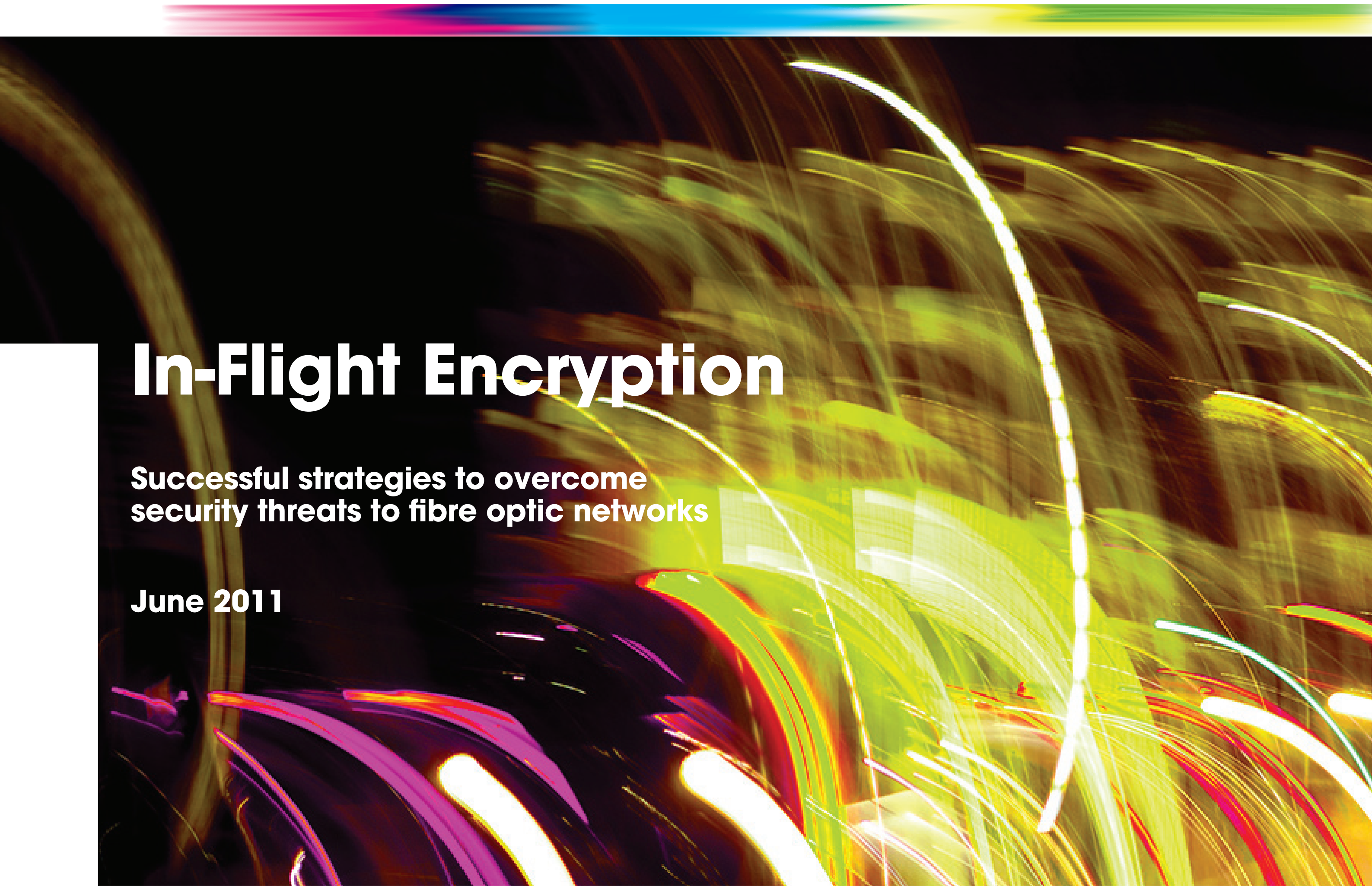
White paper

colt
smarter / faster / further



In-Flight Encryption

Successful strategies to overcome security threats to fibre optic networks

June 2011

The information delivery platform for European business

Contents

Introduction

The bigger the prize, the greater the threat. It is a simple truth, and it is also the reason why state-of-the-art fibre optic networks are attracting the growing interest of white-collar criminals.

Fibre optic networks are now commonplace. They interconnect sites in towns and cities, as well as linking sites across countries via WANs. They also form the backbone for backup and disaster recovery infrastructures using SANs.

A number of common myths have persisted however, each claiming that fibre optic networks are somehow immune from attack for a variety of reasons. However, these myths have been exposed for what they are – by a series of high-profile security breaches.

This white paper looks at the security breaches, areas of risk and successful strategies that use reliable In-Flight Encryption to protect confidential data.

> **// For a long time fibre optic cable networks were deemed to be the most secure way to transport data between different networks ... this reputation has turned out to be false. //**
>
> IDC analyst Romain Fouchereau (Fiber Optic Networks: Is Safety Just an Optical Illusion? IDC, 2009).

Security breaches – a story of escalating costs and penalties

In recent years, more companies have run into serious problems. Examples have included:

- Three main trunk lines belonging to a leading European telecoms operator being breached at an airport
- An illegal eavesdropping device hooked into an optical network used by a mutual fund company, discovered shortly before the release of their quarterly figures
- A portfolio information system for a financial services firm being compromised, potentially exposing 1.2 million records, including names, addresses, account numbers and transaction details.

Since these incidents in 2000/2003, the number and costs of vulnerabilities increased, while compliance entered the picture.

In 2008, the Identity Theft Resource Centre reported a 47% increase of data breaches. Interestingly, only 2.4% of those affected had encryption or other strong protection methods in use. By 2009, the cost of dealing with security breaches had risen sharply.

In its study **Cost of a Data Breach**, the Ponemon Institute that year estimated the cost of dealing with an incident had risen to $6.7m (compared to $1.5m in 2005). However, a security breach cost one company an astounding $31m to resolve. It was no wonder that an estimated 58% of companies in the survey were increasing their spending on encryption.

Meanwhile, enterprises and service providers have also had to abide by tougher compliance legislation – especially in sectors such as finance, healthcare, pharmaceuticals and manufacturing. SEC, HIPAA, Sarbanes-Oxley and GLBA have required that customer information must be encrypted - with fines as high as $1m per day. In addition, the Safe Harbor Act, EU Data Protection Act (Europe, US) and Data Protection and Misuse Act (United Kingdom) have sought to broaden and deepen compliance.

In 2010, the seriousness of vulnerabilities being reported was underlined by research carried out by analysts Frost & Sullivan. Looking at the global picture in Q3 of that year, researchers found that over 83% of reported vulnerabilities ranked as ‘high’ or ‘critical’ in their severity.

So what has convinced many organisations that their fibre optic networks are safe – when this is far from the case? And where do the vulnerabilities exist?

Six deadly areas of risk

There are six areas where many organisations are more vulnerable than they realise.

1) Eavesdropping can go unnoticed

It has often been believed that data in fibre optic cables are safe from eavesdropping. However, network operators' distribution boxes can be a soft target. These unprotected boxes are used for maintenance and link the individual fibre optic cables. It is easy to record and analyse the unencrypted data stream however using a bending coupler – a standard piece of kit used by technicians for testing.

This kind of eavesdropping usually goes unnoticed as it has little impact on network operations. But more sophisticated techniques **cannot be detected at all** – because they avoid direct contact with the data. Here, the light that radiates naturally from every cable is captured by sensitive photo-detectors and amplified. The data is then interpreted by data and spectral analysers. These can record, monitor and analyse the data in real time.

2) Size does not matter - any volume can be at risk

Organisations sometimes make the mistake of thinking that large volumes of data are safe from attacks because of their size. But – armed with corresponding IP numbers or keywords – certain programs can filter out information and store them in real time. These 'packet sniffer' programs record, monitor and analyse network data. In the past, it has been well documented that data traffic can be analysed this way at high speeds, regardless of whether Ethernet, Fibre Channel / FICON or SDH / SONET traffic was involved.

3) WDM networks are vulnerable too

WDM (Wavelength Division Multiplexing) networks optimise bandwidth capacity by transmitting the data streams in an optical fibre in different spectral colours. This is highly cost effective. The extra complexity does not provide protection in **itself** however. The separation of these individual channels presents no problem to an informed criminal with a spectrum analyser and optical filters (tuneable or fixed). Data can be analysed in the same way as discussed previously.

4) Complex protocols can be overcome

Storage Area Network (SAN) infrastructures are geographically separate – for disaster recovery considerations – but are interlinked to one another via a fibre channel network. However the complexity of the fibre channel protocol and the block-based data transmission used offers no added protection.

5) Dedicated dark fibre does not guarantee security

Here, the word 'dedicated' can be misleading. It does not refer to the infrastructure. Instead, 'dedicated' applies to the transmitted data, and in many cases, dark fibre connections will run across the public domain, provided for and maintained by a third party provider. This takes us all the way back to **Risk 1** we identified earlier. Worse still, rather than making the job **harder** for the hacker, it makes it **easier**. The link only transmits data from a dedicated customer, rather than a mass of different customers.

6) Signal loss is not enough of a clue

Optical monitoring tools can check the pulse of a fibre optic cable, picking up changes such as attenuation loss. This is a common method for measuring the availability and quality of the communication line. However, it is not enough to raise the alarm when something sinister is happening. This is because any attack can fall comfortably within the 0.5 and 1dBm tolerance level that optical monitoring tools use to cope with laser disparity, temperature variations and other outside influences. In fact, the very latest "non-touching" tapping technology will cause **no additional line loss whatsoever**. Put simply, signal loss is not a safe way to monitor the security of confidential data.

Successful strategies

In-Flight Encryption is the obvious solution to protect data transmitted over today's fibre optic networks. It is increasingly favoured by regulators and policy makers as an end-to-end security mechanism. However, before we look further, it is important to stress that In-Flight Encryption should be seen as a part of an **overall strategy** for security and risk management.

In-Flight Encryption from a best-in-class partner provides reliable protection from the risks outlined earlier in this document. Encryption solutions offer all-round, secure information exchange in MAN, WAN and SAN networks with 100% encryption throughput. The encryption uses algorithms with a key length of 256 bits that re-generate every few minutes. This can be combined with market-leading device architecture to stop eavesdropping and manipulation. It can meet the most demanding needs of customers in sectors where compliance and confidentiality are especially sensitive.

By following this strategy, organisations can benefit from secure and reliable connectivity – without any negative impact on performance, latency or bandwidth.

Safeguarding latency or bandwidth

There may be a common view that In-Flight Encryption causes performance and latency problems.

Many businesses rely on network Layer 3 Internet Protocol (IP) encryption. However, in case of high bandwidth (up to 10Gbps) and small packets (real-time VoIP and video), Layer 3 encryption can adversely impact the efficiency of operations.

It is possible for data transmission to take place in virtual real-time however, **with no loss of bandwidth**. Performance and latency problems can be avoided. Furthermore, available bandwidth can be utilised at levels greater than 99.9 %. The correct encryption solution can also reduce complexity, as well as any operating and administrative effort.

With the correct encryption solution at a lower layer, you can:

- Avoid a huge overhead that expands the size of the data packets and impacts operational throughput
- Keep latency under control, with impact in the order of the micro-second
- Encrypt a variety of protocols with the same encryption solution.

Flexible approaches

It is possible to deploy encryption in two forms - to suit the security needs and preferred strategies of every type of organisation.

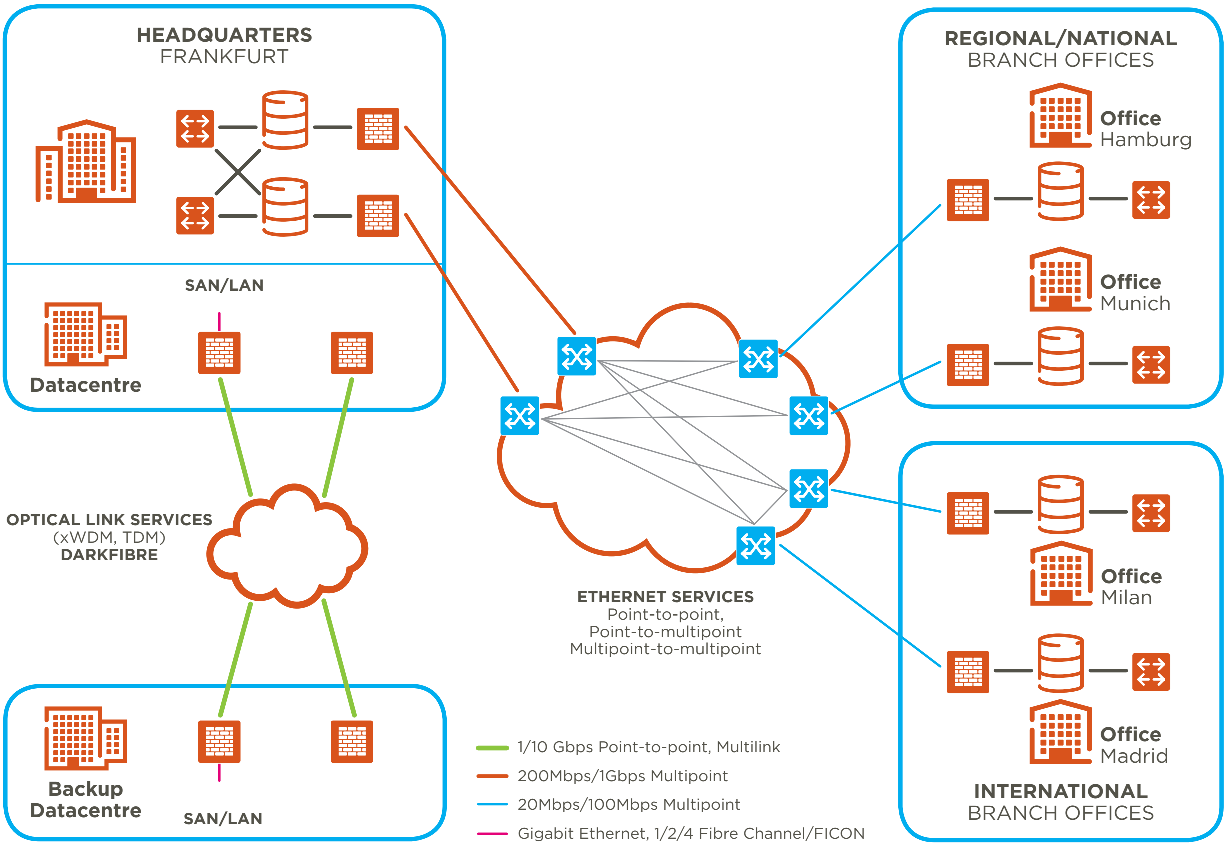
Add-on appliances for customer-owned equipment

Where a customer owns and manages their equipment, a solution provider can offer an encryption service that uses hardware to protect confidential data with the highest possible security level and quality.

This can be a leased service with a one-off installation fee for the appliance and monthly rental. The solution provider takes care of the operation and availability of the hardware.

The service can work with Point-2-Point or Multipoint encryption scenarios. Comprehensive and flexible, this approach is suitable for Ethernet, SONET/SDH, and Fibre Channel/FICON networks up to 10Gbps.

- Encryption can ensure 100% performance with no capacity reduction; added latency of <5 μs; and typical bandwidth options of 20, 100 and 200Mbps / 1 and 10 Gbps.
- It is important that any dedicated hardware appliance has the highest security design – for example meeting military-grade standards – with 99.999% availability. An appliance should also be designed for longevity and minimal maintenance. Redundant power supplies and ventilation (hot-pluggable) are also greatly beneficial.
- The service can be unmanaged (with 24-hour customer help desk) or managed with on-site support, proactive management, performance reporting and enhanced Service Level Agreements (SLAs). It may be a standalone service or linked to another solution from the same provider.

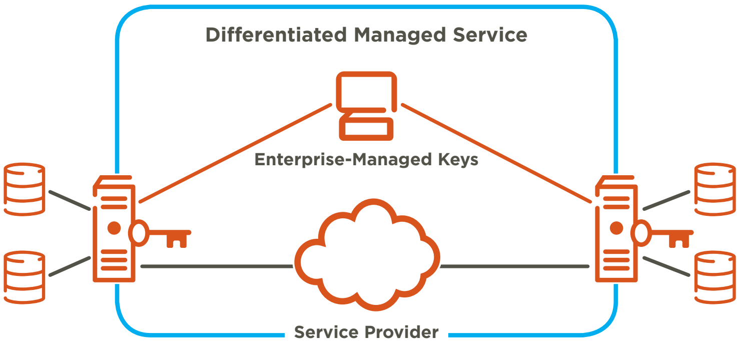


In-Flight encryption cards for managed WAN security

A card-based solution combines strong security with easy operation and administration. This plug-and-play approach affords greater flexibility. It can also be a cost-effective way to ensure reliable, multi-service connectivity across an infrastructure.

The solution can work as follows:

- The provider supplies the card and its encryption key to the customer. The provider then will manage the links and provisioning as well as their administration and performance – as with any other solution.
- The customer connects to the card via a network security dashboard that enables them to manage the issuing and close control of encryption keys, locally or remotely. Service providers manage the service; creating a separation of management between the service transport layer and the encryption layer.
- The customer also monitors the security end-to-end basis, reviewing logs and becoming aware immediately of any security alarms.
- First line support is made available by the solution provider, who manages all other tasks to maintain the service and meet the SLA.



Conclusion

In-Flight Encryption should be seen as part of a holistic approach to security.

Measures for secure connectivity should go hand-in-hand with secure business applications, secure networking (traffic filtering, intrusion detection and protection against distributed denial of service attacks) and secure communications such as IP-based voice services. By following this strategy, organisations can avoid the scenario of being caught by surprise by a sudden security breach that attracts media exposure, damages confidence and leads to serious and expensive legal ramifications.

Rather, these organisations can meet their compliance obligations (see Appendix A) in a measured, confident and cost-effective way.

The impact of such regulation is obvious: the security industry is going to have to concentrate on helping businesses ensure they are compliant with the many standards they are responsible for meeting, as well as protecting them from emerging threats not covered by those standards.

Colt Technology Services would like to thank InfoGuard and Ciena for the contribution to this white paper.

Appendix A: Impact of Regulations

Increasing national, international, and trade group regulation is forcing companies to monitor their levels of compliance continuously. For example, the Basel II financial accords and the US Sarbanes-Oxley (SOX) Act did not just impose financial regulation - they also imposed tougher information security standards throughout the financial industry.

The Payment Card Industry Data Security Standard (PCI-DSS) is a standard shared by the major credit card companies and businesses using their services are subject to yearly compliance evaluation[1]. At the time of writing, the US is considering tightening its own regulation for businesses to ensure that they keep data secure.

A rough count of compliance standards indicates that a European financial company that does business in the US is theoretically responsible for the following list of compliance standards: PCI-DSS, SOX, the Gramm-Leach-Bliley Act, ISO 27001, US State Laws, Basel II, and the national laws of that specific European country, which hopefully match with EU regulation. Health, insurance, and utility/energy companies face further regulations[2].

Even doing business in Europe only requires to comply with a number of regulations. The table below indicates the major EU regulatory legislation that companies are generally obliged to be in compliance with.

Regulation	Brief description
Data Protection Directive (95/46/EC)	Main regulation for the protection of privacy and personal data.
e-Privacy Directive (2002/58/EC)	Ensures security and confidentiality of communications over EU electronic communications networks.
MIFID (Markets in Financial Instruments) Directive 2004/39/EC	Comprehensive EU legislative framework for the establishment and conduct of investment firms, multilateral trading facilities and regulated markets.
Single Euro Payments Area (SEPA)	Initiative of the European banking industry, making all electronic payments across the Euro area (for example by credit card, debit card, bank transfer or direct debit) as easy as domestic payments.
Payment Services Directive 2007/64/EC	Legal framework enabling SEPA, as well as for better payments in all EU countries.
Basel II/III Accord	Recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision, to be used by banking regulators.
Euro-Sox Directives	Three directives on corporate reporting requirements: Fourth Directive 78/660/EEC, Seventh Directive 83/349/EEC, Eighth Directive 84/253/EEC in the process of implementation.
PCI-DSS (Payment Card Industry - Data Security Standard)	A set of comprehensive requirements for enhancing payment account data security developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global scale.

[1] "PCI Quick Reference Guide: Understanding the Payment Card Industry version 1.2" PCI Security Standards Council, 2008, p 5.

[2] Compliance Web Page of netForensics http://www.netforensics.com/compliance/