

# PROTECTING CRITICAL NATIONAL INFRASTRUCTURE DATA NETWORKS

SOLUTION PAPER



# 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.

## Cyber-threats to critical national infrastructure

The growth of the global economy has been fuelled, in large part, by the extensive digitalisation of all aspects of commerce, industry and government. The resulting improvements in efficiency and connectivity have eliminated systemic silos and created a truly digital world.

However, ubiquitous connectivity also poses a threat to security. In the case of critical infrastructure, the traditionally isolated nature of command and control systems acted as an effective line of defence. In an IoT world, these physical defences no longer exist, exposing a range of sectors to emerging cyber threats.

In times of increasing geopolitical conflict, and growth in skilled and well-resourced cyber gangs, critical national infrastructure has become a primary target. Whether for financial gain or intent to do harm, attacks on critical national infrastructure have become an everyday reality.

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.

## Cryptographic and platform agility for all networks

As technology has evolved, communications networks have become increasingly complex. The use of multiple network protocols (types) is now commonplace, with more being demanded from public and private infrastructure alike - enabling cloud services, datacentre interconnect, and the delivery of critical data and applications to the network edge.

When it comes to protecting these multi-layer networks, and the data moving across them, it is essential to choose the right encryption technology.

For optimal protection, encryption security should be transparent to the network and support all modern network protocols and topologies. It will also need to be cryptographically and platform agile to meet these needs.

The very nature of critical infrastructure demands the use of high-assurance security: the use of standards-based, authenticated encryption, state-of-the-art encryption key management and dedicated, tamper-proof encryption hardware. Furthermore, FIPS, CC, NATO and ANSSI certification is preferred, if not mandated, because it provides assurance the solution is "suitable for government and defence use". Solutions that have met the rigorous requirements of these certification bodies are actively sought by security-conscious commercial and industrial entities..

## 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

### National Cybersecurity Regulations

In addition to specific national infrastructure regulations, national governments have implemented cybersecurity laws signifying the seriousness of cyber threats to national infrastructure.

In the US, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), was passed into law in March 2022. It requires defined national infrastructure companies (including financial services) to report cybersecurity incidents, such as malware/ransomware attacks, to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of discovery.

Within the EU, the Directive on Security of Network and Information Systems (NIS) calls for a "high common level of security" across member states, and the wide-ranging scope of the EU Security Union strategy acknowledges the need for industry-specific initiatives - including a drive to make critical infrastructure "more resilient against physical, cyber and hybrid threats". The intent here is to significantly tighten risk assessments, security and reporting requirements for organisations in critical infrastructure sectors.

In Asia, countries including Singapore, Japan and South Korea have all initiated increased security requirements within their critical infrastructure sectors.

# 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 decoupled 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 a significant increase in the number and complexity of cyberattacks targeting critical infrastructure. 2022 saw a 140% increase in attacks targeting industrial operations, with the impact felt across both information and operational technology systems.

In the US, according to the FBI, more than a third of reported ransomware attacks effected organisations within critical infrastructure sectors, with healthcare, manufacturing and financial services amongst the worst hit.

Some of the most notable attacks in recent years have targeted the energy and utilities infrastructure in countries across the world:

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.

In 2020, Israel's water systems were attacked several times, with the attacks designed to compromise the command and control systems of the nation's pumping stations, sewer systems, waste water plants and agricultural pumps.



# SECURING THE IOT

The exponential growth of the Internet of Things (IoT) has seen more and more devices become connected. In 2023, this digital universe comprises around 15 billion connected devices - a number that is expected to double to around 30 billion by the end of the decade.

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.

# CRITICAL INFRASTRUCTURE CASE STUDIES

**CypherNET encryptors are used by numerous critical infrastructure organisations to protect their networks and network data around the world, in industries from energy to healthcare.**

## Nuclear energy

Concerned about an evolving threat landscape, this UK energy supplier was looking to protect its core infrastructure and wider area networks against malware attacks. With critical infrastructure vulnerable to state-sponsored attacks and cyber-terrorism, it was also looking to ensure the integrity and authenticity of its operational data.

Given its multi-layer network infrastructure, it was essential that a single, unified encryption platform could be used to provide protection at Layers 2, 3 and 4, without impacting network performance.

High-assurance CypherNET CN6000 encryptors are used to secure the core network links, operating at 1Gbps. Distributed SCADA control links are secured using CypherNET CN4000 encryptors, operating between 100Mbps and 1Gbps.

## Defence manufacturing

The defence industry is a high-value target for cyber attackers. This global enterprise manufactures a range of critical products for its defence agency customers and was looking to protect its sensitive data and intellectual property against emerging cyber threats.

Part of the defence network supply chain, it was essential that any encryption solution met the exacting requirements of US FIPS Level 3 security certification.

Security could not come at the expense of performance or convenience. Near zero latency and low network overhead was a must, as was in-field upgradability and centralised encryptor management.

Significantly, this customer also required cryptographic agility to future proof the solution against tomorrow's Quantum computing threats. This was necessary to meet the US government's mandate for future quantum resilience.

CypherNET CN6000 encryptors are used to protect data in motion across networks that span two continents and operate at speeds from 1Gbps to 10Gbps. These high-assurance devices are certified to FIPS Level 3 standards and operate in a mix of point-to-point and fully meshed networks.

## Rail transport

Australian state government owned-and-operated, this rail network operations company was looking to not only protect sensitive customer and business data, but also operational SCADA links. They needed both data protection and data network integrity security, preventing ingress of malware that would interfere with rail operations.

The distributed nature of the rail network meant extending data encryption security all the way to the edge of the multi-point network infrastructure. However, the rail operator was insistent upon one solution for all topologies and protocols.

Core links, operating at 10Gbps, were protected using CypherNET CN6000 encryptors. Compact, 'desktop' CypherNET CN4000 encryptors were chosen for locations at the edge of the network without server rooms. All CypherNET hardware encryptors are fully interoperable and are simple to deploy and manage.



## Oil extraction

Like all energy industry customers, this customer required maximum security protection against cyber-attacks on its oil drilling, exploration, and business operations. One of the largest oil companies in Asia, it had adopted a maximum cybersecurity policy stance.

This customer was looking to protect oil rig data control network links from both data loss and ingress of malware (data integrity). Fully authenticated encryption was required to support mixed network protocols and topologies. However, encryption security could not come at the expense of network performance, so low overhead and low latency were a prerequisite.

CypherNET encryptors were chosen because of their policy-based, network independence. Their ability to support Layer 2, 3 and 4 protocols meant the customer was able to protect both data and control (SCADA) links.

The deployment comprises CypherNET CN6000 and CN4000 encryptors, operating in a hub-and-spoke architecture.

## Air traffic control

Command and control systems, like air traffic control, are high-profile targets for cyber-attack. Bad actors from state-sponsored hacking groups to cyber-terrorists could interrupt operations, with potentially catastrophic consequences.

Early investigation of encryption alternatives highlighted a number of complexities and vulnerabilities arising from the embedded MPLS network architecture. It was initially assumed that the mix of network protocols (Layer 2, 3 and 4) would require multiple solutions, which would add a significant management burden and potentially introduce further points of vulnerability.

Following a successful PoC, CypherNET encryptors were selected as they met every criterion on the customer's "wish list":

- A single solution for all network topologies and protocols
- Maximum security, certified to Europe's Common Criteria EAL4+ and ANSSI standards
- Low latency and encryption overhead to preserve network bandwidth and performance

A single, dedicated hardware solution, CypherNET encryptors are used to ensure not just confidentiality, but integrity and authenticity of critical operations data.

## Law enforcement

Senetas CypherNET encryptors are used by law enforcement agencies across the US, UK, Australia, and the Middle East. They are used in a wide range of applications, from HD CCTV networks to in-field communications and general network data protection.

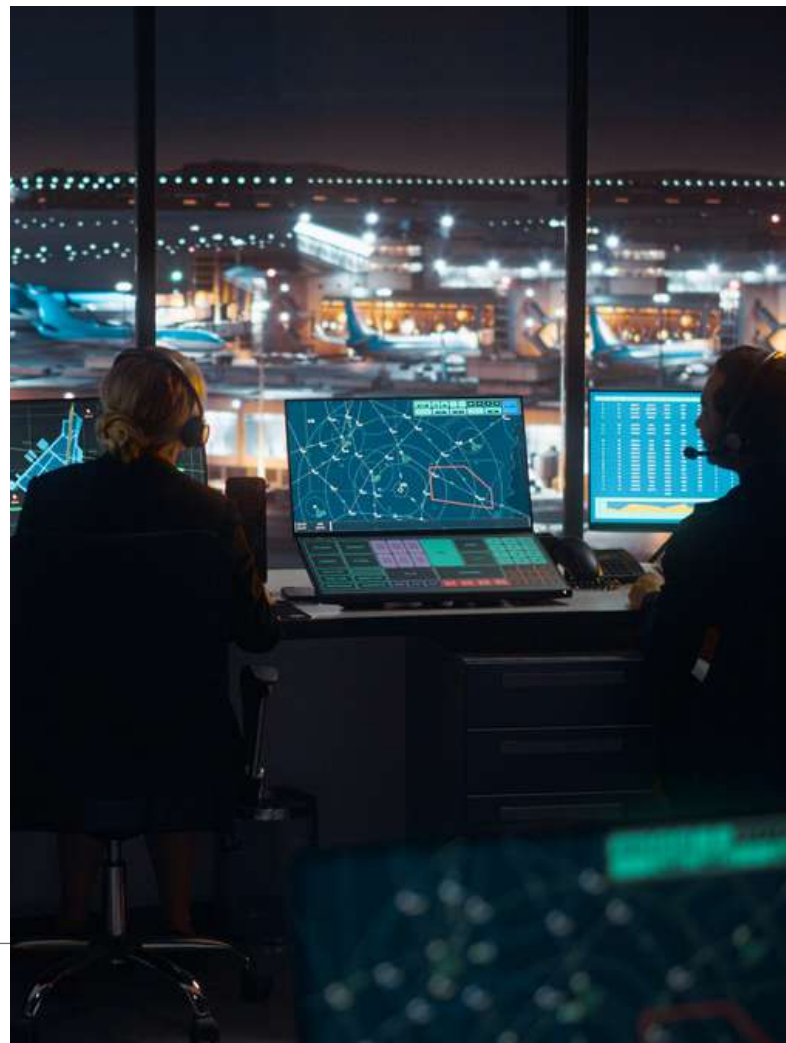
Whilst the applications (and the network protocols and topologies) vary, they share many common requirements – maximum security with minimal impact on network performance, interoperability, and ease of management.

Senetas' law enforcement customers include national security agencies, blue light services, and national border forces. Data confidentiality and integrity are paramount to these customers and cybersecurity certification is typically mandated.

CypherNET encryptors are manufactured to meet multiple certification standards, including:

- FIPS Level 3 (USA)
- Common Criteria EAL 4+ (International)
- NATO
- ANSSI.

From a security perspective these customers seek state-of-the-art encryption key management and security. Cryptographic agility has been a key factor to some law enforcement customers, so that the solution they buy today will protect against threats tomorrow, e.g. Quantum computing. They are aware their data is typically 'long life' demanding long-term protection.





# 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.

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, the Senetas CypherNET series of hardware 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 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 a 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 a 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.

In addition to our hardware encryptors, the CypherNET range include the CV series of virtual encryption appliances, which provide concurrent, multi-layer encryption at up to 15Gbps. Scalable to support thousands of endpoints, the CV series is suitable for wide area network applications, delivering high-performance encryption security all the way to the network edge.



# COMBINING HARDWARE AND VIRTUALISED ENCRYPTION

The choice between hardware and virtualised encryption is based on an organisation's individual needs and preferences. Often, it is not a case of 'either/or' – but a blend of the two technologies together.

## Security versus performance and network link use

Hardware encryptors deliver predetermined high-performance, not able to be matched by software/virtualised encryption. They also provide maximum data security through multi-certified, high-assurance credentials.

## Network link use cases

High-speed links (>10Gbps) are more commonly used to connect IT infrastructure such as data centre interconnects, or Big Data feeds.

Encrypting data in motion between branch locations is of equal importance, though network speeds will vary between these locations.

These links ideally require both maximum data protection and best performance, only offered by hardware encryptors.

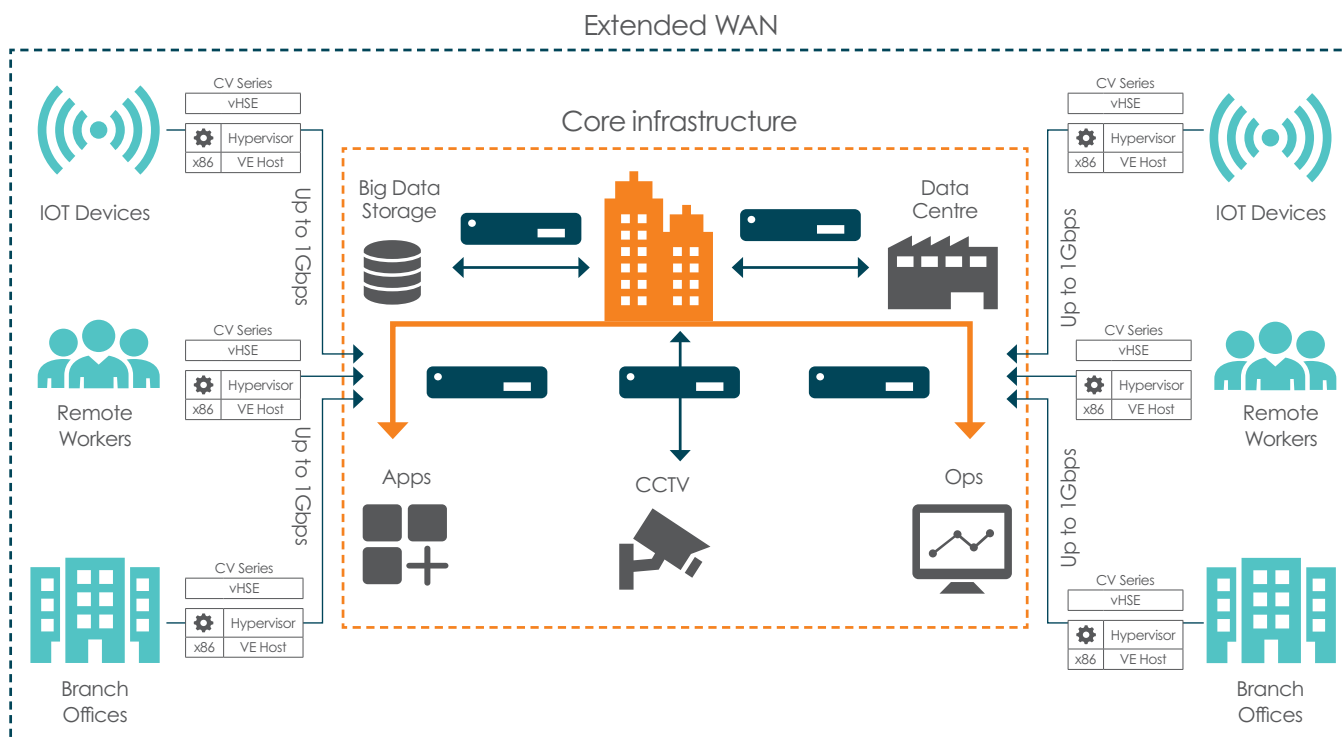
However, for extended WAN links and high-scale virtualised links that typically run at 10Gbps or less, a virtual encryptor is likely to be a more flexible and cost-effective solution.

## Mixed use cases






Organisations often only deploy hardware encryption to protect core IT infrastructure data in motion. Many operate unprotected extended WAN links.

Virtualised encryption provides an opportunity to encrypt all data in motion through a single compatible technology.

Ultimately, organisations should utilise dedicated hardware encryption for their main feeds, interconnects and branch locations, while virtualised encryption is used to provide scalable, cost-effective encryption for devices at the network edge.



# WHY CHOOSE CYPHERNET ENCRYPTORS?

 <p><b>Performance</b></p>	<p><b>High Speed</b> Market-leading performance. Operating anywhere from 10Mbps or 100Gbps, Senetas encryptors consistently win competitive performance test.</p>	<p><b>Low Latency</b> Operating in full duplex mode, at full line speed, without packet loss. Latency is as low as 2 microseconds per unit at 100Gbps.</p>	<p><b>Zero Impact</b> The zero impact of Senetas encryptors is not limited to network bandwidth and latency; it extends to network operations and management.</p>
 <p><b>Security</b></p>	<p><b>Certification</b> For over 20 years, Senetas R&amp;D has remained committed to the principle of certification in depth. Senetas CypherNET CN Series encryptors are certified by: FIPS, Common Criteria, ANSSI and NATO.</p>	<p><b>Key Management</b> All CypherNET encryptors feature state-of-the-art encryption key management. Keys are securely stored and encrypted, and only accessible by you.</p>	<p><b>Solution Integrity</b> Senetas high-assurance encryption solutions feature dedicated, tamper-proof hardware and provide gapless, end-to-end, authenticated encryption.</p>
 <p><b>Versatility</b></p>	<p><b>Crypto Agility</b> All Senetas CypherNET encryptors are 'crypto-agile'; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.</p>	<p><b>Topology Support</b> Senetas CypherNET CN encryptors operate in point-to-point, point-to-multipoint and fully meshed network topologies.</p>	<p><b>Flexible Management</b> Configuration may be performed locally or remotely through the intuitive Senetas CM7 management software.</p>
 <p><b>Efficiency</b></p>	<p><b>Cost Effectiveness</b> Senetas CypherNET CN series encryptors provide excellent TCO through a mix of network bandwidth savings, ease of management and longevity.</p>	<p><b>Reliability</b> All carrier-grade CypherNET CN series encryptors are hot-swappable, feature dual redundancy and deliver 99.999% uptime.</p>	<p><b>Flexibility</b> Use of FPGA technology enables maximum operational flexibility, including use of custom encryption and in-field upgradability.</p>
 <p><b>Innovation</b></p>	<p><b>Network Independence</b> Advanced, network layer agnostic encryption technology enables concurrent, destination policy-based, multi-layer encryption (Layer 2,3 and 4).</p>	<p><b>In-Field Operations</b> As the IoT brings critical data all the way to the network edge, Senetas is providing high-performance encryption in ruggedised forms for use in remote and hostile environments.</p>	<p><b>Quantum Resilient</b> Senetas is already providing "hybrid" encryption, incorporating the best of today's proven technologies with tomorrow's quantum-resilient encryption algorithms.</p>



# SENETAS CYBERSECURITY SOLUTIONS AT A GLANCE

## CypherNET network encryption

Senetas CypherNET encryption solutions provide high-performance, crypto-agile network data protection. Our range of hardware and virtualised encryption solutions leverage end-to-end encryption and state of the art encryption key management to provide long-term data protection, without compromising network performance or user experience.

Our **CypherNET CN series** of hardware encryptors provides high-assurance data protection in an uncertain world. Delivering exceptional performance and near zero latency, the CN series supports networks operating at anywhere from 10Mbps to 100Gbps.

**CN9000** – ultra-fast, 100Gbps devices for core network infrastructure

**CN6000** – rack-mounted, carrier grade devices for high-speed networks

**CN4000** – compact devices, delivering security to the network edge

Our **CypherNET CV series**, virtualised encryption, is a software application of our trust high-assurance hardware devices. Scalable to thousands of endpoints, it provides cost-effective, policy-based, multi-layer data protection at up to 15Gbps.

## SureDrop encrypted filesharing

The file sharing, storage and collaboration marketplace is crowded with applications promising to deliver on the potential of a 'work anywhere, with anyone', culture. However, not all of them offer a level of security suitable for maximum data protection.

SureDrop is different. Simple to use, it is also secure by design. It features strong encryption and data sovereignty control, without impacting on usability. It is designed for organisations that have embraced remote working, but who also take security seriously.

Offering high-performance and high-availability, SureDrop offers flexible deployment: on-premises or in the cloud. It boasts compatibility with a broad range of enterprise software integrations and supports all file types, sizes, and formats. For added peace of mind, it also provides 100% control over file storage location, ensuring transparency and data sovereignty.

## Votiro ZT Cloud

Votiro ZT Cloud is a Layer 7, Open API-based service that integrates seamlessly with your existing IT and Security platforms. Deliver safe content via email, web browser, portal uploads, file transfers, cloud apps, content collaboration platforms, and more.

Votiro ZT Cloud leverages patented, next gen CDR 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 not just with known threats, but with undisclosed cyberattacks and zero-day exploits. At the same time, it preserves 100% of original file content and functionality, without disrupting user workflows.

With Votiro ZT Cloud you can detect and disarm malware and ransomware borne by content coming into your organisation. Detailed analytics provide insight into your threat, privacy, and compliance landscapes. Finally, Votiro ZT Cloud can significantly reduce the workload for you SOC, data security, and IT teams.

## 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](http://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: <a href="mailto:infoasia@senetas.com">infoasia@senetas.com</a>
Australia & New Zealand	T: +61 (03) 9868 4555	E: <a href="mailto:info@senetas.com">info@senetas.com</a>
Europe, Middle East & Africa	T: +44 (0)1256 345 599	E: <a href="mailto:infoemea@senetas.com">infoemea@senetas.com</a>
The Americas	T: +1 949 436 0509	E: <a href="mailto:infousa@senetas.com">infousa@senetas.com</a>

## 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 ZT Cloud extension.

## DISARM MALICIOUS CONTENT

Votiro ZT Cloud 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** 