Market Share

# Worldwide Modern Endpoint Security Market Shares, July 2021–June 2022: Currency Exchange Rates Slightly Trimmed Accelerating Growth

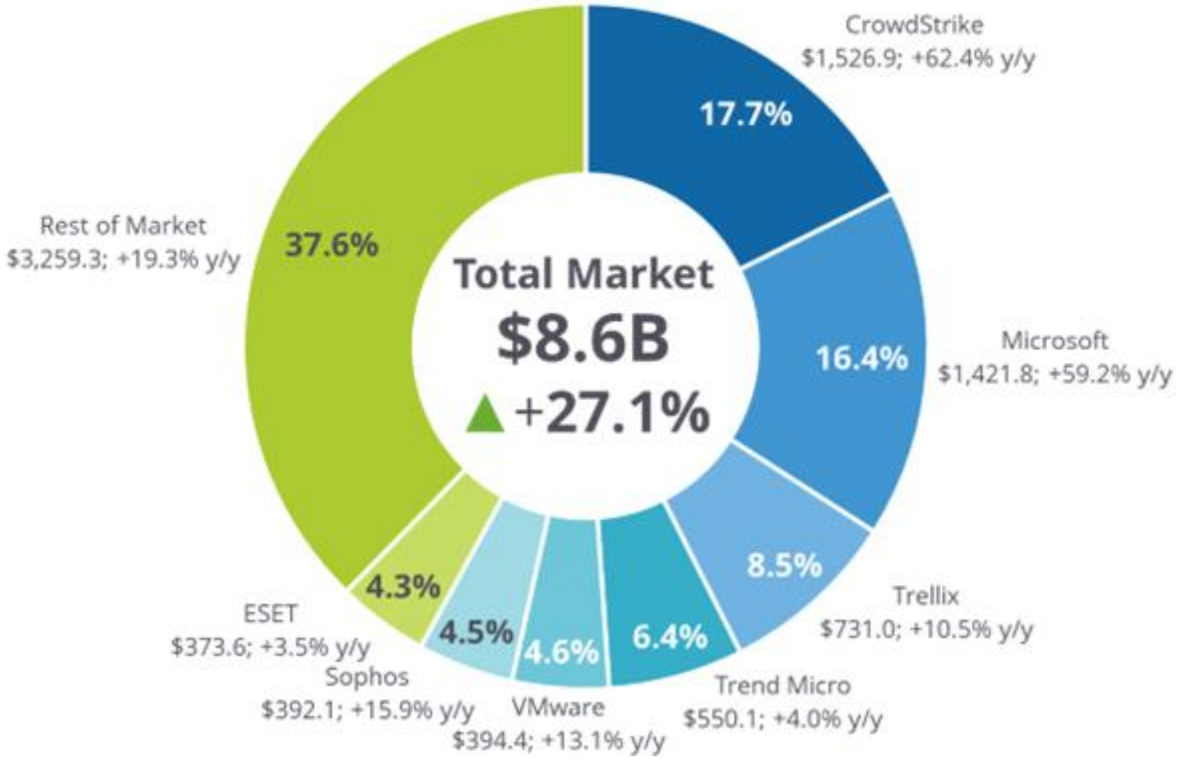
Michael Suby

## THIS IDC MARKET SHARE EXCERPT FEATURES ESET

## IDC MARKET SHARE FIGURE

### FIGURE 1

**Worldwide Modern Endpoint Security July 2021-June 2022 Share Snapshot**



Note: 2022 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2023

## IN THIS EXCERPT

The content for this excerpt was taken directly from IDC Market Share: Worldwide Modern Endpoint Security Market Shares, July 2021–June 2022: Currency Exchange Rates Slightly Trimmed Accelerating Growth (Doc # US49982022). All or parts of the following sections are included in this excerpt: Executive Summary, Market Share, Who Shaped the Year, Market Context, Appendix and Learn More. Also included is Figures 1, 2, 3, and 4 and Table 1 and 2.

## EXECUTIVE SUMMARY

The worldwide modern endpoint security market increased by 27.1% from the 12-month period ending June 2021 to the 12-month period ending June 2022. In the 12 months since June 2021, vendor revenue increased by $1.8 billion, from $6.8 billion to $8.6 billion.

The correlated factors of a widening attack surface and the pain threat actors can cause are at the foundation of accelerating market demand. Security buyers, in turn, are spending more on endpoint security and related technologies and vendor-provided managed services.

This IDC study reviews the worldwide modern endpoint security market for the 12-month period ending June 2022.

"There is no evidence through the first half of 2022 that worsening macroeconomic conditions is applying the brakes on demand for modern endpoint security solutions," according to Michael Suby, research vice president, Security and Trust at IDC. "Rather, our market analysis shows that the pace of growth has continued to accelerate."

## ADVICE FOR TECHNOLOGY SUPPLIERS

Vendors participating in the modern endpoint market are on a multiyear transformation in their customer and channel partner relationships. Moving away from relationships principally defined by purchased products and point-solution comparative outcomes, vendors are recasting their relationships as centered on a platform architecture that delivers broader, strategic outcomes. In consideration of this transformation, IDC offers the following advice:

- **Promote the full value of cybersecurity.** Promoting cybersecurity's full value to customers has traditionally been a challenge for vendors and their channel partners. For many organizations, the cybersecurity is viewed as an operational function and is distant from defining or differentiating who they are in the industries they compete in. However, with the linkages between cyber-risk and business resiliency gaining greater executive and board attention, vendors should seize upon the broadening opportunities to promote the fuller value of their platforms to a wider audience.
- **Segment and target.** The market for cybersecurity solutions in general and modern endpoint security specifically is not homogenous. A one-size-fits-all approach in packaging, pricing, and promotion will fail to meet any vendor's market aspirations. Instead, the alternative of refined segmentation and targeting will benefit the vendors that can master these skills.
- **Simplify.** What is more homogeneous is the recognition from cybersecurity buyers and practitioners that cybersecurity is a life cycle of complexity. From deciding what to buy and from whom, deploying, operationalizing, and eventually retiring as new cybersecurity tech

supplants the old, organizations face a heap of complexity and with that, uncertainty on whether they're doing cybersecurity with the level of efficacy their organizations demand. Like segment and target, vendors that can simplify the cybersecurity life cycle improve their chances of fostering lifelong, platform-embracing customer relationships.

## MARKET SHARE

The worldwide modern endpoint security market increased by 27.1% from the 12-month period ending June 2021 to the 12-month period ending June 2022. Over these two 12-month periods, revenue increased by $1.8 billion, from $6.8 billion to $8.6 billion (see Table 1). CrowdStrike and Microsoft produced the largest increases in revenue and market shares. CrowdStrike's market share increased by 3.8 percentage points from 13.8% to 17.7%, and Microsoft's market share increased by 3.3 percentage points from 13.1% to 16.4%. Combined, these two vendors now account for 34.1% of this market. The vendor with the next largest change in market share was SentinelOne, which increased by a 1.1 percentage point from 1.7% to 2.8%.

The strengthening of the U.S. dollar relative to other currencies had a depressing impact on the worldwide year-over-year percentage growth rates. Shown in Figure 1 and Table 1, the worldwide modern endpoint security market increased by 27.1% year over year based on current exchange rates. When calculated on a constant exchange rate, IDC estimates the year-over-year change was 29.6%, 2.5 percentage points higher.

As the geographic footprints of vendors in this market differ, the extent that exchange rates negatively impacted an individual vendor's year-over-year growth rate varies. ESET is among the vendors most impacted by currency exchange rates (i.e., strengthening of the U.S. dollar relative to other currencies).

Exchange rates relative to the U.S. dollar change in both directions. While the two 12-month periods compared in this document highlight the negative impact of a strengthening U.S. dollar on worldwide revenue, historically the impact oscillates between negative and positive as shown in the comparison of year-over-year worldwide growth rates based on current currency exchange rates and a constant currency exchange rate (see Figure 2). Regardless of the impact of fluctuating currency exchange rates, the trend lines, nevertheless, highlight a market that has been on an uninterrupted path of accelerating growth.

## TABLE 1

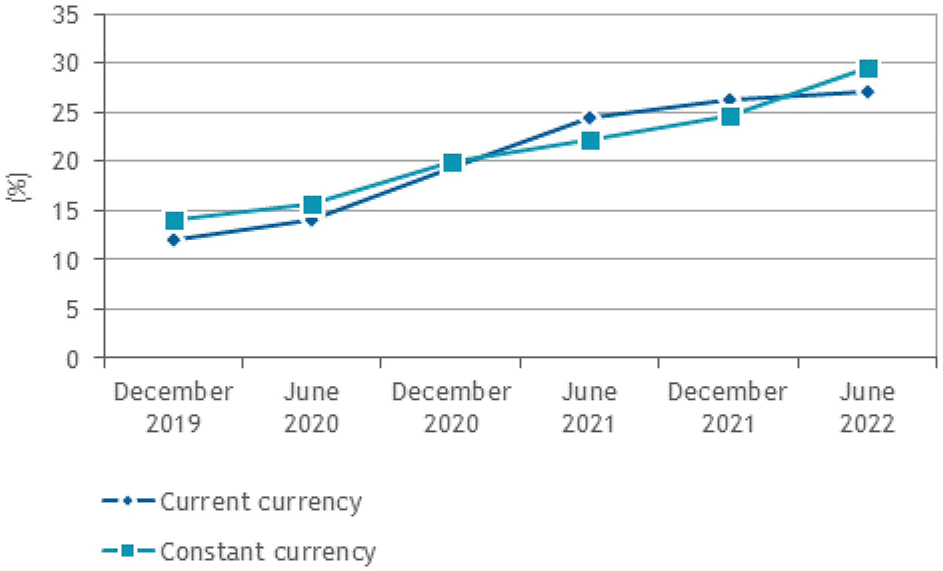
### Worldwide Modern Endpoint Security Revenue by Vendor, June 2021 and June 2022

| | June 2021 Revenue ($M) | June 2022 Revenue ($M) | 2022 Share (%) | 2021–2022 Growth (%) |
|---|---|---|---|---|
| CrowdStrike | 940.0 | 1,526.9 | 17.7 | 62.4 |
| Microsoft | 893.0 | 1,421.8 | 16.4 | 59.2 |
| Trellix | 661.6 | 731.0 | 8.5 | 10.5 |
| Trend Micro | 529.0 | 550.1 | 6.4 | 4.0 |
| VMware | 348.8 | 394.4 | 4.6 | 13.1 |
| Sophos | 338.4 | 392.1 | 4.5 | 15.9 |
| ESET | 361.1 | 373.6 | 4.3 | 3.5 |
| Broadcom Software | 368.2 | 317.0 | 3.7 | -13.9 |
| Kaspersky | 232.6 | 251.1 | 2.9 | 7.9 |
| SentinelOne | 116.1 | 243.0 | 2.8 | 109.3 |
| Other | 2016.0 | 2448.3 | 28.2 | 21.4 |
| Total | 6,804.9 | 8,649.2 | 100.0 | 27.1 |

Source: IDC, 2023

## FIGURE 2

### Worldwide Modern Endpoint Security Year-Over-Year Revenue Growth, December 2019–June 2022



Note: 12-month period ending year-over-year growth rates are shown.

Source: IDC, 2023

## WHO SHAPED THE YEAR

This excerpt was prepared for ESET but also included the following vendors: Microsoft, Trellix, Trend Micro, VMware, Sophos and others.

### ESET

ESET's worldwide revenue in the modern endpoint security market increased by 3.5% from the 12-month period ending June 2021 to the 12-month period ending 2022 (see Table 1). When this period-over-period growth rate is calculated based on constant currency exchange rates, ESET's growth rate more than doubled to 7.3%, a positive 3.8 percentage point difference.

In addition to the strengthening U.S. dollar, the Russia-Ukraine War was also a material impairment to ESET's period-over-period growth rate. Leading up to the war, ESET was a major security vendor in Russia and Belarus. Following the start of the Russia -Ukraine War, ESET ceased all sales to businesses and organizations in Russia and Belarus and terminated all Russian channel partnerships. An obvious reduction in ESET's sales pipeline during first half of 2022, this reduction will have a longer tail impact as existing customer contracts are not renewed. Countering, ESET's overlapping market footprint with Kaspersky outside Russia and Belarus has augmented ESET's positioning as a vendor replacement for Kaspersky's European Union (EU) customers.

Accompanied the war, ESET has leveraged its dense, in-region threat research to document the increase in cyberattacks targeting Ukraine. ESET operates three research centers in Czechia, three in Slovakia, and one each in Poland and Romania. From the intelligence reports emanating from these centers, ESET has gained well-earned notoriety and experienced increased demand by governments, Ukraine-based organizations, and global organizations for ESET's threat intelligence services and security products. As evidence, ESET states March 2022 was its highest revenue month in its 30-year history. Note that ESET's threat intelligence services are not included in IDC's sizing of the modern endpoint security market.

The war has not interrupted ESET's investments in product-directed research and development (R&D). According to the company, its R&D investments have doubled in size from 2016 to 2022 and the company is planning to add to its R&D employee base in 2023. Other signals of ESET's continuing R&D focus are expanded space dedicated to R&D personnel in all of its locations and introduction of flexible work policies to accommodate changing work dynamics. The company is also preparing to build a new headquarters campus in Bratislava, which will be in close proximity Slovak Academy of Sciences and University of Technology.

Principally reaching small and midsized business via its channel partners, ESET cultivates its partner relationships across all elements that contribute to increased end-customer spending and partner profitability. Those elements include but are not limited to localized program design, low touch end-customer experiences from deployment through daily operations, single console reach across ESET's entire product portfolio with support for multitenancy, and pricing. On the latter, ESET's ongoing efforts are toward a fully-fledged subscription-based model where the company's partners are charged based on the actual usage of their end customers rather than contracted. In addition, ESET's onboarding of new end customers is via a self-service partner mechanism.

Although competition is unrelenting in the modern endpoint security market, ESET's longevity, continuing investments, technical prowess, and financial stability positions the company well to strengthen its market growth in EU. Furthermore, IDC contends that in the current and future uncertain economic times, some of ESET's competitors will in the near term be scaling back their market-expanding investments in favor of profitability within their current geographies.

## MARKET CONTEXT

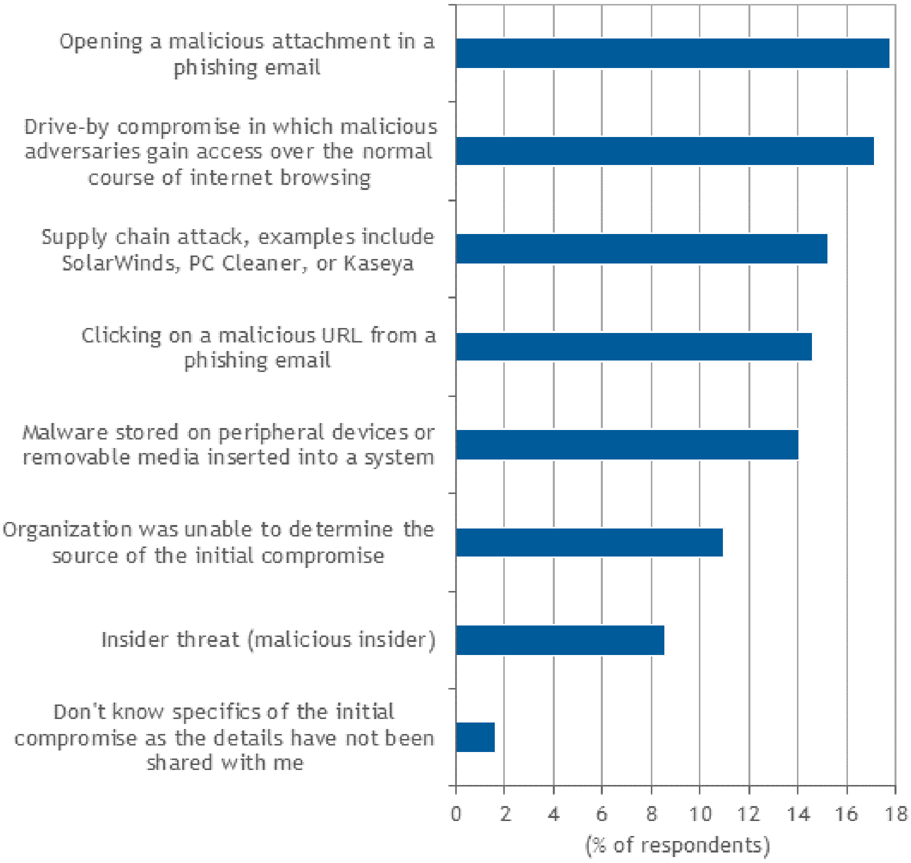
Contributing to the double-digit growth in the worldwide modern endpoint security market is end users and their devices being popular points of entry for threat actors, a material share of device-using employees routinely work remotely, and vendors' strategic investments in managed service platforms.

Ransomware continues to be a popular criminal activity. Ransomware success is also dependent on threat actors invading the victim's IT systems. Consequently, gaining an entry into IT systems is essential and frequently end users and their devices have been the soft targets used by threat actors to gain entry (see Figure 3).

## FIGURE 3

### Most Significant Sources of Initial Compromise in Ransomware

*Q. For your most recent ransomware incident that blocked access to systems or data, what was the most significant source of the initial compromise?*



n = 829

Note: Data is weighted by country GDP (500+ employee size).

Source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 7,* August 2022

Threat actors' success in ransomware and other types of cyberattacks is elevated when an organization has unprotected end-user devices or uneven protection across these devices. Threat actors may only need to infect one device in order to invade the organization's IT systems.

At the same time in a highly connected world, organizations are challenged to maintain a consistent and continuous level of threat protection across their entire end-user device population. Among the challenges is a portion of these devices are operating outside the perimeter defenses that form an additional layer of security for devices when operating in a corporate location (i.e., onsite).

While incidents of remote working rose during the COVID-19 pandemic, a reversal has not occurred and is not expected in 2023. According to IDC's recent North America-based *Endpoint Security*

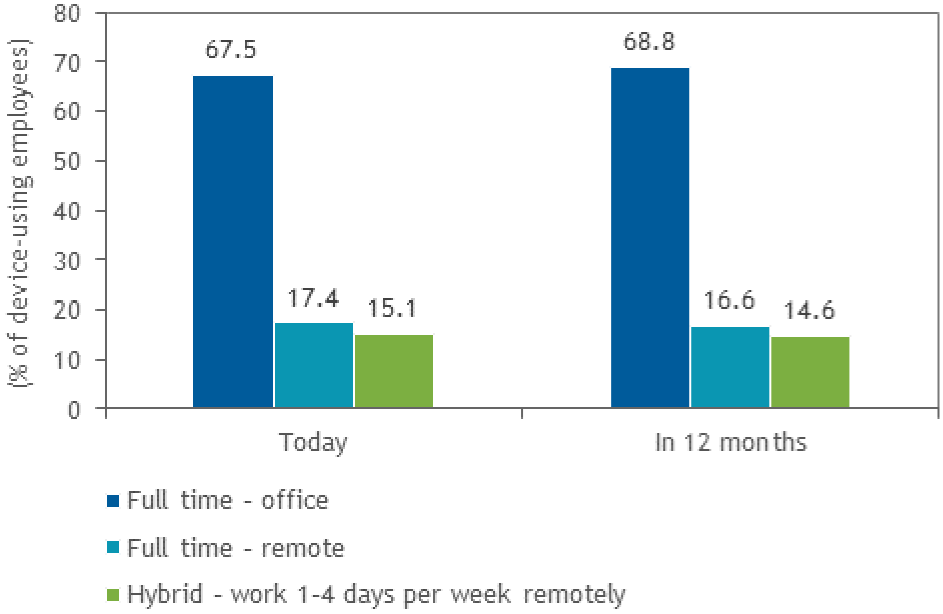
*Survey,* over 30% of device-using employees are remote working at least one day a week and only a slight reduction in this percentage is anticipated in 2023 (see Figure 4).

## FIGURE 4

### Average Percentage of Device-Using Employees Currently Working in Office, Remote, or Hybrid Work Arrangements

Q. *What percentage of your employees that require a PC, tablet, and/or smartphone to do their jobs currently work in the office, work remotely, or hybrid?*

Q. *And what do you expect that to look like in 12 months?*



n = 1,015

Source: IDC's *Endpoint Security Survey,* December 2022

Modern endpoint security vendors have connected the following dots in devising their long-term business strategies:

- Channel partners are essential in expanding the vendor's market reach and selling more of its products
- More products effectively used equates to sticker customer relationships and deeper partner engagements
- Effectively using the vendor's products requires vendor knowledgeable cybersecurity talent and perennial talent shortages plagues both end customers and channel partners

The solution is vendor-provided managed detection and response services that are optimized and sold with the vendor's security products, notably its EDR product. Evidence of this strategy is the number of modern endpoint security vendors that have launched a MDR offering has been expanding (see Table 2). Of the largest vendors in the worldwide modern endpoint security market that are not on this list are two that have, so far, strictly adhered to a products-only strategy in part to avoid potential channel conflict. Those two are Trellix and Broadcom Software.

## TABLE 2

### Modern Endpoint Security Vendors Offering MDR

| Vendor | Current MDR Offering Name | Launched | OilRig 2022 |
|---|---|---|---|
| CrowdStrike | Falcon Complete | 2018 | Yes |
| Trend Micro | Managed XDR | 2018 | Yes |
| SentinelOne | Vigilance Respond | 2019 | Yes |
| Sophos | Sophos Managed Detection and Response | 2019 | Yes |
| WithSecure | WithSecure Countercept Managed Detection and Response | 2020 | Yes |
| ESET | ESET PROTECT MDR | 2021 | |
| Kaspersky | Kaspersky Managed Detection and Response | 2021 | |
| VMware | VMware Carbon Black Cloud Managed Detection and Response | 2021 | |
| Microsoft | Microsoft Defender Experts for XDR | 2022 | Yes |

Note: "Yes" indicates vendor was a participant in MITRE Engenuity's 2022 ATT&CK managed services evaluation in defending against the OilRig adversary.

Source: IDC, 2023

In execution on its MDR strategy, IDC maintains that vendors will utilize their MDR platforms as a continuous experiential lab. As an experiential lab, IDC anticipates that vendors will leverage their operational experiences to refine their MDR-supporting platforms and integrated products and develop repeatable playbooks.

Both of these initiatives directly serve the vendor's channel partners by softening the complexity of the vendor's products and shortening partners' time in developing curated playbooks. Practiced earnestly, these MDR-supporting initiatives will accelerate and elevate channel partners' ability to profitably scale their businesses and deliver improved security outcomes for their end customers. Cycling back to the vendor, channel partners will be in an improved state of business enablement from which to promote and sell a fuller stack of the vendor's product line to more customers, existing and new.

Advantageous for modern endpoint security vendors that have an MDR offering, the MITRE Engenuity organization conducted an ATT&CK evaluation in 2022 for managed services based on the OilRig adversary. This evaluation provided participants with a third-party test of their MDR capabilities from a recognized tester and with that, notoriety. Over half of the modern endpoint security vendors with MDR offerings participated in this ATT&CK evaluation (see Table 2). Reasons for not participating varied across vendors. For example, Kaspersky applied to participate but was denied by MITRE Engenuity, and Cybereason and ESET chose to direct their internal resources to other activities.

Another MDR-related initiative vendors are pursuing is the creation of different packages of their MDR capabilities. One packaging approach is tiering of capabilities: standard and premium. As customers' interest and available budget for MDR services varies, a standard tier provides a lower cost alternative to engage and prove satisfaction before moving up to a broader, higher-priced premium tier. Another packaging approach is to align capabilities with the size and maturity of customers' SecOps teams. For some of these teams, a package of threat intelligence and advisory capabilities is better aligned with their needs than hands-on operational support. Like the experiential lab, IDC anticipates vendors will hone their packaging as an added means to assist their channel partner in achieving their business objectives.

Measuring modern endpoint security vendors' progress with their MDR offerings is, unfortunately, incomplete. Of the vendors listed in Table 2, only two have publicly stated any type of customer metrics. CrowdStrike in its second-quarter fiscal year earning call, stated it added 1,000 Falcon Complete customers during the first six months of its fiscal year (February 2022 to July 2022). Sophos in its October 18, 2022, press release stated it had over 12,000 Sophos MDR customers. In support of this document, Sophos shared its MDR customer count reached 14,000 in December 2022.

## Significant Market Developments

Changes in the vendor landscape in the past 12 to 18 months has not been as numerous as a few years ago.

One notable change was the creation of Trellix formed through the acquisitions of McAfee's Enterprise business and FireEye products by Symphony Technology Group. In September of this year, the company held its first in-person Xpand Live conference. IDC's perspective is expressed in *Trellix's Transformation Is Well Underway* (IDC #lcUS49758722, October 2022).

On a smaller acquisition scale, CrowdStrike and SentinelOne signaled their intentions to expand their product suites into identity exposure assessment and threat detection and response with the acquisitions of Preempt and Attivo Networks, respectively. IDC's perspective on this development is contained in *SentinelOne Broadens Its XDR Aspirations with the Acquisition of Attivo Networks* (IDC #lcUS48983322, March 2022).

Other vendor landscape changes are more internal. For example, in 2022 BlackBerry reignited its focus on the technologies and products it acquired from Cylance with extensive talent acquisitions and resurrection of the Cylance brand. IDC anticipates 2023 will be a pivotal year for BlackBerry in the security industry as it reintroduces itself to the market with an updated segmentation strategy, positioning, and product portfolio.

Also in 2023, the acquisition of VMware by Broadcom is expected to be completed and is currently making its way through the various approval and regulatory review processes (e.g., VMware stockholders approved the acquisition and U.K.'s Competition and Markets Authority initiated an anti-competition investigation in November 2022).

Only time will tell whether Broadcom will manage this transition with less customer and partner departures than the transition following the acquisition of Symantec. A bit of mix signals is present. On one hand in June 2022 the company stated it will be rebranding the Broadcom Software Group as VMware but on the other hand in late November/early December 2022 the departure of Tim Gillis, senior vice president and general manager of VMware's networking and advanced security business group, surfaced.

In addition to the heightened emphasis on vendor-provided MDR offerings, modern endpoint security vendors are also engaged in the preliminary stages of the battle for XDR supremacy. In 2021 and 2022 vendor efforts were concentrated on preparation: cross-product and vendor integrations, third-party ecosystems, data management architectures, initial pricing and packaging designs, and console rebuilds and refinements. In 2023 and beyond, IDC anticipates vendors will shift from promoting their XDR readiness to demonstrating tangible proof of XDR's multifaceted value. Included in this value demonstration is the following: sharpening organizations' understanding of cyber-risk and the pathways to structurally reduce that risk, improving performance metrics (e.g., mean time to detect, investigate, and respond), and curbing the impact of cybersecurity's technology sprawl on organizations' overall security expenditures and collective complexity.

## METHODOLOGY

The purpose of this section is to provide an overview of the methodology employed by IDC's software analysts for collecting, analyzing, and reporting revenue data for the categories defined by the software taxonomy. IDC strives to uniformly present revenue for all companies based on generally accepted accounting principles (GAAP). While it is standard for publicly held companies to report revenue according to GAAP, revenue reporting by private companies varies. When necessary, IDC will take reasonable steps to convert private company revenue to align with GAAP reporting.

IDC's industry analysts have been measuring and forecasting IT markets for more than 40 years. IDC's software industry analysts have been delivering analysis and prognostications for the commercial software market for more than 25 years.

The market share and analysis methodology incorporates information from five different but interrelated sources, as follows:

- **Reported and observed trends and financial activity.** This includes reported revenue data for public companies.
- **IDC's software vendor interviews and surveys.** IDC interviews and/or surveys significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.
- **Product briefings, press releases, and other publicly available information.** IDC's software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.
- **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by the product area model on more than 1,000 worldwide vendors.
- **IDC demand-side research.** This includes interviews with business users of software solutions annually and provides a fifth perspective for assessing competitive performance and market dynamics. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in IDC's software studies and pivot tables represents our best estimates based on the previously mentioned data sources as well as reported and observed activity by vendors and further modeling of data that we believe to be true to fill in any information gaps.

*Note: All numbers in this document may not be exact due to rounding.*

## 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, 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 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 product, services and products 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.

## RELATED RESEARCH

- *Market Analysis Perspective: Worldwide Corporate Endpoint Security, 2022* (IDC #US48579622, September 2022)

- *Worldwide Corporate Endpoint Security Forecast, 2022-2026: Upselling and Cross-Selling Power a Double-Digit Growth Rate* (IDC #US48579922, June 2022)
- *Worldwide Corporate Endpoint Security Market Shares, 2021: Year-Over-Year Growth Hit an All-Time High* (IDC #US48580022, May 2022)
- *Worldwide Modern Endpoint Security Market Shares, July 2020-June 2021: CrowdStrike and Microsoft Outdistancing All Other Vendors in a Rapidly Expanding Market* (IDC #US48616621, January 2022)
- *IDC MarketScape: Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment* (IDC #US48306021, November 2021)
- *IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment* (IDC #US48304721, November 2021)

## 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