NETWORK SECURITY

Overview of patent out-licensing opportunities

LexInnova

Contents

Executive Summary

With the advancement of the internet, there is a growing need to protect ones data from external threats. Many network security threats today are spread over the internet, making it imperative to monitor and prevent unauthorized access, misuse, modification, or denial of a computer network and other network-accessible resources. The architecture of the internet has been created to accommodate machines supported by different operating systems. Due to the generic interoperability of machines, a lot of loopholes remain in the architecture of the internet. System attackers are exploiting these loopholes for making a profit. Understanding the attack methods and corresponding loopholes can allow for the implementation of better and more appropriate security measures. Many businesses have been securing themselves over the internet through firewalls and encryption mechanisms; however network security is now undergoing a transformational stage with the advent of cloud computing and rapid penetration of mobile devices.

In this report, the technological landscape of this impactful technology has been explored from the perspective of Intellectual Property (Patents). This material also provides an overview of out-licensing opportunities that exist within this domain. We find that the majority of patenting activity in this technology has occurred in the sub-domains of protocols, distributed computing, and packet switching technology. We have also identified the various prominent assignees in this domain. According to our research, Cisco leads innovation in this domain with around 6,442 patents/patent applications, followed by Symantec and Juniper Networks who also have a significant number of patents/patent applications in their portfolio. Geographically, the United States has seen the maximum patent filings related to this technology, followed by China, Canada and Australia, who are advancing quickly.

We have analyzed similarities in the patents assigned to prominent assignees and find that the patents/patent applications assigned to Trend Micro are similar to those assigned to Symantec. We also evaluated the out-licensing opportunities of McAfee, and find it maximum potential in out-licensing its patents in the fields of Security Protocol and Antivirus Systems. Using our proprietary patent analytics tool, LexScore^{TM}, we identify Cisco as the leader in this technology domain, with a high quality patent portfolio and high patent filing activity.

The following sections contain our detailed analysis of the Patent Landscape of this technology domain.

Introduction

The rapid development of internet technologies has created new possibilities and led to the creation of several new methods of doing business, such as Software as a Service (SaaS), Information as a Service (IaaS), Platform as a Service (PaaS), etc. Private, public, and government sectors worldwide are relying increasingly on such services. One successful Denial of Service (DoS) attack on a network infrastructure behind SaaS can cost a company upwards of $400K.[1] The amount of data that companies are working with and relying on today is the largest it has ever been, and is only expected to grow further. The more data assets we possess, the bigger is our vulnerability to network security risks.

These security dangers mainly comprise of unauthorized access, misuse, modification, or network failure of accessible information and resources. Network security deals with monitoring and preventing attacks on computer systems. Network Security defines the protocols and policies used by network administrators to restrict unauthorized access to network resources. The measures adopted for the monitoring and prevention of attacks depends on several factors, including the type of network (public or private), the network's size, the classification of information being protected, etc. Selection of the best methods to minimize security risk requires a good understanding of network structures and the nature of attacks.

The layered Open Systems Interconnection (OSI) model has been illustrated in this report for the purpose of highlighting the consequence of cyber-attacks. Table 1 shows a scheme of possible attacks to the damaged OSI layer, as well as the severity of the attack. It is evident that a compromise of confidentiality, integrity, and availability of information affects all layers of the OSI model.

The Physical layer, which handles the transmission and reception of byte streams across the physical medium, is subject to interception attacks on wired and wireless networks. The Data link layer which is employed for establishing and maintaining connections between the nodes of the network and ensuring error free transmission of data streams is vulnerable to Man in the Middle (MITM) attacks, and Address Resolution Protocol (ARP) spoofing.[2]

The Network layer, which performs switching and routing of the packets to different networks (such as the internet or local area network (LAN)), often falls prey to DoS attacks such as Internet Message Control Protocol (ICMP) flooding. The Transport layer manages the transmission of messages between layers 1 to 3, which ensures error-free transmission among the hosts. This layer can be vulnerable to SYN flooding and IP spoofing.[3]

The Session layer controls connections among hosts in the network and is commonly susceptible to session hijacking. The Presentation layer acts a translator, formatting the information before presenting it to the user through application layer, or converting it into a suitable format for transmission. Secure

[1] http://www.kaspersky.com/about/news/business/2015/A-single-DDoS-attack-can-cost-a-company-more-than-400000-dollar
[2] http://www.uoregon.edu/~joe/nitrd/up-and-down-the-osi-model.html
[3] https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

Sockets Layer (SSL) DoS and Kerberos Service are the most common types of attacks at this layer. The Application layer serves as the user interface that is responsible for taking inputs from the user and displaying the received information to the user. This layer is vulnerable to injection attacks, such as SQL and LDAP injections, cookie poisoning, cross-site scripting (XSS), compromise of passwords, keys or session tokens, and parameter tampering .[4][5][6]

Layers	Attack Type	Mode of Attack	Result of Attack
Physical	Eaves dropping	By receiver tuning to proper frequency	Compromise of confidentiality of information assets (messages are seen by unauthorized user)
	Jamming	By malicious node with known communication frequency	Compromise of availability of information assets by preventing the reception of legitimate packets
	Active interference	Blocks the communication channel	Compromise of integrity of information assets by changing the order of messages
Data Link	Selfish misbehavior of nodes	Selfish nodes	Compromise of availability of information assets by dropping of packets
	Malicious behavior of nodes	Disrupts operation of routing protocol	Misdirecting traffic
	Traffic Analysis	Topology information	Compromise of confidentiality of information assets (messages are seen by unauthorized user)
Network	Black hole attack	Fake optimum route message	Loss of confidential information on packet
	Wormhole attack	Tunnel between malicious nodes	Loss of safe route
	Rushing attack	Subvert route discovery process	Loss of safe route
Transport	Session hijacking	Spoofs victim node IP address	Compromise of availability of information assets by a DoS attacks
	SYN flooding attack	Open TCP connection with victim node	DoS attacks
Application	Injection (SQL, LDAP, OS)	Occurs when untrusted data is sent to an interpreter and executed as part of a command or query	Attack to Database or OS
	Repudiation attack	Denial of participation in parts of communication	Communication failure
	Cross Site Scripting (XSS)	Occurs when an application takes untrusted data and sends it to a web browser without proper validation	Hijacking of user sessions, defacing web sites, redirecting the user to malicious sites

Table 1: Layer-wise Attacks Type[7]

[4] https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf
[5] http://www.slideshare.net/nurkholishhalim/osi-layer-security
[6] http://www.dmst.aueb.gr/dds/secimp/webmob/app.htm
[7] http://www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503173.pdf

Cyber-attacks are not new. Throughout 20th and 21st century numerous incidences of hacking have been witnessed. One of the most notable hacks is the interception of Axis powers' communication by allies and hacking of the Enigma coded messages dating back to World War II. Some of the recent incidences of cyber-attacks include hacking of Mt.Gox resulting in bankruptcy of the exchange[8] (Bitcoin worth $460 million and $27.4 million from bank accounts were robbed in this attack), Sony's PlayStation network hack in 2011 (account data of 100 million users was stolen in this attack), SQL injection attack on Heartland payment systems in 2008 (134 million credit and debit card details were stolen) [9], and hacking of the network of office supply retailer, Staples in 2014 (details of 1.16 million credit cards were stolen).

In today's Information Age, network security has evolved into a flourishing industry. The estimated size of the network security market in 2014 was $95.6 billion. It is expected to grow at a compound annual growth rate (CAGR) of 10.3%, reaching $155.74 billion by 2019, according to analysis done by market research firm, MarketsandMarkets[10]. The explosion of the mobile industry and rapid adoption of cloud based services are expected to guide the network security industry. The reach of the internet has expanded due to the introduction of affordable smartphones. It is further supported by a reduction in the prices of internet access by telecommunication service providers. The study by MarketsandMarkets predicts North America as the primary market for network security and Asia Pacific, Middle East, and Africa as the upcoming markets. Capital investments of firms (such as venture capital, angel investors, and private equity) have injected $1.4 billion in the network security market in the period between 2012-13, according to a study by CB Insights[11]. The figure below shows the number of deals concluded and the total amount spent on network security from Q2 in 2008 to Q3 in 2013. The interest shown by these firms strengthens the belief that the network security market has ample potential to grow in future. The amount invested also stimulates rapid growth of the industry by providing capital to small companies and startups.

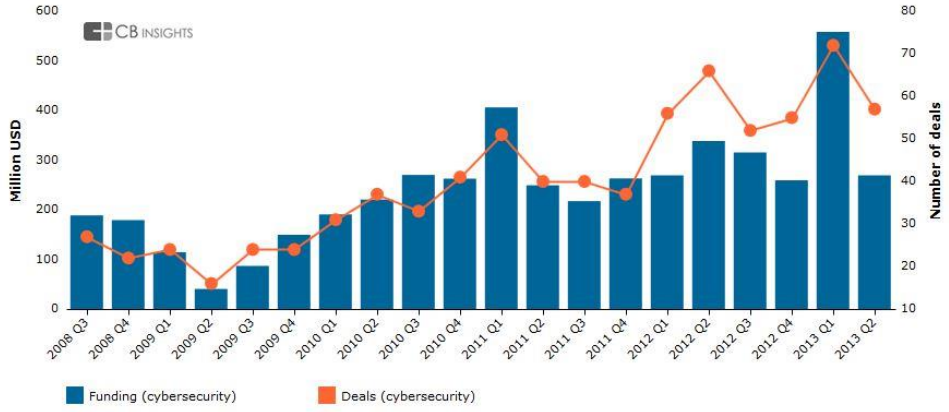

Figure 1: Quarterly funding and deals in cyber-security

[8] http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history
[9] http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html
[10] http://www.marketsandmarkets.com/PressReleases/cyber-security.asp
[11] https://www.cbinsights.com/blog/cybesecurity-venture-capital/

A similar study by TechNavio predicts a Compound Annual Growth Rate (CAGR) of 8.2% over the period 2013-2018. It also identifies North America, EMEA (Europe, the Middle East and Africa), and APAC (Asia Pacific) as the key regions for the network security market. Further studies also predict that the Mobile-to-Mobile network security market will grow at a CAGR of 22.9% over the same period (2013-2018)[12]. The major market share holders in this industry include technology giants such as Cisco Systems, Check Point Software Technologies, Fortinet, Juniper Networks and Palo Alto Networks. Cisco Systems dominates the network security market and has been at the apex of this field for quite some time now.

The network security industry is a diverse domain, covering various aspects, such as network infrastructure security, data security, access control, firewall technology (control of the incoming and outgoing network traffic), encryption techniques for secure transmission of information, intrusion prevention, etc. Advances in the mobile and cloud security sectors are expected to broaden the network security domain in future. Depending on the security requirements and the type of data being secured, a combination of the above mentioned techniques can be used to provide a full network security solution. This involves hardware components (routers, switches) as well as software tools. Data backup & restoration, application delivery appliances, and cloud storage – all these fields are closely associated with network security (and sometimes are included as part of network security services). Most of the network security service providers also include these services to broaden their portfolio and supply a complete package of services.

The network security industry is highly competitive, and dominated by big companies such as Cisco, Symantec, and McAfee. These companies try to protect their market position through constant innovations and frequent acquisitions. According to Bob Ackerman, nearly 80 startups in the network security industry resulted in initial public offerings (IPOs) or acquisitions with a tenfold return on investment on average. These include FireEye's IPO in 2013 and Cisco's acquisition of Sourcefire for $2.7 billion[13] in 2014. Reasons for these M&A's are twofold. The first reason involves the desire to provide a comprehensive solution to cyber security risks (also known as Unified Threat Management), and second reason implies the fear of being outdated by competition. The figure below shows the number of cyber security firms that have exited through M&A and IPO from Q3 2008 to Q2 2013.

[12] http://www.technavio.com/report/global-m2m-network-security-market-2014-2018
[13] http://venturebeat.com/2014/01/19/cybersecurity-is-hot-but-a-bubble-its-not/

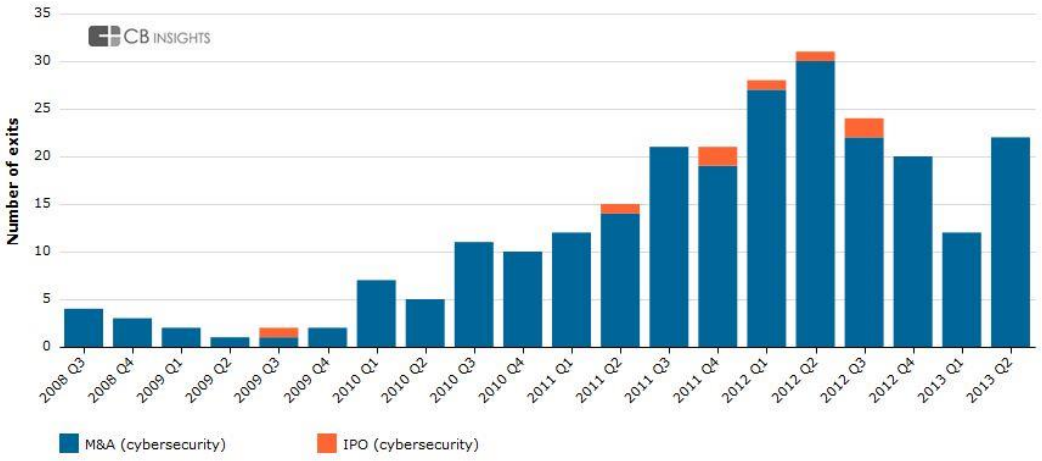

Figure 2: Number of cyber security firms exited through M&A and IPO from Q3, 2008 to Q2, 2013

This report is focused towards analyzing the portfolios of prominent companies operating in the network security domain. For this analysis, we have focused only on the assignees that are featured in Gartner's magic quadrant for the network security sector. The representatives that were categorized as niche market players were not included in the analysis. In this report we have also analyzed assignees that have a good market share, but might lack internet protocol connectivity (IP assets) to support their products.

In order to categorize patents/patent applications in the network security domain, we have divided them into broad technology sub-domains. We refer to these domains as Level 1 categories. Each technology sub-domain is further divided into methods/functions/applications covered in those technology sub-domains; which are referred as Level 2 and Level 3 categories. Patents generally describe these methods/functions/applications within the technology sub-domains. The categorization of patents/patent applications into various categories is done on the basis of IPC classification codes, keywords, and a combination of both. As patents generally discuss methods/functions/applications which may be used in more than one technology area, a patent may be categorized under more than one Level 2 heads.

Prominent Assignees

According to our analysis, Cisco, Symantec, Juniper Networks and McAfee have significantly large patent portfolio compared to the rest of the companies owing to their early start and constant growth. Prominent market players such as Check Point Technology, Palo Alto Networks have miniscule patent portfolio when compared to the top four assignees. For the entire analysis, we will refer to Cisco, Symantec, Juniper Networks and McAfee as Top Assignees and the remaining assignees as Niche Assignees.

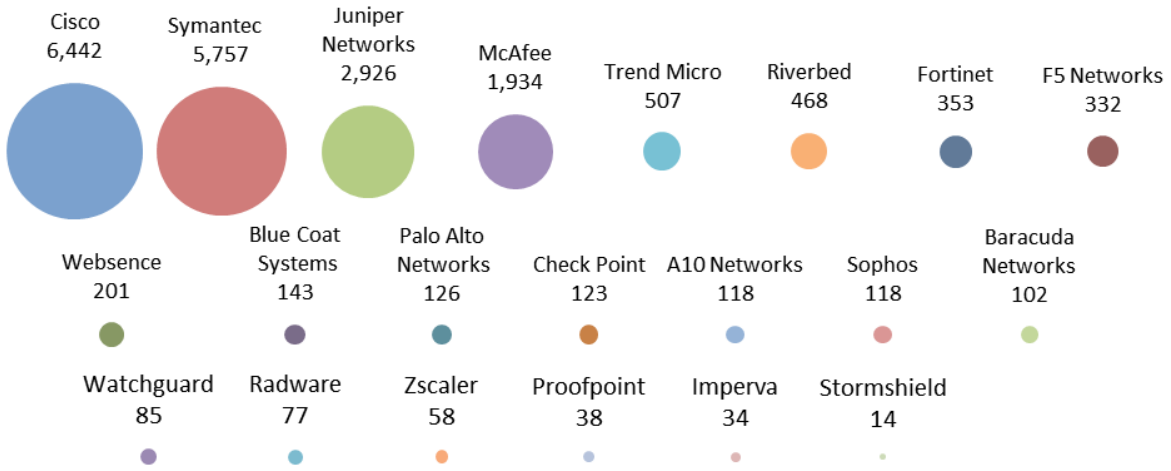

Figure 3: Prominent Assignees

The table below shows the Gartner magic quadrant and the corresponding market leaders in each quadrant.

Garner Magic Quadrant	Market Leaders
Enterprise Network Firewalls	Check Point Software Technologies, Palo Alto Networks
Secure Email Gateways	Proofpoint, Cisco
Secure Web Gateways	Blue Coat Systems, Zscaler, Cisco, Websense, McAfee
Unified Threat Management	Fortinet, Check Point Technologies, WatchGuard, Sophos
Web Application Firewalls	Imperva
Application Delivery Controllers	F5 Networks

Table 2: Gartner magic quadrant and the corresponding market leaders in each quadrant

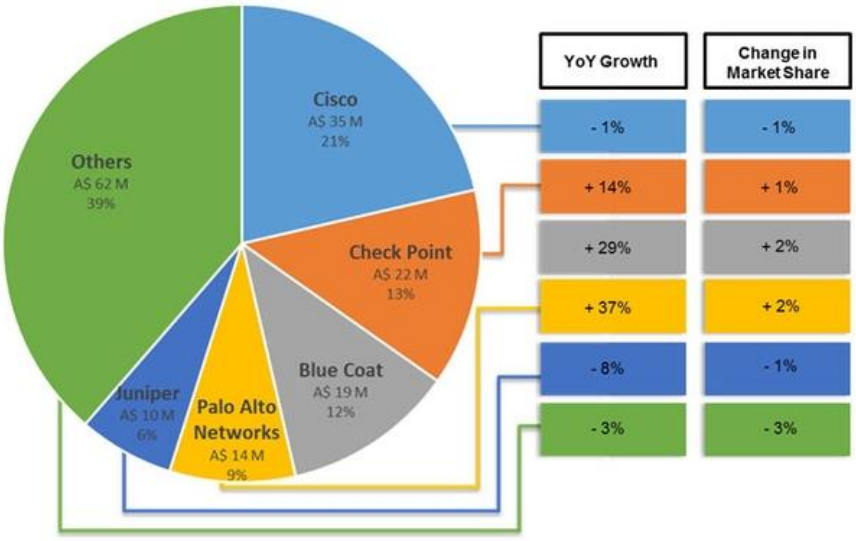

Figure 4: Market Share by value[14]

Cisco remains at the apex of the network security domain with 21% market share. Check Point, Blue Coat and Palo Alto Network are the niche assignees that hold the 2nd, 3rd and 4th positions in terms of market share in the year 2014. Juniper Networks, which is one of the top assignees, occupies the 5th spot. Together, these 5 market leaders cover 61% of the network security market[15]. The YoY growth figure shows that the niche assignees have expanded quickly and have successfully captured the market from major players such Cisco and Juniper Networks. These niche assignees have been successful in gaining market share, but their patent portfolio is insignificant when compared with top assignees, rendering these assignees vulnerable to litigations. Two of the four major representatives, Symantec and McAfee are not featured in the top 5 representatives and have less than 6% of market share. In an industry that is guided by M&As, as highlighted in the introduction, the existence of niche assignees among top market players hints towards the possibility of acquisition of niche assignees by top assignees.

Another important note is that most of the niche assignees are either publicly traded or owned by private equity/venture capital investment firms. Blue Coat Systems, Websense, and WatchGuard are some of the niche players owned by investment firms. The possibility of acquisition of these companies is higher because the firms invested in the niche players may choose to monetize their assets. Check Point Software Technologies, Proofpoint, Fortinet, Imperva, Palo Alto Networks, Barracuda Networks are publicly traded companies.

[14] http://www.computerworld.com.au/article/573443/security-appliances-australian-utm-market-growth-continue/
[15] http://www.computerworld.com.au/article/573443/security-appliances-australian-utm-market-growth-continue/

Taxonomy

The figure below shows the diversity and number of categories under which patents/patent applications have been classified. Network security is categorized into Network Infrastructure security, Host security, Encryption, Identity and Access Management, and Security protocols.

One can notice from the table below that there are certain categories such as: security protocols, distributed computing in data processing, packet switching in network switching, and packet filters in firewall, that have a large number of patents / patent applications.

Level 1	Level 2	Level 3	Hits
Network Infrastructure Security	Firewalls*	NAT	1,705
		Packet Filters	2,351
		Proxy	1,370
		Stateful Packets Filters	218
	Network Switching	Admin and Maintenance	1,677
		Control	155
		Gateway	418
		Message Switching	318
		Packet Switching	2,478
		Multiplexing	702
		Others	2,104
	Network Monitoring	Error Detection and Correction	1,989
	Content Security*	Antimalware	489
		Antivirus	1,875
Host Security	Data Processing	Distributed Computing	2,900
		Management	209
		Program Controls	1,349
		Others	811
	Memory Architecture		1,492
Encryption	Information Exchange		680
	Content Protection*		397
	Other Encryption		485
Identity and Access Management	Authentication		1,753
	Authorization		1,841
Security Protocols	Protocols		5,622

Figure 5: Taxonomy

**Overlaps with Host Security*

Assignee Similarity

For the purposes of this analysis, companies having a significant patent portfolio (comprising ~2,000 or more patents/patent applications) are classified as Top assignees (Cisco, Symantec, etc.); and companies having a smaller portfolio (~500 or lesser patents/patent applications) are identified as Niche assignees (Trend Micro, Riverbed, etc.). The table below shows the similarity between these two representatives. The numerical term represents the number of times patents/patent applications of the top assignee appears in the forward or backward citation of the niche assignee.

For example, the number 121 in the first row of the table represents the number of occurrences of Cisco's patents/patent applications in forward or backward citations of Trend Micro's patent set. Red color represents a high level of similarity and green color represents a very low level of similarity. A considerable similarity between the portfolios of the top and the niche companies indicates a high chance that a niche assignee would be infringing upon the patents of the top assignee.

NICHE ASSIGNEES\TOP ASSIGNEES →		Cisco	Symantec	Juniper Networks	McAfee
↓	Patents/Patent Applications	6442	5757	2926	1934
Trend Micro	507	121	431	20	317
Riverbed	468	298	43	62	14
Fortinet	353	367	184	86	143
F5 Networks	332	362	133	127	31
Websense	201	61	129	16	296
Blue Coat Systems	143	70	19	24	34
Palo Alto Networks	126	15	19	43	9
Check Point	123	71	64	42	134
A10 Networks	118	52	16	10	0
Sophos	112	36	39	8	37
Barracuda Networks	102	20	21	5	9
Watchguard	85	49	23	6	12
Radware	77	66	14	11	13
Zscaler	58	10	10	2	11
Proofpoint	38	10	36	0	17
Imperva	34	12	4	1	1
Stormshield	14	5	0	0	2

Figure 6: Assignee Similarity Analysis

***Note**: For this analysis, we have considered only those occurrences of the patents/patent applications of the top assignees, which were present in our analysis set (related to network security). We have neglected occurrences of the patent/patent applications s that were not related to Network Security.*

As can be inferred from the table above, Cisco's portfolio is similar to that of Riverbed, Fortinet and F5 Networks. Similarly, Symantec's portfolio is similar to that of Trend Micro; and McAfee's is similar to both Trend Micro and Websense. Among the top assignees, Juniper Networks' patent portfolio is least similar to niche assignees, with F5 Networks being the most similar one. Another important note is that Check Point Software Technology's patent portfolio is remarkably similar to that of McAfee, as it has 123 patents/patent applications that cite McAfee's patents/patent applications 134 times, implying a high level of similarity between their patents/patent applications. In the same manner, Proofpoint and Radware's patents/patent applications are comparable to Symantec and Cisco's patents/patent applications, respectively; however due to their smaller portfolio, they are highlighted as less significant.

McAfee's Licensing Opportunities Chart

For this analysis, we have chosen one of the top assignees i.e. McAfee and tried to identify its licensing opportunities in various technological domains, with respect to the niche players (Trend Micro, Riverbed, etc.).

The values in the table below are based on the arithmetic product of two parameters. The first parameter represents the share of patents/patent applications related to a technology domain out of the total patents/patent applications filed by a target company (for e.g. Trend Micro has a total of 507 patents/patent applications, out of which 197 are related to 'Antivirus' technology, hence the share of the patents/patent applications related to Antivirus filed by Trend Micro is (197/507=0.389). The better the share of patents, the more are the chances that their products being related to that particular technology segment. The second parameter represents the share of patents/patent applications related to a technology domain out of the total patents/patent applications filed by a top assignee (for e.g. McAfee has a total of 1934 patents/patent applications, out of which 532 are related to 'Antivirus' technology. Hence, the share of patents/patent applications related to Antivirus filed by McAfee is (532/1934=0.275). The better the share of patents, the more is the strength of the company in that particular technology area. In conclusion, a large value of the products of the 1st and 2nd parameter (indicated by shades of red) represents either that the top assignee is very strong in the domain, the target company is quite vulnerable in the domain, or both.

Technology\Assignee	McAfee	Trend Micro	Riverbed	Fortinet	F5 Networks	Websense	Blue Coat Systems	Palo Alto Networks	Check Point	A10 Networks	Sophos	Barracuda Networks
Antivirus	532	10.7	0.2	10.8	0.7	8.5	3.1	1.3	6.5	0.2	2.7	0.8
Security Protocol	492	7.2	5.4	8.9	7.0	12.4	8.2	5.5	12.0	8.8	5.0	5.2
Authorization	417	5.7	0.1	2.8	0.8	4.7	0.5	0.9	3.9	3.1	1.2	0.8
IPS	391	3.8	1.1	6.0	0.2	0.9	4.2	7.2	2.8	3.1	6.0	0.0
Distributed Computing	295	1.6	4.1	2.5	5.1	2.6	6.3	1.0	2.1	4.0	1.0	3.9
Error Detection & Correction	240	2.6	1.0	1.2	0.9	1.3	0.3	0.9	2.5	0.4	1.0	0.2
Firewall PacketFilters	227	1.2	0.6	2.9	1.6	0.2	2.3	2.6	2.5	0.4	0.4	1.4
Antimalware	226	0.7	0.0	0.2	0.0	0.0	0.2	1.1	0.0	0.0	0.6	0.1
Firewall Proxy	211	0.5	1.3	1.7	1.5	2.0	3.4	0.3	1.2	1.4	2.8	1.3
Authentication	183	1.4	0.2	0.8	1.2	1.6	0.7	0.5	1.8	0.6	1.6	0.6
Program control	143	0.8	0.5	0.4	0.5	0.7	1.3	0.3	0.1	0.8	0.3	0.1
Information Exchange_DP	133	0.7	0.5	0.4	0.7	3.3	0.5	0.1	0.2	0.1	0.5	1.2
Memory Architecture	129	0.9	0.3	0.5	0.3	0.9	0.6	0.2	0.8	0.1	0.8	0.5
Admin & Maintainence	125	0.2	1.4	0.7	0.8	0.2	0.6	0.4	0.5	0.4	0.3	0.1
Encryption	91	0.3	0.2	0.1	0.1	0.0	0.0	0.1	0.9	0.0	0.2	0.2
Content Protection	83	0.3	0.0	0.2	0.0	0.6	0.0	0.0	0.2	0.0	0.5	0.1
Information exchange_IS	80	0.3	0.0	0.0	0.2	0.4	0.6	0.0	0.1	0.1	0.0	0.2
Firewall NAT	72	0.0	0.4	0.7	1.4	0.0	0.5	0.1	0.6	1.5	0.1	0.4
Packet Switching	65	0.1	0.3	0.6	0.2	0.1	0.2	0.1	0.2	0.4	0.1	0.2
Message Switching	29	0.1	0.0	0.0	0.0	0.2	0.0	0.0	0.0	0.0	0.1	0.0

Figure 7: McAfee's Licensing Opportunities Chart

Trend Micro, the largest among the niche assignees (in terms of number of patents), has patents/patent applications similar to that of McAfee's as identified in the previous section. The table above strengthens that observation further by highlighting that Trend Micro has a decent patent portfolio that spreads across the top technology focus areas for McAfee (in terms of patent filings), with only three exceptions (NAT firewall, anti-malware, and proxy firewall). Check Point also has a patent portfolio which is similar to that of McAfee, but most of the areas are highlighted red due to its smaller patent portfolio when compared with that of McAfee's.

Blue Coat systems, Palo Alto Networks and Check point are among the top market share holders, but they too have a small patent portfolio. These assignees have a very small patent portfolio compared to McAfee, across mostly all technology areas, with only a few exceptions. The chances of them infringing on another assignee's patents are very high, and it is recommended that they acquire licenses (or patents) supporting their product to sustain their market position.

LexScore™

We use LexInnova's proprietary LexScore™ framework to identify leaders in the network security technology domain, from the perspective of intellectual property. The figure below depicts the competitive positioning of prominent assignees in the network security technology domain. The assignees are compared on the basis of filing score and quality score. We use our proprietary algorithm (based on bibliographical information and claim characteristics of an invention) to calculate the quality of their inventions.

The green region comprises assignees that have a big patent portfolio in terms of the number of patents/patent applications, and have fairly good patent quality. Only Cisco appears in this region owing to its huge portfolio of patents/patent applications.

The blue region contains assignees that possess good quality patents but lack on the patent filing front. Some significant assignees lying in this region are Check Point, Palo Alto Networks. These are promising companies but are found lacking here, due to their reduced patent filing.

The red region contains assignees that possess comparatively lower quality patents, and lack on the patent filing front as well. Juniper Networks, McAfee and Trend Micro are some of the significant names appearing in this region.

The orange region represents assignees that have a big patent portfolio but are lacking in patent quality. Although Symantec has sufficiently high filing score, it appears in this region owing to the low quality of its patent portfolio.

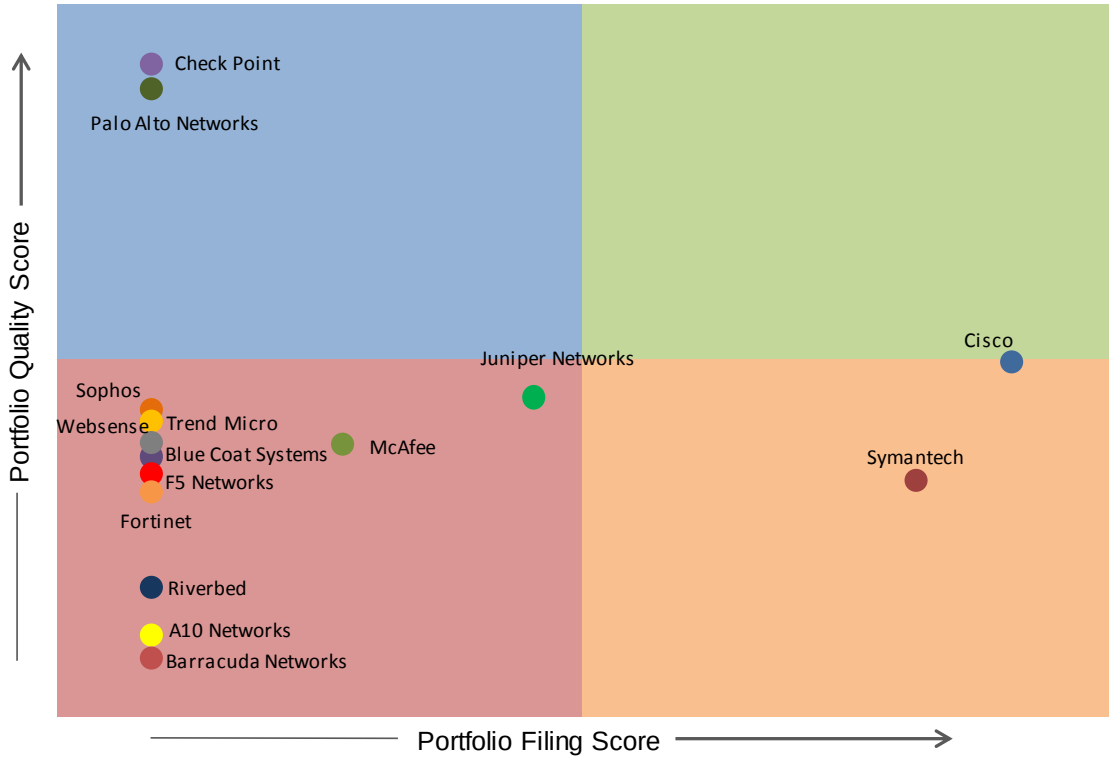

Figure 8: LexScore™

Geographical Coverage

The map below shows the geographical distribution of patent filings in the network security domain. The United States has witnessed maximum inventions, followed by China which occupies the second spot, witnessing 1/3rd of the patents/patent applications compared to United States. Other countries that have significant patent filings potential in this field include Canada, Australia, Japan, Germany and Austria.

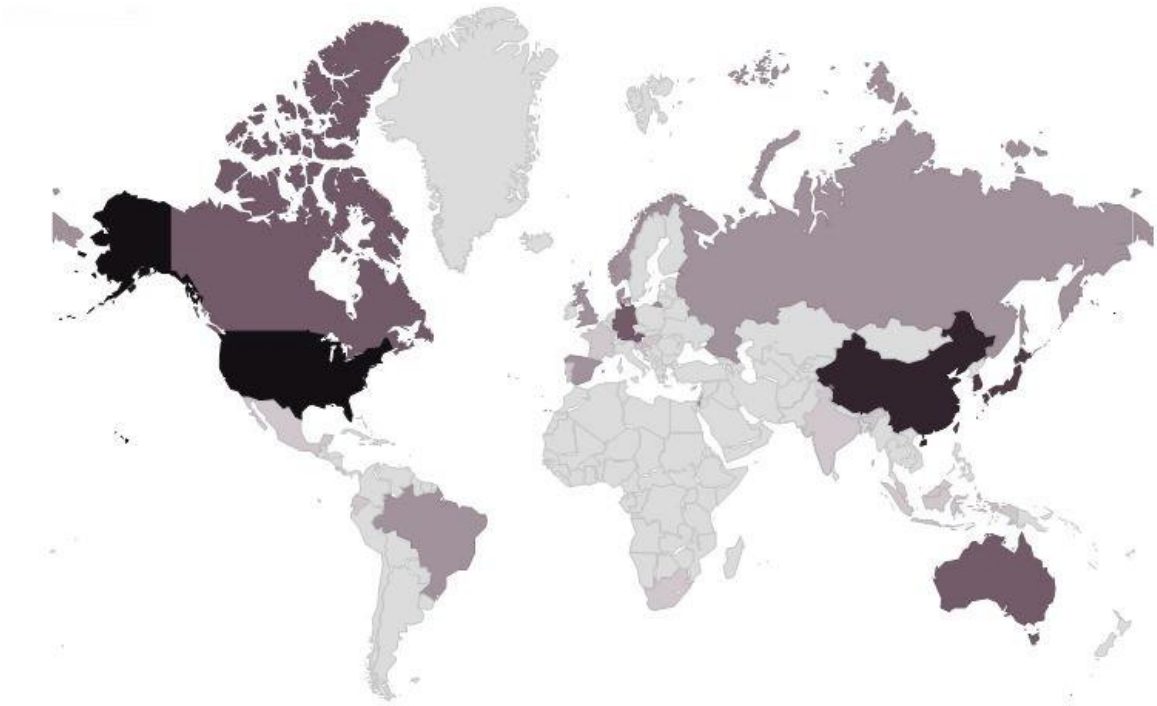

Figure 9: Geographical Coverage

Appendix

Taxonomy Heads	Definition
NAT	The patents/patent applications falling in this category talk about the process of modifying the IP information in IP packet headers so that the packets can be routed to the required destination.
Packet Filters	The patents/patent applications falling in this category describe about a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.
Proxy	The patents/patent applications falling in this category refer to security software firewall installed on a proxy server to act as a barrier between internal and external networks and, thereby, to both prevent unauthorized entities from gaining access to internal company resources and block internal users from gaining access to unauthorized external resources.
Stateful Packet Filter	The patents/patent applications falling in this category talk about a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it.
Admin & Maintenance	The patents/patent applications falling in this category talk about monitoring and testing arrangements for managing data switching networks.
Control	The patents/patent applications falling in this category talk about the mechanism for temporarily stopping the transmission of data on Ethernet family computer networks.
Gateway	The patents/patent applications falling in this category talk about the arrangements for connecting networks having differing types of switching systems.
Message Switching	The patents/patent applications falling in this category talk about the network switching technique in which data is routed in its entirety from the source node to the destination node.
Packet Switching	The patents/patent applications falling in this category talk about digital network transmission process in which data is broken into suitably-sized pieces or blocks for fast and efficient transfer via different network devices.
Multiplexing	The patents/patent applications falling in this category talk about methods by which multiple analog message signals or digital data streams are combined into one signal over a shared medium.
Error Detection & Correction	The patents/patent applications falling in this category talk about network monitoring systems for fault detection and correction.

Antimalware	The patents/patent applications falling in this category talk about the software program designed to prevent, detect and remediate malicious programming on individual computing devices and IT systems.
Antivirus	The patents/patent applications falling in this category talk about software designed to detect and destroy computer viruses.
Distributed Computing	The patents/patent applications falling in this category talk about the combination of two or more processors for a simultaneous processing of several programs.
Management	The patents/patent applications falling in this category talk about the data processing methods specially adapted for administrative and management purposes.
Program controls	The patents/patent applications falling in this category talk about the arrangements for controlling various aspects of programs such as initialization, loading and resource allocation etc.
Memory Architecture	The patents/patent applications falling in this category talk about accessing, addressing or allocating resources within memory systems or architectures.
Information Exchange	The patents/patent applications falling in this category talk about the transfer of information or other signals between devices and component.
Content Protection	The patents/patent applications falling in this category talk about the security arrangement for safeguarding access to data.
Authentication	The patents/patent applications falling in this category talk about any process by which a system verifies the identity of a user who wishes to access it.
Authorization	The patents/patent applications falling in this category talk about the process of allowing authenticated users to access the resources by verifying whether the user has access rights to the system.
Protocols	The patents/patent applications falling in this category talk about communication control characterized by protocol.

Authors

Amin Rida

Amin Rida is a Technology Consultant for LexInnova. He is an engineer and entrepreneur, and is currently working in product development for a technology startup in Silicon Valley. With a Ph.D. in Electrical Engineering from Georgia Institute of Technology, he has worked for Toyota Technical Center and Northrop Grumman. Amin has also worked as a systems engineer and a cyber-architect in the information systems field, as well as developed and taught courses in the cyber security domain. He is passionate about technology in general and cyber security in particular. He also holds seven patents/patents pending.

Aditya Bansal

Aditya is a Senior Technology Analyst at LexInnova. He completed his bachelors in Electronics & Communication Engineering from Delhi College of Engineering, Delhi. He is proficient in invalidity/validity searches, landscape, whitespace, portfolio analysis and technology due-diligence. He has managed 100+ IP projects related to Electronics, Electrical, Control Systems, Computer engineering, Mechanical, Networking, and Chemical Manufacturing domains.

Mayank Laroia

Mayank is a Senior Technology Analyst at LexInnova. He completed his bachelors in Chemical Engineering from Indian Institute of Technology (IIT), Delhi. He specializes in portfolio analysis, competitive benchmarking, and white space analysis. Apart from this he is proficient in invalidity/validity searches, patentability searches, freedom-to-operate searches and technology due-diligence. He has managed 100+ IP projects related to Electronics, Chemical Engineering, Control Systems, Environment Safety, Petroleum Engineering, Life Sciences and Chemical Manufacturing domains.

Alok Nath Yadav

Alok is a Technology Analyst at LexInnova. He completed his bachelors in Mechanical Engineering from Indian Institute of Technology, Delhi. He specializes in indirect arc welding, design and vibration analysis of the passenger seat in automobiles. His area of expertise includes IPR, contentions, infringement, invalidity search and FTO. He has also worked on patent portfolio analyses for various firms.

IS 607655

FS 614196

ABOUT US

LEXINNOVA TECHNOLOGIES LLC DRAWS ON A COMBINATION OF TECHNICAL AND LITIGATION EXPERTISE TO SOLVE THE CHALLENGES THAT ARISE AT THE INTERSECTION OF TECHNOLOGY AND THE LAW.

OUR CREDENTIALS

ISO 27001:2013 CERTIFICATION DESIGNATION VALIDATES LEXINNOVA'S COMMITMENT TO INTERNATIONALLY RECOGNIZED SECURITY STANDARDS

ISO 9001:2008 CERTIFICATION DESIGNATION VALIDATES LEXINNOVA'S COMMITMENT TO INTERNATIONALLY RECOGNIZED QUALITY MANAGEMENT STANDARDS

DISCLAIMER

LEXINNOVA HAS PREPARED THIS RESEARCH INDEPENDENTLY BASED ON RELIABLE PUBLIC DATA AND REVIEWED THE RESULTS BASED ON ITS PROPRIETARY METHODOLOGY, WITH THE BELIEF THAT IT IS FAIR AND NOT MISLEADING. THE INFORMATION AND ANALYSIS IN THIS REPORT IS TECHNICAL IN NATURE, AND SHALL NOT BE CONSTRUED AS LEGAL ADVICE OR A LEGAL OPINION OF LEXINNOVA.

U.S.A (San Jose)
560 S. Winchester Blvd, Suite 500,
San Jose, California 95128
Tel: +1 857-246-9999

U.S.A (Houston)
Suite 530, 550 Westcott Street
Houston, Texas 77007
Tel: +1 713-893-0716

India (Gurgaon)
4th Floor, B - Block, Building No. 14
Cyber City
DLF City Phase - III, Gurgaon
Haryana 122002
Tel: +91 124-400-3400

Japan (Gifu)
Operasu - Konohana 2F,
6-12 Konohana-cho,
Gifu-shi, Gifu Prefecture,
Japan 500-8333
Tel: +81 582-137-855