IDC MarketScape

IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 Vendor Assessment

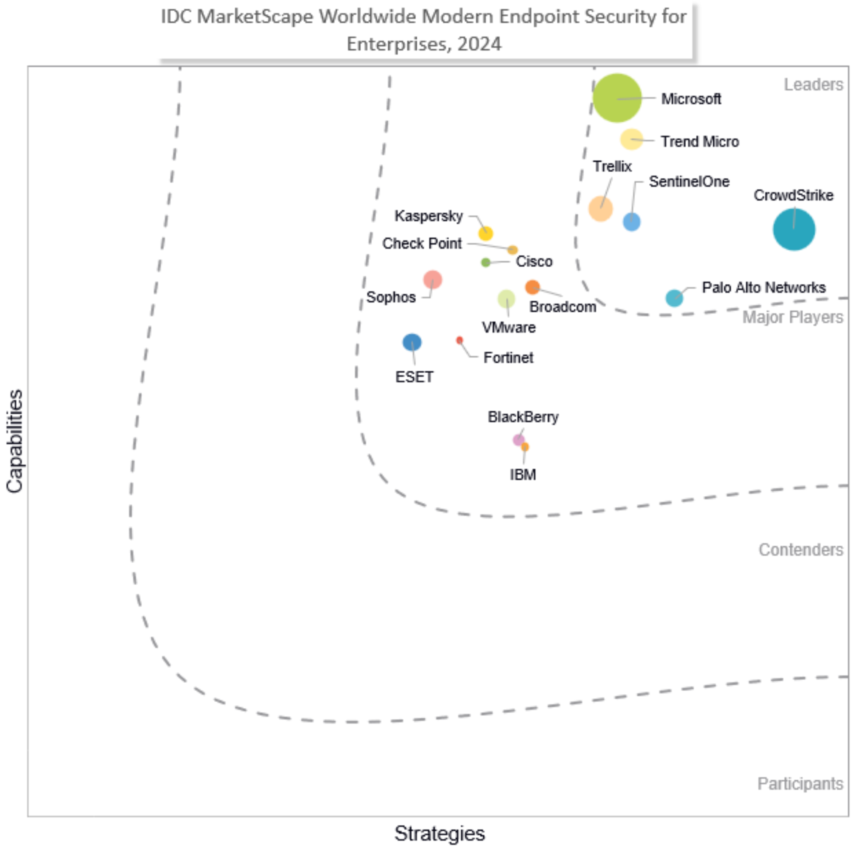
Michael Suby

THIS IDC MARKETSCAPE EXCERPT FEATURES TRELLIX

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Modern Endpoint Security for Enterprises Vendor Assessment



Source: IDC, 2024

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

January 2024, IDC #US50521223e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2024 Vendor Assessment (Doc # US50521223). 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 are 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 deceive 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.

Undoubtedly, this is a tall order that should rightly be met with a healthy dose of skepticism. Nevertheless, the alternative, stagnation in cybersecurity, is effectively relenting to cyberadversaries.

Each vendor in this IDC MarketScape has been and is continuing to enhance its endpoint security multifunction platform.

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 enterprise segment (2,500+ employees worldwide) of at least $75 million

ADVICE FOR TECHNOLOGY BUYERS

As modern endpoint security vendors cannot be stagnant in advancing their solutions against a threat landscape that is never standing still, technology buyers must also be active in evaluating options. Your organization's digital footprint and cyber-risk objectives have likely changed. To assume that your current MES products or combination of products are the best fit is missing an opportunity to make a positive change or reaffirm change is unnecessary. Guiding your evaluation, IDC offers the following advice.

- **Be assertive:** The MES market is highly competitive. Vendors are anxious to count your organization as a customer or, if already a customer, expand the offerings you buy. Set your bar of expectations high. In expectations, consider not only what the MES solution can do but how. On the how, gauge what your organization's capacity to proficiently manage the MES solution and a solution that likely spans a greater number of security functions. Be objective in asking whether your organization can operationalize the MES solution with current security staff and what the timeline will be for staff members to reach the necessary level of proficiency. Remember that threat actors are not going to sit on the sideline as you change vendors, MES solutions, or build up proficiency. Also, if your organization is staff restrained, evaluate managed services options, those offered by the MES vendor and its channel partners and vendor-agnostic managed security service providers (SPs). Again, be assertive about expectations and remember that whether just product or product plus services, the market is competitive, and you hold the purse strings.
- **Treat MES as a long-term strategic decision:** MES has evolved from a set of point products to an expanding multifunction platform. The platform can do more because it has to do more, again, to combat advancing adversaries. But in choosing a multifunction platform, you are making a longer-term commitment on what your organization will rely upon. Substituting a point product for an included platform function after the platform has been acquired will entail greater operational and financial trade-offs than in the past changing of antivirus products. Therefore, to support your organization's long-term interest, you should evaluate MES solutions holistically across the functions and deeply within each function.
- **Test thoroughly:** A lot is riding on your MES decision whether that decision is to change vendors or to remain with your existing vendor. You need confidence that the right decision will be made. Unlikely outside your routine but worth reiterating, testing MES offerings from multiple vendors in your production environment is critical to confident decision-making. Plus,

there are side benefits. You gain valuable insights and justification to ratchet up your vendor expectations and gauge what your timeline to proficiency will be.

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.

Trellix

Trellix is positioned in the Leaders category in the 2024 IDC MarketScape for worldwide modern endpoint security for enterprises.

Time has moved quickly since Symphony Technology Group acquired McAfee's enterprise business and FireEye products to form Trellix in late 2021. Judging by past mammoth pairings of security vendors, Trellix inherited a cynical perception bias. Now more than two years out, Trellix has proven that this bias was misplaced. The company has effectively merged the two companies culturally and operationally to foster a unified customer-facing mission of bringing the best of the two companies together and forming a foundation of continuous advancement. While the full transformational effect remains to play out, progress is confirmed and confidence moving forward is strong.

Strengths

Trellix has one of the broadest portfolios of security products in the industry. While noteworthy, the benefit of broadness is diminished without effective management. Trellix ePO, enterprise-class policy management system, is unquestionably one of Trellix's most significant competitive advantages. As other MES vendors endeavor to develop their own centralized policy management systems, Trellix is building on an established foundation.

IDC's perspective on MES architecture is that the agent and the cloud are each extensible platforms jointly optimized to deliver an evolving range of capabilities for customers. An early outcome following the creation of Trellix, this dual-platform architecture represents another Trellix strength and, from a more practical perspective, enabled Trellix to meld together the best technologies from both companies and provide customers with an increasingly unified experience and operational footprint.

Another aspect of agent and cloud platforms is adjusting detection based on real-time circumstances. In circumstances when network connectivity is interrupted, Trellix's agent-side detection automatically switches to a more aggressive mode and reverts to an agent-cloud collaborative mode when connectivity is restored.

Prior to the combination, both companies had significant presence in the enterprise segment with complementary functional concentrations, such as, McAfee in protection and FireEye in forensics. This combination of existing enterprise customers and complementary capabilities has contributed to Trellix's retention and growth among enterprise-size customers.

Financially, Trellix is in a strong position to fund its product research and development initiatives and market expansion.

Answering with confidence the difficult questions of "am I exposed," "should I care and why," and "how do I move forward" requires experience and relevant data, and Trellix Insights delivers. Trellix Insights is another part of Trellix's core in bringing cross-product, posture-strengthening benefits to its customers.

Other Trellix's capabilities that exceeded the peer group average in this IDC MarketScape include device vulnerability management, integration with Intel TDT, range of endpoint protection technologies (host-based firewall and IPS/IDS, DNS filtering, device control, DLP, and encryption), mobile threat defense, anti-tampering features, and post-ransomware attack recovery. With regard to anti-tampering, Trellix utilizes its modular agent architecture to block agent tampering to bypass security functions. Rootkit prevention modules evaluate malicious drivers and kernel modules. On post-ransomware attack recovery, Trellix's process-based agent sensors trigger recording, and the change log is retained until it is determined whether the suspicious process is malicious or benign. This recording includes saving the folder system and end-user files when a suspicious process is detected. Upon further review, if the process is deemed benign, the changes are finalized and version history is dropped. If the process is confirmed as malicious, the process is terminated, and changes are reverted to the original state.

Challenges

The most significant competitive challenge facing Trellix is being cast as a legacy and therefore inferior provider of security solutions. The strengths listed previously conversely argue that legacy is not an impairment but can be an advantage with proper execution. Moreover, Trellix's legacy delivers capabilities that non-legacy vendors are at a disadvantage to match, such as, support for legacy device platforms and offering both on-premises and cloud-based deployment options for management and security analytics.

Consider Trellix When

Trellix should continue to be a strong consideration among its enterprise customers. Trellix's unwavering intention and execution is to serve its existing enterprise customers better. Instinctively, in serving the existing base better, the same breadth of capabilities, focus on security outcomes, and openness add to Trellix's attractiveness to enterprises that have had suboptimal experiences with non-legacy 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 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)
- *Market Analysis Perspective: Worldwide Corporate Endpoint Security, 2023* (IDC #US51059423, 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 enterprises 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. As organizations are attracted to multifunction endpoint security platforms, buyers need to be pragmatic. Choosing a multifunctional platform is a strategic decision that is not easily undone. In the highly competing MES market, buyers have the latitude and justification in serving their organizations well by being assertive in expectations, thorough in evaluations, and patient in their decision-making."

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