IDC EMEA, 389 Chiswick High Road, London, W4 4AE, U.K. Tel.+44.20.8987.7100 www.idc.com

COMPETITIVE ANALYSIS

# IDC MarketScape: Western European Enterprise Endpoint Security 2012 Vendor Analysis

Kevin Bailey

## IDC OPINION

The endpoint security market is a submarket of the secure content and threat management (SCTM) functional market defined in *IDC's Software Taxonomy for 2012* (IDC #235401, June 2012). It remains very relevant and continues to grow because the technology behind it doesn't remain static. Vendors are using technologies such as reputation services, cloud-based scanning, and white listing to keep current with improvements in attacker capabilities. However, from a Western European perspective, this has been tempered by the economic challenges still affecting the region. This IDC study presents a vendor assessment model called an IDC MarketScape. Key findings include:

- IDC's analysis of this market's dynamic indicates that growth in Western Europe is driven by a mixture of increased attacks against the growing plethora of devices (mobile, BYOD, consumerization of IT) and the need to automate advanced malware detection. The demand for product offering to be accessible as hardware, appliance, and software delivered via on-premises and cloud/SaaS recognizes the diverse and challenging conditions organizations should consider for this area of threat mitigation.

- IDC believes this market in Western Europe continues to be a competitive battlefield, with leaders and major players protecting their market position while innovating their product delivery with advanced integration and malware identification features. At the same time contenders are expanding their reach into new markets or attempting to maintain a strong hold in the European markets. When assessing the eleven vendors included in this study, the distribution of vendors acknowledges their relevance to and focus on the European markets.

- For Western Europe, appreciation of regional go-to-market characteristics is a significant factor when assessing which vendor can provide the best combination of product and service. European incorporated vendors may lack in revenue, but demonstrate greater flexibility in sales, marketing and support functions and with anticipated higher levels of end user required innovation and integration; they challenge the traditional U.S.-based vendor prominence.

- IDC believes that for a vendor to be truly successful in this market, its capabilities must recognize the interoperability with other web, network, messaging and vulnerability products, providing efficiencies in risk mitigation via single policy engines that appreciate all devices types. Delivery of these capabilities then needs to be driven throughout the culturally dissimilar adoptive segments across the European region.

Filing Information: March 2013, IDC #IS01V, Volume: 1
European Security Products and Solutions: Competitive Analysis

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## IN THIS STUDY

This IDC study assesses the technology capabilities and Western European business strategy of several vendors in the enterprise endpoint security market. This research is a quantitative and qualitative assessment of the characteristics demonstrated by vendors that indicate their position and momentum in this market. This evaluation is based on a comprehensive IDC framework used to define a set of characteristics/criteria that assess vendors relative to one another and to those factors expected to be most conducive to success in the Western European market in the short and long term. This study is composed of two key sections, the first defining the characteristics/criteria IDC believes lead to success in this market and the second part, a bubble chart to illustrate the observed vendors in the market through means of a visual aggregation. In addition, the study provides profiles of the included vendors in relation to their assessment and essential guidance for end-user organizations considering investing in this market.

### Methodology

The IDC MarketScape is designed to provide an overview of the competitive viability of the key providers in the Western European enterprise endpoint security market. The criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured vendor discussions, companies' quarterly and annual reports, earnings calls, analyst events and vendor conferences, interviews with end users, buyer surveys, IDC research, and publicly available information. A bubble chart presents vendor positions with a strategic axis, representing a three to five-year span, and a capabilities axis, representing current product and Western European go-to-market execution. The market revenue for each vendor is indicated by the size of the circle representing the vendor. The plus, minus, and neutral symbols next to each vendor's name in parentheses indicate whether that vendor is gaining, losing, or steadying, respectively, its current market share.

The results of this IDC MarketScape study aims to provide an accurate, balanced, and consistent assessment of each vendor's characteristics, behavior, and capability within this market in comparison to each vendor included in the study.

## SITUATION OVERVIEW

### Introduction

The endpoint security software market encompasses products designed to protect endpoints from attack or to directly protect information residing on endpoints. At the macro level, the market segments into those products purchased by consumers and those acquired by corporations and other organizations. For this MarketScape, the enterprise endpoint security market is additionally segmented into the following four subcategories:

- **Antimalware** software consists of products that provide antivirus and antispyware protection. It includes both products that are signature based and

products that use other technologies, such as behavioral or heuristics, to prevent the installation or execution of malicious software.

- **Server security** solutions include antimalware, desktop firewall, and host intrusion detection and prevention software designed to maintain the integrity of servers. This category also includes products designed to protect hypervisors and virtual servers.

- **Security suites/platforms** include multiple endpoint security tools in a single, centrally managed package. Endpoint security suites/platforms normally contain antivirus, antispyware, desktop firewall, host intrusion prevention, and application control.

- **Access and information protection** products perform one or more of the following: encryption (full disk, file, and folder), device and application control, data leak prevention, or network access control.

Endpoint security has long been a component in the IT security arsenal. It is used to detect and remove computer viruses, prevent the implanting of spyware, protect the computer from hacking attacks while connected to the Internet, and provide data protection with encryption. With each defense, attackers would expand their abilities, which required more security. The proliferation of security products placed on a single device has become daunting to acquire and manage, and equally expensive. In response, many organizations now purchase a single product that can handle multiple security requirements. Security suites/platforms have the advantage of being easier to install than multiple applications and easier to manage, provided they can be managed with a single console. Vendors continue to improve the manageability of their products.

Endpoint security remains a prominent security solution. Growth in the Western European market can be attributed to a number of connecting and individual factors. Firstly, there is the increasing as the number of attacks that are being directed toward the endpoint. Most of these attacks come via Web interactions and are difficult to defeat at a network level and must be halted at the endpoint. Adding to this complexity is the ever-expanding perimeter. As mobile computing devices become an island unto themselves, they must have robust security capabilities because they can't rely on network security features when they aren't connected to the corporate network.

In parallel, the differing economic and adoption trends require vendors and organizations within Western Europe, to be insightful of market knowledge to ensure that budgets and strategies are employed correctly to minimize inappropriate technologies implementation while maintaining the highest security posture.

## Market Characteristics

IDC believes that to be successful in the Western European market, vendors and their software products must have a number of characteristics that include:

- In-country, native-speaking, go-to-market and customer support programs with localized software products tailored to the particular cultural, economic, and business drivers of customers.

- Strong current and continued commitment to developing and supporting an ongoing network of in country service provider and systems integrator partnerships.
- Substantial and sustained financial commitment by a vendor to the development, marketing, and support of their software product in relation to the needs of Western European customers.
- A heterogeneous capability to support a broad range of hardware and software technologies up and down the IT stack across traditional and cloud-based datacenters and/or services from other vendors.
- A focus on creating prebuilt patterns in relation to common IT activities and application deployments to accelerate a customer's time to deployment, return on investment, and reduction in operational complexity.

## Vendor Inclusion Criteria

In selecting vendors to include in this IDC MarketScape, the following criteria were applied:

- The IDC MarketScape methodology requires the top 5 vendors in the Western Europe market, by revenue, to be included in the analysis.
- Vendors that are recent entrants into the Western European market with strong positions in related markets should demonstrate a well-funded commitment to rapidly grow their presence through organic development and/or acquisition.
- Vendors must support a minimum of two operating systems and virtualization.
- Each vendor must have a minimum of 500 customers in Western Europe.
- A vendor's presence in Western Europe must be within 5 of the major countries.
- A product with enterprise endpoint security capabilities must have been at least available since 2010.
- Vendors were not included that had less than $50 million in reported security revenue for 2011 in Western Europe and/or announced they are exiting or downplaying the market.

## Market Evaluation Criteria

IDC believes that enterprise endpoint security vendors must exhibit the characteristics outlined in Tables 1 and 2 to be considered by end-user organizations. The factors are weighted as shown because IDC believes some characteristics are more important to end-user organizations than others.

**TABLE 1**

Key Strategy Measures for Success: Western European Enterprise Endpoint Security

| Strategy Criteria | Criteria for Success | Sub Criteria Weighting |
|---|---|---|
| Offering strategy | | |
| Functionality or offering roadmap | Excellence is achieved by plans to offer a complete and integrated endpoint security offering spanning both physical and virtual infrastructures, either through organic, acquisition or partnerships. Fully supported means it could be marketed as a standalone offering. Visibility of coverage for full enterprise endpoint security management and mobile computing will address market needs. Acknowledgement and/or alignment to industry standards are important. | 3.00 |
| Delivery model | Excellence is achieved by plans to support emerging architectures and particularly flexible delivery models such as SaaS, in order to enable benefits such as faster adoption and leverage of evolving operational (rather than Capital) adoption delivery models (e.g., Cloud). | 3.00 |
| Cost management strategy | Efforts to empower customers with the lowest TCO possible. Adaptive and segment related market wide pricing and consistent product offerings should be an objective. The extent to which the vendor provides customers with economical options, ROI metrics, and provide clear paths by which the client can gain efficiency of budget aligned to their delivery model strategy. | 1.00 |
| Portfolio strategy | Overall scope of capabilities provided by endpoint security vendors and its ecosystem including complimentary software and hardware to address the full scope of client needs. Clear and explanatory access to the benefits of the vendors current and planned range of offerings, that allows them to make the most effective use of the solutions offered. | 1.00 |
| Range of Services Strategy | Excellence is achieved by vendors that are able to articulate their intentions to show flexibility of financial arrangements that integrate with their proposed delivery model strategy. Growth plans to provide self administered tools including physical and online support across cultural and segment boundaries. | 1.00 |
| New Release/Revisions Strategy | Excellence is achieved by vendors that are able to outline to their markets on the rational regarding their ongoing product release strategy, its applicability to market trends and needs, and how existing and competitive challenges are being addressed to resolve offering deficiencies. | 1.00 |
| Offering Strategy Total | | 10.00 |
| Go-to-market strategy | | |
| Pricing model | Superior planning for future pricing alignment with market direction. Support for subscription pricing, ELA, concurrent user, and appropriate maintenance policies are considered. Pricing plans will encourage appropriate adoption of relevant components of the portfolio to meet user issues. Effective transition pricing to full suite (as appropriate) and/or adjustment in delivery method. | 3.00 |
| Sales/distribution strategy | Appropriate routes to market (RTM) leveraging direct, channel, and integration partners exist based on customer buying preferences. Any RTM strategy needs to instill a level of confidence that those organizations and individuals understand both the security landscape and also conversant in the appropriate delivery method(s). Excellence is demonstrated by plans to serve new vertical and segment markets, plus innovative RTM strategies demonstrated by the vendors | 2.00 |

**TABLE 1**

Key Strategy Measures for Success: Western European Enterprise Endpoint Security

| Strategy Criteria | Criteria for Success | Sub Criteria Weighting |
|---|---|---|
| | and channels/partners. | |
| Marketing strategy | Organizations with longevity have well-articulated plans, brands, budgets and appropriate event schedules to drive ongoing business growth. There is a strategic plan that can be articulated across the marketing mix, utilizing traditional and new communication vehicles, that aligns to market opportunity over the strategy planning period. Excellence is achieved via well articulated security issues based marketing strategies. | 2.00 |
| Customer service strategy | Ability to meet the full set of regional customer support, training and professional services needs either on own or through the partner network. Whatever the current client retention rate is currently, customer 'first' vendors will have a well-articulated plan for lowering customer churn and increasing the support experience. Positive assessments of day-to-day support and ability to resolve unexpected problems will score highly. | 3.00 |
| Go-to-market strategy Total | | 10.00 |
| Business Strategy | | |
| Growth strategy | Successful vendors will need to articulate an organizational growth strategy for the next three to five years, that is aligned with market trends, future opportunities and collaborative business integration points that address customer requirements. | 3.00 |
| Innovation/R&D pace and productivity | Strength of market viability is demonstrated by strategic plans for attaining or retaining functional superiority in the competitive market, either organically or via an acquisitive strategy. The vendors release strategy for the next 12-18 months reflects an understanding of market issues and resolution options. Support for multi-region/global customers as needed. | 3.00 |
| Financial/funding model | Customer buying centers should and do concern themselves with vendor viability. Success requires vendors to have a viable funding and solvency strategy for the next three to five years, with continuous alignment and improvements for industry benchmarking associated with employee to revenue ratios. | 2.00 |
| Employee strategy | Vendor success is relative to employee satisfaction. A clear strategy that invests in employee retention via workplace satisfaction and career development is essential to minimize employee churn and promote confidence to the customer community. | 2.00 |
| Business Strategy Total | | 10.00 |

Source: IDC, January 2013

**TABLE 2**

Key Capability Measures for Success: Western European Enterprise Endpoint Security

| Capabilities Criteria | Criteria for Success | Sub Criteria Weighting |
|---|---|---|
| Capabilities Offering | | |
| Functionality/offering delivered | A customer aligned solution offers a full range of appliance, software and virtual offerings that provide the option for collaboration with other suppliers. Success is further demonstrated by the depth of capability in areas such as full enterprise endpoint management and mobile computing, and the implemented innovation of each offering. The ability to market individual offerings as standalone, with local/regional support for the customer and also alignment to standards regulations. | 3.00 |
| Delivery model appropriateness & execution | Buyers are provided with operational flexibility to meet their existing business models, with visibility of how the same offering can have their delivery method amended as a customer adjusts its delivery priorities. | 2.00 |
| Cost competitiveness | A customer aligned solution is viewed as cost effective and delivers rapid ROI, whether the return is required immediately or during a fiscal quarter, fiscal year or a longer investment period. | 2.00 |
| Range of Services | Excellence is achieved when a vendor is able to demonstrate their value around financial, implementation and support, where a customer can understand a vendors 'value chain', that will allow resolution of issue, through effective pre/post engagement opportunities. | 1.00 |
| Impact of New Release/Revisions | Excellence is achieved where a vendor is able to provide customers with pro-active management for known and unforeseen issues, that could affect the operational and near term use of implemented offerings. | 2.00 |
| Offering Capabilities Total | | 10.00 |
| Go-to-market capabilities | | |
| Pricing model options & alignment | Current pricing for the vendor offerings should be flexible to meet the needs of the different segmentation sizes and industry verticals. Appreciating the customer needs for movement from Capex to Opex budget allocations. An attractive distribution pricing strategy (where applicable|) should encourage up/cross sell. In addition customers should understand how multi-offering purchases, provide discount opportunities. | 3.00 |
| Sales/distribution-structure, capabilities | An exclusive monopoly for any single vendor for a specific customer is rare, so a vendor should have a RTM plan in operation that encourages the integration possibilities of the offering with other vendor products. The vendor and its partner ecosystem should be fully conversant to address the customer issues with the most appropriate delivery/pricing and portfolio strategy. | 3.00 |
| Marketing | Excellence is achieved when the vendor is able to execute on day-to-day deliverables that drive all elements of the marketing mix and new communication vehicles that service the customer / prospect community both via the vendor organization and also as demand generation tools for the partner ecosystem. Segment and vertical marketing functionality should be available where applicable. | 3.00 |

**TABLE 2**

Key Capability Measures for Success: Western European Enterprise Endpoint Security

| Capabilities Criteria | Criteria for Success | Sub Criteria Weighting |
|---|---|---|
| Customer Service | Successful vendor's investment in their customer service organization echo's their need and ability to support and resolve variable customer, regional and product issues. Day-to-day customer satisfaction ensures that issues are resolved, while minimizing negative commentary about the vendor and its offerings to the IT ecosystem. | 3.00 |
| Go-to-market capabilities Total | | 10.00 |
| Business capabilities | | |
| Growth strategy execution | Excellence is provided through the current fiscal plan that outlines how the vendor is approaching market momentum and trends in its execution strategy. Existing customers look to understand opportunities that are relevant to themselves, while the vendor will have a plan of product/country/regional growth to meet industry and internal objectives. | 3.00 |
| Innovation/R&D pace and productivity | In a very competitive market the ability to show release schedule advancements, combined with near term acquisitions that increase the value of the vendors portfolio. An active retirement/replacement program should be well communicated and implemented, to ensure maturation of the portfolio. | 3.00 |
| Financial/funding management | Excellence is marked through a visible understanding of a vendor's financial viability. Investment into development activities should be appreciative of the changing pricing models due to customers moving to Opex from Capex that may affect recognizable revenue in the short term. | 2.00 |
| Employee management | Consistency of personnel relationships between the vendor and its customers encourages long term partnerships. The ability for the vendor and its partner ecosystem to maintain a low attrition rate and operational career development program. | 2.00 |
| Business capabilities Total | | 10.00 |

Source: IDC, January 2013

## FUTURE OUTLOOK

### IDC MarketScape: Western European Enterprise Endpoint Security 2012 Vendor Assessment

The IDC vendor assessment for the Western European enterprise endpoint security market represents IDC's opinion on which vendors are well positioned today through current capabilities and which are best positioned to gain market share over the next three to five years. Positioning in the upper right of the grid indicates that vendors are well positioned to gain market share. For the purposes of discussion, IDC divided

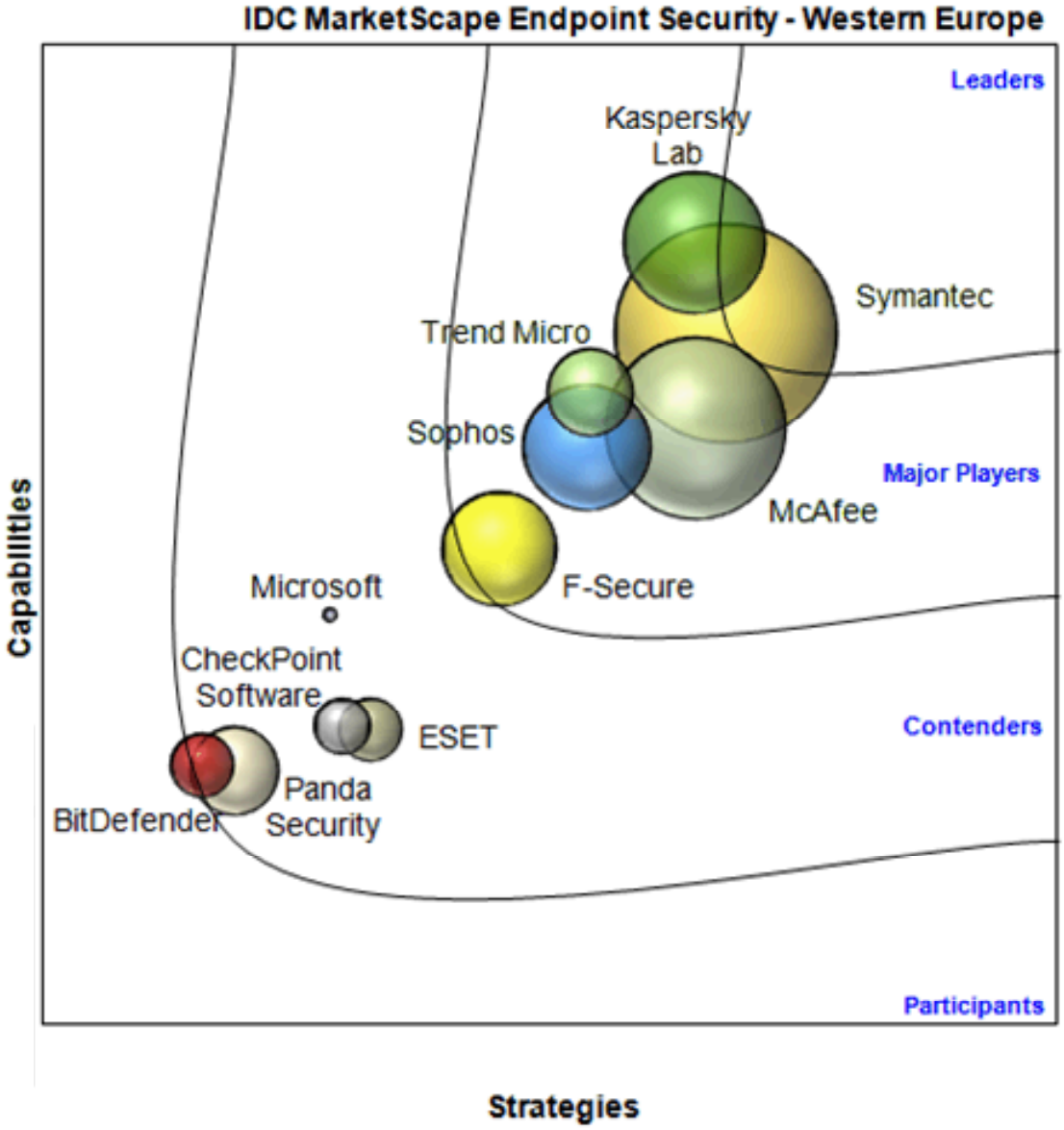
potential key measures for success into two primary categories: capabilities and strategies. Positioning on the y-axis reflects the vendor's current capabilities and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and the product today, here and now. Under this category, IDC analysts look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market. Positioning on the x-axis or strategies axis indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level strategic decisions and underlying assumptions about offerings, customer segments, and go-to-market plans for the future (in this case defined as the next three to five years). Under this category, analysts look at whether or not a supplier's strategies in various areas are aligned with customer requirements over a defined future time period.

Figure 1 shows each vendor's position in the vendor assessment chart. A vendor's market share is indicated by the size of the bubble.

**FIGURE 1**

IDC MarketScape: Western European Enterprise Endpoint Security 2012




## Vendor Summary Analysis

### *Bit Defender*

Bit Defender (enterprise.bitdefender.com) is headquartered in Europe out of Bucharest, Romania, and provides endpoint security with its hyper visor agnostic Virtual Appliance. As Bit Defender transitions from its previous role two years ago of only white labeling its offerings via third-party organizations into a respected security brand, IDC anticipates the organization will grow over the coming fiscal periods to

challenge the leaders. IDC positions Bit Defender as a **Contender** in the Western Europe Endpoint Security Software IDC MarketScape.

Positioning its security appliance in front of all other virtual machines eliminates the need to cross scan from one VM to another, complimented with a security console that provides policy creation and reporting for resource groups.

Targeting the high end enterprise organizations that have been first to market with virtualizing their critical systems, Bit Defender supports all of the traditional operating systems (Windows, Mac Windows Servers), and is initially offered as an appliance. However, a cloud offering will only be available as part of its future roadmap.

Utilizing a 100% channel route to market in Europe that focuses on the DVAR and VARs and supported with a new channel program including the basics of deal registration, the Bit Defender organization is committed to supporting opportunity closure in virtualized environments for the channel primarily across the DACH, Scandinavia, and the U.K.

### Areas of Strength

- Bit Defender has been in the endpoint security market for a long period and understands this market where it scored well for local language support in the capabilities criteria, albeit under the covers by providing their offerings via a white label strategy.

- Bit Defender now focuses on the growth market of virtualization via its virtual appliance, using a technical architecture that minimizes breach opportunity and enhances efficient scanning.

- Bit Defender implemented an efficient route to market (RTM) strategy utilizing the VAR community to increase value and revenue to the reseller, up skilling its own organization in Europe to support the channel.

### Areas of Concern

- Although critical system virtualization is gaining moment for end users, a lower score was applied in the strategy criteria as there is still the need to support non-virtualized devices to appreciate the balance within datacenters. This area of weakness is further concentrated, as Bit Defender's focus market is the high end Enterprise that will have a mixture of virtualized and non-virtualized system across disparate locations and business entities.

- Mobile anti-malware technologies are major requirements in the endpoint security space due to the growth of mobile/BYOD adoption. Bit Defender provides no current support for any mobile OS platform, minimizing its current capability and strategy criteria scoring and subsequent opportunity in the enterprise segment.

- In the competitive enterprise segment, Bit Defender needs to increase its 'Awareness' above the noise of more established vendors. IDC scored Bit Defender at the midpoint within the go-to-market criteria as we believe that greater European use of web 2.0 needs to be escalated, alongside improved channel engagement communications.

- With no cloud delivery model at present, many of Bit Defender's target market will opt for alternative vendors, especially as the ability to secure virtualization

infrastructures is a key operational and cost essential in these non on-premises offerings.

**Areas of Opportunity**

Bit Defender is well positioned in the European market to leverage the maturity of its knowledge in the endpoint security market. Its virtualized offering acknowledges the changes that end-users apply to efficient operations. An increased awareness program across its targeted European countries, aligned with its channel incentives, will lead to a higher level of 'consideration' by prospective end users. However, Bit Defender needs to maintain roadmap schedules for mobility and cloud offerings, as this will increase IDC evaluation scoring in the business strategy criteria section in future MarketScapes, and reduce the risk of missing its growth targets.

### *Check Point Software*

Check Point Software (www.checkpoint.com) has dual headquarters in Tel Aviv, Israel and San Carlos, California. It provides a security software blade architecture that can be deployed on both a network gateway and also on endpoint devices. The software blade architecture has a wealth of security functionality that positioned Check Point as #8 for secure content and threat management (SCTM) in the 2012 IDC Western European vendor share report, within this report's focus on endpoint security. Checkpoint's offering is available as software, hardware or cloud delivery, with the cloud delivery model leveraging Check Point's 'ThreatCloud' real-time intelligence network. All policy management is controlled via the 'Endpoint Policy Management Software Blade', providing a single interface for policy enforcement, status awareness for users and devices, and reporting across all functions. Check Point acknowledges the need to support collaborative solutions with other database and software vendors using a secure operating system to increase its customers' security posture. IDC positions Check Point Software as a **Contender** in the Western Europe Endpoint Security Software IDC MarketScape

Check Point delivers its European support from Tel Aviv and Sweden, utilizing the wealth of knowledge from its regional partners that provide regular yearly feedback on the region, but also providing direct Check Point support for end users via its Tel Aviv offices.

**Areas of Strength**

- Scoring at midpoint within the business strategy criteria, the flexibility of 'Software Blades' provides a very rich set of endpoint, encryption and VPN features, alongside existing network capabilities, creating an up stack capability for end users and channel partners.

- *Endpoint Policy Management* simplifies endpoint security management by unifying all endpoint security capabilities via an intuitive dashboard that simplifies complex endpoint solutions for enterprise organizations.

- With Check Point's Israeli background, localization for the local European markets is very strong in terms of language support, critical system support and appreciation of the different market segments in Europe compared to a generic worldwide perspective, all of which are recognized in the go-to-market criteria.

- Check Point's mobile device support has started well with VPN access for the majority of the key OSs, with ongoing MDM and mobile security advancements planned in 2013.

**Areas of Concern**

- Check Point is failing to leverage the wealth of implementations it has via its network offerings and translate this to the endpoint security market. The European market continues to be a tough market for Check Point to obtain sustainable growth, with IDC reporting a 13.7% 2010–2011 revenue decline in the SCTM market, dropping its vendor share to 3.3%. In addition, it does register on the endpoint security vendor list.

- Check Point continues to rely on Kaspersky Lab for its core AV engine functions, minimizing vendor differentiation, with Kaspersky Lab having a wider attraction for the same markets.

- The scoring in the capabilities and strategy criteria recognized that although Check Point's protection primarily supports the Windows PC with development growth for Mac OS X, it is challenged with supporting other major OSs around email and file sharing that are growing in relevance to changing device preferences. This is of particular concern given the general industry trend of falling PC sales.

- Check Point acknowledges the movement of end users to annualized rather than perpetual licensing, but a lack of coordination across the product portfolio such as virtualization and mobile management still requires end users to purchase additional components, thereby increasing resource requirements.

**Areas of Opportunity**

Check Point has a very positive opportunity to turn its fortunes around with the European market, pulling together a concentrated message that incorporates its 'ThreatCloud,' software blade, and network offerings, which would increase its strategy criteria score. Although a reasonable amount of development work needs to be conducted internally, this is not insurmountable, minimizing the effect of endpoint security decline affected through a competitive positioning that has recognized end-user optimization and intentions slightly earlier than other vendors. Local channel partners will be retained if the above can be demonstrated, maintaining a level of consideration from these partners when they are faced with customer opportunities in the endpoint security market.

### *Eset*

Eset (www.Eset.com) has headquarters in Bratislava, Slovakia, and delivers Eset Endpoint Security, Eset Endpoint Anti-Virus and Eset Mobile Security products. With over 20 years providing antivirus products predominately to the consumer market, and entering the SMB segment initially in 2007, Eset approaches the enterprise segment market with a positive investment attitude. IDC positions Eset as a **Contender** in the Western Europe Endpoint Security Software IDC MarketScape

Eset's ability to recognize the distinct European markets means it will not follow the 'pack', but rather approach its growth strategy in a sustainable fashion, balancing product functionality with market needs and correct 'tone of voice'. Its route to market strategy that embraces a distribution network also widens the company's reach.

Eset outperformed the Western European growth target of 5.94%, recognizing a 7.4% growth ($39.5 million) for endpoint security in 2011 as reported in the 2012 IDC Western European vendor share report, maintaining its 1.9% vendor share, establishing the vendor at ninth position.

### Areas of Strength

- A good score in the capability criteria acknowledges Eset's background over the last 20 years in the antivirus market. This has provided the organization with an in-depth knowledge of malware detection which treats signatures as an advanced algorithm and optimizes multipoint heuristics to detect malware and reduce false positives. Its 'honey pot' collection is used for internal research, but can be complemented with 'Eset LiveGrid' for statistical malware and intelligence for its cloud-based reputation system in any specific region.

- Appreciative of the footprint issues for the SMB market that many other security vendors have learnt, the installation and operating requirements of the Eset endpoint security offerings require minimal resources to execute, both in physical man power and system requirements.

- Eset complements its endpoint offerings with encryption, DLP, backup and secure authentication for specific market conditions.

- Eset is beginning to roll out its endpoint security cloud offering in Europe after its initial go-to-market strategy was launched in North America. IDC scored Eset well in the strategy criteria relative to this delivery option, but believes that a targeted European country plan for cloud may have provided equal success closer to home.

- Eset gained success in the larger segments utilizing the 'word of mouth' success that the company has built from Eastern Europe. Trust has been a key contributor to success in the Eset strategy to date.

- Mobile device management is a known essential for the company, with the launch of Eset Mobile Security Business Edition that was ruggedized from its consumer offering. Android has been added to the portfolio via its endpoint security platform.

- IDC has identified that Eset provides an agreement that allows Microsoft to license the Mac and Linux support for their MEP offering, increasing its revenue and scoring in the business subcriteria.

### Areas of Concern

- Eset's strategy to provide customer needs rather than a vendor range of products, has identified the need to provide augmented features for DLP, Encryption, backup and authentication under a reseller agreement. IDC believes that these features should be bought in-house as Eset products to create a holistic offering from the company without fear of competitive differentiation. This has affected its go-to-market criteria scoring compared to other contenders growing in this market.

- The SMB market will embrace the simplistic web based reporting facility, although the larger midmarket and enterprise organizations will require a more

complex facility, as scored within the product appropriateness subcriteria, with APIs from the endpoint security offerings into larger SIEM products

- Many of Eset's product policy management capabilities are independent of each other where multiple operating systems (windows, Mac, Linux, etc.) are supported, increasing the resource intensity of each offering. The policies can be cloned from one product to another, but development work for the integration of these engines should be a priority over the next 18 months.

- The cautious approach for Eset as a privately held organization may ensure it provides products that meet on-demand requirements, although the company needs to view the larger segment spaces as an opportunity to invest in feature 'innovation' to catch the eye of possible customers, otherwise; it risks losing market and higher revenues to the security innovators.

#### Areas of Opportunity

Eset is in the first full year of its strategic plan of competitive growth in the enterprise arena and will continue to conquer many of the concerns listed previously. The organization has to continue its investment strategy to position itself as a robust and recognizable enterprise class endpoint security vendor. Not following the 'pack' may be a good option in certain areas, but time to market and innovation, especially where the current product family disconnects from the needs of the growth SMB market across the EU-27, can be addressed with the intended strategic plans of the company.

### *F-Secure*

F-Secure (www.f-secure.com) has corporate headquarters in Helsinki, Finland, and, delivers endpoint security either through the hosted 'Protection Service for Business' or on-premises 'Business Suite'. F-Secure is growing in stature across all segments of the European market, taking vendor share from established and smaller vendors through its focus on dedicated endpoint protection. Its lack of security management capability is overcome via the ease of integration with collaborative organizations that provide end users with minimal overlap. IDC positions F-Secure as a **Major Player** in the Western Europe Endpoint Security Software IDC MarketScape

The appreciation of offerings that meet end users' needs to move from on-premises to cloud delivery, maintain a simple but very effective alternative to other offerings.

#### Areas of Strength

- F-Secure delivers very focused endpoint security solutions, scoring very well in the business criteria for innovation, resisting the trend to branch out into other areas of security management and earning praise from its European customers for its high level of technical and support capabilities.

- F-Secure's MDM offerings are represented in the capabilities criteria that acknowledge the varied types of OS in its target SMB and low enterprise markets. This is delivering via a cloud based offering that also appreciates the opportunity to attract a large installed base in Europe and ease of management outside of the datacenter.

- The local presence of F-Secure in Europe is an asset that is not captured in other worldwide vendor reports, and its shows a 14.1% revenue growth in the 2012 IDC Western European SCTM vendor share report, the third highest in the

region. As a result, it has grown its market share to 6.1% in 2011. Initial revenue data from 4Q12 IDC Security Tracker continues to show good year on year growth in Germany and the United Kingdom.

**Areas of Concern**

- F-Secure has achieved some excellent growth over the past couple of years, although there continues to be a perception in the market that the company's offerings are simplistic and basic in their functionality.
- As with other vendors in this report, F-Secure requires the intelligence of Bit Defender for its signatures, affecting its capability criteria scoring as this may create a negative impact for the cloud-based offering in the event that Bit Defender does not meet its service levels.
- Advanced controls and functionality provided by other vendors in this space such as data loss, encryption, virtualization, and cross-functionality integration are reflected in the strategy criteria, as this will deter potential customers from adopting F-Secure as a long-term partner.

**Areas of Opportunity**

F-Secure has an opportunity to continue its growth across the European market and establish itself [further] as a reliable and effective offering for endpoint security in the SMB segment. Many of the concerns outlined above can be turned into strengths, which would enhance its capabilities and strategy criteria as the company drives further expansion into more European countries, and the ability to deliver functional enhancements to challenge the competitive landscape within its immediate radar.

### *Kaspersky Lab*

Kaspersky Lab (www.kaspersky.com) has corporate headquarters in Moscow. The company has delivered notable growth over the past decade to the SMB and enterprise markets through its suites of targeted endpoint security solutions. Kaspersky continues to focus on organic growth and innovation as a key differentiator to the M&A activity that other security vendors are initiating. The latest Kaspersky Endpoint Security for Business (KESB) platform demonstrates the company's ability to develop issues-based offerings challenging resource, management and cost complexities in this category. IDC positions Kaspersky Lab as a **Leader** in the Western Europe Endpoint Security Software IDC MarketScape.

Revenue for Kaspersky Lab was slightly down (-1.4%) in Europe for 2011 as reported in the 2012 IDC Western European vendor share report, although the direct feedback from customers and partners is that this is was more of an execution issue, rather than product concern, as the renewal rates within Europe for Kaspersky Lab are very high, in part due to its recognized exceptional technical support service. Initial revenue data from the 4Q12 IDC Security Tracker continues to show stable year on year growth in the DACH region and good penetration in the Nordic region

Kaspersky Lab has significant goals and is focused on the aspiration of being a $1 billion a year company within three to five years, growing from its current $600 million revenues. Looking at its consumer background in 1998, the growth of the company through focused, innovative products and a customer-driven regime, this goal looks achievable.

### Areas of Strength

- Kaspersky Lab focuses on what it does very well: Endpoint security. The high scoring for capability and strategic criteria recognizes the organic development within the company that ensures, where possible, the various components for workstations, laptops, mail, collaborative servers and Internet gateways utilize the same code base for ease of updates and continuity in the event of a product failure.

- Kaspersky Lab recognizes that management is a key essential for its end users and is augmenting the existing management features of policy and reporting to include mobile device management, vulnerability analysis, and systems management functions.

- Kaspersky Lab continually maintains support for all definitions of endpoint devices, whether they are servers, PCs, or all current flavors of mobile devices; ensuring existing users minimize outages when adopting operational changes to device security.

- Kaspersky Lab is enhancing both its current device control features and encryption capabilities, both tied in with its malware policies challenging many of the existing providers that offer solutions that require individual management.

- European users recognized that Kaspersky Lab endpoint security offerings allow them to implement a 'light' memory footprint, which scales from small business to low enterprise, alongside a highly skilled organization that responds quickly to malware, resulting in a high score for business and capabilities criteria.

- The pricing strategy for the European market appreciates the need to deliver hybrid as well as point endpoint security offerings, with a flexible approach to upgrade and cross-grade needs from the end-user base, making Kaspersky Lab a viable offering for current and potential business partners.

### Areas of Concern

- Kaspersky Lab is a mature and recognized expert in the endpoint security market, but IDC has scored Kaspersky slightly lower in the product appropriateness element of its strategy criteria as the organization lacks an area of other leaders in the MarketScape by not having its own SIEM tool to feed the logs and activity, completing the portfolio with its Kaspersky Security Network (KSN).

- Kaspersky Lab's focus on organic growth has its benefits in common code and internal development controls, but the double-edged sword to these benefits is that Kaspersky Lab might end up late to market and reactive to user concerns rather than providing innovation early.

- Data Loss Prevention is a missing component, although future integration into existing endpoint security platform offerings will meet the implementation expectations of the SMB market.

- Customers of Kaspersky Security for Virtualization (KSV) environments appear to have started to ramp up their implementations, which will be critical to addressing the growth needs of the enterprise segment that are exploiting virtualization for critical systems.

#### Areas of Opportunity

Kaspersky Lab continues to go in the right direction in the European market, accelerating its awareness and consideration to existing and prospective users as a vendor of choice in the SMB markets. The potential wider growth with existing Endpoint 8 and Kaspersky Endpoint Security for Business (KESB) products is sure to cause concern to peer group competitors. Kaspersky Lab should ensure it does not take its focus off the European market, while extending its coverage in North America. IDC has not scored Kaspersky down in the market divergence subcriteria of its go-to-market strategy, but will be monitoring the focus of the organization on the European market.

### *McAfee (An Intel Company)*

McAfee is a subsidiary of Intel (www.Mcafee.com) with its EMEA headquarters in Amsterdam. It scores very well in this IDC MarketScape with its depth of product functionality within its portfolio of offerings in the Total Protection and Endpoint Protection suites. At the core of all McAfee products is the McAfee ePolicy Orchestrator (ePO) platform enabling unified control and security status across organizations' security and compliance products. IDC positions McAfee as a **Major Player** in the Western Europe Endpoint Security Software IDC MarketScape,

As one of the most established pure security organizations in Europe, McAfee's security product portfolio evolved over the last 10 years to be included on all end user requests for proposal (RFP).

Breaching the $300 million revenue waterline in 2011, with growth of 5.8%, McAfee continues to hold #2 position both worldwide (18.7%) and in Europe (15.1%) for endpoint security. After the completion of Intel's purchase of McAfee in February 2011, the organization has been very positive about the work to embed certain endpoint security functions within the Intel chipset, while also settling the IT industry's fears that the McAfee strategy will continue as before, but now in parallel with anything that happens at Intel. Consistency continues to follow McAfee as the initial revenue data from 4Q12 IDC Security Tracker continues to show 5% quarterly growth year on year.

In Europe, McAfee puts all its trust for its route to market strategy in the channel, with almost 98% of its business led, developed, and closed by the channel community. All internal European personnel, across its five sub-regions, are dedicated to making this sales operation work, providing sales, technical, marketing, and support resources to all its channel partners.

#### Areas of Strength

- The depth of product functionality for endpoint security, covering HIPS, NAC for endpoint, virtualization, and MDM, among others, attracts all end users to consider McAfee as a resolution to their security concerns, across all organizational segments. This, in addition to the longevity of the company in the European market, has helped to scored McAfee highly in solution and device offerings within the strategy criteria.

- IDC sees McAfee's ability to provide agent and agent-less antimalware scanning in VMware environments as a key area of strength.

- Associated with Endpoint security to bolster McAfee credibility, the go-to-market criteria scoring appreciates the acquisitions of Nitro Security (SIEM) and the

development of an anti-rootkit offering, Deep Defender, providing examples of work between McAfee and its parent.

- McAfee is expanding its endpoint security channel efficiencies with enhanced CRM integration between McAfee and its channel partners to capture and resolve business opportunities. IDC views this as an essential across geographical and cultural boundaries.

- McAfee provides accessibility of its endpoint security solutions via traditional and subscription-based delivery models with flexible pricing to allow movement between each as required by the end users' business needs. It also recognizes the feedback and business needs from its channel partners and translates them into a good capabilities criteria score.

**Areas of Concern**

- McAfee addresses the small business market with a subset offering of its enterprise product, possibly creating a heavy product that only meets the needs of this market segment if its functions are not initialized,

- McAfee employs a 100% channel model to widen its touch points across the region. A midpoint score within the routes to market subcriteria was applied as IDC needs further reassurance that McAfee does not lose touch with its end user customers, even with the skills of the channel partner taking much of this role.

- McAfee's coverage for MDM needs to be expanded to support more of the security functions of MDM, such as threat management and identity, rather than relying on the basic functionality. IDC does expect this issue to be resolved in 2013, with the movement of all identity offerings transferred from Intel to McAfee in the latter part of 2012.

- As the prospect of lower PC sales and the PC-less employee becomes a growing possibility in the next three to five years, McAfee's focus [from Intel] on the PC needs to be revisited.

**Areas of Opportunity**

IDC has scored the strategy criteria slightly lower than its peer group as we believe that McAfee is at a reflex inflection point in its European growth, as peer group organizations prepare to deliver unique integrated offerings, while others are reviewing their business model to grow at faster rates than the European industry growth. The endpoint security portfolio with its centralized management engine (ePO) continues to drive opportunity, but a clearer understanding of future architectural and functionally developments will help to thwart any possible decline in its account base.

### *Microsoft*

Microsoft (www.microsoft.com) with its headquarters in Redmond, Washington, offers its Microsoft Endpoint Protection (MEP) solution. The continued dominant position that Microsoft holds in the PC market allows the organization to provide the functionality of its endpoint security product as 'No or Low Cost' deployment within its overall Microsoft licensing policies. Microsoft challenged the market's negative reaction regarding the robustness and applicability of its security products for many years. IDC believes that the enhanced security functionality in Windows 8 will bolster its ability to convince customers that it is moving in the right direction to provide a

solid endpoint security offering. IDC positions Microsoft as a **Contender** in the Western Europe Endpoint Security Software IDC MarketScape

Microsoft grew very slightly in revenue terms in 2011, achieving $2.27 million, up 13% on its 2010 position, as reported in the 2012 IDC Western European SCTM vendor share report. Microsoft's current revenue achievements do not provide it with a top 15 ranking within the western European vendor share report. Initial revenue data from 4Q12 IDC Security Tracker continues to show flat quarterly year on year growth of 1%, which will not help in raising Microsoft's market standing.

#### Areas of Strength

- Microsoft is able to offer endpoint security for Mac and Linux clients via an agreement with Eset, increasing it score for go-to-market criteria.
- Any organization that takes advantage of Microsoft's Enterprise CAL or Core CAL program will receive Microsoft Endpoint Protection for no additional cost, which is a very attractive offering for budget constrained 'less security aware' end-user organizations.
- A well integrated facility via System Center Configuration Manager means that existing SCCM users only need install the MEP agent.

### *Areas of Concern*

- Microsoft's investment in the endpoint security market appears to be limited, with advancements around advanced malware detection (signature, behavioral, heuristics) sadly trailing those of the dedicated security organizations, thereby affecting their product relevance and roadmap subcriteria scores.
- Microsoft did not provide IDC with reasonable content to allow the evaluation of its effectiveness in this market. As a result, IDC was unable to score its go-to-market strategy criteria higher than midpoint from channel and end user interview feedback.
- IDC does not experience a large volume of inquiries from end users requesting validation of the Microsoft MEP offering, compared to high levels of review requests for its competitor peers.
- Although Microsoft appears to recognize the growing importance of security in its flagship Windows 8 operating system, no innovation appears to be transitioning into its MEP offering.
- Advanced functionality around DLP, encryption, firewall and reporting facilities are dramatically lacking in policy and user ability against equivalent competitive offerings.
- Microsoft needs to increase its positive nurture for endpoint security across all devices as the threat landscape continues to find the easiest point of entry. Scoring for communication, marketing, and pricing subcriteria were detrimentally affected. The positive consideration by potential MEP prospects can be enhanced if it demonstrates a pricing-based value proposition.

### *Areas of Opportunity*

Microsoft continues to have the greatest opportunity to grow its endpoint security revenues and reputation of all the vendors, due to its dominant position across PCs and servers. A focused appreciation of the value that other vendors in this market attract could significantly change Microsoft's position in this space. The synopsis of this Microsoft review has contained very limited regional appreciation due to the lack of available content and market differentiation being experienced by IDC, channel partners, competitive vendors, and end users

### *Panda Security*

Panda Security (www.pandasecuirty.com) with its headquarters in Bilbao, Spain, targets its endpoint security solutions at organizations that focus on cloud delivery. Panda Security's historical European presence is demonstrated by its strategic focus within the region, spread across western and southern markets. Panda Security has developed a cloud delivery model via Panda Cloud Office Protection. Its established on-premises offering, Panda Security for Business/Enterprise, complemented by the Panda Cloud Systems Management offering, highlights a good understanding of the convergence of security and systems management. The strategy of cloud and on-premises appreciates the diverse adoption rates of organizations in Europe, where Panda Security also allows for hybrid implementations of its offering, providing continuous operations during transition. IDC positions Panda Security as a **Contender** in the Western Europe Endpoint Security Software IDC MarketScape

Panda Security grew 5.7% ($74.6 million) for endpoint security in 2011 as reported in the 2012 IDC Western European vendor share report, slightly dropping their market share by 0.1% to 3.6%, due to missing the region growth target of 5.94%. Despite this, it remains in sixth position for the Western European market.

#### Areas of Strength

- The simplicity across Panda's cloud offering embraces the SMB segment and makes the development of new features on the roadmap less disruptive than traditional on-premises offerings. The convergence of the systems management console in the cloud is innovative for a security organization and sets a standard for competitive vendors.

- The flexible annualized and monthly pricing policy of the company has been built with the changing ecosystem of the user in mind, so it can optimize its capital and operating budget, based on the delivery method, as well as catering for the operational practices of its channel partners.

- The Panda Security Cloud Office Protection product employs remote control tools, allowing users to initiate activity via the Panda console for an endpoint and take over the device, and assign tasks, shell access, terminate a process, among others.

- The channel partner portal provides a 'super user' facility, enabling the partner to assign new functionality and licenses to the customer immediately without having to request these changes with Panda Security directly.

#### Areas of Concern

- The ability to run a hybrid mix of cloud and on-premises products requires the customer to run multiple management consoles. IDC has factored this into the

scoring in the go-to-market strategy criteria as we do not expect to see the convergence of these consoles, given Panda Security's focus on its cloud strategy.

- The offering strategy criteria recognizes the lack of a solid MDM offering, whether on-premises or as part of their new cloud strategy. This will deter SMB prospects as they are high users of business mobile and BYOD implementations across the European region.

- Existing Panda Security customers need to be aware that the process to move from on-premises endpoint security to Cloud is not automated and will require detailed planning to manage the uninstall and re-install, requiring the possibility of a resource intensive project.

- Functional and operating system development across the platform range needs to be accelerated to include virtualization, encryption, DLP, Mac and Linux support. The lack of these functions has been applied to the product functionality subcriteria.

- Although Panda Security targets all market segments, the lack of identified functionality will deter complex enterprise organizations that require these distinct features.

- Panda Security go-to-market criteria acknowledges its very vocal strategic direction of focusing on cloud deployments moving forward. Any organization with its on-premises offering will have to evaluate its viability for the organization's environment or risk operating a trailing product with a lower level of development priority.

#### Areas of Opportunity

Panda Security made a bold statement within the Endpoint security market to focus its long term strategy on the delivery of its products via a cloud model. With a distribution of existing customers across all market segments, the company needs to raise its profile across the European markets and the SMB segment that need this level of security simplicity. The recent increase in focus of Panda Security's channel partnerships will be a key success factor to enable the organization to expand its reach, although success will also require an internal skills investment of sales, marketing, and support to compete efficiently with its competitive peer vendors.

### *Sophos*

Sophos (www.sophos.com) has dual headquarters in Oxford, England, and Boston, U.S. It has its engineering headquarters in Oxford, England, allowing the organization to organically develop global products with local nuances factored into their value. The recent arrival of a new CEO (Kris Hagerman) and CMO (Matt Fairbanks) provides an insight into the Sophos strategy to accelerate its capabilities outside of the European market and make a sustainable position in North America. Explicit in its focus on businesses both midmarket and enterprise, the "Sophos Anti-Virus – Business" and recently announced 'Sophos UTM'(Firewall, Network, Web, Endpoint Protection, Email), supports all major OSs and devices types, delivered on-premises using a channel engagement model with Sophos endpoint specialists supporting the reseller, creating a combination of concentrating on doing explicitly well across all (product, sales, marketing, etc) focus areas.IDC positions Sophos as a **Major Player** in the Western Europe Endpoint Security Software IDC MarketScape.

Sophos was equal first in its growth (17%) for endpoint security ($155.2 million) in 2011 as reported in the 2012 IDC Western European SCTM vendor share report, advancing its market share to 4th in the market (7.6%), only 1.8% away from the third placed vendor. Initial revenue data from 4Q12 IDC Security Tracker shows Sophos maintaining growth in alignment with the Western European CAGR for endpoint security, recording a 6% quarterly year on year growth.

Awareness of Sophos in European (and wider audiences) has been achieved via its Naked Security Blog, which acts as an excellent reference of essential and topical security information.

**Areas of Strength**

- Sophos's Europe-based engineering allowed it to grow its regional business to the point where its endpoint security (and wider portfolio) offerings can challenge the wider global market.

- Sophos's endpoint security products were developed to support all major server, PC and mobile device OSs, scoring high in the strategy criteria, extending their malware detection capabilities to compliment areas such as application, encryption, data loss, among others.

- Sophos's execution within the capabilities go-to-market criteria scored well, appreciating the European market in its pricing flexibility, providing user-based rather than device-based controls and recent user-based pricing for endpoint security within its complete Security Suite or Mobile Device Management offerings.

- Appreciation of virtualized and non-virtualized environments is further augmented with a wide range of DLP features and context-driven encryption policies for all removable media types.

- IDC scored Sophos higher than others in the go-to-market communications subcriteria as it has recognized the changes that have happened across business segments and is a leader in its use of Web 2.0 tools to promote its own endpoint security products, but also to educate the market about security concerns, issues and best practices.

- Sophos is extending its MDM offering for endpoint protection during 2013 to focus on many of the security aspects of the management controls that are being overlooked in this space, ensuring that data and applications are confidently managed on mobile devices.

- Sophos scores well in customer support through its SCP certification as well as positive feedback on the high levels of security issue resolution.

**Areas of Concern**

- Sophos's recent entrance into the UTM market (via the Astaro acquisition) will provide a wider market opportunity, but Sophos needs to address the integration capabilities for management of this and its other software endpoint security products. Sophos has a unique ability to grow within the vast European SMB market if it increases its integration plans across all endpoint, management, and policy tools.

- Sophos is well-recognized in the European market, but its lack of penetration in the U.S. may divert valuable program funds away from the European market and into the U.S. market. With a new CMO and CEO in the U.S., the Oxford team needs to ensure that new investment budgets for the U.S. do not diminish the installed base awareness in Europe, causing a slightly lower score in its strategy go-to-market criteria.

- Lessons will have been learned regarding the 'False Positive' situation in 2012, requiring increased beta testing that will allow Sophos to score higher in the next report within the subcriteria for its offering criteria. The local presence of Sophos in Europe mitigated what could have been a more sizeable challenge to overcome, though this is not to minimize the effect it had on the installed base.

#### Areas of Opportunity

Sophos has the ability to grow its European business with focus on some of its newly acquired products that potentially represent upsell opportunities into its current install base of endpoint security customers. The appreciation of the SMB market needs of Europe, and Sophos's relative minimal complexities as an organization can help it react and complete opportunities faster than some of its major competitors. This last statement needs to be grasped before anticipated success in the U.S. may divert product and resource attention to the larger (opportunity) market.

### *Symantec*

Symantec (www.symantec.com) has EMEA headquarters in Reading, United Kingdom, and maintains its worldwide #1 market share and revenue position in endpoint security across the European market. Symantec's core endpoint security solution is Symantec Endpoint Protection (SEP 12) and SEP Small Business Edition 2013, all built on four layers of protection: network, file, reputation, and behavioral. In addition, SEP provides application and device controls and Symantec offers Symantec Mobile Security to protect Android and Windows phones. The flexibility of the Symantec products allows it to provide licensing programs across all segments on a per seat/per year basis. IDC positions Symantec as a **Leader** in the Western Europe Endpoint Security Software IDC MarketScape

Symantec's maturity in the security market allows the organization to compliment its endpoint security offerings with suites and point products that cover encryption, authentication, certificate management, and systems management among others. This provides Symantec the ability to serve the diverse European markets with issue-based offerings and locally resident support, spearheaded with a regional direct and indirect sales and marketing focus.

#### Areas of Strength

- Symantec's portfolio recognizes its position in the European market, with on-premises and cloud offerings to satisfy the needs of all segments across economically disparate countries.

- Symantec's local presence in all of the European countries has been recognized in the capabilities criteria, with the resources of up to 33,000 channel partners utilizing, their reach and touch to ensure good response and support activities in local languages.

- Symantec's recent release of Symantec Endpoint Protection is 12.1.2 and addressed product support for VMware vShield Endpoint, Mac Mountain Lion and Windows 8, plus the latest small business edition 2013.

- Symantec's endpoint security coverage for mobile devices was revamped to become Symantec Mobile Management Suite, which includes a combination of mobile security, mobile management, and mobile application management.

**Areas of Concern**

- The Symantec endpoint suites were an excellent proposition to take advantage of the company's portfolio within a bundle, appreciating that the European market adopts products at different rates. A midpoint score for elements of its go-to-market subcriteria acknowledges the need for 'total' endpoint integration and hybrid pricing policies plus the need to simplify its product management and integration, in the ways that its competitors are starting to launch and Symantec is currently lacking.

- Despite over $200 million of upside revenues compared to Symantec's closest competitor, the flat revenues in 2011 over 2010 as reported in the 2012 IDC Western European vendor share report caused Symantec to drop market share — (1.6% to 25.9%) as it fell behind the Western European actual regional market growth for the year. Initial revenue data from the 4Q12 IDC Security Tracker continues to show low single digit quarterly year-on-year growth (1.6%), requiring recovery in its full fiscal year 2013 endpoint security revenues

- At the time of writing, IDC is unsure of Symantec's product strategy and has scored the strategy criteria lower as the organization needs to demonstrate its execution and long term investment as it addresses much of its product and route to market concerns that competitors are exploiting, to mitigate the rising challenge to its revenue and dominant vendor position.

- Endpoint security via a cloud/SaaS delivery model needs to be prioritized. Symantec needs to overcome regional resistance and address local datacenter coverage, or suffer the loss of competitive growth.

**Areas of Opportunity**

IDC believes that Symantec can maintain its lead position in the European market if it addresses many of its product and organizational changes identified above and covered in the media for the past five months. The move to higher cloud/SaaS endpoint security delivery is a gap that can address the aspired growth in the SMB space. Acknowledging the growth competitive landscape that sees Symantec as a target for replacement, where flexibility from smaller competitive vendors could be countered with culturally developed back office automation and local autonomy of authority. Symantec's new leadership team's Symantec 4.0 strategy may introduce a new level of vigor and focus on its overall security practice and build many of the concerns outlined above into opportunities for revenue and market growth

### *Trend Micro*

Trend Micro (www.trendmicro.com) has its headquarters in Tokyo, Japan, utilizing a predominately Taiwanese management team, providing its OfficeScan for desktops and laptops and Deep Security for server products. Trend Micro has a heritage of

being extremely capable as a technically proficient organization, which is demonstrated in the delivery of many first to market offerings, such a VShield and MDM/MAM/Mobile security integration across its strategic business regions in APAC and EMEA. Trend Micro has a solid growth base in the DACH region, validating its technical prowess in these countries. The high level of security technical ability is a key essential for prospective customers, as cyber activity becomes more complex and its frequency grows. This is underpinned with the Deep Discovery offering for forensic and pro-active identification of threats in the growing virtual infrastructure environment. Over 40% of Trend Micro's business in Europe is delivered from the SMB business, a position that many other vendors in this competitive and lucrative market would aspire to achieve. IDC positions Trend Micro as a **Major Player** in the Western Europe Endpoint Security Software IDC MarketScape

Trend Micro was equal first in its growth (17%) for endpoint security ($74.6 million) in 2011 as reported in the 2012 IDC Western European SCTM vendor share report, advancing its market share to 3.6%, and only $1.3 million adrift of the vendor above it. Initial revenue data from 4Q12 IDC Security Tracker continues to show good penetration in the non Tier 1 countries, contributing to a 2.6% quarterly year on year growth.

**Areas of Strength**

- Trend Micro's offerings for on-premises and managed services across PCs, Laptops, desktops and servers recognize behavioral malware, that identifies non-signature–based heuristics variances producing consistent high scores in the go-to-market criteria.

- Trend Micro's Control Manager (TMCM) provides a single interface for reporting integration across endpoint and complimentary security products.

- Trend Micro's MDM offering provides coverage across all the major mobile operating systems (iOS, BB, Android, Symbian) with Windows 7/8 on the roadmap, enabling corporate and BYOD implementation.

- Trend Micro's pricing policies are reflected in the delivery and licensing subcriteria as it acknowledges the adoption differences of many organizations in SMB and enterprise segments, providing flexible controls around upgrading and product diversification, including perpetual, subscription, SaaS, and cloud delivery choices.

- IDC views the recent corporate marketing and European organizational changes to have increased the opportunity for the European organization to adjust its tone of voice in marketing, messaging, and channel engagement and a positive enabler to increase awareness and consideration of the Trend Micro endpoint products and solutions in the region. IDC believes that this organizational change will enable Trend Micro to increase its communication subcriteria scoring in the future as it realizes the benefits with some positive product enhancements on the horizon in 2013.

**Areas of Concern**

- Trend Micro appears to punch below its ability within many of the European countries in terms of acquiring new customers, given its high retention rates for existing customers. IDC 's scoring in the channel subcriteria reflects its belief that

a revision of its channel route-to-market strategy, understanding their concerns and positives, could provide a consecutive high actual growth for 2012–2013.

- The development and support for vShield and comparative offerings across the OfficeScan products needs to be escalated to ensure that the company is dealing with device endpoint protection via the targeted device.

- Trend Micro's scoring in the go-to-market strategy criteria was slightly lower than its peers as it needs to consider its positioning of a single policy management interface, rather than just a reporting facility (control manager), as many peer group competitors are driving their roadmaps to meet end-user requirements in this space.

- As an organization that innovates (sometimes too early), there is a disconnect between marketing and product development, minimizing the value that both organizations are providing. Innovation should be linked to market need, appreciating any incubation projects; all other products should either be positively disruptive to the market or meet known customers' needs. The scoring within the market alignment and product appropriateness subcriteria is scored at midpoint, reflecting this disconnect.

### Areas of Opportunity

Trend Micro can widen its go-to-market strategy in the broader European base, without compromising its current focus. Its routes-to-market channel needs a more streamlined message of the issues-based differentiation that the company provides. The coverage of products across the common operational operating systems on all device types provides an opportunity for Trend Micro to steal an opportunity in the mobile and consumerization of IT space against its competitors (if it gets a complimentary single policy management platform to market).

## ESSENTIAL GUIDANCE

### Advice to End Users

- **Consider, Evaluate and Engage.** The European market has some of the most innovative and mature markets in the world. As the MarketScape report has shown, product functionality should only be one consideration when choosing a suitable vendor partnership. You need to balance product suitability with regional support, cultural appreciation, pricing flexibility and speed of resolution (sales, support, signature updates, upgrades, among others)

- **Ensure that you engage with 'integration' vendors.** The efficiency of endpoint security has transitioned from a single point of exposure to a variable set of entry points (pc, mobile, smartphone, etc). You should engage with innovative vendors that can demonstrate how their integrated architectural strategy (not marketing solutions) secure all your endpoints from all ports of entry (web, messaging, apps, etc) as a single [evolving] offering

- **Endpoint security is the last point of defense.** [Experts] are being dismissive that anti-virus products are no longer required and ineffectual in the war against malware. Security has some of the most complex barriers to halt the advance of the hacktivist, but when all is said and done, they succeed, leaving endpoint security as the last line of defense. It is essential that endpoint security attracts a

high level of consideration compared to firewalls, vulnerability, SIEM, and identity among others.

- **Ease of policy and management effectiveness.** Resource intensity is growing as cyber criminals find new ports of entry and complex parallel attacks. Vendors need to minimize the initial and ongoing management of endpoint security offerings, acknowledging the growth in personnel, devices, application usage, and so on, that increases the pressure on the security administrator that may be managing endpoints across geographic boundaries and multiple business departments. Vendors should recognize that organizations will prioritize a vendor with a single policy engine combined with effective product functionality to reduce the opportunity for the cyber activist to find a weak link and breach a device or the user of that device. The end goal is the same — *'increased security posture with minimal endpoint management'* — the architecture is your choice.

## Advice to Vendors

- **Delivery model flexibility is essential.** Two-thirds of enterprises will have deployed some form of cloud/SaaS endpoint offering in the next 24 months, according to IDC's *2011 Cloud Security Survey.* In Europe, where SMBs make up over 90% of the market, the market still requires a mixture of on-premises, software, hardware and virtual endpoint offerings, while transitioning to these new delivery offerings. Choice is still the end user's decision and choosing a single delivery method will minimize your applicability to any prospect's (and existing customer's) security architectural requirements.

- **Simplifying security needs to be communicated.** The MarketScape process unveiled some remarkable developments by vendors to help the end user simplify their complexity of endpoint security. This innovation was not balanced with lasting (longer than a quarter) and effective awareness marketing to the end user, minimizing the positive impact on their security needs and reducing the vendors' ability to be considered. Extended educational and awareness campaigns focused on 'needs-based' content using a mixture of traditional and web 2.0 tools executed with regional 'tone of voice' variants, will provide thought leadership and sustained engagements

- **Mobile is <u>the</u> priority endpoint.** As growth in mobile working and consumerization of IT outpaces traditional PC computing, mobility management and security has been cited as the priority for end users *(IDC #IcUK23586612, July 2012)*. Endpoint security support across all mobile OSs (android, iOS, Windows, BB, Symbian, plus new variants of Linux) should be accelerated to meet end user [multiple provider] adoption, recognizing the need for many within the EU 27 that are at the 'bleeding edge' of mobile commerce device usage due to the lack of fix line infrastructure, as they transition from tactical to essential mobile working

- **Endpoint security barriers to entry are eroding.** The IT Industry expects vendors to focus on the 'main' players, but innovation and a plentiful supply of VC investment have meant that the [market] leaders are no longer the only targets to grow revenues. A full 360 degree appreciation of endpoint offerings from all vendors (geographically and segment focused) that have gained traction by meeting user needs should be evaluated seriously when planning your go-to-market strategies. The past 5 years has seen 'dismissible' vendors become

market forces to be taken seriously, causing leaders that have been complacent with license renewals to lose share.

## LEARN MORE

### Related Research

- IDC's Software Taxonomy, 2012 (IDC #235401, July 2012)
- 2012 End-User Software Trends in Europe (IDC #LC53U, March 2012)
- EMEA Mobile Security Market 2011-2016 Forecast and Analysis (IDC #LM56U, Nov 2012)
- Western European Secure Content and Threat Management Software 2011 Vendor Share: The Imperfect Storm: Unstable Economics, Positive Cloud Adoption, and Increased Attacks Affect the Landscape (IDC #IS02U, July 2012)
- Western Europe Security Software Forecast, 2012-2016 (IDC #IS01U, May 2012)
- Western European Dedicated Private Cloud, 2011-2016: Hardware, Software, Networking and Services (IDC #SR03U, July 2012)
- Mobile Hits Fever Pitch: How are Enterprises Adjusting to the "New Normal" of Mobile? Results from IDC's 1H 2012 Biannual EMEA Enterprise Mobility Survey (#IcUK23586612, July 2012)

### Synopsis

This IDC study is a vendor assessment model called an IDC MarketScape. This is a quantitative and qualitative assessment of the characteristics that explain a vendor's success and challenges in the market. The study assesses the technology capability and business strategy of several distributed server/workload automation vendors in Western Europe.

"Analysis of the Western European enterprise endpoint security market has indicated that IDC believes that this market in Western Europe continues to be a competitive battlefield, with the leaders and major players protecting their market position, while the contenders are expanding their reach into new markets or attempting to maintain a strong hold in the European markets. When assessing the eleven vendors included in this study, the positioning of vendors in the IDC MarketScape clearly indicates their relevance, focus and appreciation of the European markets," said Kevin Bailey, research director, IDC European Security Software. "The integration of endpoint security and other corresponding threat mitigation technologies will change the landscape and prominence of vendors in Europe over the next two to three years".