Market Share

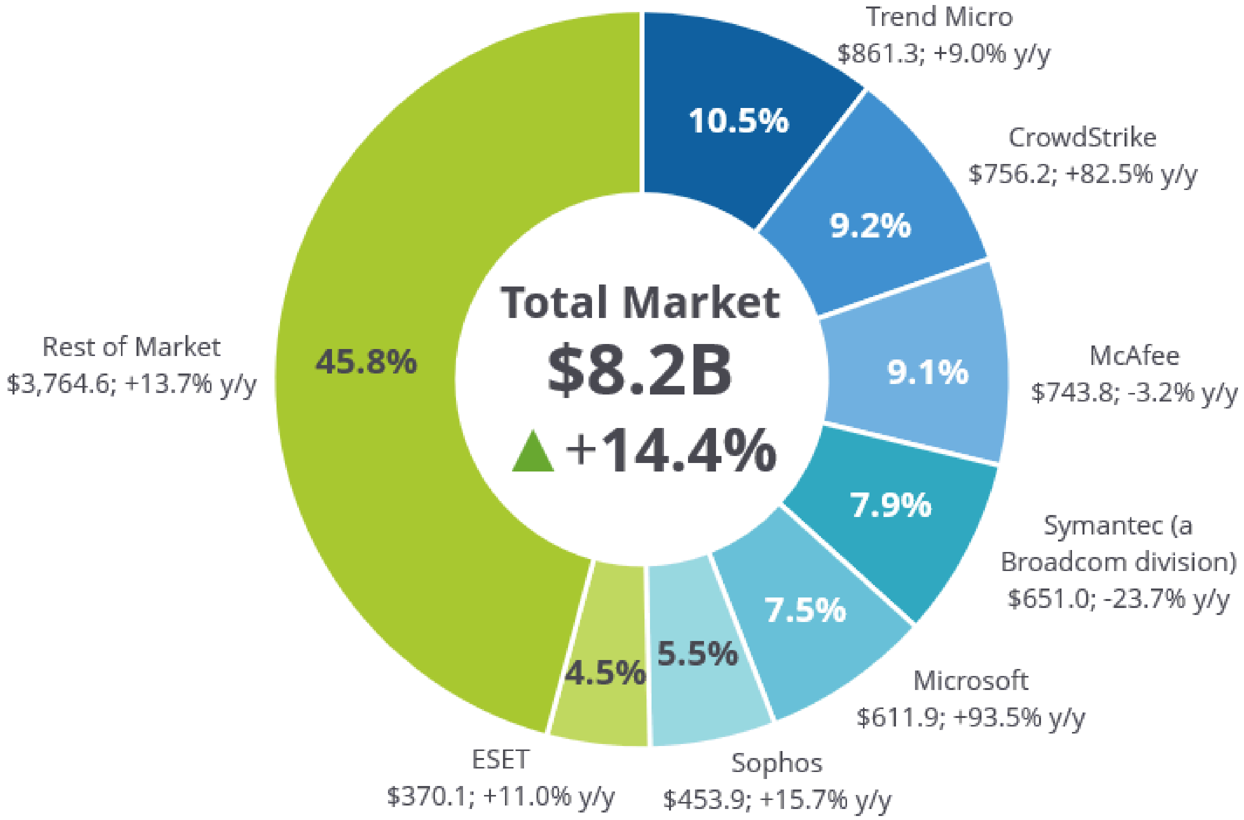
Worldwide Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth

Michael Suby

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Corporate Endpoint Security 2020 Share Snapshot



Note: 2020 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2021

EXECUTIVE SUMMARY

The worldwide corporate market for endpoint security increased by 14.4% in 2020. Revenue grew by $1.0 billion from $7.2 billion in 2019 to $8.2 billion in 2020.

The COVID-19 pandemic added fuel to this high-growth market. Confronted with the rapid transition from onsite work locations to work from home (WFH), the criticality of protecting end users' devices intensified. Also, recognizing that systematically blocking all potential compromises is not feasible, organizations increased their spending on endpoint detection and response (EDR) capabilities to aid security operations and bolster security efficacy. Collectively, the modern endpoint security submarket – the combination of endpoint protection platforms (EPP), EDR, and mobile threat management (MTM) – increased by 15.9% in 2020 to reach $6,070.7 million.

Organizations' transitions from on-premises datacenters to public cloud platforms and workload expansion in public clouds continued their upward trends in 2020. Although sales of security solutions for physical servers stagnated in 2020, server security – the combination of physical server security and cloud workload security – increased by 14.7% in 2020 to reach $1,681 million.

Propelled by the aforementioned market growth in server security and high single-digit growth in modern endpoint security, Trend Micro moved upward in the corporate endpoint security market in 2020 to capture the highest share, at 10.5%. Markedly increasing their market shares were CrowdStrike and Microsoft. Conversely, the market shares of McAfee and Symantec (a Broadcom division) retreated year over year.

This IDC study reviews the corporate endpoint security market for 2020.

According to Michael Suby, research vice president, Security and Trust at IDC, "The corporate endpoint security market is highly competitive and evolving. With threat actors relentlessly targeting end users and their devices as their first steps in attack campaigns, endpoint security is an essential first line of defense. As a first line of defense, organizations want more. They are expecting vendors to deliver a broader set of integrated and synergistic prevent, protect, and post-compromise detect and respond capabilities."

ADVICE FOR TECHNOLOGY SUPPLIERS

In this competitive market, corporate endpoint security vendors cannot rest on their past accomplishments. They must continue to innovate to effectively compete in this market and, in serving their customers, adapt to a changing threat landscape. IDC has the following advice for corporate endpoint security vendors:

- **Elevate prevention in your endpoint security stack.** While the current market momentum is materially fueled by customer adoption of EDR capabilities and, progressively in the future, extended detection and response (XDR), IDC contends that a more balanced approach to endpoint security is warranted. In this balanced approach, prevention takes center stage to minimize windows of exploitability and structurally contain endpoint compromises that do occur (i.e., reduce the attack surface and contain the blast radius). Next, protection mechanisms should be extensive, immediate, and certain. With threat actors evolving in their evasion techniques, protection engines must operate at machine speed and be capable of digesting a broadening array of telemetry to arrive at high-fidelity verdicts and respond with immediate and surgical countermeasures. Endpoint security solutions that excel in prevention and protection also improve the efficacy of EDR. With more attacks interrupted during the earlier stages of the attack chain, the volume of blinking red alerts and incidents becomes more manageable. With a more manageable volume, seasoned security professionals can redirect more of their time on initiatives that structurally improve the organization's security state and less on unravelling the trail threat actors left behind.

- **Go below the operating system (OS).** While the bulk of cyberattacks maneuver at and above the operating system layer, threat actors will find ways to burrow into the firmware (if they have not already) to add another dimension to their arsenals. Like ransomware and other attack types, criminal organizations will commercialize their firmware-takeover assets. Endpoint security vendors should prepare themselves to battle below, at, and above the OS.
- **Be a leader in supply chain integrity.** The SolarWinds supply chain compromise is a reminder that, within the mass of cyber adversaries, there is a subset that play the long game and can play it well. If IT management software can be compromised, one should assume that the same is true of other categories of business software. Given the extensive footprint of endpoint security software, infiltrating this software is a logical candidate for cybercriminals and nation-states. Endpoint security vendors should be prepared to demonstrate the integrity of their software and the cloud environments where they store customer data as this demonstration may in the future become a frequent criterion in vendor selection.

MARKET SHARE

The worldwide corporate market for endpoint security increased by 14.4% in 2020. Revenue increased by $1.0 billion from $7.2 billion in 2019 to $8.2 billion in 2020. The market also became more compacted. In 2019, the difference between the vendor with the highest market share (11.9%) and the vendor with the fifth-highest market share (5.5%) was 6.4 percentage points. In 2020, that difference dropped to 3.0 percentage points (10.5% and 7.5%, respectively). This occurred while the combined market share of the top 5 vendors shrank by 0.7 percentage points, from 44.8% to 44.1%.

Trend Micro demonstrated its resiliency in this market with a 2020 market-leading share of 10.5% (see Table 1).

TABLE 1

Worldwide Corporate Endpoint Security Revenue by Vendor, 2019 and 2020

	2019		2020		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2019–2020 Growth (%)
Trend Micro	790.3	11.0	861.3	10.5	9.0
CrowdStrike	414.4	5.8	756.2	9.2	82.5
McAfee	768.8	10.7	743.8	9.1	-3.2
Symantec (a Broadcom division)	853.4	11.9	651.0	7.9	-23.7
Microsoft	316.2	4.4	611.9	7.5	93.5
Sophos	392.5	5.5	453.9	5.5	15.7
ESET	333.5	4.6	370.1	4.5	11.0
VMware	249.3	3.5	308.2	3.8	23.6
Kaspersky	276.8	3.9	287.6	3.5	3.9
Tanium	210.3	2.9	229.9	2.8	9.3
IBM	207.8	2.9	206.0	2.5	-0.9
Palo Alto Networks	159.2	2.2	190.9	2.3	19.9
Check Point	144.2	2.0	187.4	2.3	29.9
Cisco	170.7	2.4	157.2	1.9	-7.9
BlackBerry	116.3	1.6	137.4	1.7	18.2
WatchGuard	119.2	1.7	132.7	1.6	11.4
SentinelOne	65.0	0.9	121.0	1.5	86.1
Cybereason	63.0	0.9	117.0	1.4	85.7
Bitdefender	66.4	0.9	101.7	1.2	53.2
Malwarebytes	77.6	1.1	92.0	1.1	18.6
FireEye	75.5	1.1	83.7	1.0	10.9
Qi An Xin Group	65.5	0.9	74.0	0.9	12.9

TABLE 1

Worldwide Corporate Endpoint Security Revenue by Vendor, 2019 and 2020

	2019		2020		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2019–2020 Growth (%)
OpenText	54.6	0.8	59.2	0.7	8.4
J2 Global	58.6	0.8	58.6	0.7	0.0
Ahnlab	52.7	0.7	55.6	0.7	5.5
Avast	50.4	0.7	51.2	0.6	1.6
Other	1,029.1	14.3	1,113.1	13.6	8.2
Total	7,181.2	100.0	8,212.8	100.0	14.4

Source: IDC, 2021

Modern endpoint security, the largest submarket within corporate endpoint security, increased by 15.9% in 2020. Modern endpoint security revenue increased by $833.7 million, from $5.2 billion in 2019 to $6.1 billion in 2020. CrowdStrike became the largest vendor in this submarket with an 80% increase in revenue, pushing its 7.9% market share in 2019 to 12.2% in 2020. Microsoft as well increased its position in the market with a 94% increase in revenue. While their market share increases were not as significant, Sophos, VMware, Cybereason, and SentinelOne each saw an increase in their annual revenue by over $45 million from 2019 to 2020 (see Table 2).

TABLE 2

Worldwide Modern Endpoint Security Revenue by Vendor, 2019 and 2020

	2019		2020		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2019–2020 Growth (%)
CrowdStrike	412.5	7.9	741.9	12.2	79.9
Microsoft	316.2	6.0	611.9	10.1	93.5
Trend Micro	489.4	9.3	507.1	8.4	3.6
McAfee	534.5	10.2	501.4	8.3	-6.2
Symantec (a Broadcom division)	538.8	10.3	372.9	6.1	-30.8
ESET	314.5	6.0	329.4	5.4	4.8
Sophos	282.4	5.4	329.3	5.4	16.6
VMware	249.3	4.8	307.8	5.1	23.4
Tanium	206.0	3.9	224.8	3.7	9.1
Kaspersky	213.0	4.1	219.5	3.6	3.1
BlackBerry	116.3	2.2	137.4	2.3	18.2
WatchGuard	119.2	2.3	132.7	2.2	11.4
SentinelOne	65.0	1.2	121.0	2.0	86.1
Cybereason	63.0	1.2	117.0	1.9	85.7
Bitdefender	66.2	1.3	101.5	1.7	53.2
Palo Alto Networks	87.6	1.7	100.9	1.7	15.1
Check Point	83.2	1.6	95.4	1.6	14.6
Malwarebytes	76.1	1.5	90.2	1.5	18.5
Cisco	68.6	1.3	85.7	1.4	25.0
FireEye	69.3	1.3	76.5	1.3	10.5
OpenText	54.6	1.0	59.2	1.0	8.4
J2 Global	58.6	1.1	58.6	1.0	0.0

TABLE 2

Worldwide Modern Endpoint Security Revenue by Vendor, 2019 and 2020

	2019		2020		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2019–2020 Growth (%)
IBM	58.7	1.1	58.4	1.0	-0.6
Ahnlab	52.7	1.0	55.6	0.9	5.5
Qi An Xin Group	42.2	0.8	47.9	0.8	13.7
Avast	45.3	0.9	46.0	0.8	1.5
F-Secure	40.4	0.8	41.3	0.7	2.3
Other	513.4	9.8	499.3	8.2	-2.8
Total	5,237.0	100.0	6,070.7	100.0	15.9

Source: IDC, 2021

The server security submarket revenue increased by 14.7%, from $1.5 billion in 2019 to $1.7 billion in 2020. Consisting of two product types on divergent trend lines, revenue for physical server security was relatively flat year over year, while revenue for cloud workload security continued to climb. Nominally, Trend Micro led all vendors in this submarket with an increase of $53.3 million, from $300.9 million in 2019 to $354.2 million in 2020 (see Table 3). Additional analysis on cloud workload security can be found in *Worldwide Cloud Workload Security Market Shares, 2020: Time to Shift Left* (IDC #US47837121, forthcoming).

TABLE 3

Worldwide Server Security Revenue by Vendor, 2019 and 2020

	2019		2020		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2019–2020 Growth (%)
Trend Micro	300.9	20.5	354.2	21.1	17.7
McAfee	171.1	11.7	184.8	11.0	8.0
Symantec (a Broadcom division)	160.7	11.0	147.2	8.8	-8.4
Sophos	85.9	5.9	103.3	6.1	20.2
Check Point	61.0	4.2	92.0	5.5	50.8
Palo Alto Networks	71.5	4.9	90.0	5.4	25.9
Cisco	102.1	7.0	71.5	4.3	-30.0
Kaspersky	63.8	4.4	68.1	4.0	6.7
IBM	57.0	3.9	56.4	3.4	-1.0
ESET	11.4	0.8	34.0	2.0	198.0
Sysdig	12.0	0.8	31.7	1.9	164.5
Qi An Xin Group	23.4	1.6	26.1	1.6	11.6
Other	345.4	23.6	421.7	25.1	22.1
Total	1,466.2	100.0	1,681.0	100.0	14.7

Source: IDC, 2021

With data leakage prevention (DLP) features being added to modern endpoint security products, standalone endpoint information protection and control product sales are shrinking relative to sales of modern endpoint security and server security products. Despite declining in 2020, Symantec continues to maintain the largest market share in this submarket, at 28.4% (see Table 4).

TABLE 4

Worldwide Information Protection and Control Revenue by Vendor, 2019 and 2020

	2019		2020		
	Revenue ($M)	Share (%)	Revenue ($M)	Share (%)	2019–2020 Growth (%)
Symantec (a Broadcom division)	153.9	32.2	130.8	28.4	-15.0
IBM	92.1	19.3	91.2	19.8	-1.0
McAfee	63.2	13.2	57.6	12.5	-8.9
Sophos	24.2	5.1	21.3	4.6	-11.9
Other	144.6	30.3	160.1	34.7	10.7
Total	478.0	100.0	461.1	100.0	-3.5

Source: IDC, 2021

WHO SHAPED THE YEAR

Trend Micro

Holding onto the largest share in corporate endpoint security market, Trend Micro's growth in the server security submarket is the principal contributor to overall market growth. In this category, the company added a market-leading $53.3 million in 2020. With this increase, Trend Micro outdistanced other vendors in serving the market with cloud workload security solutions. IDC delves more into this market in *Cloud Workload Security Market Share, 2020: Time to Shift Left* (IDC #US47837121, forthcoming).

In modern endpoint security, Trend Micro remains among the largest vendors. Compared with its legacy peers, McAfee and Symantec, Trend Micro's revenue increased slightly year over year over the past two years ($12 million in 2019 and $18 million in 2020), whereas McAfee and Symantec each saw a decline in their annual modern endpoint security revenue over the same two-year period. Relative to newer competitors, the comparison shows just the opposite scenario. Newer competitors — CrowdStrike, Microsoft, VMware, SentinelOne, and Cybereason — and well-established Sophos and Bitdefender with strong presences in North America and Western Europe (approximately 80% of their revenues) accounted for the majority of the year-over-year revenue increase in modern endpoint security.

Despite being among the oldest security disciplines, endpoint security has not faded in relevance nor pace of innovation. In the past half decade, EDR has attracted significant attention as a complement to

EPP. But EDR is shaping up to be a stepping-stone to XDR. The salient context of XDR is Trend Micro has directed the bulk of its product development efforts into XDR, as well as in cloud workload security. Starting in 2019 and continuing into 2020, Trend Micro has steadily added to the capabilities and comprehensiveness of its Vision One cloud-based XDR analytics and management platform and expanded its native sources of XDR telemetry to include endpoint, server, cloud, email, and network security. In early 2021, telemetry from IoT and mobile are planned additions. While the future is not 100% predictable, Trend Micro's past and future investments in XDR and cloud workload security will contribute to the company's market success across its security portfolio and in the modern endpoint security submarket.

CrowdStrike

With annual revenue increases of $208 million in 2019 and $341.8 million in 2020, CrowdStrike rocketed to become the second largest vendor in IDC's measurement of the corporate endpoint security market. With reported annual recurring revenue (ARR) of over $1 billion at the end of its 2021 fiscal year (January 31, 2021), CrowdStrike is on a trajectory to become the first vendor to exceed $1 billion in annual revenue in the corporate endpoint security market.

By the numbers, CrowdStrike's multimodule, cloud-native architecture has been a growth engine. In the 12 months ending January 31, 2021, CrowdStrike's number of subscription customers increased 82.2%, from 5,431 to 9,896; quarterly subscription revenue for the quarter ending January 31, 2021, increased 76.3%, from $139 million to $245 million; and subscription customers with four or more cloud modules increased from 50% to 63% and those with five or more modules increased from 33% to 47%.

From its cloud-native platform, CrowdStrike has, since its inception, steadily introduced new modules. In the second half of 2020, the company launched Falcon X Recon, Falcon Forensics, and Falcon Horizon. In expanding its multimodule portfolio, CrowdStrike, like other vendors in the market pursuing a similar strategy, is broadening the security functionality that organizations can acquire from a single vendor. On the acquisition front, CrowdStrike acquired Humio for its index-free XDR technology and Preempt Security for end-to-end visibility and enforcement of identity data via the CrowdStrike Falcon platform. From a customer perspective, tying multiple sources of telemetry together, applying advanced analytics, and centralizing policy administration into a single console streamline security operations and contributes to improved security efficacy.

CrowdStrike also actively invests in technology partnerships and the CrowdStrike Store to deliver a more comprehensive security solution set for its customers. In 2020, CrowdStrike announced the introduction of Spectra Alliance, a technology partnership including CrowdStrike, Okta, Proofpoint, and Netskope. The CrowdStrike Store has grown to have over 20 partner applications.

With its market success, CrowdStrike has, however, become a principal target for other competitors in the corporate endpoint security market. This market is highly competitive with several vendors growing at multiples of the market rate (refer back to Table 1). While ammunition used to favorably position themselves against CrowdStrike varies, recurring themes center around CrowdStrike's lightweight software agent and cloud-native architecture, and cost. Vendors that pack more autonomous functionality into their software agents claim a more rapid ability to detect and stop more threats in the early stages of the attack chain. On cost, CrowdStrike's reported financials provide a proxy for the challenges of maintaining revenue per customer while growing the customer base. Based on IDC's calculations, CrowdStrike's subscription average revenue per customer (ARPC) has not increased as the percentage of CrowdStrike customers subscribing to multiple modules has increased. Arguably, a changing mix of customers as CrowdStrike acquires smaller-sized businesses depresses averages. Yet this dynamic has not negatively impacted the company's profits and ability to fund reinvestment. CrowdStrike's gross profit per subscription customer has been stable, and its total gross profit percentage (subscription and professional services combined) has steadily increased.

McAfee

In 2020, McAfee's growth in the corporate endpoint security lagged behind the market. Correspondingly, the company's market share declined from 10.7% in 2019 to 9.1% in 2020.

Principally contributing to this share decline was weakness in McAfee's position in the modern endpoint security submarket where the company's market share fell from 10.2% in 2019 to 8.3% in 2020. McAfee's share decline in the server security submarket was not as precipitous as rising sales in cloud workload security offset expected weakness in physical server security as organizations transitioned from owning and operating servers to renting server capacity in public clouds.

From an ownership perspective, 2021 will be a transitional year for McAfee. Announced in March of this year, Symphony Technology Group (STG) will be acquiring the enterprise business of McAfee with closure anticipated by the end of this year. The impact on McAfee's market position is uncertain. In 2020, its enterprise revenue increased slightly by 1.2% over 2019 following a strong fourth quarter for the company with a 4.8% year-over-year increase. Fourth quarter momentum, however, did not continue as 1Q21 revenue was flat relative to 1Q20. The introduction of new products, MVISION Insights in 2020 and MVISION XDR in 2021, does demonstrate the company is continuing to innovate.

Symantec (A Broadcom Division)

Symantec experienced a decline in market share in 2020, which was partially attributable to an accounting rule and not entirely a reflection of market loss. With the acquisition of the enterprise portion of Symantec by Broadcom, there was a required reassessment of Symantec's deferred revenue. How much of the $202.4 million decline in Symantec's corporate endpoint security revenue from 2019 to 2020 is because of a lower assessment of deferred revenue is not known by IDC.

Symantec's year-over-year revenue decline within corporate endpoint security varied among the three submarkets: modern endpoint security, information protection and control, and server security. By far, the largest year-over-year decline, numerically and on a percentage basis, was in the modern endpoint security submarket. Similar to McAfee, competing vendors routinely claimed customer takeaways. Another contributing factor is Symantec's concentrated focus on strategic accounts as it became part of Broadcom. Anecdotally, competing vendors stated Symantec's refined focus sowed seeds of uncertainty among smaller-sized and less strategic Symantec accounts and Symantec channel partners that sell into these accounts — further opening the door for customer takeaways.

With over $600 million in corporate endpoint security revenue, Symantec is not inattentive to this evolving market. The company continues to improve and add features to its Endpoint Security Complete product. Its Active Directory Defense, made possible through its late-2018 acquisition of Javelin Networks, is a distinctive capability and valuable in blunting attacks that rely on compromising domain controllers. Upcoming, Symantec will be launching Adaptive Protection, a feature developed through organic innovation and powered by Symantec's threat intelligence. Adaptive Protection systematically reduces attackers' avenues to move laterally and abuse trusted applications running on corporate endpoints. As a transparent capability, Adaptive Protection is designed for immediate use, causes no adverse impact to legitimate application and business processes, and is tailored to each customer. Consequently, the set of blocked avenues is unique to each customer, causing attackers to devote more resources to counter. Across Symantec's security portfolio, Symantec introduced portfolio license agreements (PLAs). Constructed for maximum flexibility, customers that enter into a PLA can shift their usage among included products without restrictions and increase usage, try new products, and change deployment models (e.g., migrate from on premises to cloud based) without incurring additional fees throughout the PLA term. While the near-term market-shifting impact of these and other advancements Symantec introduces into its products and customer engagements will likely be indistinguishable, competitors should take note that future customer takeaways will be more challenging.

Microsoft

Microsoft has quickly moved into the top 5 in the corporate endpoint security market. IDC estimated the company had 2.4% market share in 2018. With annual revenue increases of 114% in 2019 and 93.5% in 2020, the company's market share reached 7.5% in 2020 according to IDC estimation, 3 percentage points from the market share leader Trend Micro.

Of significance in comparing Microsoft's market share with the rest of the market, IDC's estimation of Microsoft's revenue is solely of Microsoft Defender for Endpoint, an EDR product. We do not assign a revenue value for Microsoft Defender AV, an EPP product, as that functionality is included in the Windows license. Conversely, our revenue estimations for all other vendors in this market are considerably more expansive as they include sales of standalone and combined EPP and EDR products.

Our primary research also confirms Microsoft as a prominent endpoint security vendor. In our early 2020 survey of North America-based small and midsize businesses (100-2,500 employees), 8% of the survey respondents identified Microsoft as their primary endpoint security vendor. This same result was repeated in our late-2020 survey of North America and Western European organizations with 2,500 or more employees.

Contributing to Microsoft's market ascension is the security efficacy of its Defender AV and Defender for Endpoint products, a steady and frequent flow of feature updates and introductions, and a shrewd licensing model that encourages buyers to view endpoint security as part of a broader IT and security licensing decision.

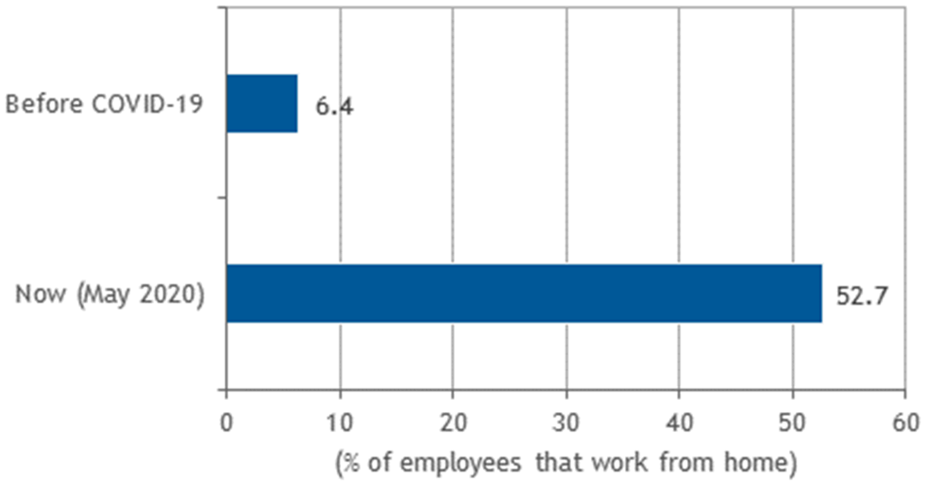
MARKET CONTEXT

The COVID-19 pandemic was the seminal contributor to the 2020 market increase in corporate endpoint security. Forced to react to stay-at-home edicts, organizations shifted work from "locations for many" to "many remote locations." The magnitude of this shift was extreme. In IDC's May 2020 survey of IT decision makers, the percentage of employees working from home increased by a factor of 8 relative to pre-pandemic times (see Figure 2).

FIGURE 2

Employees Working from Home

Q. What percentage of your organization's employees were working from home before COVID-19, and what percentage are working from home now (as of May 2020)?



n = 101

Notes:

Survey respondents are based in the United States.

Survey was conducted May 21-28, 2020.

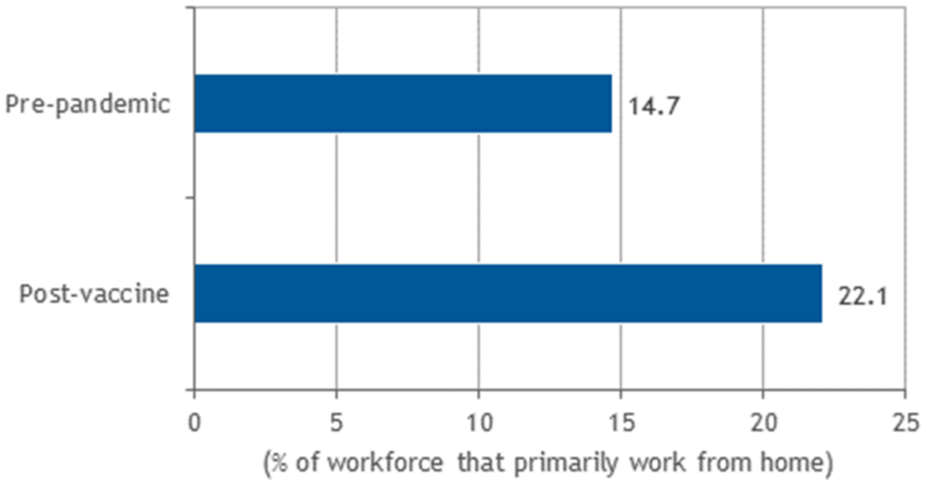
Source: IDC's *COVID-19 Impact on IT Spending Survey*, May 2020

With vaccinations on the horizon, organizations began to make return-to-office plans. Those plans, however, do not entail a full return. According to IDC's August 2020 survey of IT decision makers, expectations are that the workforce working from home after vaccines have been widely administered will be 50% greater than before the COVID-19 pandemic (see Figure 3).

FIGURE 3

Workforce Working from Home

Q. What percentage of your workforce was, is, or is expected to be in each of the following categories (before COVID-19 pandemic and post-vaccine)?



n = 835

Notes:

Survey respondents are based worldwide.

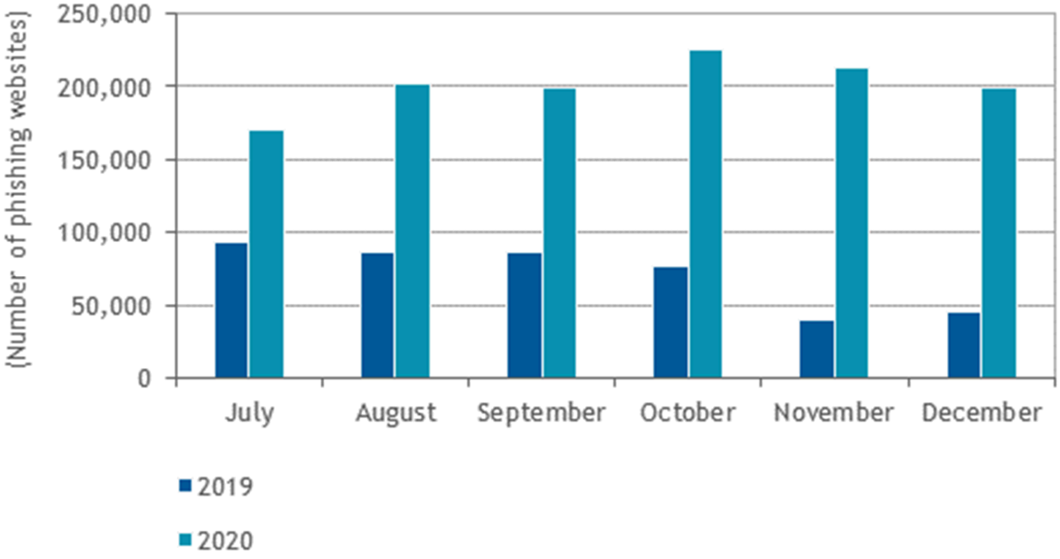
Survey was conducted August 5-17, 2020.

Source: IDC's *COVID-19 Impact on IT Spending Survey*, August 2020

Never complacent, threat actors pounced on the broadened attack surface that the rapid shift to work from home ushered in. No longer protected by corporate perimeter security mechanisms and end users connecting to business systems and applications through unmanaged home networks with a mix of personally owned and corporate-owned devices that are unlikely to be monitored and maintained with the same degree of diligence as in pre-pandemic times, the opportunity was ripe for threat actors. In addition, cast into unusual working conditions and facing multiple, concurrent veins of life uncertainty, end users were rightly viewed as more susceptible to threat actors' tactics that prey on human emotions, such as phishing perpetrated through email and websites. Data curated by the Anti-Phishing Working Group (APWG) shown in Figures 4 and 5 confirm the rapid rise in phishing.

FIGURE 4

Phishing Websites

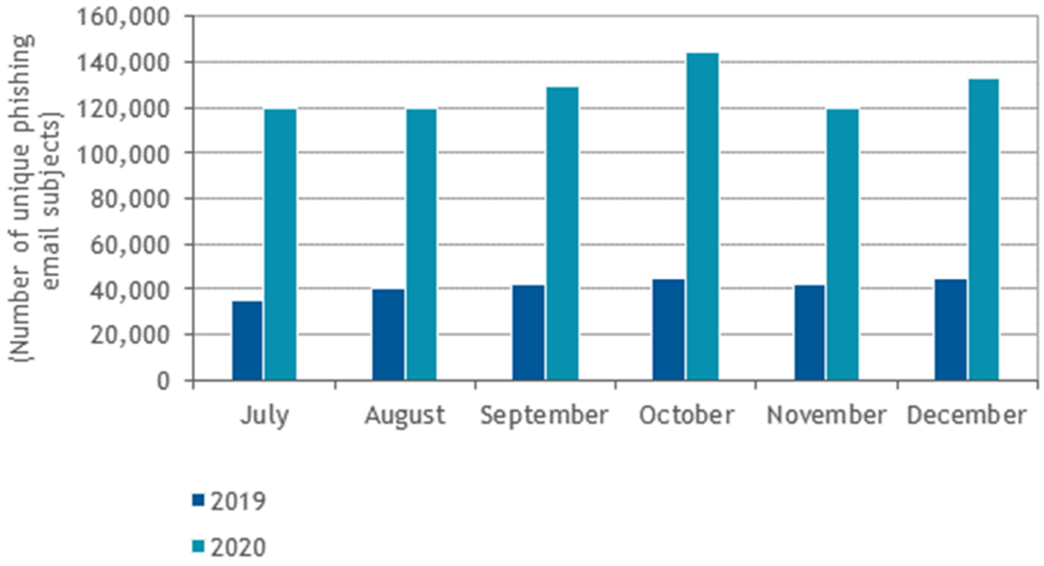


Note: Data shown is from APWG's *Phishing Activity Trends Reports* for 3Q19, 4Q19, 3Q20, and 4Q20.

Source: Anti-Phishing Working Group, 2019-2020

FIGURE 5

Unique Phishing Email Subjects



Note: Data shown is from APWG's *Phishing Activity Trends Reports* for 3Q19, 4Q19, 3Q20, and 4Q20.

Source: Anti-Phishing Working Group, 2019-2020

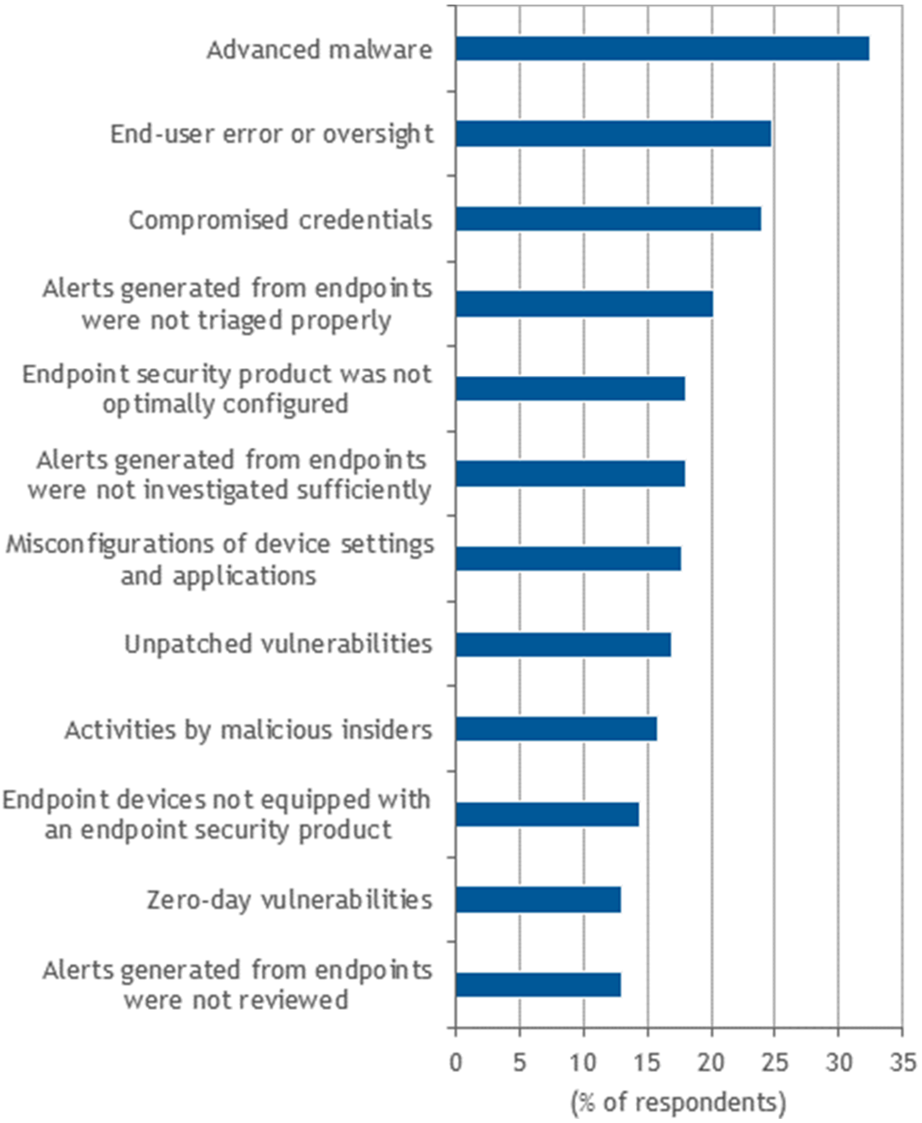
Malware is purposeful, and in 2020 and continuing into 2021, that purpose was frequently in support of ransomware attack campaigns. Phishing emails and websites are two common vectors for injecting ransomware onto end-user devices, but not the only ones. Independently confirmed by the U.S. National Cyber Investigative Joint Task Force (see "Ransomware: What it Is & What to Do About It," February 2021) and Coveware (see "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Payments," February 1, 2021), exploiting poorly configured and monitored remote desktop protocol (RDP) is another common vector used by threat actors to deposit ransomware onto end users' remote operating devices. Frequently, threat actors will use brute force credential guessing or stolen credentials harvested through phishing or purchased on the dark web to access end-user devices through RDP.

Security professionals are not blind to threat actors' tactics and WFH's risk-heightening circumstances. This is evident in IDC's December 2020 survey of security professionals. Advanced malware, end-user error or oversight (e.g., opened a document from an untrusted source, clicked on a link from an untrusted source, entered credentials into a phishing site), and compromised credentials were the most frequently cited top 3 contributors to security breaches (see Figure 6). Correspondingly, organizations responded in 2020 by fortifying their positions in endpoint security, contributing to the 14.4% year-over-year increase in the corporate endpoint security market and a higher 15.9% year-over-year increase in the modern endpoint security submarket.

FIGURE 6

Frequent Cited Contributors to Security Breaches

Q. Which of the following were the most frequent contributors to security breaches? (Select up to three.)



n = 367

Source: IDC's *EDR and XDR Survey*, December 2020

Also contributing to growth in the corporate endpoint security market is security teams' gravitation to post-compromise detection and response solutions, prominently EDR. These solutions are constructed to aid security operations and improve security efficacy (i.e., detect and mitigate more threats before damage to the organization occurs). IDC's research confirms this need. Various forms of incomplete endpoint alert management were cited as contributors to security breaches (refer back to Figure 6).

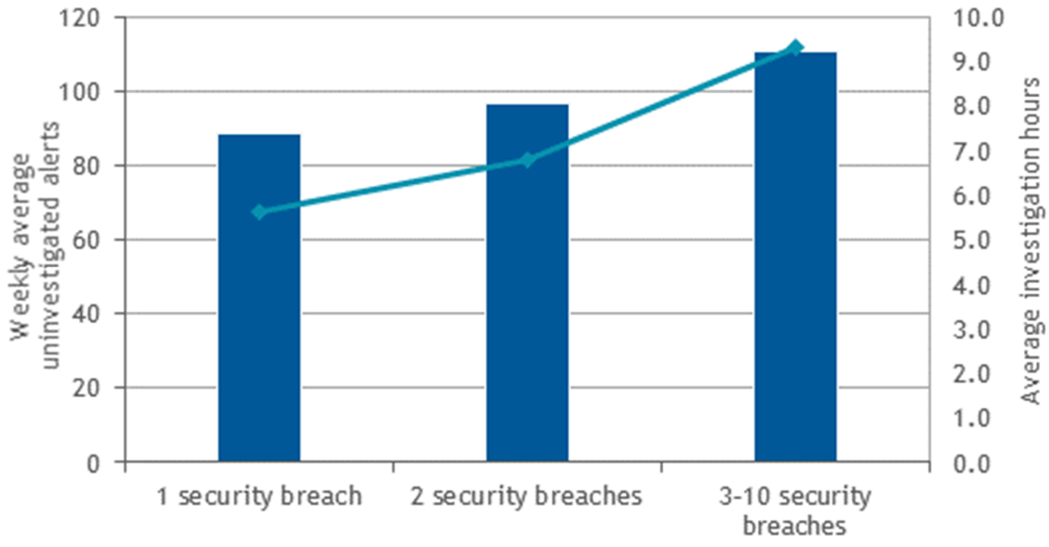
The positive correlation of security breaches with uninvestigated alerts and elapsed time to investigate triaged alerts is shown in Figure 7.

FIGURE 7

Positive Correlation of Major Security Breaches in Past Two Years with Uninvestigated Alerts and Elapsed Investigation Time

Q. *Approximately how many major security breaches has your organization had in the past two years that involved spending significant extra resources to rectify?*

Q. *How many suspicious alerts are your security and IT staff able to investigate, and how many go uninvestigated each week, regardless of the severity? After an alert has been triaged and deemed worthy of investigation by a Level 1 analyst or person performing a role/function of a Level 1 analyst, how quickly can your organization investigate suspicious threat activity?*



n = 432

Source: IDC's *EDR and XDR Survey*, December 2020

Accelerated transitions to the cloud was another contributor to the growth in the corporate endpoint security market. Detailed in *Worldwide Cloud Workload Security Market Share, 2020: Time to Shift Left* (IDC #US47837121, forthcoming), organizations' spending on security solutions to strengthen and protect their expanding use of virtual machines (VMs), containers, and serverless functions hosted in public cloud platforms continued to increase in 2020. This increase is incorporated into the 14.7% increase in the server security submarket. Restraining the increase in this submarket is the flat year-over-year expenditures on physical server security.

Significant Market Developments

Impacting 2020 were endpoint security expanding acquisitions of 2019. Three of the acquisitions contributed to 2020 year-over-year vendor growth rates that were above the market growth for three of the acquiring vendors. They were:

- BlackBerry's acquisition of Cylance in February 2019
- VMware's acquisition of Carbon Black in October 2019
- Fortinet's acquisition of enSilo in October 2019

Not all 2019 acquisitions produced above-market growth rates in 2020. Falling below-market growth were:

- HP Inc.'s acquisition of Bromium in September 2019
- Broadcom's acquisition of Symantec Enterprise in November 2019
- OpenText's acquisition of Carbonite in December 2019

In 2020, there was one notable acquisition completed: WatchGuard acquired Panda Security in June 2020. Like Symantec enterprise division changing ownership in late 2019, another ownership change involving a top 5 vendor is expected to be completed by the end of 2021. That ownership change is the acquisition of McAfee enterprise division by Symphony Technology Group.

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'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 commercial software markets for more than 25 years.

The market forecast 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 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

The endpoint security market encompasses products designed to protect physical and virtual endpoints from cyberattacks through detection of malicious code and behaviors and by limiting exposure through preventive techniques across operating systems (OSs) (e.g., Windows, Linux, macOS, iOS, and Android), and these products are offered to both the corporate and the consumer segments. Endpoint security software products provision security leveraging an endpoint agent, client, or the host operating system as a core or fundamental component.

Submarkets in endpoint security are modern endpoint security, server security, and consumer security. Modern endpoint security and server security are in the corporate market segment. In detail:

- **Modern endpoint security:** This submarket includes products that protect personal computing devices (PCDs; workstations, desktops, notebooks, and detachable tablets), mobile devices, and physical servers (when packaged with protection for PCDs) by detecting and responding to (e.g., alerting, blocking, removing, isolating, and reverting the endpoint to last known good state) cyberthreats that compromise endpoints through the installation of malware and/or by manipulating existing software code for malicious intent.

  Detection has evolved considerably over the years. Originally based on file signatures, detection is now fueled by multiple engines that also examine system, memory, application, and process behaviors and network communications. When detection is automatically conducted and immediate, this is called endpoint protection or endpoint protection platform (EPP).

  As threat actors continue to advance in their evasion techniques, EPP may not detect all instances of malicious code or process behaviors immediately. Endpoint detection and response (EDR) provides a second stage of detection. Operationally with EDR, multiple forms of telemetry are gathered, correlated, and analyzed to reach an infection verdict and then, as appropriate, initiate a response. Originally sold as a separate product from EPP and from a separate vendor, more common today is for the products to be packaged as an integrated endpoint security solution from the same vendor. A deviation from EPP and EDR being sold together is when EDR supplements native security features included in the device's operating system (e.g., Microsoft Defender).

  Managed EDR, where a third-party entity operates the EDR product for the user, has been a growing services category of the security market. In the sizing of modern endpoint security products, revenue for managed EDR is included when this services component is included in the same SKU as the modern endpoint security product. Commonly with product and services package, the product vendor is also the service provider (SP) but only extends service to endpoints installed with the vendor's endpoint agent.

Modern endpoint security products do more than detect malicious code and behaviors. They also offer features that thwart threats during the early stages of an attack and reduce the endpoint's attack surface area or exploitability. Early stage attack prevention and surface area reduction features 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; data loss prevention (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.

For many organizations, mobile devices (i.e., smartphones and tablets) are part of their device inventory, support essential operations, store sensitive data, and are interchangeably used by end users to access the same systems and applications as their PCDs. Consequently, threat actors target mobile devices just as they do PCDs. Modern endpoint security includes functionality that protects mobile devices either as a dedicated mobile threat management product or as a supported platform in a PCD-oriented endpoint security product.

- **Server security:**
  - **Physical server security solutions** maintain the integrity of hardware-based 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 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 in that traditional endpoint security products 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.
  - **Software-defined compute (SDC) workload** security solutions protect software-defined compute solutions, which encompass a number of compute abstraction technologies that are implemented at various layers of the system software stack. SDC 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. Workload security solutions are designed to maintain the integrity of SDC servers, providing protection features that include antimalware, desktop firewall, host intrusion detection, application control, and integrity monitoring. These products accomplish their goals by ensuring the system does not run malicious software that can compromise business applications and data on the servers. Like the other endpoint security submarkets, software-defined compute workload security solutions are a mutually exclusive category with no overlap with other categories such as physical server or antimalware and suites. Workload security solutions provide protection to three categories of SDC 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 an operating system segmentation technology, 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 and 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 maintains a database of resource state and policies.

- **Consumer security:** Products in this submarket are designed to protect consumer-owned PCDs and mobile device from cyberthreats. For vendors that serve both corporate and consumer segments, many of the same capabilities are similar but priced and packaged for consumers based on feature sets (e.g., standard versus premium) and number of devices (e.g., individual versus family).

  A common sales approach in the consumer market segment is to offer consumers a low-feature free version (e.g., limited to antivirus) from which to upsell to a paid, more feature-rich version. Another approach is free trial periods.

  Most vendors employ multiple channels to sell into the consumer segment. Channels include direct (online or packaged software), through resellers (e.g., internet service providers), through device manufacturers as preinstalled software, or incorporated into services offered by broadband service providers and internet SPs. Some vendors also offer complimentary versions of their consumer-branded products to their business customers to install on their personal devices with the option to upgrade to a version with more features for a subscription fee.

  Recognizing that devices are not the only targets for bad actors, consumer endpoint security vendors have branched out to offer products and services that more holistically protect the consumer's digital life. These products and services include but are not limited to connected home security, parental controls, password management, file backup, identity protection, consumer VPN, device performance tuning, and software management. Digital life protection products and services are sold individually or as part of a suite.

  The consumer segment includes estimated revenue for all digital life protection services sold individually or as part of multiproduct suites offered by traditional endpoint security and pure-play vendors. There is one exception. At this time, LifeLock-branded identity protection is excluded. This is done to maintain continuity with IDC's historical revenue estimates for the consumer segment and to minimize incongruity in comparing revenue with other vendors in the consumer segment. For them, identity protection is an ancillary offering. Conversely, LifeLock identity protection is in a unique class in premium capabilities and revenue size. IDC estimates LifeLock identity protection revenue to be over $800 million annually.

RELATED RESEARCH

- *IDC's Forecast Scenario Assumptions for the ICT Markets, April 2021* (IDC #US47665121, May 2021)
- *How Do Pandemic-Induced Changes in Work Practices and Technologies Impact 2021 Automation Investments?* (IDC #US47492121, March 2021)
- *Intel Provides New Tools to the Cybersecurity Task: The Results Could Be Game Changing* (IDC #US47495021, March 2021)
- *Insights from IDC's EDR and XDR 2020 Survey: Operational Challenges and Initiatives Are Abundant* (IDC #US47357921, January 2021)
- *Organizations Are Crying Out for Assistance in Measuring IT and Security* (IDC #US46984720, November 2020)
- *What Percentage of the Workforce Will Be Remote After a COVID-19 Vaccine?* (IDC #US46974820, November 2020)
- *Market Analysis Perspective: Worldwide Endpoint Security, 2020* (IDC #US46777719, August 2020)
- *Worldwide Corporate Endpoint Security Software Market Shares, 2019: Best of Suite Battle Looming in the Years Ahead* (IDC #US46734320, July 2020)
- *Which Endpoint Security Technologies Will SMBs Be Adopting Within the Next Year?* (IDC #US46345620, May 2020)

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