
SENETAS
Security without compromise
SECURING HI-TECH INDUSTRY DATA
SOLUTION PAPER

A FROM CYBER THREAT TO CYBER WARFARE

All high-tech and critical national infrastructure industry sectors are high value targets for cyber-criminals, rogue states and other bad actors. Whatever the intent - financial gain, theft of high-tech intellectual property or business disruption – these industries' IT systems are subject to multiple attack vectors, where vulnerabilities may be maliciously exploited.

The rapidly growing space industry is a standout example because it is both high-tech and part of our critical national infrastructure. All types of bad actors may have the space industry in their sights.

Space industry cyber-threats are more wide-ranging than data breaches, loss of IP and malware attacks. The industry faces threats of a more catastrophic nature, with attacks designed to vandalise, or take control of and cripple, space-based critical national infrastructure such as satellite communications. The sophisticated nature of bad actors, and their nefarious motives, are changing the game from cyber-crime to cyber-warfare.

An evolving threat landscape

The threat landscape for the space industry is diverse, spanning everything from general business applications to launch control systems, ground assets and orbital communications and operations. The potential for harm is as varied as it is real.

Space industry infrastructure, satellites, ground stations and data links at national, regional and international levels play a key role running a country's infrastructure; from telecommunications to transport (shipping, air and road), trade and financial services. Weather forecasting, environmental monitoring and defence systems also depend on the space industry.

Moreover, the space industry itself is a growing part of a nation's exports and international technology and security relationships.

The space industry faces a battle on three primary fronts: breaches where confidential data is stolen; network ingress where control systems are breached and attacks where malicious content is deployed.

Day to day business activities, including research & development, command and control, and even simple file-sharing and collaboration, are all data dependent. It is here that vulnerabilities lie.

Using data networks to transmit sensitive data (from intellectual property to launch codes and satellite communications) provides high-value opportunities for cyber-criminals. They are equally exposed to data theft, data injection or attacks that deploy malicious content to infiltrate targeted systems.

Space organisations are an increasingly attractive target due to the rich rewards and/or serious harm bad actors can achieve with relative ease. Business transforming technologies, including cloud and IoT systems, are dependent on public and private networks, but these are rarely encrypted. Hence, eavesdropping and other breaches of unencrypted data are not uncommon.

With the increased use of network dependent technologies, space organisations face an evolving threat landscape, making cybersecurity increasingly important. In this case, the only answer is to ensure network data is encrypted using high-assurance, crypto-agile solutions. These are tried and tested and are the first choice of defence and military organisations the world over. There is no excuse for breaches of unencrypted data.

Day-to-day business activities such as file-sharing, work-group collaboration and use of email expose organisations to potentially catastrophic infiltration of undetected malware/ransomware and other malicious content attacks. All file types can be carriers of malicious content and once released little can be done – whether the malicious content is known, unknown or a zero-day attack. These attacks are often so effective that firewalls fail to detect and prevent the threat.

Where there's data, there's value

The global technology marketplace continues to see strong growth, with the top 200 tech companies (according to Forbes Global 2000 list) having a market value in excess of US$9 trillion. This includes several space organisations, making them high-risk targets.

High-speed data networks may yield terabytes of data in a matter of minutes. By intercepting this data, cyber-criminals improve their odds of stealing sensitive information or using it to gain systems access; including command and control systems used in space operations. Should this happen in the space industry, the stakes would be very high indeed.

According to Goldman Sachs, the global space industry (currently valued at US$360 billion) could be worth US$1 trillion by the 2040s. Alongside significant government funding from the US, Europe, China, India and Russia, the market has seen large private investments. Satellite revenues have doubled in ten years; with major players like Airbus, Boeing, Thales and Mitsubishi contributing to a commercial market value in excess of $250billion.

The Australian government is also involved. The Australian Space Agency has announced it is joining forces with NASA, spending $150 million over five years that will see the collaboration supporting exploration missions to Mars and the Moon.

However, as these opportunities grow, the space industry is increasingly exposed to cyber-threats. There can be no doubt that the industry's growth is attracting the attention of a broadening mix of bad actors.

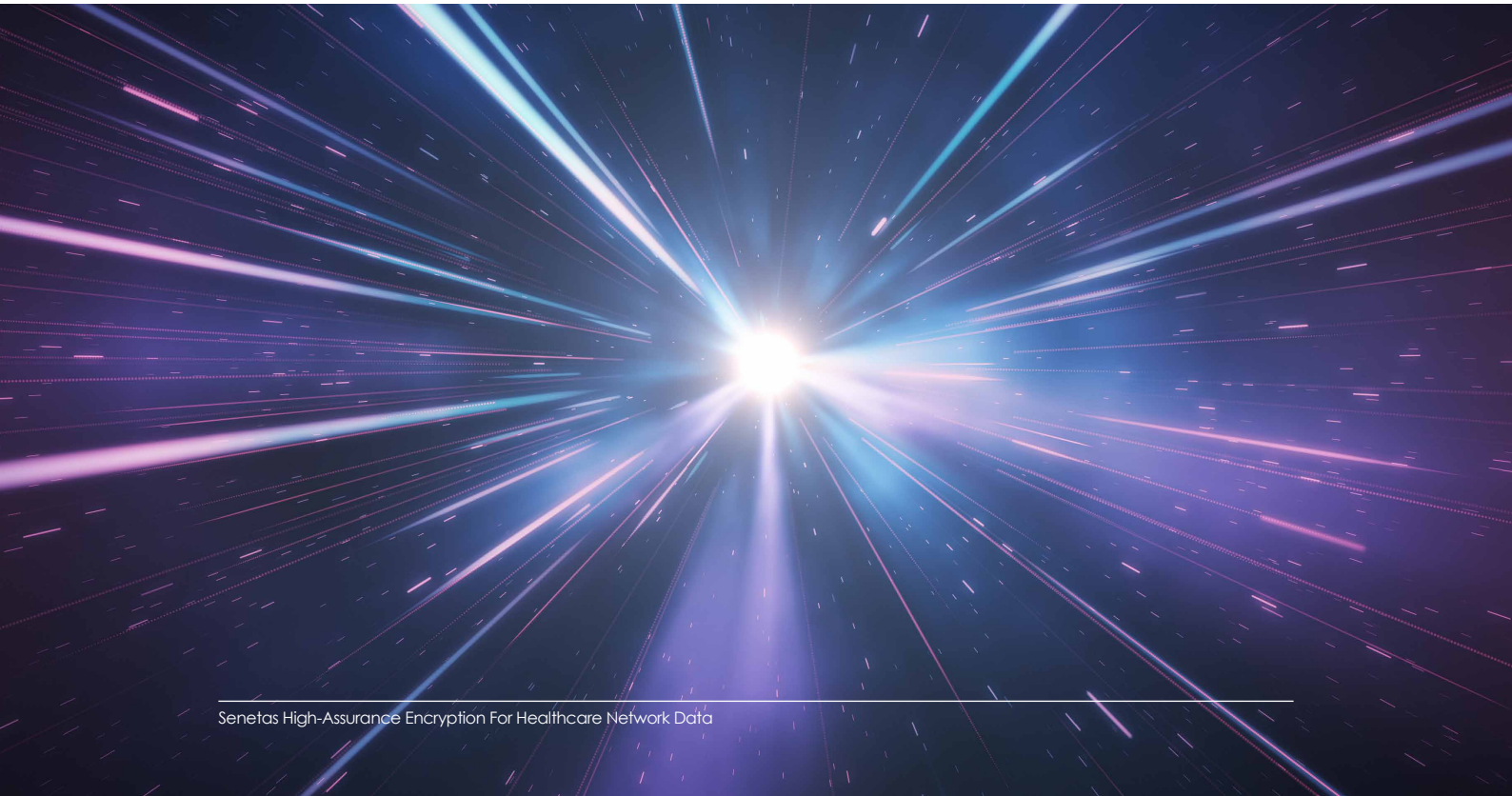
Critical communications infrastructure

The space industry's crucial activities in commercial/civilian and military activities have national economic and security roles. It is an important part of the nation's critical national infrastructure. Few other industries have such direct roles in both economic and military functions. Because almost all military activities depend on space-based assets, any cyber-security vulnerabilities will undermine confidence in national security.

At a national level, the impact of a successful cyber-attack could seriously harm trade, financial services and even enable cyber-terrorists taking over a country's strategic military weapons. Cyber-attacks on satellites include communications signal jamming, malware and malicious content attacks on networks. The most serious would involve targeting command and control systems, attacks on ground infrastructure and even mission packages.

In USA defence most aspects of national security, including the detection of threats, use of weapons, deployment of forces and re-supply, are dependent on the integrity of critical space-based infrastructure and capabilities. Those capabilities and systems are referred to as Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance (C4ISR) and logistics. Hence any successful cyber-attack on space-based assets would be catastrophic.

Cyber-attacks that cause lost data, service disruptions, systems interference or the loss of satellite control or capabilities are unthinkable. A bad actor may take control of a satellite via its command-and-control systems, alter or corrupt the data it provides, even redirect its orbit, thus transforming the asset into a weapon against other space infrastructure.



When the status quo doesn't cut it

The daily evidence of successful malware, ransomware and other malicious content attacks highlights how conventional anti-malware/firewall security solutions don't provide enough protection. Such attacks are pervasive, reaching to all corners of IT infrastructure. All organisations must look to next generation technologies for protection against malicious content for two reasons.

First, conventional anti-malware falls short of security standards required to protect modern infrastructure used by the space industry. The embedded malicious content is increasingly sophisticated. Second, email and other file-based attack vectors remain the primary point of ingress for successful malware attacks. Unknown and zero-day attacks are increasingly used.

The regular reports of malware attacks show how today's reactive anti-virus and malware protection aren't up to the job. Organisations must look to emerging technologies, such as Content Disarm and Reconstruction (CDR), for effective protection. Most malware protection relies upon external libraries of known threats to protect content. But what if the threat is unknown, or new? How do you protect against zero-day attacks? Next-gen solutions succeed because they apply new thinking to new threats. Votiro Disarmer, for example, leverages patented CDR technology to stop zero-day malicious content in milliseconds.

The Cybersecurity and Infrastructure Security Agency has commented that critical infrastructure has increasingly become the primary target of such attacks and that the targets are often inadequately protected against, and prepared for, these threats.

Secure solutions and data sovereignty

Tackling the cyber-security challenge within the space industry is complex. The optimal approach is to break the systems and operations down to their component parts, noting that all are linked by the data networks they use.

A solid solutions foundation begins with long-term network data security, and protection from ingress of rogue data, using high assurance, authenticated encryption. Protection of all systems against the infiltration of malicious content requiring enterprise-wide CDR is also a worthwhile investment. It's essential that all work group file collaboration and file-sharing workflows use an encrypted application with similar high-assurance features. Critically, a space organisation must see all data as sensitive, requiring maximum security.

What are the most common cyber-risks that must be addressed? In order of statistical occurrence, the top five begin with: Denial-of-service (DoS) attacks, Man-in-the-middle (MitM) attacks, followed by Malware (all types), Drive-by Attack (malicious code injected into websites) and Phishing and Spear Phishing (email) attacks.

Recently, the issue of 'data sovereignty' has become so significant it's now treated as a cyber-security issue. It is often a deal-breaker when selecting a cloud-based solution by organisations concerned about where their data is located. Many companies now require data location control to ensure their data is only stored on their sovereign soil. Because space industry organisations work with high-value intellectual property, data sovereignty should be a factor when considering any as-a-Service solutions.

Where to Now?

Whilst there are many attack vectors to be exploited by cyber-criminals, the challenge is to identify the vulnerabilities – from networks carrying data, to everyday use of business systems and files. The common link between all business-critical workflows is the data network infrastructure. All network transmitted data should be encrypted.

Like all high-tech organisations, systems-wide CDR anti-malware, and encrypted file-sharing collaboration applications are essential protection. In the face of an evolving threat landscape, security solutions must be agile and quantum-ready to ensure long-term data protection.

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

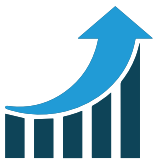
In addition to the standards-based AES256 and 128-bit algorithms, Senetas CN series encryptors support the use of customer-requested algorithms, custom curves (BYOC) and entropy (BYOE).

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 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.

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 modest 10Mbps 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.

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 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.

HITECH-SP0821

SENETAS