KuppingerCole Report

LEADERSHIP COMPASS

by John Tolbert | February 2018

Enterprise Endpoint Security: Anti-Malware Solutions

This report provides an overview of the market for Enterprise Endpoint Security: Anti-Malware Solutions and provides you with a compass to help you to find the Anti-Malware product that best meets your needs. We examine the market segment, vendor product and service functionality, relative market share, and innovative approaches to providing Anti-Malware solutions for enterprises.

by **John Tolbert**
jt@kuppingercole.com
February 2018

Leadership Compass
Enterprise Endpoint Security: Anti-Malware Solutions
By KuppingerCole

Content

Content of Tables

Content of Figures

Related Research

Leadership Brief: Defending against ransomware - 70336

Buyer's Guide: Ransomware Protection - 72599

Advisory Note: Understanding and Countering Ransomware - 70282

1 Introduction

Both malware and anti-malware solutions have been around for a long time. Accordingly, individuals and organizations have been using an ever-changing mix of anti-malware software on endpoints. The earliest anti-virus programs were designed to combat file-based malware, often delivered via floppy disks. With the widespread adoption of email, it became the primary vector for spreading computer viruses. Network worms were (and still are) created by malicious actors to distribute malware across networks without needing users to open files or email attachments. Worms jump from host to host by compromising services listening to well-known TCP or UDP ports. Malefactors also found that users could be easily infected by placing their malware on heavily used websites, corrupting commonly used applications, packaging malicious executables in otherwise innocuous-looking data, using macros in Office documents, etc.

In recent years, the ransomware phenomenon has risen to prominence. Ransomware is a type of malware that encrypts user files and directs the user to pay the malware author a ransom for the decryption keys, usually in Bitcoin. These types of attacks often arrive in Office docs with malicious macros. The best advice for end users and organizations is to not pay the ransom, as the authors don't always deliver the decryption keys, and one shouldn't encourage future bad behavior by compensating the programmers for their fraudulent efforts.

At the time of publishing this report in 2017, we are witnessing another phase in the evolution of malware. The perpetrators are innovating by employing the worm delivery technique for ransomware. With the Petya/NotPetya attack, we have seen a type of malware that mimics ransomware, but seems to be intended for mostly destructive purposes rather than for financial gain. Suffice it to say that the variations in malware types has increased exponentially over the last few decades and will continue to be a significant threat for the foreseeable future.

Who are the malefactors behind all these attacks? At a high level, the major malware creators are hacktivists, fraudsters, and state sponsors. Each group has different motivations for making malware, and often different intended targets. But as with their biological analogs, computer viruses often infect unintentional targets as well. Malicious actors have learned and applied the "as-a-service" model, and now malware can be purchased on the so-called dark web and deployed by those who are not proficient at coding. This increases the frequency of attacks, as the ability to launch them now does not require technical skills, just malicious intent.

In the early days, anti-virus vendors gathered virus samples and created signature files that could recognize the more limited number of virus patterns. The vendors delivered the signature file updates to their customers; at first infrequently, but as the volume of viruses grew, updates grew more frequent. For vendors using signature files today, their clients typically receive updates several times a day.

Signature-based scanning alone is an ineffective malware prevention measure today. Malware has become far more sophisticated, often using polymorphic techniques to change their appearance to fool signature-based scanners. In the endpoint security market, most vendors have added new detection capabilities to more efficiently and effectively prevent malware infections. These new approaches to malware detection will be discussed in more detail later in this report.

Malware detection and prevention can happen in many places within a computing environment: at the network perimeter, email gateways, web proxies, application firewalls, desktop, virtual desktop, etc. Contemporary security researchers and analysts describe the potential points of intercept in an attack as the "cyber kill chain™". A defense-in-depth approach is always recommended, thus anti-malware and related security solutions should be deployed at each possible point in the cyber kill chain™ and physical architecture to maximize detection/prevention and minimize risks.

Endpoint security products may contain more features than anti-malware, such as URL filtering, application whitelisting, backup, configuration management, patch management, disk and file encryption, etc. The focus of this report is on anti-malware solutions at the endpoint, specifically desktops and laptops running Microsoft Windows, Mac OS, and Linux variants. Most of the vendors considered herein provide solutions for servers, virtual desktops, and mobile devices. Mobile anti-malware solutions will be the subject of another report.

This KuppingerCole Leadership Compass provides an overview of the leading vendors in this market segment. Picking solutions always requires a thorough analysis of customer requirements and a comparison with product features. Leadership does not always mean that a product is the best fit for a customer and his requirements. However, this Leadership Compass will help identify those vendors that customers should look at more closely.

1.1 Market Segment

The anti-malware market is steady, with more than 1 billion devices deployed in the world. Mobile platforms are on the rise, and have overtaken PC-based hardware systems in popularity in recent years. Desktops and laptops and the concomitant need for protecting them against malware will persist into the foreseeable future, especially given the increasing frequency and complexity of malware attacks.

There are many vendors in the anti-malware market. There are quite a few that have been long-established in the space, dating back decades and providing the first signature-based anti-virus programs. In the last few years, new startups have emerged with new techniques to discover and prevent malware infections. In some cases, the small companies have been acquired by the major players in the space, with their technologies integrated into the suite vendors' products.

1.2 Delivery models

Anti-malware solutions are made of two primary components: agents on the endpoint and one or more management consoles. Endpoint agents are designed per operating system, such as Microsoft Windows versions 7, 8, 10; Mac OSX; the various flavors of Linux, Virtual Desktops, and mobile devices. Management consoles are used by administrators to deploy, monitor, activate/deactivate certain features, push updates, review status, and start investigations. Management consoles for on-premises deployment are usually Windows Server based. Many vendors now offer management consoles in their proprietary clouds as SaaS. Licensing is generally per managed node.

1.3 Required Capabilities

Various technologies support all the different requirements customers are facing today. The requirements are

- Detect and prevent infection by
  - Viruses
  - Worms
  - Polymorphic malware
  - Botnet malware
  - Ransomware
  - JIT/File-less malware
  - Rootkits
  - Unknown types of malware / Zero-day exploits
- Remove infections if discovered
- Agents self-protect by process obfuscation, kernel mode driver implementation
- Agents operate autonomously if disconnected from network
- Report telemetry to management console and SIEM or other security intelligence systems
- Deployment options for management console: On-premises or cloud.
- Multi-factor authentication for management console administrators: SmartCards, tokens, OTP, Biometrics, Mobile apps, etc.
- Delegated and role-based administration
- Activity dashboards and customizable reporting

Many organizations are feeling and responding to the pressure to provide a more robust defense against an increasing number of malware attacks, particularly ransomware. The criteria evaluated in this Leadership Compass reflect the varieties of use cases, experiences, business rules, and technical capabilities required by KuppingerCole clients today, and what we anticipate clients will need in the future. The products examined meet many of the requirements described above, although they sometimes take different approaches in solving the business problems.

When evaluating these products and services, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- core features of Anti-Malware technology

We considered a series of specific features. These functional areas, which are reflected in the spider charts for each company in Chapter 5 include:

Enterprise	TheThe ability to ability to deploy, update, assign policies, and collect telemetry from all nodes in an organization constitutes enterprise management. This also distinguishes enterprise solutions from consumer-grade solutions. Organizations need to be able to remotely deploy endpoint anti-malware agents, push updates, and define groups of nodes and apply different protection policies per group. Administrators also need to be able to collect information from covered nodes automatically. Typically, solutions in the space provide dashboards and reports for Security Operations Center (SOC) personnel. The best products have full integration with in-suite patch management, fully automated Endpoint Detection/Response (EDR), SIEM, and investigative analysis tools.
Admin Security	Admin security encompasses two primary factors: authentication options for administrators and authorization models. Given the sensitivity and importance of enterprise anti-malware admin consoles, we believe that they should be protected by strong authentication methods, such as Smart Cards, USB keys, mobile out-of-band apps, or federated via SAML. Enterprise anti-malware solutions should also support role-based or delegated access controls, so that large organizations can delegate areas of responsibility to appropriate personnel without giving them more control than necessary to do their jobs.
Test Results	Consolidation and analysis of multiple, independent anti-malware testing programs. Detection rates, false positive rates, and successful removal rates are considered here. Rates for effectiveness may vary widely between when agents can or cannot connect to their vendor's cloud analytics services. Most threats are present while users are online, but simply being internet-connected is not enough to increase protection via the anti-malware solution: because there are occasions when malicious actors block access to security vendors' services over public Wi-Fi. It is important to note that not all vendors submit their products for independent testing. Participation is key: not participating leaves a low or zero score.
Pre-execution analysis	Examination of files and code prior to runtime execution using machine learning techniques. Scanner looks for potential malware based on known patterns of typical malware behavior, including specific API calls, memory allocation, testing for anti-malware, testing to determine if it is in a sandbox or virtual machine, etc.

Runtime analysis	Includes several technical components, including sandboxing, micro-virtualization, and memory analysis. Sandboxing is a malware detection technique that executes possible malware in a somewhat isolated environment to examine what its effects are and to determine whether or not the subject code is malicious. Sandboxes can be as simple as separate browser tabs, separate memory spaces governed by distinct threads or processes, or in many cases today, remotely "in the cloud" in the vendor's environment. Sandboxes should emulate many environments or features within computing infrastructures, such as common software, browsers, and "the Internet" (providing expected feedback to the suspected malware as if it is on the Internet, contacting its command and control servers). Micro-virtualization: Malware detection technique that executes possible malware in a virtual machine instance for greater containment. This technique is generally a more secure method, but can result in usability concerns for users who need to download or upload content. Memory analysis looks for patterns and attack signatures in memory, particularly for those function call sequences that may have no corresponding file or disk image. File-less Malware Detection requires runtime analysis. File-less malware, code or scripts, can be injected into RAM from compromised sites unbeknownst to the user. Governments and companies in the finance industry have been primary targets of this type of attack. This malware can use tools such as PowerShell, SC, and netsh to assemble additional functions, modify registry entries, move laterally around a network, and capture and transmit data, all without being written as a file on a hard drive. This method evades all signature-based scanners, and can only be detected by comprehensive runtime analysis: looking for memory-resident only code executing that hasn't been loaded from disk image, code that attempts to inject other processes, and potential exfiltration attempts. In addition to detection, limiting the use of admin privileges helps thwart this technique. Other runtime techniques involve looking for known exploit patterns and process injection attempts.
Ransomware	TheThe most prevalent forms of ransomware today encrypt users' files. most prevalent forms of ransomware today encrypt users' files. Most anti-malware programs use a number of different functions to detect, shut down, and in some cases, roll back changes made by ransomware. By monitoring for suspicious-looking calls to cryptographic functions via native APIs or in third-party libraries, security programs can interrupt potential ransomware attacks. For ransomware variants that bring their

	own crypto, other detection methods are needed, such as File System Monitoring. Ransomware generates a large number of predictable read, copy-on-write (COW), and/or filename extension change requests on the filesystem. For example, many ransomware packages will attempt to read, encrypt, and rename every file in the "\MyDocuments" folder. Most ransomware starts by enumerating all files of a certain type, such as .docx, .jpg, .mp3, etc. Anti-malware agents can monitor for these types of actions and shut down the offending process to lessen the damage, even for unknown ransomware variants. Almost all ransomware types also attempt to delete the volume shadow copy of data files from the users' hard drives. These are essentially backup copies of user data. If the user could simply restore these, there would be no need to pay the ransom. However, there is no reason a user or program should ever attempt to quietly delete the volume shadow copy, so anti-malware programs also look for programmatic calls to delete it and terminate the request.
Rootkit	RootkitsRootkits are low-level programs, usually implemented like device drivers, that can take over a system surreptitiously and allow the bad actor complete control over it. Rootkits can be used for keylogging, collecting user data and credentials, or for botnet activities. To protect against rootkits, anti-malware agents are usually implemented at the kernel level, mediating which device driver are low-level programs, usually implemented like device drivers, that can take over a system surreptitiously and allow the bad actor complete control over it. Rootkits can be used for keylogging, collecting user data and credentials, or for botnet activities. To protect against rootkits, anti-malware agents are usually implemented at the kernel level, mediating which device drivers load and when.
Node OS	supportThis is a measure of the variety of node operating systems supported. We consider Windows 10, 8, 7, Vista, XP, and Windows Server versions; Mac OSX, Debian, Red Hat, and SuSe Linux.

We believe that the use of multiple detection, prevention, and removal techniques increases the likelihood of malware detection, overall effectiveness and efficiency of the solution. For example, there is still value in signature-based scanning, though it is not effective at picking up polymorphic or other advanced malware types, as it usually less CPU intensive and can still detect certain types of threats.

Each of the categories above will be considered in the product evaluations below. We've also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market.

Please note that we only listed major features, but also considered other capabilities as well when evaluating and rating the various endpoint anti-malware products.

2 Leadership

Selecting a vendor of a product or service must not be only based on the comparison provided by a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

Figure 1: The Overall Leadership rating for the Endpoint Anti-Malware market segment

Several companies topped the Leader section. McAfee leads the field, showing strong ratings in all Leadership categories.

Kaspersky Lab, Symantec, ESET, and F-Secure also appear in the top of the spectrum. Each company has decades of experience fighting malware for their customers, bringing innovation where needed, and capturing a significant customer base. Microsoft also appears in the Overall Leader segment due to the strength of their Defender anti-malware product on Windows 10.

In the Challenger segment, Bitdefender, and Sentinel One approach the boundary of Overall Leaders. These companies have pursued somewhat different technical trajectories, as will be detailed below. In this side of the Challenger block we see companies with innovative features and growing market share. Next up, Carbon Black and Sophos are at the center of the Challenger area. Carbon Black brings full-fledged EDR to bear, and Sophos is integrating the recent Invincea acquisition. Digital Guardian also made it into the Challenger section.

Overall Leaders are (in alphabetical order):

- ESET
- F-Secure
- Kaspersky
- McAfee
- Microsoft
- Symantec

2.2 Product Leadership

Product Leadership is the first specific category examined below. This view is based on the analysis of the completeness and quality of the product/service features.

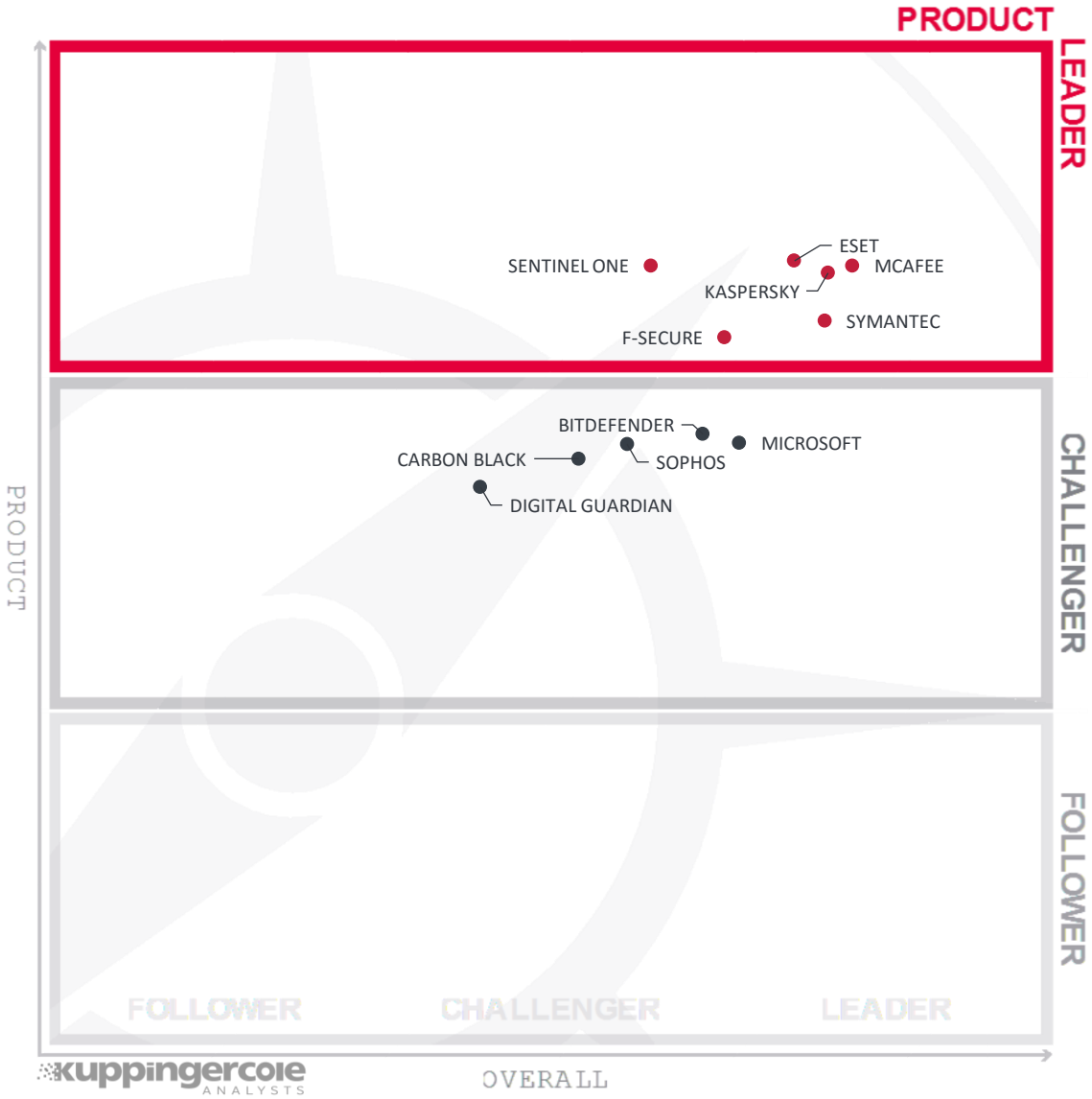


Figure 2: Product leaders in the Endpoint Anti-Malware market segment

Product Leadership, or in some cases Service Leadership, is where we examine the functional strength and completeness of products. McAfee is in front, with their comprehensive anti-malware solution addressing a wide range of Endpoint Anti-Malware business requirements, including strong authentication for administrators. They are closely followed by Kaspersky. Though Kaspersky doesn't currently have strong admin authentication, it is on their roadmap for 2018. Symantec, ESET, F-Secure, and Sentinel One also place very highly in Product Leadership. Each of these offers strong anti-malware

capabilities in each of the defined areas, plus offers strong admin authentication, security infrastructure integration, and excellent reporting.

In the Challenger section, we see a close clustering of vendors near the top of the range, including (in alphabetical order) Bitdefender, Carbon Black, Digital Guardian, Microsoft, and Sophos. All of them have their specific strengths, but commonly lack some features we expect to see. In almost all independently tested cases, each is highly effective.

Product Leaders (in alphabetical order):

- ESET
- F-Secure
- Kaspersky
- McAfee
- Sentinel One
- Symantec

2.3 Innovation Leadership

Next, we examine **Innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation in anti-malware means:

- Developing new techniques to detect and remove every-increasingly sophisticated malware
- Presenting a wide array of detection and removal methods, rather than relying on a single technology
- Integrating with patch management, EDR, SIEM, and investigative tools
- Creating, consuming, and sharing cyber threat intelligence research, including IOCs in standard formats such as STIX, TAXII, CyBox, or OpenIOC
- Protecting the endpoint security system itself, as in requiring strong admin authentication and role-based / delegated authorization.

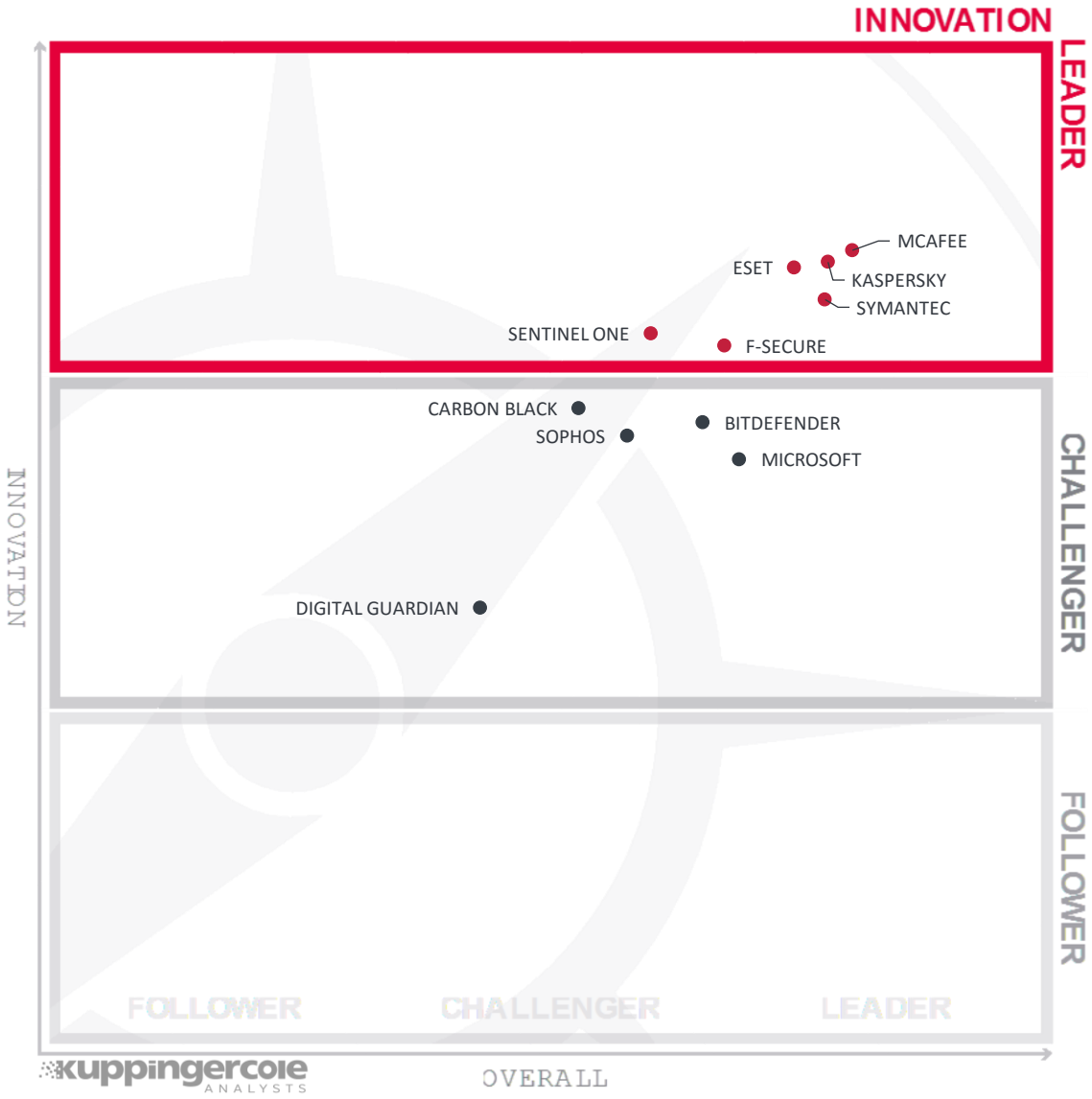


Figure 3: Innovation leaders in the Endpoint Anti-Malware market segment

When looking at Innovation Leadership, McAfee is slightly ahead of all others, based on the product's advanced malware and ransomware detection functions, multifactor authentication options, and integration with the McAfee Global Threat Intelligence network. Kaspersky is next, also with comparably strong malware and ransomware detection capabilities, and excellent history of publishing leading edge security research. ESET, with excellent rootkit detection; F-Secure with comprehensive Mac OS support via XFENCE; Symantec, with configurable anomaly sensitivity; and Sentinel One, featuring SAML authentication and STIX/OpenIOC standards support, finish out the Innovation Leaders.

In the Challenger segment, we find Carbon Black at the top of the range, nearly a Leader. Carbon Black's continuous risk evaluation and trust learning model give it an edge. In the remainder of the Challenger block, in alphabetical order, we find Bitdefender, Digital Guardian, Microsoft, and Sophos. Each product is

progressing along its own feature roadmap, in response to evolving threats and customer requests, particularly in terms of enterprise management.

Innovation Leaders (in alphabetical order):

- ESET
- F-Secure
- Kaspersky
- McAfee
- Sentinel One
- Symantec

2.4 Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

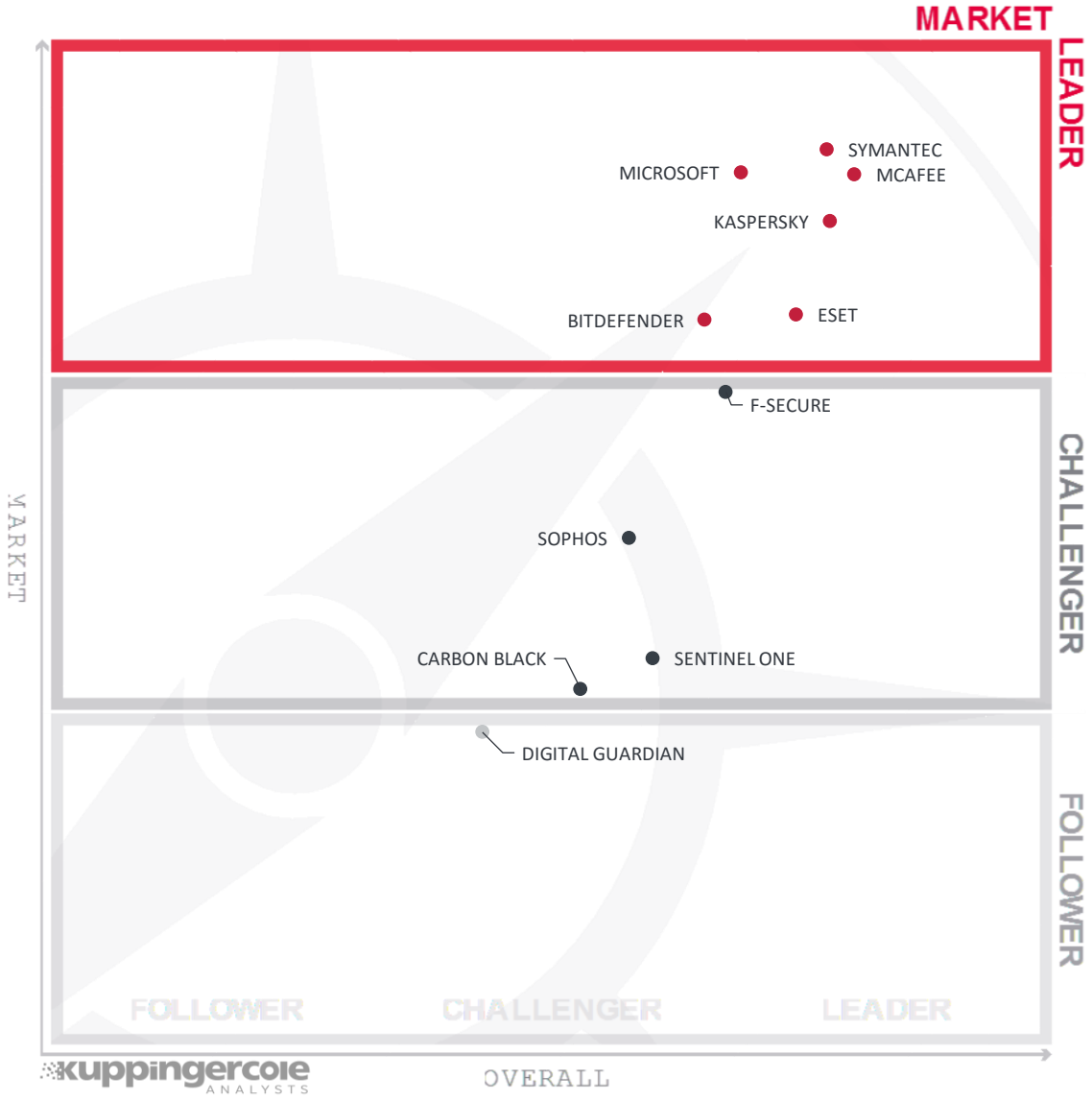


Figure 4: Market leaders in the Endpoint Anti-Malware market segment

Bitdefender, ESET, Kaspersky, McAfee, Microsoft, and Symantec share the top spots for Market Leadership. All Windows systems ship with Microsoft security tools, so it is not surprising to find them at the high point for Market Leadership. McAfee and Symantec are well-known security suite vendors that have been providing antivirus services for customers for decades. Kaspersky and Bitdefender also

command significant market share, protecting hundreds of millions of endpoints around the world. Rapid, global growth on top of a large customer base puts ESET into the Market Leader section also.

F-Secure is the top market Challengers. F-Secure has captured large numbers of customers, and has a very good support ecosystem. Sentinel One, and Sophos complete the Challenger section of the Market Leadership.

Finally, we see Carbon Black and Digital Guardian in the Followers section. Carbon Black and Digital Guardian have good North American market penetration, and are looking to expand.

Market Leaders (in alphabetical order):

- Bitdefender
- ESET
- Kaspersky
- McAfee
- Microsoft
- Symantec

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership

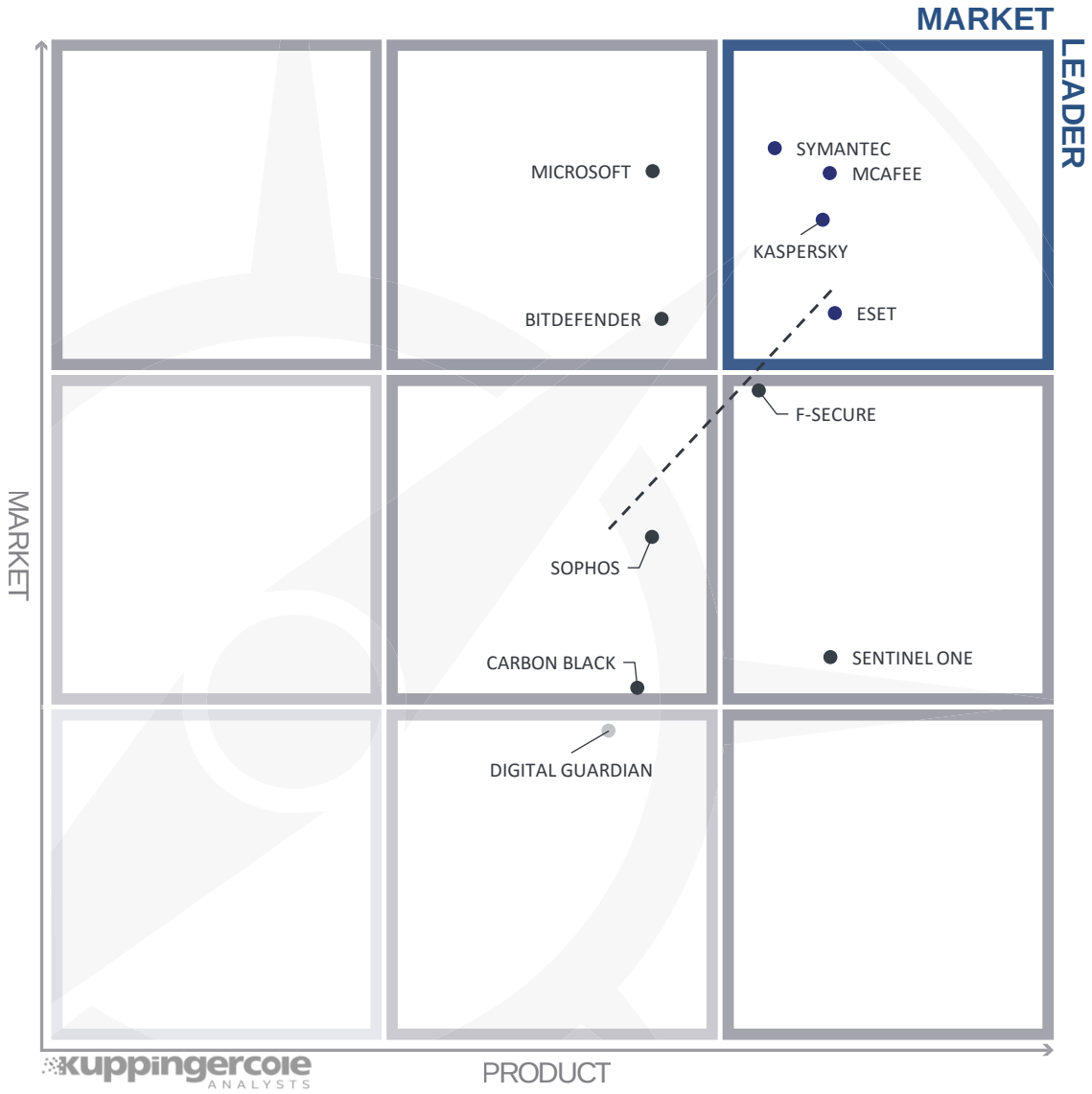


Figure 5: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. It is rational that these are mainly the very large vendors, while vendors below the line frequently are innovative but focused on specific regions.

The matrix shows a picture that is typical for evolving market segments, with a rather broad distribution of the various players across the quadrants and a weak correlation between Market Leadership and Product Leadership.

In the upper right box, we find ESET, Kaspersky, McAfee, and Symantec. These vendors are leading in both the product and market ratings.

Below these, we find F-Secure and Sentinel One, which are product leaders but not (yet) in the Market Leader's segment. The strong feature set indicates good growth potential.

On the other hand, in the center top box, we see Bitdefender and Microsoft, both having a significant market share while not being counted amongst the Product Leaders.

In the center of the graphic, we find CarbonBlack and Sophos just below the line. This is a respectable position in both the Product Leadership and Market Leadership ratings and thus are interesting options to the leading vendors.

Digital Guardian is right below the center square, having a smaller market share.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with few exceptions. This distribution and correlation is mostly constrained to the line, with a significant number of established vendors plus some smaller vendors.

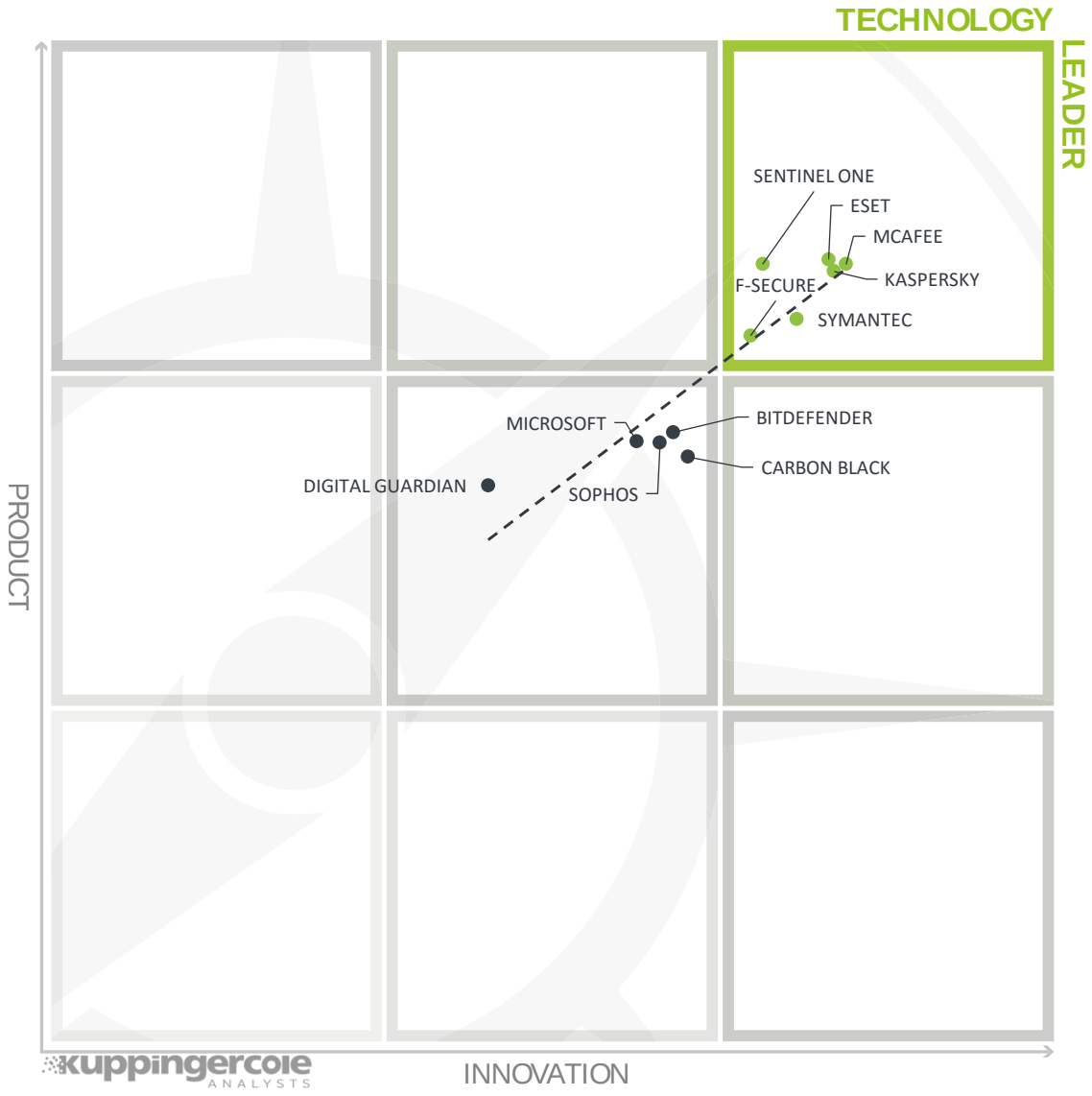


Figure 6: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

This chart shows a quite interesting picture. Most vendors are near the line, showing a balanced ratio of product capabilities and innovation. This also demonstrates that innovation is market driven. ESET, F-Secure, Kaspersky, McAfee, Sentinel One, and Symantec are the Technology Leaders, with many advanced features in line with what customers need.

The spaces below and to the left of technology leaders are empty. In the central square, we find Bitdefender, Carbon Black, Digital Guardian, Microsoft, and Sophos with strong products containing many innovative features.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, they might also fail, especially in the case of smaller vendors.

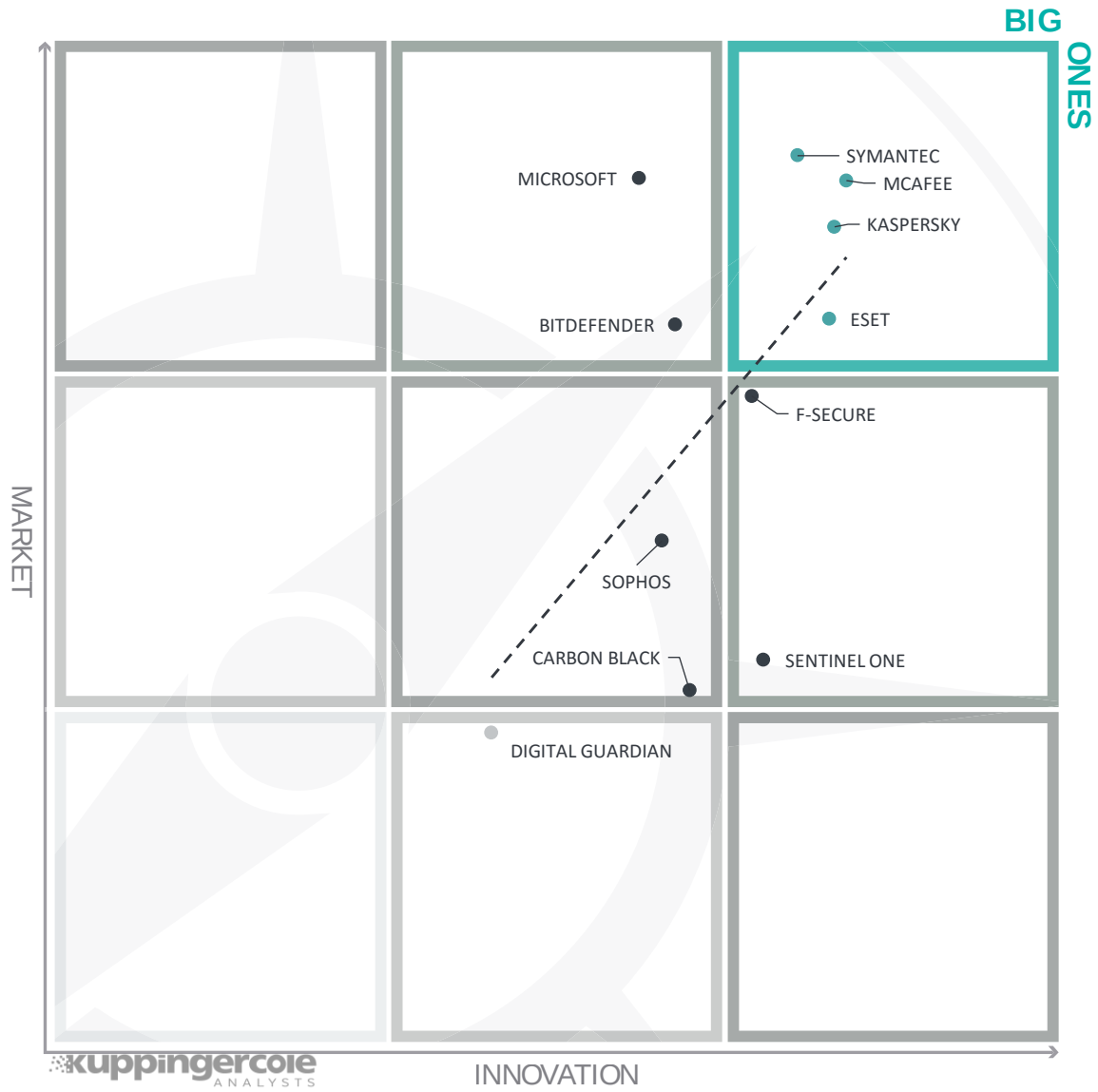


Figure 7: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating; while vendors below the line show an ability to innovate, and thus the biggest potential for improving their market position.

ESET, Kaspersky, McAfee, and Symantec occupy the top right sector, having both an excellent position in the market and delivering innovative anti-malware capabilities to their customers. F-Secure, on the top of the center right, is almost a Big One. Sentinel One appears on the right side also, indicating very strong innovation, but having less market share.

Bitdefender and Microsoft are also on top of the market, and are distributed across the top center box according to their relative innovation.

Carbon Black and Sophos are in the center of the chart, with room to innovate and grow.

Digital Guardian is slightly below the center, about to move into the main sequence.

4 Products and Vendors at a glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Endpoint Anti-Malware. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

4.1 Ratings at a glance

Based on our evaluation, a comparative overview of the functional ratings of all the products covered in this document is shown in table 1.

Product	Security	Functionality	Integration	Interoperability	Usability
BITDEFENDER	positive	positive	positive	positive	positive
CARBON BLACK	positive	positive	positive	strong positive	positive
DIGITAL GUARDIAN	positive	neutral	positive	strong positive	positive
ESET	positive	strong positive	strong positive	positive	strong positive
F-SECURE	positive	strong positive	strong positive	positive	positive
KASPERSKY	positive	strong positive	strong positive	positive	strong positive
MCAFEE	strong positive	strong positive	strong positive	positive	strong positive
MICROSOFT	strong positive	positive	strong positive	neutral	positive
SENTINEL ONE	strong positive	positive	strong positive	strong positive	positive
SOPHOS	neutral	positive	positive	strong positive	positive
SYMANTEC	positive	positive	strong positive	positive	strong positive

Table 1: Comparative overview of the functional ratings for the product capabilities

Furthermore, table 2 shows an overview which contains four additional, non-functional ratings for the vendor. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
BITDEFENDER	positive	strong positive	positive	positive
CARBON BLACK	positive	weak	weak	neutral
DIGITAL GUARDIAN	neutral	weak	weak	neutral
ESET	strong positive	strong positive	positive	positive
F-SECURE	positive	positive	positive	positive
KASPERSKY	strong positive	strong positive	strong positive	strong positive
MCAFEE	strong positive	strong positive	strong positive	strong positive
MICROSOFT	positive	strong positive	strong positive	strong positive
SENTINEL ONE	strong positive	weak	neutral	neutral
SOPHOS	positive	neutral	positive	neutral
SYMANTEC	positive	strong positive	strong positive	strong positive

Table 2: Comparative overview of the non-functional ratings for vendors

5 Product/service evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

5.1 Bitdefender GravityZone

Bitdefender is a private company, and was founded in 2001 in Bucharest, Romania. The company specializes in cybersecurity technologies for Windows PCs, Macs, iOS, Android, and virtual environments. Related products in their suite handle APT protection, IaaS and SaaS security, disk encryption, application whitelisting, patch management, email system security, etc. The company reports over 500 million endpoints are covered by their anti-malware solutions.

Strengths	Challenges
• Large installed user base • Advanced hypervisor support for better malware detection and resource efficiency in virtual environments • Strong pre-execution ML engine • Free ransomware protection download	• Incompatible with some other security tools • No 2FA or MFA for administrators • No local sandbox or micro-virtualization

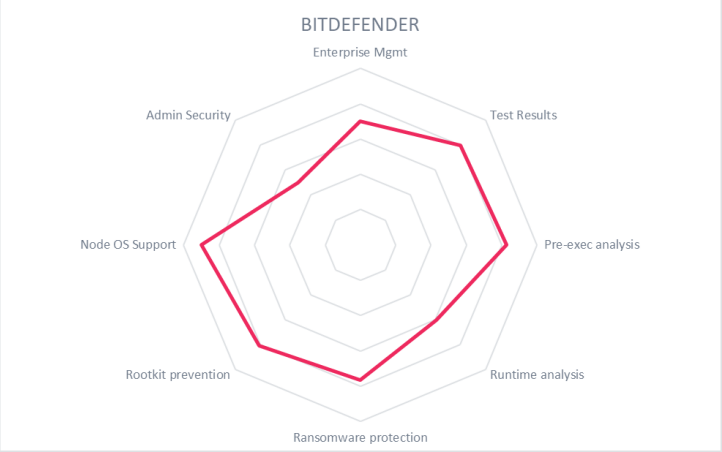
Table 3: Bitdefender's major strengths and challenges

Bitdefender uses a layered defense against malware: signature scanning; pre-execution file scanning using ML techniques such as neural net, binary decision tree, etc.; dynamic analysis at execution monitors process behavior; agent-integrated cloud sandboxing; rootkit prevention driver; and JIT/File-less malware detection capabilities. It includes also EDR capabilities, providing insights into suspicious activities to enable organizations to react quickly on emerging threats. Their Ransomware Vaccine was released last year, and stops encryption by common forms of ransomware. Bitdefender offers the Ransomware Vaccine for free on its website.

Bitdefender agents function autonomously if separated from the network. Enterprise deployments can be managed from on-premises or cloud-based consoles. The on-premise console can also be deployed as a virtual appliance. Role-based and delegated administration are possible. Strong and multi-factor authentication are not yet supported. The console can send event data via syslog with in-product filtering for SIEM integration.

Security	Positive
Functionality	Positive
Integration	Positive
Interoperability	Positive
Usability	Positive

Table 4: Bitdefender rating



Bitdefender has a large user base and good relationships with OEM vendors, and therefore have many enterprise and consumer users. The product has strong anti-malware features, and consistently performs well in independent real-world tests. The JIT/File-less malware detection feature is new and improving. Like many other solutions, it lacks strong administrative authentication. Bitdefender is a solid contender and should be considered as an enterprise endpoint security/anti-malware solution for RFPs.

5.2 Carbon Black Cb Defense

Carbon Black, was founded in the Boston area as Bit9 back in 2002. Bit9 was long known for its strong application whitelisting capabilities. Bit9 purchased Confer, an anti-malware maker, and changed their name in 2016. The venture-backed endpoint security company is reportedly moving toward IPO. Cb Defense is their cloud-delivered endpoint solution, and it contains not only anti-malware functionality, but also streaming prevention technology and robust EDR features. Carbon Black also offers Cb Protection, application control for servers; and Cb Response, threat hunting and incident response for SOC teams. Cb Defense works with Microsoft Windows and Mac machines.

Strengths	Challenges
• Some 2FA options for administrators • Interoperable with many other agent-based security tools • Advanced behavioral analysis techniques • Auto-quarantine of untrusted apps	• Coarse-grained admin model; no delegation • In-network threat intelligence only • Cloud-based console only • Cloud-based sandbox/detonation only

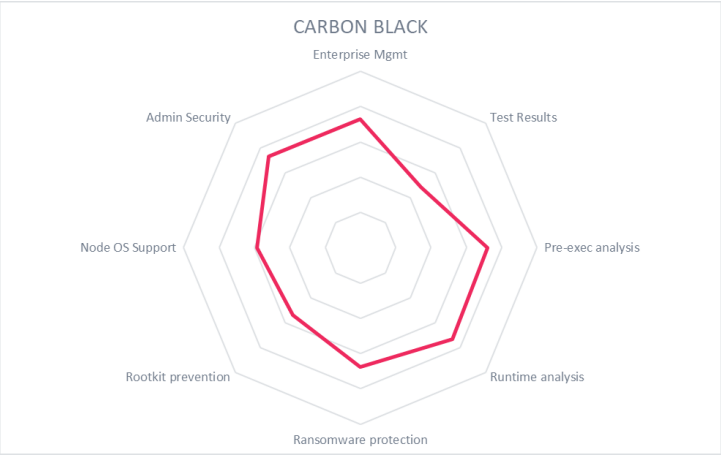
Table 5: Carbon Black's major strengths and challenges

Cb Defense employs both pre-execution and runtime malware scanning. Before execution, it performs signature-based scanning, Yara rules evaluation, and file/URL/process reputation analysis. Runtime protection is based on ongoing behavioral analysis of all running processes against historical patterns. Cb Defense constantly risk scores all activities and can terminate processes if suspicious. It can detect and prevent polymorphic, JIT, and file-less malware. New or unknown applications are quarantined automatically until they become trusted.

Carbon Black's is cloud-based only. It can send event data to SIEMs and responds to REST API queries as well. The console provides dashboard and reports. One such built-in report provides detail on sequences leading up to a potential breach including the attack chain showing techniques. The console allows admins to create device groups and apply different risk sensitivity policies per group. Carbon Black recently announced Cb Defense for VMware, which provides advanced threat prevention and detection for that virtual platform. Carbon Black supports Duo Security and Google Authenticator for mobile and stronger authentication options.

Security	Positive
Functionality	Positive
Integration	Positive
Interoperability	Strong positive
Usability	Positive

Table 6: Carbon Black's rating



Cb Defense has advanced behavioral analysis techniques which give it advantages over traditional signature-based anti-malware products. The ability to require 2FA for administrative access is a plus. The company has a smaller market share, concentrated in North America, but is growing. Carbon Black takes a different approach to anti-malware and endpoint security, and thus is worth consideration at RFP time.

5.3 Digital Guardian

Digital Guardian, based in Boston, provides a number of endpoint security solutions beyond anti-malware, including data discovery and classification, data loss prevention, and cloud data protection. Digital Guardian's anti-malware capabilities are built into their client agents, and run on Windows 10/8/7, Windows Server 2016/2012/2008, Mac OS, Red Hat, CentOS, Debian, Ubuntu, Suse Linux, and VDIs. The management console can be run either on-premises or in the cloud.

Strengths	Challenges
• Tested to work with other security agent software • Free anti-ransomware upgrade for customers • Feature parity across Mac, Windows, Linux and VDIs • Bundled DLP and EDR capabilities	• Digital Guardian does not delete/remove malware by default • Does not perform pre-execution heuristics, local sandboxing, or micro-virtualization • No recent independent test results

Table 7: Digital Guardian's major strengths and challenges

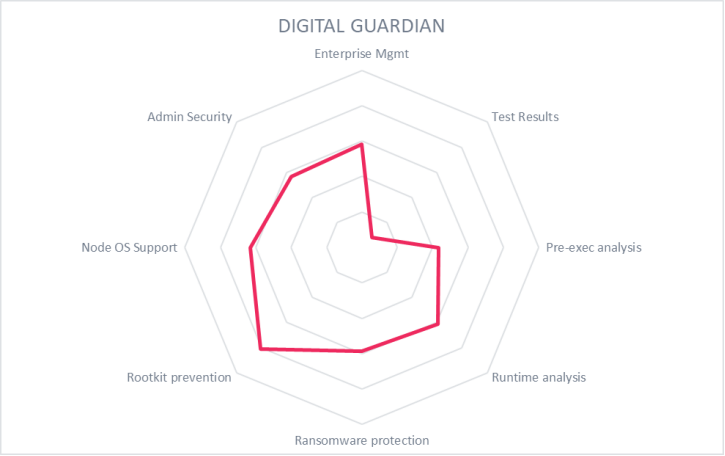
Digital Guardian deploys multiple techniques: signature-based scanning, and runtime process and memory analysis. Rule-based behavioral analysis can detect and stop file-less based attacks such as those that leverage PowerShell or WMI. Other features of its runtime analysis include monitoring process executions, DLL loads, network operations, registry modifications, etc. Digital Guardian works in conjunction with FireEye and Blue Coat (now Symantec) for network sandboxing, but does not perform endpoint sandboxing. Agent components are obfuscated for self-protection and it is implemented at kernel-level for better rootkit detection. For ransomware discovery and damage prevention, Digital Guardian monitors crypto API/library calls and attempts to change file types and extensions en masse. Although it doesn't remove malware by default, admins can configure custom remediation responses.

Digital Guardian provides advanced reporting and analytics through their SaaS or standard reports through the console and allows API access to log data as well. It can send event information over syslog for SIEM and provides connectors for ArcSight, QRadar, and Splunk. Digital Guardian supports integration of 3rd party threat intelligence feeds.

Differing levels of administrative access can be defined. The solution does allow LDAP authentication to the console; therefore Smart Card or other strong authentication mechanisms could be configured via LDAP. It is possible to use **www.authy.com** for 2FA as well, though it is not a default choice.

Security	Positive
Functionality	Neutral
Integration	Positive
Interoperability	Strong positive
Usability	Positive

Table 8: Digital Guardian rating



Digital Guardian's anti-malware features are part of an overall suite designed for data protection and general EDR. It works best as part of that solution rather than as a standalone anti-malware product.

5.4 ESET Endpoint Security

ESET, headquartered in Bratislava, was founded in 1992, and has been in the security business since. ESET covers all Windows endpoints and servers, Mac OS, all commercially supported Linux variants, mobile devices, and VDIs. The endpoints can be managed from either on-premises or cloud-based consoles. In addition to endpoint security products, ESET makes full EDR software, security for Microsoft SharePoint and a variety of email gateways.

Strengths	Challenges
• Global customer base and support ecosystem • Uses internal and external threat intelligence • 2FA for administrators is configurable • Hierarchical/ delegated administration • Local and cloud-based sandboxing • Sophisticated rootkit detector	• Some discovered malware may require specialized tools for removal, available at ESET • Not tested for compatibility with other endpoint security solutions

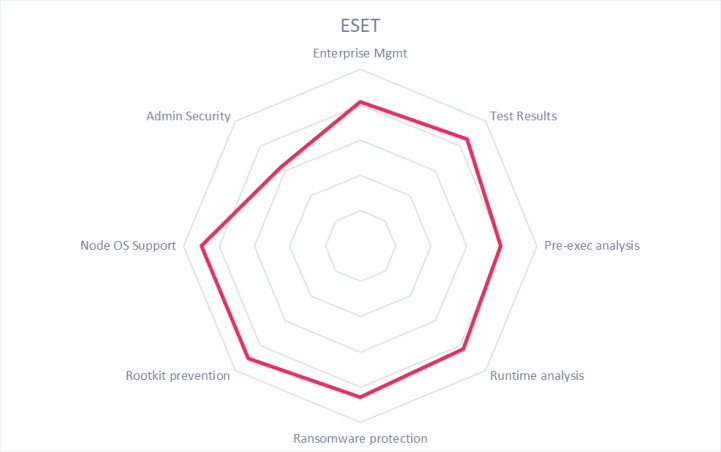
Table 9: ESET's major strengths and challenges

ESET has a multi-faceted detection regime, which includes signature-based scanning, machine learning pattern analysis prior to execution, advanced memory scanning for runtime analysis, and both cloud and local sandboxing. The sandboxing function supports browser, VM, and internet emulation. The product can detect and prevent polymorphism, JIT/File-less malware, and ransomware. ESET has a sophisticated, low-level rootkit detector that even works for Mac OS.

ESET permits 2FA for administrators either through integration with Microsoft Active Directory or via the ESET mobile app. The enterprise version supports different administrative levels and hierarchical administration. ESET console can send event data to ArcSight and QRadar or any SIEM via syslog. The console provides granular and customizable reports, plus an API for access by other analytics programs. Agents function autonomously if unable to contact the console.

Security	Positive
Functionality	Strong positive
Integration	Strong positive
Interoperability	Positive
Usability	Strong positive

Table 10: ESET's rating



ESET has strong anti-malware functionality, covering all techniques except micro-virtualization. Full EDR and HIDS/HIPS features are bundled with the product. ESET provides a large number of pre-defined reports, and more can be customized. The fact that this solution is one of the few reviewed that can support 2FA for administrators is a definite plus for internal security. The delegated administrative model is also useful for large organizations. Given the good features for both anti-malware and manageability, and the global reach of customers and support, ESET should be on the shortlist for consideration in enterprise RFPs for anti-malware solutions.

5.5 F-Secure Business Suite / Protection Service for Business

Founded in 1988 in Helsinki, F-Secure has been providing anti-virus and other security tools for nearly 3 decades. F-Secure provides support for all versions of Windows, Mac, Red Hat and Suse Linux, mobile, and VDIs. In addition to broad client support, they offer network scanning appliances, email gateways, vulnerability scanning and management products, and a managed detection and response service (Rapid Detection Service).

Strengths	Challenges
• Excellent regional/language support • Strong malware removal and quarantine capabilities • Multi-engine scanning	• Removes other anti-malware products, upcoming EDR product can co-exist • 2FA/MFA ability coming in 2018 • Strong sales in EU, growing elsewhere

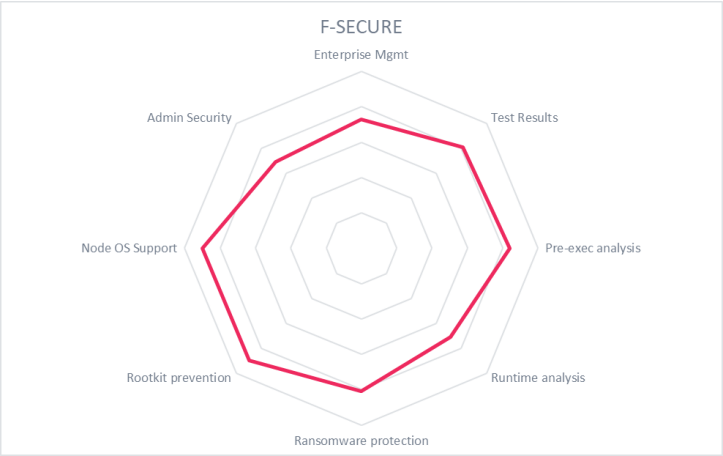
Table 11: F-Secure's major strengths and challenges

F-Secure employs 5 types of malware detection: web content, file signatures, system scanner, cloud-based sandbox, and a pre-execution heuristics scanner. Additionally, the Deep Guard heuristics scanner can monitor executables at runtime. The agents can detect and prevent polymorphic and Powershell-based JIT and File-less malware. The system scanner continuously examines memory to look for dormant malware. Kernel mode drivers in the agent can detect and remove rootkits. The solution detects and stops malware by both signature-based scans and monitoring for common ransomware techniques such as shadow file deletion. DataGuard module provides DLP-like functionality for additional layer of ransomware protection. XFENCE for Mac delivers comprehensive security for that platform, including defenses against ransomware, rootkit, and webcam/microphone snooping.

F-Secure's on-premise console supports syslog and CEF for data transfer to SIEMs. The cloud portal allows query via REST APIs. The console provides pre-defined, non-customizable reports for administrators. Agents function on their own if disconnected from the console.

Security	Positive
Functionality	Positive
Integration	Strong positive
Interoperability	Positive
Usability	Positive

Table 12: F-Secure's rating



F-Secure is well-established amongst the leading products in the Endpoint Anti-Malware market, particularly in Europe. The company is growing in other parts of the world. F-Secure is adding 2FA/MFA for the administrative console in 2018. The solution is strong in terms of malware discovery techniques and removal capabilities. This makes it worth considering when looking for Endpoint Anti-Malware solutions.

5.6 Kaspersky Lab Endpoint Security

Kaspersky Lab, headquartered in Moscow, was founded as an anti-virus company in 1997. Kaspersky Lab provides anti-malware and other security software, such as Kaspersky Anti-Targeted Attack and Industrial Control Solutions. For endpoint anti-malware, Kaspersky provides agents for all Windows endpoints and servers, Mac OS, all commercially supported Linux variants, mobile devices, and VDIs. The endpoints can be managed from either on-premises or cloud-based consoles.

Strengths	Challenges
• Global customer base and partner ecosystem • Leading cyber threat research publisher • Advanced Disinfection technology removes sophisticated malware and rootkits • Threat intelligence provider • Free anti-ransomware tool available	• 2FA/MFA not available for admins yet • Some incompatibilities with similar endpoint security tools

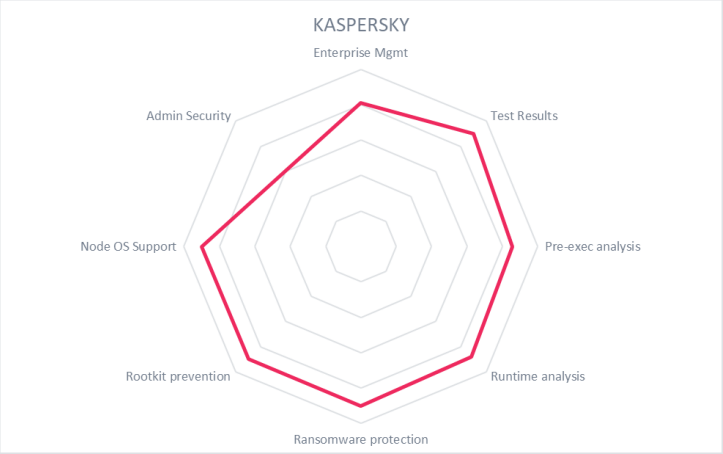
Table 13: Kaspersky's major strengths and challenges

Kaspersky's scanning engine employs multiple techniques, including signature-based scanning, pre-execution heuristics, system monitoring, real-time behavioral analysis, and sandboxing. The System Watcher function, for example, maintains lists of all process activities and evaluates them for indirect indicators of maliciousness. Kaspersky's sandboxing methods are the most complete of all compared, including VM, Browser, Internet, and Application emulation. The engine can also use micro-virtualization for the maximum separation of malware from production environments. The product can detect and prevent polymorphism, JIT and File-less malware, and ransomware. The anti-ransomware feature can roll files back to a fresh state prior to encryption attempts.

Kaspersky's endpoint security solutions support syslog for SIEM and integrate with ArcSight and QRadar. More advanced queries are possible via REST APIs. The console, though it doesn't allow 2FA/MFA yet, does permit role-based administration. The console provides up to 50 different reports and 25 different dashboard configurations for excellent visualization.

Security	Positive
Functionality	Strong positive
Integration	Strong positive
Interoperability	Positive
Usability	Strong positive

Table 14: Kaspersky's rating



Kaspersky Lab is a well-established security vendor with a wide-range of strongly integrated tools. Their anti-malware capabilities are top-notch. The solution provides detailed reports. Kaspersky Lab contributes much leading cyber threat intelligence to the research community. Adding MFA for administrators would strengthen the solution. Kaspersky Lab should be on the shortlist for endpoint anti-malware RFPs.

5.7 McAfee Endpoint Protection

Silicon Valley based McAfee was an early pioneer in the anti-virus business. McAfee was founded in 1987, acquired by Intel in 2011, then spun off from Intel in early 2017. Their endpoint protection product provides agents for all Windows endpoints and servers, Mac OS, all commercially supported Linux variants, Unix, mobile devices, and VDIs. McAfee makes a full set of related products, such as DLP, Threat Intelligence, SIEM, network and email scanners, etc. Endpoints can be managed from either on-premises or cloud-based consoles.

Strengths	Challenges
• Global customer base and partner ecosystem • Leading cyber threat research publisher • Integration with McAfee Global Threat intelligence • 2FA/MFA to console via Windows AD or SecureAuth integration • Advanced anti-ransomware detection	• May remove similar endpoint security tools • Does not use micro-virtualization for quarantining suspicious processes

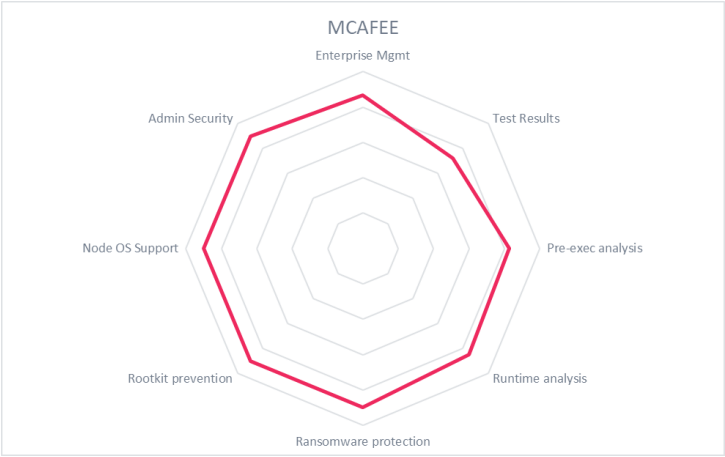
Table 15: McAfee's major strengths and challenges

McAfee's detection and prevention engine uses signature-based scanning, pre-execution heuristics, system monitoring, runtime behavioral analysis, and both local and cloud-based sandboxing. Dynamic application control (DAC), the local sandbox function, isolates untrusted apps and processes for analysis. The product can detect and prevent polymorphism, JIT and File-less malware, and ransomware. It is implemented at the kernel level to detect and remove rootkits. The "Advanced Threat Protection" module provides the anti-ransomware functions, is now enabled by default upon installation. It uses both major categories of techniques to identify potential ransomware: crypto API/library monitoring and filesystem monitoring.

McAfee's endpoint security solutions can integrate with the own SIEM, and support syslog for sending data to other SIEMs. More advanced queries are possible via REST APIs. McAfee console can be integrated with Microsoft Active Directory for administrative user authentication and authorization. McAfee has also partnered with SecureAuth for additional strong and multi-factor authentication options. The console provides dashboards for real-time visualization and a number of pre-defined yet customizable reports.

Security	Strong positive
Functionality	Strong positive
Integration	Strong positive
Interoperability	Positive
Usability	Strong positive

Table 16: McAfee's rating



McAfee is a top tier cybersecurity vendor. Their anti-malware capabilities are very strong, particularly in methods used to detect ransomware. Integration with McAfee Global Threat Intelligence is a definite plus. The ability to require strong authentication via Microsoft AD or SecureAuth is distinctive advantage. McAfee should be on the shortlist for endpoint anti-malware RFPs.

5.8 Microsoft Windows Defender

Redmond-based Microsoft began offering Defender as an anti-spyware program more than a decade ago. Defender has evolved considerably since then, becoming a full endpoint security solution working in conjunction with other security functions within the Windows operating system. For the purposes of this report, we consider Defender along with the anti-malware features components in the OS across all extant versions. Defender runs on Windows only, with standard support back to Vista and Server 2012.

Strengths	Challenges
• Large in-network threat intelligence that is shared externally • Cooperation with third-party threat intelligence providers • Administrator MFA and role-based access controls	• Versions for older operating systems are less effective • Primarily Windows coverage, though some components such as Advanced Threat Protection are available for Android, iOS, Mac, and Linux

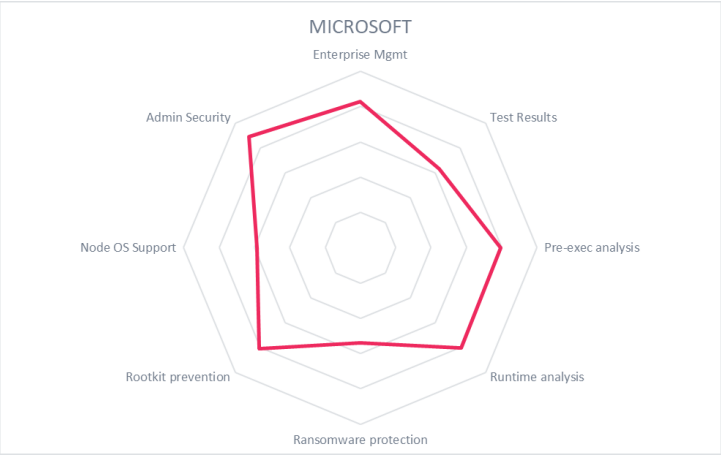
Table 17: Microsoft's major strengths and challenges

Defender uses several detection methods, including signature-based scanning, pre-execution heuristics, runtime memory analysis, local and cloud-based sandboxing. The sandbox can emulate the filesystem, full OS, browser, and applications, but not internet emulation. Windows 10 itself now provides virtualization-based security, and can create separate virtual environments for applications and system processes. Defender can detect and stop illegal cross-process injection techniques which are often used by File-less malware types. Unified Extensible Firmware Interface (UEFI) Secure Boot technology helps prevent rootkits and kernel-level malware at bootup. Defender on Windows 10 along with the Edge browser are far more effective at detecting and containing malware than previous versions.

The enterprise console supports 2FA/MFA for administrators, including Smart Cards, mobile apps, SMS OTP, etc., via Active Directory. Fine-grained access controls and delegated administration models are also possible. The console can integrate with a variety of SIEM tools. Many report are available to administrators, and more can be configured. Defender agents function autonomously outside of the home domain.

Security	Strong positive
Functionality	Positive
Integration	Strong positive
Interoperability	Neutral
Usability	Positive

Table 18: Microsoft's rating



The spider chart reflects an average of Microsoft Defender capabilities across all Windows versions from XP to 10. Pre-Windows 10 versions are not as robust. But the combination of Windows 10 OS controls, Defender, ATP, and Edge provide excellent protection against ransomware and rootkits. All Windows 10 systems have it installed by default. But many organizations run older versions of Windows. If your organization has pre-Windows 10 machines, consider the features that Defender has for each version when performing anti-malware RFPs.

5.9 Sentinel One

Sentinel One, headquartered in Mountain View, CA, is a 5-year old security startup focused on delivering tightly integrated anti-malware, EDR, and auto-remediation capabilities. The solution also includes lateral movement detection, credential theft protection, and is agnostic to the attack vector. Their platform covers all versions of Windows, all the way back to XP, Macs, Debian/Red Hat/Suse Linux, and VDIs. They offer customers a warranty in the event that any customer data is irretrievably encrypted by undetected malware. Sentinel One can be managed from either on-premises or cloud-based consoles.

Strengths	Challenges
• 2FA authentication for administrators • SAML federation for administrators • Advanced ransomware detection techniques • Ransomware prevention warranty • STIX and OpenIOC standards support	• No sandboxing or micro-virtualization • Smaller but growing presence outside of North America • No recent independent test results

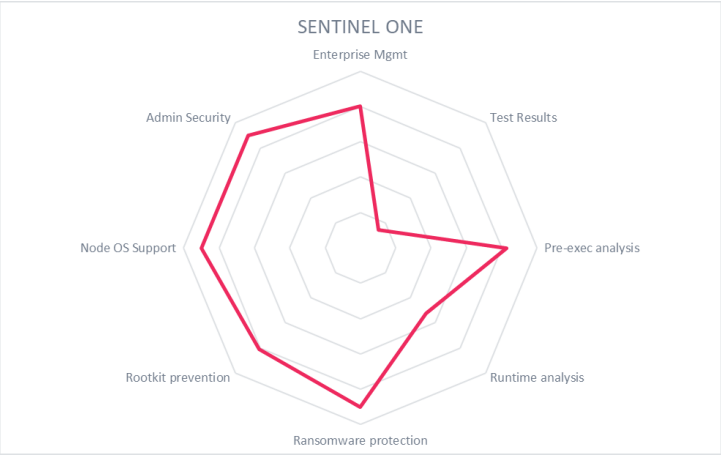
Table 19: Sentinel One's major strengths and challenges

Sentinel One uses advanced machine learning techniques for static file analysis instead of signatures. The agent monitors all processes and associated memory spaces by direct injection via asynchronous procedure calls into all running processes. This approach allows Sentinel One to detect and stop many forms of malware, including JIT/File-less and polymorphic malware. The solution does not use sandboxing for runtime evaluation or micro-virtualization for investigative isolation. The agent has a kernel-level component for detecting and blocking rootkits. To protect against ransomware, Sentinel One looks for typical ransomware methods such as large numbers of reads, copy-on-writes, mass file extension changes and deleting volume shadow copies.

Sentinel One supports CEF for communication with SIEMs. The console allows role-based administration, as well as 2FA for administrators with Duo Security or Google Authenticator. Agents function autonomously if they can't reach the cloud. The platform can receive threat intelligence in STIX and OpenIOC formats.

Security	Strong positive
Functionality	Positive
Integration	Strong positive
Interoperability	Strong positive
Usability	Positive

Table 20: Sentinel One's rating



Sentinel One has some innovative techniques in the fight against malware. The wide range of endpoints it can protect make it a good candidate for environments with a lot of variety, including older OSes. The inclusion of sandboxing or micro-virtualization strategies may make the product stronger. Sentinel One earns bonus points for allowing 2FA and SAML federation for administrator console authentication. Organizations looking for strong administrative security and advanced malware detection techniques should consider this solution.

5.10 Sophos Endpoint Protection

Sophos, headquartered in the UK, has been producing anti-virus and encryption solutions for 30 years. The Endpoint Protection product covers all versions of Windows, including back to XP on support contract, Macs, Red Hat and Suse Linux, and VDIs. They also offer email, network, and web gateways, encryption solutions, and anti-phishing testing and training software. Endpoint Protection can be managed from either on-premises or cloud-based consoles. In February 2017, Sophos acquired Invincea, another leading anti-malware company that employs non-signature machine learning methods.

Strengths	Challenges
• Strong exploit protection • Compatible with other endpoint security tools • Former Invincea integration provides "deep learning" neural net pre-execution analysis	• No 2FA/MFA for administrators yet • Some anti-malware features distributed across multiple products

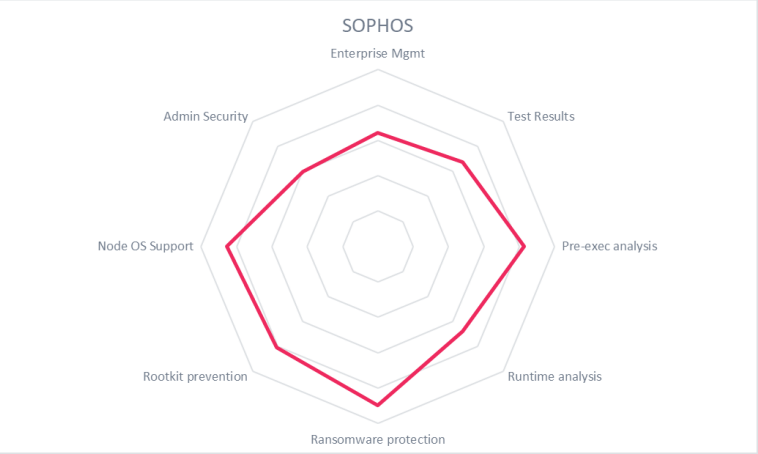
Table 21: Sophos's major strengths and challenges

Sophos uses multiple detection and prevention methods, such as signature-based scanning and runtime behavioral analysis including multi-path execution and dynamic memory analysis. The memory analysis functions can detect JIT/File-less malware. The solution does not use sandboxing for runtime evaluation or micro-virtualization for investigative isolation. Sophos Clean, a related cloud-based product, can be used to scan for and remove other malware, such as rootkits. Intercept X, a related agent-based product, can be used to detect, stop, and rollback encryption from ransomware attacks. Invincea's machine learning techniques have recently been integrated into Intercept X.

Sophos provides an API for extracting data for SIEMs. The console allows fine-grained administration, but no support for strong administrator authentication yet. Agents function autonomously if console is unreachable temporarily. The Report Manager function provides basic and configurable reports on system activities.

Security	Neutral
Functionality	Positive
Integration	Positive
Interoperability	Strong positive
Usability	Positive

Table 22: Sophos's rating



Sophos has been in the anti-malware business for a long time, and has a large, strong customer base with global support. The wide range of endpoints it can protect make it a good candidate for environments with a lot of variety, including older OSes. The anti-malware functionality is spread among several products. A unified approach would be easier for licensing and easier for customers to deploy. MFA for administrators is on the roadmap. The Invincea acquisition adds new machine-learning / pre-execution heuristics capabilities to the product. The solution is worth considering when conducting enterprise anti-malware RFPs.

5.11 Symantec Endpoint Protection

Mountain View-based Symantec provides a comprehensive set of security, management, and disaster recovery tools. The Symantec Endpoint Protection (SEP) product covers all version of Windows, Mac OS, Red Hat and Suse Linux, IaaS environments, and VDIs. Endpoints can be managed from either on-premise consoles or cloud-based consoles.

Strengths	Challenges
• Large global customer and support base • Agents for many types of endpoints • Excellent threat intelligence service integrated with SEP • Uses emulator and micro-virtualization methods	• No 2FA/MFA for administrators yet, coming in 2018 • Tighter integration across endpoint products would be helpful for enterprise administrators

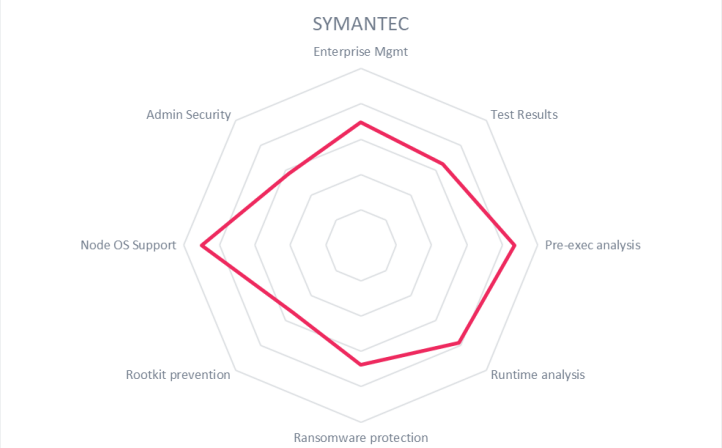
Table 23: Symantec's major strengths and challenges

Symantec utilizes several methods to detect, prevent, and remove malware: signature-based scanning, pre-execution heuristics, sandbox/environment emulator, and micro-virtualization. SEP can detect polymorphism via machine learning techniques, and uses memory analysis to thwart JIT/File-less malware. Rootkits and botnet infections can be detected by Early Launch Anti-Malware (ELAM) system, a kernel driver component that performs static analysis, behavioral analysis, and monitoring for C2 activity. Static analysis, exploit prevention, and file system monitoring are used to detect and stop ransomware. SEP is tightly integrated with Symantec forensic tools for more efficient investigations.

Symantec does not yet support 2FA/MFA for administrators, but does allow for role-based and delegated administration. Data from SEP management consoles is exportable for SIEMs and connectors are provided for ArcSight and ServiceNow. Symantec provides robust dashboard and reporting capabilities. SEP management console allows admins to configure different sensitivities for monitoring and blocking suspicious software; sensitivity levels can then be applied per AD object and/or by groups.

Security	Positive
Functionality	Positive
Integration	Strong positive
Interoperability	Positive
Usability	Strong positive

Table 24: Symantec's rating



Symantec has a long track record in the anti-virus business. They have a large set of customers and support infrastructure across the globe. While SEP is evolving to be tightly connected with the EDR functions, Symantec would benefit by better integration across their entire product suite. 2FA/MFA for administrative access is a must, and it will be coming in 2018. SEP is worth consideration for enterprise anti-malware RFPs.

6 Vendors and Market Segments to watch

Aside from the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors but do not fully fit into the market segment of Endpoint Anti-Malware or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

6.1 AVG

AVG started in the Czech Republic back in 1992. It has grown into a global anti-virus company, offering its anti-malware product in the "Freemium" model. AVG provides anti-malware products for Windows, Mac, Android, and iOS. The product also comes with a device firewall and anti-ransomware capabilities.

6.2 Avira

Avira is a German security software offering free versions of anti-malware and anti-spyware software for Windows, Mac, Android, and iOS. It uses both signatures and pre-execution heuristics to identify malware. They also have PC tune-up tools, privacy tools, and a recovery system for clean-booting PCs to remove malware from the boot sector of hard drives.

6.3 Cylance

Cylance is an anti-malware startup that has developed advanced "AI" techniques to detect and prevent malware from executing. As such, they do not use signatures, heuristics, behavioral analysis, sandboxing, or virtualization methods. The company offers agents for all Windows, Mac, and RedHat Linux machines. The agents function autonomously and do not rely on the cloud for analysis.

6.4 Darktrace

Darktrace is a cybersecurity startup that uses unsupervised "AI" techniques to learn normal behavior on an endpoint, monitor for deviations, identify malware, and prevent infection. The product, the Enterprise Immune System, is also available for industrial controls, SCADA nodes, and IoT environments. The company is positioned to serve both the IT and OT markets.

6.5 Trend Micro

Trend Micro is a major security software vendor with a suite of products encompassing endpoint, network, email, web, and IoT protection. The enterprise endpoint product uses a combination of signature-based, pre-execution heuristics, memory analysis, file reputation, and sandboxing techniques. Trend Micro declined to participate in this survey.

7 Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders in that market segment. It is the compass which assists you in identifying the vendors and products/services in a particular market segment which you should consider for product decisions.

It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

7.1 Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the Endpoint Anti-Malware market. These products deliver most of the capabilities we expect from Endpoint Anti-Malware solutions. They are mature.
- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

7.2 Product rating

KuppingerCole as an analyst company regularly does evaluations of products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

Functionality – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

Integration—integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated.

[1] http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability—interoperability also can have many meanings. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to insure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

Usability —accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided is of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

[2] http://www.kuppingercole.com/report/cb_apieconomy16122011

7.3 Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself, but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

7.4 Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

Strong	OutstandingOutstanding support for the support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.
Positive	Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.
Neutral	Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.
Weak	Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.
Critical	Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

7.5 Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC Endpoint Anti-Malware, we look at the following eight areas:

Test Results	Consolidation and analysis of multiple, independent anti-malware testing programs. Detection rates, false positive rates, and successful removal rates are considered here. Rates for effectiveness may vary widely between when agents can or cannot connect to their vendor's cloud analytics services. Most threats are while users are online, but simply being online is not enough to increase protection, because there are occasions when malicious actors block access to security vendors' services over public Wi-Fi. It is important to note that not all vendors submit their products for independent testing. Participation is key: not participating leaves a low or zero score.
Pre-execution analysis	Examination of files and code prior to runtime execution using machine learning techniques. Scanner looks for potential malware based on known patterns of typical malware behavior, including specific API calls, memory allocation, testing for anti-malware, testing to determine if it is in a sandbox or virtual machine, etc.

Runtime analysis	Includes several technical components, including sandboxing, micro-virtualization, and memory analysis. Sandboxing is a malware detection technique that executes possible malware in a somewhat isolated environment to examine what its effects are and to determine whether or not the subject code is malicious. Sandboxes can be as simple as separate browser tabs, separate memory spaces governed by distinct threads or processes, or in many cases today, remotely "in the cloud" in the vendor's environment. Sandboxes should emulate many environments or features within computing infrastructures, such as common software, browsers, and "the Internet" (providing expected feedback to the suspected malware as if it is on the Internet, contacting its command and control servers). Micro-virtualization: Malware detection technique that executes possible malware in a virtual machine instance for greater containment. This technique is generally a more secure method, but can result in usability concerns for users who need to download or upload content. Memory analysis looks for patterns and attack signatures in memory, particularly those that may have no corresponding file. File-less Malware Detection requires runtime analysis.File-less malware, code or scripts, can be injected into RAM from compromised sites unbeknownst to the user. Governments and companies in the finance industry have been primary targets of this type of attack. This malware can use tools such as PowerShell, SC, and netsh to assemble additional functions, modify registry entries, move laterally around a network, and capture and transmit data, all without being written as a file on a hard drive. This method evades all signature-based scanners, and can only be detected by comprehensive runtime analysis: looking for memory-resident only code executing that hasn't been loaded from disk image, code that attempts to inject other processes, and potential exfiltration attempts. In addition to detection, limiting the use of admin privileges helps thwart this technique. Other runtime techniques involve looking for known exploit patterns and process injection attempts.
Ransomware	TheThe most prevalent forms of ransomware today encrypt users' files. most prevalent forms of ransomware today encrypt users' files. Most anti-malware programs use a number of different functions to detect, shut down, and in some cases, roll back changes made by ransomware. By monitoring for suspicious-looking calls to cryptographic functions via native APIs or in third-party libraries, security programs can interrupt potential ransomware attacks. For ransomware variants that bring their

	own crypto, other detection methods are needed, such as File System Monitoring. Ransomware generates a large number of predictable read, copy-on-write (COW), and/or filename extension change requests on the filesystem. For example, many ransomware packages will attempt to read, encrypt, and rename every file in the "\MyDocuments" folder. Most ransomware starts by enumerating all files of a certain type, such as .docx, .jpg, .mp3, etc. Anti-malware agents can monitor for these types of actions and shut down the offending process to lessen the damage, even for unknown ransomware variants. Almost all ransomware types also attempt to delete the volume shadow copy of data files from the users' hard drives. These are essentially backup copies of user data. If the user could simply restore these, there would be no need to pay the ransom. However, there is no reason a user or program should ever attempt to quietly delete the volume shadow copy, so anti-malware programs also look for programmatic calls to delete it and terminate the request.
Rootkit	preventionRootkits are low-level programs, usually implemented like device drivers, that can take over a system surreptitiously and allow the bad actor complete control over it. Rootkits can be used for keylogging, collecting user data and credentials, or for botnet activities. To protect against rootkits, anti-malware agents are usually implemented at the kernel level, mediating which device drivers load and when.
Node OS	supportThis is a measure of the variety of node operating systems supported. We consider Windows 10, 8, 7, Vista, XP, and Windows Server versions; Mac OSX, Debian, Red Hat, and SuSe Linux.
Admin Security	Admin security encompasses two primary factors: authentication options for administrators and authorization models. Given the sensitivity and importance of enterprise anti-malware admin consoles, we believe that they should be protected by strong authentication methods, such as Smart Cards, USB keys, mobile out-of-band apps, or federated via SAML. Enterprise anti-malware solutions should also support role-based or delegated access controls, so that large organizations can delegate areas of responsibility to appropriate personnel without giving them more control than necessary to do their jobs.
Enterprise	TheThe ability to deploy, update, assign policies, and collect telemetry from all nodes in an organization constitutes enterprise management. This also distinguishes enterprise solutions from consumer-grade solutions. Organizations need to be able to remotely deploy endpoint anti-malware agents, push updates, and define groups of nodes and apply different protection policies per group. Administrators also need to be able to

collect information from covered nodes automatically. Typically, solutions in the space provide dashboards and reports for Security Operations ability to deploy, update, assign policies, and collect telemetry from all nodes in an organization constitutes enterprise management. This also distinguishes enterprise solutions from consumer-grade solutions. Organizations need to be able to remotely deploy endpoint anti-malware agents, push updates, and define groups of nodes and apply different protection policies per group. Administrators also need to be able to collect information from covered nodes automatically. Typically, solutions in the space provide dashboards and reports for Security Operations Center (SOC) personnel. The best products have full integration with in-suite patch management, fully automated Endpoint Detection/Response (EDR), SIEM, and investigative analysis tools.

We believe that the use of multiple detection, prevention, and removal techniques increases the likelihood of malware detection, overall effectiveness and efficiency of the solution. For example, there is still value in signature-based scanning, though it is not effective at picking up polymorphic or other advanced malware types, as it usually less CPU intensive and can still detect certain types of threats.

The spider graphs provide comparative information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas, while being strong in other areas. These might be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on Endpoint Anti-Malware.

7.6 Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- Lack of information supply: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.

- Borderline classification: Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their Endpoint Anti-Malware offerings in chapter Vendors *and Market Segments to watch*. In that chapter, we also look at some other interesting offerings around the Endpoint Anti-Malware market and in related market segments.

8 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com