BIG DATA
INDUSTRY PAPER

SENETAS
Security without compromise

INFORMATION-RICH BIG DATA IS UNDER INCREASING THREAT OF THEFT AND BUSINESS DISRUPTION. AS THE NETWORKS AND TECHNOLOGIES THAT ENABLE BIG DATA COLLECTION, ANALYSES SHARING AND STORAGE GROW, SO TOO DOES THE ATTENTION OF CYBER-CRIMINALS!

OVERVIEW

The term Big Data describes the exponential growth in the collection, sharing, analytics and storage of multi-source information. A powerful information management concept that is applied to the number of large data sets found in every industry sector, Big Data relies heavily upon the high-speed data networks that transmit it.

It's fair to say that by its very makeup – aggregation of multiple information sources – Big Data is sensitive information. However, stakeholders expect their information to be secure in the hands of organisations that use it.

Organisations that invest in Big Data seek to maximize its value, which involves the regular transmission and sharing of large volumes of this 'information rich' data.

The increasing volumes and details of information captured by organisations have extra impetus fuelled by the data explosion driven by the Internet, by multimedia and by social media.

These overwhelming volumes of information-rich data mean government, commercial and not-for-profit organisations are exposed to new data security risks.

Respected data security experts, Trustwave, commented:

*"If they do it right, advanced attackers can quietly infiltrate a network and steal data or information at will for months or even years."**

Big Data technologies offer significant benefits to the organisations embracing it however, the high-speed network data transmission necessary to aggregate, share and analyse Big Data expose those organisations to increasing risks of unauthorised high-speed network:

- Data "sniffing";
- Information theft;
- Loss of valuable intellectual property;
- Redirection of sensitive data streams;
- Business disruption;
- Identity theft;
- Damaging data asset and information integrity attacks.

These risks are real and growing. Furthermore, the consequences can be catastrophic:

- Major financial loss;
- Expensive litigation costs;
- Loss of reputation;
- Loss of stakeholder confidence;
- Devastating impact on intellectual property assets and business revenue;
- Consequential losses from identity theft, business disruption and asset damage.

Data encryption is the optimal answer, but most encryption solutions degrade the data network performance or adversely affect the transmission and sharing of Big Data.

Senetas high-speed network data encryption avoids the downsides. Our unique world-leading high-speed encryptors provide maximum data protection without compromising high-speed network performance. That's why Senetas encryptors are used by the most secure organisations around the world.

Only by encrypting the data itself is it effectively protected against a successful network breach by unauthorised parties. Whilst protecting the networks that enable the Big Data technologies is important, it is not a matter of "if" there will be a successful breach, but "when"!

Preventative measures are a game of catch up, whereas encrypting the data that is transmitted provides the last line of defence against a successful breach. It renders the data useless in unauthorised hands.

Despite efforts to protect the data networks, the optimal solution is to protect the data itself – by encrypting it. Encryption renders Big Data meaningless in the hands of unauthorized parties in the event of a successful breach.

Unfortunately, data network protection is a process of catch-up. However with a focus on the data itself, data encryption is the optimal last line of defence.

* Trustwave paper: Inside a Hacker's Playbook.

BIG DATA NEEDS "DEFENCE-GRADE" ENCRYPTION

Breaches of unprotected Big Data expose organisations to the serious costs of privacy breaches; theft of valuable intellectual property; substantial financial loss; loss of reputation and trust, and devastating damage to the data.

The benefits of Big Data technologies require high volumes of data transmission and the increasing need for high-speed data networks. Data transmission is growing rapidly as more data sources are aggregated, analysed and shared.

Big Data is driving the growth and expansion of high-speed data networks – enabling the sharing, analytics, remote storage and use of that data. Cloud computing often plays an important role in the collection and analytics of Big Data, again requiring high-performance high-speed data networks.

Often remote data centres are required to store, back up and enable disaster recovery of that data, again requiring high-speed data transmission. But by its very nature Big Data is sensitive – information rich! The multiple layers of correlated information – customer, financial, identity, research, supplier, product, services and a vast range of other data – must be protected against successful unauthorised access.

Therefore, cyber-criminals have also turned their attentions to the increasingly information-rich data networks transmitting these enormous volumes of Big Data. The risks of unauthorised "sniffing", data theft, redirection and damaging attacks require solutions that do not degrade the data network performance and in turn adversely affect the performance of the Big Data applications themselves.

DATA NETWORKS ARE NOT SAFE!

But, data networks are not inherently safe! In its 2012 Global Security Report, Trustwave reported that as much as 62.5% of data theft occurs while the data is in transit!

The exponential growth in Big Data has been followed by increased risks of data breaches – the often hidden risks to data while being transmitted between locations. Big Data offers cyber-criminals and other unauthorised parties high rewards.

The risks of data "sniffing", theft and malicious damage can be devastating – from financial loss, litigation costs, damage to reputation, lost research and intellectual property, to regulatory costs arising from compliance and privacy breaches.

Protecting Big Data while it is in transit has been a challenge to most organisations due to its very size and volumes, especially as they attempt to maximise data transmission efficiency and minimise impediments.

However, many organisations have resisted encrypting transmitted high-speed data for fear of heavy costs to network performance. Of equal concern is that some organisations opt for "low-grade' data encryption technologies that appear to be effect, but these come at a cost:

- Compromised high-speed network performance;
- The 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.

The optimal data protection is to ensure that when it falls into unauthorised hands, it is meaningless. Senetas defence-grade encryption provides that protection.

Senetas' world leading high-speed data encryptors provide Big Data the assurance of the ultimate last line of defence without loss of network performance – and that's certified!

SENETAS LAYER 2 DATA ENCRYPTION – TRIPLE-CERTIFIED

The typical use of Layer 3 data networks for the transmission of Big Data comes with built–in network performance impediments – at a bandwidth speed cost of 50% to 70%!

However, the use of Layer 2 networks with their inherently simpler and easier to manage characteristics and cost efficiencies enable the advantage of Senetas' world-leading high-speed encryptors without network performance compromise!

Only Senetas' high-speed data encryptors provide triple-certified data network protection without a loss of network performance and the simplicity of "configure and forget" defence-grade encryption. Senetas encryptors ensure that data protection need not come at the significant cost of lost bandwidth and network performance – so critical in data centre services.*

Senetas' high-speed encryptors - unlike any other high-speed encryptors of their type – hold certifications by the three leading international, independent government testing authorities – FIPS (US), CAPS (UK) and Common Criteria (international and Australia) – your assurance of security without compromise!

Because Big Data applications rely heavily upon uninterrupted data flows and processing, organisations can be assured that protection of the data in transit comes with the dependability of 99.999% up-time availability.

Similarly, commercial and government organisations implementing secure dedicated, everywhere anytime Cloud computing applications that use and generate Big Data, have peace of mind that Senetas encryptors are providing a defence-grade last line of defence – without compromise.

*Senetas Layer 2 encryption performance versus conventional encrypted Layer 3 network performance.

SENETAS BIG DATA SOLUTIONS

Senetas encryptors have been selected to protect Big Data transmitted across high-speed networks based on the following requirements. In each case customers ran their own extensive performance testing and benchmarking. Senetas encryptors excelled:

- Near-zero latency and maximum network performance;
- Consistent and dependable latency performance suitable for business-critical applications;
- Maximum bandwidth performance;
- Encryptors held all testing authority certifications required;
- Extensive interoperability and backward compatibility of Senetas encryptors;
- Flexibility to tailor the devices to specific unique customer requirements;
- Efficient "total cost of ownership";
- Zero impact on other network assets;
- Ease of ongoing encryptor management;
- Best practice reliability (99.999% uptime);
- Multi-network protocol compatibility.

Senetas' encryption on Big Data includes government and commercial customers.

SUGGESTED FURTHER READING

TOPIC	DESCRIPTION	LOCATION
Senetas CN Series encryptors	CN Series Brochures	View website
Senetas Encryptors at a Glance	Specifications of Senetas CN Series encryptors	Download PDF
White-paper "The Business End of Data Protection"	From the moment data is in motion, you are actually no longer in control of it, and it can be easily and cheaply 'tapped' by cyber-criminals for all variety of unauthorised reasons.	View website Download PDF

GLOBAL SUPPORT AND DISTRIBUTION

Senetas CN series encryptors are supported and distributed globally by Gemalto N.V. under its 'SafeNet' encryption brand. Gemalto also provides pre-sales technical support to hundreds of accredited partners globally: systems integrators, networks providers, cloud and data centre service providers, telecommunications companies and network security specialists.

www.gemalto.com/enterprise-security/enterprise-data-encryption

SENETAS PARTNERS

Senetas works exclusively with leading systems integrators and network service providers across more than 35 countries worldwide.

Our master distributor, Gemalto, and its global network of partners have proven expertise in high-speed data networks and data protection.

What's more, Senetas partners are committed to investing in the latest technical training for network data protection, high-speed data encryption and customer needs analysis.

TALK TO SENETAS OR OUR PARTNERS

Senetas also works with customers' existing data network service providers, systems integrators and information security specialists to specify the optimal high-speed encryption solution for your needs.

The optimal specification of Senetas CN Series encryptors for your network data protection is dependent upon many factors, including IT and network environments, technical and business needs.

Wherever you are, simply contact Senetas to discuss your needs. Or, if you prefer, your service provider may contact Senetas on your behalf.

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com