PROTECTING COMMERCIAL NETWORK DATA IN MOTION

WHO SHOULD READ THIS DOCUMENT

Layer 2 Data Networks Managers and Support staff, Data Network Architects, Data Security Managers and staff, Chief Information Security Officers, Chief Information Officers and Data Security Procurement Staff.

KEYWORDS

Layer 2 Data Networks, Network Data Encryption Hardware, High Speed Data Networks, Network Data security, Encryption Data Security, Network Data Encryption, Certified Layer 2 Network Encryptors, High-Assurance Network Encryptors, 10Mbps, 100Mbps, 1Gbps, 10Gbps and 100Gbps Data Encryptors and Commercial Network Data Security.

SENETAS

Security without compromise

Modern organisations have become dependent upon the fixed, high-speed data networks that serve as their core network infrastructure; providing Big Data, Cloud, SaaS and other digital transformation technologies.

These critical technologies and applications generate huge volumes of data. Data that is often transmitted across wide and Metro Area Networks; exposing it to a variety of cyber-threats. Unfortunately, this "data in motion" is often over-looked when it comes to cyber-security planning.

Across the world, commercial organisations are required to comply with a wide variety of cyber-security regulations. Adherence to these standards, whether independent or sector specific, are often a prerequisite to operate within the sector.

However, private and public-sector organisations alike need to understand that managing cyber-security risks to network data goes well beyond essential privacy and compliance issues.

Some of the risks are serious enough that they can threaten the core of an organisation's operations; its value, intellectual property, business intelligence or physical assets.

Despite the high-profile stories of data breaches that have dominated the headlines for the past five years, research repeatedly highlights that these risks are being underestimated; or worse still, ignored.

This is often because of a presumption that fibre-optics used in core network infrastructure, such as high-speed Ethernet networks, are safe. They are not.

Whether your network infrastructure is carrier-provided (public) or corporate-owned (private), it could be carrying large volumes of data, streamed at anything from 10Mbps to 100Gbps.

As a result, it is a high-value target for eavesdropping and all manner of cyber-attacks. As James Caplan from McKinsey and Company puts it "The larger the data volume, the greater the risk."

When it comes to securing core network infrastructure, the risk is even greater. The vulnerabilities present in major vendors' network devices (such as routers and switches) place an additional burden on infrastructure managers.

Interrupting day-to-day network operations to implement a long list of security software patches is nobody's idea of best practice.

Assuming they can stay up to date with the latest patches, IT professionals are still fighting a losing battle. High-speed networks are not inherently secure and breaches are inevitable.

As innovation and collaboration sit at the heart of modern infrastructure, potentially sensitive or valuable data is constantly in motion across core networks for a variety of reasons:

> Data centre network links for data storage with multiple redundancy for back-up and disaster recovery planning

> Sharing with collaborating partners, suppliers and customers across WAN and MAN links

> Big Data analytics used for research and development

> Cloud and SaaS applications for day-to- day operations

In a global economy, data has become the life-blood of commercial organisations of all sizes. Protecting this data should be priority.

The commercial sector is amongst the most cyber-security aware sectors in the world. As big data applications and the IoT have come to dominate day-to-day operations, they have focused the minds of cyber-security professionals.

Experts are predicting that cyber-security spend will exceed $1 trillion over the next five years.

The commercial sector's involvement in high-value innovation, science and technological development makes it a high priority target for cyber-attacks from a variety of vectors; including cyber-activists, organised crime syndicates, global competitors, even state-sponsored attacks.

As tighter regulations come into force and organisations are bound by mandatory breach notifications, the true scale of the problem is becoming apparent.

The breach landscape has been dominated by web-based vectors in recent years, as cyber-criminals seek to gain from identity theft, financial or account access.

No industry sector is safe, with high-profile breaches spanning healthcare, energy, telecommunications, banking, retail and technology companies.

The River City Media breach was one of the largest ever, with over 1.3 billion email addresses exposed because of a faulty back-up process.

The cost of a data breach continues to rise. In its 2016 Report, the Ponemon Institute put the average cost of a breach at $4m, up 29% since 2013.

Consider eavesdropping on core network infrastructure. How and when would an organisation know its data streams are the subject of eavesdropping?

When eavesdropping is discovered, what damage has already been done and what future damage may be done?

> What products have been compromised?

> What R&D investment has been lost?s

> Which customers will no longer buy your products?

> What will the downstream effect be – i.e. damage to reputation, trust and brand?

This downstream effect has become increasingly damaging, where manufacturers with unique product technologies discover their intellectual property has been stolen.

In the US, rogue state actors eavesdropped on the core network infrastructure of international advertising and marketing agencies used by global enterprises.

Concerns among agencies and their clients identified that business critical product development, pricing and other secrets had reached competitors in foreign states. The costs to the agencies and customers involved are being measured in hundreds of millions of dollars.

The business of cyber-crime

Cyber-crime is not limited to activities of common criminals and bored teenagers. It is now a key domain and skillset of terrorists and state-sponsored hackers.

Like any well-run business, cyber-criminals have plans based on objectives – whether to do serious harm, engage in espionage (industrial, defence or state), or just make money.

A recent Verizon Cyber Security Report states, "Cybercriminals care most about ROI (return on investment), so make yourself expensive to hack."

The report suggests where would-be hackers discover high-quality data protection, rather than a challenge to overcome, it acts as a deterrent and encourages them to "move on and attack organisations that are not so well protected".

Cyber-criminals have become more skilled and better equipped in recent years, but prevention technologies have struggled to keep pace.

Like most anti-crime measures, prevention is a process of catch up. This, in part, explains the shocking statistics quoted by Gemalto in its latest Breach Level Index:

> 1.4 billion records were involved in some sort of data breach in 2016

> The number of records lost or stolen in 2016 was up 86% on the previous year

> 'Malicious actors' were responsible for 68% of data security compromises

When it comes to protecting network data in motion, a robust cyber-security strategy needs to include elements of both prevention and protection.

Prevention uses technologies designed to stop a data breach. Whether that breach occurs while data is in motion or not, breach prevention technologies are key components of any cyber-security strategy.

However, if there is one truth in data security, it's that it's not a matter of if a breach will occur, but when.

Protection is concerned with safeguarding data in the event of a breach. Only by encrypting your data can you ensure that when prevention fails, your data remains protected.

However, not all encryption solutions are the same. Today, and as we look towards the future, encryption solutions must be crypto-agile and provide high-assurance data protection.

High-assurance encryption solutions provide long-term protection for data; well beyond its useful life. They also provide protection against the increased use of traffic flow analysis, where cyber-attackers seek to gain insights from analysing data flow patterns.

It may be surprising to know how much cyber-criminals can learn from core network infrastructure traffic flows.

Initially a defence force tactic used to infer intelligence about enemy troop movements, traffic flow analysis has also become an important cyber-security issue for commercial organisations. Targets are frequently oblivious to the eavesdropping and inferences made by the cyber-attacker.

The future holds greater uncertainty, as new technologies like Quantum Computing evolve.

Although a viable quantum-computer may still be 5-10 years away, its arrival will render much of the technology currently used to secure public key infrastructure redundant; unless your encryption solution has agility built-in.

What is high-assurance encryption?

The term is used to differentiate between encryption methodologies and features. Four critical components make up high-assurance network data encryption:

1. Secure and tamperproof hardware; 100% dedicated to encryption
2. End-to-end, authenticated encryption; ensuring no data is unencrypted when in motion
3. State-of-the-art, zero-touch encryption key management; ensuring only the customer can ever access the keys
4. Use of recognised, standards-based encryption algorithms; such as AES256

In addition to high-assurance criteria, robust encryption should also be officially certified by independent standards authorities as suitable for government and defence use.

Certification represents an independent validation of your chosen solution. The three key standards organisations are:

> Federal Information Processing Standard (FIPS) – United States

> Common Criteria (CC EAL) – International

> North Atlantic Treaty Organisation (NATO) – All Member States.

Since developing the first CN encryptor, Senetas has chosen to differentiate its products through certification. Multiple certifications form a key part of the 'certified high-assurance' Senetas proposition.

We refer to this commitment as 'Certifications In-Depth'. Having developed expertise in security standards and testing requirements, certification is a cornerstone of Senetas' hardware encryption design and development.

In recent years, four key factors have emerged as critical cyber-security risks within the commercial sector.

An increase in collaboration has led to the sharing of sensitive information outside of the data security safe-zone (with customers, employees, partners and suppliers).

The Internet of Things has broken down the borders of traditional infrastructure and exponentially increased the number of access points to the network.

Old-fashioned human or technical error, whilst on the decline, still accounts for almost 1 in 5 of all lost or stolen data records (2017 Gemalto Breach Level Index).

Security vulnerabilities discovered in core network infrastructure devices significantly add to the cyber-security risks of data in motion.

Examples include:

> Network devices discovered to have security weaknesses that may be exploited by cyber-criminals

> Inferior or poorly engineered devices that promise added encryption security, but use weak encryption processes

In one instance, PC World reported that over 840,000 Cisco networking devices from around the world were exposed to a vulnerability akin to one exploited by a hacking group.

Research by SEC Consult revealed further vulnerabilities in over 900 products; with poor encryption key-management processes used by routers and switches that promise "hybrid encryption".

This highlights three key issues for defence industry organisations that take data security seriously:

> The importance of certified encryption solutions and government evaluations

> Why encryption security must be a 100% dedicated and separated function

> That hybrid network and security products do not offer optimal data protection

"Encryption should be enabled for everything by default, not a feature you turn on only if you're doing something you consider worth protecting."

Bruce Schneier.

Cyber-security experts continue to warn that too many organisations underestimate and underinvest in protecting data in motion.

Whether all data in an organisation is sensitive per se, is not the point; nor is it a reason to avoid protecting it with encryption. Data has become the currency of modern business and the rewards for cyber-criminals, hackers and terrorists can be significant.

Beyond the potential for privacy breaches, and a failure to meet regulatory compliance obligations, the impact of a data breach can be catastrophic.

Loss or corruption of critical business data and management information can have a wide-ranging impact on day-to-day operations.

Even greater impact would come from the loss of intellectual property or "secret" information that provides any degree of competitive advantage.

Under new, stricter, data protection regulations, organisations found to be in breach of the rules could face significant financial penalties; especially if it is not a first offence.

The GDPR, though originating within the EU, will impact on just about every organisation and includes the potential for eye-watering penalties (up to 4% of global revenues) for repeat offenders.

Emerging regulations will also see individuals within organisations liable for financial penalties and even custodial sentences in the case of negligence.

This will place a greater responsibility and "duty of care" on both data owners and processors within the commercial sector.

Longer-term implications of a breach can also be derived from a loss of reputation or trust; jeopardising future revenues.

For example, US industrial software developer AMSC – a listed company – discovered that critical software intellectual property had been stolen and was being used by foreign competitors.

Despite swift action by AMSC (with the aid of the FBI), stock values fell from $370 per share to just $5 per share while the matter was being prosecuted.

What makes Senetas encryptors stand out from the crowd? Security without compromise!

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 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 10Gbps, 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 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 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.

*As surveyed in 2014 and 2015, Senetas hardware was on-site engineers' preferred hardware.

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

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 as well as 99.999% up-time reliability.

RELIABILITY

Senetas CN encryptors provide proven reliable 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 high-speed 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.

GLOBAL SUPPORT AND DISTRIBUTION

Senetas high-assurance encryptors are supported and distributed globally (excl. AUS & NZ) by Gemalto – the world's largest data security company - under its SafeNet Identity and Data Protection Solutions brand.

Gemalto also provides pre-sales technical support to hundreds of accredited partners around the world; including systems integrators, data network providers, cloud and data centre service providers, telecommunications companies and network security specialists.

TALK TO SENETAS OR OUR PARTNERS

Senetas and Gemalto also work with customers' own data network service providers, systems integrators and information security specialists to specify the optimal high-assurance encryption solution for their needs.

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

CERTIFIED HIGH-ASSURANCE NETWORK DATA ENCRYPTION

Whatever your Layer 2 Ethernet network security needs, Senetas has a high-assurance solution to suit. They support data network links from modest 10Mbps and 100Mbps to high speed 1Gbps and 10Gbps as well as 10 x 10Gbps and ultra-fast 100Gbps bandwidth.

Certified, scalable, agile and easy to use; Senetas high-assurance encryptors provide maximum data security without compromising network performance.

SENETAS CORPORATION LIMITED

E info@senetas.com
www.senetas.com

Senetas manufactures high-assurance Layer 2 Metro Area and Carrier Ethernet network encryptors. They support all Layer 2 protocols and topologies.

Our multi-certified encryptors are used by some of the world's most secure organisations; including governments and defence forces, commercial and industrial enterprises, Cloud, data centre and telecommunications service providers in more than 35 countries.

gemalto
security to be free

SafeNet CN Series Ethernet encryptors

www.gemalto.com

GEMALTO DISTRIBUTION & SUPPORT

Senetas CN Series certified high-assurance network encryptors are distributed and supported internationally by Gemalto (North America, Europe, Asia, Middle East and Africa) as SafeNet CN Ethernet Encryptors.

COMNDS-SP0817