IDC MarketScape

IDC MarketScape: Worldwide Modern Endpoint Security for Small Businesses 2024 Vendor Assessment

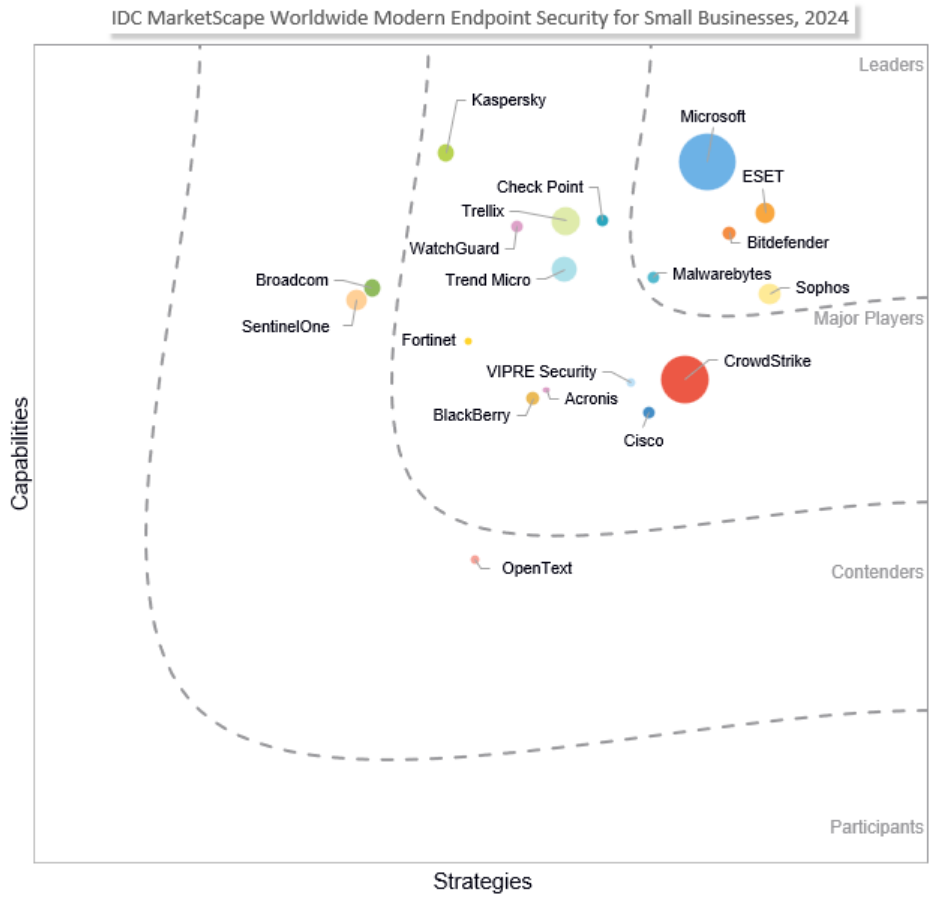
Michael Suby

THIS IDC MARKETSCAEP EXCERPT FEATURES ESET

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Modern Endpoint Security for Small Businesses Vendor Assessment



Source: IDC, 2024

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

March 2024, IDC #US50521424e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Modern Endpoint Security for Small Businesses 2024 Vendor Assessment (Doc # US50521424). 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.

IDC OPINION

Over the past decade, endpoint security has been transforming from discrete point products to multifunction platforms. This transformation is directly attributed to a primary cause followed by a mitigating effect:

- **The cause: End users and their devices are inherently attractive targets because they are inherently exploitable.** Each is a unique and dynamic system. Whether the system consists of hardware (HW), firmware, operating system (OS), and applications or represents a collection of human experiences, knowledge, biases, and circumstantial reasoning, complexity and change reign over sameness and stability. Consequently, the number of individual end user and device interactions and interaction sequences is boundless. As such, completely and accurately identifying and permitting only legitimate interactions while preventing all other interactions is, in practice, impossible. There will always be a gray zone of uncertainty between the legitimate and illegitimate. This gray zone has afforded cyberadversaries ample room to operate. And with end users and their devices being externally accessible, virtual gateways to higher-value internal assets, cyberadversaries also have ample justification to target and exploit them.
- **The effect: Multiple layers of security technologies are needed to shrink the gray zone and effectively react when adversaries compromise devices or manipulate end users into unknowingly supporting their exploits.** In addition, over the past decade, endpoint protection platforms (EPPs) and endpoint detection and response (EDR) solutions have advanced to battle an adversary that is incrementally evolving its techniques to evade protection schemes and obscure its movements and intentions. The proverbial cat-and-mouse game never ends. And while EPP and EDR form the basis of modern endpoint security (MES) solutions, they are not enough. Modern endpoint security solutions are evolving to become broader multifunction platforms that marry EPP and EDR together and add technologies that extend the string of functionality to include posture-strengthening prevention and post-attack recovery.

The value of these multifunction platforms is not in superficial packaging of point products. Rather the value is realized through an optimized assembly of technologies that streamlines security operations from prevention through recovery and leverages incident response (IR) experiences to fortify prevention and protection. In establishing this continuous improvement cycle, organizations are systematically shrinking the gray zone and elevating their ability to preempt cyberattacks.

As appealing as the value of multifunction platforms appears, small businesses (less than 100 employees) will not instinctively gravitate to these platforms unless these platforms also directly address their pressing constraints in reaching their cybersecurity goals. For most small businesses, compared with larger organizations, they do not have the time or expertise to tune the platform for their circumstances and monitor for and respond to cyberincidents. Their need is not just what the platform can deliver but how delivery occurs.

Considering the how, we contend that operational simplicity and functional reliability are among the primary attributes small businesses will consider in their evaluation of multifunction endpoint security platforms. In addition, driven by limited in-house resources to monitor for and respond to complex cyberincidents, we also contend that small businesses will assign greater importance to prevention and protection functional capabilities than to detection and response and recovery capabilities (refer to the criteria weights in Table 2).

Operational simplicity and functional reliability are also relevant in overcoming small businesses' budgetary constraints. Vendors, in our opinion, need to position the price of their multifunction platforms in terms of overall value. Demonstrating that the platform can be operationalized by current staff and that each function, particularly prevention and protection, consistently performs as intended is a demonstration of value. Also, value pricing should also entail cost certainty for small businesses. A pricing structure that favors per unit versus variable is advisable. Per unit does not preclude higher prices for additional functionality. Provided value is demonstrated, an increase in per-unit price is justified.

Often the case, the sales and servicing path for MES vendors to small businesses is through value-added resellers (VARs). VARs, however, are not uniform. They vary in employee size, geographic footprint, targeted industries, investments in security expertise, and maturity in selling and servicing cybersecurity solutions to small businesses. Those differences notwithstanding, we contend that the same platform attributes that appeal to small businesses — operational simplicity, functional reliability, and predictable pricing (in this case, what the VARs pay the vendor for products it sells and commission structure) — are also universally aligned with the business goals of VARs. We also add that vendor-provided life-cycle management tools (enrollment, installation, configuration, monitoring, management, and reporting) need to be easy for VARs' staffs to master and support multitenancy.

The number of small businesses is significant and so too is the market opportunity to elevate their level of cybersecurity readiness and resiliency. Multifunction endpoint security platforms will, in IDC's opinion, be essential cybersecurity infrastructure for nearly all small businesses. The challenge for vendors targeting small businesses and VARs that service small businesses is devising a product and sales channel strategy that appeals to both of these constituents, evolving that strategy as circumstances warrant, and minimizing conflict with the vendor's large business strategy and friction with its VARs.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Participating vendors met the following criteria:

- Offer a software product or products that deliver endpoint protection platform capabilities or endpoint detection and response capabilities, or combined EPP and EDR capabilities according to the description included in the Market Definition section (If the vendor offers products that are promoted as extended detection and response [XDR], those products qualify if EDR capabilities are fully included in the XDR products.)
- Support end-user devices that run the latest general availability (GA) version of Windows and macOS
- Had product sales in calendar year 2022 to the small business segment (less than 100 employees worldwide) of at least $20 million

ADVICE FOR TECHNOLOGY BUYERS

The reality for small businesses is similar to that for larger businesses. Small businesses are just as likely to have digitally transformed their operations as large businesses have done and, with that, broadened and deepened their dependency on a digitalized environment. Also confronting both small and large businesses, the cyberthreat landscape has transformed. Once principally consisting of simplistic attacks broadcasted indiscriminately, the commercialization of the cyberunderworld and advanced technologies have made sophisticated targeted attacks profitable at scale for cybercriminals. This combination of broad and deep digitized business environments and commercialization of the threat landscape places underprepared small businesses as susceptible to destructive cyberattacks as underprepared large businesses. As such, the reality for small businesses is that they cannot ignore the need to strengthen their cybersecurity readiness and resiliency. While there are many components to an effective cybersecurity strategy, a comprehensive approach to endpoint security is essential. For that, we strongly recommend consideration of multifunction endpoint security platforms.

A democratizing benefit of these platforms for small businesses is in mimicking the size advantage of large businesses and enabling small businesses with more affordable access to similar cybersecurity functionality used by large businesses. For larger businesses, their larger size affords them escalating scale economics. Simplistically, they can spread the costs of cybersecurity products and security personnel over a larger base of employees and assets. For the same cybersecurity functionality, larger businesses have a lower per-unit cost. Furthermore, the per-unit incremental cost in upgrading cybersecurity capabilities is less and that contributes a lower threshold in proving business case justification. In a race to be better prepared to combat cyberattacks, larger businesses have a scale advantage, and that advantage, perversely, places smaller businesses that have underestimated cyberthreats and have been slow to strengthen their cybersecurity readiness at greater risk.

Partially driving the affordability of multifunctional endpoint security platforms is cloud economics. While the majority of endpoint security activity occurs at the endpoint in software (i.e., autonomous detection, blocking, and policy enforcement), collaborating with the endpoint software agent in support of post-compromise functionality (e.g., EDR), setting and propagating security policies, directing posture strengthening actions, and life-cycle management of the agent is conducted in and from the cloud. Servicing the vendor's customers, small and large, the vendor gains scale economies to expand accessibility and improve affordability of endpoint security functionality for all customers. In addition, the pervasiveness of cloud operations by virtue of being hosted in one or several of the major cloud provider platforms mitigates network latency and resource contention in agent-cloud collaborative operations.

In evaluating multifunction endpoint security platform options, small businesses should also consider who will be responsible for operational management. While MES vendors have driven high-confidence automation into their platforms' functionality, human engagement is still required, such as to detect and respond to highly evasive attacks, monitor and modify security configurations and settings, and make decisions on risk-mitigating actions that have the potential to adversely impact business operations.

If your choice is to fully own these responsibilities, our advice is to evaluate the ease and effectiveness that these responsibilities can be completed by your staff. In addition, evaluate the comprehensiveness of the platform, paying close attention to tasks that require your staff to manually gather information from other sources or pivot to another management console.

If your choice is to comanage with a managed service provider (SP) or fully outsource these responsibilities, you are in a beneficial position as management options have been expanding in managed services offered by the vendor and those offered by the vendors' VARs. Although there is an incremental cost for these managed services, our advice is to judge this cost against the unrealized benefits of optimized utilization of the endpoint security platform's capabilities and the potential costs associated with business-impacting cyberattacks.

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.

ESET

ESET is positioned in the Leaders category in the 2024 IDC MarketScape for worldwide modern endpoint security for small businesses.

ESET earned its longevity and durability as a private entity by continuous evolution in its security capabilities in support of public and commercial organizations and its channel partners.

Strengths

The expansiveness of ESET's endpoint security-focused product portfolio is a principal strength. IDC commends ESET in terms of the following capabilities:

- Number of endpoint protection functions (host-based FW and IDS/IPS, DNS filtering, device control, DLP, and device encryption) with half of these functions offered as standard features
- In-browser policy controls
- Antiphishing protections
- Anti-tampering precautions
- Intel TDT integration (introduced in early 2022)
- Mobile threat detection
- Customer security advisory recently enhanced with the commercial launch of device vulnerability management and patch management and integration with Microsoft Intune

As an active participant in independent product evaluations, ESET consistently receives competitive results in terms of protection and performance as well as in EDR.

Go-to-market partnerships have also contributed to ESET's market momentum and in expanding geographically. The addition of RESTful APIs in 2023 will directly contribute to new integrations with other security providers in the future. Also, riding on the heels of a successful strategic relationship with Canon Japan, ESET and Canon India form their own strategic relationship.

Pertaining to ESET detection and response capabilities, automated resolutions for ESET-curated detections are now included in ESET Inspect, the company's detection and response product. With threat intelligence an essential ingredient in detection and response, ESET joined the Joint Cyber Defense Collaborative (JCDC) in early 2023 as a partner in threat intelligence sharing. In addition, with

a sizable consumer customer base, ESET is well positioned to leverage insights gained in protecting consumers in serving its business customers.

ESET is also a member of the App Defense Alliance, an alliance launched by Google in 2019 to protect the safety of apps available in the Google Play Store. ESET's detection engine is used to actively scan the Google Play Store for existing and emerging cyberthreats. Also pertaining to Google, ESET is extending the ESET Cloud Office Security beyond Office 365 to include Google Workspace.

Challenges

ESET's large and growing base of small business customers is a testament to the company's focus and execution. As expanding and enhancing product capabilities is a necessary and continuous endeavor in which ESET has excelled, ESET needs to also equally excel in capabilities that help its sales channel partners succeed in the competitive small business segment. ESET's planned introduction of ESET Protect Hub, a one-stop account portal for channel partners, and the January 2024 introduction of ESET MDR are favorable developments in supporting channel partners.

Consider ESET When

With extensive capabilities in prevention and protection, maturing capabilities in detection and response, and upcoming developments tailored for channel partner success, ESET is a strong consideration for small businesses and VARs that service small businesses.

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 (e.g., workstations/PCs and laptops) and mobile devices (e.g., smartphones and tablets) from cyberattacks through the detection of malicious code and behaviors present or operating within the devices and then facilitate a response (e.g., block, remove, or isolate).

With increasing commonality, modern endpoint security products combine detection and response mechanisms differentiated based on elapsed time and human involvement. Endpoint protection platforms (EPPs) reach detection verdicts and initiate responses in real time and autonomously (i.e., without human involvement). Endpoint detection and response (EDR) is the 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 the minimum, to validate detections and/or authorize responses.

Managed EDR (also categorized in the broader context as managed detection and response [MDR]) entails a third party that provides operational support for the EDR product, and it has been a growing services category. In estimating the size of the modern endpoint security market, vendor revenue for managed EDR is included when vendor-provided services are included in the same SKU as the EDR products and services, which are contractually sold together (i.e., multiple SKUs in a single contract agreement) or are sold as an "inclusive" package. Regardless of arrangement, the commonality is the purchase of the vendor's managed EDR service is packaged with and contingent upon the purchase of the vendor's EDR product.

Modern endpoint security suites may also accomplish more than detecting malicious code and behaviors and initiating mitigating responses. They may include capabilities that thwart threats during the initial stages of an attack and reduce the endpoint's attack surface area and exploitability. Early-stage attack prevention and surface area reduction capabilities vary by vendor and include, but are not limited to, URL filtering; hardening of device, OS, and application controls; file sandboxing, sanitization, and integrity monitoring; browser isolation; application allowlisting; antiphishing; DLP and data-at-rest encryption; vulnerability assessment and patch and software management; policy configuration of host-based firewall and intrusion detection functionality; and deception. Modern endpoint security suites are included in IDC's sizing of the modern endpoint security market if the suites are sold as a package/single SKU with EPP, EDR, or combined EPP and EDR functionality.

LEARN MORE

Related Research

- *What Do Four Recurring Surveys Tell Us About Trends in Ransomware Incidents?* (IDC #US51857624, February 2024)
- *IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024 Vendor Assessment* (IDC #US50521323, February 2024)
- *IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 Vendor Assessment* (IDC #US50521223, January 2024)
- *Worldwide Corporate Endpoint Security Forecast Update, 2023-2027: Endpoint Security Platformization Propels Robust Growth* (IDC #US51606823, January 2024)
- *IDC MarketScape: Worldwide Cyber-Recovery 2023 Vendor Assessment* (IDC #US49787923, November 2023)
- *IDC MarketScape: Worldwide Risk-Based Vulnerability Management Platforms 2023 Vendor Assessment* (IDC #US50302323, November 2023)
- *Worldwide Modern Endpoint Security Survey, 2023* (IDC #US51241623, September 2023)
- *2022 Endpoint Security Survey – Permanent Exclamation Point on Endpoint Security's Strategic Relevance* (IDC #US49349123, August 2023)

Synopsis

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

"Modern endpoint security products have evolved from point products to multifunction platforms that entail more than EPP and EDR functions to include additional capabilities in prevention and postattack recovery," according to Michael Suby, research vice president, Security and Trust at IDC. "Small businesses should not underestimate the potential and impact of cyberincidents and take action now to reassess their endpoint security readiness."

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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

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