END-TO-END ENCRYPTION SOLUTIONS: SECURING BIG DATA

SENETAS

Security without compromise

Big Data

We live in a data-driven world. Every minute, the internet receives over three million gigabytes of traffic and by 2020 it is estimated that 1.7MB of data will be created every second, for every person[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 predicting that the global volume of data will grow from 33 zettabytes in 2018 to 175 zettabytes by 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 Gartner the number of devices connected to the IoT will exceed 20 billion by 2020.

Currently over four thousand IoT connections are made per minute[3] by these devices sitting at the network edge, making them major contributors to the volume of Big Data being transmitted.

THREATS TO BIG DATA

The richness of Big Data makes it appealing to cyber criminals, who are using ever-more sophisticated techniques to breach organisations and either manipulate this information or steal it, often for fraudulent use.

In the event that a breach occurs, organisations are left exposed to wide-ranging consequences that can take the form of anything from loss of IP and customer data to direct financial loss and reputational damage.

As well as existing threats, Big Data users must be aware of emerging ones such as the impending age of quantum computing.

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 6.0
[2] The Digitization of the World from Edge to Core - IDC
[3] Domo, Data Never Sleeps 6.0

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 197 days to identify a data breach and a further 69 days to contain[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 20 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.

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.

[4] 2018 Cost of A Data Breach Study – Ponemon Institute.

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.

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 November 2018, Marriott Hotels announced a breach in which 500 million records were stolen. This contained the personal information of all Starwood hotels customers dating back to 2014, in some cases including credit card details and passport information.

In May of 2018 LocalBox, a personal and business data search service, leaked 48 million data records containing data from multiple sources – including scraped data from social media platforms – after a cloud storage repository was left publicly available.

In September 2017 one of America's most prominent credit rating agencies, Equifax, suffered a data breach in which 143 million records were stolen. Sensitive information contained in these records was collected from a number of sources and included names, social security numbers and driver's license details.

*Trustwave paper: Inside a Hacker's Playbook.

Securing Big Data

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

Choosing the right encryption solution

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.

Borderless infrastructure and edge computing sees Big Data flowing from devices across the network, meaning this data must be secured throughout its journey.

In the same way, Big Data transmitted across metro area networks must be secured at all points as a single vulnerability will result in a failure across the network.

As recommended by leading data security and encryption analysts; for a network encryption solution to be truly robust and provide long-term data protection (well beyond the useful life of the data), it must be a "high-assurance" solution.

So-called 'hybrid' encryption devices – such as network routers/switches with embedded encryption or those using MACSec or similar standards (not originally intended for WAN and MAN security) provide "low assurance" data protection.

By contrast, Senetas CN Series 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 Ethernet network encryptors' security credentials include all four, essential high-assurance features:

> Secure, tamper-proof hardware; dedicated to network data encryption

> State-of-the-art encryption key management; featuring secure, client-side key storage

> End-to-end, authenticated encryption

> Standards-based encryption algorithms

For real-time data applications such as financial platforms and CCTV monitoring, latency is a significant issue. Whilst adding a level of encryption through a hybrid device may seem like an attractive option; it will often result in higher latency and lower throughput performance than a dedicated device.

In some instances, using hybrid encryption devices 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 hybrid device is used, the lifespan of the encryption protection will be tied to the host network device and will need to be replaced when the switch is changed.

Modern network infrastructure, such as SD-WAN, can utilise multiple transport technologies that may operate at layers 2, 3 or 4. So, organisations should look for a vendor that provides Layer agnostic encryption where possible.

Senetas CV Series virtual appliances provide concurrent, multi-Layer encryption and support DPDK for up to 5Gbps performance.

Like the CN Series hardware encryptors, our virtual appliances support all topologies, from P2P to Hub & Spoke and fully meshed networks.

Combining hardware and virtualised encryption

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.

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 (>1Gbps) are more commonly used to connect IT infrastructure such as datacentre interconnects, or Big Data feeds.

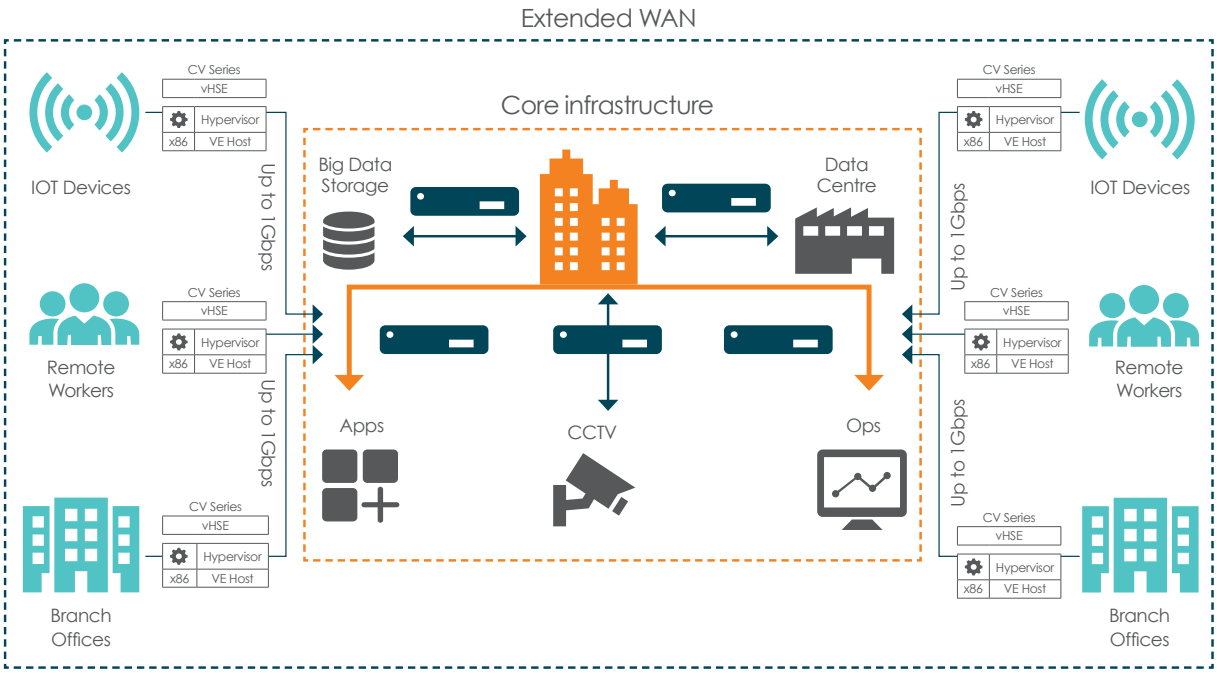
These links ideally require both maximum data protection and best performance, only offered by hardware encryptors.

However, for extended WAN links and high-scale virtualised links that typically run at up to 1Gbps, 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 using Big Data should utilise dedicated hardware encryption for their main feeds and interconnects, while virtualised encryption is used to provide scalable, cost-effective encryption for devices at the network edge.



Senetas CN9000 dedicated hardware encryptor

The CN9100 is the world's first commercially available certified high-assurance 100Gbps Ethernet network encryptor that supports all network topologies.

Like all Senetas CN encryptors, the CN9000 Series provides maximum high-assurance network data security, without compromising network and application performance. It boasts ultra-low latency of just 1.5 microseconds in customer testing.

Developed in collaboration with customers and service providers, Senetas CN9100 encryptors (also known as SafeNet CN9100 Ethernet Encryptors) are designed to meet the exacting requirements of all 100Gbps use cases, making them an ideal application for securing Big Data networks.

Senetas' CN and CV Series encryptors include integrated support for SafeNet KeySecure (Gemalto's centralised cryptographic key management solution) that provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

USE CASE: DATA CENTRE INTERCONNECT

Commercial provision of 100Gbps national and international fibre network links to enterprise and government customers.

In this instance, the customer's 100Gbps links were used to support SaaS, Cloud-based 'mega data' applications and data centre interconnect services.

Additionally, the customer already encrypts Layer 2 Carrier Ethernet 10Gbps and 1Gbps links to meet government customers' requirements for FIPS certified high-assurance network data encryption security.

The certified high-assurance encryption of the 100Gbps 'backbone' links is provided by Senetas CN9100 and CN9120 (WAN and MAN respectively) encryptors. Similarly, the 1Gbps and 10Gbps high speed links are protected by Senetas CN6010 and CN6100 encryptors respectively.

In addition to certified high-assurance requirements, it was essential that the Senetas solutions provided:

> 100% encryptor interoperability among CN6000 and CN9000 Series encryptors and any future Senetas CN products implemented

> Support for all topologies by all CN Series encryptors

> The same crypto-agility and Quantum ready features among all CN Series encryptors

> Flexible multiple topology support within the overall architecture

The service provider's multiple data centre-to-data centre data transmission and aggregation and storage and back-up are included in the complex network architecture.

Senetas CV1000 virtualised network encryptor

The CV1000 is a Network Function Virtualisation (NFV) appliance providing strong and effective data encryption security with designed-in crypto-agility. Designed for large-scale WANs, the CV1000 delivers transport-Layer agnostic encryption for high-speed networks at >1Gbps.

As an NFV appliance, the CV1000 stands out from the crowd. Instant scalability means it may be deployed rapidly across thousands of network links. It delivers the same flexibility and scalability as other virtualised network functions.

The CV1000 offers state-of-the-art encryption security and key management without impacting on network or application performance*. Unlike IPSec-type encryption solutions, the CV1000 is transparent to the network; making it ideal for securing your WAN, right to the virtual edge.

Integrated support for SafeNet KeySecure (Gemalto's centralised cryptographic key management solution) provides maximum security for the storage of master keys, the integrity of security policies and the source of entropy for the generation of cryptographic keys.

KEY BENEFITS

Unmatched benefits of the CV1000 expressed by end-user customers and service providers include:

> The CV1000 enables adoption of a virtualised encryption solution that does not compromise on security or network and application performance

> Instant scalability to match the scale and flexibility of virtual and software-defined networks

> No requirement to deploy large numbers of hardware encryption devices to achieve high-scale implementation of network encryption

> The CV1000 encryption security and key management model is optimised for strong and effective encryption security

> Through Transport Independent Mode, the CV1000 is suited to a multi-Layer network environment

> Competitively, the CV1000 delivers up to 30% network performance benefit over other solutions

> Ease of deployment with centralised, 'zero-touch' provisioning

> 100% interoperability with Senetas CN Series encryptors

> As a software implementation of the Senetas high-assurance encryption platform, the CV1000 provides a flexible, cost-effective way to encrypt all the way to the virtual edge

> Data centre service providers identified the CV1000 as an optimal solution; providing strong and effective encryption security among devices within the data centre itself

*Subject to host appliance performance.

What makes Senetas CN Series encryptors stand out?

Best Performance

High-speed

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

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

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

Ultra-Low Latency

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

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

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

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

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

Best encryption key management

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

Solution integrity

Senetas encryptors provide maximum solution integrity; unlike 'low assurance' solutions, such as router-based network data encryption or so called 'hybrid' encryptors.

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

Versatile & Simple

Crypto-agility

All Senetas encryptors are 'crypto-agile'; from 100% compatibility and interoperability to customisable encryption and FPGA based flexibility.

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

Support for all protocols

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

Support for all topologies

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

Custom Encryption

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

Ease of Use

Set and forget simplicity and network transparency are underlying Senetas design themes. They ensure ease of implementation, operation and management.

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

Interoperability

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

Local or Centralised Management

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

Low cost, high efficiency

Suitability

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

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

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

Cost-efficiency

Senetas encryptors provide excellent total cost of ownership through a mix of network bandwidth savings, ease of management and reliability.

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

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

Reliability

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

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

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

Flexibility

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

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

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

International

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

US Federal Government

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

Australia and New Zealand

ANZ Partner Community.

GLOBAL SUPPORT

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

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

GET IN TOUCH

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

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

Customers are free to contact Senetas directly to discuss their requirements; or a service provider may contact us on their behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

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

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

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

SECURE FILE SHARING

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

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

www.senetas.com

Senetas is a leading developer of encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider data in over 35 countries.

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

Regional Contacts:

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

BDE-SP0219