Government Insights
An IDC Company

Worldwide Headquarters: 7600 Leesburg Pike, East Building, Suite 310, Falls Church, VA 22043, USA P.703.485.8300 F.703.485.8301
www.government-insights.com

SMART 2007/0005

Survey and Analysis of EU ICT Security Industry and Market for Products and Services

D.7.3 Final Study Report
The Evidence Base - Supply Analysis

IDC Government Insights

April 2009

SMART 2007/0005

Survey and Analysis of EU ICT Security Industry and Market for Products and Services

D.7.3 Final Study Report
The Evidence Base – Supply Analysis

The opinions expressed in this Report are those of the authors and do not necessarily reflect the views of the European Commission.

Author(s)	IDC European Competitiveness and Innovation Expertise Centre – Government Insights
Deliverable	7.3 Draft Final Study Report: The Evidence Base – Supply Analysis
Date of delivery	April 30 2009
Version	1.0
Addressee officers	Gerard Galler European Commission Information Society & Media DG Unit A3: Internet; Network and Information Security Office BU33 05/087, 33 Avenue Beaulieu, B-1160 Bruxelles Tel: +32 2 299 93 55, e-mail: gerard.galler@ec.europa.eu
Contract ref.	Contract Nr 30-CE-0150192/00-00

TABLE OF CONTENTS

P

1. Introduction **1**

2. The Supply Side of the NIS Market **2**

Overview 2
Organization of the Supply-side: description of the offering 3
The Hardware Market 3
The Software security Market 5
The Security Services Market 8
Classification of the Main NIS Vendors 11
Main Vendors Ownership 14
Classification of Main Suppliers by Size 16
Competitive Maps of EU NIS Suppliers 19
Perceived key success factors 22
Perceived barriers to market development 24

3. The EU NIS Market structure: Maturity and Concentration by cluster **26**

The EU NIS Market Clusters 26
The EU NIS Market Concentration by Cluster 28
NIS Market Concentration Indicator: Cluster 1 29
NIS Market Concentration Indicator: Cluster 2 31
NIS Market Concentration Indicator: Cluster 3 32
NIS Market Concentration Indicator: Cluster 4 33
EU NIS Market Concentration: Conclusions 35

4. Supply Chains and Emerging Business Models **37**

Main Supply Chain Models 37
Security products for end users 37
Security for professional users 38
Emerging Business Models for the Business Market 39
Emerging Business Models for the Consumer and SOHO Market 41

5. International NIS Markets Description **43**

The US NIS Market 43
The Role of Regulation 44
The Socio-economic Context 45
The Japan NIS Market 45
The Role of Regulation 47
The socio-economic Context 48
The Asia-Pacific NIS Market 49
The Role of Regulation 52
The Socio-economic Context 53

6. Conclusions **54**

Key Supply Side Trends 54
General Conclusions 56

7. Methodology of supply analysis **57**

LIST OF TABLES

		P
1	Advanced NIS taxonomy: Security Hardware	4
2	Advanced Market Taxonomy: Security Software	5
3	Advanced Market Taxonomy: Security Services	9
4	Main Suppliers by Type and Geographical Market Scope	12
5	Main Suppliers by Type of Ownership	15
6	Classification of Main NIS Suppliers by Size (Headcounts)	18
7	The EU NIS Market segmented in clusters	27
8	EU NIS Market Concentration Indicator Scale	29
9	USA Total Security Market 2005- 2007 M$ (% of total market)	43
10	Japan Security Market M Yens	45
11	APAC Ex-J Market Size M $	49
12	List of Suppliers	58

LIST OF FIGURES

		P
1	Advanced NIS taxonomy: Security Hardware	4
2	Advanced Market Taxonomy: Security Software	6
3	Advanced Market Taxonomy: Security Services	9
4	Competitive Map of NIS Software Suppliers	20
5	Competitive Map of NIS Hardware Suppliers	21
6	Competitive Map of NIS Hardware Suppliers	22
7	EU NIS Market: Revenues by Functional Market Segment and by Cluster, 2007 M€	28
8	Cluster 1 Market Concentration Indicator (combined market share of top 5 vendors, in %, 2007)	29
9	Cluster 2 Market Concentration Indicator (combined market share of top 5 vendors, in %, 2007)	32
10	Cluster 3 Market Concentration Indicator (combined market share of top 5 vendors, in %, 2007)	33
11	IT Security Business Model for the Business Market (Vendors are on top, users are on bottom)	40
12	Home User and Soho Business model (Vendors to Client - Top Bottom description	42

1. INTRODUCTION

The focus of this study is the Network and Information Security Market in the EU27. This report is part 3 of the Final Study Report (**Deliverable 7.3: The Evidence Base: Supply Analysis**) produced by IDC EMEA for the study "Survey and Analysis of the EU ICT Security Industry and Market for Products and Services" on behalf of the European Commission, DG Information Society and Media.

This report presents the detailed results of the Supply Analysis, on the basis of interviews with main suppliers and desk research. These data represent part of the evidence base used to reach the conclusions and recommendations of the study. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

The other components of the Draft Final Study Report are:

- **D.7.1 – The EU NIS Market: Scenario, Trends and Challenges**, which presents the overall NIS market scenario, the main conclusions and recommendations of the study, and the set of indicators proposed to monitor the market. This report is addressed to policy makers and main stakeholders.

- **D.7.2 – The Evidence Base: Demand Analysis**, which presents the detailed results of the business and consumer demand analysis. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

- **D.7.4**: **The Evidence Base: Critical Issues Analysis,** which presents the detailed results of the qualitative analysis of the main critical issues for the development of the NIS market, carried out on the basis of desk research and interviews with a selected sample of stakeholders. This report is addressed to the security market experts and all parties interested in the in-depth analysis of the results.

2. THE SUPPLY SIDE OF THE NIS MARKET

Overview

This chapter presents the main results of the analysis of the supply-side of the Network and Information Security market in the EU 27. The main goal is to present the competitive scenario of the supply-side, based on interviews and desk research (for more details see Methodology chapter at the end of this report). This chapter describes the suppliers strategic positioning, the marketing mix, key success factors, and the main development trends of the offering.

The Internet world is characterized by high levels of insecurity, which have increased with the rapid diffusion of broadband connectivity. Virus attacks, spam messages, phishing (fraudulent messages trying to steal personal data) are just some of the many disagreeable issues Internet users are forced to endure simply by being online.

To fight against Internet threats (and global IT vulnerability), the IT industry developed a full range of solutions that are now organized in a structured market. But it is important to understand that these solutions, features and technology can only reduce risk exposure and mitigate the impact of attacks. None of the IT security vendors can claim to offer full safety.

By nature, the IT world is made of unfinished software (that needs to be patched because of hidden vulnerabilities), open systems (that enhance communication between individuals rather than limiting exchanges), anonymous users (the Internet allows any user to generate his/her own identity, or use a stolen one) and unprotected wealth (it is often said that in the IT world, Information is the currency, but is poorly protected).

The only way to achieve full Security in the IT world would be to use closed systems. Defense and military systems are often built in such a way, with closed, non-connectable systems, governmentally approved users, closed mono-task software, protected by full secrecy (and even these systems may be breached if sufficient effort is made).

This means that e-mail and Instant Messaging, On-Line transactions, multiple task Operative Systems and applications, social networks, mobile tools, are, by design, totally insecure.

Because of this, the supply-side of the security market is generally very fragmented with players who focus their expertise on key issues such as Identity Management, Threat Mitigation and Compliance solutions.

No single vendor is capable of addressing the full spectrum of security issues, primarily due to the fact that the investment in skills required to develop such a broad range of products is prohibitive. Vendors often

target one or two, often complementary, issues such as Anti-Virus and Anti-Spam or Identity and Compliance.

As a second factor leading to fragmentation, IT security clients often do not wish to depend on a single vendor for all their security needs. They prefer multiple vendors procurement that will limit risk exposure (limited chance that all vendors fail in the same moment). They also need strong confidence and trust in their suppliers, based on their specific knowledge for specific application areas. This situation leads to a supply scenario with multiple layers of vendors of security solutions.

When considering their basic security needs they often take the view that implementing products from multiple vendors (the so called "best of breed" approach) will eliminate the risk that a catastrophic failure of a single product or suite of products will totally expose their information assets.

In addition, these users often need to have developed a high level of confidence and trust in a supplier before buying from them. Taken together, this can lead to a situation where IT security is composed of multiple layers of products from multiple vendors.

The disadvantage of this approach is that it makes effective, centralized management of the security environment very difficult without further investments in management and monitoring solutions.

Organization of the Supply-side: description of the offering

The NIS offering is divided in three main functional markets, that is hardware, software and services. The following paragraphs describe the advanced taxonomy of the products and services falling in these three functional markets. Different suppliers also dominate them.

Business Availability services, software and hardware are included in the analysis but only for the business users market segment. This includes back up and recovery applications. The software and services areas include respectively network security software and services which apply to fixed and mobile infrastructures, (including wireless connections such as WiFi, Radio-frequency Identification (RFID), and data protection). Physical security systems are excluded from the scope of this study.

The Hardware Market

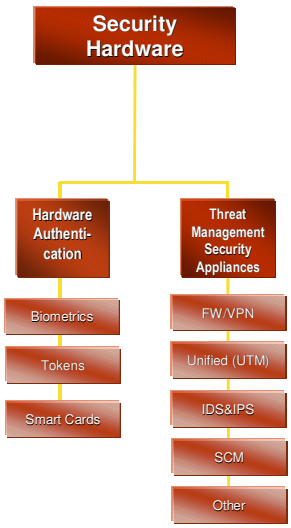
The security hardware market is a niche market, dominated by Cisco. The most important product category is constituted by Threat Management Security Appliances**.** They are network based security systems (called appliances). They are usually made of a specific server (independent Power, independent chipset) loaded with an expert Security software. The combination of specific server with specific software allows very high performances when it comes to email

security (filtering), Firewalling (filtering) or remote access. It also allows high availability and high scalability.

Major players in this field besides Cisco (the Network Company) are Fortinet and Sonicwall

FIGURE 1

Advanced NIS taxonomy: Security Hardware



Source: Government Insights, 2008

TABLE 1–

Advanced NIS taxonomy: Security Hardware

Hardware Authentication	It includes the hardware token market, such as the token authentication server, USB authentication tokens, software licensing authentication tokens exc.
Threat Management Appliances	in the majority of the situations, theses market replicates the software market taxonomy. It offers combination, of Software (Dual Mode – Triple mode) embedded into a specific Hardware. The vast majority of security appliance deal with Threat management on a dual mode basis (Firewall + VPN). A new product generation called UTM (Unified Threat Management) gathers 3 features in the same box (Firewall, Antivirus and Network based Intrusion Prevention system).

Source: Government Insights, 2008

The Hardware Authentication products are very small security appliances with very limited storage capability for encryption keys (Tokens). Major players in this tokens field are RSA and Gemalto.

Cisco has a strong foot-print across the EU, but there are also local vendors (Netasq, Astaro) active in some national markets. Local players aggregate OEM (Original Equipment Manufacturers, that is third parties) technologies, which brings a fluctuation in cost of production, so they enter the market with a limited break-even product portfolio.

As a leader, Cisco embeds acquired technologies, which limits the production cost fluctuation. Cisco enters the market with a break-even portfolio and can assume price flexibility.

The Software security Market

IT security solutions (*Figure 2 and Table 2*) are mainly software solutions that can automate security processes. They can be delivered throughout a license when they are pure software, throughout an appliance when they need to be positioned in the infrastructure, or as a service (in the emerging scenario of "cloud computing"). The following paragraphs describe the main product categories of security software.

TABLE 2

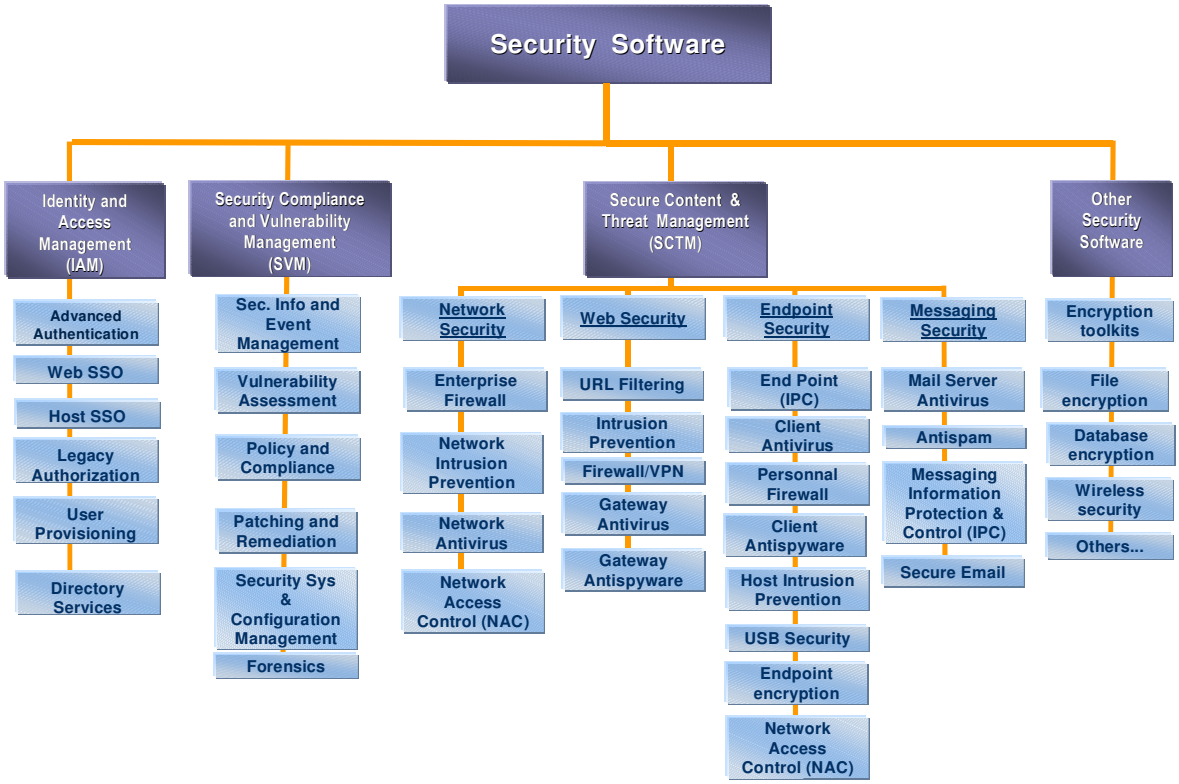
Advanced Market Taxonomy: Security Software

Identity and Access Management (IAM)	Identity and access management (IAM) is a comprehensive set of solutions used to identify users in a system (Home user, employees, customers, contractors, and so on) and control their access to resources within that system by associating user rights and restrictions with the established identity.
Security and Vulnerability Management (SCVM)	Security compliance and vulnerability management (SCVM) software is a comprehensive set of solutions that focus on allowing organizations to determine, interpret, and improve their risk posture.
Secure Content and Threat Management (SCTM)	SCTM products defend against viruses, spyware, spam, hackers, intrusions, and the unauthorized use or disclosure of confidential information. Products in this market are offered as standalone software, software married to dedicated appliances, and hosted software services. They are further segmented in: Network Security, Web Security Endpoint Security, Messaging Security.
Other Security Software	It covers emerging security functions and some of the underlying security functions, such as encryption tools and algorithms, that are the basis for many security functions found in other software and hardware products.

Source: Government Insights, 2008

FIGURE 2

Advanced Market Taxonomy: Security Software



Source: IDC, 2008

Note : IAM, SCVM, SCTM and OSS are the main areas of security coverage where technology faces threat for mitigation and remediation.

Identity and access management (IAM)

The Identity and Access Management (IAM) market is relatively narrow with IBM presenting strong market domination. Main vendors are IBM, Novell, Oracle, HP, CA, Sun Microsystems, RSA, Entrust.

This area of security requires vendors that have a great deal of experience in IT systems, and only the major IT players can benefit from such a high level view. Behind IBM there are major international and global players such as EMC, CA, Verisign, and Oracle. Only Bull SAS is visible in Cluster 2 as a regional player.

Secure Compliance and vulnerability management (SCVM)

This market includes vulnerability detection applications (around 5000 software vulnerabilities are detected in commercial software every year). Compliance tools are a combination of Analysis tools and reporting tools. SCVM vendors must have specific tools and experience for Software analysis at any level (Server, Desktop), strong

vulnerability database and effective patching process. Main vendors are usually the same then in SCTM : Symantec, McAfee, Trend Micro.

On the compliance side, legal and reporting capacities are important. Compliance operations can rarely be automated as they are process oriented. These processes are applied at different levels in organizations, mainly outside the IT department. Major organizations tend to outsource some compliance driven operations (log management, Intrusion detection) to external partners in order to find savings. Most compliance software are advanced checklist or reporting tools with the goal of fulfilling a compliance audit. Symantec dominates this market for the same reasons as previously described.

The Secure Compliance & Vulnerability Management is also a narrow market, which is dominated by Symantec. This market grows rapidly but is threatened by the shift to services.

Secure content and Threat Management (SCTM)

This market covers Threat mitigation and systems remediation at any level (Network, Desktop, Laptop). SCTM vendors need a very wide network of probes (private or shared) to collect samples all over Internet. They collect theses samples and need very strong analysis capacities (Virus analyst) before releasing patch and remediation tools. SCTM vendors are based on Network capacities (for sample collection and patch distribution) and Skills (they very often use local universities to co-educate students). Availability and reactivity request them to be organized 24-7 365 days per year. They usually set laboratories around the world to keep " follow –the sun" skills available.

Main vendors are Symantec, McAfee, Trend Micro, Cisco, Fortinet, Websense, KasperskyLabs, Norman, Sophos, F-Secure, Eset, Bit Defender, AVG, Alwill, Panda (see fig.2)

SCTM is a wide market where vendors compete for second position behind the market leader Symantec that is the market leader across the entire region. The major competition to Symantec comes from McAfee and Trend Micro.

Eastern Europe presents a strong regional competition to Symantec with ESET, AVG and Bit Defender, each demonstrating a strong local challenge, although they are unlikely to obtain the position of market leader.

Symantec dominates the SCTM market for the following reasons:

- Symantec has a long history in the security market, with a very strong brand name and extensive marketing activity across the region.

- Symantec's local presence across the region at a country level is very strong.

- Symantec covers a wide area of information protection, including data security, data protection, data backup and recovery.

- Symantec uses a specific and very strong brand name for the consumer market – i.e. Norton.

The agility of vendors in Clusters 3 and 4 is due to:

- Local SCTM companies mostly rely on local universities for advanced skills and lab cooperation

- ESET, Bit Defender and AVG use their strong relationship with neighboring universities.

- Local vendors are usually supported by local governments, which usually become major clients

- Governments tend to favor local vendors.

Other Security Software

This market is made out of very narrow expertise as Encryption. In this field, local competition is visible from Utimaco, Safenet, EMC-RAS. Main vendors are Utimaco (acquired by Sophos in 2008) and Safenet.

The main reasons are:

- In the field of local encryption, markets are always very fragmented and local players are often very influential.

- As encryption covers many governmental needs, local governments for strategical means prefer local players. Building public offering on top of Governmental products, these vendors can rapidly gain local market footprint.

The globalization of a vendor's offering in the encryption field does not seem to be possible due to these local considerations.

The Security Services Market

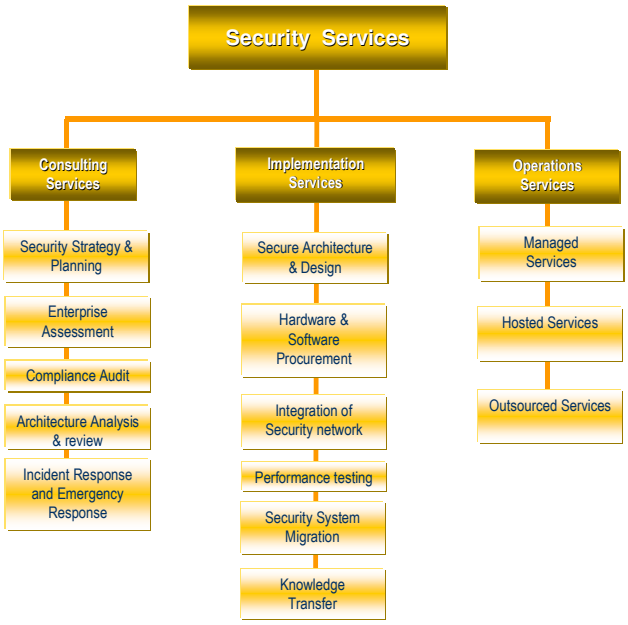
The security services market is in rapid growth, driven by the evolution of demand towards increasing maturity. Given the high level of connectivity, some users require "in the cloud " security where the network embeds security processes. In the field of services, players do not invent technologies or solutions; they mainly implement, manage and maintain them on behalf of their clients (*figure 3 and table 3*).

Major players in this field are IT Services firms, System Integrators and increasingly telecommunications operators. In recent years telecommunication operators have made considerable inroads into the market, starting with relatively simple offerings that complemented their basic connectivity services, but quickly expanding their offerings to include more advanced services and managed services.

These players are particularly well placed to address the small and medium enterprise market, due to their extensive installed base of basic connectivity services in this segment, but have also being making an impact in the large enterprise segment. In general, neither the systems integrators nor the telecommunications operators will offer security services as a stand-alone offering, but will more often bundle security with other services.

FIGURE 3

Advanced Market Taxonomy: Security Services



Source: IDC, 2008

TABLE 3

Advanced Market Taxonomy: Security Services

Consulting	Security strategy and planning, Assessment, Compliance Audit, Architecture, Analysis and Review, IR and Forensics
Implementation	Design, HW & SW Procurement, Integration of Security Architecture, Performance Testing, Transition/ Migration, Knowledge Transfer
Operations (Education included here)	Managed Security Services, Hosted Services, Outsourced Services

Source: Government Insights, 2008

The offering and delivery of security services is quite varied.

Delivery centers for outsourced or managed services are usually manned by skilled, high level engineers. Security outsourcing can consist of remote management of devices (Firewalls, Intrusion Detection Systems) or fully hosted solutions which can include physical and environmental security issues. Many players who offer managed or outsourced security services use standard products from leading vendors on which to base their services, although in-house developed solutions are also used to provide specific functionality

Consulting and implementation services are aimed at helping users understand the threats and risks they face, developing a plan for how to address these issues, guidance for developing a security policy, advice on which technologies to implement and assistance in installing and configuring security products, as well as integrating them within the existing IT framework.

Education and training is the smallest part of the market. It consists usually of technical training (Training and certification) for Security teams, user training regarding security policy and recognition of security threats.

In Security Services, Consulting Services, Implementation and Operations are the largest functional markets that are highly fragmented and highly competitive. The largest segment is Consulting, followed by Implementation.

This fragmentation results in many local players operating within the market. Even if IBM (through IBM Global Services) can be considered as a leader, each European region sees local players among the top rankings.

Local Telco started became increasingly important in 2005 and have captured increasingly visibility since then.

Some local, narrow system integrators also reach top five ranking, due mainly to:

- Market capillarity: local players are better at covering territories. They often represent global brand names and serve the clients as local partners.

- Standardization of skills and education allows local partners to reach the best technical levels at the closest client's level. Global vendors often rely on these local skills to distribute their solutions without local cost.

Proximity generates trust in the security field especially amongst SMEs and consumers.

Classification of the Main NIS Vendors

According to IDC research, the EU 27 NIS market includes at least 88 vendors (of which the main 30 vendors have been profiled for this study). Amongst the 88 active vendors:

- 42 are based or headquartered in the EU 27
- 40 are based or headquartered in the US
- 2 are based in Japan
- 1 is based in Norway
- 1 is based in Israel
- 1 is based in India

This classification by country of origin gives very little information about the real market fragmentation. Most of the suppliers active in the security market are, at least, multi-regional and act in a minimum of two neighboring countries. The country in which a company's headquarters are based means little, compared to yearly revenue streams and market shares. Nevertheless, we can conclude that within the EU 27 there is certainly a critical mass of local vendors.

More specifically:

- US based and non-EU vendors tend to be positioned in multiple markets. For example, IBM is positioned in the software market and services market, with multiple functional market positions.
- Symantec is only positioned in software, however, its coverage is very wide.
- EU-27 based vendors tend to focus on a single market (e.g. Bit Defender, ESET, and AVG cover no more than two or three sub-functional markets) and develop a real in-depth expertise.

The main typologies of suppliers can be classified as follows depending on their main offering and business strategy:

- Specialised Vendors, whose main business is the IT security market (chief among them Symantec)
- Global IT vendors (Cisco, IBM and others) also active in the IT security market
- IT service providers and system integrators (e.g. Accenture)
- Telecom Operators, ISP (Internet Service Providers), ASP (Application Service Providers) who are oriented to the provision of network information security solutions and services.

The following table presents the 30 main suppliers active in the EU and profiled by this study by type and by geographical market scope, showing where in the world and in the EU they are active.

TABLE 4

Main Suppliers by Type and Geographical Market Scope

Supplier Type	Name	HQ base	Geographical Market Scope	
			World	EU
Specialised Vendors	Alwill	CZ	No	Europe
	AVG	CZ	No	Europe
	Bit Defender	Romania	All	Europe + OEM partnership
	ESET	Slovakia	No	Europe + USA
	F-Secure	Finland	All	Europe + Nordics + WW Agreements with ISP (Saas)
	Kaspersky Labs	Russia	All	Western Europe + Former CIS countries + OEM agreements WW
	McAfee	US	All	All
	Norman	Norway	All	Nordics + WW OEM partnerships
	Panda Security	Spain	No	Euorpe + Iberics + Spanish World (Southern Americas)
	Symantec	US	All	All
	Sophos	UK- US	All	Europe, USA, APAC
	Trend-Micro	Japan	All	All
Global Vendors	Cisco	US	All	All
	HP	US	All	All
	IBM	US	All	All
	Microsoft	US	All	All
IT Service providers and System Integrators	Accenture	US	All	All
	Atos Origin	FR	All	All

TABLE 4

Main Suppliers by Type and Geographical Market Scope

Supplier Type	Name	HQ base	Geographical Market Scope	
			World	EU
	Cap Gemini	FR	All	All
	CSC	US	All	All
	EDS	US	All	All
	Fujitsu Services	JAP	All	All
	Siemens	Germany	All	All
	Tieto-Enator	Fin.	No	Europe-Nordic Countries
	Verisign	US	All	All
Telecom operators, ISP, ASPs	BT	UK	All	All
	CompFort-Meridian	Pl	No	Mainly Poland and Eastern Europe
	DT	D	No	EU, USA, APAC - Selected countries due to network terminations.
	Gity	CZ	No	Czech Republic and neighboring countries
	ICZ	CZ	No	Czech Republic and neighboring countries
	Magyar	Hu	No	Hungary and neighboring countries
	Telecom Italia	I	All	Focus on Europe- Extended countries due to network terminations
	Telefonica	E	All	Focus on EU- Extended countries due to network terminations
	Telia-Sonera	Sw	No	Focus on Europe- Extended countries due to network terminations
	Verizon	US	All	All

Source: Based on reports and estimations – IDC 2008

Main Vendors Ownership

The Typology of ownership is the key differentiator between local and international players on the market.

- Symantec, IBM, McAfee, CA, Trend Micro, HP, and Cisco are examples of US, Japanese and Indian vendors which are all listed on major stock-exchanges.

- Telcos (BT, Deutsche Telecom, Orange, Magyar) are all public companies, as are some smaller service players such as Risc Group

- In the European extended security world, only F-Secure (Finland), Norman (Norway) & Gemalto (NL) are public companies.

- In 2007, Sophos (UK) attempted an IPO. The operation was postponed due to the impact of the sub-prime crisis. Later in 2008, Sophos acquired Utimaco, a Major German exprt in Encryption solutions.

- All the other EU-27 originated companies (BitDefender, AVG, Mkt-Virus, Alwill, ESET, GFI) are private, often funded by local or regional partners.

By being fully privately own, EU-27 players can only self-finance their growth and future development - or external contribution (VC's).

This situation limits their development capacities. As an example, Kaspersky Labs reinvests the totality of its net margin. IDC estimates the net margin for Kaspersky Labs at 10 %, which is a generally accepted margin level in this industry. Reinvestment capacity is also considered as being very low.

They force these players for a better agility, a smarter Cooperation and many coo-petition situations. This situation explains why EU based vendors are more agile in alliance, partnerships and joint operations.

Meanwhile, publicly listed companies can rely on investment from the stock exchanges and whilst they must remain compliant with various laws & regulations, such as quarterly reporting, private companies do not have this obligation.

TABLE 5

Main Suppliers by Type of Ownership

Supplier Type	Name	Type of Ownership
Specialised Vendors	AVG	Private
	Bit Defender	Private
	ESET	private
	F-Secure	Public
	KasperskyLabs	Private
	McAfee	Public
	Norman	Public
	Panda Security	Private
	Symantec	Public
	Sophos	Private
	Trend-Micro	Public
Global Vendors	Cisco	Public
	HP	Public
	IBM	Public
	Microsoft	Public
IT Service providers and System Integrators	Accenture	Public
	Atos Origin	Public
	Cap Gemini	Public
	CSC	Public
	EDS	Public
	Fujitsu Services	Public
	Siemens	Public

TABLE 5

Main Suppliers by Type of Ownership

Supplier Type	Name	Type of Ownership
	Tieto-Enator	Public
	Verisign	Public
Telecom operators, ISP, ASPs	BT	Public
	CompFort-Meridian	Private
	DT	Public
	Gity	Private
	ICZ	private
	Magyar	Public (Now T-systems- DT)
	Telecom Italia	Public
	Telefonica	Public
	Telia-Sonera	Public
	Verizon	Public

Source: Based on reports and estimations – IDC 2008

Classification of Main Suppliers by Size

When it comes to comparing company headcounts, it is obvious that international companies based in the US, Japan and India rank as the main enterprises. Most of the EU based vendors are mid-sized companies (between 250 and 500 employees) after having been in business for 10 years (e.g. Sophos, Netasq). The following table presents the 30 profiled suppliers by size.

The youngest or very focused companies are definitely in the "Small" category, with less than 250 employees. Systems Integrators and telecommunications operators, who have only relatively recently started to offer extensive security solutions are exceptions to this rule.

The main reasons for this situation are;

- Security solutions require highly skilled people, which usually means small teams – these skills are in relatively short supply and

are expensive to obtain, which means most operations remain relatively small.

- European-based security companies are relatively young and the founders usually come from the local universities from which they recruited friends and other co-founders. These small and very united teams often support the first decade of company's life.

- Delivering software requires less resource than delivering a service - especially in the fields of consulting and implementation.

- Leveraging a company with thousands of employees requires a stable income. Market consolidation sees most of these young companies being acquired before reaching critical mass. For example: EDS acquired Vistorm (UK), Verizon acquired Ubizen-Cybertrust (Belgium), BlackSpider (UK) was acquired by SurfControl, later acquired by Websense. However, this is not a solely European issue, as there are some notable examples of European companies acquiring small, but well known, US security companies. The most obvious examples are BT's acquisition of California-based Counterpane, and Getronics' (now part of KPN) acquisition of Texas-based RedSiren. Both of these acquisitions were intended to strengthen the acquiring firms capabilities in managed security services.

- Public SME companies tend to stay independent due to their capital dilution. For example, F-secure in Finland or Norman in Norway.

TABLE 6

Classification of Main NIS Suppliers by Size (Headcounts)

Supplier Type	Name	Large Suppliers (over 500 employees)	Medium Suppliers (250-500 employees)	Small Suppliers (less than 250 employees)
Specialised Vendors	Alwill			X
	AVG			X
	Bit Defender			X
	ESET			X
	F-Secure		X	
	Kaspersky Labs	X		
	McAfee	X		
	Norman			X
	Panda Security			X
	Sophos	X		
	Symantec	X		
	Trend-Micro	X		
Global Vendors	Cisco	X		
	HP	X		
	IBM	X		
	Microsoft	X		
IT Service providers and System Integrators	Accenture	X		
	Atos Origin	X		
	Cap Gemini	X		
	CSC			
	EDS	X		

TABLE 6

Classification of Main NIS Suppliers by Size (Headcounts)

Supplier Type	Name	Large Suppliers (over 500 employees)	Medium Suppliers (250-500 employees)	Small Suppliers (less than 250 employees)
	Fujitsu Services	X		
	Siemens	X		
	Tieto-Enator	X		
	Verisign	X		
Telecom operators, ISP, ASPs	BT	X		
	CompFort-Meridian			X
	DT	X		
	Gity		X	
	ICZ		X	
	Magyar (T-Sytemes / DT)	X		
	Telecom Italia	X		
	Telefonica	X		
	Telia-Sonera	X		
	Verizon	X		

Source: Government Insights, 2008

Competitive Maps of EU NIS Suppliers

Summarizing the considerations presented, it is possible to draw the competitive map of the NIS suppliers by functional market (software, hardware and services), because this allows to highlight the main variations between vendors' core business and competitive factors.

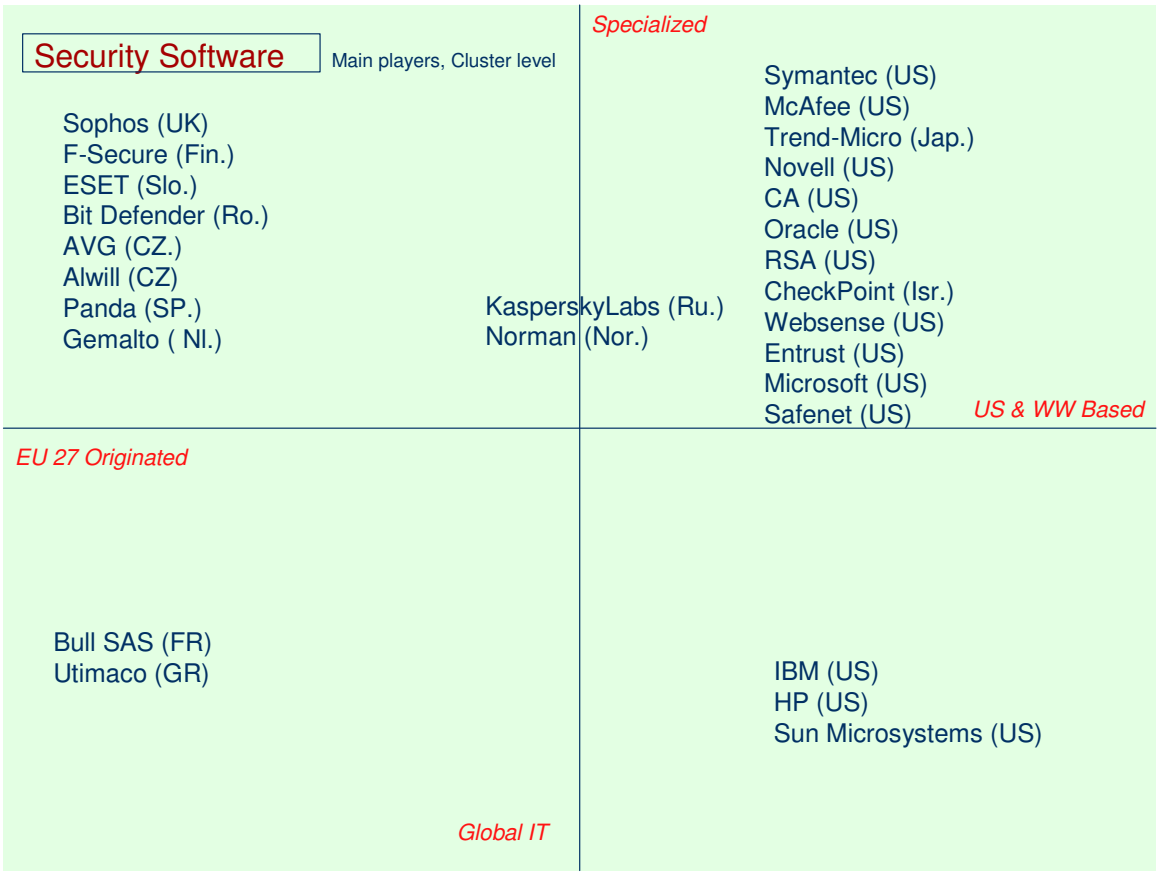
The following figures shows the Competitive Maps for software, hardware and services. The Maps are structured along two main axes, which are the following:

- **Geographical Origin of the vendors and market scope**: EU vendors with an European market scope, against global vendors with a worldwide market scope. Moreover, as indicated above, most EU players have a narrower scope than global security vendors, who in turn dominate most national markets.

- **Offering Portfolio**: focus vendors specialized in the security market, against global players active beyond security in other ICT market segments.

FIGURE 4

Competitive Map of NIS Software Suppliers

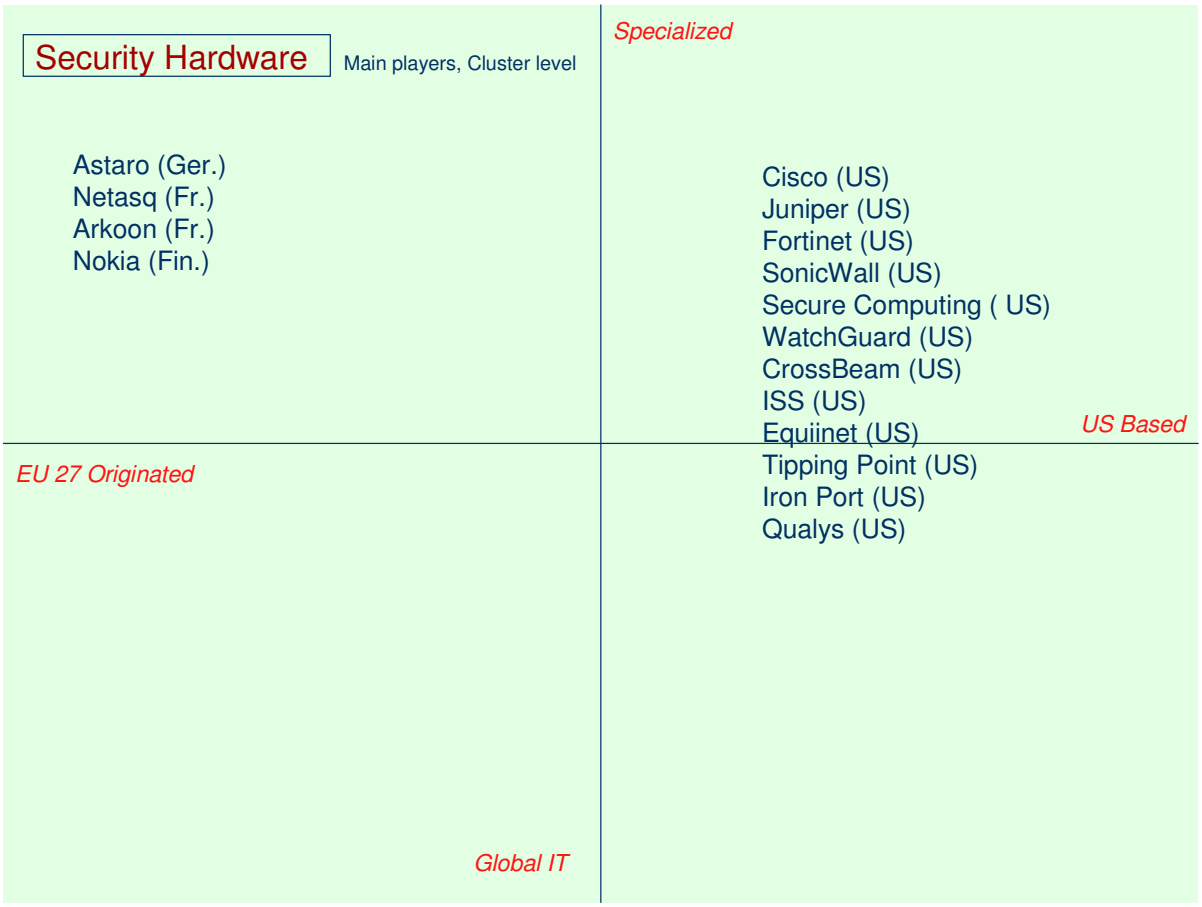


Source: IDC Government Insights, 2008

In the Security software market (Figure 4), it is obvious that WW vendors are more numerous. Nevertheless, it is important to monitor the importance of EU 27 Vendors. During the last 3 years they gained credibility and market footprint.

FIGURE 5

Competitive Map of NIS Hardware Suppliers



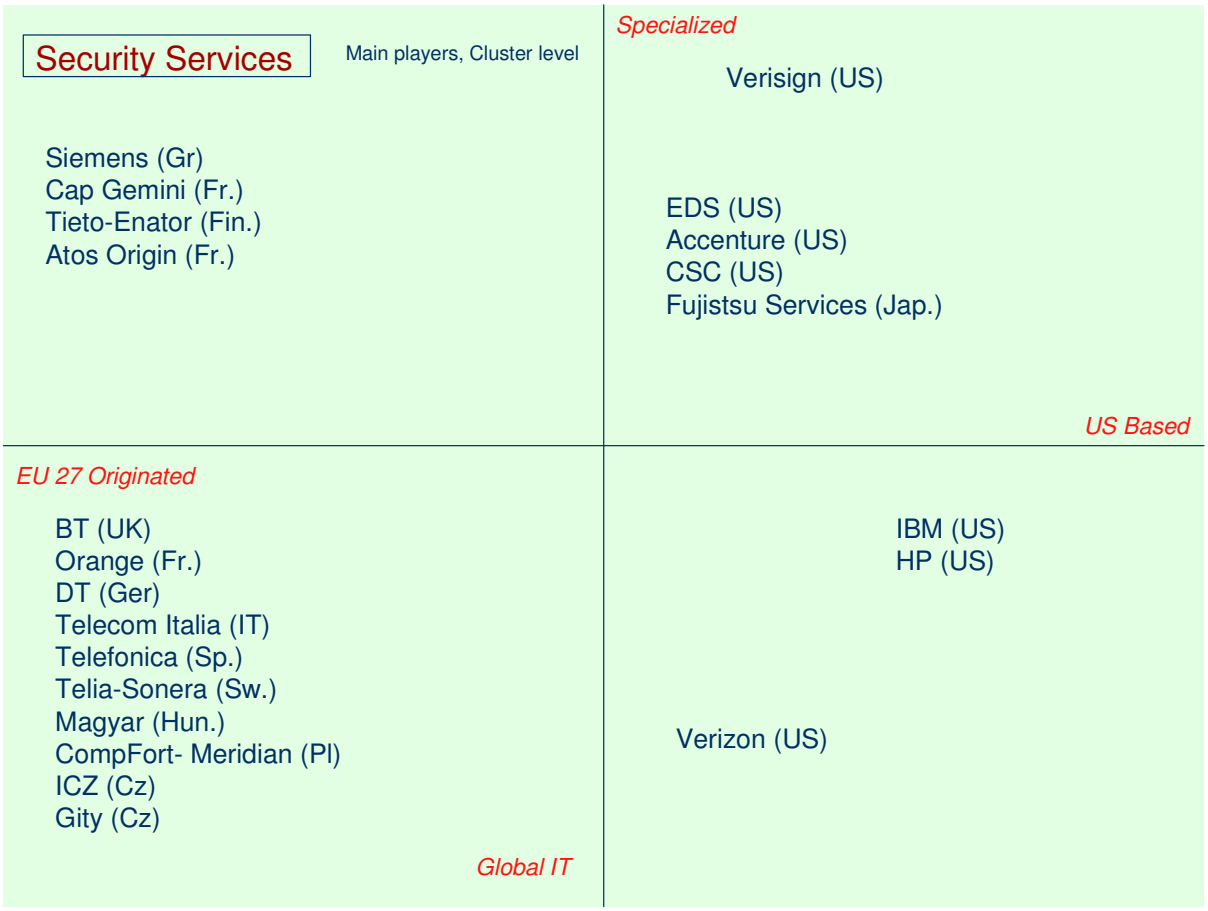
Source: Government Insights, 2008

In the Security Hardware market (*Figure 5*), vendors are mainly based outside EU 27 area. Security hardware market is a very skilled market where vendors must invest massively in research. EU 27 vendors are a small number; due to the fact the competition for mature technology markets is very hard.

In the Security Services market (*Figure 6*), competition is widely open. EU 27 vendors (Telco's and System Integrators) can rely on local connection with end-users.

FIGURE 6

Competitive Map of NIS Hardware Suppliers



Source: Government Insights, 2008

Perceived key success factors

In the IT Security field, as in many other markets, success is measured by market share increase and the growth rate of Yearly revenues, but not only. For example, EU 27 based vendors qualify success on profitability (after 5 years, after 10 years…), top contracts and partnerships.

Key success factors for market penetration, in order of importance are:

- Highly skilled research and remediation teams

No matter who the vendor is, or what the price points of the products are, their expertise in providing effective security solutions, as perceived by the market, is a key success factor. Failure of products and associated breaches of the security defense capabilities will generate an immediate loss of credibility. Possessing the skills to, as far as possible, prevent these breaches and provide effective remedial support in the event of a breach is a critical consideration for any security vendor.

- Proven experience in, and public awareness of, threat mitigation to develop trust

It is also important that successful vendors be seen to be making a public contribution to the fight against security threats. Generally speaking, when a vendor discovers a breach or a vulnerability, this is reported to the press. Once or twice a year many vendors also publish a security report summarizing these issues and the actions taken. These public relations operations are important for user organizations because they demonstrate the vendor's capacity to understand the threats being faced and offer remedial action.

- Strong marketing capacities to fight against commoditization and competition. Brand awareness is also very important.

From the end-user perspective all Anti-Virus products are basically the same. They offer protection form known threats, but cannot offer protection from unknown threats. Consumers and business users tend to avoid technical comparisons between vendors based on expert analysis. Rather they increasingly seek the best trade-off between price and features. As a consequence of this commoditization price becomes one of the main elements of differentiation for anti-virus products. Successful vendors need strong marketing capacities and funds to gain visibility and protect its market value and brand name. Failure to do this would mean competing in a price-focused, commodity market with little room to generate added value for clients.

- Effective Management of Multiple Channels To Market

Many of the best-known names in the security industry have customers ranging from individual consumers to large enterprises and governments. Managing these multiple channels– including on-line distribution, retailers, value added resellers and global systems integrators - and a mix of direct and indirect selling models, is a core strength. Often these vendors will rely on global Systems Integrator (SI) partners for access to large enterprise and government accounts. In these accounts, security technology may often be purchased as an element of a larger IT project, and the influence exerted by these global SI's on the buying process is of major importance. Strong relationships with a number of the major global SI players are a key business success factor.

Smaller, local players are generally dependent on their local reputation and smaller channel partners within their home geographies. In many cases they will be forced to focus their business on the consumer and small and medium enterprise segments of the market, and may not have the breadth or depth to effectively address the large enterprise segment directly. Generally, addressing this market segment means developing partnerships with large systems integrators, but effectively managing these relationships and gaining visibility with the partner is a major challenge for small vendors, and an extra cost that many cannot support.

- Investment capacities for new areas of coverage (acquisitions or R&D)

The IT security market is not innovative in terms of developing new, in-depth defensive solutions. Anti-Virus and Firewall products have been using the same basic technologies for decades with major updates every 18 months or so. In general, the IT security industry develops more new features than technologies. Global vendors generally do not do fundamental research in the area of security, rather they acquire new solutions and technologies that are then integrated into existing product sets. This approach greatly speeds up their time-to-market for new features.

Being able to acquire ready-to-launch technologies is a key advantage compared to the usual life-cycle of R&D. In this way global companies can be agile enough to rapidly address new areas of need.

In contrast, smaller, local players have little choice but to enter into co-opetition agreements to gain access to new technologies. These Original Equipment Manufacturer (OEM) agreements allow them, for a fee, to integrate the technology of other vendors into their products. For smaller players this can be a very costly option, but developing the required technology in-house would usually be prohibitively expensive. In addition, these OEM agreements can bring benefits by providing smaller players with access to larger clients through the association with a major player.

Perceived barriers to market development

In technical terms, much knowledge and expertise is freely available and access to effective technologies at a reasonable price point is possible. In general the main technologies (threat mitigation, and data protection) can be obtained at a competitive price and sometimes, via open source, for free.

Partnerships, cooperative agreements, technology sharing and OEM practices are common and the dominant positions that some vendors have achieved in specific market segments is mainly due to effective marketing and sales investments.

From a vendor perspective, access to skilled resources remains a key issue, and broadly speaking, skilled security specialists are in relatively short supply in the EU region. Technical standardization (e.g. IP, ISO) gives European vendors a good opportunity to build a an organization with the required levels of skills, and Universities and academic institutions are able to deliver student with standard, recognized qualifications. However, despite this competition for skills remains robust, and particularly in less mature markets smaller and local companies must often take individual steps to meet their skills needs.

Examples of this are Bit Defender (Romania), ESET (Slovakia) and AVG & Alwill (Czech Republic) – all of whom have set up dedicated

programs with local universities to generate a sufficient level of skilled personnel to meet their business growth needs. Without these programs it is unlikely that these companies would have been able to sustain their market positions in the face of international competition. For security vendors in less mature markets, where skills may be in relatively short supply and international competition growing, these sort of initiatives, aimed at increasing the pool of available talent, should be recommended and can be seen as best practices.

Overall, smaller security vendors within the 27 member states generally lack the financial resources to extend their Research & Development capabilities or market coverage. However, this situation is a straightforward result of a highly competitive market situation, and cannot be considered an unfair barrier.

3. THE EU NIS MARKET STRUCTURE: MATURITY AND CONCENTRATION BY CLUSTER

The EU NIS Market Clusters

The level of maturity of the EU IT markets varies considerably and this affects the structure and the evolution of the NIS market. This chapter analyzes the main variations of the NIS market supply scenario by dividing the 27 EU Member States in 4 main groups (clusters) with broadly similar levels of IT spending, security market size and trends, and level of maturity (*table 7).* This division in clusters was developed for the business demand and scenario analysis, particularly through the NIS Market Maturity Synthetic Indicator by cluster (*refer to D.5.1 Draft Final Study Report: The EU NIS Market Scenario for more details*). The focus of the supply-side analysis is on the level of concentration by cluster, that is the market share controlled by the top 5 vendors, and the balance between EU and global vendors in each cluster. According to the study results and the NIS Market Maturity Indicator the EU NIS market can be divided as follows:

Cluster 1 – The Champions includes the Scandinavian countries, the Netherlands and the UK (20% of the EU population), well known as the most advanced IT and service-based economies. Very High NIS Market Maturity characterizes this cluster.

Cluster 2 – The Pillars includes the most important continental EU countries, plus Ireland, which are the pillars of the EU economy (representing 34% of the population and 42% of EU GDP in 2007). These countries are almost as advanced as Cluster 1 from the point of view of IT development. Cluster 2 presents High NIS Market Maturity.

Cluster 3 – The Runners Up is composed by Southern European countries (Italy, Spain, Portugal and Greece and the more technologically advanced of the new member States, that is the Czech Republic, Hungary and Slovenia, plus Cyprus. They represent 30% of the EU population and 26% of GDP. This Cluster presents a Growing NIS Market Maturity level.

Cluster 4 – The Learners is composed by the remaining New Member States. Their revenues represent only 2% of the overall EU NIS market, even if they represent 5% of the EU GDP and 16% of the population. This cluster presents a Low NIS Market Maturity level.

The NIS market structure is evolving from a dominance of software to a dominance of services, even if software revenues are expected to remain relevant. This reflects a growing maturity, as services reflect a more advanced and sophisticated approach to IT security than basic software solutions. A major shift to Security as a Service is visible in all clusters and markets. This shift is driven by a demand-side need to reduce the complexity of security operations and the scarcity of staff with a sufficient level of security expertise. This trend is particularly

strong in Clusters 1, 2 & 3. The nature of the market for security as a service and the need for trust and confidence in the supplier mean that local European players are able to gain visibility and build market share. Currently, all markets appear to be fair and free for effective competition.

The security market split, between hardware, software and services, varies considerably between Clusters 1&2 and Cluster 3&4 (*figure 7*). In Central and Eastern European countries, the weight of the hardware segment is much higher than in the rest of Europe. The main reasons for this difference are that the growth in hardware solutions is faster and are preferred by Central and Eastern European governments (Cluster 3 & 4) for control and centralization. Also, security services are complex for local VAR (Value added resellers) and system integrators to implement.

Similarly, less mature markets are those where IT investment has been lower, often due to less well developed industrial and business practices, and where availability of leading IT products and services was low or non-existent. Over time, as these markets grow in maturity, spending shifts towards a less product led scenario, to a more services-led scenario. In the security market, this trend has also been observed, but shows peculiar variations, particularly concerning security services, which in many respects are a newer offering than traditional security products (e.g. anti-virus and firewall products).

Interestingly, within the 27 EU countries, even the less mature markets demonstrate a relatively high level of services spending, which may be indicative of an accelerated maturity path. In many instances (particularly when there is a direct comparison available with economic neighbors), less mature markets will take advantage of the newest offerings in technology and services to "leapfrog" the traditional development curve. However, the investment in Hardware needed to build the basic IT/security infrastructure remains.

TABLE 7

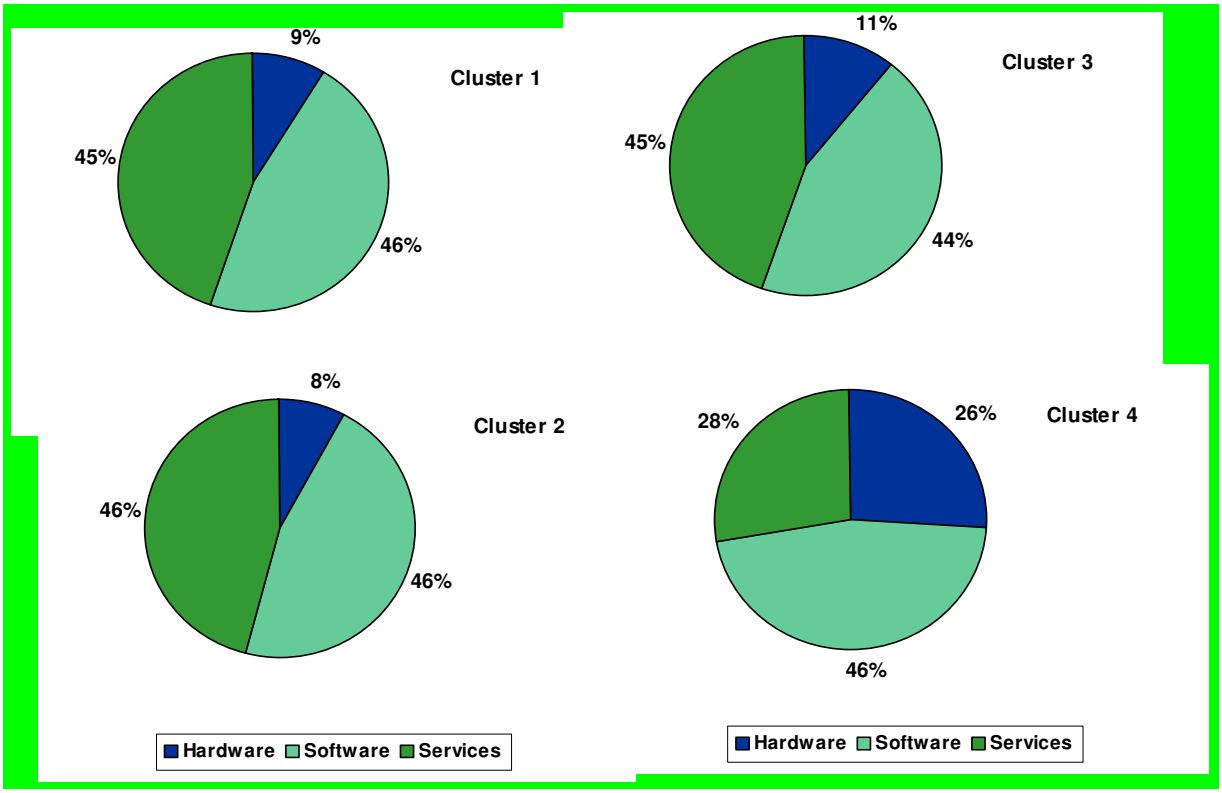
The EU NIS Market segmented in clusters

CLUSTER 1 – THE CHAMPIONS	CLUSTER 2 – THE PILLARS	CLUSTER 3 – THE RUNNERS UP	CLUSTER 4 – THE LEARNERS
Denmark	Austria	Cyprus	Bulgaria
Finland	Belgium	Czech Republic	Estonia
Netherlands	Luxemburg	Hungary	Latvia
Sweden	France	Greece	Lithuania
UK	Germany	Italy	Malta
	Ireland	Portugal	Poland
		Slovenia	Romania
		Spain	Slovakia

Source: Government Insights, 2008

FIGURE 7

EU NIS Market: Revenues by Functional Market Segment and by Cluster, 2007 M€ (%)



Source: Government Insights, 2008

The EU NIS Market Concentration by Cluster

One of the goals of this study was to analyse the level of market concentration or fragmentation. For the purposes of this report, Market Concentration is defined as the combined market share of the Top 5 vendors in a specific country or Cluster. The EU NIS Market Concentration Indicator is calculated on a scale where concentration starts when the top 5 vendors control more than 35% of the market revenues.

The Market Concentration Indicator shows that the 5 top vendors (Symantec, IBM, McAfee, Cisco and Trend Micro) had 20% of the EU NIS market in 2007: this means that the market is fragmented and open to competition by a wide range of security providers, both global and European players. According to our analysis, this is positive since users across the EU have access to any security technology or service needed.

TABLE 8

EU NIS Market Concentration Indicator Scale

Degree of Concentration	Top 5 Vendors Market Share
Highly concentrated	< Than 50%
Concentrated	From 35% to 50%
Fragmented	From 20% to 35%
Highly Fragmented	Under 20%

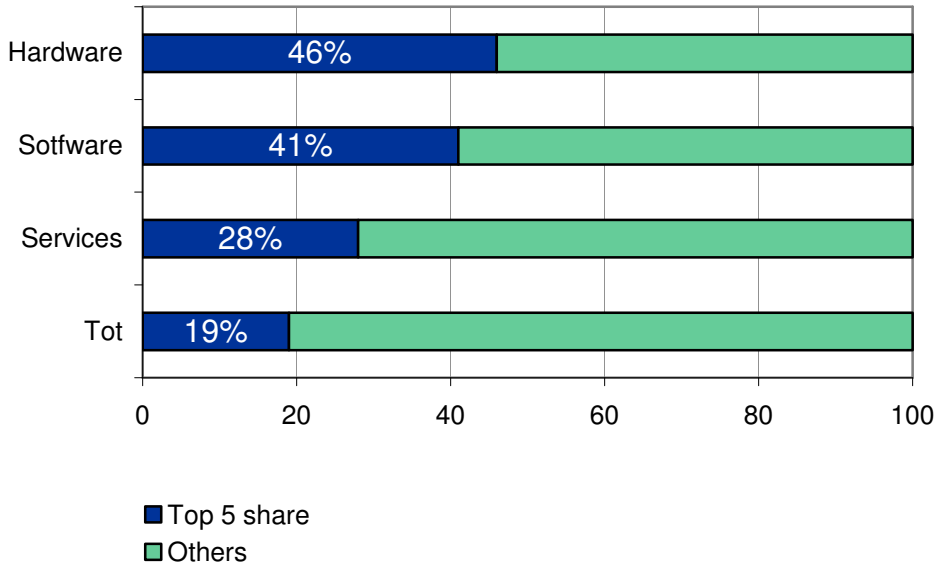
Source: Government Insights, 2008

NIS Market Concentration Indicator: Cluster 1

In terms of the overall Security market, Cluster 1 can be classified as Highly Fragmented. The combined market share of the Top 5 vendors in 2007 was 19%. In 2005, the Top 5 vendors accounted for 22.8% of market share, indicating that market Fragmentation has increased. In Cluster 1, the Security Software market is concentrated but has been subject to increasing fragmentation since 2005 (48,6 % market share for Top 5 Vendors in 2005 compared to 41,3% in 2007). The security Hardware market is concentrated, corresponding to a general trend in security hardware markets. Finally, the services market is fragmented.

FIGURE 8

Cluster 1 Market Concentration Indicator (combined market share of top 5 vendors, in %, 2007)



Source: Government Insights, 2008

There are many factors behind this decrease of concentration. The growth in end-user mobility and the use of mobility-enhancing devices such as laptop computers etc., coupled with a growing penetration of broadband network access in the EU27 countries, has meant a larger dispersion of the end-user population. This increasing mobility requires more sophisticated and agile security solutions to counteract the security threats inherent in a mobile lifestyle. These solutions will often involve hardware, software and services.

Market maturity and the generally high levels of competition coupled with organizations' willingness to switch vendors provide good opportunities for new players to gain a market foothold. With the right product and value proposition new players can build market share.

As is the case in other clusters, the Top 5 vendors in this cluster differ from the Top 5 across the whole region.

Market fragmentation is generally most visible in the "Others" section of the market, outside the Top 5. Here many new entrants and very small vendors are active, and gain market share at the expense of the market leaders. In general, the positioning strategy of these vendors is to offer the same features and functions at a lower price point.

In the hardware segment, the market leader, Cisco, has been steadily gaining market share since 2005 (from 16 % in 2005 to 25.9 % in 2007). Cisco's dominance and its ability to increase its market share by leveraging its huge installed base of network equipment is a leading reason for this level of concentration. Netasq (France) is also gaining some market share (from 0.7 % in 2005 to 5,9 % in 2007), however, all of the other players in the Top 5 have lost market share in the same period.

In Cluster 1, as in all other Clusters, the Security Services market is fragmented. Many vendors share the market space and there are no dominant players. Services delivery is often characterized a "local" market with many small players active solely in a single geography, leading to generally high levels of fragmentation.

The security Services market will stay fragmented for the following reasons. A scarcity of skills in the Security Services field leads to polarization in the market, with large vendors attracting some resources, while others remain with smaller, niche players. This effect, which we call the "Boutique Effect", means that very small companies (10 – 50 employees) with highly skilled staff (CISSP-ISACA-SANS-ISO Lead Auditor personal certifications), can compete effectively with larger players in specific areas of security services (e.g. strategy, policy development, security architecture, compliance)

The security services market is built on trust and strong vendor-client relationships. Smaller firms in particular are more likely to turn to local partners for security services. This creates an opportunity for local security players, contributing to the development of a fragmented market.

Home users very often turn to their ISP or telecommunications provider for basic on-line security offering. This also contributes to market fragmentation, giving more choices to final users, and making it easier for them to shop around for the lowest cost provider.

NIS Market Concentration Indicator: Cluster 2

The Cluster 2 NIS Market is characterised by a 21% share of the top 5 vendors in the total market and an increasing level of fragmentation. In the last 3 years, the combined market share of the Top 5 vendors (Symantec, McAfee, Trend Micro, IBM and Thales IS) has decreased appreciably from 28,34% in 2005 to 20,7% in 2007.

As in Cluster 1, competition from new entrants in the Software field and high levels of fragmentation in the Services field has driven this change. In terms of vendor dominance, Symantec has lost considerable market share in this period (from 13,7 % total Cluster Market Share in 2005 to 8.5 % in 2007).

Symantec's loss of market share in Cluster 2 is a prime example of how new, European players have been able to gain market entry and build share at the expense of the market leaders. The competitive challenge to Symantec began with the entry of European based vendors: Sophos, Panda Software, Eset, AVG, Bit Defender and a Russian player, Kaspersky Labs. Kasperky Labs based all its European operations in Germany and started very aggressive market shares acquisitions in the home-user market with major success in France and Germany and key retails partnerships.

The Security Software market in Cluster 2 is concentrated with the Top 5 vendors having a combined market share of 38.5%. Fragmentation has increased rapidly over the last 3 years – in 2005 the Top 5 vendors had a combined market share of 53.1%, with Symantec decreasing its dominance.

The Security Hardware market in Cluster 2 is cncentrated with a combined share of top vendors of 41.6%. Market leader Cisco, with 22.1% market share in 2007, has held this position relatively unchanged in the last 3 years.

Two local vendors from France appear in the group of Top 5 players:

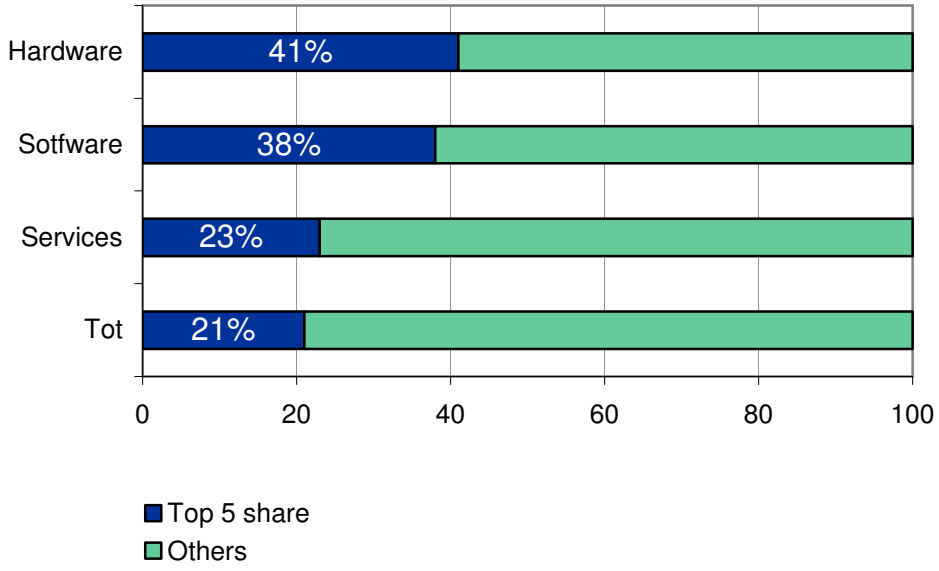
- Arkoon (France) had a market share of 1,9% in Cluster 2 in 2007, but this is down considerably from its position in 2005 when, it had a 4,3% share.

- Netasq (France) had a 3,1% market shares in 2007, showing little change from its position in 2005.

The Cluster 2 Security Services market is fragmented and this has changed little since 2005. The Top 5 vendors had a combined market share of 23 % 2007 as opposed to 23.3% in 2005. Strong EU players, who also compete internationally, are among the Top 5 in this Cluster: they are Thales, Cap Gemini and T Systems.

FIGURE 9

Cluster 2 Market Concentration Indicator (combined market share of top 5 vendors, in %, 2007)



Source: Government Insights, 2008

NIS Market Concentration Indicator: Cluster 3

Overall, the security market in Cluster 3 is fragmented and the level of fragmentation is relatively stable. The Top 5 Players have a combined market share of 24,14 %.

Symantec is the overall market leader with 7,1% market share, but this share has declined in recent years. In Cluster 3, Symantec's loss of share has been quite rapid, declining from 11,2% share of Total Security Market in 2005 to 7,1 % of Total Security Market in 2007. This decline is has been due to the rise of new local players, and stronger competition in key segments. Other top players include IBM, Telecom Italia, TrendMIcro and Cisco.

Telecom Italia had a market share of 5,3% in 2007, up from 3.6% in 2005. Telecom Italia is benefiting from the growth in the market for security services, and similarly to other telecommunications providers has increased the scope of its services offerings in the last few years.

The security software market in Cluster 3 is Concentrated (Top 5 vendors had a combined market share of 41.5% in 2007). However, this level of Concentration has decreased over the last 3 years. In 2005 the market was characterized as Highly Concentrated with the Top 5 vendors having a combined market share of 58.9%.

The Security Hardware markets in Cluster3 is Concentrated, with the Top 5 vendors having a combined market share of 47.3%. However, this is noticeably less concentrated than in 2005, when the Top 5

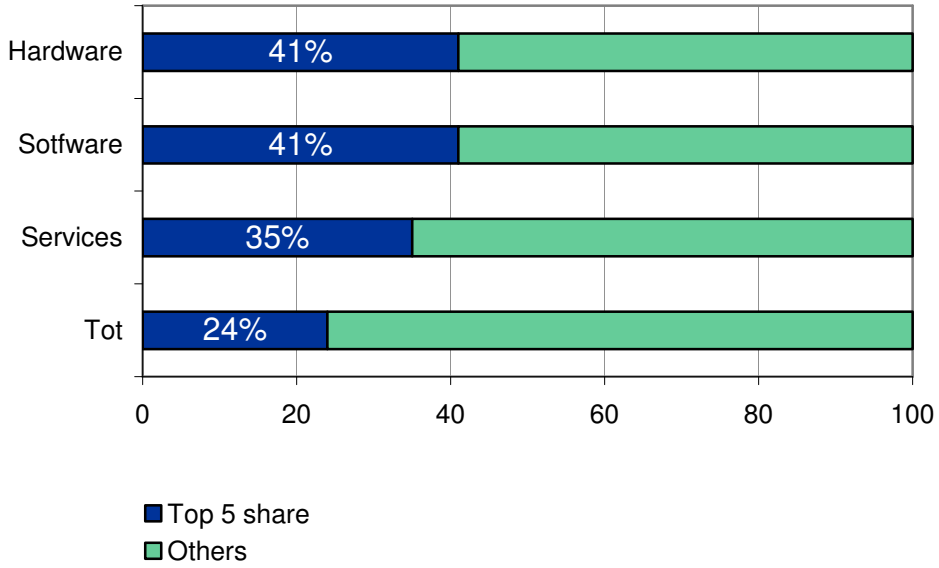
accounted for more than 55% of market share. In the intervening period, only Cisco of the Top 5 players has managed to gain market share. All the others have seen their market share decrease (including Fortinet, Juniper, Nokia and Tipping Point).

As in all Clusters, the Security Services market in Cluster 3 is fragmented. This situation has changed little in the last 3 years. The Top 5 security services vendors in Cluster 3 are Telecom Italia, IBM, Accenture, HP and EDS.

It is also worth noting that 2 local players from the Czech republic are visible and active in the security services market in Cluster 3. They are ICZ (CZ) and Gity (CZ).

FIGURE 10

Cluster 3 Market Concentration Indicator (combined market share of top 5 vendors, in %, 2007)



Source: Government Insights, 2008

NIS Market Concentration Indicator: Cluster 4

Cluster 4 is very different from the other Clusters. It brings together the European Union's newest entrants and smaller markets. EU membership means significant investments must be made to meet the required standards, and IT security investments are part of this equation – particularly as organizations start to build international businesses and expand their interests into other areas of the EU. Despite this however, the absolute size of the IT security markets is small compared to other Clusters.

As a first remark, the total security market in Cluster 4 is the least fragmented of all the clusters.

The Top 5 vendors had a combined market share of 28,4 % in 2007. Interestingly, the level of concentration in Cluster 4 has increased, with the Top 5 vendors having a combined share of 26.6% in 2005.

The main reason for this trend is a major growth in security spending in these countries in the last 3 years, as preparations for EU entry and new business opportunities peaked. Local vendors, although present, did not have the capabilities to scale up to the growth in demand, and buyers turned to large, established industry names who could deal with the volume of business. Consequently, the top vendors in 2007 in Cluster 4 are Symantec, Cisco, McAfee, IBM and Juniper.

The security software market in Cluster 4 is Highly Concentrated. The Top 5 vendors have a combined market share of 55,1 %. The trend since 2005 is towards Higher Concentration when the Top 5 Vendors represented 54,6 % the total market. This situation is unique in the across the EU27 region.

The Top 5 vendors list is also very unique in terms of names and market share.

- Symantec had 28,9 % market share in 2007, down from 30,5 % in 2005
- McAfee had 10,7% market share in 2007 down from 8,6% in 2005.
- CheckPoint had 5,5 % market share in 2007 down from 7,2 % in 2005
- PandaSoftware (Spain) had 4,9 % market share in 2007 up from 4,2 % in 2005
- BitDefender (Romania) had 5,1% market shares in 2007 , up from 3,6% in 2005

The Security Hardware market in Cluster 4 is Concentrated. The Top 5 vendors had a combined market share of 40,9 % in 2007. It is remarkable that in Cluster 4, three Hardware authentication vendors reach the Top5 in the global hardware market. In all others Clusters, these vendors do not reach the Top 5.

The Top 5 Security Hardware vendors in Cluster 4 are Cisco, RSA, Juniper, Gemalto and Oberthur,.

The Security Services market in Cluster 4 is Highly Fragmented, with the highest level of fragmentation in the region. The Top 4 vendors (of which only one is not European) together account for 10,5 % of the market in 2007. They are IBM, ATM (CZ), Comarch (Poland) and CompFort Meridian (Poland).

Spending on security services is likely to grow, following the initial investments in security hardware and software. However, few large international firms will have the organization capabilities to adapt quickly to local market conditions. In addition, the relatively small size of these markets may make them less interesting for large international players. The business users that are investing in security services are likely to favor specialized, well known local vendors, or a small number of international players. Over time we can expect that the markets in this Cluster will evolve to a situation more similar to that in Cluster 3.

EU NIS Market Concentration: Conclusions

The NIS market in the EU is dominated by a small group of global vendors, differentiated by application area. They are Symantec, IBM, McAfee, Cisco and Trend Micro.

The main conclusions of the market concentration analysis are the following.

Levels of market concentration vary across the Hardware, Software and Services market segments. Security Hardware and Software markets are generally concentrated, with clear market leaders. Security services markets are generally more fragmented, with relatively large numbers of players taking a small share of the market.

Across all market segments, Symantec has the largest market share of any single vendor. However, the combined effects of new players entering the security software market space are eroding Symantec's overall market leadership position.

In the security Hardware market space, Cisco occupies a dominant position. Despite this, successful competition is still possible. In Cluster 2, for instance, we believe local hardware vendors can successfully reach the Top 5.

Security services markets are generally fragmented, with no clear leaders across all clusters. The nature of service delivery – the requirement to be "close to the customer" – means that local players often have strong market positions in their home geographies, but have little or no market share in other geographies.

Since 2005, local vendors in all clusters have been successfully building significant market share. This is particularly visible in the software markets where companies like ESET (Slovakia), AVG (Czech Republic), Bit Defender (Romania) and Kaspersky Labs (Russia) have been able top compete successfully for market share. In their home geographies they have built significant market presence. Their competitive strategy is based on a "same features – lower price" offering, whereby their products offer similar functionality to those of the large, international vendors, but at a much lower price point. This strategy is being used with increasing levels of success to address the professional and home-user markets.

Cluster 1: Overall, Cluster 1 is Highly Fragmented. Strong growth in security services brings opportunities for new players, and these markets are subject to high levels of competitive pressure. In the Software market, new entrants contribute to increased levels of fragmentation.

Cluster 2: Cluster 2 is a fragmented market that has undergone significant fragmentation in the last 3 years. Similarly to Cluster 1, these markets offer good opportunities to services players and have relatively low thresholds to entry for new software vendors. The net result is increasing levels of market fragmentation.

Cluster 3: Overall, Cluster 3 is a fragmented market, but levels of fragmentation have remained relatively stable in the last 3 years. In the security services space, local players have successfully built business volume and market share.

Cluster 4: The overall market in Cluster 4 is fragmented, but there has been a trend of overall market concentration. In the period 2005-2007 these markets underwent rapid growth, and buyers turned to major vendors to meet the need for rapidly scalable solutions. This in turn led to an increased degree of concentration. Despite this, local vendors have successfully profited from this rapid market growth, and have been successful both within their home geographies and internationally.

4. SUPPLY CHAINS AND EMERGING BUSINESS MODELS

Main Supply Chain Models

The following paragraphs describe the main supply chain and business models prevailing in the NIS market in the EU.

Security products for end users

Security software for end users (license based)

This market is mainly based on security-suite offerings. These suites typically have a multi-user license (one to five), are based on a 12 or 24-month duration, and are distributed through retail channels.

It must be said here that competition is this consumer field is good for customers. As vendors' products often have significant overlap in core functionality, they tend to try to compete by offering more for the same price. In less than 4 years, home based security suites have shifted from basic security functions (Anti-Virus, Firewall, Anti spam) to global security suites, including Privacy protection, child browsing protection, Back-up / recovery and PC optimization. Given the solid level of basic protection inherent in these products, these additional features and capabilities provide generally better value for the consumer, and extend their protection beyond elementary issues.

In general security products reach the consumer market via three main channels. These are;

- The Original Equipment Manufacturer (OEM) channel: This is the primary channel to market, whereby the security product is bundled with another purchase. The most obvious example is the PC channel, whereby security vendors partner with PC vendors to pre-install their software on new machines. The software is usually available for a 30 day trail, after which the end user can choose whether or not to keep the solution and pay for it through the vendor's web site. Another example is the fact that many Internet Service Providers (ISP's) provide their clients with a complementary suite of security products as part of their subscription.

- The next most important channel to market is the High Street retail outlets channel, whereby security products are purchased in computer shops, household electronics shops etc.

- The third channel is the direct Internet channel. The amount of security products bought directly by consumers is small relative to the OEM and retail channel. However, increasingly vendors are pushing consumers to purchase upgrades, or license renewals via their web sites. So for instance a consumer who purchases a new PC with pre-installed security software will likely end up going to

the vendor's website to purchase a new license or an upgrade. Licenses for security products are generally renewable yearly, whereas new computers are only purchased every few years.

Free security software (open source or limited versions) are usually distributed through the vendor's portal (AVG) or the community's portal (Linux, Ubuntu's).

Security for professional users

As a general note, the security distribution system relies on the fact that security solutions rarely come as stand alone. They are more often than not integrated with other solutions, not necessarily from the same vendor, in major projects. Security vendors need expert integrators, and implementers to deliver their solutions.

Security Services distribution is mainly direct:

By their very nature services such as consulting, implementation and support are generally sold directly to the consumer of the services – but in many cases may not actually be delivered by the service provider directly.

Large contracts with enterprise or government clients will generally be sold directly and may be part of a more extensive IT initiative that goes beyond security to include application software, IT infrastructure, IT strategic planning and outsourcing. In large complex projects, a single services provider may take responsibility for delivery of all of the required services including security, but may sub0contract some of the service delivery to expert partners who are specialized in particular elements of the project. For small and mid-sized organizations, security services may also be delivered stand-alone or as part of a bigger project, or they may be purchased bundled with hardware or software purchase. Medium-sized services firms will often offer security services linked to the broader range of products or technologies they support – e.g. network security or application security. Telecommunications operators have also started to deliver security services both to large enterprises and small and medium clients. In the large enterprise space, telecommunications operators generally do not yet have the broad recognition for security expertise that systems integrators have, and many have not yet succeeded to effectively leverage their large installed base of SMA clients. Despite this, these players are growing in stature and will have a definite impact on the security services landscape in the coming years.

Security Software distribution is mainly Indirect:

Security software is mainly distributed throughout Channel vendors. These channel players are organized by type of end user market. Major System Integrators cover the high end of the market.

Regional and Local Systems integrators will cover the SME market Major vendors have highly expert direct sales teams for vertical industries (Finance, Government)

Agreements with the channel players are confidential and no information is available on the margin generation.

Security Hardware distribution is mainly Indirect

The hardware market is mainly indirect, and the same is true for security hardware. Distribution, storage and handling issues are much more complex in the hardware field.

Major warehouse centralize distribution in Europe, sometime even further. Some Fast courier companies are positioned on the " overnight " delivery for Security appliances stored in US of APAC and delivered in Europe.

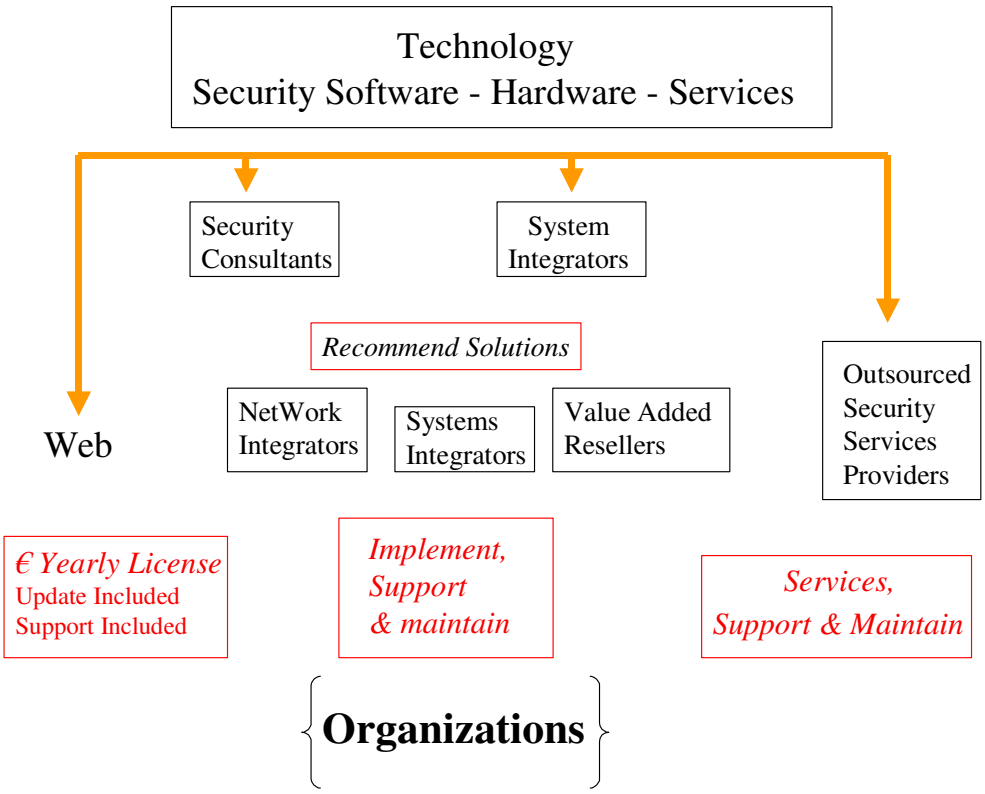
Emerging Business Models for the Business Market

The IT security market for professionals and organizations is rather complex (see figure below). As many organizations develop security policies and governance, vendors must deliver accurate consulting, implementation and support between products and end-user. Indeed, much of the IT security budget in the professional market is spent to renew existing investments and deliver new services in new geographies of use. In the consumer market, most of the budget is driven by license renewal, not to extend the secure perimeter, add new functions or comply with new rules.

Very few projects start from "scratch". So consulting work before implementation is key in order to understand the needs while respecting the existing investment. In order to face organizational complexity, the market has organized itself in multiple layers. Except for the Web, most of the market is considered as a two-tier market. Vendors must use at least two steps to reach the customer. In the opposite way, customer payment must go through 2 steps before reaching the vendor's revenue line. However, flat channel systems do exist in the business field. It is efficient for smaller SMEs and some Services players in the high-end of the market.

FIGURE 11

IT Security Business Model for the Business Market (Vendors are on top, users are on bottom)



Source: Government Insights, 2008

It is clear that "*Security as a Service*" (SaaS) has gained a great deal of attention and markets share over the past two years. Given the growing complexity of threats and security management, service players can easily position themselves as 'complexity reducers' with a flat fee, all-included approach to help clients forecast security spending.

SMEs in Europe have a lot to gain with SaaS. Most of the network and mid-size system integrators can deliver security "*in the cloud*" with no management issues and limited internal resources involvement. In all EU 27 countries, IDC noted local players (e.g. ICZ in Czech Republic, Meridian in Poland) who can address the SME with existing technologies. Such players partner with major security vendors and deliver locally managed solutions. In Western European countries, major system integrators (including telcom operators) signed wide area agreements with major companies. They often take control of the IT security infrastructure and relocate daily management to their premises. In the SME space, mid-sized security outsourcers (e.g. MessageLabs, Google Postini, Vistorm) build the path for a wider service market.

Emerging Business Models for the Consumer and SOHO Market

In the home and SOHO (small office, home office) market the security business model is relatively flat, that is the distance between vendor and client is short (*see following figure*). This market includes clients with less than 10 users within the same local network. A brief analysis of the main business models for delivery and service to the clients is necessary to anticipate future trends.

The only fully direct sales channel is based on the Web**.** In this field, all vendors can distribute their technology and their licenses throughout their own websites.

The first indirect Sales model is OEM (Original Equipment Manufacturer) in new devices or existing appliances. For example, all new Dell PCs come with a short McAfee licenses and all Sony PCs are delivered with a yearly license from Symantec.

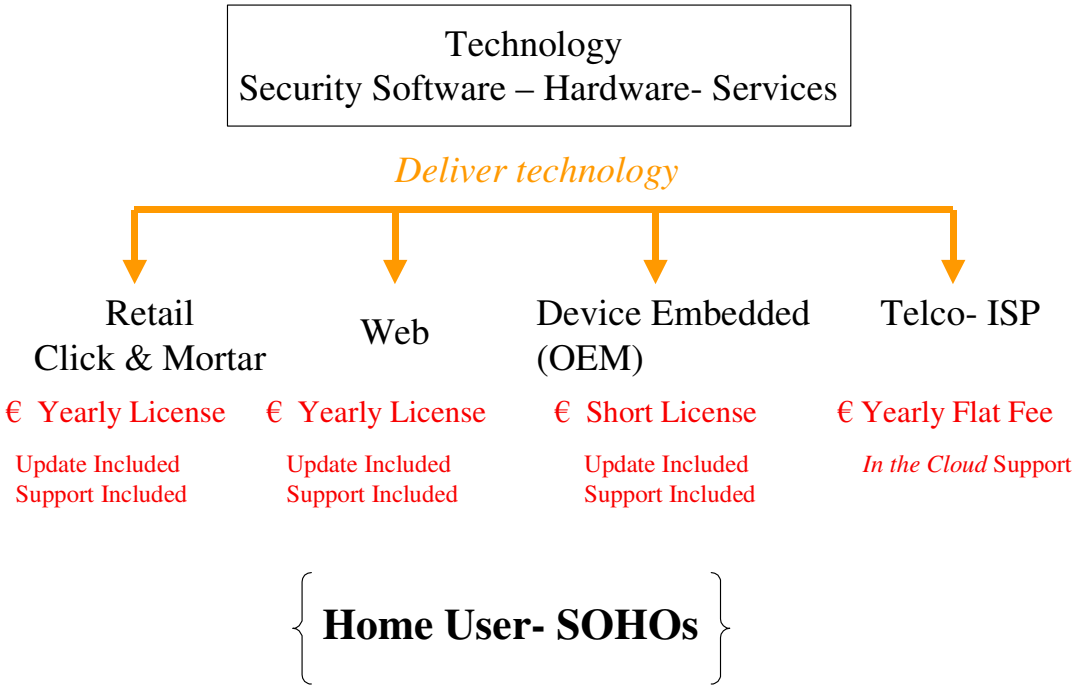
Retail (Click and Mortar) is the main indirect physical sales channel between software vendors and consumers. Retailers can be local IT boutiques or IT service providers for Soho's. Retail also consists of major supermarkets where security solutions are massively distributed. In this field, price and feature competition is very intensive.

Telecom operators and ISP (Internet Service Providers) are very active in end-user protection. They can act as ISV's (Independent Software Vendors) where they resell the security software license to the end-user. It is a limited but existing market. Generally, telcos and ISsP deliver "*in the cloud*" security features for a yearly flat-fee (free in some countries).

A major shift to services is taking place in the consumer field. Brick and mortar retail is still the major sales channel but many of the vendors' strategy is to shift those revenues online and cut the channel costs. Indeed, "in the cloud" security services from telcos are becoming increasingly important. In less than ten years, IT threats became far more complex and agile than simple virus tidal waves. Facing theses threats mean combined response and combined technologies. By assuming defense complexity, "in the cloud" providers gain major attention from consumers who will relocate all security work to external service experts.

FIGURE 12

Home User and Soho Business model (Vendors to Client - Top Bottom description



Source: Government Insights, 2008

5. INTERNATIONAL NIS MARKETS DESCRIPTION

The US NIS Market

The US NIS market is the largest in the world, with total revenues of 13.5 Billion Euros in 2007 and a growth rate The European and U.S. markets show slightly higher growth rates than Japan and Asia-Pacific region (APAC), driven especially by regulatory compliance and the level of sophistication of IT use, leading to more demanding customer requirements.

The share of Security Services is very high in the US (55%), while the trend towards Services dominance is just starting in the EU.

TABLE 9

USA Total Security Market 2005- 2007 M$ (% of total market)

	2005	2006	2007
HARDWARE	1,555	2,041	2,414 (13%)
SOFTWARE	4,661	5,271	5,998 (33%)
SERVICES	7,363	8,449	10,070 (55%)
TOTAL	13,579	15,761	18,482

Source: Government Insights, 2008

US enterprise markets have always been early adopters of security solutions. However, the recent downturn in US financial services coupled with the saturation of security technologies at the enterprise level means that mid-tier and small-business (SMB) markets will see high growth rates in 2009 and 2010.

In the past, SMB markets were poorly served by expensive and complex products originally created for the enterprise market. Recognizing these deficiencies, security vendors offer purpose-built products and services for the small business market. While vendors have adapted their products to the SMB customers, their security needs and awareness has expanded. SMB add more remote employees, more partners, suppliers and customers, they need to provide secure access to all these constituents. In addition, SMB are required to meet compliance requirements, at the state, federal and industry levels.

The sophistication of threat landscape, stringent regulatory mandates, the complex environment, and the potential impacts that security vulnerabilities present to corporations are forcing companies to invest

heavily in IT security. Additionally, data leakage from internal sources is a rising issue. In the US, compliance is the major issue followed by intellectual property (IP) protection. Even mid-tier companies are now sensitive to IP losses such as source code, future product designs, proprietary manufacturing processes, marketing strategies, and R&D strategies.

The increasing availability of broadband connections has several implications. Customers are centralizing data centre operations, pulling threat management out of the branches, and moving to host-based security services (also known as "in-the-cloud" or Software as a Service). In the messaging area, customers are blending installed Customer Premise Equipment (CPE) and hosted security service in a "hybrid" approach. In the web security area, customers are moving towards strictly hosted services.

The Role of Regulation

In the US, the NIS market is influenced by different kinds of regulation. Regulations such as PCI, HIPAA, SOX, GLBA, company specific awareness programs as well as the widely announced data breaches are significantly driving spending in the security market. The above regulations affect particular industry sectors such as, retail, manufacturing, healthcare, financial services.

The main vertical markets investing in security solutions consist of finance, government, healthcare, retail and manufacturing. Their purchases are driven by a mix of government and industry regulations.

For any company that takes or processes credit card transactions, the Payment Card Industry Data Security Standard or PCI DSS, mandates specific security policies. Because PCI is an industry-mandated requirement, it would seem not to carry the weight of Federal compliance regulations. However, its costly fines and other penalties make PCI compliance a major driver for security expenditures by retail, finance, healthcare, and any other industry that handles credit card information. .

As for financial services, this industry will always continue to invest in security solutions due to SOX, GLBA, SEC, Patriot Act, and other US and International regulation. With the current sub-prime mortgage mess, we expect even more financial regulations in the 2010 – 2012 time frame. Moreover, the nature of dealing with confidential customer information necessitates extensive security. .

In other industries, the healthcare vertical is bound by the HIPAA compliance initiatives. Healthcare is a rising issue along electronic data discovery for addressing litigation. Manufacturing and utilities are also seeing increased regulatory pressure from NERC/FERC requirements needed to protect infrastructure from terrorism and other disruptions.

The Socio-economic Context

The current economic slowdown has slightly impacted investments in the security market. Due to increased internal and external pressures, companies have become more aware of the implications of security threats and will continue to invest in security solutions. While compliance-driven budgets will remain well funded, funding for other security projects are likely to suffer slightly. In a recent visit to New York City, IDC heard many stories of stalled deals because of the financial crisis. Security threats are still a driving force as well. The threat environment is professional, profit-oriented, and very aggressive. The disarray of financial market will drive opportunities for greater fraud at all levels: spam, phishing, malware, web, and identity theft. We expect global criminal organizations to target US individuals, companies, and government organizations even more heavily. On Wall Street, it is widely believed that data breaches of confidential emails and files will increase dramatically as layoffs create large numbers of disgruntled ex-employees.

Budget pressure on security will be counter-balanced by the threat environment's increasing professionalism and the sharp rise in disgruntled employees. Unlike other markets, the "dark side" of the security is unique to this market and will continue to drive growth in hardware software, hardware, and services, albeit at lower rate than previous years.

The Japan NIS Market

The level of awareness among Japanese companies with regard to IT security continues to increase due to the implementation of the Personal Information Protection Law and compliance to the laws. As a result, the Japan security market is forecast to continue growing for the next five years. The market size is expected to exceed 1.3 trillion yen by 2012 but with the enforcement of the Japan SOX Law in 2008, we forecast that the compound annual growth rate (CAGR) between 2007 and 2012 is forecast at 12.3%.

TABLE 10

Japan Security Market M Yens

	2005	2006	2007
Hardware	28,170	34,841	39,643
Software	136,401	163,331	175,211
Services	417,300	449,004	520,363
TOTAL	**581,871**	**647,176**	**735,227**

Source: Government Insights, 2008

Rather than in large companies that have invested in system reorganization and security system integration, the security software market will see a higher growth in small and medium sized businesses (SMBs) that are expected to increase their investments due to market recovery. However, due to falling prices and competition from appliance products, the growth rate of the software market will be lower than that of the appliance or service markets.

In the security appliance market, threat management (TM) functions are already being integrated in UTM appliance products. However, coupled with falling prices and ease of deployment and operation management, it is expected that both TM appliance and secure content management (SCM) appliance products deployment will increase rapidly.

Among the security appliance products, mail security appliance will be an important product group propelling the growth of the appliance product market, as implementing measures to block out increasing spam emails have become prime tasks for ISP and companies.

The security service market is expected to register high growth in system construction and system operation management amid corporate needs for information leak prevention solutions and compliance reinforcement. After the enforcement of the Japan SOX Law in 2008, the growth rate will decrease somewhat from 2009 due to a decrease in compliance-related demand among large companies, but it will probably pick up after that.

As an essential part to prevent information leaks and strengthen compliance, the need to reinforce employees' work ethics and cultivate awareness remains high and demands for related education and training will continue to grow.

IDC forecast that the Japan security market will continue to grow rapidly in 2008 and beyond. Market drivers include security threats such as information leaks and needs to comply with regulations such as the Personal data Protection Law and J-SOX. The growth rate will decrease somewhat from 2009 due to a decrease in compliance-related demand among large companies. However, the market will remain steady on the back of continued investments from large companies and security needs in the SMB market. In the future, a growing number of companies will opt for outsourcing services rather than build their own security systems. With the growing use of hosting, collocation and SaaS(Software as a Service)-based services, demand for related security services will also increase. Thus, services will post the highest growth rate among all the segments within the Japan security market.

The main industry sectors investing in security solutions consist of finance and manufacturing, information services as they're driven by IT internal control for compliance such as the Personal data Protection Law and J-SOX.

Large companies will further proceed with implementation and operation/management of systems and security services in order

comply with the 2008 Japan SOX Law. This will promote software and appliance implementation. Although SMBs are slower than large companies in security implementation, their levels of awareness toward the need for security measures have increased. On this account, continuous investments on security measures can be expected from SMBs. The above factors will promote rapid growth of the market until 2008. In 2009 and beyond, investments are expected to decrease drastically and growth rate will fall. However, if the need for security solutions is widely recognized, we believe that constant growth will continue in this market.

Market drivers are:

- The need to comply with regulations such as the Personal data Protection Law implemented in 2005 and J-SOX implemented in 2008 will continue to exist.

- Concerns about internal security threats will increase. A strong demand for information leaks solutions is thus anticipated. The range of end-point security solutions required will expand with the types of user communications like VoIP, graphics, email, and Web and devices like USB memory, iPod, and Bluetooth.

The Role of Regulation

Japanese laws will prompt "large companies" to improve internal control systems and the coverage of the law will expand from financial areas to non-financial areas. M&A and industrial reorganization through equity exchange, which became possible in May 2007, will pick up in pace. This will stimulate the demand for information system consolidation/integration.

Amid the rampant incidents of personal information leaks, relevant ministries are strengthening their administrative instructions with focus on control/monitoring of outsourcers/consignees for personal information handlers.

As crimes of illegal credit card use are increasingly committed globally, five credit card companies compiled and are promoting the global security standard "PCI-DSS" to protect personal information and payment information handled by participating stores and payment agents.

The Ministry of Economy, Trade and Industry, the Ministry of Health, Labor and Welfare, and the Ministry of General Affairs plan to launch a joint project on health care information database between April 2008 and March 2011, and will discuss policies aimed at implementation of the Japanese PHR (Personal Health Record) management. Commercial use of such technologies began in 2008, and IP-based high-speed and wide-area communication infrastructure will be developed rapidly. The pervasion of NGN and FMC will promote business opportunities in the market for upper-layer compliance-related solutions. At the same time, more companies will seek to enhance their end-to-end security solutions.

The Kyoto Protocol states that Japan will have to reduce the amount of greenhouse gas emission between 2009 and 2012 by 6% from the level of the year 1990. With the need to strengthen corporate compliance, companies will have to store data for a longer period and to increase storage capacity, which results in the increase in power consumption of relevant IT devices. Implementation of "green IT" will be promoted from the perspective of ensuring consistency with environmental compliance.

Although the Japan SOX Law is applicable to listed companies, many smaller listed companies (e.g., in the second half of the Tokyo Stock Exchange and JASDAQ) are still not prepared for the 2008 enforcement due to a lack of consultants. As non-listed companies that received outsourced services from these listed companies will be indirectly affected by the Japan SOX Law (acquisition of SAS70 or Audit Report No. 18 or acceptance of external audit from service users), efforts to strengthen security solutions will continue to gather momentum among these non-listed companies.

However, on the negative side, companies could be snowed under workload to comply with the SOX Law and could not implement new systems and services. Instead, they would implement compliance measures to existing systems and then renew the system after passing the audits. This could lead to low motivation for new implementation. In addition, as the SOX audit evaluates risk controls at the end of the fiscal year, system changes are hold since around three months before the year-end that would be a negative factor for the market too.

The Japan SOX Law is basically a positive factor in the security product market but the impact might be limited. This is because the control framework of the SOX Law checks whether a management system is in place for risks but it does not consider the method.

Evaluation of the management system takes into account the size and frequency of the risk, as well as the economic efficiency of the control method. In other words, it is not necessary to implement new security products and services as long as the management recognizes the intensity and frequency of the risks and has a reasonable explanation for the costs involved in the control method. A control framework that the manager recognizes has specific risks through the SOX audits but they controls the risks with manual checks by the person in charge and the management approval because the cost of the product solution is inadequate could be effective.

The socio-economic Context

The Japan economy as a whole is likely to be stalled in the short term due to internal and external risks such as rising oil price, higher material costs, the appreciation of the yen, low share prices, sluggish consumer spending, an uncertain political climate, and the slowdown of the U.S, economy. Due to this situation, the recovery of corporate performance may become stagnant again among companies that rely on domestic demand and this may hamper the growth of IT investments.

The Asia-Pacific NIS Market

The Asia-Pacific NIS market (excluding Japan) had total revenues of 2.2 Billion Euros in 2007, significantly smaller than the Japanese or US market. This includes Australia (the largest market accounting for 43.1% of the total market), followed by Korea, Singapore, New Zealand, Hong Kong, India, and the People's Republic of China (PRC). Growth rates for the ICT Security market are expected to be significant, even if the economic and financial crisis will slow down the market development: much of this is driven by regulatory action on both government and local levels.

TABLE 11

APAC Ex-J Market Size M $

	2006	2007
Hardware	804,20	969
Software	928,8	1086,2
Services	1126	1284,6
TOTAL	**2859**	**3339,8**

Source: Government Insights, 2008

The APAC security market is less mature than the US or Japanese one, showing a 39% revenues share for services, 33% for software and 29% for hardware in 2007. This is typical of the countries where the information infrastructures are still in the development phase.

Although the hardware market (security appliances) is the smallest of the three submarkets (HW, SW and Services) it is expected to keep growing fastest than the others. This will be driven by new organizations rolling out IT networks, enterprises growing their IT infrastructure, and companies becoming more geographically disperse. SMEs, which traditionally have shown expensive security hardware, have also been enticed to invest by vendors that rolled out new security appliances designed specifically for SMEs. These SME appliances tend to be simpler and priced very competitively.

The security software sub-market is expected to increase only slightly less than the hardware sub-market, driven primarily by the adoption of Identity and Access Management (IAM) software and continued investments in Secure Content Management (SCM) software. With the proliferation of threats targeting endpoints, SCM and threat management software will become must haves at all endpoints, especially within an enterprise environment. Regulatory compliance needs and governance requirements will drive the growth of the IAM

market. These needs will also drive the demand for security and vulnerability management software, which has to do with managing and monitoring risks.

IDC forecasts that the security services submarket will also increase. Stringency in compliance requirements will increasingly contribute to market growth that will result in a spill-over demand for security services across all submarkets. The implementation submarket is still expected to be the largest within the security services submarket by 2011 but the fastest growing submarkets are expected to be maintenance and support and operations.

The demand for security products by the consumer and small office/home office (SOHO) market segment in the Asia/Pacific is set to grow with increasing PC penetration and Internet broadband adoption in the region.

The three major players in the consumer and SOHO market in APAC are Symantec, Trend Micro, and McAfee. Together, they account for more than 57% of the market revenue. Having said that, there are numerous other players active in the market, including CA and Panda. There are also strong local players in this region who are very popular in their home markets, like Rising in China and Ahnlab in Korea.

Regarding the managed security market in the APAC regions, it is still at a nascent stage but as enterprises expand rapidly, IT managers are struggling to secure their networks from threats, both internally and externally.

Network security continues to hover high on the list of priorities for many companies today as they come to grips with the increasing types of threats that their networks face. There has definitely been a growing uptake in security "in the cloud" services, especially among the small and medium-sized business (SMB) segment or enterprises with branch offices. In the cloud services allows enterprises to have a robust security defense mechanism without the need for a huge capital outlay or investment; it also gives them a flexible alternative to dealing with multiple vendors. In the cloud services means that network traffic is cleared of spam, viruses, and other potential threats before it reaches the networks.

IDC believes that telcos are in the best position to take advantage of this trend as they are providing the essential connection that is closest to the enterprise networks. However, certain obstacles will remain, as there will be some enterprises that are reluctant to completely forego the ownership of any customer premises equipment (CPE) and have severe reservations of sharing any platforms with other enterprises.

Being that of Managed security services a relatively new concept, it is not surprising that adoption is strongest in more mature markets. In 2007, Australia is expected to be the largest market accounting for 43.1% of the total market; this is followed by Korea, Singapore, New Zealand, Hong Kong, India, and the People's Republic of China (PRC) with 10.8%, 9.0%, 8.9%, 7.4%, 7.2%, and 6.1%, respectively.

As regards the competitive scenario in the APAC regions, in 2006 the most important market share (considering security hardware and software only) were that of: Trend Micro (365 $M in 2006), Symantec (339 $M in 2006) and IBM (118 $M in 2006).

Trend Micro is leading the Secure Content and Threat Management (SCTM) market, while IBM has the largest market share in the IAM market, followed by EMC and CA. HP, IBM and Microsoft are the main providers of Security and Vulnerability Management (SVM) solutions.

According to the most recent IDC surveys on security trends, factors driving investment in the APAC regions are:

- Increased use of the Internet and intranets in organizations of all sizes;
- Need to respond to higher customer expectations;
- New systems / applications implementations;
- Risk of security breaches;
- eCommerce / eBusiness initiatives;
- Mobile computing projects;
- Increased corporate awareness over Security threats.

Policy will continue to have high impact on market. Compliance will still drive some of the IT spending, including to the SOX. IDC do not expect compliance spending to crowd out other IT initiatives: compliance record keeping will spur initiatives in other areas as companies clean up their act.

Piracy will remain an issue especially in the SMB and consumer markets. The situation is not likely to worsen but is also not likely to improve drastically in the near term. There will be no irrational sentiment against IT and consulting like several years ago: if the buyer sentiment remains high the spending could beat forecasts.

Regarding security threat environment, software will become more rather than less vulnerable. Hackers will continue to find ways to misuse other people's software. Organizations from this region typically report that primary security threats are, in fact, external attacks. In order, reported threats are:

- Virus, Worms and Trojans
- External hacking
- Corruption or replication of data
- Employee sabotage

- Denial of service attacks
- Unwanted reconfiguration
- Shutdown of eBusiness.

Today, hackers are finding ways to just misappropriate software without vulnerabilities. The ability to bury malware within other software will become a dangerous trend that will lead to improved spyware and increase the need for software and application security tools during software development and deployment. It will also increase the need for intrusion prevention software that enforces application execution. Although great for the security market, it can have a dampening impact on software in general.

Other trends in the APAC Security marketplace are those of convergence and Security as a service.

Convergence is a complex phenomenon working in many levels – convergence of the telephone network and the internet; of communication and IT; of consumer and enterprise technologies; and even of storage, routing, and processing in datacenters. Of this, perhaps the most overarching will be the convergence of voice, video, and data communication.

Security software will be more likely delivered as a service and/or a security appliance than be bought as shrink-wrapped products. It will become more difficult to segment what is pure security software, what is inherent in a security appliance, and what is delivered as a software service. This will have a considerable impact on licensing and maintenance. Vendors will like it because of its incremental revenue and hardware vendors will like it because they can provide solutions not available to them or leverage their appliances to create a revenue stream.

It is important to underline the role of Business continuity and Disaster Recovery: awareness of the need for business continuity and DR plans will increase. Security solutions will become critical components of these plans. Adoption of best practices for business continuity and DR will have a pull-through effect on investments in security solutions.

The Role of Regulation

Compliance will still drive some IT spending, including to the SOX, Basel II, and the HIPAA. IDC do not expect compliance spending to crowd out other IT initiatives. In fact, compliance record keeping will spur initiatives in other areas as companies clean up their act. Increased attention to sound IT governance policies and compliance with regulatory requirements will drive the increased focus on storage and data management. So compliance and governance will have a positive impact on spending on infrastructure software that will aid in the archiving, protection, and recovery data.

Compliance spending will fund itself through better-run business operations. Specific vertical markets such as healthcare, government, and financial services are more heavily impacted by regulations in order to ensure a secure commercial operating environment. These verticals will be another main contributor driving growth in the security services market, more specifically in the consulting services category.

The Socio-economic Context

Asia's financial markets are becoming more closely meshed with global markets. Cost measures of financial integration, and thus potential contagion, have greatly strengthened over the past decade. Through these channels Asian borrowers will feel the pinch in international credit markets and Asia's bourses are likely to experience heightened volatility. But as Asia's banks are still the main originators of domestic credit, and their leverage and exposure to unsafe securities are low, the possibility of the credit crunch washing onto Asia's economic shores seems remote.

Most Asian economies also have ample foreign reserves in the event of an unexpected rush to sell domestic currency.

McKinsey's annual report, *Mapping global capital markets* (McKinsey Global Institute 2008) observes that at the end of 2006, the major economies of developing Asia held assets to the value of $14.2 trillion, equivalent to 250% of combined GDP. Developing Asia's financial asset holdings are dominated by the PRC, which possesses a bit over a half of them, with Korea and India together accounting for 40%. In the PRC, financial assets are over 300% of GDP, whereas in India the orresponding ratio is just over 200%. Although the PRC's financial system is still bank dominated, asset distribution in other markets is more evenly balanced among equities, debt, and deposits. However, in some countries such as India, Indonesia, and Philippines, government has a large profile in debt markets, with only a small private sector presence.

Drivers of environmental change—urbanization, industrialization, and intensified agriculture—are expected to further push the demands for water, energy, and raw materials in the coming decade.

6. CONCLUSIONS

Key Supply Side Trends

Over the period 2005 to 2007, the following trends have been noted:

1 - The constant growth of the IT security market across the region, and all countries. The market is still in its adoption phase.

Main drivers of this trend are:

- Deperimeterization: the ratio of laptop to desktop PCs in business organizations has grown from 30% in 2000 to 50% today. This means that the "information space" to be protected is growing.

- Threat Complexity and Agility: Educated and agile hackers, internal hacking, silent hacking, are increasing. IT consumerization: there are PC everywhere, no clear lines between professional and personal life, extreme personalization of IT tools. Social networks. High exposure to risk, more needs (endpoint protection warmly welcomed).

- Regulations and jurisprudences drive spending.

- IT disaster more educative than slideshows (HMRC, SocGen, M&S).

- Public and political involvement in Personal Internet Security (U.K. debate). Regulation and jurisprudential threat.

2 – The increasing dynamism and growth of local EU players

The main drivers for this trend are the following:

- Local players gained experience in their "natural markets" by deploying early and agile technologies with local governments and industries. This can then lead to a consumer portfolio (issued from the early developments for professional use) at an affordable price. Most of the EU based security vendors have an important revenue stream based on both consumers and "pro-sumers".

- Local players use local resources and skills. Technical skill standardization (driven by IP adoption) allows better penetration of technologies. Local universities and other academic institutions have, over the past 20 years, developed a high level of skilled professionals. This is undoubtedly one of the main contributors to the success of local vendors.

- There is better cooperation between European based vendors than their US-based counterparts. For example, Sophos (originated in UK), Norman (Norway), Bit-Defender (Romania), all OEM their virus search engines for other players. F-secure (Finland) uses

KasperskyLabs anti-virus engine. Microsoft WW uses Sophos's engine, as do many others. Smaller player often deal with other local players, bringing together seamless solutions. This kind of 'coopetition' (cooperation among competitors) does not exist in US where vendors rarely cooperate.

- Funding recently came from European based venture capitalists (VCs), bringing standardized management and methodology. As an example, BIT-Defender (Romania) is funded by a US based VC (also originated in Romania), GFI (Malta), Panda Security (Spain) are have also recently been funded by EU based VC's.

- 2006 was a bad years for global security players. As an example, Symantec was unfocused on security, due to the merger with Veritas and their consolidation activities. During this time, Symantec suffered major delays in its SCTM portfolio renewal. This opened windows of opportunity for competitors and local players.

- Local governments are very supportive and often invest in the local products.

3 - Commoditization occurring in the malware mitigation market.

Anti-malware labs are more common, given the level of skills and instruction in areas where the workforce is cheaper. Most of the Eastern European countries (Romania, Czech Republic, Slovenia) generated a local anti-malware industry that is now working across borders. These vendors tend to compete aggressively on price against the leaders (Symantec & McAfee) in the SME's market. They easily challenge the leaders in their respective countries of origin. Keeping the quality of their products at the high-end of quality standards, they are often "as good as", but with a reduced price. Anti Virus mitigation tools overlap each other in terms of quality and function and the user, unless an expert, will unlikely understand the difference. As users and decision makers find it difficult to differentiate between vendors, so price becomes the differentiator. Since 2007, these local players are becoming increasingly global, and visible in the US and UK.

4 - The gap between the use of mobile devices and the dynamics of the mobile security market

The dynamics (growth rate, innovation) of the mobile security tools market dynamics does not match the penetration of IT mobile tools. Trends show that the investments in such solutions remain weak.

Vendors report weak activity for dedicated mobile security solutions, such as F-Secure which reports less than 5% of global turnover in the mobile security portfolio.

There is a major misunderstanding between the industry and the market. Vendors tend to consider that Mobile security process must be operated in the network with " usual tools " (i.e : Firewalling, Threat mitigation, Identity Management). They do not provide advanced

solutions for mobile tools others than Laptops. So existing Security solutions for Phones and PDA are very limited due the lack of power in the mobile device. The major problem resides at the device level. Security software is a high power consumption tool and must stay constantly connected for immediate patching. There is therefore a trade-off in energy use, on mobile devices, usually in favor of the user interface or communication functionality, over security. Meanwhile users tend to use more and more their mobile device and search for Security solutions at the endpoint level.

There is also a severe lack in user understanding of mobile security and threat management. Less than 5,000 virus signatures are know in the mobile space (excluding laptops) whereas 500,000 are currently known in the fixed-world. There are limited accidents occurring in this field with the main issue being data leakage by the user (unsafe use of device storage capacity), which is poorly understood by the user.

General Conclusions

Symantec, Cisco and IBM dominate the EU 27 market supply side for the main market shares. But the market is widely open to competition after the first ranks. In other words, competition is open in the space left by the dominators. Since 2006 this space is getting wider and grows significantly every year.

Local competition is growing in the local markets. In less mature markets, local security players will initially have an opportunity as spending ramps up, but will quickly be eclipsed by the major international vendors. Building a strong channel and security services market will be the key to facilitating security innovation beyond product functionality. New local champions (systems integrators) will emerge who will combine security hardware, software and services into innovative solutions, and will be able to compete with big international systems integrators in certain market segments.

The evolution of Software as a Service offers a new platform for innovation for European companies, and facilitates the development of market penetration at the country, regional and global levels.

No visible barrier prevents any player to compete against others in any country of the EU 27. If no obstacles prevent free competition, Vendors ownership open questions about financial capacities for market growth. EU27 based Security companies are mainly private and must self-finance their development. Meanwhile major players can generate faster margins because they support limited R&D in others markets.

Commoditization in the threat mitigation area (due to major overlaps between solutions) drives competition on price, shift to services and market consolidation. Margin pressure will drive market consolidation where young and small vendors must be very agile to keep the pace of innovation and growth.

7. METHODOLOGY OF SUPPLY ANALYSIS

IDC has in-depth knowledge of the ICT vendors market, with specific expertise on competitive analysis, including the strategic positioning of main players, marketing mix and distribution channels, performances on sales, production and market shares of the top operators at national level, short and medium-long term threats and opportunities. However, IDC information on vendors is proprietary and in any case does not fully match the requirements of this study.

For this reason, the supply analysis methodology was based on the use of IDC research, additional desk research, and 20 interviews plus 10 desk research-based profiles of a representative sample of NIS vendors active in the EU 27 markets.

The sample of suppliers was selected in such a way to include a balanced representation of the main suppliers typologies and to include the most important suppliers for each of the 27 EU MS, based on size, level of turnover, and market dominance. Furthermore, the suppliers cover all the main NIS market segments and application areas.

The main supplier typologies considered were:

- Technology Providers, including specialized IT vendors (such as Symantec and Trend Micro) and global IT vendors like IBM or Microsoft;

- Service Providers, including IT Service providers and System Integrators (Siemens Business Services, Accenture..), Telecom operators, Internet Service Providers (ISP), Application Service providers (ASP).

This classification is based on the core business of the suppliers, but most of them deliver a mix of products and services and their marketing mix can be very articulated.

IDC security research manager Eric Domage led a team of IDC researchers to carry out the supply analysis in the period March-June 2008. IDC prepared as field research instruments, the Supplier Profile Template and the Market Template.

The list of selected vendors for the profiles was extracted from IDC databases, which include vendors ranking in most of the EU security markets. The following table presents the list of suppliers profiled.

TABLE 12

List of Suppliers

	Name	Country of HQ	Pub/Private	Expertise Domain
1	F-Secure	Finland	Public	Threat Management
2	Norman	Norway	Public	Threat Management
3.	Bit Defender	Romania	Private	Threat Management
4.	GFI	Malta	Private	Threat Management
5.	AVG	Czech Rep	Private	Threat Management
6.	G-Data	Germany	Private	Threat Management
7.	Panda Security	Spain	Private	Threat Management
8.	ESET	Czech Republic	Private	Threat Management
9.	Kaspersky Labs	Russia	Private	Threat Management
10.	Microsoft	US	Public	Threat Management
11.	Netasq	France	Private	Threat Management
12.	CheckPoint Software	Israel	Public	Threat Management
13.	Marshall	UK	Private	Threat Management
14.	Sophos	UK	Private	Threat Management
15.	Siemens Consulting	Germany	Public	Security audit & Services
16.	BT Global Services	UK	Public	Security audit & Services
17.	Deutshe Telekom / T-Systems	Germany	Public	Security audit & Services
18.	Cap Gemini	France	Public	Security audit & Services
19.	I-Net	Italy	Private	Security audit & Services
20.	Vistorm	UK	Private	Security audit & Services
21.	IBM Global Services	US	Public	Security audit & Services
22.	Telecom Italia	Italia	Public	Security audit & Services
23.	Message Labs	US- UK	Public	Security audit & Services
24.	Keyware	Belgium	Public	Authentication & Encryption
25.	Vasco	Germany	Public	Authentication & Encryption
26.	Utimaco	Germany	Public	Authentication & Encryption

TABLE 12

List of Suppliers

	Name	Country of HQ	Pub/Private	Expertise Domain
27.	Symantec	US	Public	Global
28.	McAfee	US	Public	Global
29.	Trend Micro	Japan	Public	Global
30.	NEW Zetes	Belgique	Public	

Source: IDC 2008