THE FUTURE OF CYBERCRIME & SECURITY

Key Takeaways & Juniper Leaderboard

Prepared for Webroot

www.juniperresearch.com

JUNIPER RESEARCH

Contents

1. Cybercrime & Cybersecurity: Key Takeaways

2. Network & Endpoint Cybersecurity: Competitive Landscape & Leaderboard

1. Cybercrime & Cybersecurity: Key Takeaways

1.1 Cybercrime Key Takeaways

1.1.1 IoT Botnets & DDoS Emerging

Security is still not being designed into much of the IoT (Internet of Things), particularly those areas that work from legacy M2M (machine to machine) networks. This leaves them open to use by cybercriminals, who leverage them as part of botnets, in the absence of immediately valuable information of their own.

1.1.2 Rising Ransomware Threat

There was a huge increase in the amount of ransomware deployed in 2016, which is also increasing in complexity. Multiple cybersecurity organisations registered large increases in the use of this kind of attack and several prevalent new variants of the software came into use.

These are also increasingly automated and presented as simple-to-use kits, meaning that these attacks are quick and easy to execute, making high-volume, low-value ransomware more common.

1.1.3 File-less Attacks Increasingly Common

Several cybersecurity institutions have reported an increase in the number of non-malware attacks over the past year. These attacks either subvert the function of normally helpful programs, avoiding the detection of file-based analysis like traditional antivirus, or are caused by malicious insiders misusing the access they have legitimately been given. Over time this will cause many more businesses, and ultimately consumers, to rely on behavioural, rather than file-based, detection methods.

1.1.4 Traditional Attack Vectors Still Strong

Data from several sources shows that many years-old CVEs (common vulnerabilities and exposures) are being exploited, despite increased awareness of the need to update systems. At the same time, social engineering remains a key way in for cybercriminals, via phishing emails and similar well-used vectors.

However, such attacks are now being used more frequently to deploy malware, rather than simply get credentials from users.

1.2 Cybersecurity Key Takeaways

1.2.1 Talent & Budget Shortage Increases AI (Artificial Intelligence) Attractiveness

Cybersecurity has a shortage of trained professionals, and those SMEs (Small & Medium Enterprises) most at risk from cybercrime frequently have no budget for cybersecurity. These factors both mean that AI-based cybersecurity packages, which filter and automatically remedy a range of threats, will be most appealing to many potential customers.

Those companies that can most effectively leverage AI (in positioning as well as products) will be in the best position to tap into the large SME market.

1.2.2 Governments Take Cybersecurity Funding Seriously, Legislation Lags

Governments worldwide are spending tens of millions on cybersecurity funding, focusing on education resource and training. The legislative measures addressing cybersecurity are still *de facto* rather than explicit, however. With more extreme cases of cybercrime expected in the coming year, affecting more vital systems, this will shift the cybersecurity conversation into a tighter regulatory framework.

Several companies already view cybersecurity in light of regulatory compliance and Juniper expects this to be part of lawmakers' conversations soon.

1.2.3 Pervasive Threat Intelligence on the Horizon

Due to the ability to use automation and machine learning capabilities in tandem, threat intelligence is likely to cease being a discrete business type in the future.

Several endpoint security providers are already positioning their offerings as incorporating threat intelligence, while threat intelligence vendors can offer real-time network and endpoint protection as a simple extension of their core intelligence offerings.

Specialised diagnostics tools may still exist as part of the software used by MSSPs (managed security service providers), but this will soon become another element of endpoint protection for business customers.

1.2.4 Market Consolidation Begins as Investor Funding Slows

Investment in cybersecurity has been one of the biggest growth areas in recent years, but the amount available for each investment levelled off in 2016, indicating that investors are becoming more cautious in their support of each new cybersecurity venture. At the same time, the array of cybersecurity products on offer is confusing buyers.

Juniper Research believes that those companies which cannot differentiate themselves to investors or customers will either close or become absorbed by their competitors.

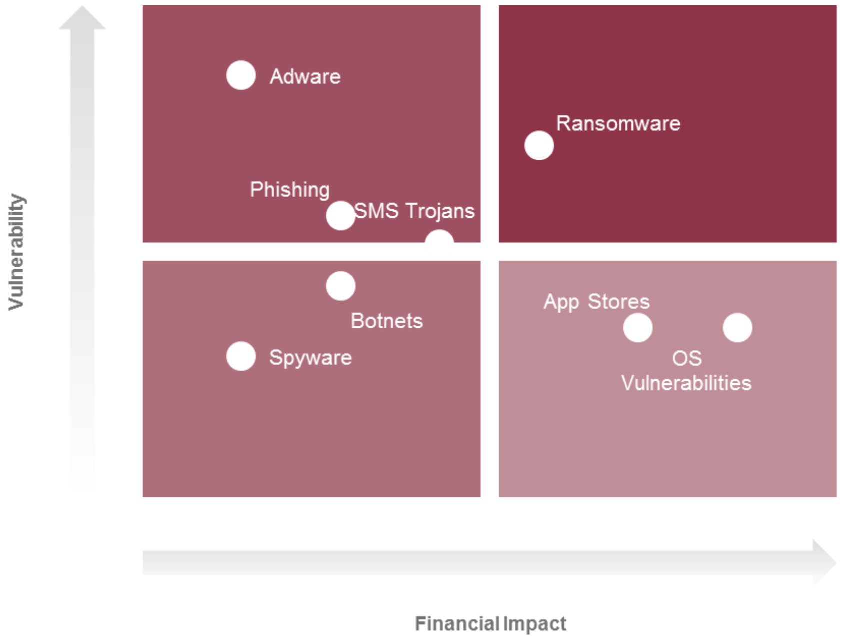
1.2.5 Device Threat Assessment

Smartphones will continue to be the most common device targeted by cybercriminals, although they will remain a small proportion of the overall malware in circulation until truly cross-platform OSs (particularly Windows-based cross-platform OSs) are introduced.

- Windows is particularly vulnerable because cybercriminals have spent years working with Windows-based systems to hack PCs. The universality of Windows 10 also means that threats can be easily transferred from traditional platforms.
- There are also sharp increases in the amount of mobile malware available, much of which comes preloaded on Android phones. Smartphone vendors need to work harder to prevent this form of preloaded malware.

a) Adware is the prevailing type of malware on smartphones and, as a result, advertising constitutes the biggest threat to smartphone security in the current environment.

Figure 1.1: Juniper Device Cybercrime Threat Landscape Assessment

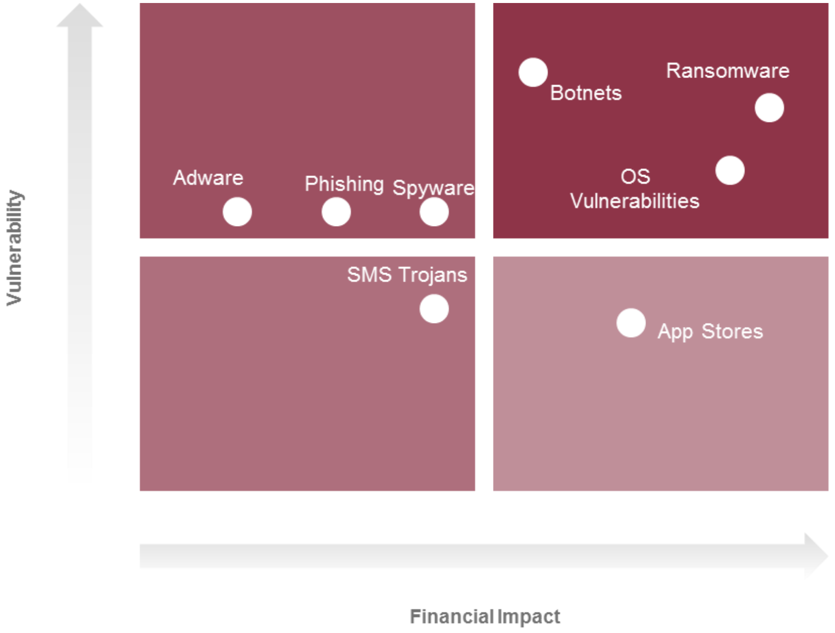


Source: Juniper Research

- While SMS is in decline as a messaging medium, the fact that MNOs (Mobile Network Operators) take a portion of premium rate revenues disincentivises them from limiting or removing premium rate SMS functionalities, meaning these scams will remain a threat for the foreseeable future.
- App stores offer a secure platform to deliver apps, with a malware screening process. However, these can be evaded by various means

(particularly at the update stage), which allows malware to impact a wide range of users.

Figure 1.2: Juniper Device Cybercrime Threat Landscape Forecast



Source: Juniper Research

- OS vulnerabilities are likely to remain to a degree, so stay a channel through which cybercriminals can effectively compromise smartphones.

  a) While they can be patched, they will be a potential weakness so long as users have the option not to make major upgrades to their smartphone OS.

- With increasing numbers of apps and retailers using biometric- and location-based verification as part of their digital platforms, we expect more spyware to be developed to leverage this data as it becomes more monetisable and is more directly linked to retail and mCommerce.

- As noted elsewhere, there is a large increase in the number of ransomware attacks. With the proliferation of smartphones in use for a wide variety of tasks, this will continue to be an attractive attack vector for cybercriminals.

- The proliferation of smartphones makes a tempting target for cybercriminals to attack with the always useful botnets. With the release of the Mirai botnet code in October 2016, these forms of attack will continue to increase, as well as their overall magnitude.

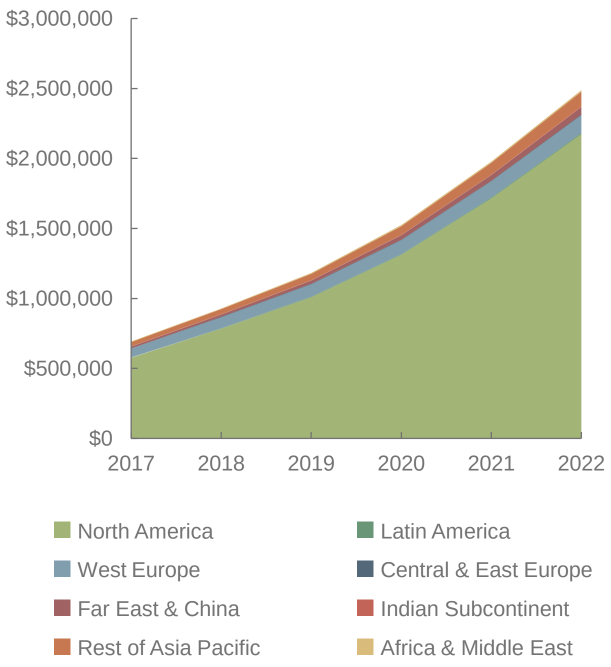
- The IoT has shown it can provide a rich ground for botnets, thanks to the attack on Dyn in the October 2016 botnet attack. This will be the primary threat to most IoT devices in the future, as the information and credentials such devices can provide is minimal, while still being able to contribute computing power to a botnet or restrict access to what information it does hold.

We expect IoT ransomware to be the most prevalent and observable cybersecurity threat to consumers, as well as providing entry points for other kinds of attack to exfiltrate details.

1.3 Cybercrime Breaches Forecasts

With an increasing number of businesses going online and particularly connecting their data with the cloud, Juniper Research expects that the total cost of data breaches worldwide will be just under $2.5 trillion by 2022.

Figure & Table 1.3: Cost of Criminal Data Breaches per annum ($m), Split by 8 Key Regions 2017-2022



- North America leads throughout the forecast period, although its share declines slightly as other regions introduce harsher penalties for incurring data breaches. Developed regions also have a much higher cost per breached record because of the cost of regulatory penalties for data breaches.
- These costs include both direct and indirect cost of breaches, covering the replacement of hardware, additional staff required, abnormal churn and other company devaluations caused by reputational damage.

	2017	2018	2019	2020	2021	2022
North America	$577,267	$784,530	$1,008,794	$1,312,237	$1,715,172	$2,175,789
Latin America	$2,002	$2,637	$3,460	$4,525	$5,961	$6,082
West Europe	$60,895	$77,621	$87,501	$99,446	$114,657	$127,867
Central & East Europe	$2,727	$3,812	$4,373	$4,805	$5,306	$5,546
Far East & China	$13,084	$16,882	$22,704	$30,532	$40,949	$52,251
Indian Subcontinent	$1,145	$1,415	$1,861	$2,410	$3,073	$3,429
Rest of Asia Pacific	$30,215	$36,783	$47,076	$63,255	$83,981	$106,476
Africa & Middle East	$4,407	$5,404	$6,582	$8,006	$9,678	$10,981
Global	**$691,742**	**$929,085**	**$1,182,351**	**$1,525,215**	**$1,978,776**	**$2,488,421**

Source: Juniper Research

2. Network & Endpoint Cybersecurity: Competitive Landscape & Leaderboard

2.1 Introduction

A rapidly growing number of players are entering the cybersecurity market with a variety of approaches. This section is not intended to provide a comprehensive list of all vendors in the market, but instead to introduce the reader to selected vendors that have been active and successful recently in this space. Vendor profiles for each of these are included at the end of this section.

We have chosen a range of providers from across the cybersecurity market, from device vendors and component manufacturers to service providers, to illustrate the range of possible operators in this growing space.

2.2 Vendor Analysis & Juniper Leaderboard

Due to the differences between various kinds of cybersecurity offerings, we will be evaluating enterprise network and endpoint cybersecurity offerings and cloud cybersecurity in separate Juniper Leaderboards. Where vendors have both kinds of product, we have applied different scoring to reflect the different products offered. Any consumer offerings will be noted in the profiles but not reflected in the Leaderboard scoring.

2.2.1 Network & Endpoint Cybersecurity Vendors

The following vendors are compared in the Juniper Leaderboard overleaf.

- Barracuda
- Carbon Black
- Cylance
- DarkTrace
- FireEye
- Fortscale
- PatternEx
- SecureWorks
- Skycure
- Symantec
- Tanium
- Webroot

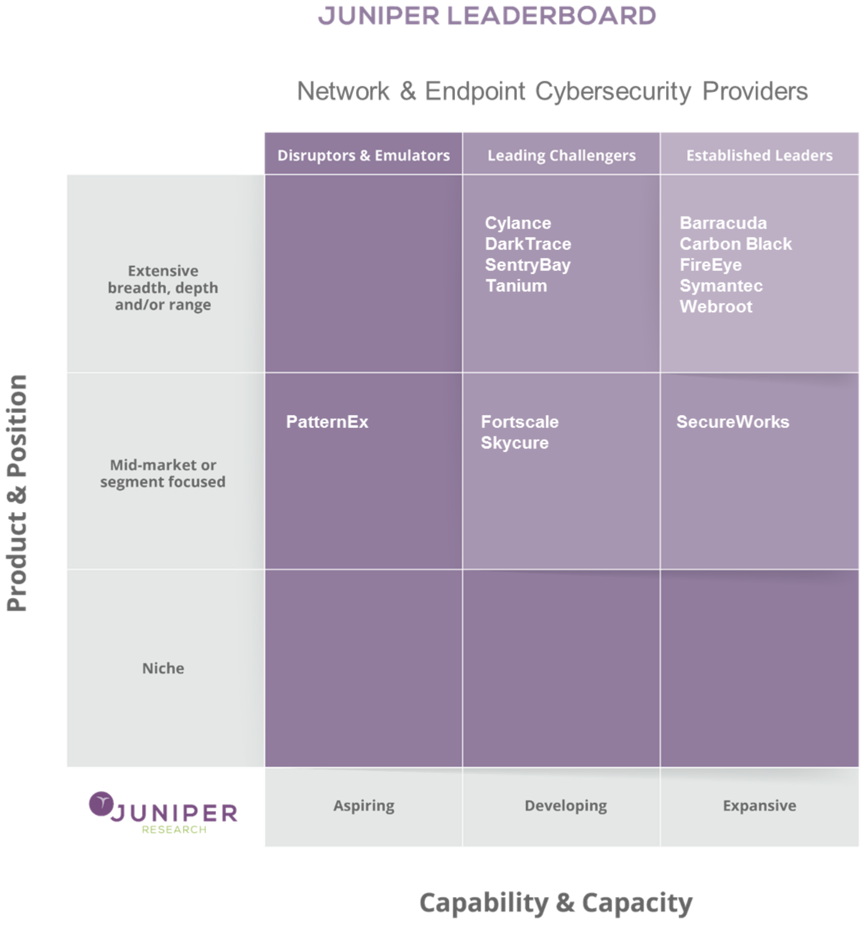
2.2.2 Stakeholder Assessment Criteria

Our approach is to use a standard template to summarise vendor capability. This template concludes with our views of the key strengths and strategic development opportunities for each vendor.

This technique, which applies quantitative scoring to qualitative information, enables us to assess each vendor's capability and capacity and its product and position in the cybersecurity market. The resulting Leaderboard shows our view of relative vendor positioning. We have assessed each vendor's capabilities against the criteria listed overleaf.

2.3 Juniper Leaderboard for Network & Endpoint Cybersecurity

Figure 2.1: Network & Endpoint Cybersecurity Providers Leaderboard



JUNIPER LEADERBOARD

Network & Endpoint Cybersecurity Providers

Product & Position	Disruptors & Emulators	Leading Challengers	Established Leaders
Extensive breadth, depth and/or range		Cylance DarkTrace SentryBay Tanium	Barracuda Carbon Black FireEye Symantec Webroot
Mid-market or segment focused	PatternEx	Fortscale Skycure	SecureWorks
Niche			
JUNIPER RESEARCH	Aspiring	Developing	Expansive

Capability & Capacity

WEBROOT Smarter Cybersecurity

Webroot has seen strong growth in recent years, and has had particular success with OEM (Original Equipment Manufacturers) partners. However, its endpoint solution leverages similar state of-the-art techniques to other vendors, so it will have to diversify and expand its offerings to keep its position.

Source: Juniper Research

Table 2.2: Network & Endpoint Cybersecurity Providers Leaderboard Scoring

	Corporate Capability					Product & Positioning				
	Experience in Sector	Financial Performance in Sector	Operations	Marketing & Branding Strength	Mergers & Acquisitions	Range of Product Features	Range of Solutions	Compatibility & Interoperability	Customers & Deployments	Future Business Prospects
Barracuda	🟩	🟩	🟩	🟩	🟢	🟡	🟩	🟢	🟢	🟩
Carbon Black	🟩	🟩	🟩	🟡	🟩	🟩	🟢	🟡	🟡	🟩
Cylance	🟠	🟩	🟩	🟩	🟡	🟡	🟡	🟩	🟢	🟡
DarkTrace	🔴	🟩	🟩	🟠	🔴	🟩	🟩	🟡	🟠	🟩
FireEye	🟡	🟢	🟢	🟢	🟩	🟢	🟢	🟩	🟡	🟡
Fortscale	🟠	🟠	🟠	🔴	🔴	🟠	🟩	🟡	🟡	🟡
PatternEx	🟩	🔴	🟡	🔴	🟡	🟡	🟩	🟡	🟢	🟡
SecureWorks	🔴	🔴	🔴	🔴	🔴	🟠	🟠	🟡	🔴	🟠
SentryBay	🟢	🟩	🟢	🟡	🟡	🟩	🟩	🟡	🟡	🟢
Skycure	🟠	🟠	🟠	🟠	🔴	🟡	🟩	🟩	🟠	🟠
Symantec	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟩	🟢	🟢
Tanium	🟡	🟢	🟠	🟡	🔴	🟢	🟩	🟢	🟡	🟢
Webroot	🟢	🟩	🟡	🟢	🟩	🟡	🟡	🟩	🟩	🟩

HIGH 🟢🟩🟡🟠🔴 LOW

Source: Juniper Research

2.3.1 Limitations & Interpretation

Our assessment is based on a combination of quantitative measures where they are available (such as revenues and numbers of employees) that will indicate relative strength and also of qualitative judgement based on available market and vendor information as published. In addition we have improved our in-house knowledge from meetings and interviews with a range of industry players. We have used publicly available information to arrive at a broad, indicative positioning of vendors in this market, on a ‘best efforts’ basis. However, we would also caution that our analysis is almost by nature based on incomplete information and therefore some elements of this analysis we have had to be more judgemental than others. For example with some vendors, less detailed financial information is typically available if they are not publicly listed companies.

We also remind readers that the list of vendors considered is not exhaustive across the entire market but rather selective. Juniper Research endeavours to provide accurate information. Whilst information or comment is believed to be correct at the time of publication, Juniper Research cannot accept any responsibility for its completeness or accuracy: the analysis is presented on a ‘best efforts’ basis.

The Leaderboard compares the positioning of network and endpoint cybersecurity vendors and service providers based on Juniper’s scoring of each company against the criteria Juniper has defined. The Leaderboard is designed to compare how the vendors position themselves in the market based on these criteria: relative placement in one particular unit of the Leaderboard does not imply that any one vendor is necessarily better placed than others. For example, one vendor’s objectives will be different from the next and the vendor may be very successfully fulfilling them without being placed in the top right box of the Leaderboard which is the traditional location for the leading players.

Therefore, for avoidance of doubt in interpreting the Leaderboard we are not suggesting that any single box implies in any way that a group of vendors is more advantageously positioned than another group, just differently positioned. We additionally would draw the reader’s attention to the fact that vendors are listed alphabetically and not ranked in any way in the box of the Leaderboard.

The Leaderboard is also valid at a point in time: April 2017. It does not indicate how we expect positioning to change in the future, or indeed in which direction we believe that the vendors are moving. We caution against companies taking any decisions based on this analysis: it is merely intended as an analytical summary by Juniper as an independent third-party.

2.3.2 Webroot

WEBROOT Smarter Cybersecurity

i. Corporate Profile

Webroot, founded in 1997, delivers next-generation endpoint security and threat intelligence services to protect businesses and individuals. The threat intelligence platform is a cloud-based collective approach derived from millions of real-world devices.

Through acquisition, Webroot technology now includes machine-learning generated threat intelligence, network anomaly, endpoint malware and anti-virus protection.

As a privately held company, Webroot does not publicly reveal its financial performance. 2 funding rounds have been completed since its inception (the last of which took place in 2010), generating $109 million. The company announced a record year for fiscal 2016 (ending June 2016), with business growth recorded at 36%.

Key executives at the company include Dick Williams (CEO); Hal Lonas (CTO); John Post (CFO).

ii. Geographic Spread

Webroot's headquarters are in Colorado, US, with additional offices elsewhere in the US, Europe and Australia.

iii. Key Clients & Strategic Partnerships

- The company has large scale partners such as Cisco F5 Networks, Aruba, Palo Alto Networks, A10, in addition to others. Overall, its client base numbers 120,000 with over 40 million users
- Webroot's partner network consists of managed service providers, resellers and technology partners.
- Conosco announced a partnership with Webroot in November 2016, with the aim of using the latter's technology to secure enterprise endpoints.
- The company partnered with CMS Distribution in October 2016 to extend its ability to reach customers in the UK.

iv. High Level View of Offerings

Webroot SecureAnywhere Business Endpoint Protection is the company's core product, offering Software as a Service endpoint protection with an emphasis on low-power continuous monitoring and automated remedial action. The product includes a threat intelligence platform and supports both mobile and virtual endpoints, in addition to traditional deployments. The monitoring platform is also scalable, offering cloud-based management of over 100,000 endpoints.

- The key service underpinning Webroot's solutions is its Threat Intelligence Platform and Brightcloud Threat Intelligence services. Here, the company utilises its licensed endpoints and the installed products of its technology partners as a large-scale sensor network to detect threats the moment they surface anywhere across the globe. To this Webroot adds elements such as exploit honeypots, spam traps, semi-open proxy farms, naïve user simulation and third party data, to build a comprehensive picture of the threat landscape. As each detected malicious packet can be associated with an IP address, the platform is able to dynamically adjust what it considers malicious IP addresses in near-real-time.

- The Threat Intelligence Platform also benefits from 5th Generation Machine Learning, to build a statistical picture of the behaviour of applications running on a company's network to classify their intent. If the intent is judged to be malicious, the application can be removed by the agent.

Webroot has a number of solutions that can be incorporated by technology partners to add features, capabilities and increase the efficacy of their security offerings.

- Web Classification: Analyses uncategorised sites using advanced machine learning at a rate of 5,000 URLs/second. Categorises URLs across 83 categories.
- Web & IP Reputation: Scores website risk regardless of Internet category to deliver an up-to-date security check of the websites users are visiting. Delivers dynamic IP reputation scores and provides a dynamic list of malicious IPs at any given time to block malicious traffic from entering a network.
- Streaming Malware Detection: Real-time detection of malicious files, unknown and zero-day threats, at the network perimeter using on-device, machine learning-based malware detection technology.
- Real-Time Anti-Phishing: Provides anti-phishing protection through real-time scans before sites are visited.
- BrightCloud Threat Intelligence for IoT Gateways: Reputation-based IoT communications permissions tool. Deployed on IoT gateways, Webroot's agent occupies a footprint of 750Kb, making it suitable for a wide range of devices.
- File Reputation: Continuously updates real-time lookup service of known malicious and whitelisted file identifiers. Handles over 4 billion queries a day, equating to 50,000 per second.
- Mobile App Reputation: Categorises and scores apps using multi-stage analysis and advanced algorithms to ensure they are safe and compliant. Over 55 million Android and iOS apps have been analysed to date.
- Mobile Security Software Development Kit: Offers enhanced mobile security, including anti-virus, anti-malware, device and application interrogation, secure web browsing and overall device risk score.

v. Juniper's View: Key Strengths & Development Opportunities

- Webroot's low-power and scalable solutions make it an ideal solution for the Internet of Things deployments. It is possible that the business can evolve in this direction specifically, as running alongside other endpoint protection software is a key selling point for the company's products.
- The use of BrightCloud in a range of contexts means that Webroot can deploy the solution both as an integrated solution for its technology partners and as a product for end users and Managed Security Service Providers, giving it a very flexible position in the market.