InfoGuard
and information becomes secure

White Paper

Data Security In The Converged Enterprise Network

Version 3.4

Table of Contents

1 The Evolving Enterprise Network

Enterprise networks continue to grow and evolve at a torrid pace; driven by changes in the underlying technologies, changes in business requirements and the evolution of architectures.

While fundamental drivers such as cost effective processing power, new applications and pervasive information sharing continue to grow network traffic, a changing business environment has both accelerated the pace of this growth, and driven networks to become highly geographically dispersed. Industry mergers, out sourcing, off shoring, SAN, home shoring, alliances and business continuity are but a few of the driving factors. Looking into the near future, new approaches in conducting business such as collaborative and cloud computing promise to further accelerate the growth of high throughput distributed networks.

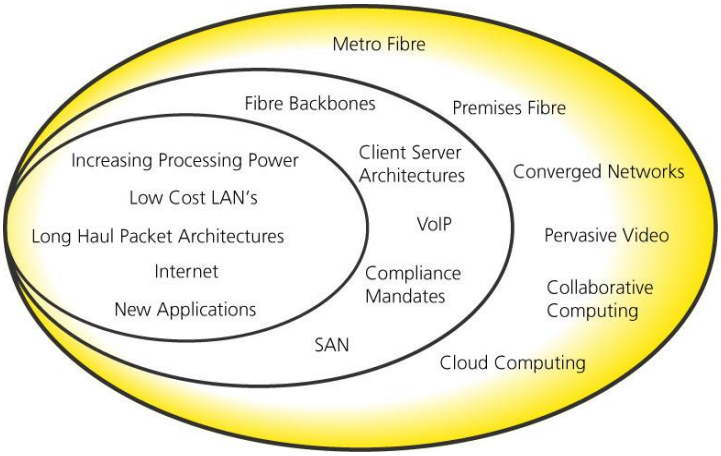

Figure 1: Drivers of Enterprise Network Evolution

Fortunately network technologies have kept pace with these demands. In the local area network the ubiquitous adoption of Ethernet has driven per port prices down sharply, while throughput has grown from 1Mbps to 10Gbps. The cost effectiveness of fibre, combined with its throughput, has provided the technology to drive tremendous price/performance improvements, initially in long haul infrastructure, and most recently in the metro area infrastructure. Modern buildings and expanding cities have been installing fibre infrastructure for years, while in other more established areas utility companies, governments, startup carriers and even traditional carriers have been making the investments to bring fibre within the reach of major customer sites. In parallel, service providers have been effectively migrating their network architectures, working to driving all forms of traffic onto a single converged IP network riding on top of the fibre infrastructure, which will yield further economic gains.

Figure 2: Comparison of Copper and Fibre Cables of the Same Capacity (Source: Corning Incorporated)

However the widespread deployment of geographically distributed networks leveraging high capacity shared fibre infrastructure, often connected across multiple service providers, brings the question of data security right to the foreground. In this paper we explore the requirements for data security in today's networks, alternate solutions to meet those requirements, deployment options and implementation resources.

2 Network Security Technical Risks: Myths and Reality

Historically network-based data security was a technology utilized only by sophisticated organizations with highly sensitive data. For instance military and intelligence organizations have for a long-time successfully used encryption devices on their network links. This attitude began to change as organizations began to commercially exploit the Internet on a widespread basis, and learned the very real security issues inherent in a shared network infrastructure. As a result, all prudent organizations today employ technologies such as SSL and VPNs to successfully encrypt and protect their valuable data in transit.

Similar risks exist in the broadband fibre networks now being deployed by enterprises. However, as with any new development, these risks may not yet be understood. Let us explore the most common misconceptions:

Myth	Reality
One of the most common misconceptions circulating in the market is the myth that fibre optic cables can not be tapped; an information relic of the early years of the fibre optic industry.	A variety of readily available commercial tools enable personnel with general technical skills and access to the fibre anywhere along its route to easily tap it (see Figure 3). These tools include some which cause no network disruptions: • Splicers: easy to use but cause a temporary disruption • Splitter/couplers: more sophisticated, but do not cause even temporary disruptions • No-touch technique: most sophisticated, and again, no disruptions
Monitoring transmission losses across the network will enable you to detect fibre taps.	The diagram below illustrates that highly effective tapping devices are available which consume less than 1% of the transmitted light, making detection impractical. Note that the costs of the taps and associated miscellaneous hardware are comparable to the standard equipment used by any software hacker.
The volume and complexity of data that exists within a fibre makes interception highly unlikely.	As discussed previously, the build out of fibre infrastructure has been substantial, producing a market for a variety of reasonably priced analysis tools. These tools are readily available, and are perfectly suited to intercepting and decoding a fibre steam. Available tools include: • Spectrum analyzers to filter out particular wavelengths • Data analyzers that can capture, record and post-process common high speed data streams, including Gigabit Ethernet, SONET/SDH and FC protocols
Leasing private dark-fibre channels is inherently secure.	Whether a channel is provisioned or dark, it will follow a similar network path, providing similar opportunities for tapping at closets, junction boxes, equipment rooms and other vulnerable locations. For long haul links the channel is likely to go through multiple carriers, and may go through different countries with different data protection norms or objectives. John Pescatore of Gartner estimates that 75% of fibre cables are publicly accessible.

Splicer: Inserts a «Y» bridge in the cable

Splitter/Coupler: Light emitted from bent cable picked up by adjacent

No-touch: Normal low-level light emitted from cable picked up by sensitive receiver

Figure 3: Common Fibre Tapping Techniques

As you can see, all of these myths are quite flawed. Like any network technology, today's fibre-based links are vulnerable to interception. The volume of data, in fact, makes those links more attractive and prized targets.

3 Network Security Business Risks

Network security exposure is a function of both technical risk, which we established above, and business risk. What are the major factors that may motivate an individual or organization to tap into your network? Based upon experience, most breaches have been motivated by one of three factors:

- Corporate/industrial/financial espionage
- Adversarial governments
- Internal personnel issues

While these types of breaches do not occur every day, there is enough history to demonstrate a pattern of risk, which is causing industry and governmental bodies to adopt preventative measures, which we will discuss below. Examples of publicly exposed breaches include:

- Discovery of an illegal fibre eavesdropping device placed on the Verizon network serving a mutual fund company, as documented in the Wolf report[1].
- Deutsche Telekom's three main trunk lines were found to have been breached at Frankfurt Airport[2].
- According to the 2007 Security Situation Report by the German BTI, "40 percent of all organizations will be the targets of financially motivated criminal attacks by 2008"[3].
- Optical taps were discovered on the networks of large pharmaceutical companies in the UK and France[4]

[1] Wolfgang Müller-Scholz , Wolf Report, "Das Schweigekartell I & II", March 2003

[2] Hacking At The Speed Of Light, SecuritySolutions.com, April 1, 2006, Sandra Kay Miller

[3] The IT Security Situation in Germany in 2007, Federal Office for Information Security, p45

[4] Fiber Optic Networks Vulnerable to Attack, Information Security Magazine, November 15, 2006, Sandra Kay Miller

[5]Credit Card Security Falters, WSJ, April 29,2008 and FTC Treats TJX Unfairly, Wright's Legal Beagle, http://hack-igations.blogspot.com/2008/03/ftc-treats-tjx-unfairly.html

- Theft of 4.2 million credit and debit card records over a 3 month period from PCI compliant Hannaford Supermarkets[5], reportedly through tapping a fibre-optic cable in the internal network
- In the 2006/2007 Security Survey carried out by the Association for Security of the Economy (ASW), 52% of German enterprises reported that they were confronted with economic espionage and tapping attacks[6]. This data aligns with popular reports of highly professional commercial hacking groups[7].
- Numerous examples of governments tapping the networks of other nations, as well as networks internal to their own nation:

  1) The US government is widely reported, in sources such as CNN, to have built the capability to tap submerged fibre cables from both last and current generation submarines[8]

  2) Illegal monitoring equipment was discovered on the Dutch and German police networks[9]

  3) The French government has tapped UK networks to gain access to top management conversation during competitive bids against French companies

  4) 14% of German enterprises reported that they are faced with espionage carried out by national intelligence services[10]

  5) The US government was discovered to have set up monitoring rooms at AT&T facilities to tap the fiber links connecting WorldNet to global networks[11]

One way to put a more quantifiable face on the adversarial government threat is to look at the narrow experience of one country. In 2004 the U.S. government reported that individuals from almost 100 countries attempted to acquire sensitive U.S. technologies, which are of course a subsector of the total threat profile. That data is roughly comparable to the 2003 data. Note that of these attempts, only 36% were made by foreign governments or entities controlled by them[12]; commercial entities and individual were responsible for the remaining attempts.

---

[6] CIO Magazine on-line, German Economy Fears Attacks on the Net, June 6, 2007, http://www.cio.de/knowledgecenter/security/836171/

[7] Theft ring accused of hacking 41 million credit card numbers, StarTribune, August 6, 2008

[8] USS Carter Will Be Able To Eavesdrop, February 18, 2005, John J. Lumkin, http://www.globalsecurity.org/org/news/2005/050218-uss-carter.htm

[9] Fiber Optic Networks Vulnerable to Attack, Information Security Magazine, November 15, 2006, Sandra Kay Miller

[10] CIO Magazine on-line, German Economy Fears Attacks on the Net, June 6, 2007, http://www.cio.de/knowledgecenter/security/836171/

[11] Stumbling Into a Spy Scandal, Wired, May 17, 2006, http://www.wired.com/science/discoveries/news/2006/05/70910; Inside The Feds Secret Wiretapping Rooms, Jeffrey Klein and Paolo Pontoniere, New American Media, September 20, 2006, http://www.alternet.org/story/41819/

[12] Annual Report To Congress on Foreign Economic Collection and Industrial Espionage – 2004, Office of the National Counterintelligence Executive, April 2005

4 Securing Your Data: The Business Perspective

Given the current environment, combined with the vulnerability and attractiveness of backbone links as targets, the era when protecting such links was considered a "nice to have" option has drawn to a close. There are a variety of compelling business reasons that IT managers are using to prioritize protection of these links:

- **Compliance.** Industry studies show that compliance with regulatory requirements is a major concern to corporate management. A broad range of regulations are currently in place with requirements in some specifically mentioning encryption, or simply implied in others. For instance:

  - Payment Card Industry Security Standard (PCI) – Applies globally to merchants who transmit cardholder data; requiring them to encrypt data across open, public networks.
  - EC Directive 2002/58, Data Protection Act 1998, EU – European community rules that require both technical and organizational protection against unauthorized access or processing of private data.
  - Gramm-Leach-Bliley Act (GLBA) – A law requiring financial institutions in the U.S. to consider whether encryption of customer financial information while in transit is appropriate. With the Federal Financial Institutions Council handbook indicating that financial institution should employ encryption to mitigate the risk of alteration or disclosure of information in transit, the burden is placed on the institution to show that encryption is not needed.
  - Health Care Information and Portability Act (HIPAA) – Requires protected health care information in the U.S. to be encrypted in transit if it is determined to be reasonable and appropriate.

  With numerous other regulations and guidelines such as SOX, Basel II and ISO 27001/27002 in place, it is clear that companies are being strongly guided to take measures to secure sensitive data in transit.

- **Due Care.** Irrespective of specific regulations, in many countries companies, and the managers within companies, are legally expected to exercise "due care" in protecting the company's assets and the information entrusted by their customers (the formal legal concept is known as "duty of care" in some countries. In other countries the legal concept is covered by the supervisory obligations of top management[13]). Should a damaging incident occur, they will not be held liable if it can be proven that sufficient care had been taken. This means you should understand the typical and prudent measures taken by other organizations, and meet or exceed those standards (for instance ensuring you meet best practices). Perhaps the best source of information for understanding typical and prudent measures is the widely read Computer Crime and Security Survey[14] issued annually by the CSI with the participation of the U.S. Federal Bureau of Investigation. In Figure 4 we see that each year a greater percentage of respondents have adopt the use of encryption technology for data in transit, with the 2008 data showing that 71% of the 521 respondents are users. This

[13] The IT Security Situation in Germany in 2007, Federal Office for Information Security, p51

[14] 2008 CSI Computer Crime and Security Survey, by Robert Richardson, p19

data reinforces the point made above, that standards have been rising quickly to encompass protection of data in transit, particularly when 3rd party and shared network elements are utilized.

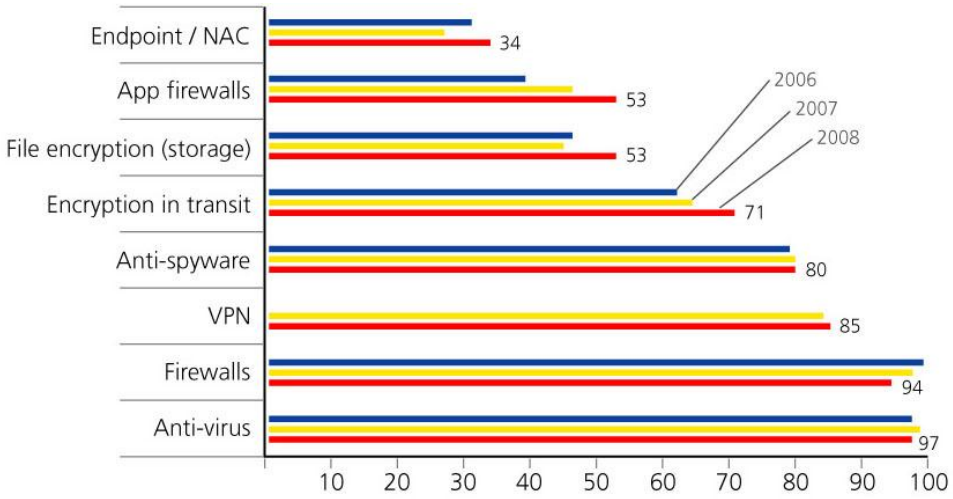

Figure 4: Data Security Measures, incl. Encryption in Transit

.

- **Financial and Reputational Risk.**
  Breaches in network security can lead to both direct financial losses, in the case where the target of the breach is proprietary information, and loss of reputation. From an overall financial perspoective, the average cost of a breach in 2007 was $6.3 million; an increase of 43% over 2005[15]. Increasingly organizations are being required by law to notify customers of security breaches. In the U.S., laws of this type are sweeping through the state legislatures at a rapid pace, with at least 43 states having enacted some form of notification legislation[16]. Other countries have similar laws, such as the EU Data Protection Directive. In today's highly competitive market, such revelations, when your company may be spending enormous sums of money to develop brands and loyalty, can be just as significant as the direct financial losses. An indication of this is the breakdown of actual costs reported by 35 breached companies participating in a 2007 study; showing 56% was due, in their cases, to revenue declines resulting from lost customer business.[17]

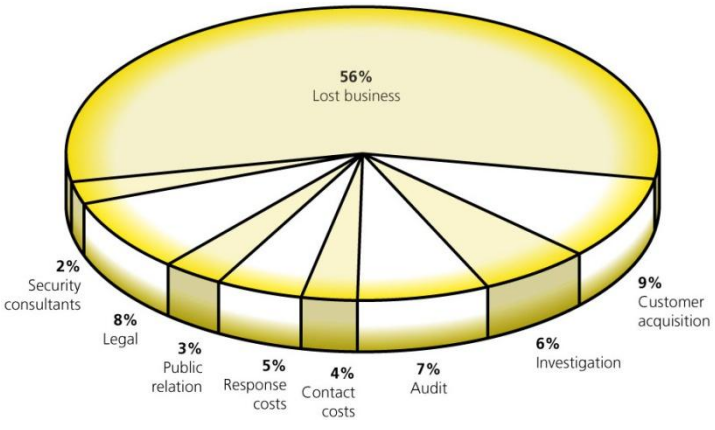

Figure 5: Percent of Total Breach Cost by Category

[15] 2007 Annual Study: U.S. Cost of a Data Breach, Ponemon Institute, November 2007, p2

[16] State of California Office of Privacy Protection, Recommended Practices on Notice of Security Breaches Involving Personal Information, May 2008, p6

[17] 2007 Annual Study: U.S. Cost of a Data Breach, Ponemon Institute, November 2007, p10

In fact, of the breached companies participating in the 2007 Ponemon study, the number one technology measure implemented following their breach was encryption.

5 Technology Alternatives

Given that best practices dictate the need to protect data on valuable network links, there are two basic approaches to encryption that can be taken. We will examine the tradeoffs inherent in each approach.

1. **Encrypting at the network link layer (layer 3)**, typically using an IPSec option in the network routers. With this option the data packet is encrypted with the encryption option and an additional IP header is added to the encrypted packet as shown in Figure 6, resulting in additional overhead which effectively shrinks the bandwidth. Disadvantages of this approach include:

   - **Introduces significantly more processing latency** (40% to 60% in independent tests), which is an issue given the trend toward converged networks that include delay sensitive applications such as VoIP, video, transactional data, synchronous data mirroring, real-time monitoring and so forth.

   - **Reduces network throughput** due to the additional encryption overhead added, as shown in red in Figure 6. This is a particularly big issue for smaller frames (64 and 128 bytes) which comprise 65% of traffic globally. For instance the typical overhead of 57 bytes added to a 64 byte frame results in incremental overhead of 47%! Also note that additional overhead and latency can be generated in the case of large frames where the L3 encryption overhead will cause additional fragmentation.

   - **At higher network speeds, throughput may be further degraded** due to the fact that the hardware is not purpose built. In some devices multiple cards can be added to attempt to overcome performance limitations; however this adds significant complexity and cost to the solution.

   - **Complex to setup and administer**. With encryption being performed within the router, at setup, and whenever the network configuration changes, security policies must be updated in local and remote routers. This may require the use of additional management software.
     Furthermore, due to the additional overhead and latency added when enabling L3 encryption, it may become necessary to introduce additional QoS schemes, adding further configuration complexity. Whenever changes are made, they will also need to be tested and verified.

The advantage of layer 3 encryption is that it can be implemented within the network router. However this typically requires one or more options to be added to the router, essentially negating this advantage.

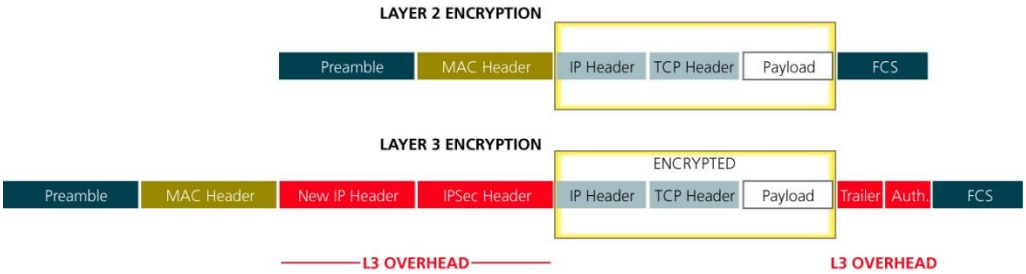

Figure 6: Comparison of Layer 2 and Layer 3 Encryption Techniques

2. **Encrypting at the data link layer (layer 2)**, typically using stand-alone encryption devices. This approach introduces no additional overhead, as demonstrated in Figure 6, there by maximizing network throughput. Other advantages include:

   - **Introduces minimal latency** (in the µs range), which is positive for all applications, but is especially necessary for real-time applications such as video, VoIP, data mirroring, real-time monitoring and converged networks which may contain these data types.

   - **Does not introduce additional overhead, maximizing throughput.**

   - **Provides support for all protocols**, providing application flexibility and enabling deployment of a single common approach to network security across the enterprise. An IPSec encryption approach only supports IP traffic.

   - Purpose built devices are used, which are designed for specific network speeds, ensuring there are **no throughput limitations and a longer lifecycle**.

   - **Easy to use**. Since purpose built independent devices are used, they are easily configured offline and installed quickly, without impacting other network equipment. There are no issues with software compatibility, and no need to deal with VPN/policy/tunneling/routing table rules and configuration.

- **Lower cost of ownership**. The cost of ownership for a L2 versus a L3 solution is comprised of differences in both upfront costs, plus the differences in on going operating costs of each solution. These will vary depending upon site specific factors such as equipment types, communications line cost and loading. However in general L2 solutions are notably lower in total cost of ownership. Although there may be some differences in the relative costs of hardware and software for these approaches, the biggest differences are in the area of operating costs. As noted above, the L3 approach is notably more complex, resulting in higher costs for installation, initial configuration, on-going configuration changes and testing. Furthermore, due to the L3 overhead, additional bandwidth may be required to maintain performance, adding incremental carrier costs.

In summary for high speed networks, layer 2 encryption provides wirespeed throughput, minimal latency, broader protocol support, less complexity and lower cost of ownership than layer 3 encryption, making it a clearly preferable solution.

6 Securing Network Traffic with Layer 2 Encryption

Although today's converging networks can result in very sophisticated architectures, Layer 2 encryption technology is available which is capable of supporting virtually all common application scenarios; enabling you to protect your data regardless of topology, carrier service or protocol. InfoGuard is one of the leading suppliers of L2 encryption solutions, and is unique in their ability to provide a family of solutions capable of supporting a broad range of network architectures, protocols and speeds. Below we review some of the most popular examples of applications selected from their customer base in over 130 countries, to illustrate the simplicity of securing sensitive network traffic.

6.1 Point-to-Point Topology

One of the simplest applications of InfoGuard's encryption devices is the ubiquitous point-to-point topology used to connect backup centers to the primary data centers, suppliers to production centers, and so forth. As we see in Figure 7 the devices are of course deployed in pairs to enable encryption and decryption of the traffic crossing the network. In the case of the InfoGuard family of encryption devices, the fibre can be enterprise owned or carrier provided, and both Ethernet and SDH/SONET interfaces up to 10 Gbps are supported for connecting to the network from the user facilities. This configuration is exceptionally easy to get up and running.

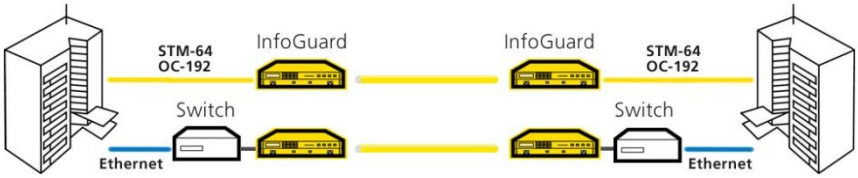

Figure 7: Typical Point-to-point Configuration

Because of the ample throughput provided by fibre connections, many users want to share these point-to-point connections among applications. InfoGuard's family of devices allow this to be done easily, as shown in Figure 8, without the need to involve another vendor, or to purchase additional encryption devices. A single encrypted 10 Gbps stream is transmitted on the fibre, with multiplexing (TDM) taking place on the client network side. InfoGuard supports a variety of client protocols, including Ethernet, Ficon and Fibrechannel, at a variety of speeds up to the capacity of the selected product. As a result the products are utilized in a wide variety of applications, including storage area networking (SAN), wide area data networking (WAN), disaster recovery and so forth.

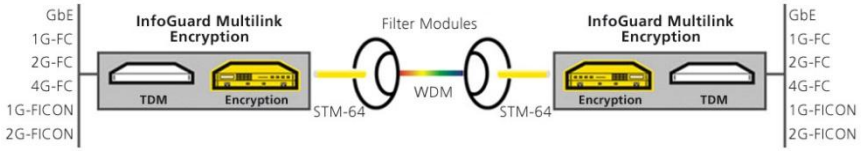

Figure 8: Typical Multiplexed Configuration

6.2 Mesh Topologies

Over the last several years carriers have begun to introduce a variety of carrier grade Ethernet services. Enterprises are migrating from their older services, such as Frame Relay, ATM and leased lines to these newer services, due to the simplicity of managing Ethernet services, the lower cost of ownership and the increased flexibility provided. Not only can increased bandwidth be easily provisioned, but the carriers are capable of supporting a variety of topologies, ranging from point-to-point, to full mesh topologies which provide complete connectivity between multiple end points; supporting multiple virtual connections at each end point. Although point-to-point deployments still predominate, point-to-multipoint, and full mesh topologies are significant and growing faster, as they provide improved connectivity at a lower cost; for instance allowing a headquarters location to connect to all branches (point-to-multipoint), or all divisions of an enterprise to connect with each other (full mesh).

Figure 9 shows a typical example. InfoGuard devices are placed between the user/network interfaces to provide encryption, similar to the point-to-point topology. Note, however, that only a single device is required at each location, although each location is connected to all other locations, providing significant savings in hardware and operational cost. A variety of services such as dark fibre, WDM, EoMPLS, VPLS or VPWS can be utilized at various throughput levels to provide the necessary connectivity, allowing you to select the appropriate service for your needs. As in the point-to-point case, the flexibility of the InfoGuard devices allows support for a wide variety of applications ranging from campus or metropolitan area networking (e.g. connecting suppliers to a nearby factory) to WAN.

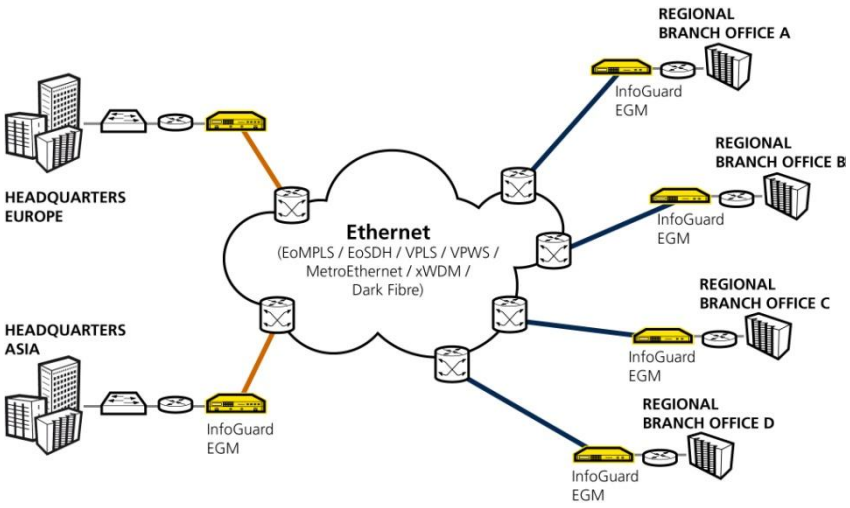

Figure 9: Typical Mesh Configuration

7 The InfoGuard Solution

InfoGuard is one of the leading suppliers of L2 encryption devices, providing the support needed to analyze your requirements in detail, and recommend the appropriate solution. InfoGuard is a member of the Crypto Group of companies, which employ over 300 security experts supporting over 130 companies globally. Since 1952 the group has been producing world class encryption equipment in Switzerland, long known as a secure global expertise center for encryption technology. This track record of financial and technical security places InfoGuard in a unique position as a dependable global supplier of L2 encryption solutions.

In order to support the full range of applications reviewed above, InfoGuard provides three lines of encryption products; Ethernet, SDH/SONET and multiprotocol. An overview of their functionality is provided in Figure 10.

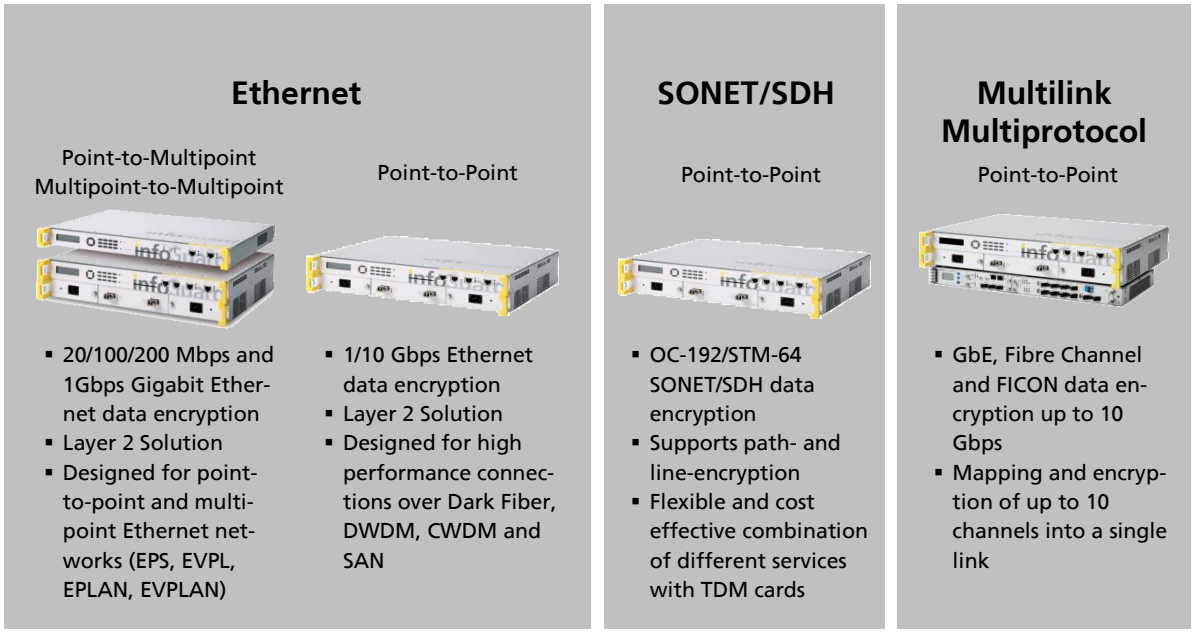

Figure 10: InfoGuard Encryption Product Line Overview

All the products provide a variety of common features designed to make the devices highly secure, easy to setup and manage:

- Selectable 128/256 bit AES encryption
- Automatic key generation via random number generator and key distribution via Security Card or inter-unit management
- Automatic key exchange/update without link loss at selectable time intervals
- Secure local and remote management
- Audit and event logging
- A MTBF greater than 50,000 hours, with dual hot-pluggable power supplies and fans

The products are supported by a customer support center which operates 24x7 to ensure your critical data is never at risk.

To begin your project it is recommended that you consult with InfoGuard's experienced staff of application specialists who will work to design the optimal solution for your needs, develop an implementation plan, and support your organization throughout implementation.

8 Conclusion

In this paper we have established that:

- Virtually all enterprises of significant scale employ a wide variety networking connections containing sensitive data
- This data is vulnerable from both a technical and business perspective
- The current business environment not only supports, but requires sensitive data be protected in transit
- The most effective means of protecting this data is with Layer 2 encryption
- Layer 2 encryption devices are available that support all common application scenarios
- InfoGuard is an experienced provider of Layer 2 encryption devices with the product line breadth and support infrastructure which will enable you to secure your data quickly and effectively
- InfoGuard has the track record of business success to become a reliable long term partner to your organization

You are invited to obtain more information by:

- Visiting InfoGuard's web site at http://www.infoguard.com
- Emailing InfoGuard at info@infoguard.com