The Economics of Network Security

Michael Del Monte

Economist, Equity Analyst, Recruiter

General Overview of the Market

There are two types of companies out there; those who know they've been breached, and those who don't. According to FireEye, the median amount of time a hacker is inside a network before they're identified is 209 days. For precisely scenarios such as this, network security has become increasingly more of a focal point over the past decade by virtually every company, especially those who store data in mass. From healthcare to energy, properly securing data from threats has been a top priority, especially when it comes to protecting trade secrets and client information. With an increased occurrence of datacenter breaches over the past decade with the addition of the SAFETY act, companies are liable when it comes to information, including customer data, thus sparking a new age of cyber security. This is the era of the faceless, anonymous hackers who now hold the power to bring entire enterprises to their knees without ever being detected. A study conducted by McAfee estimates that the annual cost to the global economy from cybercrime is more than $400 billion, and the total impact could be as high as $575 billion. (McAfee, Inc.) In PwC's report, *The Global State of Information Security Survey 2015*, the number of detected incidents has increased 48% year over year to 42.8 million incidents, or 117,339 incidents per day. (PwC) According to AV-Test, from 2013 to 2014, new malware occurrences jumped over 71% from 83M to 142M.

In their annual security report, Check Point Software Technologies found that 86% of organizations accessed a malicious site in 2014. 83% of organizations have existing bot infections. A whopping 96% of organizations used at least one high-risk application and 42% of businesses suffered mobile security incidents costing more than $250,000 to remediate. On a daily basis, Check Point found that 106 unknown malware downloads were occurring per hour, up from 2.2/hr from the previous year 2013. In addition to these findings, 20% of enterprise hosts are not running desktop firewalls, 10% don't have updated service packets, 25% don't have updated versions of their software, 17% don't have any antivirus installed, and 35% allow users to have local administrator permissions.

Today's hackers have become increasingly more sophisticated in their attacks, utilizing various tools and techniques in order to gain access to a company's most delicate information. Attackers are no longer individuals aimlessly seeking to wreak havoc; they're now nation-state sponsored groups, teams of people who are well funded in order to gain access to trade secrets, M&A information, bank accounts, credit card and debit card information, government secrets, among all other data sought useful. The top three industries targeted, as provided by Evercore ISI, are Business & Professional Services, Retail, and Financial Services. (Evercore May 19, 2015) Hackers generally target consumers, who are engaging in online monetary transactions and ecommerce. Another opening for hackers is to target those who access public WiFi, which opens doors to stores of information (literally everything stored on your smart-device) if the network isn't secure. These attacks aren't necessarily targeting networks and servers, but are acquiring information through email and the internet (WiFi), manipulating

users to click on links that can trigger malware. Third party research would suggest, as provided by Wunderlich, that 80%-90% of data breaches start from some form of email.

With this in consideration, there are multiple ways for companies to fend from these threats. The big picture is to increase the cost of a breach by investing in newer technologies and increasing IT security staff. Addressing the second point, in today's current market, there is a shortage of IT security administrators and engineers relative to market demand. The average Security Engineer costs on average $80k-120k, while managers cost $110k-170k in order to maintain a competitive edge in the marketplace. Because of the shortage and high costs of staff, companies are turning to SaaS ("security as a service") in order to fill their needs. Companies similar to FireEye have positioned themselves to sustain this growth in services. For example, FireEye's acquisition of Mandiant helped place the company at an optimal positioning, thus expanding their professional services, which include incident response and consulting services.

Generally speaking, the biggest revenue drivers for these network security firms mostly lie within the Subscriptions and Services, which I am expecting to range between 47-70% of total revenue for various network security firms, whereas product sales are expected to range 30-53%. Y/Y growth for Subscriptions and Services is substantially larger than product revenue growth due to add-ons, refresh-cycles, renewals, and repeat customers. Users typically subscribe to Palo Alto's subscription services for about a year, whereas FireEye typically locks in a 1 or 3-year contract with a renewal rate at 90%. Mandiant (acquired by FireEye in 2014) plays a huge role in both FireEye professional services model. As suggested in the prior paragraph, security engineers are a very scarce commodity, especially for companies who have been priced out of the market by their larger competitors who can afford an entire security team. Because of the shortage of prime candidates in today's network security market, I'm under the impression that SaaS and consulting services will play a more dominant role throughout the next few years before the candidate pool catches up, allowing companies to purchase and maintain their own security products and personnel, with the addition of paid subscriptions.

Subscriptions are key for increasing revenue over time for network security companies. Though product sales play their role with new clients, companies will generally only purchase new IT infrastructure products when their existing products fully depreciate. On average, an infrastructure refresh occurs every 3-5 years, where firewalls will be upgraded or replaced entirely. The end of the refresh cycle would be the optimal time for these NGFW (Next Generation Firewalls) providers to step in and gain market share. As these emerging network security companies ground their market share, in the long-run, subscriptions and services will emerge as the main driving force behind sales.

Another issue network security firms face is competition with companies similar to Cisco Services and Juniper Networks, who offer fully integrated software and hardware across the entire infrastructure and can afford to offer discounts on products to loyal long-term enterprise clients. Aside from this benefit, Gartner gave Cisco a lower rating and reported that Juniper is losing market share in a growing market. (Gartner Magic Quadrant)

Network Security technology is shifting into high gear. NGFWs are starting to become the norm throughout companies of all industries. A key factor when comparing yesterday's firewalls to NGFW is the ability to leverage application visibility, URL filtering and intrusion prevention, and the ability to add user identity to the evaluation criteria in order for the NGFW to better predict a threat. (Gartner) These NGFWs stand out from yesterday's firewalls with a probabilistic approach to threat detection and the utilization of big data. Instead of having a definite approach, the probabilistic approach utilizes big data in order to generally classify what is and isn't a threat. This approach inverts the focus to detecting and identifying breaches, rather than strictly prevention. This can be said to be the main differentiator between yesterday's firewalls and NGFWs.

What is a Next-Generation Firewall?

Gartner defines a Next-Generation Firewall as a machine that consists of all the capabilities of a firewall with the addition of next generation features. This consists of integrated deep packet inspection intrusion detection, and application identification and granular control. What differentiates products are IPS effectiveness and fine-grained policy enforcement. (Gartner Magic Quadrant) NGFWs, as compared to yesterday's firewalls, are developed to detect threats in order to prevent intrusion, or to isolate and exterminate an intrusion (sandboxing).

A good visualization would be to imagine a *Game of Thrones* type of setting in a castle with high standing walls. The walls can be considered the firewall; it's there to keep the bad guys out and allow the proper citizens access in and out with ease. The Next-Generation Firewall would be the knight's watch and kings guard who actively seek out harm and eliminate all threats. Because of the high frequency of new, never before seen threats, as compared to the wildlings and white walkers, the knight's watch, or NGFW, has to constantly adapt to the new threats. The NGFW is able to identify new threats as well as adapt to new environments, recognize user patterns, and user errors.

Sandboxing, as defined by Gartner, is a proven technique for detecting malware and targeted attacks. From detection, the threat is sent to the sandbox to be analyzed and assigned a malware probability score and severity rating. (Gartner Network Sandboxing)

Company Comparison

Over the past few weeks, I have been analyzing some of the big name players in network security, including but not limited to FireEye, Palo Alto Networks, Fortinet, and Cisco for general reference. At a general level, each company provides its own version of a NGFW. The main differentiator between these firms lies within the add-on products, Subscriptions and Services. The most effective way to present this data would be to discuss each company on an individual basis with a brief overview of who they are and what they do and discuss their products and services. Once the groundwork is laid out, I'll compare and contrast in order to create a better understanding of each product's position in the market. Because I'm using Cisco as a general reference point, I'll start with them.

Cisco

Cisco has been the industry standard for designing, manufacturing, and selling IP (Internet Protocol) technologies in the communications and IT industry since the 1980s. The products Cisco develops include routers, switches, video cable and telecommunications boxes and modems, VOIP phones and call center, datacenter servers and blade servers, WiFi, and firewalls, which include network security, web and email security, cloud web security, advanced malware protection, datacenter security, and network admission control and identity services. Cisco provides numerous firewall products to the market, such as their stand-alone firewall ASA (Adaptive Security Appliance) with FirePOWER services which includes Sourcefire IPS (Intrusion Prevention System) AMP (Advanced Malware Protection) with an application visibility control. According to Gartner, Cisco firewalls scored relatively low compared to competitors in the firewall market regarding client satisfaction. Cisco was also said to be the most frequently replaced firewall. Cisco's main competitive products are SourceFire FireSIGHT, which automate security through continuous awareness, threat detection, and protection across its portfolio. This includes NGIPS, NGFW, and advanced malware protection.

As previously mentioned, Cisco is a recognizable name brand which holds a tremendous market share. According to Citi, however, Cisco only grasps roughly 12% of the overall firewall market. In my opinion, Cisco, negating the recent purchase of SourceFire, is going to be slowly losing market share in the firewall market, maintaining the assumption that network security is evolving. SourceFire has helped Cisco gain additional security market share, but nowhere near the exponential rate of PANW or FEYE.

FireEye

Since 2004, FireEye has been one of the leading innovators and providers of Next Generation security, driving the market in cyber security solutions for detecting, preventing, and resolving advanced cyber-attacks. FireEye provides their product both in physical, virtual machines, and cloud-based softwawre with the addition of subscription-based offerings. In 2010 FireEye has been pioneering the development of automating features of the sandboxing technology (Gartner). They provide Network Threat Prevention Platform (NX Series) which analyzes web traffic, Email Threat Prevention Platform (EX Series) which protects from unknown operating systems, browsers, appliances, and blocks malicious code embedded in emails, Endpoint Threat Prevention Platform (HX Series) which keeps the network computers protected, Mobile Threat Prevention (MX Series) which can be used with Android and Apple devices, Threat Analytics Platform (TAP) which provides cloud-based solutions, and Dynamic Threat Intelligence Clout (DTI) which interconnects FireEye appliances in order to provide real-time threat intelligence data. FireEye is also provided as a services (FireEye-as-a-Service; FEaaS) for companies who wish to outsource their IT Security needs. These services have been proven to be extremely beneficial to SMB (small-midsized businesses), which typically have a slimmer budget for IT and are priced out of the candidate pool for a good IT Security staff. At the end of 2013 through early 2014, FireEye acquired Mandiant, who provides incident response and consulting to those who have been breached. FireEye is also certified by the Department of Homeland Security for its Multi-Vector Virtual Execution Engine and Dynamic Threat Intelligence Cloud. FireEye has recently gained a competitive advantage by partnering up with HP, Telefonica, Deutsche Telekom, and Singtel.

FireEye stands ahead of the herd with its FEaaS and Mandiant services. FireEye utilizes its Adaptive Defense approach which helps reduce false positives, ensure policy compliance, determine which threats will have a more serious potential business impact, and emphasize best practices for incident resolution. FireEye recently was named winner of the 2015 SC Magazine Excellence Award for Best Advanced Persistent Threat Protection.

Palo Alto Networks

Since 2005, Palo Alto Networks has pioneered the next-generation of enterprise security by providing Next-Generation Firewalls, Advanced Endpoint Protection, and Threat Intelligence Cloud. Their products include the Firewall, Unified Threat Management (UTM), Web Gateway, Intrusion Detection and Prevention (IDS/IPS), Specialized Threat Analysis and Protection (STAP), Virtual Private Network (VPN), and Enterprise Endpoint Security technologies. One of their key differentiators for PANW is that they provide a vast array of products for any size company. From their PA-200 (NGFW) to their PA-7050, their products can fit into almost any environment, provided either as a physical unit or virtual machine (VM). Like FireEye, Palo Alto Networks provides numerous subscription-based services to provide a more targeted security network. Their subscriptions consist of Threat Prevention, which provides integrated protection from exploits, malware, dangerous files and content, and ISP functionality, URL Filtering, which controls web activity based on user category level controls, Global Protect, which provides consistent security to all users in any locations, and WildFire, which is a cloud-based application that detects previously unseen malware and polymorphic malware and provides a signature feed which logs and analyzes data to be sent to the firewall, and receives new malware protections every 30 minutes. WildFire API enables users to programmatically submit files to WildFire (sandbox) and integrates with Bit9 and Morta solutions. Global Protect includes a mobile application in order to provide a greater barrier from malware.

Something that stands out about Palo Alto Networks is its ability to tone down the noise in data. With their product, PAN-OS, the mountains of data that flows inward gets filtered before it reaches the in-house network security team. The biggest aspect of this product is that it can help reduce the likelihood of human error which can lead to additional issues and downtime. Another great feature that Palo Alto Networks provides, through its WildFire product, is the consolidation of findings in the data. All the information on malware found through WildFire is sent back to Palo Alto Networks in order to apply the new information to all 6,000 WildFire subscribers. In my opinion, this utilization of data will give Palo Alto Networks the advantage over other firms when it comes to threat detection.

Fortinet

Since 2000, Fortinet has gained a strong footing in the network security industry by providing solutions to some of the largest enterprises, service providers, and government organizations across the globe. Fortinet is best known for FortiGate physical and virtual appliance products which provide integrated security and networking functions to protect data, applications, and users from network and content-level security threats. Their functions include firewall, IPS and anti-malware, application control, VPN (Virtual Private Network), web-filtering, vulnerability management, anti-spam, wireless controller, and WAN acceleration. They provide FortiGate from the very affordable FortiGate-20 to the FortiGate-

5000. They have a vast array of plug-ins which include FortiAP, FortiWeb, FortiMail, FortiDB, FortiClient, FortiScan, FortiSwitch, FortiBridge, FortiAuthenticator, FortiADC (Application Delivery Controller), FortiSandbox, FortiCache, FortiDNS, FortiDDos, and FortiVoice. Fortinet also provides various products within FortiGate which include FortiManager to centrally manage all FortiGate products, and FortiAnalyzer which logs, analyzes, and reports solutions. Fortinet also provides FortiCare Technical Support Services, which entail support services for the software, firmware, and hardware.

As a Whole

Each of the companies observed, as do all companies, seem to have their strengths and their weaknesses. One of the biggest mountains to overcome for each company, especially the newcomers, is to compete with those who have dominated the market for years with full infrastructure integration. As previously stated, PANW and FEYE are going up against CSCO and JNPR who can offer discounts on infrastructure. Though, as seen by various growth models, CSCO has seen flat growth in security, while JNPR has been dropping. PANW and FEYE have consistently and significantly grown Y/Y, gaining 1,500 and 400 customers respectively each quarter. PANW takes a strong innovative lead with their single-pass parallel processing architecture. This process is said to run more efficiently than other NGFWs in response to it performing operations once per packet. Processing it through the firewall includes running the policy look up, identifying the application, and signature matching. Experts in the field claim that this is one of the most effective firewalls on the market; though, the price of this technology can make some buyers hesitant when considering the overall effectiveness/price of the unit. FireEye, on the other hand, is more focused on the endpoint security by utilizing its large network to find new malware and regularly update their system. Utilizing big datasets, FEYE uses a probabilistic approach in detecting intrusions and malware. Like Palo Alto Networks, however, FireEye has proven to be a quite expensive product that would be most utilized in a large enterprise environment. That being said, FireEye does have the upper hand in providing their security as a service through FEaaS (FireEye-as-a-Service). They also close the loop by providing Mandiant's consulting team, furthering their edge on today's security market.

3rd party Analysis

In today's security market, NGFWs seem to be the way to go, especially with this surge of "next-generation threats". Another product that stands out that is very similar to NGFWs is a Unified Threat Management (UTM) system. UTMs are typically packed with a broad array of security capabilities that are meant to provide network security to SMBs. Because of the less in depth functionality of UTMs, they're meant to target companies who are priced out of Next-Generation Enterprise Security. NGFWs fit perfectly, if integrated properly, in a large scale datacenter where top of the line security will meet top of the line threats. Something that may cause a slower adoption rate is the refresh cycle. Firewalls are generally replaced every 3-5 years. This may stagger new business for these emerging security companies.

In my point of view, there are many different aspects that go into selecting a NGFW. Getting the obvious out of the way, money stands out the most. Surprisingly, a lot of these NGFWs tend to be quite

pricy, especially when considering the additional subscription features and add-ons that help ensure a foolproof system, with the addition of services, support, maintenance, and a specialized team of security engineers to top it off. Another factor that may cause a company to choose one NGFW over another is integration throughout the infrastructure. Companies like Cisco, HP, and Dell, who develop a wide variety of products, from IP products to PCs and network servers, may hold an advantage over those who solely produce security products. Gartner noted that companies tend to purchase HP firewalls because they already have other HP security products. There have been findings, according to Deutsche Bank, that Cisco and Juniper are "effectively giving the equipment away if there is a professional services engagement or multiyear support contract as part of it". Competitors of these firms, such as Palo Alto Networks, may provide companies with a secondary firewall to complement already existing security systems.

Something that's remarkably interesting is how tied network security is to big data analytics. There are vast amounts of data coming in that cannot effectively and efficiently be observed. According to Morgan Stanley analysts, a security network with a SIEM ("Security Information Event Management") system reported on average 15,000 events per second in 2000. That number is now at 80,000! One effective way to sort through the data to find threats would be to consolidate and automate the process. Palo Alto Networks is working to reduce this signal-to-noise ratio within the security environment by releasing AutoFocus.

One of the major complaints, as portrayed by a survey run by Gartner, is a performance impact when using a NGFW. For example, an email filter may misclassify a coded email as a threat and may not send it through to the recipient, even if the email doesn't contain a threat after all. According to Gartner, "fewer than 2% of deployed enterprise firewalls will have web antivirus actively enabled on them through 2018, although more than 10% of enterprises will have paid for it". (Gartner, NGFWs and UTM)

My expectation for the near future of network security, ranging between 5-10 years, is to see SaaS dominate the market. Cloud and Cloud-based service seem to be one of the largest differentiators when it comes to network security providers. As stated above, Security engineers and managers are both expensive and scarce. When broken down and viewed inward, companies will have to purchase an expensive product, expensive subscriptions, expensive people with intensive competition for retention, and expensive maintenance; or, they can take the route of purchasing a SaaS package, outsource additional costs, and allow time for the network security market to saturate and become more affordable. Do note, however, that Cisco shouldn't be included in this portion of the analysis for multiple reasons. First, their long market share has created a long-standing demand for Cisco engineers and admin who specialize in all Cisco products. For the sake of simplicity, I will state that a security engineer will be classified differently than a Cisco network engineer who specializes in configuration of all Cisco products, including the firewalls.

When observing the financial data of these companies, it can be seen which direction each company is going in. Every company I reference, other than Cisco, has a dominating revenue stream from services and subscriptions over product revenue (also excluding PANW, though by a tighter margin than Cisco). With Cisco being an infrastructure provider and not a sole Network Security company, this

is expected. ProofPoint is on the complete opposite end of the spectrum, showing services as a percentage of revenue at 97%, and products at 3%. As the market for NGFWs continues to grow and refresh cycles come to a close, I expect the services and subscriptions revenue to increase across the board.

Market Confidence

Cyber Security and cybercrime go hand in hand, similar to Batman and the Joker in *The Dark Knight*. Without cybercrime, there is no market for cyber security. The director of National Intelligence named cyber threat as the number one strategic threat in the United States, surpassing traditional terrorism. On April 1st, 2015, President Obama issued an executive order declaring that "the increasing prevalence and severity of malicious cyber-enabled activities constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States. I hereby declare a national emergency to deal with this threat". (Evercore ISI) Laws against cybercrime in the United States are becoming more and more relevant. Employed cybercriminals working for the state are attacking US domestic companies while the attacker's government either turns a blind eye or persuades this criminal activity. Unless all companies start working on closed source networks and restrict users of all from accessing the network, I don't see this problem fading. The overall point of the matter is that Network Security is a big thing now, and will remain a big thing over time. What a lot of people are wondering, as I am myself, is whether this is a big hype phase, or if this is true growth in the market backed by true growth and earnings by these companies.

As we are all aware, modern Network Security has been around for only roughly a decade now. With Palo Alto Networks and FireEye popping up and dominating in growth to scale, legacy firewall developers are striving to compete and maintain market share. Acquisitions are typical for these larger firms to gain access to quickly get up to speed. In fact, acquisitions can be observed by nearly all the strong standing network security companies, with FireEye purchasing the private company Mandiant, Palo Alto Networks purchasing Morta and CirroSecure, Cisco purchasing SourceFire, and Dell purchasing SonicWall. Partnering up with other firms to fight crime isn't completely unheard of as well. Recently, FireEye teamed up with Visa to gain access to their vast database in order to fight POS and credit fraud.

Conclusion

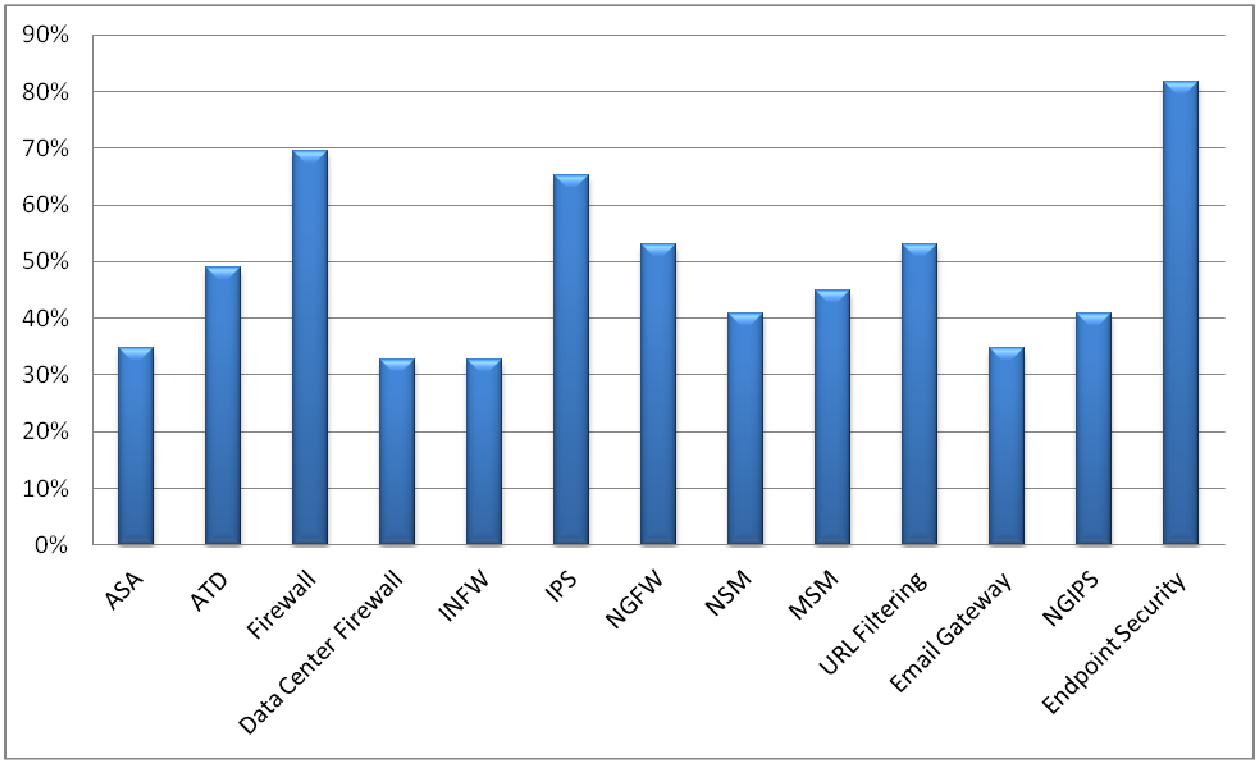
Network security is here to stay. With the constant threat of the next large scale data breach, companies can either leave their data open for the taking, remove all liability by providing it to government officials (SAFETY Act), or amp up their network security. Though some companies don't value network security as highly as they should, I feel that once a major breach does occur within their company, their perception will change. The costs of associated breaches in 2014 ranged $400 million, or an estimated $2.7 million per incident. In a survey jointly conducted by Chilton Capital Management and JDA Professional Services, inc, it was found that 60% of Houston security professionals would choose to implement a FireEye security system and 56% for Palo Alto Networks. Cisco's SourceFire ranked 6th in preference with other industry giants lagging far behind. Interestingly enough, when network security

budget is considered, Palo Alto Networks is ranked at the top at 41% with FireEye and SourceFire (Cisco) following closely at 37% and 27% respectively.

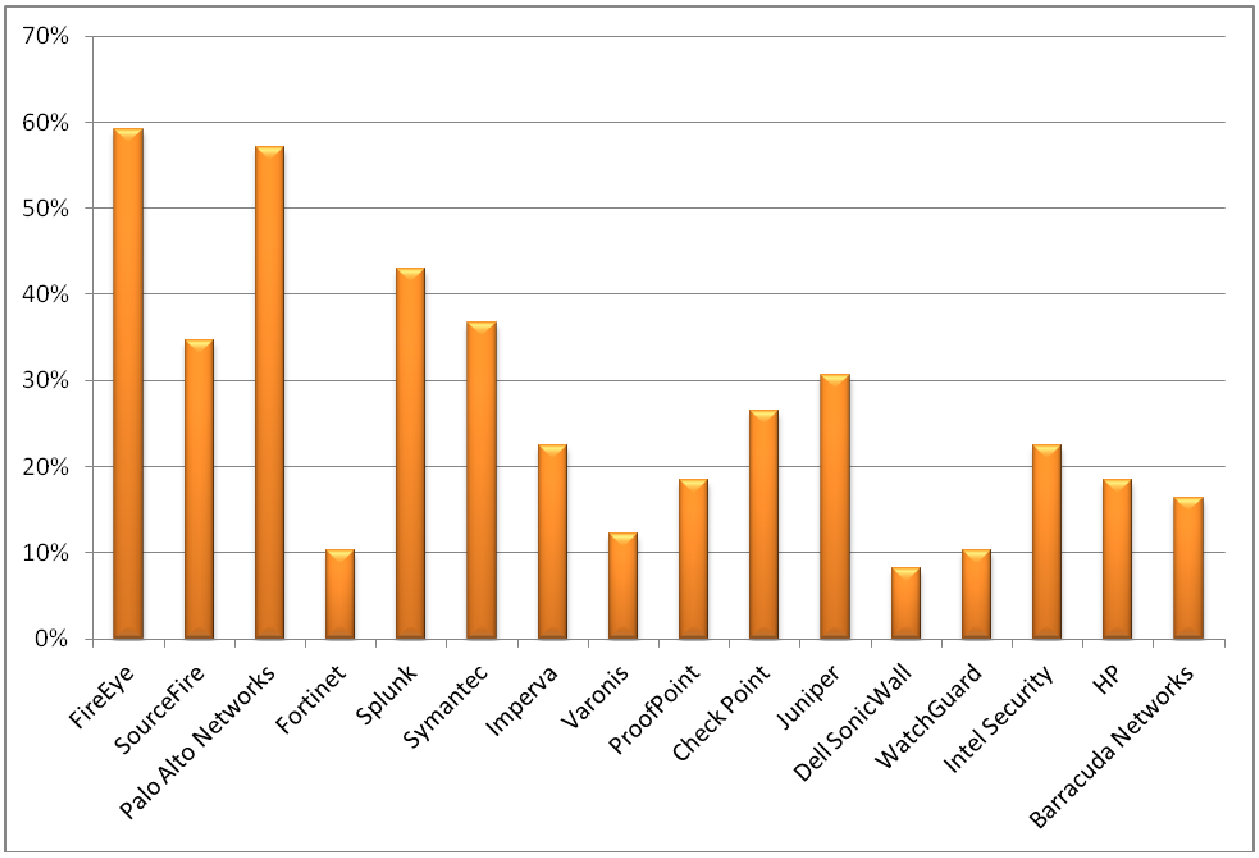
Companies I expect to emerge from the pack are those who have a strong focus in endpoint security, mobile security, and those that provide cloud technology. Endpoint was considered the top valued security feature by security specialists. Something that stood out as a surprise was how low a standalone NGFW was rated, suggesting that having a dedicated machine solely for security wasn't a priority. Mobile and email security weren't as highly regarded in the survey even though network security companies claim these are the top access points for malicious intrusions. As previously stated, 80% of all breaches begin with an email. With the increased occurrence of BYOD (bring your own device), mobile security, in my opinion, should begin to pick up, especially when considering how easily a smart phone can be hacked. In Check Point's security report, there has been a 91% increase in personal mobile devices being added to corporate networks over the past two years. 44% of the organizations do not manage corporate data on their employee's devices.

With all this in consideration, a strong protected network is only as good as the least aware member. The most inattentive piece in the system, whether it's an outdated patch or a gullible employee, can cause a full enterprise breach. Traditional security alone can no longer stand up to today's threat. If this shortage of good security professionals continues, SaaS and consulting services should be the center of network security. Don't assume that your system is secure and that you don't need a next-generation security system. As initially stated, you either know you've been hacked or you're unaware.

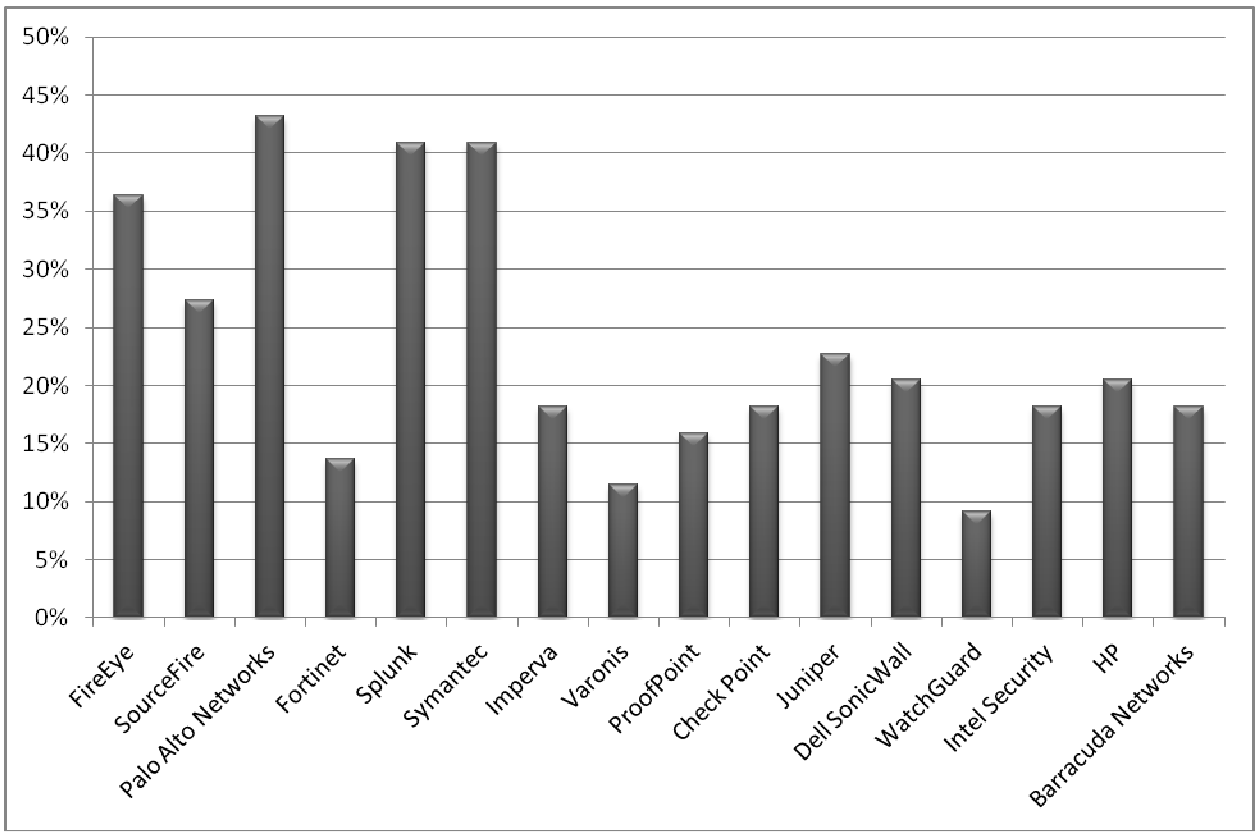
Top Security Technologies



Top Choice Vendors



Top Choice Under Budget Constraint



Glossary

ASA – Adaptive Security Appliance

ATD – Advanced threat detection

FEaaS – FireEye as a Service

INFW – Internal Network Firewall

IP – Internet Protocol

IPS – Intrusion Prevention System

MSM – Mobile Security Management

MSSP – Managed Security Service Provider

NGFW – next-generation firewall

NGIPS – Next-generation Intrusion Prevention System

NSM – Network Security Management

SaaS – Security as a Service

SMB – small or midsize business

UTM – Unified threat management

VM – Virtual machine

VPN – Virtual private network