

World Unified Threat Management (UTM)

Products Market 2008

N48C-74

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation.

Frost & Sullivan reports are limited publications containing valuable market information provided to a select group of customers in response to orders. Our customers acknowledge when ordering that Frost & Sullivan reports are for our customers' internal use and not for general publication or disclosure to third parties.

No part of this report may be given, lent, resold, or disclosed to non-customers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the permission of the publisher.

For information regarding permission, write:

Frost & Sullivan
2400 Geng Road, Suite 201
Palo Alto, CA 94303-3331
United States

Table of Contents

CHAPTER 1

Executive Summary

Summary	1-1
<i>Executive Summary</i>	1-1
Key Findings	1-2

CHAPTER 2

Total World Unified Threat Management Market

Market Overview and Growth Factors	2-1
<i>Market Overview and Definition</i>	2-1
<i>Market Engineering Measurements</i>	2-3
Market Stage	2-3
Number of Competitors	2-4
Degree of Technical Change and Predictions for the Future	2-4
Price Sensitivity and Future Pricing	2-4
<i>Market Drivers</i>	2-6
Replacing Legacy or Outdated Point-security Solutions	2-6
Increasing Flexibility in Network Security	2-6
Regulatory Compliance for the Network	2-7
Proliferation of End-user Mobile Technology in the Work Place	2-7
Web/Enterprise 2.0 and Instant Messaging in the Workplace	2-7
<i>Market Restraints</i>	2-8
Conflicting Budget Priorities	2-8
UTM is Not Ready for Enterprise or Data Center Deployments	2-8
Creating Network Backdoors	2-9

Economic Downturn	2-9
The Inability of Providing Security Out of the Box	2-9
'If it's Not Broke Why Should I Replace it' Mentality	2-9
Application Support and Policy Obstacles	2-9
Market Trends and Forecasts	2-10
<i>Revenue Forecasts</i>	2-10
<i>Degree of Technical Change</i>	2-12
<i>Geographical Trends</i>	2-12
<i>Vertical Market Analysis</i>	2-17
<i>Technology Trends</i>	2-19
<i>Distribution Trends</i>	2-20
<i>Pricing Trends</i>	2-22
<i>Legislative Trends</i>	2-24
Homeland Security	2-24
California Law SB 1386	2-25
The Patriot Act	2-25
HIPAA	2-25
GLB	2-25
Government Information Security Reform Act	2-26
Computer Security Enhancement Act of 2001	2-26
Basel II	2-26
Canadian Personal Information Protection and Electronic Documents Act	2-26
Sarbanes-Oxley Act	2-27
European Data Protection Directive	2-27
Payment Card Industry Data Security Standard	2-27
Competitive Analysis	2-27
<i>Competitive Structure</i>	2-27
<i>Market Leader</i>	2-29
Fortinet INC	2-29
<i>Market Challengers</i>	2-30
Cisco Systems, Inc.	2-30
IBM/ISS	2-31
Check Point	2-32
SonicWall	2-32

<i>Market Contenders</i>	2-33
WatchGuard Technologies, Inc.	2-33
Crossbeam Systems Inc	2-34
Juniper Networks	2-34
Secure Computing	2-35
<i>Emerging and Receding Participants</i>	2-36
Astaro Corporation	2-36
Cyberoam (A division Elitecore Technologies)	2-36
3Com	2-37
<i>Niche Participants</i>	2-38
Global Data Guard	2-38
Calyptix Security	2-38

List of Figures

CHAPTER 1

Executive Summary

1-1	Total UTM Market: Revenue Forecasts and Unit Sales (World), 2004-2014	1-5
-----	--	-----

CHAPTER 2

Total World Unified Threat Management Market

2-1	Total UTM Market: Revenue Forecasts and Unit Sales (World), 2004-2014	2-2
2-2	Total UTM Market: Market Drivers Ranked in Order of Impact (World) 2008-2014	2-8
2-3	Total UTM Market: Market Restraints Ranked in Order of Impact (World), 2008-2014	2-10
2-4	UTM Market: Revenue Forecasts and Unit Sales (North America), 2004-2014	2-14
2-5	UTM Market: Revenue Forecasts and Unit Sales (EMEA), 2004-2014	2-15
2-6	UTM Market: Revenue Forecasts and Unit Sales (Asia Pacific), 2004-2014	2-15
2-7	UTM Market: Revenue Forecasts and Unit Sales (Latin America), 2004-2014	2-16

2-8	Total UTM Market: Percent of Revenues by Market Vertical (World), 2004-2014	2-17
2-9	Total UTM Market: Average Price Offered by Major Market Participants (World), 2007	2-23
2-10	Total UTM Market: Competitive Structure (World), 2007	2-28
2-11	Total UTM Market: Competitive Market Share Trends of Major Market Participants (World), 2007	2-29
2-12	Total UTM Market: UTM Feature Break Out for Key Industry Participants (World), 2007	2-39
2-13	Total UTM Market: UTM Feature Break Out for Key Industry Participants (World), 2007 (Continued)	2-40
2-14	Total UTM Market: Database of Key Industry Participant Web Sites (World), 2007	2-41

List of Charts

CHAPTER 1

Executive Summary

1.1	Total UTM Market: Revenue Forecasts and Unit Sales (World), 2004-2014	1-5
-----	--	-----

CHAPTER 2

Total World Unified Threat Management Market

2.1	Total UTM Market: Revenue Forecasts and Unit Sales (World), 2004-2014	2-3
2.2	Total UTM Market: Market Engineering Measurements (World), 2007	2-5
2.3	Total UTM Market: Percent of Revenues by Geographic Region (World), 2007	2-16
2.4	Total UTM Market: Small/Home Office to Enterprise Percent of Sales (World), 2007	2-18
2.5	Total UTM Market: Percent of Revenues by Market Vertical (World), 2007	2-18
2.6	Total UTM Market: Percent of Revenues by Sales Channel (World), 2007	2-21
2.7	Total UTM Market: Percent of Software versus Hardware Sales (World), 2007	2-21

2.8	Total UTM Market: Percent of the Type of OEM Software per Provider (World), 2007	2-22
2.9	Total UTM Market: Average Price Offered by Major Market Participants (World), 2007	2-23
2.10	Total UTM Market: Competitive Market Share of Major Market Participants (World), 2007	2-42
2.11	Total UTM Market: Competitive Landscape (World), 2007	2-43

I

Executive Summary

S U M M A R Y

Executive Summary

The 2007 Unified Threat Management (UTM) Market study provides an in-depth analysis of solutions that provide firewall, virtual private networks (VPN), content filtering, anti-malware and other network security products within one solution. This study titled the World Unified Threat Management Market, provides an in-depth analysis of solutions that provide firewall, virtual private networks (VPN), content filtering, anti-malware, and other network security products, within one solution. UTM can be defined as hardware or a software solution that provides inbound network and traffic protection through services, such as the use of firewalls, virtual private networks VPN, intrusion detection and prevention systems (IDS/IPS), and anti-malware. In addition to the aforementioned specifications, UTM is also defined as any solution that provides content filtering and emerging security-technologies, such as wireless fidelity (Wi-Fi) and data leakage prevention (DLP).

Yesterday's threat landscape was made up of the 'usual suspects' or threats, such as 'denial of service' attacks and malware such as viruses and worms. The aforementioned threats took down corporate networks for a matter of hours or even days in their effort to inoculate the threat. The inoculation method was composed of numerous independent or stand-alone network-security products, such as antivirus software and stateful packet-firewalls. However, the threat landscaped has morphed into a more deadly threat that not only takes down corporate networks but rob networks of priceless proprietary information and data. Additionally, trojans, viruses, and worms have been combined to form an even more lethal attack methodology, called a 'blended attack'. The methodology uses a combination of malware such as attacks trojans and viruses that manifest faster than their predecessor. To counter this methodology, business corporations and governments continue to use earlier methodologies that use independent network-security appliances that counter threats. Additionally, the daily management and maintenance of desperate technologies is not only non-effective but is also cost-prohibitive. The operational and management costs are prohibitive due to the additional man-hours cost that are needed to administrate each stand-alone appliance. Network security providers, such as SonicWall and Cisco Systems recognized the ineffective and cost-restrictive nature of stand-alone appliances. Therefore, they address the issue with an amalgamation of network-security solutions. The amalgamation brings together firewall/VPN, anti-malware content filtering, and emerging security-technologies, such as data leakage prevention, into one solution, called Unified Threat Management UTM. They brought about the technology to provide an overall solution that addresses the growing threat landscape, budget and management restraints, and complexity of network security.

KEY FINDINGS

Since the inception of network security, information technology (IT), and business professionals have deployed multiple network-security products, such as firewalls, IDS/IPS, and anti-malware solutions, to protect networks of all sizes. At the time, each solution was deployed as a software or hardware-form factor. By running multiple solutions, it became cost-prohibitive and complex for companies and their IT staffs. The problem was due to the associated cost of purchasing solutions from various vendors and the high learning-curve for managing disjointed technologies. The concept of UTM technology became appealing, due to two primary factors or drivers, which are reduction of total cost of ownership and reduced complexity. Therefore, business leaders and IT technicians foresaw the technology as a viable solution for their networking and security requirements for their small to medium sized businesses (SMBs) or their remote office or branch offices (ROBOs). UTM was a major driver for large-size businesses, with remote or branch office (ROBO) to adopt an Internet-based communication. Before the introduction of UTM companies used expensive and complex T-1 lines to connect their branch offices to the corporate networks in order to provide network security and management. However, during the initial roll out UTM products and solution businesses perceived the technology as only suitable for their SMBs and branch-size offices. This was due to the negative paradigm that UTM appliances lacked the low latency, high throughput, and performance, needed to support large-size business with 500 or more users. Additionally, they felt that same limitations were unsuitable for large-size data centers also.

However, UTM providers recognized the negative paradigm and reengineered UTM products into enterprise-class solutions. The enterprise solution incorporated the same high-speed processing and throughput found in stand-alone enterprise-class appliances. Starting in 2007, UTM has started to appear in enterprises and data-center class networks. As stated before business managers and administrators viewed UTM appliances as a viable solution for the enterprise due to the low latency and high throughput performance requirements needed to support large size business with 500 or more users and for large size data centers. Past solutions also could not integrate with complex network topologies found in present-day enterprises. Moreover, network managers and administrators viewed UTM as a single-point failure, which is a major restraint for the market. Moreover, network and system administrators were looking for a more decentralized or distributed threat-solution to avoid performance-bottlenecks. Administrators were also quick to point out that UTM appliances could not handle the onslaught of the growing level of malware compared to enterprise-class anti-malware solutions. System administrators and their managers were also seeking solutions to prevent network-performance degradation posed by in-line solutions such as IDS. However, UTM providers, such as SonicWall and similar businesses recognized the shortcomings of the technology and developed solutions to meet the business needs of large enterprises. UTM providers developed enterprise-class appliances that provided low latency and high throughput while at the same time provided the required security-solutions, such as firewall, anti-malware, and IDS/IPS, in a single appliance.

In addition to providing a low total-cost of ownership and low-level complexity, UTM provides a higher level of agility as compared to disjointed or stand-alone network-security appliances. Disjointed or stand-alone security appliances lack the ability to be monitored and managed through centralized console. The lack of centralized management hampers system and network administrators to configure security appliances, to respond to 'blended threats'. Blended threats attack networks from multiple vectors, such as wired and wireless networks, using various vehicles, such as malware, social engineering, and root kits, to exploit the number of network and software vulnerabilities. The ability to respond effectively to these threats is hampered by the time it takes to configure stand-alone appliances. Depending on the number of stand-alone appliances and the number of system administrators needed to configure each appliance, it could take hours to respond to an emerging threat. However, existing UTM appliances provide centralized management consoles through command line or graphical user-interface. Centralized management allows system and network administrators the ability to configure and deploy network countermeasures from one centralized interface, thereby reducing hours to minutes, which are need to respond effectively to new threats. Additionally, centralized management has the potential to reduce the number of system administrators, either for an SMB or a small to medium size enterprise.

Apart from providing agile SMB and enterprise-class UTM technology, there is fierce competition between providers in the market. As a result, UTM companies are competing with one another by differentiating their products. Network-security giants, such as SonicWall and Fortinet are developing award-winning and corporately recognized UTM solutions that solve some of the common market restraints, such as being “single point for failure” and not being agile or robust enough for enterprise and data center class networks. The aforementioned vendors and their competitors are also developing products and solutions that address existing and emerging technology and compliance needs, such as Wi-Fi, data leakage, and payment card industry data security standards. The ability to address common leakage problems, such as social security and credit card numbers, from leaving the network. They also provide industry best practices of mapping commonly found corporate and government standards for their technology. This methodology has been found to be more appealing to both corporate leaders and their IT staffs. Therefore, companies, such as Fortinet, WatchGuard Technologies, Inc., and SonicWall INC., have won major contracts from both public and private institutions, such as the Department of Defense and Fortune 500 companies.

In terms of technology and market share, UTM providers, such as Fortinet, WatchGuard Technologies, Inc., and SonicWall have made significant gains in 2007. UTM providers are addressing emerging threats, such as blended attacks, scalable for any class of networks, and ability to meet present and future business needs, such as mobile workers and compliance issues. Fortinet's FortiASIC processor is one of the few products in the market that provide both heuristic detection along with signature-base technology. Therefore, the technology provides real-time protections against both known and unknown threats. WatchGuard Technologies, Inc.'s Firebox X Core technology is one of the leading UTM appliances that provide security for both mobile and teleworkers. Through the use of state-of-the-art, SSL/VPN, IPSEC, and PPTP augmented with single-sign-on authentication-security, Firebox X Core technology provides perimeter-class security for the growing number of mobile and teleworkers. Finally SonicWall's E-class network security appliance (NSA),UTM appliance-line has the scalability needed to be deployed in a medium to large-size enterprise. SonicWall's E-class UTM solutions provide deep-packet inspection without the high latency and low throughput found in similar products. The ability of providing deep-packet inspection with low latency and high throughput makes E-class and similar UTM products, a viable contender to enterprise-class stand-alone edge products, such as Cisco and Juniper's firewall and anti-malware appliances.

The 2007 world UTM market grew to \$1.6 billion in the US dollars, with an estimated 198,133 units sold worldwide. During the forecast period of 2008 to 2014, the market has an expected revenue of \$6.9 billion and a compound annual growth (CAGR) of 23.0 percent for revenues and 28.1 percent for units. 2007 to 2014. Qualitatively, the market continues to respond to the growing demand for the UTM appliances and services. Fueling the demand for UTM are the companies searching for solutions that have the ability to protect their networks from inbound and outbound threats, such as malware and user misuse. At the same time, they are looking for solutions that have a low cost of ownership and can be deployed in an SMB, branch office, or enterprise environment.

Figure 1-1 and Chart 1.1 show the revenue forecasts and unit sales for the world UTM market from 2004 to 2014.

FIGURE I - I

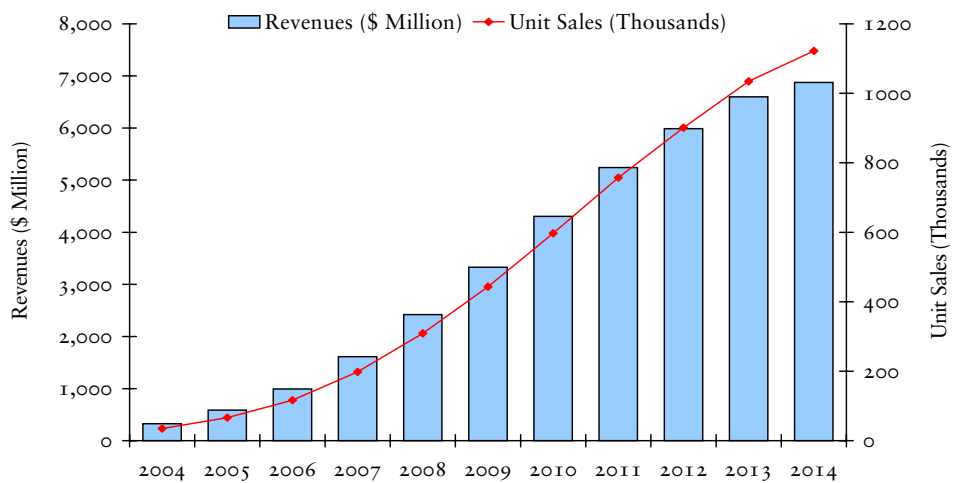
Total UTM Market: Revenue Forecasts and Unit Sales (World), 2004-2014

Year	Revenue		Unit	
	Revenues (\$ Million)	Growth Rate (%)	Unit Sales (Thousands)	Growth Rate (%)
2004	325.1	---	35.3	---
2005	587.8	80.8	66.5	88.3
2006	991.0	68.6	116.8	75.6
2007	1,613.6	62.8	198.1	69.6
2008	2,418.0	49.9	309.2	56.1
2009	3,330.0	37.7	443.4	43.4
2010	4,305.0	29.3	596.9	34.6
2011	5,242.0	21.8	757.1	26.8
2012	5,988.0	14.2	900.9	19.0
2013	6,599.0	10.2	1,034.2	14.8
2014	6,874.0	4.2	1,122.2	8.5
Compound Annual Growth Rate (2007-2014):		23.0%		28.1%

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

CHART I . I

Total UTM Market: Revenue Forecasts and Unit Sales (World), 2004-2014



Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

2

Total World Unified Threat Management Market

MARKET OVERVIEW AND GROWTH FACTORS

Market Overview and Definition

This research service provides executive summary, key findings, market drivers and restraints, as well as a high-level overview of market trends and forecasts analysis for the world Unified Threat Management (UTM) market. The study also provides a competitive analysis of companies, such as WatchGuard Technologies, Inc., Fortinet, and SonicWall who provide their UTM solutions through direct or indirect sales, such as in-house sales or value added resellers (VAR).

The base year for this study is 2007 and revenue forecasts and trends are provided through 2014. Historical data will also be quantified in an effort to reveal the trends since 2004. Market size and market share measurements reflect the actual results for 2007. All revenues are attributed to the world UTM market and segmented by geographical regions and vertical markets for further analysis.

The primary benefit of the UTM technology is its capability to secure the enterprise from both inbound and outbound threats from one appliance. The ability of providing protection from one appliance is essential to companies seeking products and solutions that address all Internet-based threats without the need of purchasing costly stand-alone appliances. UTM provides protection from inbound threats, such as malware and hackers. UTM also provides protection from insider threats, such as non-productive bandwidth draining applications, such as file sharing and data leakage, through content filtering and data leakage prevention (DLP) technology. These capabilities are essential for companies that are in need of a solution that can provide protection and assist in compliance with corporate, industry, and government regulations. UTM technology will also be an essential tool for corporations and businesses of all sizes seeking additional ways to secure and effectively leverage their messaging technology, such as e-mail, instant messaging, and emerging Web technology, such as Enterprise 2.0.

The critical need for protecting data and preventing data breaches makes a good case for IT managers or executives to request additional funding to purchase and deploy UTM solutions to the network. However, UTM also has its limitations. UTM technologies can become a single point of failure and sometimes lack the ability to support medium to large-sized enterprises and data centers. However, SonicWall and Check Point's products are addressing these concerns by integrating enterprise-class technology into their appliances. The integration of enterprise-class technology makes a single appliance fault-tolerant and self-scaling to meet the high throughput and low latency demands for medium to large-sized enterprises and data centers.

Figure 2-1 and Chart 2.1 Illustrates the global units and revenue projections for the total world UTM market forecast period, as well as their respective growth rates from 2004 to 2014.

FIGURE 2 - 1

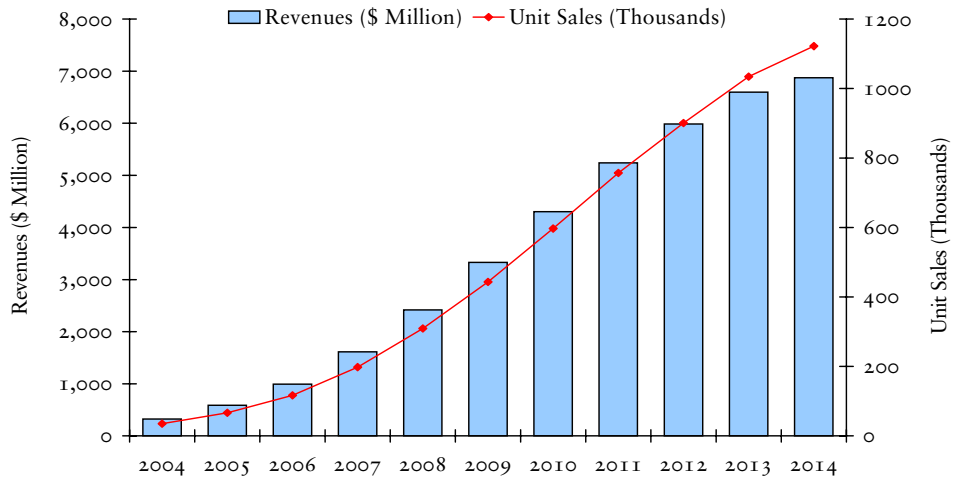
Total UTM Market: Revenue Forecasts and Unit Sales (World), 2004-2014

Year	Revenue		Unit	
	Revenues (\$ Million)	Growth Rate (%)	Unit Sales (Thousands)	Growth Rate (%)
2004	325.1	---	35.3	---
2005	587.8	80.8	66.5	88.3
2006	991.0	68.6	116.8	75.6
2007	1,613.3	62.8	198.1	69.6
2008	2,418.0	49.9	309.2	56.1
2009	3,330.0	37.7	443.4	43.4
2010	4,305.0	29.3	596.9	34.6
2011	5,242.0	21.8	757.1	26.8
2012	5,988.0	14.2	900.9	19.0
2013	6,599.0	10.2	1,034.2	14.8
2014	6,874.0	4.2	1,122.2	8.5
Compound Annual Growth Rate (2007-2014):		23.0%		28.1%

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

CHART 2.1

Total UTM Market: Revenue Forecasts and Unit Sales (World), 2004-2014



Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Market Engineering Measurements

MARKET STAGE

The UTM market is in a mature market stage. The market continues to grow at a fast pace. The high growth of the market is due to its ability to meet the multitude of present-day threats, such as phishing and blended-based attacks with signature-based technology. Additionally, UTM has the ability to meet over-the-horizon or zero-day threats, through use of heuristic and deep-packet inspection technology. The use of this technology enables UTM to detect and mitigate attacks before they become a threat to the enterprise. The market continue growing, due to the high demand for solutions that can meet present and emerging threats, while at the same, reduce the total cost of ownership.

An ideal UTM solution is comprised of a multitude of primary and secondary network-security products. The primary products are firewall, VPN, IDS/IPS, and anti-malware modules. These features are paramount in protecting any type of network from inbound threats. The primary features will also allow proper protection required by corporate, industry, state, or federal policy, regulations, and laws. Secondary UTM-security products and solutions can provide an additional layer of security protection from the emerging technologies and threats. North America, Western Europe, and portions of East Asia are expected to see an increase in the number of mobile and remote workers, due to energy and global-warming concerns. Therefore, corporations will need to find innovative ways to deploy corporate applications and services to their mobile workforce. Therefore, secure socket layer and virtual private network (SSL/VPN), application firewalls, and load balancing will be an essential part of an UTM solution. Without these technologies, business will be unable to address security problems associated with non-secure end-points that do not have the latest patches and antivirus signatures.

NUMBER OF COMPETITORS

Frost & Sullivan has found that vendors, such as SonicWall, WatchGuard Technologies, Inc., Fortinet, Juniper and Zyxel, are offering outstanding UTM solutions that have been deployed worldwide in governments, financial, and Fortune 500 companies. A majority of UTM customers, including government and private agencies, have pointed out that the aforementioned companies' UTM solutions were instrumental in preventing serious security breaches.

DEGREE OF TECHNICAL CHANGE AND PREDICTIONS FOR THE FUTURE

Even though the technology used in UTM appliances are similar to their stand-alone counterparts, the degree of technical change for the UTM market is higher. UTM appliances have shifted from being edge security-products for SOHOs, ROBOs, and SMBs and are currently protecting medium to large-sized enterprises and their data centers. UTMs are being designed to scale to meet the security needs of businesses, no matter their size. UTM products are being built with best-in-class products, materials to provide high throughput rates and low latency and have fail over, and load-balance capabilities. All of the aforementioned products are found in enterprise-class products. The future for UTM evolves its virtualization and is becoming part of a MSSP offerings. UTM providers are developing virtualized UTM products and solutions to meet the needs of the business. Virtualized UTMs will enable business companies to reduce the size of their data centers, save energy and cooling cost, and thereby, making the company 'greener' or environmentally responsible. MSSPs will also be able to market enterprise-class UTMs as a hosted or an on-premise management solution to businesses, no matter their size. MSSPs will also be able to harness virtualized UTM services either as a turnkey business model or as a software as a service (SaaS), for businesses seeking a short to medium-term security solution.

PRICE SENSITIVITY AND FUTURE PRICING

The overall price sensitivity for the UTM market is medium, due to a large variety of vendors and pricing strategy. As of 2008 there are over forty-one UTM companies offering a variety of UTM solutions. As of 2007, the market price for UTM appliances ranged from \$2,000 to \$20,000 and the average price per user was just over \$10.00 per users. However, larger enterprise deployments can cost anywhere from \$35,000 to \$100,000 dollars. The price UTM appliances is expected to decline by two or three percent each year, as more SMB and medium to large-sized enterprise businesses adopt UTM products and services.

Chart 2.2 shows the Market Engineering measurements for the total world UTM market for 2007.

CHART 2.2

Total UTM Market: Market Engineering Measurements (World), 2007

Market Engineering Drives Market Strategy and Planning



Measurement Name	Measurement	Trend
Market stage	Growth stage	Increasing
2007 revenues	\$1.6 billion	Increasing
Potential revenues (maximum future market size)	\$6.8 billion	Increasing
Base year revenue growth rate	62.8%	Decreasing
Forecast period revenue compound annual growth rate	23.0%	Decreasing
Potential unit sales (maximum future market size)	198,113	Increasing
Base year unit growth rate	69.6%	Decreasing
Forecast period unit compound annual growth rate	28.1%	Decreasing
Average device selling price	\$2,000 to \$20,000 per units	Decreasing
Price sensitivity	Medium	Increasing
Competitors (active market competitors in base year)	41	Decreasing
Degree of competition	Medium-High	Increasing
Degree of technical change	Medium-High	Increasing
Customer satisfaction	Medium	Stable
Customer loyalty	Medium	Stable
Market concentration	39.3%	Decreasing

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Market Drivers

REPLACING LEGACY OR OUTDATED POINT-SECURITY SOLUTIONS

Businesses of all sizes are looking to replace legacy or outdated point-security solutions, such as anti-malware gateways, routers, and stateful inspection-firewalls. However, with the recent downturn of the economy, business leaders are slashing budgets for all departments, including IT. Therefore, IT managers and executives are looking at UTM appliances as an affordable alternative to replace point-security solutions

Network and system administrators must configure each network device individually from separate consoles. This process uses a large amount of network resources, which are needed elsewhere. Additionally, stand-alone network security products are not agile enough to withstand zero-day or over-the-horizon attacks. It takes systems administrators minutes or hours for the systems to implement port blocks at firewalls, upload the latest signatures to anti-malware gateways, and upload patches to systems. However, UTM appliances can be monitored, configured, and managed from one central console. The administrator can use either a command line or graphical user interface to reconfigure network permissions, upload patches, and to deploy latest patches.

INCREASING FLEXIBILITY IN NETWORK SECURITY

In the past corporations of all sizes purchased network-security products as the need increased. For instance, a business would purchase anti-malware gateways or content-filtering solutions after network-wide virus outbreak or after being sued from sexual harassment after sexually explicit e-mail were sent throughout the company. However, most UTM products come with a plethora of network -security features that are built into one box. Primary security features, such as firewall and anti-malware services, are turned on during the initial installation. When an emergency or business-model change arises, other UTM features can be turned on or upgraded. For example, if a business is suspecting that someone is hacking its network, then it can turn on the IDS/IPS features. Additionally, businesses can add Wi-Fi protection while deciding to implement mobile services for their employees.

REGULATORY COMPLIANCE FOR THE NETWORK

As the inherent security risks of using computer networks evolve, federal and state legislation have been enacted to protect financial and other private information. Federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and California's data breach disclosure notification law SB 1386, directs the companies and agencies to seek out IT security solutions to protect their networks and data. Europe and Asia have learned from these widely publicized and costly security breaches and have enacted similar legislation, such as the European Union's Data Protection Directive and JSOX.. Emerging UTM products solutions are beginning to incorporate content filtering and DLP features. These features will be crucial in allowing the business to be compliant with present and future businesses, industry and government regulations and laws.

PROLIFERATION OF END-USER MOBILE TECHNOLOGY IN THE WORK PLACE

The proliferation of end-user mobile technologies, such as laptops, PDAs, and smartphones, has become common in today's work place. Corporations are replacing desktop workstations with laptops to allow more flexibility for the workers, such as working from home or to be more effective during business trips. Therefore, businesses will need to provide some form of network-security protection for their mobile and wireless users. Present and emerging UTM appliances have incorporated Wi-Fi firewalls into their UTM devices. Wi-Fi firewalls will protect business of various sizes, from both external and internal threats. The external threat of war-driving and other wireless threats can leverage UTM features, such as Wi-Fi firewalls, to protect their networks. Additional internal threats, such as wireless bandwidth consumption and non-productive wireless activities can be throttled by using Wi-Fi, imbedded in UTM products. UTM providers, such as SonicWall and WatchGuard Technologies, Inc. are offering Wi-Fi protection packages that automatically protect a business from external and internal Wi-Fi-based attacks.

WEB/ENTERPRISE 2.0 AND INSTANT MESSAGING IN THE WORKPLACE

UTM technology can become a vital counter-measure against controlling Web or Enterprise 2.0 and instant messaging (IM) technology in the work. An increasing number of organizations are allowing and encouraging employees to share ideas and experiences through corporate and public blog-site. Employees are also uploading documents or discussing personal identifiable or intellectual information over unprotected or publicly accessible corporate Web sites. As a result, corporations are experiencing data breaches, due to information being exposed on the site. UTM providers, such as Juniper, Check Point, and Astaro are incorporating their UTM products to counter or control Web/Enterprise and IM technology.

Figure 2-2 shows the market drivers ranked in order of impact for the total world UTM market from 2008 to 2014.

FIGURE 2 - 2

Total UTM Market: Market Drivers Ranked in Order of Impact (World) 2008-2014

Rank	Driver	1-2 Years	3-4 Years	5-7 Years
1	Replacing legacy or outdated point-security solutions	High	High	High
2	Increasing flexibility in network security	High	High	High
3	Regulatory compliance for the network	High	High	High
4	Proliferation of end-user mobile technology in the work place	High	High	High
5	Web/Enterprise 2.0 and instant messaging in the workplace	High	High	High

Source: Frost & Sullivan

Market Restraints

CONFLICTING BUDGET PRIORITIES

Conflicting budget priorities will be the key restraint that may prevent any new technology, such as UTM, from being deployed within a corporation's network. For the near future, corporate IT budgets are expected to continue competing with other internal budget requirements, such as research and development. Therefore, internal budget battles may prevent IT managers, chief security officers (CSOs), or chief information officers (CIOs), from seeking funding for network-security solution. However, IT managers, CSOs, and CIOs are likely to overcome this restraint by pointing out how a UTM product can cut cost, in terms of replacing stand-alone security products with one product

UTM IS NOT READY FOR ENTERPRISE OR DATA CENTER DEPLOYMENTS

Initially, UTM appliances were considered as a security solution for branch offices and SMBs. Network engineers argued that UTM appliances were not adaptable for medium to large-sized enterprises and data centers. Medium to large-sized enterprises and data centers need leading-edge products that provide low latency, load balancing, and high throughput capabilities. Additionally, engineers pointed out the fact that UTM could not withstand inbound attacks, such as 'denial of service' attacks, due to their low throughput. However, companies, such as Juniper, SonicWall/SONICWALL, INC., and Check Point, have developed UTM appliances to meet the need of enterprises and data centers. Their products provide a high level of security that has high performance, high throughput, and low latency.

CREATING NETWORK BACKDOORS

The notion of putting a single product at the network gateway to manage routing and security causes fear and hesitation in the minds of corporate executives and IT managers. However, UTM providers of all sizes, such as Astaro and Juniper have addressed this issue by adding load balancers and failovers technology.

ECONOMIC DOWNTURN

Due to sub-prime loan and bank failures, some companies hesitate to upgrade their computer infrastructure. Therefore, businesses and corporation of all sizes have slashed employee operations and IT budgets. Consequently, IT-purchases, such as network infrastructure deployments, have been placed on hold or have been cut altogether. Again, company executives and network managers can harness the cost benefits from UTM. UTM technology can cut cost, in terms of managing stand-alone network-security products, personnel needed to manage different appliances, and power and cooling cost needed for desperate network appliances.

THE INABILITY OF PROVIDING SECURITY OUT OF THE BOX

With all network security products, IT administrators and managers complain that security products do not provide security “out of the box.” UTM is not immune to this criticism. Administrators and managers are fearful of a high learning-curve and the time needed to configure UTM products and solutions to immediately provide protection for their network. However, UTM providers, such as Juniper, SonicWall, and Cisco are incorporating GUIs that are familiar to the common day network or system administrators who are familiar with their products. Additionally, the GUI is very intuitive and allows systems administrators to configure and deploy the data protection package to the enterprise within hours.

'IF IT'S NOT BROKE WHY SHOULD I REPLACE IT' MENTALITY

As with budget restraints and other financial priorities, many businesses are reluctant to replace their legacy network-security products, because they feel that they are protecting their networks. While this is understandable, it will be important for the network security providers to explain to potential customers that outdated security-products, such as firewalls, cannot protect networks from present and emerging security threats.

APPLICATION SUPPORT AND POLICY OBSTACLES

Many system administrators and business leaders are fearful that UTM appliances are unable to support their Web-based applications and security policies. However, this restraint is quite rare. UTM vendors are providing appliances with application firewalls and other features that scan for vulnerabilities and threats at all levels of the OSI stack. Additionally, UTM providers are mapping UTM configurations and networking rules to be in line with current company, industry, and government regulations.

Figure 2-3 shows the market restraints ranked in order of impact for the total world UTM market for 2008-2014.

FIGURE 2 - 3

Total UTM Market: Market Restraints Ranked in Order of Impact (World), 2008-2014

Rank	Restraint	1-2 Years	3-4 Years	5-7 Years
1	Conflicting budget priorities	High	High	High
2	UTM is not ready for enterprise or data center deployments	High	High	Medium
3	Creating network backdoors	High	Medium	Medium
4	Economic downturn	High	Medium	Low
5	The inability of providing security out of the box	High	Medium	Low
6	'If it's not broke why should I replace it' mentality	High	Medium	Low
7	Application support and policy obstacles	High	Medium	Low

Source: Frost & Sullivan

MARKET TRENDS AND FORECASTS

Revenue Forecasts

In 2007, the UTM market revenues grew at a rate of 62.8 percent and the unit growth rate was 69.6 percent. Worldwide revenues grew \$1.6 billion in revenues with over 198 thousand units sold worldwide. The estimated compound annual growth rate (CAGR) from 2007 to 2014 is 23.0 percent for revenues and 28.1 percent for unit sales. The overall prediction for this market is a sustained growth and in some cases a rapid growth throughout the forecast period. Sustained and rapid growth will contribute to UTM developers providing enterprise-class appliances and corporations that are undergoing a technology refresh, which involves the decommissioning of non-effective or legacy security-products. Additionally, they are seeking solutions to integrate their disjointed or stand-alone network-security appliances, such as anti-malware and content-filtering appliances. Lastly, corporations are looking for solutions that will assist in their 'going green' initiatives. The initiatives are in response to the recent 'Green IT Movement'. The movement is motivating data center size reduction and the lessening of cooling and power cost. From a system or network administrator's viewpoint, they are looking for network-security solutions that can be monitored and configured from a centralized console. Centralized consoles provide the required speed and agility to deploy network counter measures to counter the growing magnitude, lethality, and speed of external and internal attacks, such as blended attacks and data leakage.

New malware and hacking tools are becoming so effective that they can circumvent firewalls and intrusion-detection systems within seconds. Network-security experts have publicly argued that UTM appliances do have the required agility and speed to combat existing and emerging threats. They are campaigning that a centralized network-security solution would allow administrators to quickly configure and deploy counter measures to combat threats. An average network administrator spends hours reconfiguring, monitoring, and updating firewalls, content filtering, and anti-malware-appliances to combat the latest threat. Providers have designed UTM appliances to meet corporate, industry, and government regulations. Both smaller and larger UTM providers, such as Check Point and Astaro are mapping their technology to cover a corporation's 'acceptable-use policy' and industry standards, such as PCI-DSS and government banking regulations, such as Sarbanes Oxley. The mapping of technology will allow businesses to quickly deploy solutions, while at the same, meeting corporate, industry, and government compliance. No matter the size of the corporations or businesses, their networks are vulnerable to attacks. Therefore, all vertical markets are in need of a UTM solution to protect their networks, data, and end users. They are also looking for solutions to be as compliant with laws, such as HIPPA and SOXs. Any violation of the laws can result in large fines and penalties.

In 2007, the average UTM appliances cost corporations from \$2 to \$20,000 per unit that equated to \$2 to \$20 per a user. However, wide scale or enterprise deployments of UTM appliances for the both enterprises and branch offices are estimated to cost in the \$100,000 to \$1 million dollar range. Despite the need for UTM products and solutions, unit sales prices are projected to decline from two to four percent a year, throughout the forecast period. The forecast is predictable, due to the increased demand for UTM appliances and solutions from all types of companies. Therefore, there are a large number of small to mid-sized UTM providers competing with UTM giants, such as the WatchGuard Technologies, Inc., Cisco Systems, Inc., and Junipers. Smaller UTM providers, such as Calyptix, are winning larger deals, due to their ability to deliver product- services that are tailored to their customer's needs. Additionally, larger network-security providers, such as Cisco who is participate in multiple markets will find increased competition from UTM providers, such as Astaro, that concentrates only on UTM technology. Stand-alone providers are more concentrated on engineering UTM technology and are therefore, more disciplined and astute with the technology. Stand-alone UTM providers are offering more efficient products that quickly and seamlessly integrate with other software and network vendors, such as IBM and Microsoft.

Degree of Technical Change

Due to the need for increased network size and growing cost of maintaining them, the need for virtualized offerings will be an effective element for UTM technology. UTM providers, such as Crossbeam are providing virtualized appliances to meet the needs of corporations seeking to reduce the size of their networks and data centers. Companies, such as Crossbeam, provide enterprise-class virtual security appliances that have programmable architectures that provide the most advantageous prices and performance needed to protect medium to large-size enterprises. By providing best-in-class architectures, companies such as Crossbeam, are delivering available, reliable, and best-in-class security on virtualized platforms.

Geographical Trends

In 2007, the North American market accounted for 46.0 percent of total UTM sales. North America's market share is due as a result of companies of all sizes seeking integrated solutions that quickly fight inbound and outbound threats. Also, corporations are seeking ways to reduce the cost, in terms of personnel and network-appliance purchases. Moreover, the U.S.-based business corporations need to comply with the numerous federal and industry laws and regulations that govern the primary verticals, such as healthcare, government, finance, and utilities.

The European/Middle East and Africa (EMEA) and Asia Pacific accounted for 39.6 percent and 13.3% of the total UTM market. Europe and Asia are experiencing explosive growth, due to similar needs found in the United States.. Almost all European-based companies are pushing for green technology. UTM technology is being used as a solution for this need.

The Latin America region accounted for only 1.1 percent of the market, although it is poised to be a revenue-generating wildcard. Currently, the LA region is unlikely to experience significant growth, due to the lack of stable electrical and information networks. However, as the region's telecommunication and computer-network infrastructure grows, the LA region will start to experience growth. The start of growth will be attributed to security needs to secure the emerging infrastructure. At present, Latin America lacks intellectual resources needed to manage their growing infrastructure. However, as the region grows, so will their education and technological needs. As a result, the Latin American population will become educated and talented enough to handle their own network needs. Therefore, they will be in a position to offer a rich source of off shore opportunities for the North American companies that are seeking to enter the Latin American market or to offshore their activities to this region.

In 2007, the North American UTM market accounted for \$742.3 million in revenues with over 91 thousand units sold. Again, North America's market share is due to business of all sizes seeking integrated solutions that quickly fight inbound and outbound threats. Secondly, corporations and businesses are seeking ways to reduce in terms of personnel and network appliance purchases. Lastly, US based business and corporation need to comply with the numerous federal and industry laws and regulations that govern the primary verticals such as healthcare, government, financial and utilities. Although the North American market is suffering from an economic downturn and a weakening dollar, the market is predicted to experience steady growth, due to the need for security safeguards. Additionally, the North American companies will benefit from a weak dollar, due to the rise of foreign currency such as the EU's Euro, which can buy more products and services from the U.S.-based companies. By 2014 the North American UTM market is expected to reach \$3 billion in sales with over 489 thousand units sold. The estimated CAGR for the market is 31.1 percent in terms of revenues and 27.2 percent in unit sales from 2007 to 2014.

In 2007, the EMEA UTM market was worth over \$638.8 million with 78.3 thousand unit sold. The market is estimated to grow at a CAGR of 22.7 percent in revenues and 27.8 percent in unit sales from 2007 to 2014. The EMEA UTM market is expected to grow, due to similar North American computer-network needs. Additionally, the European Union is pushing the 'Green Initiative' to its members. Moreover, former Soviet block countries, such as Russia, Ukraine, and Yugoslavia, and North African countries, such as Egypt, are likely to experience a moderate growth. The aforementioned countries are updating their outdated computer network and telecommunication infrastructures to be in step with 21st century technology and to be competitive in the global market. By 2014, the EMEA UTM market is likely to account for \$2.7 billion in revenues, with over 437 thousand units sold.

In 2007, the Asia Pacific UTM market demonstrated a steady growth of 65.0 percent, resulting in \$214.5 million in revenues and only 26.3 thousand units were sold in the region. Frost & Sullivan expects Zyxel to be a major participant, in the Asia Pacific region due to its strong presence and acceptance in the region. Zyxel is leveraging its UTM offerings to meet the UTM needs for the region. By 2008- 2014, the region is expected to reach \$1.1 billion in revenues, with over 178.9 thousand units sold in the region. This is expected to represent impressive revenues and unit sales that are likely to grow at a CAGR of 26.2 and 32.0 percent, respectively.

The Latin American UTM market is currently experiencing a steady but minimal amount of growth due to marginal adoption rates in their limited electrical and data infrastructure. However, Frost & Sullivan believes that Latin America is a largely untapped market that has the potential to be a windfall for technology deployments, similar to India and China. Information and telecommunication companies that provide leadership and reasonable investments in the region will be the predominate providers in the region. In 2007, the region generated only \$18.0 million in revenues and 2.2 thousand units were sold in the region. The market is predicted to grow to \$101.0 million in revenues by 2014, as smaller telecommunication and IT vendors attempt to improve their IT infrastructure to be on par with the 21st century technology.

Figure 2-4 shows the revenue forecasts and unit sales for the North American UTM market from 2004 to 2014.

FIGURE 2 - 4

UTM Market: Revenue Forecasts and Unit Sales (North America), 2004-2014

Year	Revenue		Unit	
	Revenues (\$ Million)	Growth Rate (%)	Unit Sales (Thousands)	Growth Rate (%)
2004	140.0	---	15.2	---
2005	260.0	85.7	29.4	93.5
2006	450.0	73.1	53.0	80.3
2007	742.3	65.0	91.1	71.8
2008	1,100.0	48.2	140.6	54.3
2009	1,500.0	36.4	199.7	42.0
2010	1,900.0	26.7	263.5	31.9
2011	2,290.0	20.5	330.8	25.6
2012	2,650.0	15.7	398.7	20.5
2013	2,899.0	9.4	454.3	14.0
2014	3,000.0	3.5	489.8	7.8
Compound Annual Growth Rate (2007-2014):		31.1%		27.2%

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Figure 2-5 shows the revenue forecasts and unit sales for the EMEA UTM market from 2004 to 2014.

FIGURE 2 - 5

UTM Market: Revenue Forecasts and Unit Sales (EMEA), 2004-2014

Year	Revenue		Unit	
	Revenues (\$ Million)	Growth Rate (%)	Unit Sales (Thousands)	Growth Rate (%)
2004	137.0	---	14.9	---
2005	245.0	78.8	27.7	86.3
2006	400.0	63.3	47.1	70.1
2007	638.8	59.7	78.4	66.4
2008	950.0	48.7	121.5	54.9
2009	1,300.0	36.8	173.1	42.5
2010	1,680.0	29.2	232.9	34.6
2011	2,050.0	22.0	296.1	27.1
2012	2,300.0	12.2	346.0	16.9
2013	2,550.0	10.9	399.6	15.5
2014	2,677.0	5.0	437.0	9.4
Compound Annual Growth Rate (2007-2014):		22.7%		27.8%

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Figure 2-6 shows the revenue forecasts and unit sales for the Asia Pacific UTM market from 2004 to 2014.

FIGURE 2 - 6

UTM Market: Revenue Forecasts and Unit Sales (Asia Pacific), 2004-2014

Year	Revenue		Unit	
	Revenues (\$ Million)	Growth Rate (%)	Unit Sales (Thousands)	Growth Rate (%)
2004	45.0	---	4.9	---
2005	77.0	71.1	8.7	78.2
2006	130.0	68.8	15.3	75.9
2007	214.5	65.0	26.3	71.9
2008	340.0	58.5	43.5	65.1
2009	490.0	44.1	65.2	50.1
2010	670.0	36.7	92.9	42.4
2011	830.0	23.9	119.9	29.0
2012	950.0	14.5	142.9	19.2
2013	1,050.0	10.5	164.6	15.1
2014	1,096.0	4.4	178.9	8.7
Compound Annual Growth Rate (2007-2014):		26.2%		31.5%

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Figure 2-7 provides the revenue forecasts and unit sales for the Latin American UTM market from 2004 to 2014.

FIGURE 2-7

UTM Market: Revenue Forecasts and Unit Sales (Latin America), 2004-2014

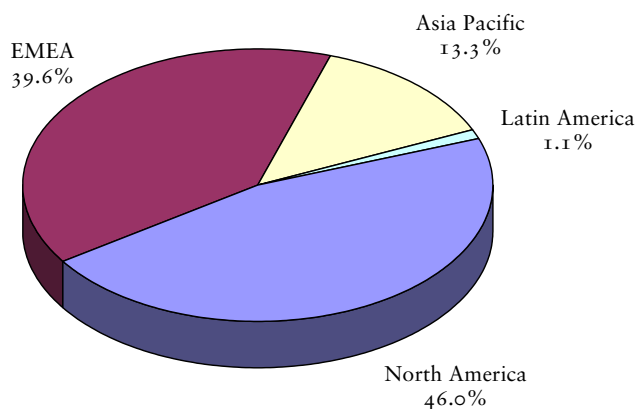
Year	Revenue		Unit	
	Revenues (\$ Million)	Growth Rate (%)	Unit Sales (Hundred)	Growth Rate (%)
2004	3.1	---	337	---
2005	5.8	87.1	656	94.9
2006	11.0	89.7	1,297	97.6
2007	18.0	64.0	2,214	70.8
2008	28.0	55.3	3,580	61.7
2009	40.0	42.9	5,326	48.8
2010	55.0	37.5	7,626	43.2
2011	72.0	30.9	10,399	36.4
2012	88.0	22.2	13,240	27.3
2013	100.0	13.6	15,672	18.4
2014	101.0	1.0	16,489	5.2
Compound Annual Growth Rate (2007-2014):		27.9%		33.2%

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Chart 2.3 shows the percent of revenues by geographic region for the total world UTM market for 2007.

CHART 2.3

Total UTM Market: Percent of Revenues by Geographic Region (World), 2007



Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Vertical Market Analysis

All the market verticals use UTM appliances. However, over 48 percent of UTM appliances are found in SMBs, SOHOs, and ROBOs with the remaining 51 and 1 percent are being deployed in enterprises and SOHOs. During 2004 to 2006 SMBs followed by SOHOs were the primary buyers of UTM appliances. However, in 2007, enterprises became the largest buyer of UTMs. Enterprises are buying UTM solutions to replace aging equipment and they are also attracted to its low cost and ease of deployment.

Figure 2-8 provides the percent of revenues by market vertical for the total world UTM market from 2004 to 2014.

FIGURE 2 - 8

Total UTM Market: Percent of Revenues by Market Vertical (World), 2004-2014

Year	Finance (%)	Man (%)	Med (%)	Govt (%)	Tech (%)	Uti (%)	Media (%)	Edu (%)	Leg (%)
2004	33.0	6.0	30.0	18.0	6.0	2.0	2.0	2.0	1.0
2005	31.0	5.5	29.6	18.0	6.3	2.8	2.8	2.5	1.5
2006	32.0	5.0	28.0	18.0	6.4	3.0	3.3	2.8	1.5
2007	32.6	4.7	24.8	17.4	6.7	3.3	4.5	3.2	2.8
2008	33.0	5.0	26.0	17.7	7.0	3.0	4.0	3.3	1.0
2009	31.0	5.2	26.8	18.9	7.3	2.8	4.0	3.0	1.0
2010	31.4	5.4	27.0	19.0	7.8	3.4	3.0	2.0	1.0
2011	32.1	5.5	27.5	19.5	8.0	2.4	2.0	2.0	1.0
2012	32.8	5.6	28.0	20.0	8.2	1.4	1.0	2.0	1.0
2013	35.0	5.0	28.0	20.0	8.0	1.0	1.0	1.0	1.0
2014	35.0	5.0	28.0	20.0	8.0	1.0	1.0	1.0	1.0

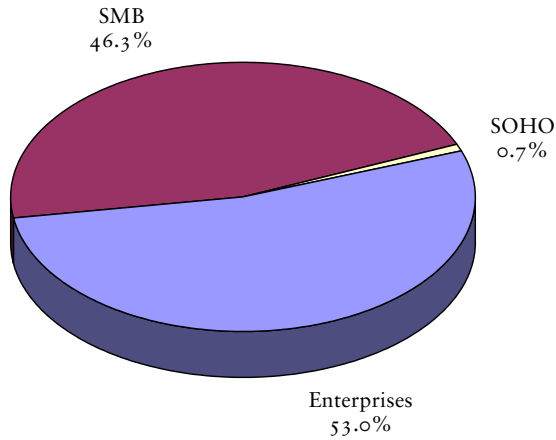
Key: Man = Manufacturing
 Med = Medical and Healthcare
 Govt = Government
 Tech = Technology
 Uti = Utility
 Edu = Education
 Leg = Legal

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Chart 2.4 illustrates the percentage of UTM sales for SOHO, small to medium sized businesses and large enterprises

CHART 2.4

Total UTM Market: Small/Home Office to Enterprise Percent of Sales (World), 2007

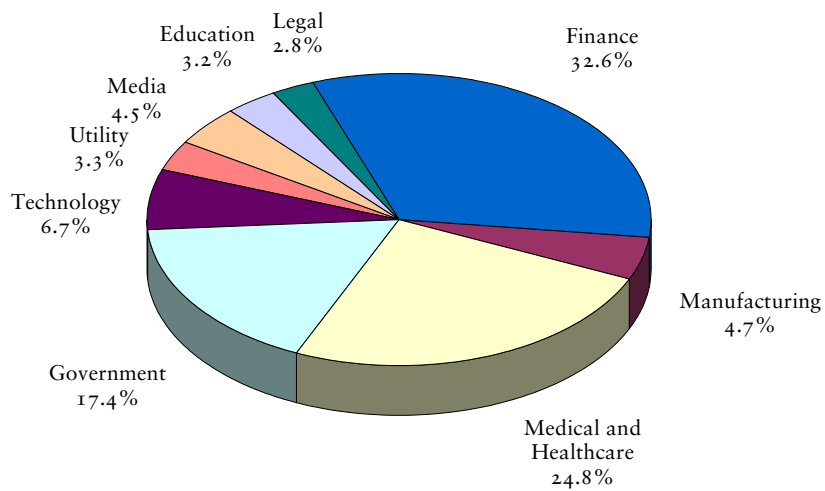


Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Chart 2.5 illustrates the percent of revenues by market vertical for the total world UTM market in 2007

CHART 2.5

Total UTM Market: Percent of Revenues by Market Vertical (World), 2007



Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Technology Trends

The initial UTM appliances provide stateful packet-inspections and IPSEC VPN technology. However, upgraded models of UTM appliances offer deep packet-inspection, SSL/VPN and content filtering. The introduction of these technologies into the appliances is important to meet the needs of enterprises, network security, and compliance requirements.

UTM technology has also evolved to counter application-layer attacks with application-layer firewalls. Hackers are using various methods to take advantage of Layer-7 vulnerabilities found in database, office suite, and business-oriented technologies, such as SQL, Lotus Notes, and SAP. These methods can quickly circumvent both traditional and present-day network-security technology, due to the weakness of Layer-7 based technology. Therefore, UTM providers, such as SonicWall, Check Point, and Crossbeam have incorporated application-layer firewall technology in their solutions. Their technology provides a means to construct granular application-specific policies. The policies offer access-control measures for the actual user, application, system, or person's IP at the subnet level. This granular process controls how applications and end users transfer information, use bandwidth, and Web-based applications.

The final technological trend for UTM is the virtualization of UTM appliances. Network-security appliances take up as much room as other network and server appliances. The green IT movement is motivating the business world to reduce the size of its data center through virtualization. Therefore, UTM providers, such as IBM, are developing virtualized UTM appliances. Virtualized UTMs will continue having the required primary and secondary security features, such as firewall/VPN, anti-malware, IDS/IPS, and content filtering. However, virtualized UTM will enable the reduction of data center's floor space and will reduce power and cooling cost. Additionally, UTM will be a desired area for MSSPs and SaaS providers. MSSPs will be in a position to offer present and potential customers with a solution, which reduces the size of their networks and to help go green. SaaS providers will be in a position to provide virtualized UTM appliances as a software service. Potential buyers could purchase UTM services on an as needed basis or as a monthly subscription. Therefore, SaaS providers can market virtualized UTM appliances as a cost-saving measure. For business will no longer have to purchase any hardware.

Distribution Trends

The distribution channel for UTM solutions, products, and services is primarily through VARs. VARs accounted for 95.6 percent of the market while the remaining 4.4 percent were sold directly to businesses or OEM'd to other companies. The sale of UTM's are primarily hardware-based and therefore account for 92.8 percent of market sales. However, UTM providers, such as Astaro, are offering software solutions and they account for 7.2 percent of market sales.

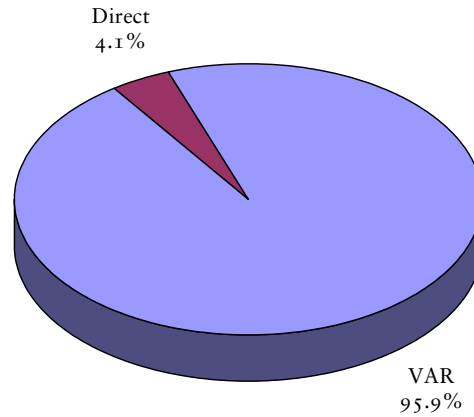
Normally, UTM products and services are delivered through appliances. However, companies such as Astaro, are offering UTM as a software option. The software could be loaded on third-party server hardware. MSSP providers, such as Global Data Guard and IBM/ISS, are offering UTM services through hosting or on-premise management. However, the MSSP market segment makes up less than 1 percent of the market only. UTM SaaS market is in its infancy. As a result, MSSPs and UTM appliance providers are experimenting with technology and are testing marketing strategies. Frost & Sullivan predicts that the market is expected to see an increased need for MSSP and SaaS services, as companies are seeking low-cost IT solutions, due to a slow down in the global economy.

With the exception of UTM providers, such as Check Point and Calyptix, most other UTM providers purchase their content filtering and anti-malware technology from larger content filtering and anti-malware companies. The primary providers are Kaspersky, Websense, Symantec, and McAfee. Kaspersky anti-malware technology can be found in 45 percent of UTM vendor offerings. Websense, McAfee, and Symantec can be found in 19, 20, and 9 percent of UTM appliances, respectively. Juniper Networks is a perfect example of a company that has integrated best-in-class anti-malware and content-filtering technologies into their UTM products and solutions. Juniper is using Kaspersky's gateway-antivirus technology to prevent malicious inbound traffic. Juniper is also using Websense's web-filtering technology for outbound protection. Websense technology provides DLP and outbound content filtering for acceptable use and policy-enforcement. They are also using Symantec's anti-spam technology to filter unwanted e-mail.

Chart 2.6 illustrates the percent of revenues by sales channel for the total world UTM market in 2007.

CHART 2.6

Total UTM Market: Percent of Revenues by Sales Channel (World), 2007

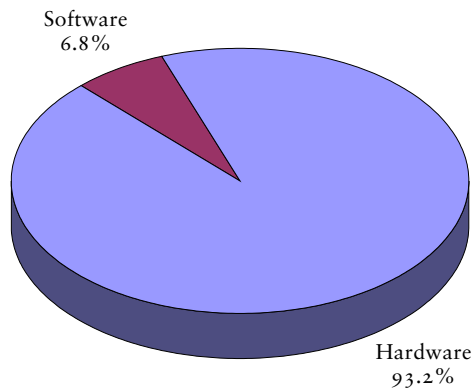


Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Chart 2.7 illustrates the percent of hardware versus software sales for the total world UTM market in 2007.

CHART 2.7

Total UTM Market: Percent of Software versus Hardware Sales (World), 2007

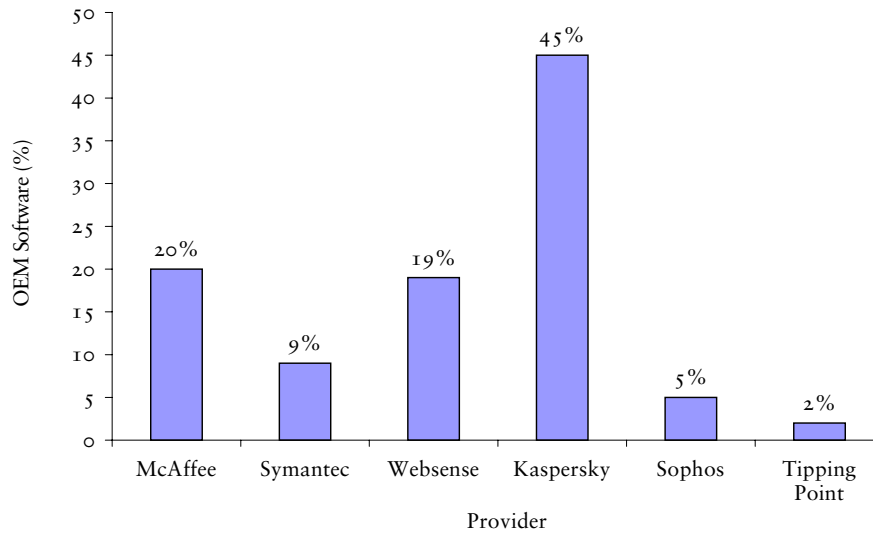


Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Chart 2.8 illustrates the percent of the type of OEM software per provider for the total world UTM market in 2007.

CHART 2.8

Total UTM Market: Percent of the Type of OEM Software per Provider (World), 2007



Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Pricing Trends

In 2007, the average UTM appliance cost businesses and corporations two to twenty-thousand dollars per unit. The price equates to \$2 to \$20 for business with more than a thousand employees and businesses with less than one-hundred employees. However, some deployments that involved installing units throughout the enterprise, which includes ROBOs and SOHOs, have the potential to cost more than one-hundred thousand dollars. Despite the need for UTM products and solutions, unit sales are projected to increase from two to four percent a year throughout the forecasting period. The forecast is predictable due to increase demand for UTM appliance and solutions for all types of businesses.

Figure 2-9 and Chart 2.9 illustrates the average price offered by major market participants for the total world UTM market in 2007.

FIGURE 2 - 9

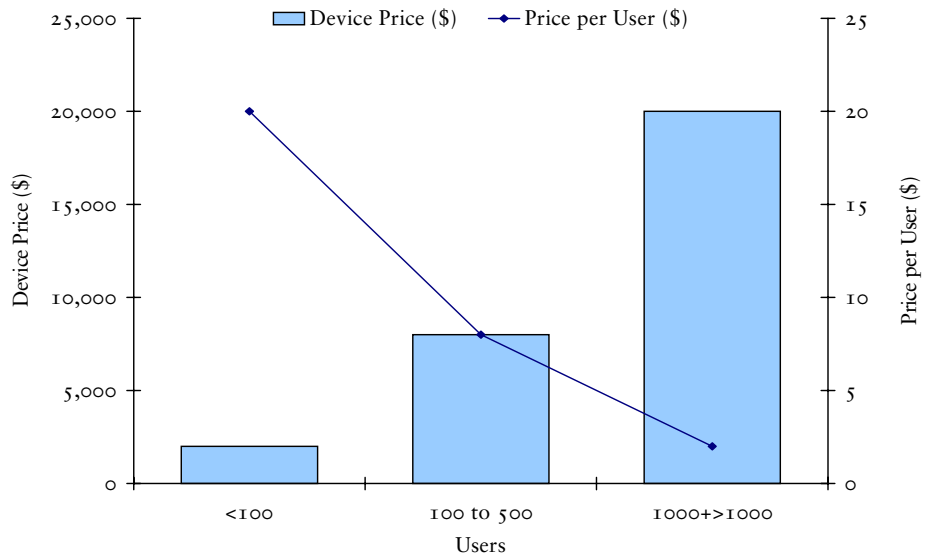
Total UTM Market: Average Price Offered by Major Market Participants (World), 2007

Users	Device Price (\$)	Price per User (\$)
<100	2,000.00	20.00
100 to 500	8,000.00	8.00
1000+>1000	20,000.00	2.00

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

CHART 2 . 9

Total UTM Market: Average Price Offered by Major Market Participants (World), 2007



Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Legislative Trends

Federal and state legislation, such as HIPPA and SOX's, along with industry specific rules, such as PCI have been some of the primary drivers behind the acceptance and implementation of UTM technology by the governments, public and private agencies, and companies. The laws and regulations require that governments and public and private businesses to implement safeguards, to protect personal information that resides in their databases. The loose or public disclosure of personal, financial, and medical information, such as social security numbers, credit card information, and medical records, can result in legal ramifications ranging from fines to incarceration. Government agencies and businesses are struggling to map laws and regulations to communication technology in order to comply with federal, state, and industry requirements. The following is a list of significant legislation and regulations, which have been enacted, regarding communications security. Additionally, other countries and states, such as Japan and Utah, are enacting similar laws that mirror the United States' SOX and California's Law SB 1386.

HOMELAND SECURITY

Homeland security's primary purpose is that of mobilizing and organizing the United States, to secure the country from terrorist attacks and reduce the vulnerabilities to terrorism, as well as coordinate efforts after terrorism occurs. At the federal level, critical infrastructure needs to share information and streamline information-sharing among law enforcement and intelligence organizations. Furthermore, there are plans to improve extradition personnel, military organizations, and the organization of the departments that are involved in national security and fighting terrorism. The President of the United States has outlined plans to create a new Department of Homeland Security that will bring together 22 different entities that currently play a role in homeland-security actions. The division of funding to the various government levels is yet to be determined and is in the preliminary stage. Funding is likely to focus on infrastructure, initial response, and information sharing between federal agencies, horizontally, and between federal, state, and local levels, vertically. This is expected to create major changes in the level of participation at the federal level. While the dollar amount at the federal level will depend on the Congress and the President, this legislation has increased the awareness and demand for managed security services.

CALIFORNIA LAW SB 1386

SB 1386 requires anyone doing business in California to notify anyone whose personal information has been obtained by an unauthorized party. Essentially, this law requires businesses to make public, any security breach that results in the compromise of personal information. By holding entities responsible for disclosing security breaches, they are likely to be more motivated to prevent such security breaches; thus, stimulating a demand for security products and services.

THE PATRIOT ACT

The Patriot Act improves the ability of government agencies to monitor communications. This legislation expands the government agency access to many types of electronic communications and requires that financial institutions keep new information records to verify customer identities. This increases the amount of confidential information that financial institutions must hold; thus, increasing the demand for security measures.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was signed into a law on August 21, 1996. The main goals of the HIPAA are to guarantee health insurance coverage for workers during job transitions, protect the privacy of patient records, and promote national, uniform security standards for the secure electronic transmission of health information. As organizations conform to HIPAA compliance regulations, a host of security solutions are being experimented with and implemented by hospitals, doctors, pharmacies, and insurance companies.

GLB

The Gramm-Leach-Bliley (GLB) is also known as the Financial Services Modernization Act. This act is targeted at the financial market and has many implications regarding the affiliations among banks, securities firms, and insurance companies. The act requires financial institutions to establish administrative, technical, and physical safeguards to ensure the confidentiality of customer records. GLB also prohibits firms from reusing or disclosing such information without the explicit permission of the customer and requires financial institutions to provide their privacy policies to the customers. This legislation has only added to the momentum created in the financial sector.

GOVERNMENT INFORMATION SECURITY REFORM ACT

This is also known as the Security Act was enacted when the U.S. GISRA amended the Paperwork Reduction Act (PRA) of 1995, by specifying new requirements, which addressed the program management and evaluation aspects of security. The Act applies to all agencies covered by the PRA. The Security Act codifies the existing requirements of the Office of Management and Budget (OMB) appendix, "Security of Federal Automated Information Resources" and requires agencies to incorporate security into the life cycle of agency-information systems. The Security Act aims to institute a system of best practices and requires that agency programs develop a formal security policy.

COMPUTER SECURITY ENHANCEMENT ACT OF 2001

This act was passed to amend the National Institute of Standards and Technology Act (NIST) in order to enhance the ability of the NIST to improve computer security. This act extends to prior efforts to promote compliance by federal agencies with existing federal computer information security and privacy guidelines.

BASEL II

Basel II is one of the series of accords held by the world's central bankers under the direction of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland. While the original accord was established in 1988 and focused on issues of credit and market risk, the most recent amendment of Basel II has specified an increased emphasis on operational risks, which includes information security, amongst others. Moreover, the accords stipulate that operational risks are to be calculated using one of the three methods: the basic, standardized, or advanced measurement approach. The latter is typically favored by the largest banks.

CANADIAN PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

The Canadian Personal Information Protection and Electronic Documents act defines the rules for protecting personal information that is collected, used, or disclosed in the course of commercial activity. Similar to other acts, the provisions are phased in over time. Since January 2004, these provisions cover all personal information that enters the commercial sphere.

SARBANES - OXLEY ACT

The Sarbanes-Oxley Act is also referred to as the Public Company Accounting Reform and Investor Protection Act, which was enacted in response to the numerous corporate accounting scandals that began to emerge in 2001. The Sarbanes-Oxley Act requires (among other things) annual reports to assess the effectiveness of internal controls and procedures for financial reporting. Section 404 of the Sarbanes-Oxley Act requires companies to perform a self-assessment of risks for business processes that affect financial reporting. Since there are inherent risks with IT systems that store sensitive financial information, SOX requires businesses to deploy protective measures to protect for their data. The task of protection becomes more difficult with the allowance of partners, suppliers, customers, and even a company's own employees' access to various portions of the network.

EUROPEAN DATA PROTECTION DIRECTIVE

The European Data Protection Directive addresses identity theft, online fraud, and privacy issues related to consumers, employees, and citizens and harmonize privacy laws among the EU members. All member states must adopt this privacy legislation or revise the existing laws. These rules ensure that personal data may be transferred only to non-EU countries that provide equivalent protection.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

In 2005, the Payment Card Industry Data Security Standard (PCI DSS) was created, due to the large amount of credit card information stolen from vendors' databases. The PCI DSS was a joint effort between American Express, Discover, Master Card, and Visa to provide a universal security standard for organizations, which process credit card transactions. PCI DSS calls for encryption and other data-security methods to protect credit card information. Any violation of PCI DSS can result in severe penalties from the PCI

COMPETITIVE ANALYSIS

Competitive Structure

The competitive structure of the world UTM market evolved substantially during in 2007. Figure 2-10 profiles the competitive structure of the market by the number of companies in the market, types of competitors, distribution structure, tiers of competition, key end-user groups, and competitive factors

FIGURE 2-10

Total UTM Market: Competitive Structure (World), 2007

Number of Companies in the Market	44
Types of Competitors	Pure plays, resellers, consolidated networking vendors
Distribution Structure	Direct, VAR
Tiers of Competition	3 Tiers, 39.5% market concentration
Notable Acquisitions, Mergers	None to report
Key End-user Groups	Vertical markets: healthcare, government, financial, education, legal, manufacturing, technology, utilities
Competitive Factors	Scalability of products, throughput, stability, GUI, deep packet inspection and fail over

Source: Frost & Sullivan

Frost & Sullivan believes that UTM technology is an overall solution to protect all sizes of businesses companies. Frost & Sullivan defines UTM as a hardware or software solution that provides inbound network and traffic protection through service such use of firewalls, Virtual Private Networks (VPN) Intrusion Detection and Prevention Systems (IDS/IPS) and anti malware. In conjunction with the aforementioned specifications, UTM is also defined as any solution that provides content filtering and emerging security technologies such as Wireless Fidelity (Wi-Fi) and Data Leakage Prevention (DLP).

The distribution channel for UTM technology and solutions is primarily through VARs. VARs accounted for 95.6 percent of the market, while the remaining 4.4 percent was sold directly to business or OEM'd to other companies.

There were no notable acquisitions in 2007 as found in other network-security markets. This was due to a mature market being dominated by network-security giants, such as WatchGuard, Cisco, Check Point, Fortinet, and SonicWall. Each company accounted for 75 percent of the market. End-user verticals, such as healthcare, government, and financial banking are the primary consumers in the UTM market as they must be compliant with the government and industry laws and regulations. Most end users agree that price-points or sales factors, such as scalability, speed, and network-policy enforcement, are the main elements used when comparing UTM offerings.

Figure 2-11 provides the competitive market share for major participants for the total world UTM market in 2007.

FIGURE 2 - 11

Total UTM Market: Competitive Market Share Trends of Major Market Participants (World), 2007

Company	2006 (%)	2007 (%)	07/06 Trend
Fortinet	13.7	15.5	Up
Cisco Systems	12.8	12.0	Down
IBM/ISS	11.8	11.8	No Change
Check Point	12.7	10.9	Down
SonicWall	12.8	9.9	Down
WatchGuard	9.0	9.3	Up
Crossbeam Systems	5.9	6.8	Up
Juniper	5.3	6.3	Up
Secure Computing	5.5	6.2	Up
Others	10.5	11.3	Up
TOTAL	100.0	100.0	

Note: Others include 3Com, Arkoon, Astaro, Calyptix, Cyberoam, DeepNines, Global Data Guard, Network Box Corporation, and Zyxel.

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Market Leader

FORTINET INC

Fortinet, a Sunnyvale, California-based company, is one of the earlier pioneers and recognized leader in the UTM-appliances market. Former Chief Executive Officer (CEO) of NetScreen, Ken Xie founded Fortinet. Ken developed Fortinet UTM appliances from the ground up by basing it around Fortinet's ASIC and FortiOS technology. The technology is designed to meet the growing threat of blended-based attacks head-on, while at the same time, providing a solution that meets the needs of enterprise of all sizes. Fortinet was one of the only companies to recognize that businesses need agility and scalability to counter present-day and future network-security threats. Fortinet provided the needed agility through scalability. The scalability is achieved through Fortinet's future proofing solutions. Future proofing provides multiple layers of security protection and management that can be scaled and mapped to business requirements. This translates into a solution that can provide infrastructure protection against the full spectrum of network-based attacks, such as malware, spam, and blended-attack methodologies. The overall solution provides businesses of all sizes with a low total cost of ownership and the superior ability to protect itself from today's and tomorrow's present and future threats.

Fortinet's product family of UTM appliances, the FortiGate, is based around ASIC technology and the FortiOS operating system. ASICs use an intelligent proprietary content-scanning engine, which uses algorithms to accelerate network-security services. This methodology provides high-end network security that meets the needs of enterprise and network carriers. Coupled with ASIC is FortiOS operating system. The operating system provides a suite of in-house created content filtering, anti-malware, and IPS, along with virtual network-security and quality of services. Fortinet is one of the few companies that develop their own suite of network-security products, such as anti-malware and IPS signatures.

Frost & Sullivan believes that Fortinet's unique ASIC technology will make them the prominent leader in the UTM market. Fortinet's ability to produce its own network-security products and push antivirus and IDS/IPS signatures to its clients will help companies of any size defend their enterprise against network and content-level threats. Fortinet's achievements can be solidified from their industry accolades, such as SC magazine and Network World's security product of the year awards.

Market Challengers

CISCO SYSTEMS, INC.

Cisco Systems, Inc., headquartered in San Jose, California, is one of the predominant leaders in UTM hardware appliances. Its line of ASA is best-in-class UTM products that can be deployed in any size-networking environment, including a large enterprise. ASA is the centerpiece of its self-defending network, which provides practical resistance that mitigates threats at the gateway. The mitigation of threats at the gateway allows networks to provide mission-critical functions with bogging down the network to fight malware. Cisco Systems, Inc. was one of the first network security providers to recognize the advantages and benefits of UTM for the enterprise. The ASA series provides any size enterprise with the ability to scale its customization features. ASA customization is achieved through its flow-specific security policies, which are adapted to the demands of the network and business-specific applications. The adaptability of ASA allows network administrators to deploy network-security modules, such as IDS/IPS and application-firewalls, when required. This flexibility allows companies to purchase security application when they need them, thus reducing their TCO. Additionally, ASA series comes with Cisco Systems, Inc., best-in-breed routing and switching functionality. Frost & Sullivan believes that Cisco will continue to increase its UTM market share due to its industry-recognized brand name, which is trusted by all sizes of businesses.

IBM/ISS

IBM was one of the first computer service providers to develop and deploy a virtualization and network security strategy for corporate networks. IBM recognized that customers could gain higher returns on their IT investments by installing virtualized networking and security appliances to their network. Therefore, IBM implemented a virtualization research project under the code-name 'Phantom'. Project Phantom was a collaboration among IBM's X-Force and other IBM research departments. The collaboration formulated IBM's virtualization strategy, which is based on three foundations or pillars, which are Infrastructure Simplification', 'Rapid Application Deployment' and 'Business Resiliency'. Infrastructure Simplification is a streamlining process that is used in the transformation of a physical IT infrastructure into a virtualized IT infrastructure. A virtualized infrastructure has a logical ability to increase the size of the data-warehouse without expanding the physical size of the datacenter. This is a significant cost-saving method for a corporation looking to reduce cost. IBM's Rapid Application Deployment also provides significant cost savings by streamlining the provisioning process. IBM provides provisioning platform that reduces the cost of development over-head, testing, and the deployment of software-based applications. Thereby, the solution provides customers with the ability to provide products and services in minutes rather than days. Business resiliency provides network administrators with a streamlined replication and restoration process for isolating and securing data. The process provides the flexibility and reliance required for network's high availability and reducing the cost of disaster-recovery solutions.

IBM's virtualization strategy includes the Proventia Multi-Function Security UTM solution. The Proventia solution was the first product produced by project Phantom. The solution provides three-hundred and sixty-degree protection by using primary security features, such as firewall/VPN and anti-malware. The appliance is primarily designed for SMBs and distributed enterprises. MFS's strong price-point is its ability of combining IBM's best-in-class security products and using extensible threat-management technology. The technology has the ability to scale with software or hardware modules. The modules can be easily configured to combat future threats, such as blended attack methodologies. Therefore, Proventia is a multi-layered solution that leverages IBM's best-in-class network-security solutions. In all, the Proventia product-line has made UTM, a comprehensive solution that is effective and affordable. Therefore, IBM has made great strides in the UTM market to meet both SMB and enterprise needs.

By 2009, Proventia MFS is expected to be a dominant participant in the UTM market and, thus reducing the market share of Fortinet INC.. This is due to its implementation of solutions that will solve a customer's network-security needs without increasing their TCO.

C H E C K P O I N T

Check Point Software Technologies LTD, is an Israel based company that is dedicated to producing software and hardware for Internet Security. Check Point's UTM-1 product offers six levels of threat mitigations, such as firewall protection, content filtering, anti-malware, zero-hour outbreak protection, and IDS/IPS. Even though Check Point provides the usual list of security features, it stands out among other UTM providers through its centralized management GUI called SmartCenter. SmartCenter provides system and network administrators with the ability to centrally manage each security function of the UTM-1. SmartCenter centrally stores security policies that can be distributed throughout the enterprise. This ability provides the enterprise to configure networks against known and unknown threats.

S O N I C W A L L

SonicWall, a Sunnyvale, California-based company, is best known for its excellent network-security products and services for SMB, such as network, Web, and e-mail security. However, SonicWall has moved in the medium to large enterprise network security market with its Network Security Appliance (NSA) and E-Class family of UTM products. SonicWall still caters to the SMB market. However, in 2007, SonicWall began to cater to the large-enterprise market with its new multi-core hardware, which has the required throughput to conduct deep-packet inspection. Deep-packet inspection can become bandwidth-intensive and can potentially degrade network performance. SonicWall's deep-packet inspection performance inspects at layer-seven without the need of proxying, which provides high-end performance for larger enterprise-class networks. The NSA and E-Class security products have throughputs that range from 50 Mbps to 5 Gbps. The base price for each class ranges from \$2,500 for its NSA appliance to \$30,000 for its E-Class product line. Frost & Sullivan believes that SonicWall's ability to cater to both SMB and large enterprises is expected to make it a UTM market contender that will take away the market share of Juniper, Cisco, and Check Point market share.

Market Contenders

WATCHGUARD TECHNOLOGIES, INC.

WatchGuard, a Seattle, Washington-based company, has historically been a strong competitor in the SOHO and SMB network-security market. However, in 2007, WatchGuard suddenly found themselves in the SME and large-sized enterprise market, due to its Core and Peak UTM product lines. This was due to a management and engineering decision made in 2006. The engineering and management team had the business foresight to add best-in-class hardware and software in terms of reliability, scalability, and throughput. The introduction of high-end features made WatchGuard, an attractive purchase in the SME and large-enterprise network-security market. The attractiveness resulted in double-digit growth worldwide and it experienced phenomenal growth in the EMEA region along with strong sales in the North American region. Their strong growth and best-in-class products have resulted in many industry accolades, such as winning CRN magazine's UTM (Unified Threat Management) bake-off review, being named as "BEST FOR: Maintaining High Security" by Inc. magazine and being awarded "Best UTM Product of the Year" by Information Security & Communications Privacy magazine.

WatchGuard's products were ready for enterprise deployments before enterprises were ready to expand into the UTM Market. WatchGuard prepared itself to enter the enterprise-market by implementing extensible threat-management technology into its XTM 10 series product line. The extensible threat-management technology provides the 10 series with the ability to scale to the enterprise to meet present day and emerging malware threats, such as worms and blended attacks. WatchGuard grew into the SME tier, due to its 9.X that provided advance-networking capabilities, such as VLAN and WAN support. This was accomplished by using algorithm for each interface. WatchGuard took further measures and overhauled its products-logging capabilities. The overhaul resulted in scalable and robust-reporting capabilities that now support third-party reporting products. WatchGuard's award winning Web Blocker has further enhanced its product line, by offering HTTPS URL filtering. These features will allow network administrators to monitor or prevent secure sessions that may violate corporate, industry, and government regulations, such as an acceptable-use policy, PCI-DSS and HIPPA. WatchGuard's release of XTM-1050 appliance will provide customers with even more robust features, such as redundant power-supplies, 10 Gbps firewalls, and fiber-optic capabilities.

In short, Frost & Sullivan believes that WatchGuard is on its track of becoming a major participant in the enterprise-UTM market. Additionally, Market Engineering measurements have indicated that WatchGuard has chipped away the market share formally held by Fortinet, Cisco, and Juniper.

CROSSBEAM SYSTEMS INC

Crossbeam Systems Inc, located in Boxborough, Massachusetts, provides the next-generation UTM products and solutions that are virtualized. Crossbeam's X and C series product lines provide businesses with the ability to deploy virtualized networking components, such as switches, routers, and load balances, into one system. Businesses are then given the option of deploying a combination of best-in-breed network security products, such as Check Point's Power-1 firewall and Sourcefire's SNORT IDS technology, into one appliance. Crossbeam believes that there is no de facto UTM appliance on today's market at present. Additionally, businesses are allowed to choose from a list of network security vendor's products to be incorporated in their overall security solution. Therefore, Crossbeam allows a business to bring together their own selection of best-in-breed technologies from different vendors and incorporate them into one UTM solution. Crossbeam then provides a unique centralized management system, called SecureShore. With SecureShore, system administrators can configure, manage, and monitor the system from one console. Frost & Sullivan believes that Crossbeam is getting it right with its green-IT initiative. Crossbeam is allowing businesses companies to combine best-in-class networking and network-security solutions into one box. The ability of combining solutions into one box reduces the size and complexity of the network; thereby, reducing the power and cooling-cost.

JUNIPER NETWORKS

Juniper Networks, headquartered in Sunnyvale, California, is a high-performance networking company with 20,000 enterprise customers and ranks 92 among the Fortune 100 companies. Since the inception of UTM technology, Juniper has been one of the leaders in the market. Currently, the product line comes with a variety of network-security features, such as content filtering, firewall/VPN, and anti-malware. However, a majority of the features are not made in-house. Juniper has taken the standpoint of using partnerships with Websense, Kaspersky, and Symantec, to provide a best-in-class UTM offering. Juniper is combining their partner's security features with its award winning firewall/VPN technology.

Frost & Sullivan believes that Juniper will remain a market leader for the years to come. However, Juniper is likely to continue seeing its market leadership erode to other market challengers who are offering similar products in the market.

SECURE COMPUTING

Secure Computing, headquartered in San Jose, California, is one of the few market leaders that provide thought leadership in the network security realm. Secure Computing's primary UTM offering is the Secure Firewall (formerly known as Sidewinder) product line. Secure Firewall provides the primary features one would hope to find in any UTM product. However, what makes Secure Firewall stand apart from its competitors is their TrustedSource and SSL security applications. TrustedSource is an industry-leading reputation service that provides global threat correlation. The service analyzes a particular IP's global messaging and communication behavior for factors, such as the volume of network traffic and other trends that could indicate malicious behavior. TrustedSource provides a reputation score for an IP or domain behavior. The score is then used to build firewall rules that will allow or disallow an IP's traffic to pass through. TrustedSource leverages Internet data streams, which are provided by an alliance of network-security companies, such as F5 network. In turn, each company is provided with a best-in-class reputation services that provides excellent filtering capabilities to protect their perspective customers. Finally, Secure Computing's SSL-filtering technology addresses one of the fundamental problems with SSL communication. SSL provides the required security to protect sensitive network-based communications. However, network-security administrators are unaware of what is contained in the secure traffic. The traffic may violate a company's acceptable-use policy and industry regulations, such as PCI-DSS, and legislation, such as HIPAA. Therefore, administrators are sometimes forced to limit or even block SSL traffic at the firewall. However, Secure Firewall provides administrators with the ability to decode, analyze, and filter SSL traffic as it passes through the firewall. This is accomplished by requiring that each party provide their encryption keys to the administrator. The sharing of keys will allow administrators to decode and analyze traffic against security-based rules, as they would unencrypted traffic. The combination of primary-security features and the thought leadership to provide industry-leading solutions that tackle security problems faced by customers makes Secure Computing an overall thought leader in the network-security industry.

Emerging and Receding Participants

ASTARO CORPORATION

Astaro, headquartered in Karlsruhe, Germany and Burlington, Massachusetts, is a niche company that provides UTM products in both software and hardware form. Astaro is one of a few companies to have successfully developed and deployed UTM technology as a software package, hardware, and virtualized appliance. Astaro primarily uses open-source software, such as Linux and SNORT, for its operating system IDS/IPS security offering. Astaro offers best-in-class UTM products with low TCO that can be run in SOHO, SMB, and SME enterprise environments. Astaro is also on the forefront of offering virtualized UTM products that provide companies of all sizes with the flexibility required to reduce the size of their IT infrastructure and reduce cooling and power cost. Frost & Sullivan believes that Astaro is growing to be a leading company in the UTM market, due to its niche product that is being sold in 60 countries worldwide, using 2,500 resellers.

CYBEROAM (A DIVISION ELITECORE TECHNOLOGIES)

Cyberoam, a product of Elitecore Technologies, has offices and headquarters located in North America, EMEA, and the Asia Pacific region and is a leading provider of identity-based UTM technology. Cyberoam has a unique UTM solution that is based on identity-based management. Cyberoam takes the position that the user is the weakest factor in network security, due to being targeted by malware and hackers. Cyberoam's CRi series of UTM products utilizes granular access-control methodologies to control the end user's actions on the network. Cyberoam's firewall technology can configure policies based on the user name rather than the IP address. This is important when applying rules to the person rather than the end-point. These features allow access rules to follow the person and not the end-point. Cyberoam's UTM appliance is engineered to meet the needs of all business ranging from SOHO to large enterprises. Cyberoam deploys granular access control through its Cyberoam central console (CCC). CCC can centrally configure network security features, such as anti-malware, firewall rules, and IDS/IPS signatures. CCC is also the central hub that administrates security policies based on the user's work profile. Frost & Sullivan believes that Cyberoam's unique approach of providing UTM solutions based on identity-access management makes it a niche participant in the market. Its solution provides an excellent fit for businesses looking for granular access methodologies that control the user and not the end-point.

3 C O M

3 Com, based in Marlborough, Massachusetts, is one of the founding company's for the creation of Ethernet protocol and standard. 3Com's UTM appliances are primarily geared toward SOHO, SMB, and SME-sized networks. 3Com prides itself on its ability to reduce TCO, system management, and administrative expenses. 3Com has achieved this ability through thought leadership, by mapping their products to customers needs. This is done through using standard-based and interoperable systems rather than using proprietary systems.

3 Com's superior UTM product-family called Unified Security Platforms are built on the premise of incorporating best-in-breed network-security products through partnering with leading security providers. The platform is built around their its award winning TippingPoint IPS product and the incorporation of Websense's content filtering and Commtouch's anti-spam filtering products. Together, UTM products provide firewall/VPN, stateful packet-inspection, application-bandwidth management, and routing-support in product. Their UTM products also provide detail reporting through AdventNet. AdventNet provides network and system administrators with the ability to perform detail analysis of network traffic through the reporting tools. Additionally, AdventNet provides planning tools that assist in the analytical process, which determine if the network's current throughput-capacity is meeting the enterprise's needs. Furthermore, AdventNet provides policy enforcement allowing corporations of all sizes to meet their acceptable-use policies and industry standards, such as PCI-DSS and government regulations, such as HIPPA.

In 2008, 3Com plans to spin-off TippingPoint into its own company, due to restructuring of the company. TippingPoint provides high-end security products and solutions for enterprise-customers, while 3Com will provides products for SMBs and SOHO customers. Frost & Sullivan believes that the spin-off of TippingPoint from 3Com will allows both corporations and enterprises to concentrate on providing outstanding UTM products and solutions for their perspective markets.

Niche Participants

GLOBAL DATA GUARD

Global DataGuard (GDG) based in Dallas, Texas, is a UTM provider that provides state-of-the-art UTM solutions from SMB to mid-sized and large/medium and large-sized enterprises. GDG's UTM product line, the Enterprise UTM++, is an emerging one in the enterprise-class UTM appliance sector. UTM++ goes beyond the primary network-security features, such as firewall/VPN and anti-malware suites, and provides next-generation services. The appliance incorporates behavioral correlation and vulnerability-scanner modules. The modules will provide large enterprises with the ability to detect and stop zero-day and network-security threats before causing problems, such as the proliferation of malware and exploits. GDG's all-in-one security module (ASM) is designed for SMB-sized businesses. The ASM also comes with primary network-security features found in similar classes of UTM. However, the ASM stands out, due to the incorporation of behavioral correlations and vulnerability-management features. These features are not standard in similar-class products, such as Cisco's ASA and Check Point's UTM-1. Therefore, ASM has enterprise-class features at SMB price. What makes GDG unique is its security risk managed (SRM) service offerings. SRM is one of the few true turnkey-managed security services provider offerings in the market. SRM can be deployed as an on-premise or hosted solution. Customers have the option of managing the entire system or outsourcing the management of the appliance. Therefore, SRM provides customers with the ability to scale their network-security management to their business models.

CALYPTIX SECURITY

Calyptix Security, a Charlotte, North Carolina-based company, is a premier UTM manufacturer founded in 2002, by the University of North Carolina professor Dr. Yuliang Zheng and Dr. Lawrence Teo. Calyptix develops UTM hardware and software called AccessEnforcer for SOHO and SMB enterprises. AccessEnforcer uses a proprietary algorithm called DyVax that inspects e-mail protocols, such as POP3, SMTP, and IMAP, for current and zero-day threats. AccessEnforcer also provides the usual list of UTM services, such as firewall/VPN, anti-malware, and content-filtering solutions that a potential buyer would hope to find in its product. Internet Defense Force employs distributed networking to detect and mitigate threats, such as network worms and trojans in real time. Network Management provides network core services, such as routing and DHCP services, from one box. This function will allow a potential buyer to do away with costly managed routers and switches and deploy both security and network-management in one box. Network-management leverages a comprehensive HTTP-based management console that can configure all of its network services. Calyptix also provides MSP services to over 300 customers worldwide. Frost & Sullivan believes that Calyptix is on its track to become an emerging UTM provider for both small commercial businesses and government agencies. Calyptix is achieving this milestone by forming strategic partnerships with well-known VAR and third-party providers that exclusively sell security products to SMBs and government agencies.

Figures 2-12 and 2-13 provide a UTM feature break out for each key industry participants for 2007.

FIGURE 2-12

Total UTM Market: UTM Feature Break Out for Key Industry Participants (World), 2007

Company	FW/VPN	AM	CF	IDS/IPS	WiFi	SSL/VPN	GUI
3 Com	■	■	■	■			■
Astaro	■	■	■	■			■
Calypix	■	■	■	■			■
Check Point Software Technologies	■	■	■	■		■	■
Cisco Systems, Inc.	■	■	■	■	■	■	■
Crossbeam Systems	■	■	■	■			■
Cyberoam	■	■	■	■	■	■	
DeepNines Technologies	■	■	■	■	■		■
Fortinet FORTINET INC.	■	■	■	■	■	■	■
Global Data Guard	■	■	■	■	■	■	■
IBM	■	■	■	■		■	■
Juniper	■	■	■	■		■	■
Network Box Corporation	■	■	■	■		■	■
Secure Computing	■	■	■	■			■
SonicWall INC.	■	■	■	■	■	■	■
WatchGuard Technologies, Inc.	■	■	■	■	■	■	■
Zyxel	■	■	■	■	■	■	■

Key:

FW = Firewall

AM = Anti-malware

CF = Content Filtering

IDS/IPS = Intrusion Detection and Intrusion Prevention Systems

WiFi = Wireless Fidelity (802.11 A, B, G)

SSL/VPN = Secure Socket Layer Virtual Private Network

GUI = Graphical User Interface

Source: Frost & Sullivan

FIGURE 2 - I 3

Total UTM Market: UTM Feature Break Out for Key Industry Participants (World), 2007 (Continued)

Company	AFW	VOIP	LB	DPI	QOS	SMB	Enterprise
3 Com	■	■	■	■		■	■
Astaro	■	■	■	■	■	■	■
Calyptix	■			■	■	■	■
Check Point Software Technologies	■	■	■	■	■	■	■
Cisco Systems, Inc.	■	■	■	■	■	■	■
Crossbeam Systems		■		■		■	■
Cyberoam	■	■		■		■	■
DeepNines Technologies	■	■		■		■	■
FortinetFORTINET INC	■	■	■	■	■	■	■
Global Data Guard				■	■	■	■
IBM				■	■	■	■
Juniper				■	■	■	■
Network Box Corporation					■	■	■
Secure Computing	■			■	■	■	■
SonicWall INC.	■	■	■	■	■	■	■
WatchGuard Technologies, Inc.	■		■	■	■	■	■
Zyxel	■	■		■	■	■	■

Key: AFW = Application Firewall
 VOIP = Voice Over Internet Protocol
 LB = Line Balancing
 DPI = Deep Packet Inspection
 QOS = Quality of Service
 SMB = Small to Medium size Businesses (Support 100 to 1000 users)
 Enterprise = Support a thousand or more users

Source: Frost & Sullivan

Figure 2-14 provides each UTM participant's URL address for their perspective company.

FIGURE 2 - 1 4

Total UTM Market: Database of Key Industry Participant Web Sites (World), 2007

Company	Web Site
3 Com	www.3com.com
Arkoon	www.arkoon.net
Astaro	www.astaro.com
Blue Coat	www.bluecoat.com
Calyptix	www.calyptix.com
Check Point Software Technologies	www.checkpoint.com
Cisco Systems, Inc.	www.cisco.com
Clavister	www.clavister.com
ContentWatch	www.contentwatch.com
Crossbeam Systems	www.crossbeamsystems.com
Cyberoam	www.cyberoam.com
DeepNines Technologies	www.deepnines.com
DLink	www.security.dlink.com
Endian	www.edian.com
eSoft Inc	www.esoft.com
FortinetFORTINET INC.	www.fortinet.com
Freedom9	www.freedom9.com
Funkwerk Enterprise Corporation	www.funkwerk-ec.com
GajShield	www.gajshield.com
Global Data Guard	www.globaldataguard.com
Global Technology Associates Inc	www.gta.com
IBM	www.ibm.com
Intoto Inc	www.intoto.com
Juniper	www.juniper.com
NETASQ	www.netasq.com
Netrhino	www.netrhion.com
NetSentron	www.netsentron.com
Network Box Corporation	www.network-box.com
Nokia	www.nokia.com
Nortel	www.nortel.com

FIGURE 2-14 (CONTINUED)

Total UTM Market: Database of Key Industry Participant Web Sites (World), 2007

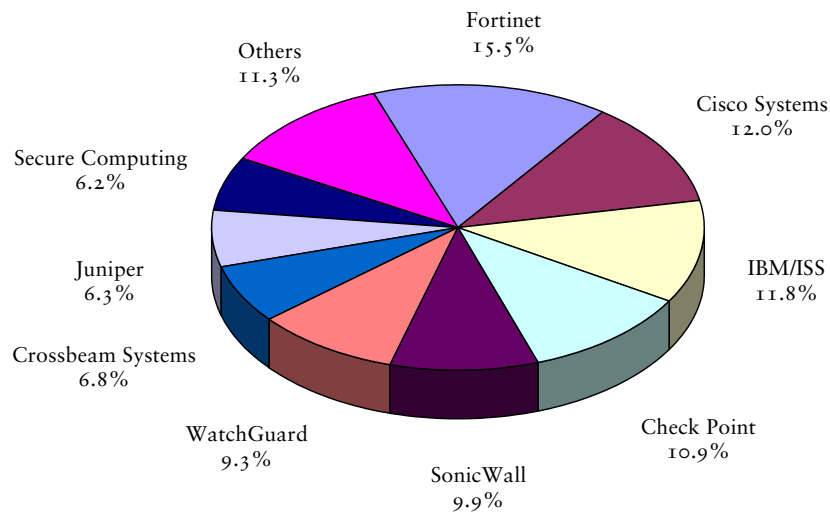
Company	Web Site
Panda Security	www.pandasecurity.com
Portwell Inc	www.portwell.com
Red Condor	www.redcondor.com
Reti Corporation	www.reticorp.com
Sarron Computing	www.sarron-corp.com
Secure Computing	www.securecomputing.com
Secure Point	www.securepoint.com
SmoothWall Limited	www.smoothwall.com
SOHOware Inc	www.sohoware.com
SonicWall INC.	www.sonicwall.com
Stonesoft	www.stonesoft.com
WatchGuard Technologies, Inc.	www.watchguard.com
Yoggie	www.yoggie.com
Zyxel	www.zyxel.com

Source: Frost & Sullivan

Chart 2.10 provides the total UTM market share trends of major market participants.

CHART 2.10

Total UTM Market: Competitive Market Share of Major Market Participants (World), 2007



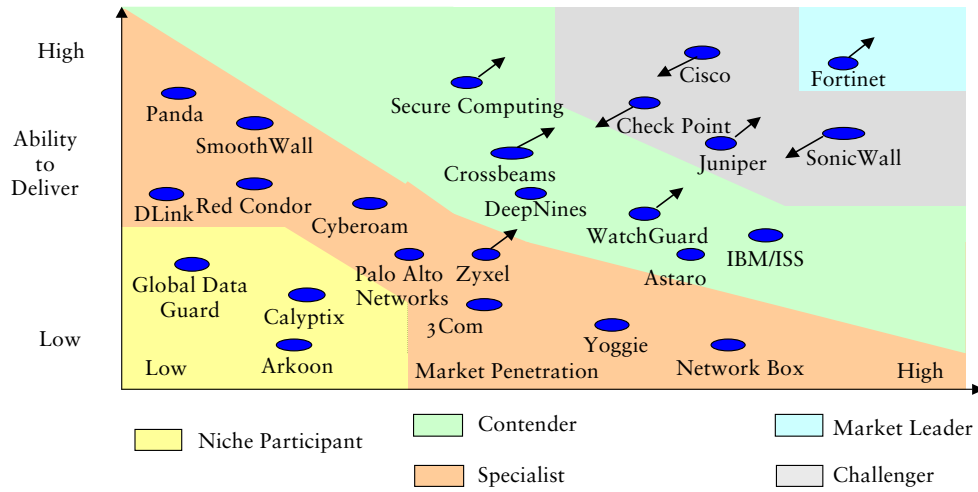
Note: Others include 3Com, Arkoon, Astaro, Calyptix, Cyberoam, DeepNines, Global Data Guard, Network Box Corporation, and Zyxel.

Note: All figures are rounded; the base year is 2007. Source: Frost & Sullivan

Chart 2.11 shows the competitive landscape of the total world UTM market in 2007.

CHART 2.11

Total UTM Market: Competitive Landscape (World), 2007



Source: Frost & Sullivan