SENETAS
Security without compromise

END-TO-END ENCRYPTION FOR HEALTHCARE NETWORK DATA

SOLUTION PAPER

A CONNECTED HEALTHCARE SECTOR

Globally, the healthcare sector has adopted a range of new technologies, as governments and private healthcare providers alike seek to realise operational efficiencies.

The need to provide an improved standard of patient care sits alongside stated objectives to improve workforce productivity, reduce management costs and better leverage the opportunities presented by technology in an increasingly connected world.

In an industry typified by geographic, stakeholder and systems diversity, technology can present as many challenges as it does solutions. However, the ubiquitous availability of connectivity, device proliferation and a concerted effort to centralise patient records has finally put the healthcare industry in a position to exploit technology to the advantage of patients and clinicians alike.

Information sharing, mobile access to patient records, remote diagnostics and collaborative case management are all helping to create better patient outcomes.

Healthcare IT infrastructure has become borderless; with clinicians, governments, advisory boards, independent consultants, office managers, patients and service providers connected via a wide range of devices.

As healthcare stakeholders and systems become better connected, the volume of healthcare data created, processed, analysed and stored
is greater than ever. The increased use of HD video – either for collaboration or patient monitoring – is also changing the nature and format of healthcare data.

Big data requires big data networks, so there has been a corresponding increase in the adoption of Cloud and data centre services; all leveraging high-speed Ethernet and Fibre Optic networks to exchange huge volumes of potentially sensitive information.

However, the benefits of connectivity are overshadowed by the increased risk to patient and stakeholder privacy and data security.

It has emerged that the healthcare industry has become heavily reliant upon data security. Organisations are constantly challenged to address patient privacy, data theft, loss of intellectual property, systems disruption, financial penalties and loss of trust; all amidst an evolving landscape of cyber-crime.

HEALTHCARE DATA IS A VALUABLE COMMODITY

The sensitive nature of healthcare data, which not only includes financial details, but medical histories, dates of birth, addresses etc. makes it a valuable proposition for potential cyber criminals.

The loss of healthcare data comes at a cost. According to IBM's 2020 Cost of a Data Breach Report the average cost of a breach was US$3.86 million. However, within the healthcare industry this was US$7.13 million.

The breach landscape has changed dramatically in recent years. The majority of data breaches used to be down to human error, system's glitches and lost or stolen devices. However, the main threat now comes from malicious outsiders.

Healthcare data is often used for the purposes of identity theft, but the depth and detail of the information available also enables criminals to participate in large scale fraud or extortion.

In 2020 it took an average of 280 days for organisations to identify and contain a breach. Why does it take so long?

Limited budget and resource could be to blame. But it also could be because some organisations have adopted a reactive strategy when it comes to privacy monitoring; only addressing breaches when brought to their attention by a victim of the breach.

TARGETING HEALTHCARE DATA

The high-speed networks used by modern healthcare organisations are becoming increasingly complex. Multiple devices and links feature across a variety of network technologies, protocols and topologies. With this complexity comes risk.

Cyber-criminals exploit areas of weakness, either within the healthcare organisation itself or at the point it connects with third party networks. Whilst the sharing of patient records and management information has become a part of day to day communications, healthcare providers often have little or no understanding of external organisations' data security.

As the global health sector evolves there are, inevitably, mergers and acquisitions. The security of legacy infrastructure is not always given due consideration during the integration phase. At the same time, the adoption of high-speed Ethernet networking devices that are running older versions of software introduces weak points into the network.

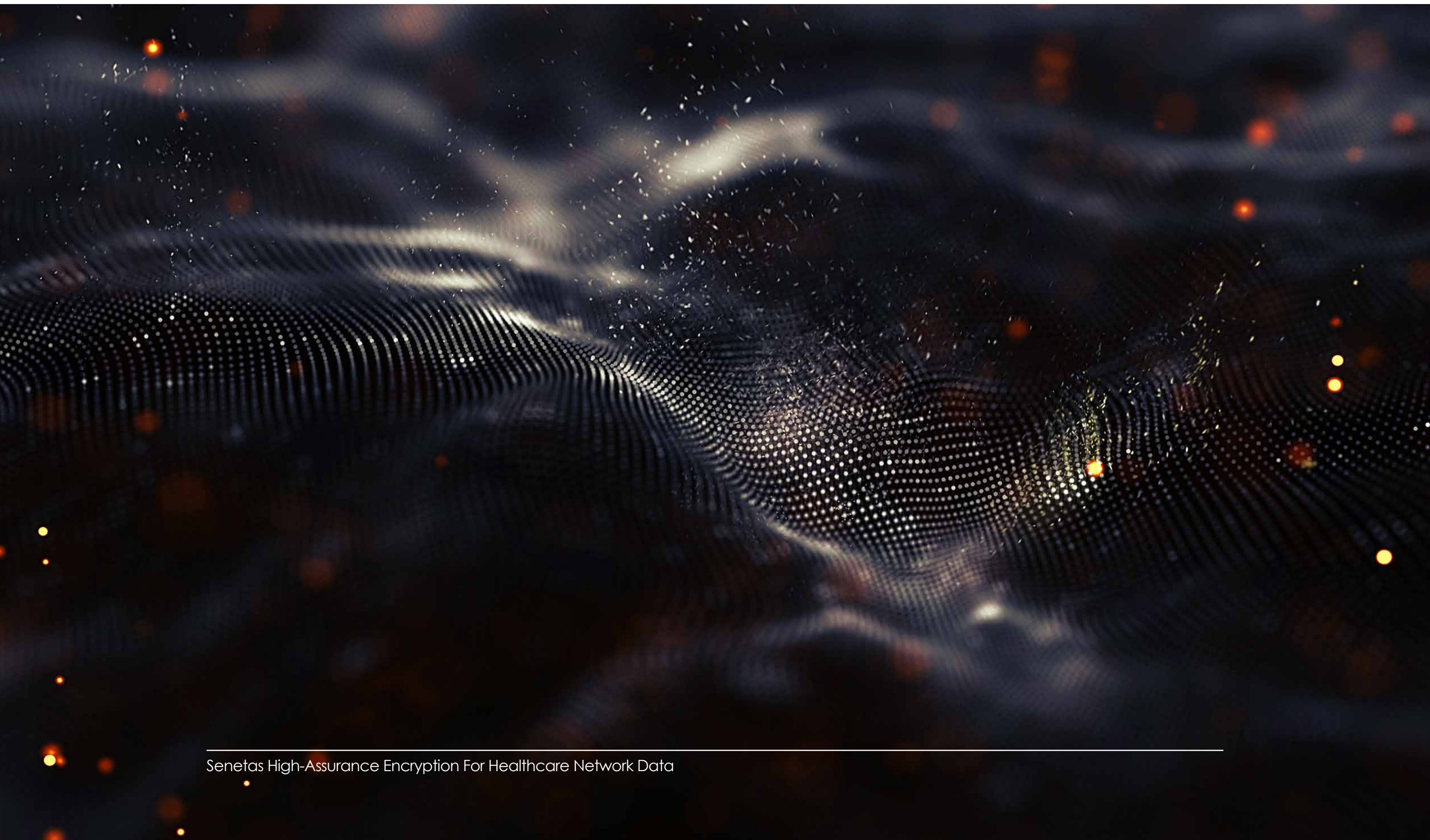
As we move further towards the Internet of Things, more and more devices are becoming connected. The more access points a network has, the more vulnerable it is. Remember, high-speed, fibre optic networks are not inherently secure.

Finally, networks that depend on multi-function devices with encryption "built-in" (such as routers and switches) are exposing themselves to even greater risk. In October 2020 Cisco announced the latest in a series of security vulnerabilities that impacted several of its carrier-grade routers.

Healthcare data is a high-value, low-risk target for cyber-criminals. The data itself has a high resale value and is often found traversing either an unsecured network or one where security policies and tools have been applied inconsistently.

> *"The number of confirmed data breaches in the healthcare sector saw a 71% increase over last year".*
>
> *Verizon Data Breach Investigations Report 2020*

As the healthcare sector embraces mobility, cloud computing and data centre services, it is exposing itself to a new range of data security risks. Use of public cloud infrastructure (typically leveraging Layer 3 Internet links) puts the data itself out of the organisation's control. It is while this data is in motion that it is at its most vulnerable.



NOTABLE BREACHES

The potential for financial gain from accessing medical records has made the healthcare sector an attractive target for cyber-criminals. Over the past 5 years, the industry has been rocked by a series of high-profile incidents.

Among the most notable breaches in recent years was that of US health insurer Anthem. In 2015 a sophisticated attack exposed the personal information of over 80 million current and former customers.

In 2016 Banner Health was breached and hackers used the payment card details of customers to make purchases at food outlets. In 2019 Banner agreed to a $6 million settlement.

In 2018 patient records of over half of Norway's population were stolen thanks to an exploit in devices running outdated operating systems.

The American Medical Collection Agency (AMCA) suffered a sustained attack over a period of 8 months from August 2018 to March 2019. The provider of billing services to the US healthcare sector exposed the personal and financial data of over 20 million customers.

2020 saw no let up, with major breaches reported by Cense AI, GEDmatch and The Hospital Group. The latter is notable as it involved the compromise of over 900 gigabytes of private surgery images.

PROTECTING HEALTHCARE DATA

So, how can healthcare organisations ensure their network data is secure? The answer is simple. Encryption. By encrypting the data before transmitting it across the network, it is possible to ensure both security and integrity.

By encrypting network data in motion, healthcare organisations are assured that, should the network be breached, the data itself would be rendered useless to unauthorised users. Sensitive information would remain secure, regardless of whether the network was public or private.

Whilst there may be some debate as to the risk/reward balance of using encryption in certain industries, the sensitive nature of the data transmitted within the healthcare sector demands maximum security.

In addition, the healthcare sector is subject to strict data protection and regulatory compliance obligations. A breach of which could result in serious financial or operational penalties.

HIGH-ASSURANCE ENCRYPTION

Not all encryption solutions are the same. The critical nature of healthcare networks (and the data they carry) requires a robust encryption solution that provides certified, high-assurance network security and maximum network and application performance; without compromise.

Senetas encryption solutions include the security assurance of certification by leading independent testing authorities. They are certified as suitable for government and defence use by FIPS, Common Criteria, NATO and CAPS.

Multi-function network devices, such as routers and switches with embedded encryption, do not provide robust network security. In some cases, they may even expose the network to device vulnerabilities and other performance inefficiencies.

Truly robust encryption solutions require more than certification alone. For Senetas, certification is just the beginning. To deliver on our high-assurance promise, Senetas encryption solutions feature the following essential attributes:

- Secure, tamper-proof hardware - dedicated to encryption
- State-of-the-art, client-side encryption key management
- Gapless, end-to-end link and network encryption
- Authenticated, standards-based encryption algorithms

COMPLIANCE VS RISK TOLERANCE

The network encryption security conundrum for many healthcare organisations is clear: compliance versus risk tolerance - a.k.a. "how big must the risk be before we invest in encryption to avoid non-compliance?"

Healthcare decision makers have traditionally needed to weigh up several factors in the risk vs. compliance vs. investment equation. Most of these factors concern either the potential impact of a breach or the financial and managerial cost of implementing a robust data security solution.

Although there is no single healthcare regulatory framework, the security compliance standards introduced by government are very high and penalties for non-compliance or successful data breaches are substantial.

The costs associated with a data breach could be felt directly, or indirectly by the breached organisation and include:

- Business disruption
- Financial penalties
- Loss of privacy
- Risk to patient wellbeing
- Loss of reputation
- Compliance failure
- Criminal prosecution

With the availability of certified high-assurance encryption solutions from Senetas, this is no longer an issue. Encrypting high-speed data networks has never been simpler, with ease of management and "set and forget" implementation.

Furthermore, high-assurance encryption does not come at the expense of bandwidth or network performance. Senetas encryption solutions feature near-zero latency, are transparent to other network devices and have zero network overhead.

Whether you are looking for a desktop device to enable encryption anywhere, or a carrier-grade, rack mounted device for ultra-high speed networks; Senetas encryption solutions' low management and support costs, interoperability and backwards compatibility contribute to an extremely low total cost of ownership (TCO).

GLOBAL HEALTHCARE COMPLIANCE

Regulatory bodies across the world have been put in place to ensure the security, confidentiality, integrity and availability of patient and employee information.

Whilst the fine details of compliance obligations vary from country to country, they each set out an industry standard for protected health information (PHI) that prescribes physical, network and process securities required for compliance.

The compliance landscape is rapidly evolving within the healthcare sector and organisations are playing catch-up as they move to implement more stringent guidelines and legislation.

Healthcare organisations need to adopt a data-first approach to network security if they are to avoid non-compliance of the emerging standards, including:

- Health Insurance Portability and Accountability (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- European Commission General Data Protection Regulation (GDPR)
- UK Data Protection Act
- Australian Privacy Act
- Japanese Personal Information Protection Act
- ASTM Standards for Medical Device Interoperability

In the US, HIPAA is designed specifically to address the security of healthcare information that is held or transferred in electronic form. It outlines the obligations of an organisation in respect of ensuring the confidentiality, integrity and availability of all PHI it creates, receives, maintains or transmits.

These US healthcare sector data security regulations include criminal as well as civil prosecution for breaches. Criminal penalties range from $100,000 fine or five years in jail to $250,000 fine or 10 years' jail time.

The GDPR sets one of the most stringent data protection standards and details the extent of financial penalties applicable for non-compliance. It is these penalties that have proved to be one of the most controversial elements of the new regulation.

Under the GDPR, serious data breaches could result in an organisation being fined up to €20 million or 4% of its global annual turnover, whichever is greater.

HEALTHCARE SECTOR EXPERIENCE

Senetas high-speed encryption technology is providing vital patient privacy, compliance and integrity of data traversing the latest generation of high-speed networks in healthcare organisations worldwide:

1.

US healthcare organisation, providing a range of wellness products, sought an encryption solution for both on-premises and cloud services.

2.

A major EMEA-based health service organisation with tens of hospitals and thousands of primary care clinics needed to provide maximum patient confidentiality to its 3,000,000 insured members.

3.

In Australia, a major healthcare insurer and medical services provider set its own requirement for certified high-assurance data network encryption that demanded support for all network topologies and backward product interoperability over time.

4.

A US$5 billion not-for-profit healthcare provider in the USA demanded secure access to its medical and management applications for more than 1,500 clinicians. Robust encryption, ease of management and cost efficiency were essential to the organisation.

5.

A large US-based healthcare insurer and its IT&T subsidiary saw the damage suffered by a competitor after a data breach. It subsequently mandated the implementation of ‘stronger, maximum data security measures’.

6.

Swedish-based regional healthcare providers required network data security that enabled improved security, no loss of employee convenience and productivity, strict regulatory compliance, minimum additional overheads and maximum patient privacy.

7.

In Northern Ireland, a healthcare organisation sought to maximise patient privacy protection and minimise the encryption solution’s total cost of ownership (TCO).

8.

A US-based healthcare network included 3,500 systems users and numerous data network links, over which a full range of medical and patient information is transmitted and shared. A robust network encryption solution was required to deliver a relatively low total cost of ownership over five years, improved security, flexibility and seamless integration.

9.

A US not-for-profit veteran’s healthcare service provider sought to enhance its patient care by providing 24/7 patient monitoring. The introduction of an HD CCTV monitoring system demanded maximum security without impacting on real-time video streaming.

10.

A French healthcare insurer managing over 10,000,000 health records for government and private hospitals required an upgrade to its network data security. The solution needed to meet strict compliance obligations without impacting on network performance.

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 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.

SCS-SP0121

SENETAS