Endpoint Security

Research Project

Introduction

In the past, most security breaches came in through the network. Today, however, threats are increasingly coming in through endpoints (devices like laptops, desktops, tablets and mobile phones), which means centralized network protection is no longer the best security solution for individual consumers or enterprises.

Endpoint vulnerabilities are increasingly being targeted because of the multiple connections between endpoints and different networks. Endpoint security software uses encryption and application control, but is still a weak line of defence because of the significant distance between the layer of security and the data in which it seeks to protect. The SaaS and remote maintenance which has satisfied consumers for years is fraught with danger.

A better endpoint security solution is to protect the data closer to the source. i.e. securing devices and data within the firmware (a small memory chip on a hardware device such as an SSD drive).

The subject of this market research report has developed a X-PHY security solution which is embedded directly into a device’s controller/ firmware, and the controller/firmware manages the flash where the data is stored. The firmware detects any anomalies in the data access patterns to find any signs of compromise. On top of that, the solution integrates with hardware sensors to add useful security features and ensure data protection from all angles.

Accordingly, this market research report aims the quantify the market opportunity for the innovative device and measure the strengths and weaknesses of its competitors. The research will focus on consumer security measures and the size of the markets that this new product seeks to challenge. All the research is secondary and source from freely available and reputable publications.

Market Size

Key Drivers

Number of mobile internet connections

The rapid proliferation of broadband-enabled mobile devices has led to a widespread prevalence of mobile computing among consumers and businesses. As the number of mobile internet connections increases, so does the attractiveness of targeting mobile devices with viruses. This has become particularly true as an increasing amount of sensitive information is being stored on mobile devices (e.g. personal financial information). As this trend continues, consumers and businesses alike will increasingly demand mobile security software, benefiting the industry. The number of mobile internet connections is expected to increase in 2019.

Number of broadband connections

As more of the population starts using high-speed internet connections, the number of targets for increasingly complex malware rises. This factor creates a larger potential customer base for industry operators. Consequently, an increase in the number of broadband connections bolsters industry demand. The number of broadband connections is expected to increase in 2019.

Per capita disposable income

As consumers' disposable income increases, so does their willingness to purchase new computers, which often necessitates the purchase of security software. In addition, when disposable income is low, consumers are less likely to upgrade their current security software. Per capita disposable income is expected to increase in 2019.

Market Performance

The Security Software Publishing industry has grown at a steady annualized rate of 8.6%, including an anticipated jump of 9.5% in 2019, to an estimated $19.1 billion. The industry's software publishers develop and distribute software products, such as antivirus, anti-keylogger, spyware removal, encryption and firewall software. Operators in the industry may also provide consulting and technical support related to this software. The recent surge in the number and types of wireless computing devices has expanded the market for industry products. Additionally, the industry has benefited from customers' changing views of security products. Once thought of as an optional cost, security software is increasingly viewed as a necessity to safeguard sensitive data and information.

Attacks spur growth

Numerous high-profile hacking incidents during the period have spurred greater demand for security software. For example, retail giant Home Depot was hacked in 2014, when as many as 56.0 million credit cards were breached. In addition, 2017 was a notably newsworthy year for cyberattacks. In the first half of 2017, more than hundreds of thousands of computers worldwide using the Microsoft Windows operating system fell victim to the WannaCry ransomware worm; the cyberattack encrypted user data and required payment (ransom) for the victim to have their data unlocked. Later, the hack of Equifax was an even greater incident, in which about 143.0 million Social Security numbers, names and birthdates were stolen by hackers, prompting a congressional investigation, a five-state class-action lawsuit and a massive stock dump. In 2018, The Harris Poll reported that nearly 60.0 million Americans have been affected by identity theft. This number is expected to increase.

Over the past five years, there has also been the rise of hacker group Anonymous, among others. The group successfully penetrated the networks of numerous businesses and government groups worldwide. When a company is targeted and successfully breached by a cyberattack, its reputation becomes threatened, as consumers are less likely to purchase that company's goods or use its services if they fear their personal data will be stolen. Attacks on government organizations could have even more devastating effects, such as the release of confidential documents that may place citizens in danger or even compromise national security. In 2014, the FBI expanded their 'Most Wanted' list to include a 'Cyber Most Wanted.'

Large-scale attacks have helped drive corporations and government organizations to pursue more extensive security efforts to stop future attacks.

Market shift

Several emerging trends in enterprise information technology (IT) infrastructure have also spurred demand for more complex, higher-margin security software, benefiting industry players that offer such software. Increasing business adoption of cloud computing has increased the complexity and breadth of security software required. Cloud computing uses servers (stored in-house or at a third-party site) to provide resources, software and data to computers and other devices on demand. For example, virtualization, a technology that underpins cloud computing, has led to security concerns regarding communications between virtual machines and visibility into virtualized server traffic.

As consumer preferences shifted toward tablets and smartphones, the industry has followed suit. Industry players have started to offer mobile security software to mitigate business concerns about the security risks posed by unsecured, employee-owned mobile devices accessing corporate networks. This product segment is growing quickly, spurred by increasing acceptance of employees’ use of personal devices to access business email, company documents and other information. Additionally, the ever-increasing percentage of services conducted online and the subsequent rapid increase in mobile and digital data, such as personal financial records, photos, music and videos, have encouraged major industry companies to increase their mobile security offerings. Revenue from mobile security software is expected to increase markedly moving forward.

Revenue Growth

Year	Revenue $ million	Growth %
2002	2,663.4	0.0
2003	3,715.3	39.5
2004	4,689.5	26.2
2005	5,220.9	11.3
2006	5,615.4	7.6
2007	7,576.5	34.9
2008	8,817.4	16.4
2009	9,543.4	8.2
2010	10,588.6	11.0
2011	11,126.3	5.1
2012	11,842.1	6.4
2013	12,365.2	4.4
2014	12,611.5	2.0
2015	13,007.8	3.1
2016	13,740.4	5.6

2017	14,999.1	9.2
2018	17,402.1	16.0
2019	19,054.6	9.5

Products and Services

Industry operators develop security software for a range of different types of customers, including enterprises, consumers and the government. While the level of technology may differ along market-lines (for example, an enterprise with a network of devices may need more powerful security software than a consumer that uses one PC), the classification of software largely remains the same or similar.

Threat protection

Threat protection software provides customers with protection against the likes of viruses, malware and zero-day vulnerability, as well as other cyberattacks and threats. Whether through the internet, an unauthorized or unsecure user on the network, or an unknown hole in software, threat protection software seeks to identify and protect against threats before they come to fruition. For example, Check Point's Next Generation Threat Extraction (NGTX) uses a variety of technology to protect against threats and zero-day attacks, and also has a network of sensors used to keep attack information up-to-date. In 2019, this product segment is expected to account for 32.2% of industry revenue.

Data protection

A major threat to businesses, government and individuals is the potential of data loss, whether through cyberattack, machine failure or a simple and innocent accident. Data protection software seeks to ensure customers quickly recover any data lost in such an event. Software products include Symantec's Granular Recovery Technology, which enables users to restore items from database backups, and McAfee's Device Control, which monitors how data is transferred and ensures data does not end up in the wrong hands. Data protection software is expected to represent 20.3% of industry revenue in 2019.

Network, internet and server

Network, internet and server security products protect against threats in the cloud, over an email server or within a company network. Such software includes McAfee's Network Security Platform, which is able to block attacks by identifying malicious traffic on a network, as well as Symantec's Secure Web Gateway, which protects online communications and ensures safe internet and cloud use. In 2019, industry revenue from this segment is expected to be 15.3%.

Security management and analysis

Security management (also known by its acronym SIEM) and analysis software is used by companies and organizations to monitor and analyze activity across a range of devices, including computers, networks and databases. By gathering information on systems, the software is able to analyze trends and spot abnormal patterns, which can trigger alerts on potential dangers. Some software can generate a plan of action to fight against a potential attack. In 2019, this group is expected to account for 11.9% of industry revenue.

Other services

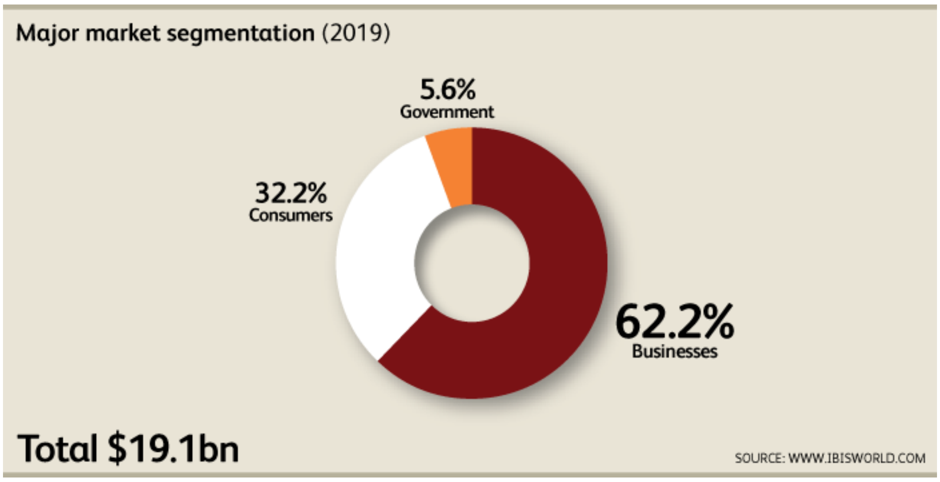
Industry companies offer a wide-range of products that may not fit under one category, such as scanning software, virus removal software and mobile security solutions. Companies also provide consulting services to businesses seeking to improve their information technology infrastructure or protect their data. While this business segment is a small share of the total industry, players use this as a way to market and sell other services to customers. Altogether, these products are expected to represent 20.3% of industry revenue in 2019.

Consumer Market

The consumer security software market accounts for 32.2% of industry revenue. This software typically protects consumers from unwanted viruses, malicious software (malware) and other intrusive programs that may steal information from the user or create problems with the software already present on the computer. Consumers often purchase subscriptions to access this software, and these subscriptions are typically offered on a yearly basis. Many products have different features and, in turn, target distinct consumer segments. For instance, an industry product may focus on antivirus software and another may feature adware protection.

More industry players have started including all of these services (e.g. anti-virus, internet security and adware prevention) bundled into one piece of software, seeking to capture consumers that are seeking an all-encompassing product. Also, companies are increasingly selling directly to consumers as operators have started selling products on their websites using e-commerce. This trend has served to grow profit as the expense of delivering the product through the internet is less than selling prepackage products through retail stores.

Many publishers are also concentrating on creating consumer security products for the mobile market, targeting the trend of fast growing smart phone sales. This trend will contribute to heightened sales over the next five years. The primary driver of mobile security software will come from business, and they will often pay for this service for their employees. Therefore, a majority of revenue from this software, which will be administered on consumers' phones, will likely come from the business market.



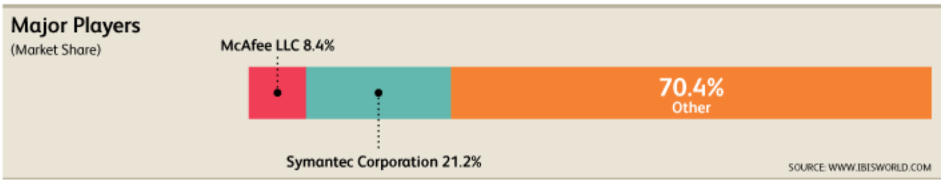
Competitor Analysis

The Security Software Publishing industry exhibits a moderately low level of concentration. In 2019, the industry's three major players are expected to account for just 32.7% of the market. Although these three companies make up a sizeable share of the industry, the nature of the industry enables new entrants to quickly scale and seize new opportunities, such as producing programs that address certain concerns in a quickly changing IT landscape. For example, two relatively recent trends, the virtualization of computing environments and the increasing adoption of employee-owned mobile devices in the workplace, have created new opportunities for industry companies (big and small) to address new enterprise security concerns.

Security Software Publishing industry products are often a sensitive purchase for customers. Users rely on these programs to defend against viruses, malware and other threats that could cause the loss of sentimental personal data, highly valuable corporate data or confidential government data. As a result, major players typically have the advantage since they have established strong reputations. These reputations resonate with consumers and businesses alike, which are generally more prepared to trust the more well-known companies with their sensitive security needs.

Even though security products are largely considered nondiscretionary, the price of a particular security product remains a basis on which companies compete. Players that can offer competitive pricing often have an edge over the competition because buyers will attempt to pay less for security products. This trend is more prevalent among consumers as this segment is more concerned about price, whereas businesses are willing to pay more to protect sensitive data.

Not every customer is seeking for the same security solution, which opens the door for industry companies to offer a wide-variety of features and purchase options. While many customers purchase packages of security programs, companies also offer ad-hoc or “buffet style” options, wherein customers can purchase only what they need. Since not every company (especially smaller companies) can offer a diverse portfolio of products, this serves as a basis of competition; companies that offer products that are attractive to customers will better compete than companies that offer outdated or products to smaller markets.



Major Companies

Symantec Corporation

Market Share: 21.2%

Brand Names: Norton, Symantec Endpoint Protection

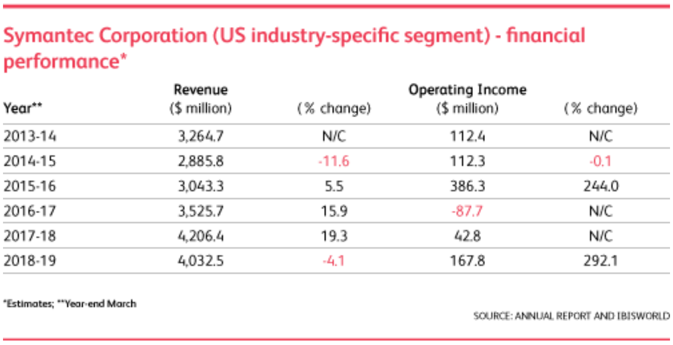
Founded in 1982 and based out of Mountain View, CA, Symantec Corporation (Symantec) has become the largest publisher of security software in the United States. The company now employs 11,800 people worldwide. Following the acquisition of Peter Norton Computing in 1990, Symantec began publishing the Norton brand antivirus software. In January 2016, the company completed the divestment of its information management businesses. The company now operates under two segments: Consumer Security and Enterprise Security (both of which are relevant to this industry). The company’s security solutions include endpoint security, encryption and mobile offerings, Secure Socket Layer (SSL) certificates, authentication, mail and internet security, data center security and data loss prevention offerings.

Symantec aggressively expanded through acquisitions over the five years to 2019. In 2016, the company acquired Blue Coat Systems (Blue Coat) and in 2017 it closed the acquisition of LifeLock Inc. (LifeLock). The two companies were purchased for nearly $7.0 billion. While this acquisition has significantly decreased its operating income in the year, it also significantly increases Symantec's consumer and enterprise capability; LifeLock specializes in identity theft protection and Blue Coat is a provider of internet security for enterprises and governments.

Symantec also has a mobile protection strategy, which it announced in 2010. The strategy aims to manage mobile devices, protect against threats and integrate mobile security software with enterprise data centers. In 2012, Symantec expanded on this strategy by acquiring Odyssey Software, a mobile device management software developer, and Nukona Inc., a mobile application management company. In 2014 and 2017, Symantec further increased its mobile security capabilities by acquiring two additional companies focused on mobile threats. Symantec is now strategically situated to offer an all-encompassing security solution for mobile devices.

Financial performance: Over the five years to 2019, Symantec's US security software revenue is expected to grow at an annualized rate of 4.3% to an estimated $4.0 billion. After consecutive declines in 2014 and 2015, the company's industry-specific revenue rebounded by posting strong gains of 15.9% in 2016 and 19.3% in

2017, though revenue declined moderately in 2018. Higher revenue is the result of two significant acquisitions of Blue Coat and LifeLock in 2016 and 2017, respectively.



Symantec Corporation (US industry-specific segment) - financial performance*

Year**	Revenue ($ million)	(% change)	Operating Income ($ million)	(% change)
2013-14	3,264.7	N/C	112.4	N/C
2014-15	2,885.8	-11.6	112.3	-0.1
2015-16	3,043.3	5.5	386.3	244.0
2016-17	3,525.7	15.9	-87.7	N/C
2017-18	4,206.4	19.3	42.8	N/C
2018-19	4,032.5	-4.1	167.8	292.1

*Estimates; **Year-end March

SOURCE: ANNUAL REPORT AND IBISWORLD

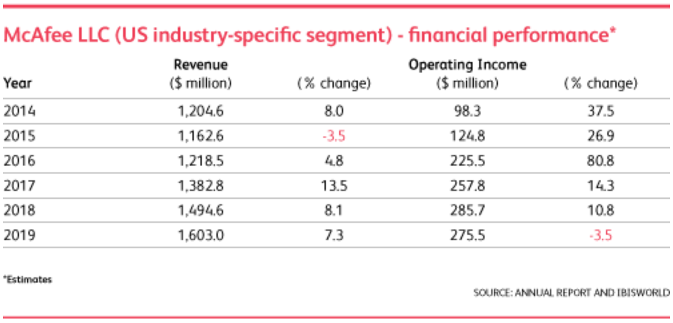
McAfee LLC

Market Share: 8.4%

California-based Intel Corporation entered the industry in August 2010 when it purchased the industry’s second-largest player, McAfee Inc., for nearly $7.7 billion. McAfee now operates as an independent subsidiary of Intel and private equity firm TPG Capital. McAfee offers security products for consumers and businesses of all sizes. In addition to PC antivirus and internet security products, the company offers identity theft protection and security packages for Apple computers and mobile devices. Its business offerings include protection packages specifically tailored for businesses in certain sectors, including healthcare and public companies. The company, which employs about 7,000 people, generated an estimated $2.4 billion in 2017.

In 2016, Intel announced it will be spinning off McAfee into a separate company, McAfee LLC. This new company is jointly owned by Intel and private equity firm TPG (49.0% and 51.0% ownership, respectively). However, the two companies have worked together to increase the security of Intel’s hardware. This gives McAfee’s security software a unique competitive advantage because other chip makers are not likely to disclose sensitive chip design information to outsiders. This makes it impossible for other security software developers to integrate their software with computer hardware products. McAfee also provides security software for mobile devices; however, McAfee lacks the encompassing array of mobile-management security and integration features that Symantec offers.

Financial performance: Over the five years to 2019, McAfee’s industry-relevant revenue is expected to grow an annualized 5.9% to $1.6 billion. Growth has largely been supported by McAfee’s acquisition by Intel, which enabled McAfee to cross-sell its products to Intel’s existing customer base. Operating income has also risen an annualized 22.9% to $275.5 million over the five years to 2019.



McAfee LLC (US industry-specific segment) - financial performance*

Year	Revenue ($ million)	(% change)	Operating Income ($ million)	(% change)
2014	1,204.6	8.0	98.3	37.5
2015	1,162.6	-3.5	124.8	26.9
2016	1,218.5	4.8	225.5	80.8
2017	1,382.8	13.5	257.8	14.3
2018	1,494.6	8.1	285.7	10.8
2019	1,603.0	7.3	275.5	-3.5

*Estimates

SOURCE: ANNUAL REPORT AND IBISWORLD

Other Companies

Check Point Software Technologies Ltd.

Market Share: 3.1%

Check Point Software Technologies Ltd. (Check Point) is an Israel-based security software company that was founded in 1993. The company’s US offices are located in California. Check Point’s software products include network and gateway security solutions, data and endpoint security solutions, mobile security and management solutions. The company employs about 4,500 people globally, about 24.0% of which are based in the United States. Check Point’s US security software revenue is expected to increase at an annualized rate of 9.8% to $586.1 million over the five years to 2019.