SENETAS
Security without compromise

END-TO-END ENCRYPTION SOLUTIONS

SECURING BIG DATA

SOLUTION PAPER

BIG DATA

We live in a data-driven world. Every minute, the internet receives over three million gigabytes of traffic and in 2020 each person individually created at least 1.7 MB of data per second, amounting to 2.5 quintillion data bytes a day[1].

This vast quantity of data is assembled from a range of sources – from online shopping and email to entertainment platforms and social media – all in different forms and without context or connection.

This is where 'Big Data' comes in. A term first coined in the '60s and '70s before gaining notoriety in the early 2000s, it describes the exponential growth in the collection, sharing, analytics and storage of multi-source information.

This information management concept is now applied to data sets used by organisations across all industries. Data is collected, analysed, quantified and used to provide insight and drive decision making. In essence, Big Data gives meaning to the seemingly random.

Big Data needs fast networks

Because of its vastness and variance, Big Data relies heavily on high-speed data networks to transmit it.

Growth in data generated is exponential, with IDC confirming that the global volume of data exceeded 64.2 zettabytes in 2020 and is set to continue to expand at a compound annual growth rate (CAGR) of 23% until 2025.[2]

This emphasises the need for high-speed data networks that are fast and reliable enough to cope with today's volume, with scope to handle the increase in traffic over the coming years.

The Internet of Things (IoT)

According to IDC, there will be 55.7 billion connected devices by 2025[3], of which 75% will be connected to the IoT.

IDC predicts that 152,000 IoT connections will be made every minute by 2025, making them major contributors to the volume of Big Data being transmitted.

Threats to Big Data

The depth and volume of Big Data makes it appealing to cyber-criminals, who are using increasingly sophisticated methods to breach organisations and either manipulate or steal operational, transactional and personal data.

The sensitive, or personally identifiable, nature of Big Data makes it particularly appealing to "bad actors" that are financially motivated. Even seemingly inconsequential data can be aggregated and analysed to exploit individuals in social engineering-led attacks.

Big Data security

While the threats to Big Data are prevalent, there is a method of protecting this information even in the event of it falling into the hands of criminals.

By encrypting Big Data in motion, it is possible to guarantee the integrity of your data and ensure that, should the worst happen and you were to suffer a breach, the information extracted will be unreadable and therefore rendered useless.

This Solution Paper analyses the threats that Big Data faces, explores why organisations should encrypt Big Data in motion and offers guidance on choosing the right encryption solution.

[1]Domo - Data Never Sleeps 8.0
[2]IDC Worldwide Global DataSphere Forecast
[3]IDC Business Models for the Long-Term Storage of Internet of Things Use Case Data

WHY ENCRYPT?

The volume and variety of Big Data makes it particularly appealing to cyber criminals and therefore vulnerable to attack.

Prevention technologies, such as firewalls, emphasise the need to protect data while it is at rest, but ignore the risks data is exposed to while in motion across private or public networks.

In order to guarantee the trust and integrity of the data being used, organisations must act to secure this data in motion against a wide array of threats.

The breach landscape

According to Gemalto's breach level index, over 13 billion data records were lost or stolen in the five years between 2013 and 2018.

Of those, a mere four per cent were 'secure breaches' where encryption was used and the data was rendered useless.

Malicious outsiders and accidental loss make up a large proportion of breaches, with stolen data most commonly used for identity theft, account access and financial access.

While data breaches occur across all industries, they are most frequent in the healthcare, financial, education, professional, government and retail sectors due to the nature of information collected.

It takes organisations an average of 280 days to identify and contain a data breach[4]. The consequences of these breaches include:

- Intellectual property theft
- Business disruption
- Compliance issues
- Loss of customer data
- Privacy breaches
- Financial loss

Alongside this, firms must address the loss of trust and reputation amongst stakeholders; something that is much more difficult to attribute a value to.

Popular trends and emerging threats

Alongside existing threats, organisations must be aware of technologies that are gaining popularity, as well as those about to be introduced.

The rapid growth in IoT devices, all of which will stream Big Data, is one such example.

Because these devices lie at the edge of the network, many organisations do not account for them when assessing their cyber security. However, if left unprotected, these devices are providing hackers with 25 billion opportunities to gain access to networks and farm sensitive information or input rogue data.

Cloud computing plays an important role in the collection, storage and analytics of Big Data, again requiring high-speed, high-performance data networks that are at risk if improperly protected.

There has also been a notable rise in hackers stealing meta data (data about data). Despite the common myth, this information is sensitive and can provide a wealth of exploitable information if not properly encrypted.

Notable breaches

As increasing amounts of data flows across networks, it leaves it vulnerable to breaches ranging from hack attacks to internal data misconfiguration or loss.

In March 2021. the personal information of over 533 million Facebook users from 106 countries, was exposed through a vulnerability. The data included phone numbers, Facebook IDs, full names, locations, birth dates, bios, and, in some cases, email addresses.

In May 2019, over 275 million Indian citizens personally identifiable data was left unprotected on the internet for more than two weeks following a data leak from multiple unsecured databases and servers.

In January 2020, it was revealed that 250 million Microsoft customer records, spanning 14 years, had been exposed online without password protection. The leak was attributed to incorrectly configured security protocols.

[4] Risk Based Security 2020 Year End Review

SECURING BIG DATA

Protection vs 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. Look for a solution that offers high-assurance data protection and is accredited against recognised world-wide security standards.

By bypassing security systems such as firewalls and gaining access to Big Data networks, hackers can intercept and steal data as it flows between points in the network. Unsolicited access can also be used to inject rogue data into Big Data analytics platforms, compromising the accuracy of the data and the insights it brings.

Network administrators must take steps in order to protect this data in motion, whilst ensuring the speed and performance of the network is not adversely impacted.

End-to-end encryption

Encryption is a crucial element in ensuring the security of Big Data networks. It should be deployed as an end-to-end solution across all layers of the network – including IoT devices – and should secure meta data alongside the main packets.

In the event of a breach, encrypted data is unreadable by hackers and is therefore rendered useless. In addition, the forward secrecy provided by encryption solutions prevents rogue data being inputted into systems.

Encrypting data also benefits organisations from a compliance perspective, with data protection regulations such as the GDPR treating 'secure breaches' differently to those that are not; potentially saving organisations from hefty fines as they demonstrate the importance of protecting the sensitive information they collect.

Network and application performance

Due to the large volumes of Big Data being transferred, it is crucial that an encryption solution does not impact on the speed or performance of the network. This is the challenge that many security professionals and network administrators face.

Of equal concern is that some organisations opt for 'low-grade' data encryption technologies that appear to be effective, but come at a cost:

- Compromised high-speed network performance
- Hidden costs of lost effective bandwidth
- Adverse impact on business-critical applications
- Complex implementation and ongoing management technical impact
- Adverse impact on other network assets

Post-Quantum Security

The coming age of quantum computing also plays a growing part in cyber security. While the immense computing power of quantum computers will have a transformative effect on computing, including Big Data analysis, there is also a risk of the technology being used for harm.

Quantum computers will be able to break current Public Key encryption algorithms in a fraction of the time taken by traditional computing methods, threatening the protocols that underpin much of the world's data security.

While this seems like a distant concern, the reality is much closer. It is estimated that a quantum computer capable of breaking today's cryptography will be available within the next 10 years, meaning organisations need to consider the shelf life of their encrypted data today as well as the their ability to migrate to quantum-safe encryption in the near future.

In 2021, Senetas introduced the first quantum-resistant network encryption solution. Agile by design, it is compatible with both classical, standards-based algorithms and the next generation of NIST shortlisted quantum resistant algorithms; providing long-term data protection in a post quantum computer world.

END-TO-END ENCRYPTION SOLUTIONS

CN Series Encryption Hardware

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

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

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

CN4000

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

CN6000

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

CN9000

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

CV Series Virtualised Encryption

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

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

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

SureDrop Encrypted File Sharing and Collaboration

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

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

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

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

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

Votiro Secure File Gateway

VOTIRO

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

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

WHAT MAKES SENETAS STAND OUT?

Best Performance

High-speed

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

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

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

Ultra-low latency

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

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

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

Zero impact

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

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

High-Assurance

Certification in-depth

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

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

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

Best encryption key management

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

Solution integrity

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

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

Versatile & Simple

Crypto-agility

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

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

Support for all topologies

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

Custom encryption

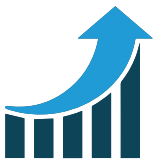
In addition to the standards-based AES256 and 128-bit algorithms, Senetas CN series encryptors support the use of customer-requested algorithms, custom curves (BYOC) and entropy (BYOE).

Ease of use

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

Local or centralised management

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



Low Cost, High Efficiency

Suitability

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

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

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

Cost-efficiency

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

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

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

Reliability

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

Flexibility

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

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas CN and CV Series encryption solutions are sold by Thales as part of its Cloud Protection and Licensing portfolio.

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. Visit our **ANZ Partner Page** for full details.

© SENETAS CORPORATION LIMITED

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file-sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** info@senetas-europe.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal encryption solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has an encryption solution to suit. Our certified high-assurance encryptors protect data across networks operating at speeds from 10Mbps to 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 5Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

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

SECURE FILE SHARING

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Disarmer extension.

DISARM MALICIOUS CONTENT

Votiro Disarmer leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

BDE-SP0621

SENETAS