IDC MarketScape

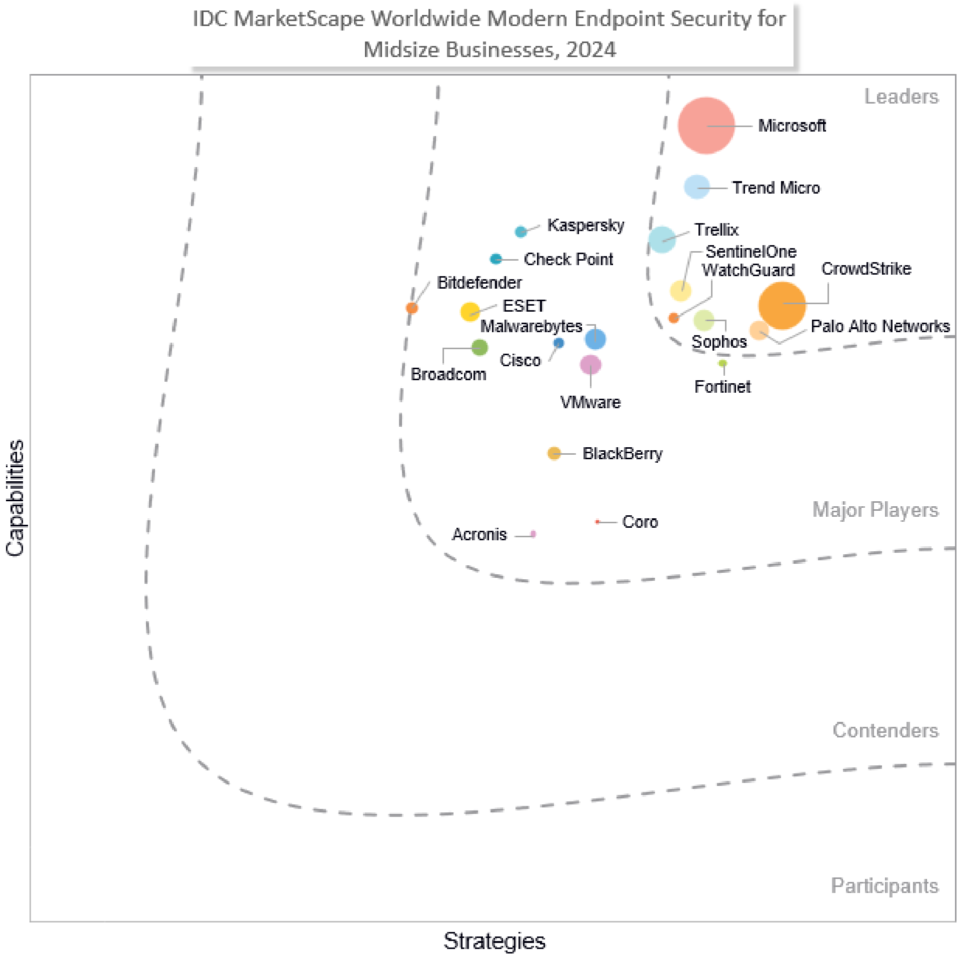
IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024 Vendor Assessment

Michael Suby

THIS IDC MARKETSCAPE EXCERPT FEATURES WATCHGUARD

IDC MARKETSCAPE FIGURE

IDC MarketScape Worldwide Modern Endpoint Security for Midsize Businesses Vendor Assessment



Source: IDC, 2024

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

February 2024, IDC #US50521323e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Modern Endpoint Security for Midsize Businesses 2024 Vendor Assessment (Doc # US50521323). 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.

Spanning organizations with 100-2,499 employees, what "security operations" actually entails can vary significantly. Criticality of end-user devices in business operations, risk tolerance, regulatory requirements, current level and future aspirations regarding their cybersecurity acumen, and spending limits are defining variables in the role security operations plays at each midsize business. As an enabling technology of security operations, these same variables also influence the attributes each midsize business assigns to multifunction endpoint security platforms.

Vendors' sales channel partners are also not uniform. For them, desired platform attributes reflect the needs of their customers, the value they present to their customers and prospects, and their business objectives (e.g., growth and profitability).

Endpoint security platforms vendors, in turn, must make platform-defining decisions based on the customers they directly serve and those they indirectly serve through their channel partners. Given the diversity within the midsize business segment, IDC's opinion is that no single vendor can build a generalized multifunction endpoint security platform that excels in meeting the needs of each midsize business customer and each channel partner. Each vendor must tailor and evolve its platform and go-to-market strategy to the needs of a definable subsegment within the broader midsize business segment.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Participating vendors met the following criteria:

- Offers 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.)
- Supports end-user devices that run the latest general availability (GA) version of Windows and macOS
- Had product sales in calendar year 2022 to the midsize business segment (100-2,499 employees worldwide) of at least $45 million

ADVICE FOR TECHNOLOGY BUYERS

The midsize business segment is an increasingly competitive market. It represents a confluence of several vendor types. Tenured MES vendors that have concentrated on enterprise-size customers are attracted to the growing enterprise-grade needs of midsize businesses. Separately, leveraging their experiences in serving small businesses, endpoint security vendors tenured in this segment sense growing market opportunity among midsize businesses for MES solutions that deliver more security functionality with the simplicity and low engagement attributes small businesses have required. Entering with network security pedigrees, vendors of network security products have added to and matured their MES offerings in a bid to be among the small set of core security vendors for midsize businesses. Last, MES vendors with existing and sizable concentrations of midsize business customers are preempting customer departures and deepening relationships by proactively evolving their MES offerings in step with changing customer needs and circumstances.

For midsize businesses and value-added resellers that serve this segment, times are favorable. Viable vendor choices are expanding, and all MES vendors are in a perpetual race for long-term relevancy. In addition, all MES vendors have internalized that reliance on their past accomplishments to drive new customer demand or retain existing customers is inadequate. To be and remain relevant in the MES market, each vendor must continuously evolve and advance its MES offerings and value proposition.

In taking advantage of this highly competitive MES market, IDC advice to buyers is to uplevel the relevancy of MES into the broader context of cyber-resiliency by following these steps:

- **Assess your current state of cyber-resiliency:** Your organization's digital footprint has likely changed and your organization's operational dependency on digital technologies has likely deepened. Not just likely but certain, cyberthreats have advanced in sophistication and potency. Assuming your organization has a suitable mix of cybersecurity technologies optimally configured and supervised to combat both mainstream and targeted cyberattacks could be fatal. With end users and their devices opportunistic cybertargets, objectively assessing your cyber-resiliency should include your organization's choice and use of a modern endpoint security platforms.
- **Evaluate options to fortify cyber-resiliency:** With gaps in cyber-resiliency pertaining to endpoints identified, ascertain if the gaps are due to lacking or limitations in current MES capabilities, underutilized MES capabilities, or both. If your role includes endpoint security, you probably already have a good sense of where to attribute the gaps. The logical next step is to assemble and evaluate options to mitigate these gaps.
- **Implement, monitor, and adjust:** Whether adding new MES capabilities, changing MES vendors, or refining how your existing MES platform operates, effectively managing change is essential to reaching your gap-mitigating objectives. However, dynamic circumstances in the threat landscape, your organization's endpoint estate, and possibly your organization's level of risk tolerance demand that assessing state of cyber-resiliency and adjusting should be a periodic if not a continuous activity.

While these steps are logical, the reality for many midsize businesses is they are not equipped with sufficient time and talent to objectively assess their organization's state of cyber-resiliency and fortify that state except on an infrequent basis or worse, after a damaging cyberincident. Fortunately, there are alternatives to overcome time and talent limitations. Those alternatives include service engagements offered by MES vendors or their value-added reseller (VAR) partners. Adding to the services option is advisory capabilities included in or offered with the MES platform.

IDC views vendor developments in platform-included advisory capabilities positively in aiding security practitioners in elevating their utilization of the preventive and protective capabilities present in their existing platform investments, reducing alert volume, and averting cyberincidents. Our advice in your evaluation of MES platforms is to examine current and upcoming advisory capabilities.

VENDOR SUMMARY PROFILE

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.

WatchGuard

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

Nearing four years since acquiring Panda Security and three years since introducing WatchGuard Endpoint Security, WatchGuard's accomplishments in melding modern endpoint security into the company's broader product portfolio have become more apparent. One notable example is the WatchGuard Endpoint Security add-on modules (Vulnerability and Patch Management, Full Encryption, Data Control, and Advanced Reporting Tool), which individually and collectively assist midsize businesses in lessening their susceptibility to security incidents and data breaches. These modules augment WatchGuard's Zero-Trust Application Service in attack surface reduction. Included in all WatchGuard's endpoint security products, this service classifies all applications and binaries as either malicious or benign. With 99.9% automatic classification and the rest through human-led analysis, WatchGuard states this service has eradicated file-based infections and eliminated suspicious file alerts.

Another aspect of these add-on modules is in bridging the disciplines of endpoint security and endpoint management together. This discipline bridging is present in WatchGuard's Advanced Reporting Tool, which is equipped with information and tooling to assist organizations in managing software licensing costs, controlling bandwidth consumption, and monitoring use of noncorporate applications. Benefitting WatchGuard customers and channel partners (e.g., managed services providers), the Advanced Reporting Tool and the endpoint security add-on modules are manageable from the same administration console and through the same agent that powers WatchGuard's EPP and EDR functionality.

Another example is WatchGuard's advancements in cyber-risk assessment. From the same dashboard, administrators are presented with a prioritized list of detected risks and affected devices. Detectable risks include patch status, disabled or absent protection controls including anti-tampering protection, and recent indicators of attack. From identified and prioritized risks, administrators can pivot to mitigation. Elevating market awareness and providing its channel partners with an attractive door opener, WatchGuard offers free access to cyber-risk reporting for a 60-day period.

A relevant and recent example of cross-product integration is in access control between endpoint security and WatchGuard's network security products. Specifically, WatchGuard Firebox and Wi-Fi access points can query WatchGuard endpoint security agents before establishing VPN connections.

FlexPay highlights another flavor of integration: account billing. FlexPay offers channel partners multiple payment term options (e.g., fixed term, prepaid, pay as you go) that can be applied to groups of end customers or at the individual end customer level. Integration comes in as the selected payment term applies to the combination of all WatchGuard software and hardware products.

Strengths

WatchGuard has a broad and broadening product portfolio that includes the aforementioned endpoint security add-on modules and other endpoint security capabilities in mobile threat defense, server security, and cloud workload security. The company also recently added NDR and XDR capabilities with its CyGlass acquisition that was finalized in September 2023.

WatchGuard has a comprehensive set of endpoint protection technologies (host-based firewall and IPS/IDS, DNS filtering, device control, DLP, and disk encryption).

Demonstrating an ability to cross-sell endpoint security in the midsize business segment, WatchGuard Endpoint Security has a high and growing concentration of midsize business customers. WatchGuard's financials are also in a strong position to fund ongoing development in endpoint security and partner-enhancing initiatives.

Challenges

Although WatchGuard's MES market presence is growing, competition in the MES market is intensifying. Consequently, WatchGuard will face stiffer competition outside its network security customer base.

In terms of product portfolio, WatchGuard does not offer SIEM or SOAR. Its SIEMfeeder, however, does pass data to third-party SIEMs. Lack of its own SIEM and SOAR is a competitive disadvantage in attracting channel partners and high-end midsize businesses that are seeking those capabilities from their MES provider. Potentially, the acquisition of CyGlass will alter this circumstance in the future.

Consider WatchGuard When

The functional and operational synergies WatchGuard has developed between its endpoint security products and other products in its portfolio is solid justification for existing WatchGuard customers to consider the company for improving their overall cyber-risk postures while reducing their number of vendor relationships. These same synergies and WatchGuard's channel-supporting initiatives add to WatchGuard's appeal as a primary vendor within partners' portfolios of represented 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 (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

- *IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 Vendor Assessment* (IDC #US50521223, 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)
- *Worldwide Corporate Endpoint Security Market Shares, 2022: Pace of Growth Accelerated Through 2022* (IDC #US49349323, June 2023)
- *IDC MarketScape: Worldwide Network Edge Security as a Service 2023 Vendor Assessment* (IDC #US50723823, June 2023)
- *IDC MarketScape: Worldwide Zero Trust Network Access 2023 Vendor Assessment* (IDC #US50844623, June 2023)

Synopsis

This IDC study represents a vendor assessment of modern endpoint security for midsize 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. "The threat landscape is complex and evolving rapidly. To keep pace, multifunction platforms must also evolve by being more holistic in capabilities, streamlined in operations, and adaptable. Fortunately for midsize businesses, there are numerous viable MES platform vendors for them to consider."

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