END-TO-END ENCRYPTION SOLUTIONS: SECURING CRITICAL NATIONAL INFRASTRUCTURE

SENETAS

Security without compromise

Critical national infrastructure

Critical National Infrastructure may be defined as "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life depends".

National Infrastructure is typically divided into 9 categories: communications, emergency services, energy, financial services, food, government, health, transport and water. Assets within these categories are measured against a criticality scale and assigned a status based on the severity of impact.

The threat landscape is constantly evolving, with potential harm originating from terrorist attack, rogue states, hackers and organised crime, the implications of the growing threat to Critical National Infrastructure are wide ranging.

Loss or corruption of data would have an obvious negative impact on financial and operational performance for the organisation suffering the breach. However, of greater concern would be the potential impact on the security or supply of critical utilities and the broader implications for national security and public safety.

Supervisory Control and Data Acquisition (SCADA) Networks

Supervisory Control and Data Acquisition (SCADA) networks are used to carry command data that ensures the safe and reliable operation of a nation's critical infrastructure. Essential services such as electricity, natural gas, water, waste treatment and rail services all rely on SCADA networks.

Traditionally, SCADA networks have been isolated, and it has been high fences and barbed wire that has kept our critical infrastructure secure.

However, with the increased threat of cyber-attack, Governments and industry regulators around the world are focussing beyond physical perimeter protection to ensure the integrity of the systems used to control our critical infrastructure.

It is these controlling networks that represent the greatest vulnerability to utilities and infrastructure organisations, not only from the theft of sensitive data being transmitted across their networks, but also the consequences of disruption or manipulation of these data flows as part of a malicious attack.

Many SCADA systems are no longer isolated and are connected to public networks via the Internet.

Sometimes this is intentional, as a means of connecting to other systems, other times it can be an unintentional consequence of providing connectivity to remote locations or offices.

Globally, there are mandates from the highest levels of government requiring that SCADA networks and other critical infrastructures are secure.

In the UK, the Centre for the Protection of National Infrastructure (CPNI) provides advice on physical and cyber security, in the US, NERC (the organisation responsible for reliability standards for the nation's utility providers) has established a set of Critical Infrastructure Protection guidelines and in the EU, the European Programme for Critical Infrastructure Protection (ECPIP) provides a similar doctrine.

"Hackers are increasingly targeting electric, natural gas and other vital utilities; threatening a disaster of epic proportions that experts say firms are doing too little to guard against."

James W Sample, Ernst & Young

Why encrypt?

The rapid growth of virtualisation, data centre and cloud computing technologies mean we are becoming increasingly reliant on our high-speed/high-availability data networks to deliver information when and where we need it.

Cyber-crime in the form of hacking, corporate espionage and even cyber terrorism, is on the rise. Information security threats remain commonplace and there is an increasing emphasis on organisations of all types to ensure the integrity and security of their data, both at rest and in motion.

We cannot rely on the assumption that our data remains secure within the perimeter of the office environment. All organisations share systems and information that rely upon common network access and most modern businesses comprise multiple offices, some separated by a few yards, others by thousands of miles.

Fibre-optic cables are used to transport Petabytes of data across private and public networks every day. Although still considered the fastest and most reliable method of moving data, Fibre networks have become increasingly vulnerable as hacking technologies become more sophisticated, less expensive and more readily available.

Protection versus Prevention

There is a common misconception within many organisations that a robust firewall is enough to prevent unwanted access to their network. Unfortunately, this is not the case. Whilst the firewall can detect and eliminate a variety of penetration or denial of service attacks, it is no protection against a physical tap either inside or outside the firewall.

The only fail-safe solution to ensure that your data is secure as it travels across the network is encryption. Furthermore, your encryption solution should be de-coupled from any specific network architecture and accredited against recognised world-wide security standards.

Notable Breaches

As our critical infrastructure becomes more connected, it exposes legacy technologies to the outside world; leaving some vital systems open to exploitation.

In recent years, we have seen an increasing number of attacks on critical infrastructure. According to the Gemalto Breach Level Index, from 2017 to 2018, the industrial sector experienced the single largest increase in the number of breached data records.

In December 2015 the Ukraine fell victim to a spear phishing attack that compromised a SCADA system. This resulted in a massive power outage, affecting over 230,000 people.

In 2013 agents allegedly acting on behalf of a foreign state managed to access the command and control systems at the Rye Brook dam in New York state.

Throughout 2015 and 2016, a hacking group known as Lazarus targeted the SWIFT global bank messaging system and successfully stole millions of dollars from unsuspecting banks.

In 2017 a joint report from the FBI and Homeland Security in the US highlighted a number of cyber attacks on nuclear power stations across the country; including Wolf Creek in Kansas.

In another 2017 report, GCHQ in the UK announced that hackers were systematically targeting the UK energy sector.

In early 2018, the New York Times reported that a cyber-attack on a petrochemical plant in Saudi Arabia was intended to not only sabotage plant operations, but to cause an explosion that constituted a genuine threat to life.

Securing the IoT

The evolution of the Internet of Things (IoT) will see over 25 billion connected devices by 2020. From a cyber-criminal's perspective, this represents 25 billion possible system vulnerabilities.

Smart Grid Technology, where the SCADA network effectively extends all the way to the meter in the end-user's premises, is a case in point. A classic example of IoT in action, it poses some unique security challenges.

The Smart Grid is a sophisticated communications network where data is collected remotely, then collated and analysed centrally before control commands are issued.

If rogue data could be injected into the Smart Grid network and compromise the command and control systems, it could result in significant service disruption, economic damage or citizen harm.

End-to-End Encryption

Encryption is a key element in ensuring the security of SCADA networks. However, for encryption to be most effective it needs to deliver against four criteria: Speed, Scalability, Manageability and Affordability.

SCADA networks deal with real-time data, so any encryption technology needs to operate at full line speed and add minimal latency.

Scalability is essential as the nature of a SCADA network means that different bandwidths are in operation at different points in the network.

Encryption solutions should offer strong and effective data protection but should also be simple at the point of use. Centralised management allows users to configure and deploy new devices across the network.

Affordability is another key consideration when it comes to retrospectively securing SCADA networks. Encryption should be viewed in terms of TCO and ROI, not capital expenditure.

High-Assurance hardware encryption for core IT and communications infrastructure

With enterprise, government, defence and 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. Designed and built to protect core IT network infrastructure; CN Series encryptors deliver security without compromising on network and application performance.

Strong and effective virtualised encryption for extended & virtualised WAN

In a world dominated by distributed WAN, virtualisation and borderless infrastructure; the need for high-performance virtualised encryption security is growing.

These extended networks and virtualised environments, beyond the core Ethernet network infrastructure, typically operate at speeds of 1Gbps or less.

The Senetas CV Series of virtualised encryption appliances delivers strong and effective encryption security for data-in-motion across high-speed Carrier Ethernet WAN links at >1Gbps.

Instant scalability means the CV Series may be deployed rapidly across hundreds (thousands) of network links.

Choosing the right encryption solution

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.

When it comes to choosing an encryption vendor, it's important to consider all the possible applications. Just as important is the realisation that all encryption solutions are not created equal.

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 Layer 2 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 Ethernet 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, 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 Layer 2 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.

What makes Senetas encryptors stand out

Best Performance

High-speed

The designed-in, market-leading performance capabilities of Senetas encryptors 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 encryptors ideally suited to the most demanding network environments.

Ultra-Low Latency

Senetas high-speed encryptors operate in fullduplex mode at full line speed 99.99% without loss of packets.

Latency is not affected by packet size (<2 microseconds per unit at 10Gbps) 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

Because Senetas CN Series encryptors include the only multi-certified products of their types, 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 encryptors are certified by: FIPS, Common Criteria and NATO.

For 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 so called 'hybrid' encryptors.

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

* As surveyed in 2014 and 2015, Senetas hardware was on-site engineers' preferred hardware.

Versatile & Simple

Crypto-agility

All Senetas encryptors are 'crypto-agile'; 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 protocols

The Senetas CN range of encryptors provides the widest feature-set. Able to operate at 10Mbps to 100Gbps, they are designed for Layer 2 Carrier Ethernet WAN and MAN networks and support all Layer 2 protocols: Ethernet, Fibre Channel; SONET/SDH and LINK.

Support for all topologies

Senetas CN 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 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 encryptors feature automatic zero-touch key management. They also feature automatic network discovery and connection.

Interoperability

Senetas encryptors supporting the same Layer 2 network protocol are fully interoperable. All Senetas CN models are backward compatible.

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 encryptors 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 encryptors provide excellent total cost of ownership 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 return on investment.

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

Reliability

99.999% uptime and conform to international requirements for safety and environment.

All carrier-grade, rack mounted Senetas encryptors are hot-swappable and provide further network operations up-time benefits thanks to dual redundancy of encryptor consumables such as fans and power supplies.

Unlike hybrid encryptors and other low-assurance solutions, network up-time is not disrupted by Senetas encryptors.

Flexibility

Senetas encryptors' use of FPGA technology enables maximum operational flexibility.

They are better able to meet customers' specific requirements and provide an optimised highspeed data encryption solution.

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

International

Senetas CN Series hardware and CV Series virtual encryptors are distributed and supported internationally by Gemalto under its SafeNet brand.

US Federal Government

Senetas CN Series hardware and CV Series virtual encryptors are distributed and supported within the US Federal Government by SafeNet Assured Technologies.

Australia and New Zealand

ANZ Partner Community.

GLOBAL SUPPORT

Senetas CN Series hardware encryptors and CV Series virtual encryptors are distributed and supported internationally by Gemalto, under its SafeNet brand, and throughout Australia and New Zealand by Senetas and accredited partners.

Additionally, Senetas provides pre-sales technical support to accredited partners and their customers around the world.

GET IN TOUCH

Looking for a service provider to encrypt your high-speed network data? Contact Senetas and we'll help you find the right partner.

Senetas works with data network service providers across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers are free to contact Senetas directly to discuss their requirements; or a service provider may contact 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 provide support for all network topologies.

Our virtual encryptors support >1Gbps speeds and all topologies. Transport Independent Mode (Layers 2, 3 and 4) is also available; enabling multi-Layer, end-to-end network data encryption security.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

SECURE FILE SHARING

Based on the proven Senetas crypto-security platform, SureDrop is the most secure files sharing and synchronisation tool available.

SureDrop uniquely enables 100% file location control for data sovereignty protection. www.sure-drop.com

www.senetas.com

Senetas is a leading developer of encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider 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 Pacific Region	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia and New Zealand	**T:** +61 (03) 9868 4555	**E:** infoanz@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** info@senetas-europe.com
North and Central America	**T:** +1 949 436 0509	**E:** infousa@senetas.com

CNIDS-SP1018