IDC MarketScape

IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment

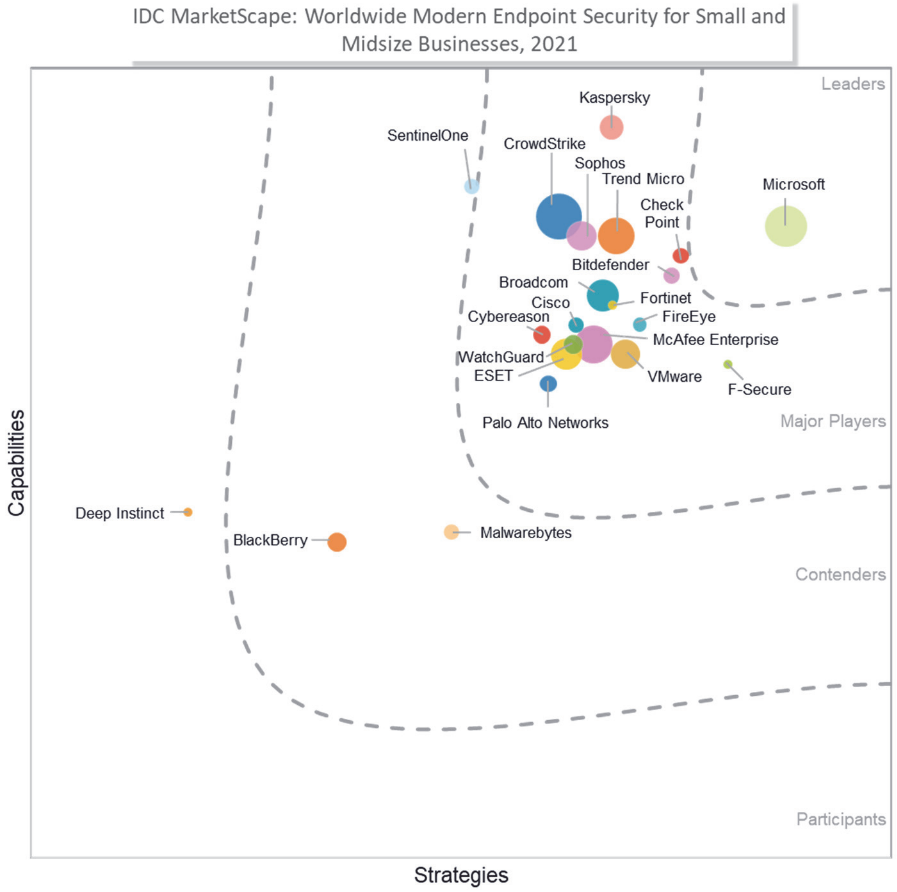
Michael Suby

THIS IDC MARKETSCAPE EXCERPT FEATURES KASPERSKY

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses Vendor Assessment



Source: IDC, 2021

November 2021, IDC #US48304721e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment (Doc # US48304721). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

The endpoint security needs of small and midsize businesses (SMBs) have escalated. A decade ago, signature-based antivirus software was considered an adequate defense in identifying and removing malware from end users' devices. Times have radically changed. Threat actors no longer rely exclusively on dropping malware onto devices to carry out their attacks. Instead, they are more apt to manipulate legitimate software programs, tools, and files (i.e., living off the land attacks). Subsequently, identifying behaviors of malicious intent has become a requirement in mounting an adequate defense.

Identifying malicious behaviors, however, is no simple task. The varied, wide ranging, and complex nature of what end-user devices are equipped to do blurs the distinction between malicious and legitimate behaviors. In addition, threat actors will orchestrate a series of actions, each seemingly benign, to further disguise their presence. Assembling the trail of related actions has become essential in uncovering active attacks and then responding with speed and precision to blunt them.

While this level of attack sophistication may only seem viable when aimed at large enterprises, that is not reality. The economics of cybercrime have advanced such that SMBs are profitable targets. On the cost side, the cyberunderworld has created a marketplace of attack tools, services, and financing that in effect arm perpetrators with more capabilities for less cost.

In addition, digital transformation, while beneficial for SMBs in competing in their respective markets and serving their customers, can also contribute to SMBs' risk of being attacked. Through digital transformation, SMBs have become more digitally dependent, and this dependency spells opportunity for cybercriminals. As the rise in ransomware attacks has demonstrated, disrupting digital-dependent operations can have dire consequences to the victims and produce monetary gains for the attack perpetrators.

The endpoint footprint has changed. Spurred by the pandemic, work has also migrated from one location for many to many locations of one. Existing outside the perimeter defenses of business locations but also being online, devices used by the remote workforce and the users themselves have become more attractive as exploitable targets for cybercriminals and nation-state adversaries.

Building up endpoint security is critical. Modern endpoint security (MES) products, the combination of endpoint protection platforms (EPPs) for deterministic prevention and endpoint detection and response (EDR) for post-compromise reaction, are the latest evolution in endpoint security designed to combat threats aimed at endpoints. It is confirmed through IDC research that the demand for modern endpoint security is on the rise among SMBs.

Like enterprises, SMBs recognize that layers of complementary and compensating security technologies are essential. This is true whether the objective is to protect a location or a scattered inventory of endpoint devices. But unlike enterprises, SMBs often lack the financial and security talent resources necessary to effectively utilize layers of security technologies and engage with multiple security vendors. Simplicity without sacrificing security efficacy in thwarting today's and tomorrow's threats is what SMBs require.

The vendors included this IDC MarketScape offer modern endpoint security solutions that serve this objective.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Participating vendors met the following criteria:

- From a single endpoint software agent, the vendor's modern endpoint security product supports both endpoint protection platform and endpoint detection and response.
- End-user personal computing device platforms supported by the modern endpoint security product must, at minimum, include the latest versions of Windows and macOS.
- Vendor began selling modern endpoint security products to customers from January 2019 or earlier.
- Sales to commercial and governmental customers of EPP (also referred to as antivirus or next-generation antivirus), EDR, and modern endpoint security products must, at minimum, totaled $30 million (following generally accepted accounting principles [GAAP]) in calendar year 2020.
- At year-end 2020, the vendor's percentage of customers with less than 2,500 protected endpoints exceeded 50%.

ADVICE FOR TECHNOLOGY BUYERS

SMBs are fortunate in that there are many capable vendors offering MES products. In addition, all vendors are actively enhancing their products. What these products deliver in the future will be more than what they deliver now. This is reassuring as threat actors will continue to advance their tradecraft and the cost and availability of security talent will remain ongoing challenges. SMBs, in essence, need and should select a vendor that can effectively adapt to a changing threat landscape while minimizing the additional time and operational duties borne by SMBs' limited security staffs. IDC offers the following advice for modern endpoint security buyers.

- Focus first on MES fundamentals:
  - Protection efficacy. IDC buyer analysis shows that SMB's top consideration in choosing a MES vendor is its research into never-before-seen threats and attack tactics. But buyers are not content with just research, they want results. There is no better result than automatically and deterministically blocking new forms of attacks. Independent evaluations on protection efficacy are useful guides in this regard but are not the panacea. IDC recommends conducting proofs of concepts (POCs). We further recommend that EPP POCs should become a routine activity. With existing vendors evolving their EPP capabilities and new vendors emerging with "next generation" approaches, comparative analysis in your environment is the best litmus test. Keep in mind that other SMBs started their search for a more effective MES product after they suffered a serious security

incident. Better to avoid this circumstance by making EPP POCs a routine practice and then acting on your assessment (e.g., augmenting with another vendor's product or replacing an existing product). This practice will assist in lessening the likelihood of attacks escalating into serious security incidents and in curbing the alert and incident inflow into EDR.

  - EDR automation. Second on the list of buyers' vendor selection criteria is incident investigation's speed and ease. The unfortunate reality is some attacks will evade the immediate preventions of EPP and establish a footprint on endpoints. Security teams need to be prepared. But just having EDR functionality is not enough, human engagement is required. Concentrating human engagement more on decision making and less on investigatory processes is vital in lessening threat actors' dwell time and the time required of your security personnel. Therefore, automation is essential and is present in various forms, such as assembling and cross-correlating relevant data, visualizing attack sequence, devising risk-rated responses, and executing on the chosen responses. In addition, SMBs cite automated threat hunting as a highly important factor in considering a MES vendor. Conducting a POC is the most effective means for evaluating the vendor's level of automation and usability fit with your security personnel.
  - Device support. MES products can only deliver EPP and EDR capabilities on endpoint device types and operating systems (OSs) that their software agents support. Obviously, you will want to confirm support for the device types and OS platforms that are in your environment. All vendors in this IDC MarketScape support recent OS versions of Windows and Mac. But Windows and Mac PCs are not the only device types attacked. Mobile devices, physical and virtual servers, and cloud workloads are also targeted. While vendors' datasheets list supported device types and OSs, IDC recommends digging deeper into feature parity and feature distinction to ensure the vendor's product is adequately equipped for all of your devices and provides unified management.
- Examine cross-function integration. Endpoint security and endpoint management functions are intertwined. Unpatched and out-of-date software applications and OS versions are targets of exploitation by threat actors. When exploited, EPP and EDP become the next two layers of compensating security. Logically, systematic patching reduces exploitability. However, budget for a dedicated patch management product and/or personnel to oversee patching may be lacking at your firm. An alternative that may be less costly, less administratively taxing, and can natively integrate patching into attack mitigating or remediating responses is the patch management capabilities offered by MES vendors in their solution suites. In addition, patch management is one of several functions that reduces an endpoint's attack surface and, consequently, exploitability. Other functions include device control, host firewall management, vulnerability assessment, microsegmentation, and application blacklisting, whitelisting, and process-level allow listing. In your consideration of MES vendors, comparing their collection of attack surface reduction capabilities with those of dedicated products may reveal an effective and possibly a more affordable approach to strengthening your security posture.
- Evaluate eXtended Detection and Response (XDR) frameworks. Reaching a complete and speedy understanding of attacks affecting endpoints may require more than telemetry gathered from endpoints running a MES software agent. Telemetry from other sources (e.g., network sensors, perimeter defenses, email and web gateways, cloud access security brokers, and identity management services) can bring in beneficial context. Many of these sources can also be control points for applying attack-mitigating responses and in refining security policies. An oversimplified description, this is the realm of extended detection and response. Nearly all vendors in this IDC MarketScape have an XDR framework that encompasses their non-endpoint security product portfolios, ecosystem partners, or a combination of both. As part of

your assessment of MES products, evaluate the vendor's current state of XDR, future developments, and incremental security value and what a transition from EDR to XDR will entail (e.g., additional cost, technology upgrades, and staff training and augmentation).

- **Question ransomware defenses and recovery options.** The consequences of ransomware incidents are a top-of-mind concern for business leaders, and for good reason. According to IDC's July 2021 *Future Enterprise Resiliency and Spending Survey, Wave 6,* 75% of IT decision makers with organizations that experienced one or more ransomware incidents in the past 12 months indicated that significant extra resources beyond what internal staff handled were required to rectify. Ransomware, like other forms of malware, frequently enters business networks through endpoint devices. Subsequently, endpoint security products, like MES, are a vital line of defense. But just as ransomware has evolved to evade detection and ultimately increased the likelihood of payment and amount of ransom payment, MES products must also evolve to detect ransomware and prevent its execution (e.g., data exfiltration and file encryption) and propagation to other endpoints and critical systems. IDC recommends that you query MES vendors about their ransomware defenses and incident recovery options for returning affected files and endpoint configurations (e.g., changes to registry keys) to their previous known good state. As you do, assess these capabilities within the context of your overall business cyber-resiliency plans.
- **Gain perspective on incorporation of built-in device security capabilities.** Worth repeating, threat actors will evolve how they conduct attacks. They will continuously probe for new avenues to enter and takeover endpoints. While not yet a mainstream avenue, attackers compromising the device's firmware is a possibility. Rather than react to this possibility once it becomes reality, ask MES vendors about their approach to confirming firmware integrity and restoration. Also ask about leveraging the device's chip-based processing features in conducting or augmenting MES functions. Eventually, the measuring stick for endpoint security solutions may entail the collaboration of built-in device security with overlay on-device security software augmented with cloud-powered features. To make security-maximized decisions on device and MES product purchases, ask MES vendors about their current and planned approaches to leverage built-in device security features.
- **Consider managed services options.** Although MES vendors have and will continue to automate and simplify the use of EDR, experienced security professionals are needed to produce maximum return on EDR's capabilities. IDC recommends that you consider the managed service options offered by MES vendors and/or their channel partners. As service needs vary by level of engagement (e.g., from on-demand collaboration to around-the-clock outsourcing) and tasks performed (e.g., threat monitoring, threat hunting, and threat response), seek a managed services arrangement that best aligns with your current needs and budget but is also flexible to adjust for changing circumstances.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Kaspersky

Kaspersky is positioned in the Major Players category in the 2021 IDC MarketScape for worldwide modern endpoint security for small and midsize businesses.

A prominent security vendor operating worldwide, Kaspersky has expanded its security product suite beyond its endpoint security roots. Its current product suite includes inline security for the common threat vectors of email and web. The company also offers security products for ICS, IoT, and network attached storage and offers fraud prevention. Kaspersky is not solely products, it has an expanding suite of services spanning assessment, training, threat intelligence, incident response, and detection and response. Focused on cross-product and service integration and reuse of a common technology base, Kaspersky's approach to new product introduction, feature expansion, and service process design and staffing is from within rather than through acquisitions.

Strengths

Capabilities of Kaspersky's modern endpoint security product are very competitive with no material deficiencies.

The company is among the most tested for EPP capabilities.

With its expanding and internally developed product suite, the company is well positioned to offer SMBs a natively integrated cross-product solution.

Kaspersky also offers a comprehensive set of attack surface reduction management functions natively integrated into its MES product (vulnerability, patch, device, and host firewall) and administrative console.

Platform support is expansive and includes cloud workloads. On personal computing device, the only gap is lack of support for Chromebooks. However, Kaspersky is not alone, only a small subset of MES vendors currently support Chromebooks.

Kaspersky offers a range of endpoint security products distinguished by different feature sets and not all meeting IDC's strict definition of MES. Nevertheless, with double-digit annual customer growth with its non-MES products, Kaspersky is building a strong pipeline of upgradable customers to its MES products.

Representing an additional and real-time source of threat intelligence, Kaspersky is a major provider of digital life protection products for consumers.

Kaspersky leverages its profitable operations to fuel product expansion and enhancement.

Challenges

Missing from Kaspersky's product portfolio is cloud security gateway (Cloud Access Security Broker). Consequently, SMBs that rely on this gateway as one of their security policy control points must engage with another vendor's product.

A subset of vendors utilizes Intel's Threat Detection Technology for firmware integrity monitoring; Kaspersky does not. It contends its technology delivers similar if not better security benefits.

With a customer footprint concentrated in EMEA, LATAM, and APAC, Kaspersky is at a disadvantage to larger vendors with greater U.S. presence in catering to United States-based SMBs.

Consider Kaspersky When

SMBs dissatisfied with the security efficacy of their current EPP product and are looking to step up their endpoint security capabilities into EDR and reduce their number of standalone products (e.g., vulnerability and patch management), Kaspersky is a solid contender. In addition, Kaspersky's managed detection and response service and tiered packaging allow SMBs to strengthen their security operations without needing to change or add vendors.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, 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 menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will 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 decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape 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 discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Modern endpoint security products protect personal computing devices (PCDs) (such as workstations and laptops) from cyberattacks through the detection of malicious code and behaviors present or operating within the PCD and then facilitate a counteracting response (e.g., block, remove, or isolate). Modern endpoint security products contain two detect and response mechanisms differentiated based on elapsed time and human involvement. Endpoint protection platforms (EPP) reach detection verdicts and initiate responses in real time and autonomously (i.e., without human involvement). Endpoint detection and response (EDR) is a second stage of detection and response for cyberattacks that have evaded EPP detection. With EDR, the time to reach detection verdicts and initiate responses can span minutes to days. How fast the cyberattack unfolds, its sequence of steps, and its sophistication and uniqueness are factors that affect the elapsed time in detection and response. Automation and predefined workflows assist in reducing the elapsed time. Security analysts (humans) are typically involved, at minimum, to confirm detection and/or authorize response.

LEARN MORE

Related Research

- *Top Technology Integration Opportunities for Unified Endpoint Management* (IDC #US48266821, September 2021)
- *Market Analysis Perspective: Worldwide Tier 2 SOC Analytics, 2021 — Where the Puck Is Going* (IDC #US47394921, September 2021)
- *Market Analysis Perspective: Worldwide Corporate Endpoint Security, 2021* (IDC #US48208121, September 2021)
- *IDC's 2021 Ransomware Study: Where You Are Matters!* (IDC #US48093721, July 2021)
- *Which Criteria Rank Highest in the Evaluation of Modern Endpoint Security Products?* (IDC #US48053021, July 2021)
- *Worldwide Corporate Endpoint Security Forecast, 2021-2025: On a Higher Growth Trajectory* (IDC #US47957021, June 2021)
- *Worldwide Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth* (IDC #US47768021, June 2021)
- *Insights from IDC's EDR and XDR 2020 Survey: Operational Challenges and Initiatives Are Abundant* (IDC #US47357921, January 2021)

Synopsis

This IDC study represents a vendor assessment of providers offering modern endpoint security for small and midsize businesses through the IDC MarketScape model.

"Modern endpoint security products, the combination of deterministic protections and post-compromise detection and response, are rapidly becoming an essential component to small and midsize businesses' cybersecurity arsenals," states Michael Suby, research vice president, Security and Trust at IDC. "Reliance on a basic endpoint security product is a risky proposition with today's advanced threats and the business harm that can inflict. Favorably for SMBs, there are many vendors with capable modern endpoint security products. Selecting a modern endpoint security product and optimizing its use, however, can be a challenge for SMBs due to their acute budget, time, and talent constraints. To alleviate these constraints, IDC's recommendation for SMBs is to first focus on the fundamentals of what a MES product is designed to accomplish and then assess ease of use, integration, and collaboration with other security technologies that strengthen security posture and the option of managed services. Finally, modern endpoint security products are continuing to advance in their capabilities. While a time-consuming effort, SMBs should conduct proofs of concept routinely to ensure their limited security budgets are well spent."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com