Market Share

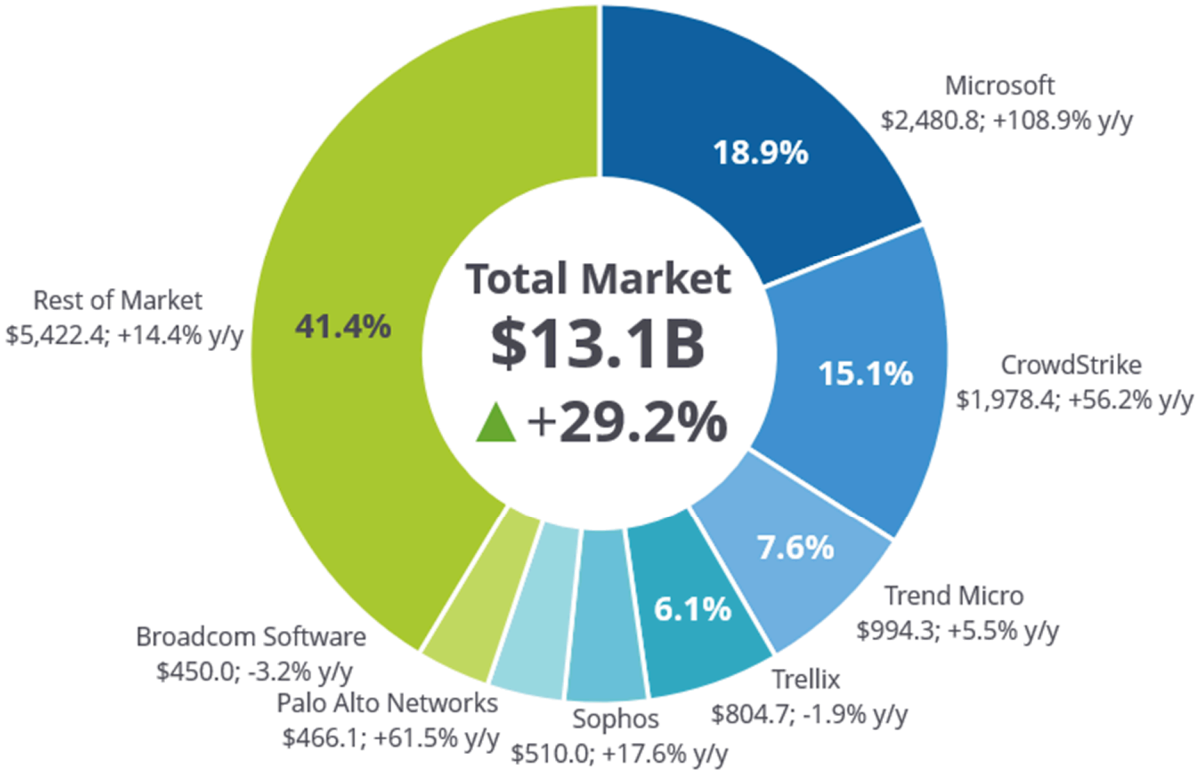
Worldwide Corporate Endpoint Security Market Shares, 2022: Pace of Growth Accelerated Through 2022

Michael Suby

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Corporate Endpoint Security 2022 Share Snapshot



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

Source: IDC, 2023

June 2023, IDC #US49349323

EXECUTIVE SUMMARY

The worldwide corporate endpoint security market grew by 29.2% in 2022. Revenue increased by $3.0 billion, from $10.1 billion in 2021 to $13.1 billion in 2022.

Both submarkets in the worldwide corporate endpoint security market increased significantly in 2022. Modern endpoint security grew by 31.2% in 2022. This submarket increased by $2.4 billion, from $7.8 billion in 2021 to $10.3 billion in 2022. Primary contributors to market growth are organizations' increasing appetite for modern endpoint security suites that contain a broader set of functionality and services, an increase in their number of protected devices, and Microsoft's push into additional market segments, notably small businesses and organizations with narrower endpoint security requirements.

Server security grew by 22.6% in 2022. This submarket increased by $527 million, from $2.3 billion in 2021 to $2.9 billion in 2022. Organizations' increasing use and reliance of cloud infrastructure services and cloud-native microservices are the primary drivers of growth of this submarket.

Material to the worldwide corporate endpoint security market is the influence of currency exchange rates. The previously stated 29.2% year-over-year growth rate is based on currency exchange rates that fluctuate across time periods (i.e., current currency exchange rates). Alternatively, calculated based on constant current exchange rates, IDC estimates that this market grew at a faster year-over-year pace of 35.3%.

This IDC study reviews the worldwide corporate endpoint security market for 2022.

According to Michael Suby, research vice president, Security and Trust at IDC, "The corporate endpoint security market has been on an accelerated pace of growth as organizations increased their spending to outduel cyberadversaries as end users and their devices remain lucrative points of entry into organizations' digital environments. This market also remains highly competitive, and to remain vibrant, vendors must be relentless in proving their customer value."

ADVICE FOR TECHNOLOGY SUPPLIERS

While the worldwide corporate endpoint security market is showing some signs of consolidation with Microsoft and CrowdStrike representing over one-third of the market as organizations increase their spend with endpoint security vendors, this market remains highly competitive and, as IDC's research reveals, the buy side of the market is diverse.

On this backdrop, IDC's recommendation to technology suppliers is as follows:

- **Find your lane.** While it is enticing to pursue all organizations across the spectrum of size, geography, industry, and security maturity, IDC contends that this growth strategy is challenging for any one vendor to maintain competitive differentiation long term. Instead, we believe that the majority of vendors in this market must tailor their product, go-to-market, and channel approaches to be more narrowly focused on a limited number of definable market segments.
- **Prove the return on investment (ROI).** IDC believes that this market has entered an endpoint detection and response (EDR) post-honeymoon period. In this period, organizations are assessing their gains in reducing their cyber-risk and in reacting to cyberincidents relative to the extra spend they incurred in adding EDR and/or managed EDR services to their cybersecurity toolset. The tag-along effect of this EDR assessment is a higher burden on

vendors to prove the incremental value of an extended detection and response (XDR) offering, especially if incremental spending is required. This spending is not limited to an increase in software licensing fees but also includes the transactional costs of changing vendors and/or products and additional training for SecOps personnel. EDR, as the gateway to XDR, will only be realized broadly in this market if vendors can first prove the enduring value of EDR.

- **Rebalance prevention with detection and response.** In this EDR post-honeymoon period, organizations will logically question whether their justifiable attention on incident detection and response may have gone too far. In doing so, their attention on improving their security posture and fortifying their preventive capabilities to thwart would-be attacks may have waned. IDC believes that there will be a rebirth in endpoint protection as organizations seek a better balance with detection and response capabilities and gravitate to vendor offerings that contain innovative leaps in endpoint protection efficacy.
- **Build an adaptable platform and partner ecosystem.** As endpoint security offerings have expanded in capabilities and into adjacent security disciplines, the strategic reliance on technology partnerships has heightened. Similarly, the platform where the vendor's homegrown technologies meld with partner technologies must be highly adaptable to account for changing technology and vendor selections. To the customer, these changes should be mostly transparent from a user perspective, except for the demonstration of improved security efficacy. Successful vendors in this market will increasingly be defined by their skillfulness in navigating technology and partner changes in meeting escalating customer expectations.

MARKET SHARE

The worldwide corporate endpoint security market increased by 29.2% in 2022. Revenue grew by $3.0 billion, from $10.1 billion in 2021 to $13.1 billion in 2022.

Led by Microsoft, the six largest vendors increased their collective market share from 48.7% in 2021 to 55.2% in 2022. Among the six largest vendors, year-over-year multi-percentage point market share gains by Microsoft and CrowdStrike were partially offset by modest declines in market shares by Trend Micro, Trellix, and Sophos. With a 62% year-over-year increase, Palo Alto Networks (PAN) replaced Broadcom Software in the top 6 (see Table 1).

TABLE 1

Worldwide Corporate Endpoint Security Revenue by Vendor, 2021 and 2022

	2021		2022		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2021–2022 Growth (%)
Microsoft	1,187.8	11.7	2,480.8	18.9	108.9
CrowdStrike	1,266.9	12.5	1,978.4	15.1	56.2
Trend Micro	942.3	9.3	994.3	7.6	5.5
Trellix	820.5	8.1	804.7	6.1	-1.9
Sophos	433.5	4.3	510.0	3.9	17.6
Palo Alto Networks	288.6	2.8	466.1	3.6	61.5
Broadcom Software	465.0	4.6	450.0	3.4	-3.2
VMware	395.4	3.9	419.0	3.2	6.0
SentinelOne	215.1	2.1	396.9	3.0	84.5
ESET	397.6	3.9	381.7	2.9	-4.0
Kaspersky	279.3	2.8	301.9	2.3	8.1
Check Point	225.5	2.2	267.1	2.0	18.5
Cybereason	181.4	1.8	225.1	1.7	24.1
IBM	171.3	1.7	183.9	1.4	7.3
BlackBerry	156.8	1.5	170.3	1.3	8.6
Cisco	152.3	1.5	159.2	1.2	4.5
Qi An Xin Group	125.2	1.2	140.2	1.1	11.9
Bitdefender	125.3	1.2	137.8	1.1	9.9
Malwarebytes	119.1	1.2	126.7	1.0	6.4
Other	2,194.4	21.6	2,512.8	19.2	14.5
Total	10,143.3	100.0	13,106.7	100.0	29.2

Source: IDC, 2023

The strengthening of the U.S. dollar relative to other currencies had a depressing impact on the worldwide year-over-year growth rate. As previously shown in Figure 1 and Table 1, the worldwide corporate endpoint security market increased by 29.2% year over year based on current currency

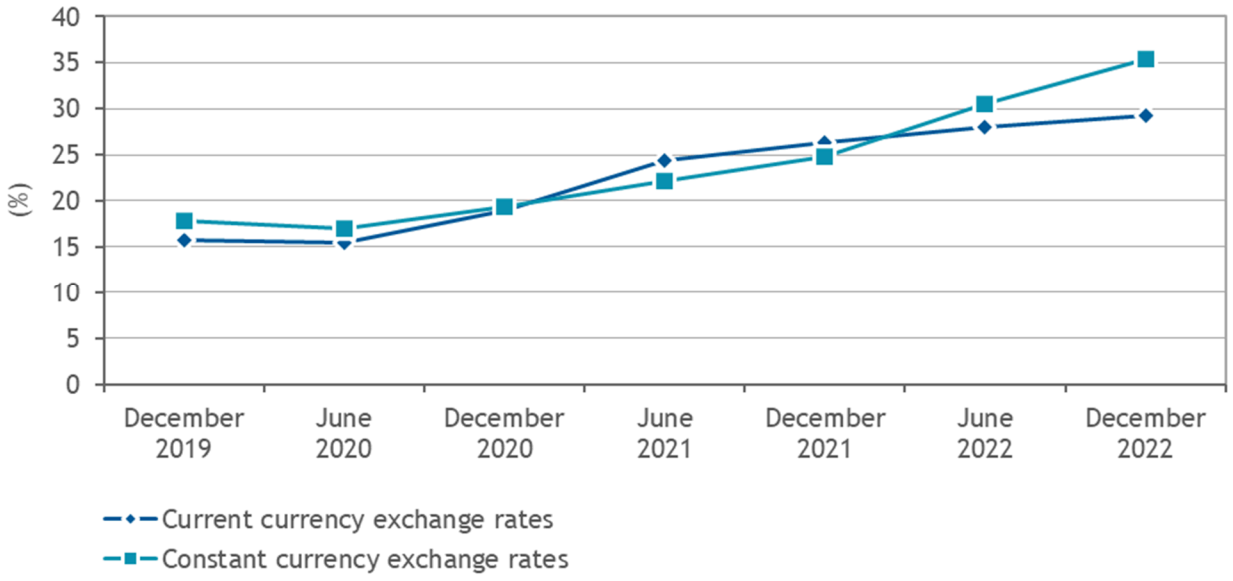
exchange rates. When calculated on constant currency exchange rates, IDC estimates that the year-over-year growth rate was 35.3%, 6.1 percentage points higher.

As the geographic footprints of vendors in this market differ, the extent that currency exchange rate fluctuations impacted a vendor's year-over-year growth rate varies. Suppressing their year-over-year growth rates shown in Table 1 are vendors with higher percentages of revenue earned outside the United States. Of the top 15 vendors in the worldwide corporate endpoint security market, the vendors most impacted by currency exchange rate fluctuations were Microsoft, Trend Micro, Sophos, SentinelOne, ESET, Check Point, and Cybereason. While Kaspersky has a high percentage of its revenue earned outside the United States, its rapidly shifting regional distribution partially mitigated the impact of fluctuations in currency exchange rates on its year-over-year growth rate.

Although currency exchange rates relative to the U.S. dollar change in both directions over time, 2022 was historically significant. Figure 2 shows the trend lines for year-over-year market growth rates based on current currency exchange rates and constant currency exchange rates. Notable in these trend lines is a market that has been on an uninterrupted path of accelerating growth since 2H20.

FIGURE 2

Worldwide Corporate Endpoint Security Year-Over-Year Revenue Growth, December 2019-December 2022



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

Source: IDC, 2023

The corporate endpoint security market consists of two rapidly growing submarkets: modern endpoint security and server security. Each submarket is defined in the Market Definition section.

Both submarkets in the worldwide corporate endpoint security market increased significantly in 2022. Modern endpoint security increased by 31.2% in 2022. This submarket grew by $2.4 billion, from $7.8

billion in 2021 to $10.3 billion in 2022 (see Table 2). Primary contributors to market growth are organizations' increasing appetite for modern endpoint security suites that contain a broader set of functionality and services, an increase in their number of protected devices, and Microsoft's push into additional market segments, notably small businesses and organizations with narrower endpoint security requirements.

TABLE 2

Worldwide Modern Endpoint Security Revenue by Vendor, 2021 and 2022

	2021		2022		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2021–2022 Growth (%)
Microsoft	1,155.6	14.8	2,300.4	22.4	99.1
CrowdStrike	1,166.9	14.9	1,824.1	17.8	56.3
Trellix	690.8	8.8	682.8	6.7	-1.2
Trend Micro	539.5	6.9	563.6	5.5	4.5
Sophos	367.2	4.7	431.8	4.2	17.6
VMware	376.6	4.8	390.0	3.8	3.5
ESET	366.5	4.7	369.5	3.6	0.8
SentinelOne	190.7	2.4	345.3	3.4	81.1
Broadcom Software	327.7	4.2	289.5	2.8	-11.7
Kaspersky	253.8	3.2	274.0	2.7	7.9
Palo Alto Networks	161.0	2.1	264.0	2.6	64.0
Cybereason	167.1	2.1	200.5	2.0	20.0
BlackBerry	156.8	2.0	170.3	1.7	8.6
Bitdefender	125.0	1.6	137.1	1.3	9.7
Check Point	110.8	1.4	127.1	1.2	14.7
Malwarebytes	116.1	1.5	123.3	1.2	6.2
Tanium	107.9	1.4	121.8	1.2	12.9
WatchGuard	96.4	1.2	113.1	1.1	17.3
Cisco	102.0	1.3	107.0	1.0	4.9
Other	1,236.4	15.8	1,416.1	13.8	14.5
Total	7,814.8	100.0	10,251.3	100.0	31.2

Source: IDC, 2023

The worldwide server security market increased by 22.6% in 2022. This submarket in the corporate endpoint security market grew by $527 million, from $2.3 billion in 2021 to $2.9 billion in 2022 (see Table 3). Organizations' increasing use and reliance of cloud infrastructure services and cloud-native microservices are the primary drivers of growth of this submarket. Additional analysis on cloud workload security can be found in *Worldwide Cloud Workload Security Market Shares, 2022* (forthcoming).

TABLE 3

Worldwide Server Security Revenue by Vendor, 2021 and 2022

	2021		2022		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2021–2022 Growth (%)
Trend Micro	402.7	17.3	430.7	15.1	6.9
Palo Alto Networks	127.6	5.5	202.1	7.1	58.4
Microsoft	32.2	1.4	180.4	6.3	459.5
Broadcom Software	137.3	5.9	160.5	5.6	16.9
CrowdStrike	100.0	4.3	154.3	5.4	54.3
Check Point	114.6	4.9	139.9	4.9	22.0
Trellix	129.7	5.6	121.9	4.3	-6.0
Lacework	80.0	3.4	108.0	3.8	35.0
IBM	90.1	3.9	88.4	3.1	-1.8
Sophos	66.3	2.8	78.2	2.7	17.9
Qi An Xin Group	63.4	2.7	71.0	2.5	12.0
Sysdig	50.7	2.2	66.0	2.3	30.2
AsiaInfo-Sec	46.4	2.0	55.8	2.0	20.2
Cisco	50.3	2.2	52.2	1.8	3.7
SentinelOne	24.4	1.0	51.6	1.8	111.6
Qingteng	45.5	2.0	51.5	1.8	13.1
Aqua Security	36.9	1.6	49.6	1.7	34.6
Other	730.4	31.4	793.4	27.8	8.6
Total	2,328.5	100.0	2,855.4	100.0	22.6

Source: IDC, 2023

WHO SHAPED THE YEAR

Microsoft

In 2022, Microsoft greatly flexed its muscle in the worldwide corporate endpoint security market. Over the past year, Microsoft's annual revenue doubled from $1.2 billion in 2021 to 2.5 billion in 2022 with contributions in both submarkets of modern endpoint security (including endpoint protection platforms [EPPs] and endpoint detection and response) and server security. In addition, Microsoft has the highest market share at 18.9% in 2022 with a market share increase of 7.2 percentage points over 2021.

As noted previously, Microsoft is one of the vendors most impacted by fluctuations in currency exchange rates. Referring back Table 1, its revenue grew by 108.9% in 2022 based on current currency exchange rates. Comparatively, IDC estimates its 2021-2022 growth at 117.3% based on constant currency exchange rates.

While multiple factors contributed to Microsoft's market share ascent in 2022, the most significant were steps that the company took in late 2021 and early 2022 to expand the reach of its Microsoft Defender for Endpoint product portfolio. In November 2021, Microsoft launched Microsoft Defender for Endpoint Plan 1 (MDE P1), catering to organizations that are not yet ready for the broader security capabilities of MDE P2, which includes EDR. Shortly after the introduction in January 2022 and the reduction of financial friction in MDE P1 adoption, Microsoft added MDE P1 to Microsoft 365 E3/A3 licenses. For existing Microsoft 365 E3/A3 licensing subscribers, a shift to P1 requires no additional licensing fees.

Separately in the small business segment, Microsoft Defender for Business (MDB) was launched in March 2022 as part of Microsoft 365 Business Premium subscription service. Standalone MDB was launched on May 2, 2022. MDB is a version of MDE P2 that is optimized for small and midsize businesses (of up to 300 users).

Another factor is Microsoft's drive to multiplatform parity across Windows, Linux, macOS, Android, and iOS. This is important as other vendors in this market have historically called out their multiplatform support as a point of differentiation to Microsoft's Windows "bias." Although differences in the degree of multiplatform support can still exist between Microsoft and other vendors, Microsoft's recurring enhancements and promotion of its multiplatform parity has the effect of diminishing competitors' claims.

CrowdStrike

With year-over-year revenue growth of 56.2%, CrowdStrike's worldwide corporate endpoint security revenue reached $2.0 billion and the company's market share continued to notch upward from 12.5% to 15.1%. Placing CrowdStrike's market size into perspective**,** its year-over-year change of $711 million from 2021 to 2022 exceeded the full-year 2022 revenue for all but three vendors in the worldwide corporate endpoint security market: Microsoft, Trend Micro, and Trellix**.** Also, Trellix would not be on this limited list if not for the combining of McAfee Business and FireEye products.

A major contributor to CrowdStrike's past and continuing revenue growth is its platform + module architecture and business model. According to the company, the percentage of its subscription customers with multiple modules has been steadily rising. For example, as of the end of CrowdStrike's FY21 (January 31, 2021), 24% of its subscription subscribers had six or more modules. In two years, this percentage rose to 39% on a base of customers that increased from 9,896 as of January 31, 2021, to

23,019 as of January 31, 2023. Correspondingly over this same two-year period, subscription revenue per customer and annual recurring revenue (ARR) per customer have each steadily increased.

IDC contends that CrowdStrike's platform + module architecture also aligns with the rising interest by organizations to reduce their number of vendors and, of heightened interest during uncertain economic times, to lower their recurring software licensing fees. As CrowdStrike has expanded its number of modules via organic development and acquisition, opportunities for organizations to substitute a CrowdStrike module for a single-purpose product from another vendor has increased. As a benefit to CrowdStrike subscription customers, they may realize a substantial reduction in their total software licensing fees and may also free their security teams to deepen their expertise in the use of products from fewer vendors.

Also of importance in CrowdStrike's architecture is periodically enhancing existing modules. A relevant example of this is the addition of the Asset Graph feature to the Falcon Platform. The Falcon Discover (security hygiene) is the first module to be paired with this feature. Asset Graph, as the name connotes, provides an organization with a visual, systemwide representation of its assets and its interactions. Through this pairing, organizations can reduce their risk of unknown and unmanaged assets and can proactively strengthen the security posture of their systemwide collection of assets.

Palo Alto Networks

Palo Alto Networks' position in the worldwide corporate endpoint security market has steadily risen. IDC estimates that in the past four years, Palo Alto Networks' market share increased with the largest percentage point jump occurring in the past year, from 2.8% in 2021 to 3.6% in 2022 (refer back to Table 1).

Market share growth has been balanced between the two submarkets of modern endpoint security (refer back to Table 2) and server security (refer back to Table 3). In server security, growth has been concentrated in cloud workload security.

Contributing to PAN's market growth have been three aspects of its market execution: continuous and balanced enhancements to its modern endpoint security products (Cortex XDR Prevent and Cortex XDR PRO), platform evolution, and market segmentation.

Since the introduction of Cortex XDR in early 2019, PAN has steadily enhanced and expanded its products' features and functionality. Akin to IDC's perspective on the underpinnings of success in the modern endpoint security market, PAN's product advancements have spanned both prevention (i.e., endpoint protection [EP]) and detection and response (EDR). On the prevention side, PAN has enhanced and expanded its coverage across the prominent file actions that occur on endpoints: write, execute, and access. In EDR, visibility and investigative features are broadening into email and identity.

Common in the vendor strategies in the corporate endpoint security market is an extensible platform architecture from which to land and grow customer engagements. Cortex is Palo Alto Network's security operations center (SOC) product line consisting of the company's most tenured products of Cortex XDR, which contains the Cortex XDR Prevent and Pro products; Cortex XSOAR, a security orchestration, automation, and response product; and Cortex Xpanse, a product for discovering and protecting organization's internet-facing attack surface (i.e., an outshine-in attacker viewpoint). In 2022, PAN launched Cortex, an extended security intelligence and automation management (XSIAM) platform, which the company states is on a faster pace of customer adoption than its other platforms.

Regarding market segmentation, PAN has been steadfast in its strategic focus on the enterprise market segment. While other vendors in the corporate endpoint security market are pursuing upward and downward segment expansion strategies, PAN has remained undiluted in its focus. And while PAN's concentrated focus narrows its total addressable market, enterprise-sized contract wins and ongoing contract cultivations can drive sizable revenue growth.

SentinelOne

SentinelOne continued to grow above the market's torrid pace in 2022. With worldwide corporate endpoint security revenue growth of 84.5% from 2021 to 2022, SentinelOne's market share increased from 2.1% to 3.0% (refer back to Table 1). This revenue growth was, however, tempered by current exchange rates. With over one-third of its revenue earned outside the United States, SentinelOne's year-over-year revenue growth was impacted by currency exchange rate fluctuations. Based on IDC's estimates, SentinelOne's revenue growth from 2021 to 2022 is 89.9% based on constant currency exchange rates and 84.5% based on current currency exchange rates.

Underneath SentinelOne's revenue growth is the strengthening in several business performance metrics. Based on SentinelOne's public reporting, a comparison between FY 4Q22 (ending January 31, 2022) and FY 4Q23 (ending January 31, 2023) shows that the customer count increased by 49%, annual recurring revenue (ARR) increased by 88%, and ARR per customer increased by 29% as the number of customers with over $100,000 in ARR increased by 74%. SentinelOne's percentage of revenue fulfilled through channel partners dipped slightly in 2022, likely attributable to the greater mix of customers with over $100,000 in ARR.

During 2022, SentinelOne continued to enhance its product portfolio and expand into new product categories. In February 2022, SentinelOne launched DataSet, a data analytics solution powered by the SentinelOne technology gained through the February 2021 acquisition of Scalyr. In March 2022, SentinelOne acquired Attivo Networks. Attivo Networks' capabilities triggered the creation of SentinelOne Singularity for Identity with three functional components: identity attack surface reduction, identity threat detection and response, and deception for identity assets. Continuing the trend among endpoint security vendors to broaden support for mobile platforms, SentinelOne formed an alliance with Zimperium in December 2021 to deliver Singularity Mobile.

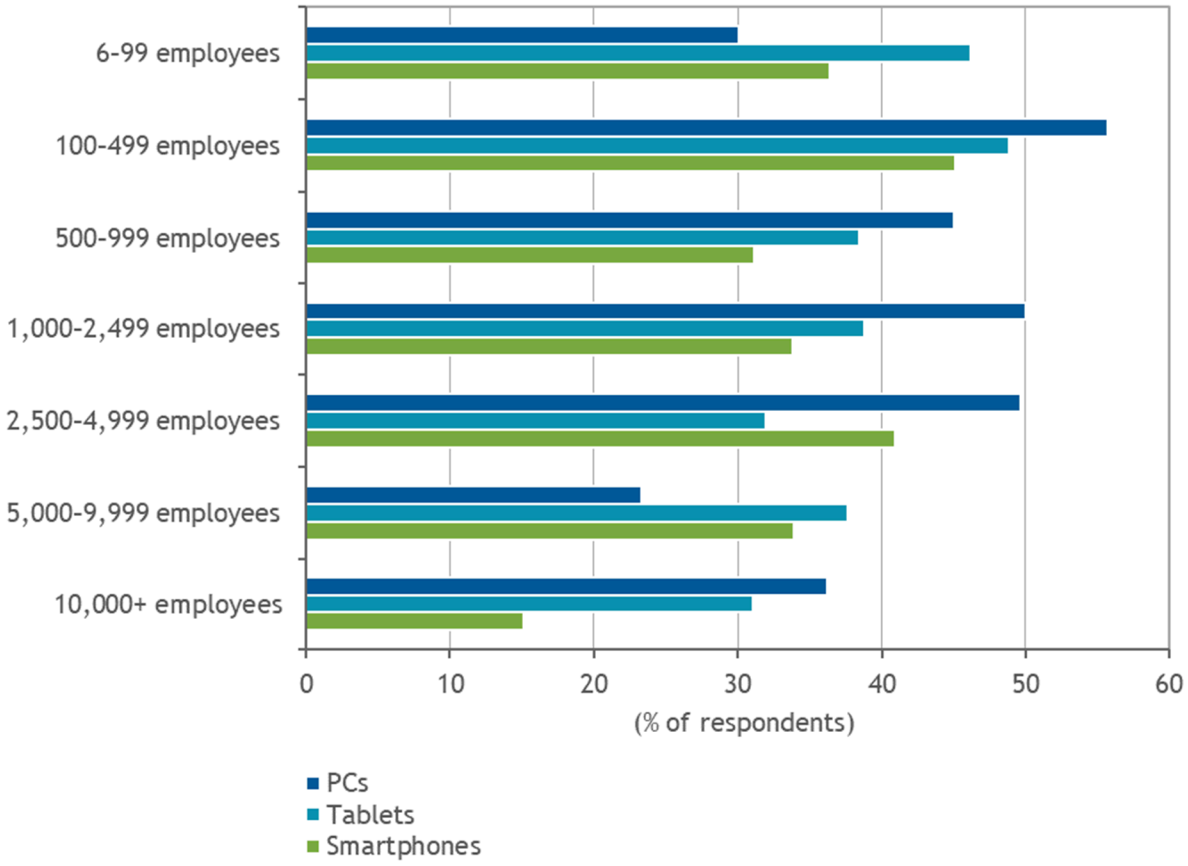
MARKET CONTEXT

Representing the majority of revenue in the worldwide corporate endpoint security market is the modern endpoint security submarket. Driving growth in modern endpoint security is the recognition that end users and their devices are principal targets for threat actors. Consequently, end-user devices are a primary battleground in cybersecurity. Demonstrating that organizations are upping their recurring investments in this battleground are three findings from IDC's *North America Endpoint Security Survey* (see Figures 3 and 4).

FIGURE 3

Number of End-User Devices with Endpoint Security That Installed and Enabled Change in the Past 12 Months

Q. *How has the number of end-user devices with endpoint security installed and enabled changed in the past 12 months?*



n = 1,015

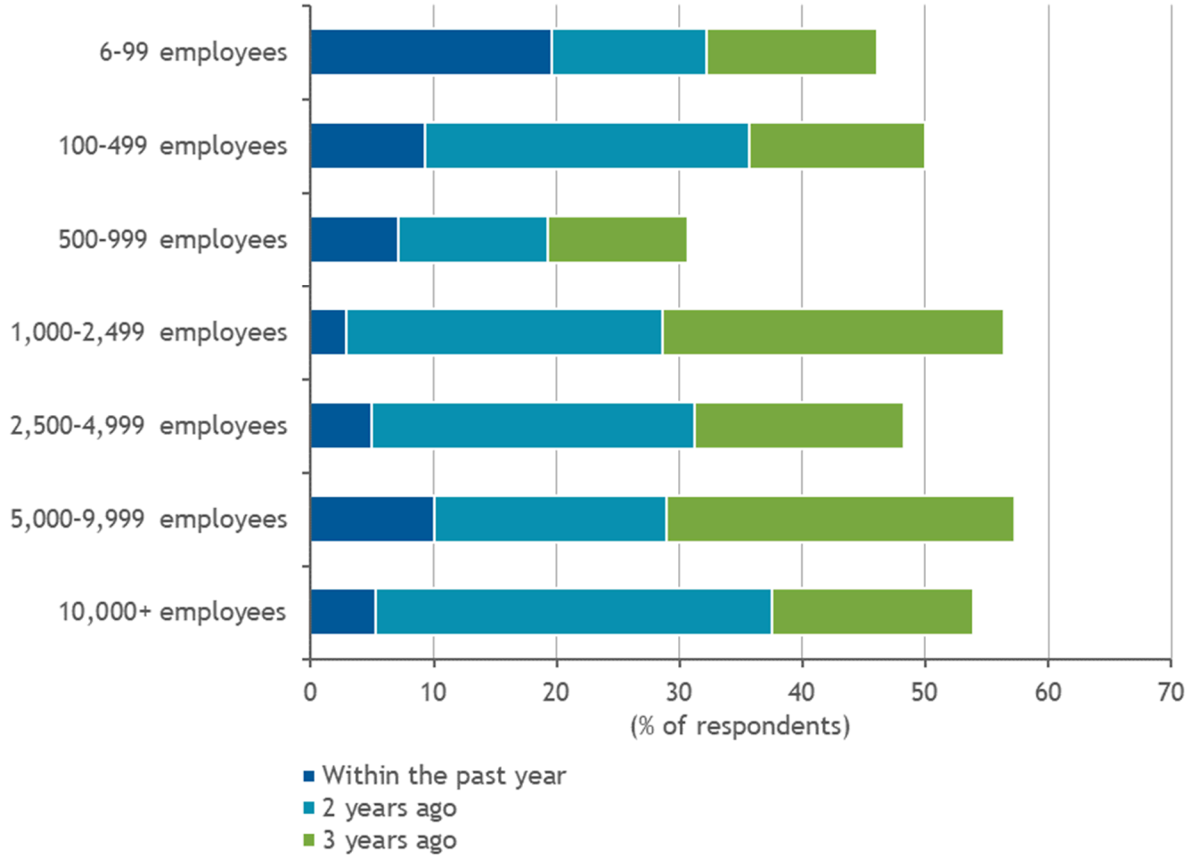
Base = respondents with 10% or more year-over-year protected device increase

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

FIGURE 4

Change in Endpoint Protection Vendors in the Past Three Years

Q. When did your organization last change its primary vendor for endpoint protection?



n = 1,015

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

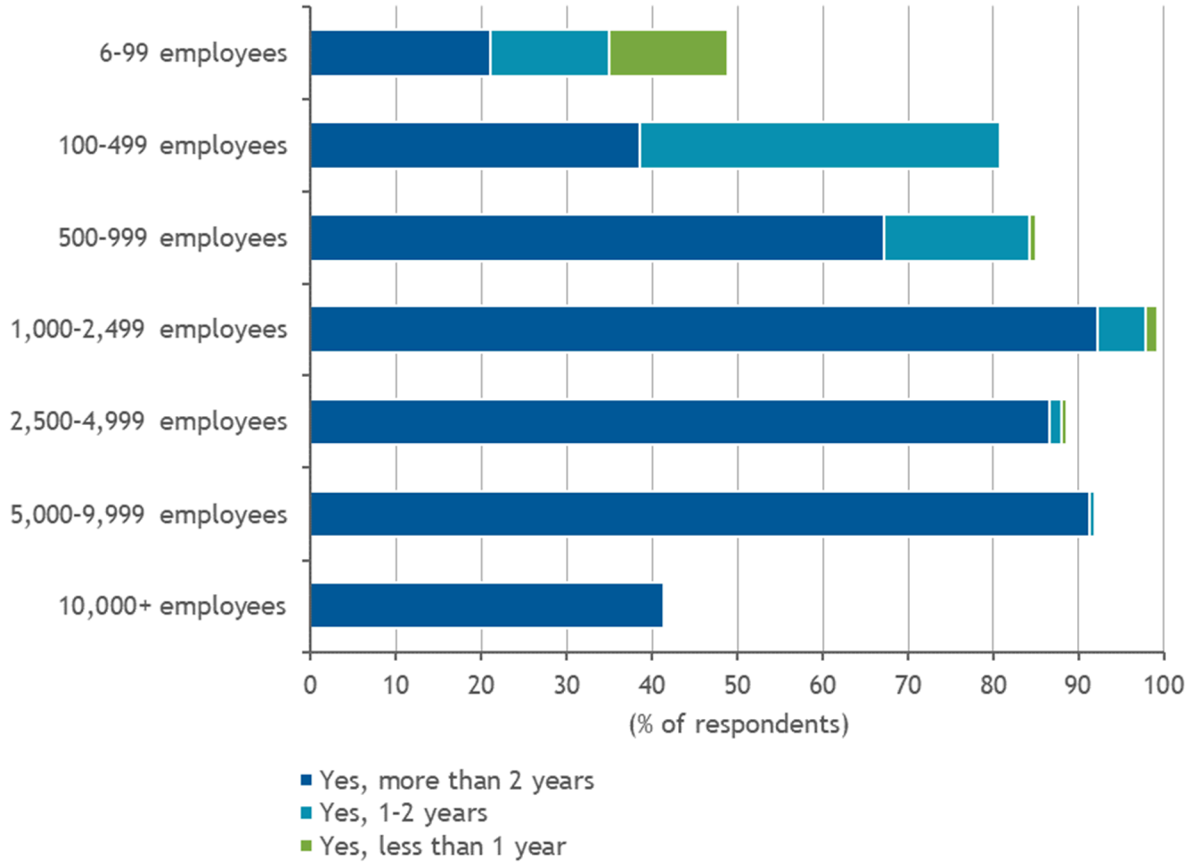
Relevant to the change in endpoint protection vendors are the reasons for changing. The top reason is a need for improved security efficacy (i.e., blocking more attacks with a lower rate of false positives). Changing vendors for a lower price was only cited by a small percentage of the survey respondents.

Increasing investments in an additional layer of defense is the adoption of EDR solutions. The lower EDR adoption percentage by organizations with 10,000+ employees is partially attributed to a higher percentage of these organizations adopting an XDR solution (see Figure 5).

FIGURE 5

EDR Adoption Reaching Pervasiveness

Q. Does your organization have an EDR solution in use, and for how long?



n = 1,015

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

Significant Market Developments

- In March 2022, F-Secure Corporation announced plans to pursue a partial demerger. Finalized July 2022, the demerger split F-Secure Corporation into two companies, WithSecure and F-Secure. WithSecure will focus on the security needs of businesses, and F-Secure will have a dedicated focus on consumer security, which is a market that IDC categorizes as consumer digital life protection.
- The May 2022 Broadcom announced agreement to acquire VMware continues to work through the necessary approvals. A firm date of closure is not available at this time.
- Trellix celebrated its one-year anniversary in January 2023. Trellix originated from the acquisitions of McAfee Enterprise and FireEye products in late 2021 by the Symphony Technology Group.
- On April 4, 2023, Cybereason announced that it raised an additional $100 million in funding from SoftBank Corp. Since inception, the company has raised $825 million in external funds.

The company has no plans for future funding and remains committed to completing its IPO when the IPO market improves. The company also appointed SoftBank Corp. Executive Vice President Eric Gan as the CEO, replacing Cybereason Cofounder Lior Div who will transition to an advisory role. With a change at the top, a period of leadership changes will undoubtedly occur. On April 20, 2023, Cybereason named Zohar Alon as the president of Cybereason Israel to oversee product and R&D teams.

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, and 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:

- **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 we maintain 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, 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

Corporate Endpoint Security

This technology encompasses endpoint security products for corporate (i.e., commercial and public/nonprofit) entities. Within corporate endpoint security, there are two technology detail segments: modern endpoint security and server security.

Modern Endpoint Security

Modern endpoint security products protect personal computing devices (e.g., workstations/PCs and laptops) and mobile devices (e.g., smartphones and tablets) from cyberattacks by detecting malicious code and behaviors present or operating within the devices and then facilitating 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 that 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 early 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 whitelisting; 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.

Server Security

Server security includes endpoint security products for physical servers and cloud workloads.

Physical Server Security

Physical server security products maintain the integrity of physical servers, providing protection from the operating system up to the hypervisor. Product features include antimalware, desktop firewall, host intrusion detection, application control, and integrity monitoring. These products accomplish their goals by ensuring that the system does not run malicious software that can compromise business applications and data on the servers. Server security products are tuned for server environments, which are very different from other traditional endpoint security products that typically deal with a wider variety of threats and use cases. These products are available for a broader array of operating systems, including, but not limited to, Windows, Unix, and Linux.

If physical server security is packaged and sold with modern endpoint security (i.e., same SKU), IDC will include this revenue in modern endpoint security.

Cloud Workload Security

Cloud workload security (also referred to as software-defined compute [SDC] workload security) products protect software-defined compute solutions, which encompass a number of compute abstraction technologies that are implemented at various layers of the system software stack. Cloud workload security solutions are not intended to protect the integrity of the SDC infrastructure (hypervisors, control plane/management, and orchestration) but to protect what runs on top of the SDC infrastructure (virtual machines [VMs] and containers). SDC technologies are often used in the context of public or private clouds but can also be implemented in noncloud environments, particularly virtualized and/or containerized environments.

Cloud workload security solutions are designed to maintain the integrity of SDC servers, providing protection features that traditionally include antimalware, desktop firewall, host intrusion detection, application control, and integrity monitoring. Cloud workload security solutions have expanded to include vulnerability management, configuration management, and application developer tools. Since the genesis of this submarket, the products and features that have been added include, but are not limited to, cloud security posture management (CSPM), infrastructure as code (IaC) scanning, and cloud infrastructure entitlements management (CIEM).

Cloud workload security offerings accomplish their goals by ensuring that the system does not run malicious software that can compromise business applications and data on the servers and/or by preventing malicious actors from accomplishing nefarious tasks. Like the other endpoint security submarkets, cloud workload security solutions are a mutually exclusive category with no overlap with other categories such as physical server or antimalware and suites. Cloud workload security solutions provide protection to three categories of software-defined compute environments:

- **Virtual machine software,** also known today as hypervisor software, uses low-level capabilities offered by certain hardware environments or installs a complete hardware emulation layer using software to support multiple operating environments and the related stacks of applications, application development and deployment software, and system infrastructure software. This segmentation is often referred to as server virtualization or partitioning.
- **Containers** are operating system (OS) segmentation technology. They are similar in concept to hypervisors, except they abstract an OS instead of server hardware. Containers rely on

segmenting away parts of the operating system. Each application is presented with a pristine virtual copy of the OS, and the application is made to believe that it is the only application installed and running on that OS. An application and its immediate dependencies are packaged into a container file. Optionally, various OS user space tools and libraries may also be included.

- **Cloud system software** represents a tightly bundled combination of server abstraction, orchestration software, and node-level controller software often sold as part of a larger cloud infrastructure platform solution. The compute resource layer represents a combination of virtual machine, container engine, and/or operating system and orchestration software running on a physical server, which is designated as a cloud compute node. The controller software virtualizes groups of compute nodes into a single logical compute resource. Cloud system software also exposes APIs that simplify the scheduling and control of VMs, containers, and bare metal servers running on the node, and it maintains a database of resource state and policies.

RELATED RESEARCH

- *How Frequently Are Organizations Changing Their Endpoint Protection Vendors and Why?* (IDC #US50041323, January 2023)
- *What Is EDR's Adoption Level and Who Provides EDR Management?* (IDC #US49983522, January 2023)
- *Has the Size and Mix of End-User Devices Equipped with Endpoint Security Changed?* (IDC #US49983122, January 2023)
- *Worldwide Modern Endpoint Security Market Shares, July 2021-June 2022: Currency Exchange Rates Slightly Trimmed Accelerating Growth* (IDC #US49982022, January 2023)
- *Market Analysis Perspective: Worldwide Corporate Endpoint Security, 2022* (IDC #US48579622, September 2022)
- *Worldwide Cloud Workload Security Market Shares, 2021: Prepare for a Wild Ride* (IDC #US49295722, July 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)

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