SENETAS

Security without compromise

END-TO-END ENCRYPTION SOLUTIONS

SECURING DEFENCE INDUSTRY DATA

SOLUTION PAPER

The defence industry has become dependent upon the fixed, high-speed data networks that serve as its core network infrastructure; providing Big Data, Cloud, SaaS and other digital transformation technologies.

These critical technologies and applications generate huge volumes of data that is often transmitted across Wide Area and Metro Area Networks. This data in motion is often over-looked when it comes to cyber-security planning; it is therefore, exposed to a variety of cyber-threats, the most serious of which are the loss on intellectual property and defence secrets.

Across the world, defence industry organisations are required to comply with a wide variety of cyber-security regulations. Adherence to these standards, whether independent or business/department specific are generally a prerequisite to operate within the sector and with Government defence departments.

However, private and public-sector organisations operating within the defence sector 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 for the past five years, research repeatedly highlights that these risks are underestimated.

This is often because of a presumption that fibre-optics used in core network infrastructure, such as high-speed Ethernet networks, are inherently 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 protecting core data networks, the risk is even greater. The vulnerabilities present in major vendors' network devices (such as routers and switches) place an addition 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.

Data network managers are also under pressure to ensure maximum network uptime and meet application performance requirements.

In addition to the disruption caused by keeping up with network and device security patches, they must meet the business requirements of their networks. These are often conflicting objectives that may expose systems to the risk of data breaches.

Ultimately, no organisation should depend on data network devices for effective data security; nor should they depend upon low-assurance network devices with embedded encryption. These face similar security and operational weaknesses.

To achieve both maximum encryption security and network performance objectives, core Ethernet network data must be protected by high-assurance, dedicated hardware encryptors.

WHY ENCRYPT SENSITIVE NETWORK DATA

The need to protect government and defence organisations' data within their internal systems is self evident. However, the need to protect their transmitted network data has not been so obvious.

As organisations increasingly adopt Cloud, SaaS and data centre technologies, the risks to core Ethernet network infrastructure have increased significantly.

Leading data security organisations highlight that many organisations do not sufficiently protect network data once outside their direct control.

Who really knows what happens to their data while it is being transmitted to another location?

If nothing else, the vast number of recorded data network breaches in recent years highlight the importance of protecting the data itself.

The defence industry is a special case because it not only faces risks to intellectual property, privacy and business secrets, like other commercial organisations, but it also exposes government defence departments and defence forces to issues of national security.

The last line of defence for any data is encryption. Only the best encryption solutions ensure that successfully breached data is useless in unauthorised hands.

Encrypting Data in Motion

In recent times, the swift growth of mobile working and an increasingly complex international data protection landscape has emphasized the need to protect data in transit.

Data travelling through networks is not just exposed to an increased risk of cyber-attack; there is a genuine risk of human error and equipment failings that can manifest more often than you would think.

However, these risks can be eliminated – and security assured - by automatically encrypting network data (including voice and video) while it's in motion.

Data security advisors highlight that almost all network data should be encrypted. They argue that in large volumes even low value data, when aggregated, can be useful to cyber-criminals and any network breach has the potential to be harmful to reputations and stakeholders' trust.

Security Without Compromise

In the past, data encryption came at the expense of network performance, due to excessive latency and encryption overheads.

Senetas encryptors provide maximum network performance and maximum data protection; featuring ultra-low latency, zero network overhead and zero impact on other network devices.

Typically, data networks used to transmit information are known as Layer 3, but when you encrypt Layer 3 networks, it comes at a serious cost of 50% to 70% of network performance.

On the other hand, Layer 2 networks do not suffer the same lost performance. They are used when high data volumes and performance needs demand more bandwidth and improved cost efficiency, together with best practice data security.

Notable breaches

Over recent years government and defence organizations have suffered escalating cyber attacks from hostile states.

In 2020 there were a record number of security breaches at the UK's Ministry of Defence, totalling 151 reported incidents, particularly where data was transferred between the MoD and its private sector partners. Incidents included many cases of classified information being shared via personal email accounts, as well as misconfigured infrastructure and compromised IT Systems.

The SolarWinds hack in December 2020 exposed numerous US intelligence agencies and departments, including the Pentagon, when an infected software update was used as a trojan horse by suspected Russian hackers.

In May 2021, it was revealed that Chinese hackers had used spear phishing to target Russia's largest submarine design bureau, attempting to steal schematics and logistical plans.

CERTIFIED HIGH-ASSURANCE NETWORK ENCRYPTION SECURITY

The best network security solutions for government and defence applications require both high performance data networks and certified high-assurance encryption. Not all encryption solutions are created equal. Multi-function 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 encryptors 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.

There are four essential capabilities necessary for high-assurance network data encryption:

- Dedicated, secure and tamper proof hardware
- Automatic, 'zero-touch' encryption key management
- Authenticated, end-to-end network encryption
- Robust, standards-based encryption algorithms

Certification. Your Assurance, Our Commitment

Senetas customers are assured of our encryptors' performance by the certifications provided by the leading testing authorities (FIPS, NATO, Common Criteria).

Certification involves years of rigorous testing by the testing authorities' own labs. Without these certifications, products are unable to be installed in the respective government data networks.

In addition to our encryptors' certifications, government and defence customers have also undertaken their own proof of concept and benchmarking testing. In every case, Senetas encryptors have excelled.

Importantly, organisations providing services to the government and defence sectors – such as Cloud computing or data centre storage services – can meet the certification requirements of their own government customers by using Senetas certified high-assurance products.

That's why Senetas encryptors secure much of the world's most sensitive data.

END-TO-END ENCRYPTION SOLUTIONS

CN Series Encryption Hardware

The CN Series of Ethernet encryptors provide certified, high-assurance data protection for core IT and communications network infrastructure.

All CN Series encryptors share a common encryption platform and are 100% compatible and interoperable.

CN Series hardware is used to secure sensitive data in motion across networks operating at anything from modest 10Mbps to ultra-fast 100Gbps bandwidths.

CN4000

Small form-factor (desktop) encryptors for 'in the field' network link security (e.g. CCTV) – offering 10Mbps, 100Mbps and 1Gbps bandwidth speeds.

CN6000

Rack-mounted high speed encryptors for business-critical applications – offering 1Gbps to 10Gbps bandwidth speeds.

CN9000

Ultra-high bandwidth, rack-mounted encryptor with "mega-data" performance – offering speeds of up to 100Gbps.

CV Series Virtualised Encryption

The CV1000 virtual encryptor provides strong and effective data encryption for large-scale and virtualised wide-area networks.

Scalable to thousands of end-points, the CV series of virtual encryptors is a software application of the trusted Senetas encryption platform. It delivers cost-effective, transport Layer agnostic data protection at up to 15Gbps (with DPDK).

As a Virtualised Network Function (VNF) that will run on any x86 hardware, the CV Series virtual encryptor is 100% interoperable with Senetas CN Series hardware encryptors and is built on FIPS compliant technology.

SureDrop Encrypted File Sharing and Collaboration

SureDrop delivers the file-sharing convenience of popular box-style applications, but with the addition of end-to-end encryption security and 100% data location control.

It also offers users a choice of the resilience of a bespoke, on-premises solution or the flexibility of a managed service provider solution.

SureDrop clients include government agencies and service providers that are concerned about the inherent risks associated with sharing documents outside of their protected LAN.

SureDrop represents a new way to enjoy secure file sharing; with the emphasis on delivering a service that meets the needs of large commercial and government organisations who are required to frequently share sensitive and confidential information across the web.

SureDrop also provides organisations with the user-authentication security benefits of active directory compatibility.

Votiro Secure File Gateway

VOTIRO

Votiro Secure File Gateway leverages patented, next generation anti-malware technology to proactively protect your files from the most advanced, persistent cyber-attacks.

It sanitises incoming, shared and stored files, enterprise-wide; eliminating the risks associated with both known and zero-day, or undisclosed, attacks. At the same time, it preserves 100% of original file content and functionality, without disrupting user workflows.

WHAT MAKES SENETAS STAND OUT?

Best Performance

High-speed

The designed-in, market-leading performance capabilities of Senetas encryption solutions are what make them stand out from the crowd.

Whether operating at 10Mbps, 100Mbps, 1Gbps, 10Gbps or 100Gbps; time after time, they consistently win competitive performance tests.

Their encryption speeds, near-zero data overhead and near-zero latency make Senetas encryption solutions ideally suited to the most demanding network environments.

Ultra-low latency

Senetas high-speed encryption solutions operate in full duplex mode at full line speed 99.99% without loss of packets.

Latency is not affected by packet size (<2 microseconds per unit at 100Gbps) meaning maximum throughput with near zero protocol overhead.

Importantly, by using Field Programmable Gate Array (FPGA) technology, this outstanding performance is predictable and dependable.

Zero impact

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

They simply fit in within the user network. They don't require changes to other devices or network reorganisation; making them a favourite among network engineers.

High-Assurance

Certification in-depth

Senetas CN Series encryptors include the only multi-certified products of their types, as a result they are trusted by governments and defence forces around the world.

Rigorous testing is carried out over many years and provides our government and commercial customers with maximum confidence. Senetas CN Series encryption solutions are certified by: FIPS, Common Criteria and NATO.

For over 20 years, Senetas R&D has included a commitment to 'certification in depth'. Customers value the benefits of exhaustive and ongoing testing authorities' product evaluation.

Best encryption key management

All Senetas products adopt state-of-the-art encryption key management. Your encryption keys are only ever held by and accessible to you, on your premises; securely stored and encrypted.

Solution integrity

Senetas encryptors provide maximum solution integrity; unlike 'low assurance' solutions, such as router-based network data encryption or multi-function devices with embedded encryption.

Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption with standards-based (AES256) encryption algorithms.

Versatile & Simple

Crypto-agility

All Senetas encryption solutions are agile by design; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

Selected Senetas encryptors also support Quantum Key Distribution (Quantum Cryptography) and Quantum Random Number Generation, for long-term data security.

Support for all topologies

Senetas CN series encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies. Senetas CN9000 encryptors are the only 100Gbps encryptors that support multipoint-to-multipoint topologies.

Custom encryption

In addition to the standards-based AES256 and 128-bit algorithms, Senetas CN series encryptors support the use of customer-requested algorithms, custom curves (BYOC) and entropy (BYOE).

Ease of use

Set and forget simplicity and network transparency are underlying Senetas design themes. They ensure ease of implementation, operation and management. All Senetas encryption solutions feature automatic zero-touch key management. They also feature automatic network discovery and connection.

Local or centralised management

Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software; which acts as the Certificate Authority in a network of encryptors by signing and distributing X.509 certificates.

Low Cost, High Efficiency

Suitability

All Senetas CN Series solutions operate at full line speed; enable maximum network performance and deliver 'set and forget' management simplicity.

The business investment case out-performs even 'cheap and cheerful' low-assurance solutions that prove very costly over time.

It is not necessary, nor beneficial, to opt for low-cost, low-assurance solutions to meet the toughest business case and TCO requirements.

Cost-efficiency

Senetas encryption solutions provide excellent TCO through a mix of network bandwidth savings, ease of management and reliability.

Longevity, interoperability, backward compatibility, minimal installation and management costs and solution flexibility all contribute to a rapid ROI.

Other cost benefits include, low power consumption minimal rack space use and combined rack space/ power utilisation efficiency.

Reliability

All Senetas hardware encryption solutions boast 99.999% uptime. Carrier-grade, rack mounted devices are hot-swappable and provide further network operations uptime benefits thanks to dual redundancy of consumables, such as fans and power supplies.

Flexibility

The use of FPGA technology enables maximum operational flexibility. This enables on-going operational simplicity, such as infield upgradability, as customers' requirements change; helping to protect their investment in technology.

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 CN and CV Series encryption solutions are sold by Thales as part of its Cloud Protection and Licensing portfolio.

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 10Mbps to 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