising on quality or network performance (EG: jitter or latency on real-time communications). High-definition video, voice and other data are distributed across point-to-point, multi-point and fully meshed network topologies in multiple locations.

Network infrastructure has variable quality and bandwidth is limited in some areas. Geography poses a challenge in many locations, so microwave and VSAT links are required.

Solutions such as IPsec are not suitable as they do not provide the required level of assurance and would compromise network performance by adding significant overhead.

The Business Need

The customer has three independent data networks, requiring communications across its intranet architecture. The primary requirement is 100% end-end encryption security for voice, video and data. Remote sites use a mix of network connections. Some use both microwave and VSAT links while others have only microwave or only VSAT. Where both links are available, the traffic is routed to the best option.

The geography and available network infrastructure add challenges, requiring a solution with optimal performance over both VSAT and microwave links. Microwave communications is line of site and VSAT is geo-synchronous orbit based, so both methods and affected by different environmental conditions.

With video, voice and data all transmitted across the same links, it is important that the encryption solution does not disrupt any data type. While the available network experiences significant latency, it is important that the encryption solution does not materially add to that, nor adversely affect the network performance and quality of video or voice traffic.

The Solution

Senetas CypherNET encryptors provide network independent encryption (Ethernet, IP, Microwave, VSAT and SCADA) providing all locations (remote and central) with secure encrypted VSAT or microwave connectivity without compromising network performance or video and voice quality. CypherNET encryptors can be used in any network topology (from point-to-point to fully meshed), enabling efficient communications among and between the central and regional locations without having to connect via the central location.

A mix of CypherNET CN Series hardware encryptors were selected, based on the available network architecture and performance requirements:

- CN4000 Series – compact, desk-top encryptors for multiple remote locations requiring a maximum of 1Gbps speed.
- CN6000 Series – rack-mounted encryptors for larger remote locations requiring a maximum of 10Gbps speed.
- CN6140 – multi-port, rack-mounted encryptors for the central location, where network architecture is optimized by using a single appliance with up to 4 ports, each capable of handling up to 10Gbps speed.

All CN Series encryptors share the same high-assurance security platform and high-performance attributes and are 100% interoperable.

WHAT MAKES CYPHERNET STAND OUT?

Senetas CypherNET CN Series hardware encryptors were the ideal solution as they met all of the exacting requirements:

- Maximum data security
- Independent security certification
- Near-zero impact on network performance
- Zero impact on high-definition video and voice traffic quality
- Global distribution and support

Other considerations that were significant to the customer's decision included:

Provides AES GCM 256 authenticated encryption security – protecting data from breaches and protecting the network from ingress of unauthorised data such as malware.

Because some sites use both microwave and VSAT links, the CN4000 encryptor's small footprint and low power usage enabled colocation without the costs of site modifications.

The high volume of voice traffic with very small frame sizes could not be supported by standard encryption techniques such as IPSec.

MACSec based solutions use multi-function network devices. They do not provide high-assurance security and would require routers in all locations.

The CypherNET management software (Senetas CM7) provides centralised and remote encryption management, as well as easy audit reporting over multiple circuits and network protocols.

CypherNET delivers a lower total cost of ownership through "set and forget" solution management, 99.999% device uptime reliability, and no software patching queues.

Network Independent Encryption. CypherNET encryptors provide a policy-based encryption method enabling them to be used in almost any network. Encryption may be concurrently conducted over Ethernet, IP and Transport Layers (Layers 2, 3 and 4).

Crypto agility. A future-proof solution that provide long-term information security. CypherNET offers customers the ability to use the AES 256 conventional standard and the NIST shortlisted quantum resistant algorithms.

> “The remarkable flexibility of the product is a big plus for us. We're able to redeploy these systems on other connections should our topology change, and we can also extend the licensed bandwidth as the usage grows. This is a huge benefit as we'll not have to refresh our encryptors in the foreseeable future.”

SECURE NETWORK INFRASTRUCTURE
WITHOUT COMPROMISING PERFORMANCE

Senetas CypherNET encryptors are used globally by government, defence, enterprise and service provider organisations to protect sensitive data transmitted over a range of data network protocols and all topologies.

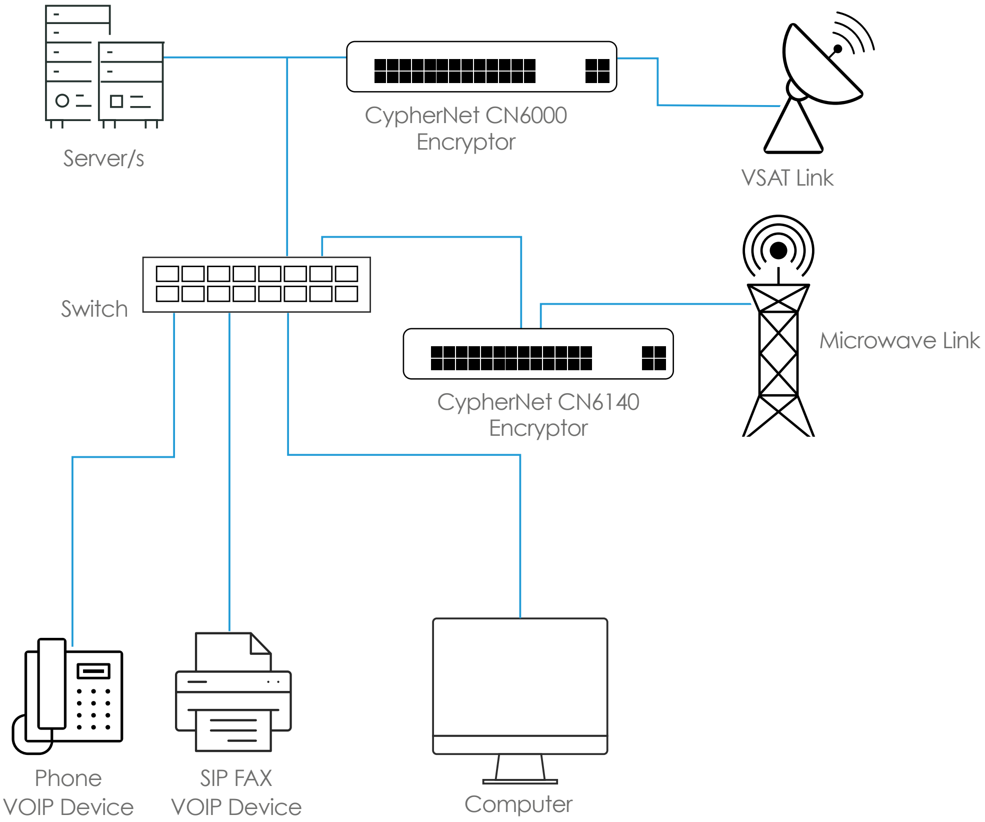
They are crypto-agile by design, offering ‘hybrid encryption’ security that features the best of todays conventional AES algorithms and the NIST shortlisted quantum resistant algorithms, providing long-term data protection in a post-quantum computing world.

Rigorously evaluated and certified by international cybersecurity testing agencies, CypherNET encryptors are approved to protect the most sensitive information: from government and defence secrets to financial transactions, healthcare data, intellectual property and all kinds of personally identifiable information.

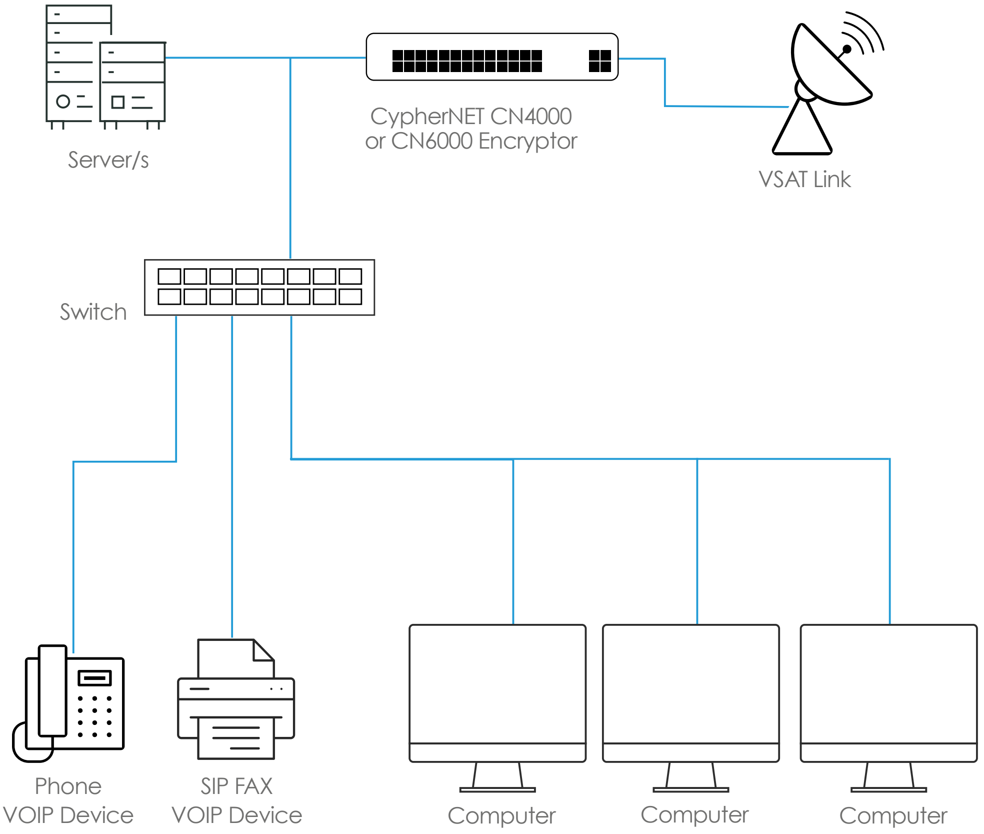
Providing maximum security without compromising network performance, the CypherNET range of encryptors offers flexible network security solutions for bandwidth speeds from modest 100Mbps to ultra-high speed 100Gbps. They range from compact ‘desktop’ format appliances to carrier-grade rack mounted and multi-port devices.

Network Independent Encryption	Supports Ethernet, Internet, VoIP, Transport Layer, Microwave, VSAT and SCADA network protocols
Near-Zero Latency	Maximum network performance
Minimal Data & Management Overhead	Lower total cost of ownership
Zero Data Impact	Optimal performance for jitter-free voice and video
High Assurance Data Protection	End-to-end encryption and state of the art key management
AES GCM Authenticated Encryption	Data protection plus network ingress prevention security
Hybrid Encryption	Conventional AES and MIST shortlisted quantum resistant algorithms
Transec Transmission Flow Security	Protects against traffic flow analysis

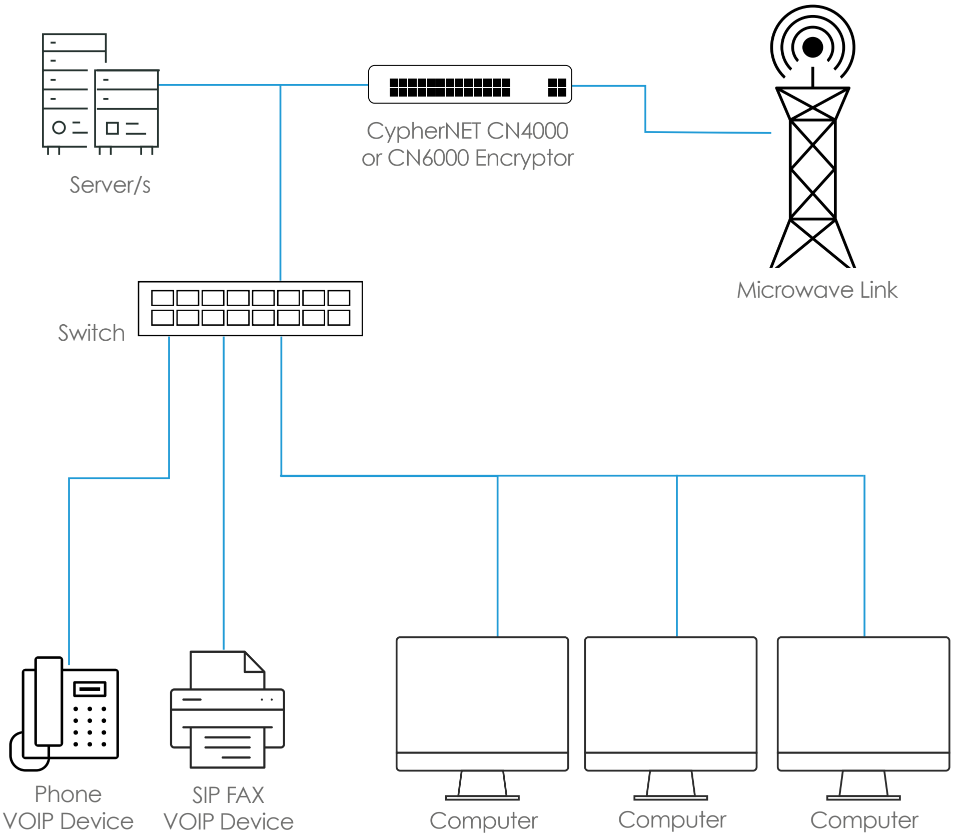
MULTI LINK ARCHITECTURE



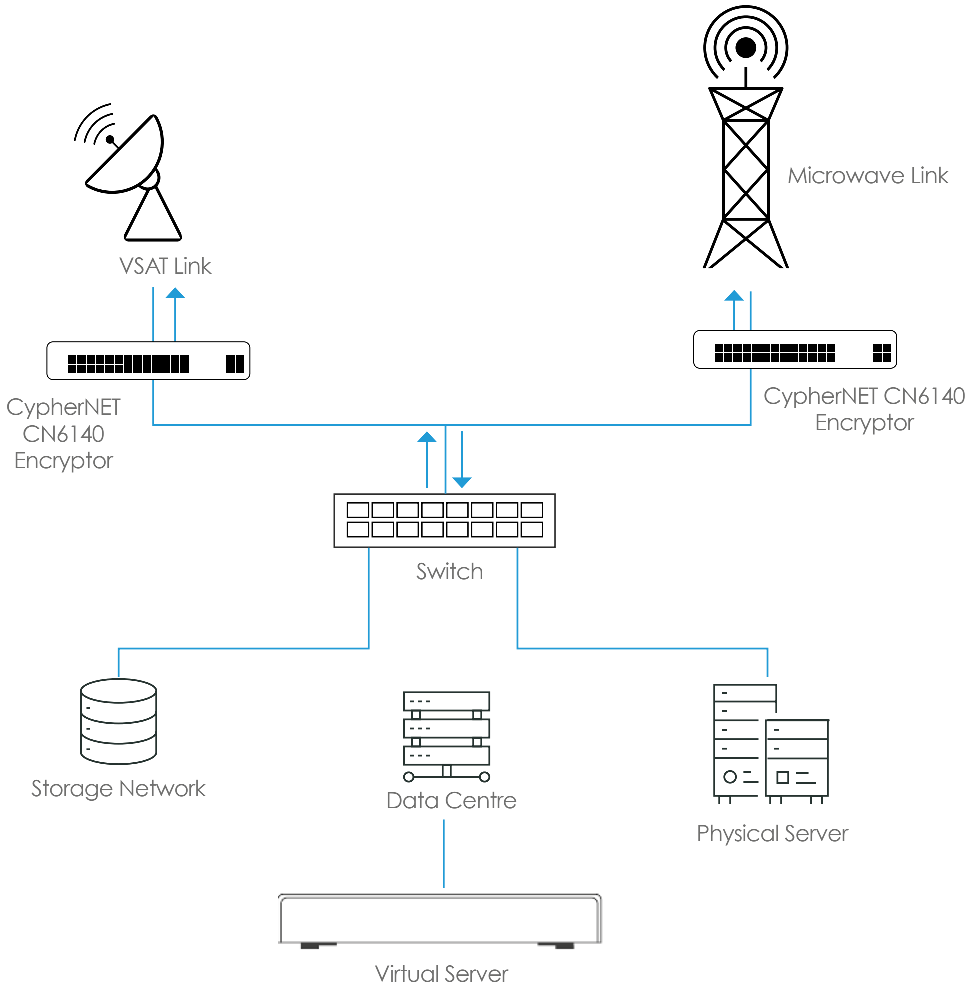
SINGLE VSAT LINK ARCHITECTURE



MICROWAVE LINK ARCHITECTURE



CENTRAL LOCATION HUB NETWORK



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:** infoemea@senetas.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