BATTEN DOWN THE HATCHES!

A GUIDE TO PROTECTING DATA WHITEPAPER

SENETAS

Security without compromise

SENETAS
Security without compromise

BATTEN DOWN THE HATCHES!

ASSESSING THREATS TO YOUR ETHERNET NETWORK – A GUIDE TO PROTECTING DATA IN MOTION.

SUMMARY

With the exponential growth in data volumes ('Big Data'); rising adoption of Cloud services and use of remote data centres driving unprecedented movement of data throughout networks, data in motion is under increasing threat. Of all reported fraud, electronic information theft is now the most common at 27%*. How and why is data theft on the rise, and which information is most vulnerable? This paper examines the risks to data in motion, plus the optimal encryption options for managing and assuring data network security.

Being breached is not a question of 'if' but 'when', therefore best practice data protection means ensuring data is effectively useless when it falls into unauthorised hands.

In this information age, technologies have enabled more powerful data collection, analysis and sharing capabilities than ever before. The corresponding exponential growth in information volumes has led to the term 'Big Data'. Importantly, the greater the aggregation of data, the more valuable it becomes, making 'Big Data' increasingly attractive to cyber-criminals.

Technologies which produce 'Big Data' lead to 'big' data networks, 'big' Cloud computing and 'big' datacentre services – all of which expose organisations to even 'bigger' threats including data theft, cyber-crime and malicious cyber-attacks.

Threats to data are not limited to fraud, theft and harm arising from breaches of privacy, but include the risks to data integrity and its serious consequences. There is also the risk of data being transmitted to an unintended location. Whether transmitted in error due to a device error, human error, or a deliberate act, the risks to privacy and integrity exist.

The need to protect data in motion from cyber-threats has also increased exponentially as data network usage grows, the data transmitted becomes increasingly valuable and bandwidth demands increase. The moment data is being transmitted to another location – control is lost and it's at risk! The effective encryption of data in motion does not attempt to prevent cyber-criminals accessing the data network. Its critical benefit lies in the fact that it protects the data! The optimal assurance is that the data itself is of no value to unauthorised parties.

*Kroll 'Global Fraud Report', 2010

WHO SHOULD READ THIS WHITEPAPER?

CIOs, data network managers, information security managers, risk managers, network architects and all senior business managers – anyone needing to understand the risks to data in motion.

INTRODUCTION

Information is how both society and organisations function and grow, but it is under increasing threat. The 2010 Global Fraud report by Kroll highlights that for the first time in history, the theft of electronic data and information has overtaken physical theft as the most commonly reported fraud (27% overall).[1]

Certain industries and organisations inherently carry a high expectation of a strong 'duty of care' in the way they use, manage, store and transport data. For example, health organisations and their patient data; e-commerce companies housing customer credit card data; government agencies handling financial, identity or personal data; membership entities with private identity information – all sensitive information and now a routine target for criminal organisations.

Organisations are becoming increasingly aware that the consequences of information loss, theft or compromise can be devastating – a potential mix of revenue and intellectual property loss, damage to a company brand, exposure to legal liabilities, and loss of customer trust and investor and shareholder confidence. But for the stakeholders, when information is stolen, these consequences might take years to occur and occur many times.

Within the information security industry, standard protection is often about plugging vulnerabilities – trying to prevent successful attacks. But this approach can lag well behind the evolving abilities of cyber-criminals. Today's reality is less about 'if' you will suffer a breach, but rather 'when', which means organisations need to assess and plan to minimise (or eliminate), the impact of that information getting into unauthorised hands.

The cyber-threat risk arises the moment data is being transmitted. The issue is lost control over the data while it travels to its destination. That's why it is not simply systems and servers that are vulnerable. As it travels across networks – internally and externally – data in motion carries its own degree of risk exposure. In fact, data in motion is just as much at risk as IT systems and data at rest. Using several tools we'll describe in this paper, today cyber-criminals have access to relatively inexpensive means of exploiting information when it is in transit. The optimal solution is to be sure that when a cyber-criminal succeeds and has that data, it is useless.

As a result, private sector organisations and governments are now increasingly exploring and investing in *data encryption* as the optimal way to secure information from being exploited when it gets into unauthorised hands. The major benefit of data being correctly and efficiently encrypted as it travels across networks is in the way it is rendered useless to an unauthorised party when a network is breached.

This Senetas whitepaper assesses the issues and risks facing data networks and data in motion. It discusses risk mitigation practices along with the protection and encryption systems your organisation can put in place to manage critical data security. In particular, the paper discusses the need to 'protect the breach' – helping to minimise damage by ensuring that any leaked data is of no value to unauthorised third parties.

HOW THE DATA NETWORK ENVIRONMENT HAS CHANGED

The complexity of current enterprise IT environments creates many opportunities for attacks by cyber-criminals. Today it is far more common for inherently sensitive information to routinely travel among networks nationally and internationally in our global digital economy (data in motion). Hence, privacy and data integrity are at increasing risk of cyber-attack.

Our era of 'big data' demands increasing bandwidth necessary to handle mega data sets and parallel processing on thousands of servers. This is fueling an increasing demand on network capacities in data centres. Data in motion security technologies have therefore become increasingly important.

Cloud (public and private) and Internet services are the largest drivers of growth in data networks and off-site data storage, including the transmission of data, as reported by McKinsey & Company in its publication, 'Protecting information in the Cloud'.[2] The resulting new 'Software as a Service' technologies now available have quickly matured and are driving increased data traffic across networks.

However, organisations, which have quickly adopted these technologies, now face new business risks where intellectual property, regulated information and privacy requirements are threatened. Individually, small and large organisations alike that once *rarely* transmitted data from one place to another or to the Cloud have now adopted technologies and services that involve the daily transmission of many gigabytes of data, all of which is now exposed to new risks.

In the current IT environment, security is typically playing 'catch-up' with cyber-criminal methods. But by focusing on protecting our most critical assets, we are better placed to minimise potential damage. Best practice, therefore, demands we consider how to ensure a 'no damage' protect the breach outcome when a successful cyber-attack or data breach occurs.

Organisations must not simply assess their exposure to cyber-threats, but must also assess the 'sensitivity' of their data and its likely 'attractiveness' or value to cyber-criminals.

HOW WILL YOUR DATA IN MOTION BE ATTACKED?

To discover current network hacking and attack trends, we can look to a well-regarded industry source. The Trustwave paper, *'2012 Global Security Report'* examined a huge number of 2011 incidents, known breaches, tests and results from forensic investigations.

According to Trustwave, data networks appear to be facing a growing threat, although awareness around the vulnerability of fibre optic networks – a rich source of data – has increased. Regarding the harvesting of data, information theft most commonly occurs when data is *in transit*, amounting to 62.5% of attacks.[3]

When it comes to accessing data, there are a number of approaches a cyber-criminal may adopt. Depending on apparent vulnerabilities, some will aim to attack data while it is at rest either within the host system or the storage subsystem, and there are a number of established intrusion detection and protection systems that address these threats. If we assume that these systems are in place, then the cyber-criminal may well direct their efforts towards the network, attempting to intercept the data in motion.

There are a number of surprisingly easy, affordable and accessible ways to access data as it travels among data networks on fibre optic cables. Data networks using copper cable are easy to tap or probe, without even gaining physical access to the wires. With fibre optics, techniques such as coupler splice-ins, fibre bending coupling, and evanescent coupling are all ways in which fibre cable can be eavesdropped, and data in motion can be altered, downloaded or otherwise compromised.

Therefore, where the data is of value to the cyber-criminal, the internal systems *and* the network traffic must both be protected. This is where data encryption proves its value, and we'll come to this topic shortly in the paper.

In a climate of increasing cyber-attack threats, organisations should regularly review their data security policies and plans. This would begin with assessing the types of data being handled and its corresponding sensitivity and value to would-be cyber-criminals. Let's look at various data types.

Data and risk – Any decision to secure your data network should be appropriate for your organisation and in line with your data types and security policy – in other words, the process is about managing any risk associated with your data being accessed by unauthorised third parties. The type of information, its value and sensitivity, traversing your network provides you with a starting point for determining whether or not you should protect the data. It is a balance between 'attractiveness' to criminals/ likelihood of attack and impact severity/potential damage from a successful attack.

Personal information and privacy – Whenever personal information is being handled it must be done in a secure manner. Aside from the decision to respect the needs of the individuals, the loss of data can have dire consequences for the public or private sector organisation to which it has been entrusted. Many countries have established laws relating to loss of data or 'breaches' (e.g. breach notification regulations), and even where such laws do not exist, you cannot assume that you are immune from litigation. In Australia the provisions of the Privacy Act 1988 apply (amended in 2012).

Commercial information – Organisations of all kinds have an obligation to protect their financial data from competitors or others who may use it for unauthorised purposes. This is particularly important if you are handling the data on behalf of others. Competitors may not hesitate to take advantage of competitive intelligence gained from the intentional or unintentional release of data.

Intellectual Property – Your IP can be the 'life blood' of your business. Mark Getty, the grandson of J Paul Getty, said, 'Intellectual Property is the Oil of the 21st century'. In today's dynamic marketplace, factors such as time-to-market and competitive-advantage can make the difference between success and failure, therefore you need to ensure that others do not take advantage of your investments and hard-earned expertise.

Data Integrity – Simply put, the critical issues in data security are the risks of damage to information privacy and integrity.

Whatever type of sensitive information is being transmitted, it is also essential that its integrity be preserved thus ensuring the data can be relied upon. The sender and recipient must know that the integrity of what is sent and received is preserved.

Whether the data being transmitted is for backup and disaster recovery, CCTV and multicast, industrial control systems, or 'rich' aggregated 'Big Data' used in business, protection of its integrity is paramount.

Data encryption technologies can render tampered encrypted data useless and harmless when it is decrypted at the time it is received.

We all have customers and stakeholders – and retaining their trust is essential. Maintaining your reputation is perhaps the single most important factor in retaining and expanding your business, or meeting your government agency charter. In the commercial arena, failure to address the impact that security breaches can have on building shareholder value is a failure in corporate governance.

It is important to understand that if your data is of potential value to others that alone makes you a possible target for cyber-attacks. The question is simple: can someone gain value (profit or harm) from this information?

The risk of technology failings – The risks are not limited to cyber-attacks. There are real risks of technology failings and errors caused by devices and technologies that can unwittingly put sensitive data into unathorised hands. If your data is sensitive, the unexpected failings of technology can have serious consequences. The risks of such technology failings (often overlooked) can include information routed to an unintended destination by a faulty router. It can be as simple as the wrong lead connected to a wrong port or a routing table error made by a network router.

However, when that data is encrypted effectively, such technology failings do not lead to serious embarrassment (at least) or even more serious damage.

The risk of time - What is potentially frightening is that the impact of a successful cyber-attack might not be known or felt for weeks or even years. The customer identity data, or the IP stolen might only be discovered years later, thus making its impact all the more devastating to the victim. In some situations organisations do not become aware that their data was stolen for some years!

THE COST OF LOSS

According to Trustwave's *'2012 Global Security Report'*, the top outcome from web or network attacks is the 'leakage of information' at 34%. This is followed by 'downtime' (24%), 'defacement' (10%) and the 'planting of malware' (9%).[4]

The costs an organisation can incur as a result of data theft and network attacks should be quantified so the benefits of mitigation can be assessed. Costs (which can be direct, indirect or hidden) are very much dependent upon the nature of the data lost and the circumstances under which the breach occurs. Each of the following should be considered when making these assessments:

- The commercial value of the data
- The legal costs around the loss of personal information
- The potential litigation defence costs
- The value of any IP risk
- The potential for fraudulent loss of assets
- The cost of any alternate protective measures
- The damages to systems
- The cost of potential data recovery
- The costs from reputation damage and loss of trust

Risk mitigation

There are a number of well-defined approaches to reducing risk. Your current business practices and processes could well mean your organisation has considered many of the guidelines below, with some already implemented. Many organisations work with independent experts for regular system intrusion and penetration testing.

But based on the identified risks most relevant to your organisation, you should certainly review each of the following:

- Intrusion detection systems (IDS) to detect hackers
- Intrusion Prevention Systems (IPS) to counter penetration attempts
- Internal access controls based on passwords or identity keys
- Encryption of all network traffic
- Access control to prevent unauthorised entry to secure areas
- Measures to discourage tailgating
- Motion detectors and/or CCTV monitoring to secure areas

At the 2012 Australian Defence Signals Directorate annual conference, delegates were informed that most government organisations should assume that they have probably had their data 'sniffed' to some degree by unauthorised third parties – and this is something that might not be discovered until years later.

This is why most organisations should strongly consider the following defense actions and capabilities:

- Identify your most sensitive data and segment your IT infrastructure
- Increase the visibility of your network activity through analytics and forensics tools
- Monitor your logs
- Encrypt your data in the most effective and efficient way possible

DATA ENCRYPTION TO PROTECT DATA IN MOTION

Organisations often spend many thousands of dollars on traditional data network security measures such as firewalls and anti-virus software, yet fail to protect their data while it is in motion over their data networks. Once the data leaves the building, it is vulnerable to attacks and outside direct control.

However by encrypting sensitive data while in motion, organisations can be assured that when data is accessed by unauthorised parties, it is useless in their possession. With best practice encryption, that data remains safe.

The down side

Many organisations mistakenly believe that any encryption of data in motion leads to huge losses of bandwidth, network performance and increased costs. But fortunately at Layer 2, this needn't be the case – encryption does not need to have a downside, as the next section examines.

Encryption methods and industry analysts

Data in transit can be protected at any of the levels within the communication subsystem; where volumes are low, software encryption based on SSL may be appropriate.

But as demands on the network increase, more efficient approaches are required, and here, encryption should be applied at either Layer 2 or Layer 3. By way of definition, Layer 2 devices such as network switches operate at the data link level (one above Layer 1 which is also known as the 'physical Layer'). Layer 3 is the next Layer up – also known as the Internet Layer, often comprised of routers or 'switch routers'.

Layer 3 encryption, more commonly known as IPSec encryption, is generally provided within the routers that are deployed throughout your data network. However, IPSec does impose a significant impact on both the performance throughput of the data network, and the effort required to manage it.

With Layer 3, overheads are typically 30-40% and while dedicated internal networks may be able to accommodate this, the use of Layer 3 encryption within and across public networks can be expensive. In effect IPSec imposes an 'encryption tax' on your data.

In practice, the higher the network speed or the greater the bandwidth requirements, the more likely it is that Layer 2 encryption should and will be used.

Due to security requirements and these network speed and performance considerations, Layer 2 encryption is increasingly being adopted globally. This is largely because, wherever the protection of data within high speed networks is required, one of the most effective approaches is to encrypt all the data at the lowest Layer possible – which is Layer 2.

Layer 2 encryption can be applied in point-to-point, meshed, and VPN or MPLS networks. The most effective form of Layer 2 encryption is provided by dedicated hardware systems that use the AES algorithm and encrypt with 256 bit keys. To ensure that these devices are secure you should always verify that they are accredited to the international security standards, FIPS 140-2 and Common Criteria EAL4. This can be checked at the following sites:

> http://csrc.nist.gov/groups/STM/cmvp/validation.html

> www.commoncriteriaportal.org/products_NS.html#NS

Industry analysts support recommendations for Layer 2 encryption.

Analyst group IDC makes a similar point about Layer 2 networks: 'A network can be secured at layer 2 without loss of performance – which remains up to 10Gbps.'[5]

CASE STUDY – STATE GOVERNMENT DISASTER RECOVERY (CUSTOMER STORY)

This Senetas customer is a state government body which provides services to health and child protection agencies. In order to ensure all their sensitive data is backed-up, the customer maintains a disaster recovery site 80km from its main data centre. This also requires regular transmissions of large volumes of data between locations. The issue was to ensure information privacy and integrity.

Challenge

Because of the highly sensitive nature of its core services and customer data being held, Senetas' government customer must ensure that all private data moving between the two sites is fully encrypted. Due to data backup requirements, network uptime is a critical consideration; so dual communications paths were required. It is also important to not adversely affect the networks' performance while encrypting the data.

Solution

The installation was based on a dual redundant path between the two sites that provided Layer 2 encryption at 10 Gbps. Importantly, each path is provisioned by a separate telecommunications carrier to reduce the likelihood of a total communications outage. While different departments within the organisation were configured to use a particular path, the use of the alternate path for backup was also fully supported.

The customer implemented Senetas' CN3000 10Gbps Layer 2 Ethernet encryptors to secure both ends of both links. The units operate at full line speed without packet expansion and allow users to take advantage of the full bandwidth of the communications links. The Senetas management system CN7, provides management of the encrypted links; allowing operators at either data centre to configure, manage, and monitor both links. The use of in-band management meant no additional data paths are required to support operations.

Benefits

The CN3000 encryptors enable our customer to fully utilise the communications networks linking the data centres. The simple 'bump in the wire' nature of the devices provided a transparent service that fully supports their requirements for a redundant efficient link.

Due to the very sensitive nature of the information, encryptor certification to international independent government testing authority standards is important.

The combination of Layer 2 network links and Senetas CN3000 encryption help ensure maximum network performance and efficient costs with minimum fuss and overhead. Additionally, the customer's selection of Senetas' independently certified CN3000 encryptors provides this government department with maximum assurance.

Signaling the increasing interest in Layer 2 encryption, this installation was viewed as a model for other government departments, which increasingly recognise the benefits of Layer 2 networking and the need to protect customer privacy and data integrity through Senetas' high-speed encryption technology.

CONCLUSION

The risks facing high-speed data networks and unencrypted data while in motion are very real and on the rise.

As information becomes one of the most valuable 'off balance sheet' assets, protection of that information and the investment in it is a paramount obligation of office-holders and management.

With that increasing asset value comes new obligations – whether specific legal obligations or a 'duty of care' to stakeholders.

Available encryption technologies help make managing these risks less complex, expensive or burdensome as they were in the past.

The signs are that customers, suppliers and other stakeholders prefer to deal with organisations that can demonstrate that their data is encrypted while being transmitted. Many organisations see it as a competitive advantage.

In South Carolina in the United States in early October 2012, it was discovered that from August 2012, overseas data hackers had penetrated the state's Department of Revenue. Personal information on 3.6million taxpayers was leaked. IT sector experts Gartner, reported that taxpayers' greatest concern was that the breach took so long to be detected – that criminals were in possession of their financial and identity records for at least 14 days.

IT analysts, Forrester Research, also reported that the data leaked was unencrypted and included social security numbers and credit card and bank account details. This is just one of numerous serious data breaches reported (and many go un-reported) every year around the world.

Where in the past organisations argued that encryption technologies were uneconomic and added an overhead to their data networks, today data encryption is mature, making cost much less of an issue. It is now also possible to encrypt data in motion without adversely impacting on data network bandwidth, speed or performance.

When current best practice data encryption technology is implemented for data in motion and data at rest, the data gained by cyber-criminals is, of course, rendered completely useless assuring no risk of adverse consequences. This is predominantly why we're seeing a widespread shift towards both encryption and Layer 2 Ethernet networks – in the Asia Pacific region along with Europe and the United States.

This whitepaper has been co-authored by Simon Galbally and Julian Fay for Senetas Corporation.

ABOUT SENETAS CORPORATION LIMITED

Senetas is an Australian listed public company (ASX: SEN), specialising in high-speed network encryption protecting data in motion whilst retaining maximum data network performance.

Senetas products are the world's only triple-certified encryptors of their type - Common Criteria (Australia and international), FIPS (US) and CAPS (UK) certification - for government and defence use and protect much of the world's most sensitive data.

Senetas secures: government information and secrets; defence and military information; commercially sensitive intellectual property; business and financial data; banking transactions; datacentre and Cloud services traffic; high volume CCTV networks; and critical industrial and infrastructure control systems.

Senetas uniquely designs, develops and manufactures in Australia. Senetas encryptors have market-leading performance characteristics and are trusted to protect data in motion in more than 25 countries.

These customers include high security organisations such as the US defence forces and Swiss banks.

www.senetas.com

1 Kroll 'Global Fraud Report', 2010

2 'Protecting Information In The Cloud', McKinsey & Company, January 2013

3 Trustwave *2012 Global Threats and Trends*.

4 Trustwave *2012 Global Threats and Trends*.

5 *Fiber-Optic Networks: Is Safety Just an Optical Illusion?'* IDC, 2009.

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