Ovum
TMT intelligence | informa

Ovum Decision Matrix: Selecting an Endpoint Protection Solution, 2017–18

Summary

Catalyst

Organizations and the devices used to enable access to their operational systems are continually attacked by assailants, who make use of the most convenient forms of malware available to steal data and put businesses and their users at risk.

Users with access to business systems and the variety of office and mobile devices used to facilitate that access are being targeted. They are the easiest place to acquire valid credentials to launch attacks, and to hijack and infect devices to become the launchpad for infecting and taking down entire business systems.

Round-the-clock access to business systems from any available device, including corporate and privately owned (BYOD) mobiles and tablets, has helped make business systems more accessible, but has also raised the opportunities available to the malware community.

Endpoint protection platforms (EPP) are needed that can keep all types of users and devices safe. When selecting an EPP solution, organizations should consider current and future security requirements and prioritize the elements of security that are relevant to the protection of their key operational systems, data repositories, and users. This report compares the layered protection approaches available from leading EPP vendors and takes an in-depth look at the latest protection propositions from a newer generation of EPP providers.

Ovum view

The EPP market consists of an eclectic mix of traditional and next-generation protection products. This ever-increasing set of cybersecurity products/services makes it difficult for security managers to select the correct range of facilities needed to address their specific business and user protection requirements.

Despite industry claims that user behavior analytics (UBA), sometimes referred to as user and entity behavior analytics (UEBA), and endpoint detection and response (EDR) tools are capable of replacing core signature-based protection products, organizations continue to invest in a mix of established protection products as well as selected next-generations alternatives.

This belt-and-braces approach exists for several reasons, not least because organizations are not yet prepared to reduce the levels of user and device protection they have in place, and because the case for trusting next-generation alternatives in isolation has not yet been proved. The situation is not helped by a reluctance from next-generation providers to have their technology compared to traditional protection products on offer from established EPP vendors, some of which also claim to have added UBA/UEBA and EDR components to their layered protection services.

Core protection products such as antivirus (AV) clearly have their limitations in that they find a decreasing proportion of new malware. Ovum estimates that this detection figure averages out at around 30% across the industry. None of the now well-established replacements have been successful enough to directly deliver that knockout blow and change the status quo. In fact, AV remains as part of established enterprise defense-in-depth strategies to remove basic vulnerabilities, enabling the proactive alternatives to focus on detecting and dealing with more sophisticated malware.

Ovum research using information gathered for the *Enterprise Security Market Forecast Model* shows that the EPP market was worth $5bn in 2016. The 2017 figure is expected to be just above $5.3bn, and close to the $5.7bn mark by the end of 2018.

Key findings

- The EPP sector consists of a wide range of traditional and next-generation protection products and services.
- The EPP market is changing and established providers are working hard to keep up.
- Next-generation EPP providers have yet to prove they have all the answers.
- Defense in depth remains a necessity for most enterprise organizations.
- Provision of protection for all types of device and user will be a key differentiator
- Mobile and consumer protection is an under-resourced area of the EPP market
- When selecting an EPP, IT decision-makers must consider current and future business protection requirements.

Vendor solution selection

Inclusion criteria

The EPP market is in a constant state of flux. There is much unrest and disagreement between the established providers of EPP products and services and the challenger next-generation providers that want to take their place. The claims made by both sides about the completeness and relevance of their respective products and services doesn't help business decision-makers decide the best way forward. However, defense in depth remains a necessity for most small, medium, and large enterprise organizations. Ovum's inclusion criteria list for this report therefore reflects this all-encompassing position.

The report focuses on vendors that cover most of the main elements of endpoint and mobile device protection, and specifically includes vendors that provide user and device protection products and services for PCs, laptops, tablets, and smart mobile devices. This includes:

- Support for a wide range of platforms and operating systems (OSs)
- Extensive coverage of core endpoint and mobile protection products and services
- Provision of user behavior analytics (UBA/UEBA) and machine learning techniques
- The inclusion of endpoint detection and response (EDR) facilities
- Coverage of web, wireless, and virtualization requirements
- Data protection facilities that include data loss prevention (DLP) and data/file encryption
- Protection for smart mobile devices that protects all devices that have access to business systems
- The central management facilities that are needed to support all facets of endpoint and mobile device protection.

Exclusion criteria

This time around, the exclusion criteria for the report proved to be more problematic than those for inclusion. This was because many of the new generation of protection providers that have entered the EPP market were not happy competing with established players if the judging criteria included signature-based technology, which they do not use it and they would therefore automatically score zero for that whole section. As a result, we are dealing with these providers in a separate “new entrants” section of the report.

Across the whole EPP sector we found a large number vendors that focus on just one or two specific areas of protection and position themselves as best-of-breed suppliers in their areas of expertise. Again, these specialists do not offer sufficient overall coverage to be included for comparison. Vendors are therefore excluded if they:

- Only provide a narrow range of endpoint and/or mobile device protection facilities
- Do not have the capacity to deal with web-related threats and protection services
- Do not offer central device management facilities
- Do not provide sufficient mainstream platform or device coverage.

Methodology

Technology/service assessment

The technology provided by the EPP vendors included in this report comprises key protection components, plus additional products/services that have been added to their respective portfolios to keep up and deal with the ever-changing threat environment.

market The vendors included for comparison in the report were measured against the range of endpoint and mobile platforms they support, as well as their web and online protection capabilities, their ability to protect data at the endpoint and on the move between devices and the business (including the use of DLP and encryption facilities), their support for web, wireless, and virtual clients, remote device coverage, and security management capabilities. The criteria groups for technology areas analyzed are as follows:

- Endpoint platforms, operating systems, and product delivery
- Endpoint and mobile protection products/services
- User behavior analytics (UBA/UEBA) and machine learning
- Endpoint detection and response (EDR)
- Web, wireless, and virtualization
- Data protection: data loss prevention (DLP) and data/file encryption
- Protection for smart mobile devices
- Central management facilities.

Execution

In this dimension, Ovum analysts review the capability of the solution around the following key areas:

- Maturity: The stage that the product/service is currently at in the maturity lifecycle is assessed here, relating to the maturity of the overall technology/service area.

- Interoperability and innovation: In these elements, we assess how easily the solution/service can be integrated into the organization's operations, relative to the demand for integration for the project. The innovation component looks at the value an enterprise can achieve from a software/services implementation.
- Deployment: Referring to a combination of assessed criteria and points of information, Ovum analysts provide detail on various deployment issues, including time, industries, services, and support.
- Scalability: Points of information are provided to show the scalability of the solution across different scenarios.
- Enterprise fit: The alignment of the solution is assessed in this dimension.

Market impact

The global market impact of a solution is assessed in this dimension. Market impact is measured across four categories.

- Revenues and revenue growth: Each solution's global technology revenues are measured and scored against a scale that reflects the maturity of the EPP market. This measure is repeated for revenue growth figures and an average score for the two components is calculated.
- Geographical penetration: Ovum determines each solution's revenues across the Americas; Europe, the Middle East, and Africa (EMEA); and Asia-Pacific (APAC). These revenues are calculated as a percentage of the vendor’s total sales figures and the scores reflect its overall geographical reach.
- Vertical penetration: Ovum reviews each vendor’s revenues in the following verticals: energy and utilities; financial services; healthcare; life sciences; manufacturing; media and entertainment; professional services; public sector; retail; wholesale and distribution; telecommunications; and travel, transportation, logistics, and hospitality. These revenues generate a presence score for each vertical and from these a vertical penetration score is calculated.
- Size-band coverage: Ovum determines each solution's presence in four company size bands: Global enterprises (more than 100,000 employees), Large enterprises (10,000 to 100,000 employees) medium-sized enterprises (1,000 to 9,999 employees), and small businesses (fewer than 1,000 employees). The vendor numbers are calculated as a percentage of overall sales to determine size-band coverage.

Ovum ratings

- **Market leader:** This category represents the leading solutions that we believe are worthy of a place on most technology selection shortlists. The vendor has established a commanding market position with a product that is widely accepted as best of breed.
- **Market challenger:** The solutions in this category have a good market positioning and are selling and marketing the product well. The products offer competitive functionality and good price-performance proposition, and should be considered as part of the technology selection.

Market and solution analysis

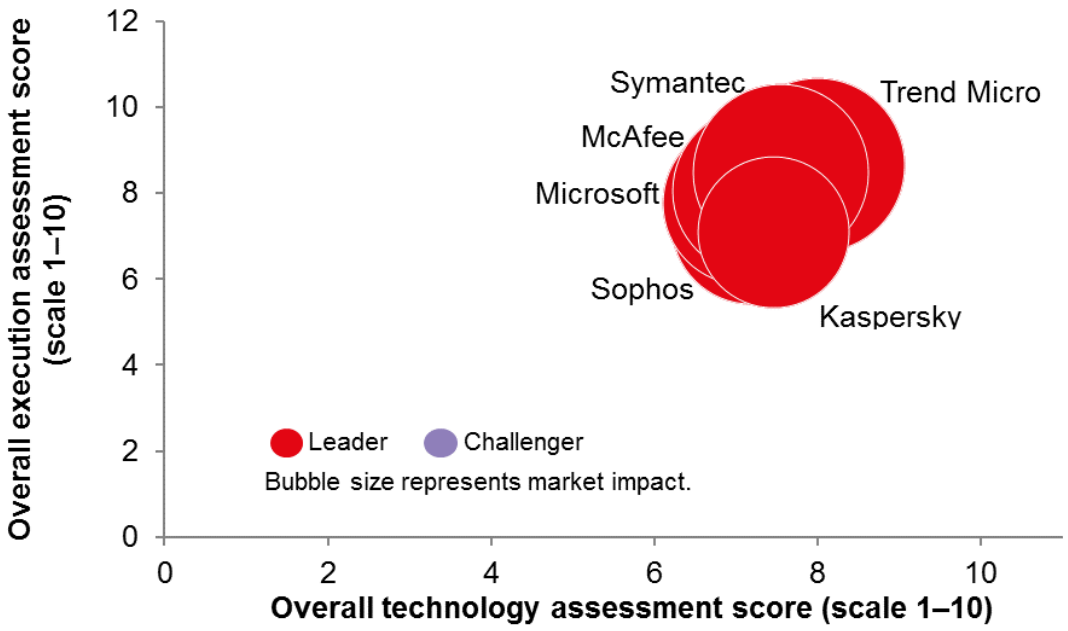
Ovum Decision Matrix: Endpoint Protection 2017–18

The need to continually improve endpoint and mobile device protection is forced on the industry by the constantly changing threat environment, and at the same time by the ever-increasing number and range of users and devices that demand connectivity to business systems. We are long past the time when it was possible to focus protection on company-owned PCs, laptops, and mobile devices. Endpoint protection must deal with every company and privately owned device that has access requirements. This includes users that own and use multiple devices and can regularly choose to use a different device depending on where they are working and the type of business access they need.

Many of the static PC and server requirements of endpoint protection remain, but endpoint security needs to be enhanced to deal with advanced threats and malware strains that can remain undetected for extended periods of time. Because of the huge number of users and devices involved and the range of threats that must be addressed, what is needed is a multilayered, defense-in-depth approach that can deal with all types of attack.

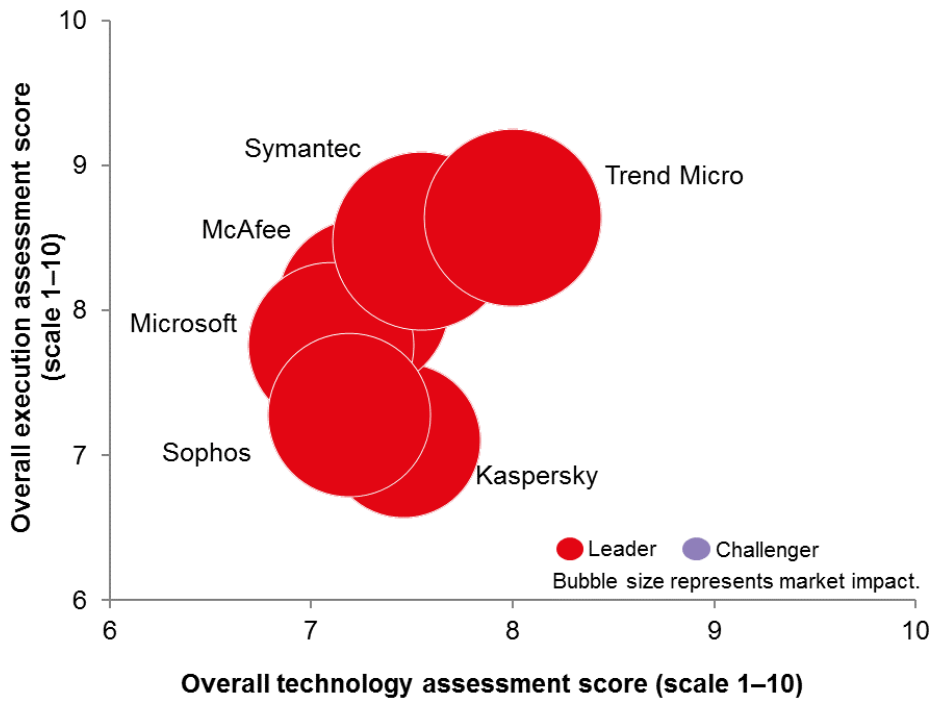
Developments within the sector demand that next-generation threat-protection techniques such as UBA/UEBA-based analytics, behavior monitoring, EDR-based detection and response, and sandboxing capabilities are part of the overall protection strategies on offer. However, no single technique used in isolation can be relied on to protect against every threat. Consolidating UBA/UEBA, EDR, monitoring, sandboxing and other next-generation techniques within a layered protection strategy therefore continues to offer the completeness of approach most businesses are looking for.

Figure 1: Ovum Decision Matrix: Endpoint Protection 2017–18



Source: Ovum

Figure 2: Expanded view of Ovum Decision Matrix: Endpoint Protection 2017–18



Source: Ovum

Table 1: Ovum Decision Matrix: Endpoint Protection 2017–18

Market leaders	Market challengers	Market challengers (continued)
Kaspersky	Bromium	FireEye
McAfee	Carbon Black	Malwarebytes
Microsoft	Comodo	Minerva Labs
Sophos	Crowdstrike	Palo Alto Networks
Symantec	Cybereason	SentinelOne
Trend Micro	Cylance	

Source: Ovum

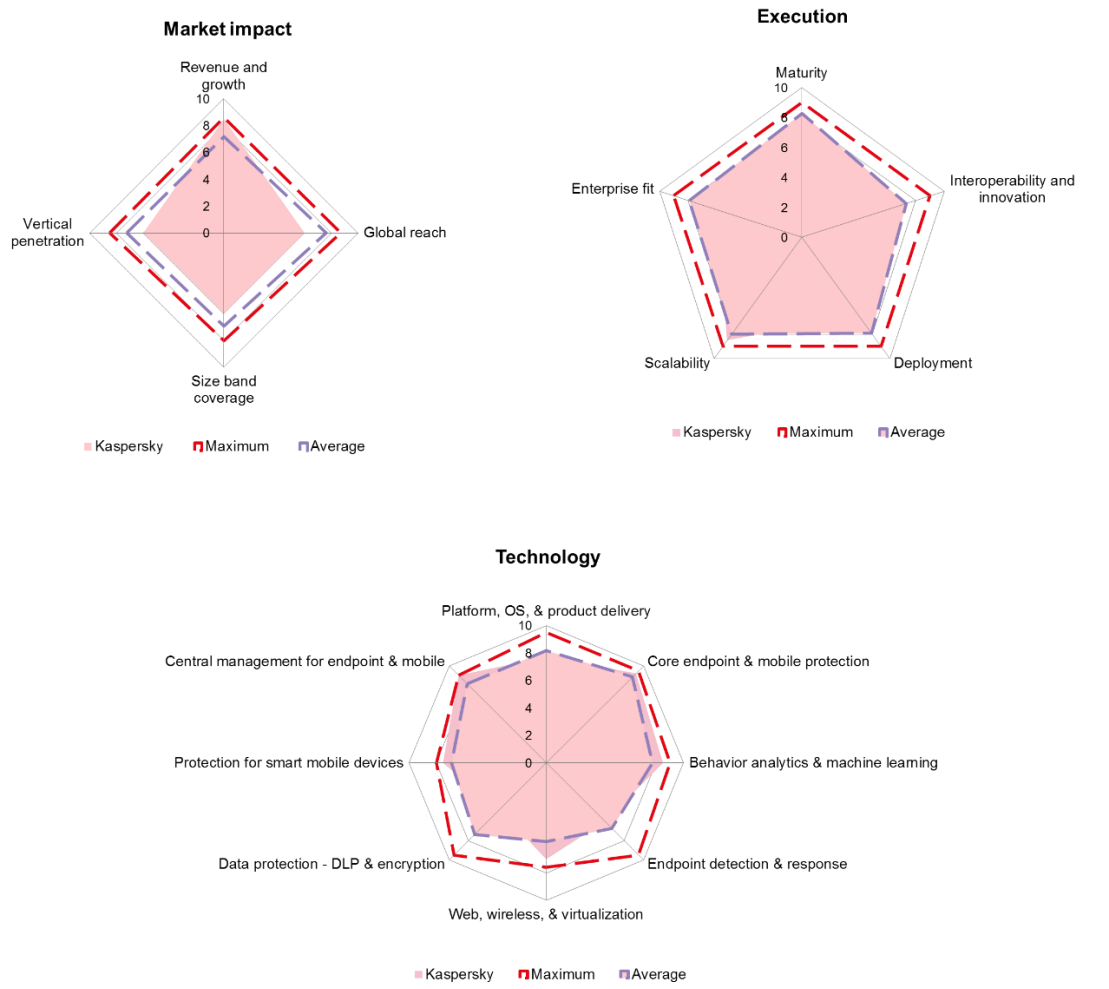
Market leaders: vendor solutions

Many established and newer next-generation vendors are competing to provide endpoint and mobile device protection products/services. There are, however, only a small number that can offer the full layered, defense-in-depth solutions that most business organizations continue to want to use. All market-leading vendors included in this Ovum report provide most of the key areas of endpoint security that Ovum has identified. Kaspersky, McAfee, Microsoft, Sophos, Symantec, and Trend Micro all offer this level of cover, and although none can claim to provide a full and complete protection service, their layered defense approaches come closer than most, and that is the main reason for including these vendors in the market leaders category.

Kaspersky: Despite the recent US government ban on federal agencies using its products, Kaspersky Endpoint Security for Business (KESB) provides enterprise-level EPP that consists of multiple layers of technology. These include traditional, signature-based approaches and technologies such as machine learning (ML) and behavioral analysis, which enable it to address the increasing amount of malware that evades signatures.

Kaspersky Endpoint Security (KES) (Ovum recommendation: Leader)

Figure 6: Kaspersky Endpoint Security (KES) radar diagrams



Source: Ovum

Ovum SWOT assessment

Strengths

KES is a mature endpoint security product

KES is on its 10th edition, making it a well-known and mature product in its market segment. While it started life in the signature-based world, it comes from signature-based beginnings, but Kaspersky Lab has expanded it significantly in recent years, moving to multilayered protection with machine-learning capabilities and behavioral analysis and pure signature-based technologies have not been

used in its products for many years. The new techniques it has adopted enable it to address the kind of malware that routinely evades signatures and other types of security products that rely on a single technological approach.

Kaspersky Lab is a major security brand

Kaspersky Lab is an established name in security. The company dates back 20 years in the consumer market. In addition, it supplied its antivirus software to several unified threat management (UTM) appliance vendors in the 2000s, which helped its brand recognition in the business market. Its enterprise offerings got underway in 2012, and it is now also a recognized vendor in this segment.

The company's GReAT researchers were instrumental in the public disclosure of the Stuxnet industrial cyber-weapon in 2015.

Opportunities

Office 365 support will expand the appeal of KES

Kaspersky Lab's plans to add support later this year for cloud environments such as AWS, and through virtual machine extensions, Microsoft Azure, as well as Office 365 via API, will increase KES's relevance in the next phase of workplace evolution.

EPP demand is solid

Ovum expects the endpoint protection market to reach $3.2bn this year and expand to $4.3bn by 2021, thanks to technology trends such as remote working and cloud, and security trends such as phishing and ransomware. KES clearly has opportunities to expand in its target market of large enterprises, and the availability of a multitenanted cloud-based version since 2016 means the company can now address a wider range of customers, leveraging MSSP partners.

Kaspersky Lab can grow as competitors struggle

Two of Kaspersky Lab's largest competitors in endpoint protection have recently experienced issues with their image, due to instability at the executive level (in the case of Symantec) and problems with the brand itself (in the case of McAfee). Although these difficulties appear to be largely over, Kaspersky Lab can capitalize on any ongoing doubt about its competitors to further its own cause.

Appendix

Further reading

2018 Trends to Watch: IT and Cybersecurity, IT0022-001074 (September 2017)

" *Software Market Forecast and Vendor Rankings: Security Software, 2016–21*" EI0025-000030 (May 2017)

Authors

Andrew Kellett, Principal Analyst, Infrastructure Solutions

Andrew.kellett@ovum.com

Rik Turner, Principal Analyst, Infrastructure Solutions

Rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo