

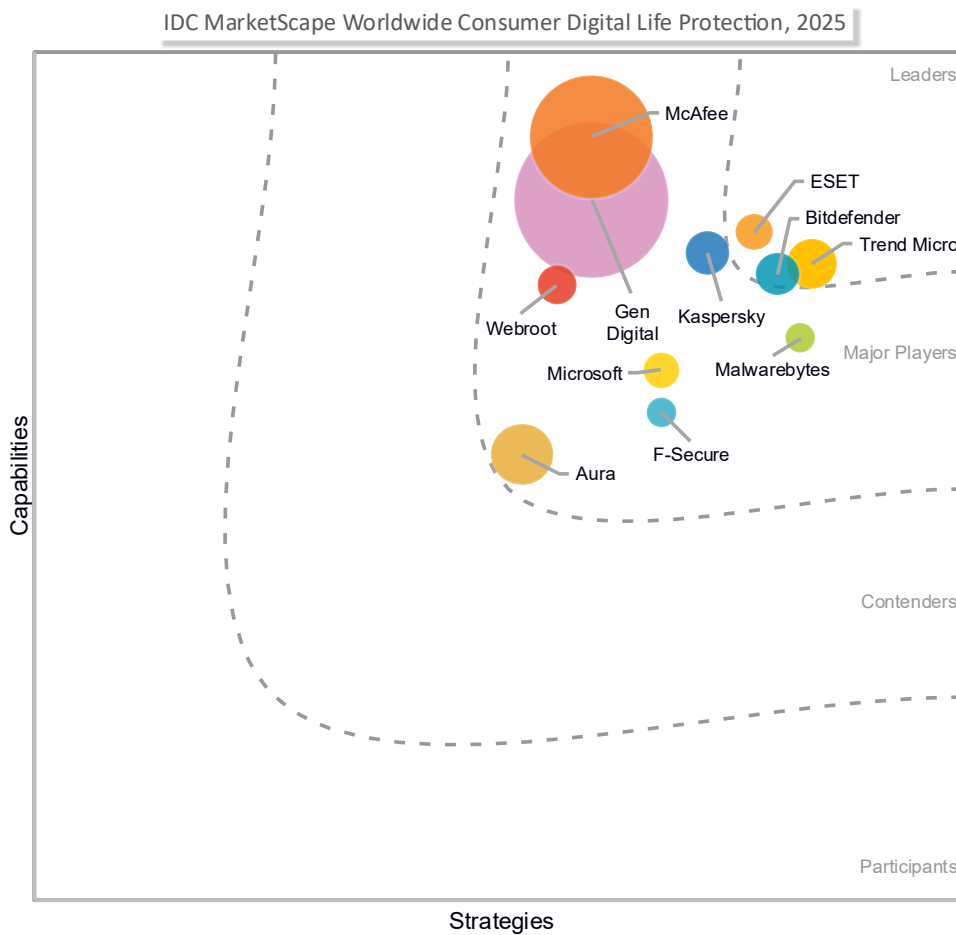
# IDC MarketScape: Worldwide Consumer Digital Life Protection 2025 Vendor Assessment

Mike Jude

## IDC MARKETSCAPE FIGURE

**FIGURE 1**

### IDC MarketScape Worldwide Consumer Digital Life Protection Vendor Assessment



Source: IDC, 2025

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

## IDC OPINION

---

Traditionally, the consumer cybersecurity market was considered to be essentially a "done deal" with nothing much happening. In fact, it was primarily considered to be synonymous with antivirus and antimalware. For most consumers, solutions were often provided with new computers and users might or might not update those installations.

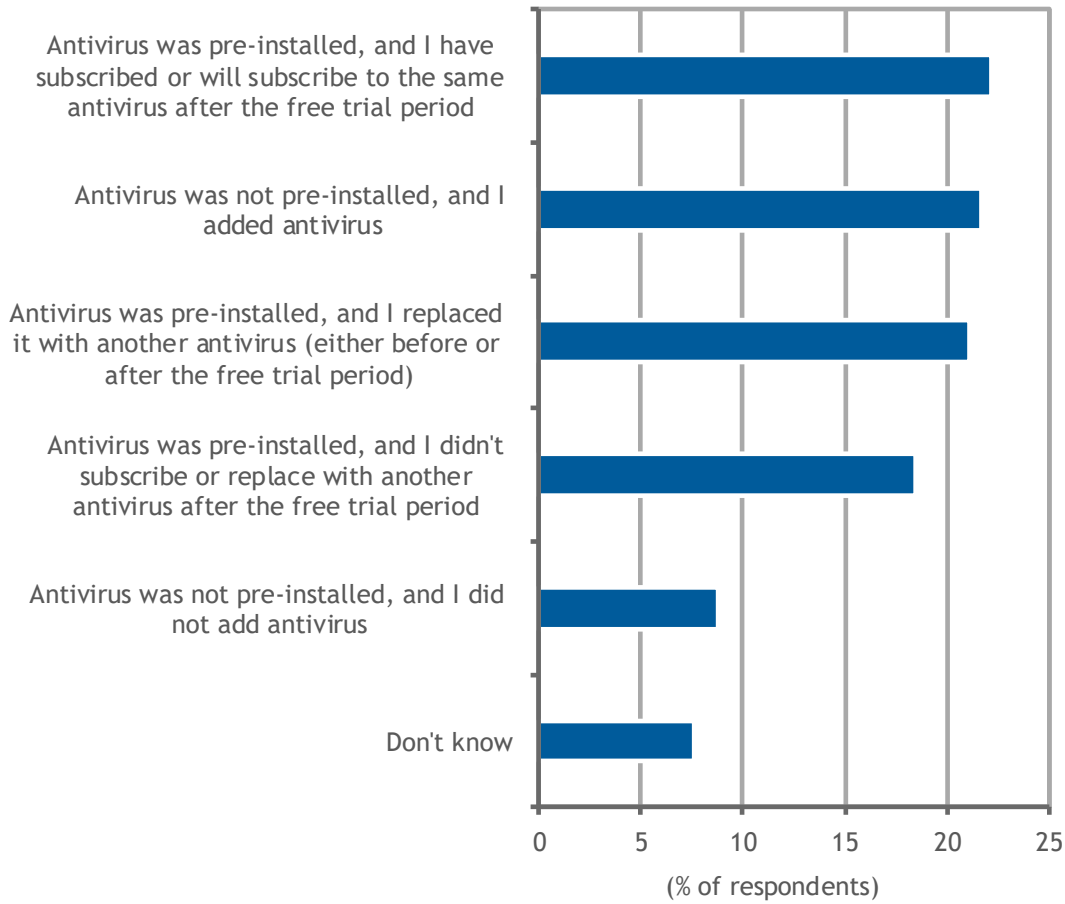
However, in the past decade, the consumer space has become markedly more complex with threat actors targeting user identity information, financial records, and other personal data. Increasingly, consumers have come to the realization that real harm can result if their online activities are compromised.

The increasing threat has impacted consumers' willingness to adopt more comprehensive cybersecurity tools and hygiene. As Figure 2 demonstrates, where consumers were once likely to simply depend on cybersecurity solutions that came with their computers, now they are equally likely to adopt third-party solutions outside of hardware acquisitions.

**FIGURE 2**

**Consumer Methods for Obtaining Antivirus**

Q. Regarding antivirus for your most recently purchased PC, which of the following applies?



Unweighted valid n = 855

Base = respondents who purchased more than 0 PCs (including laptops) for their household in the past two years

Notes:

This survey is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

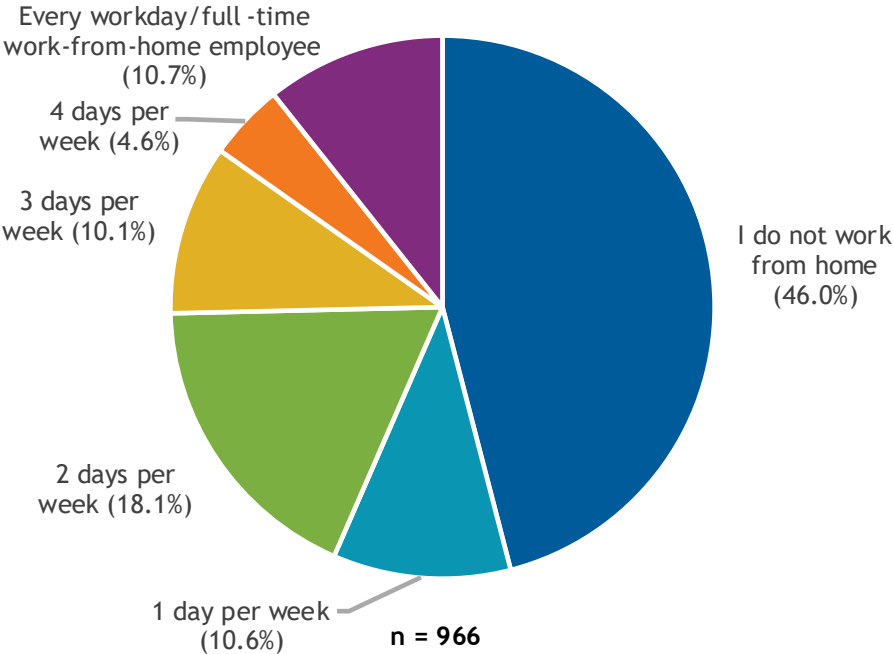
Source: IDC's *Consumer Digital Life Protection Survey*, February 2025

In addition, consumers' cybersecurity requirements have evolved beyond antivirus and antimalware to include privacy protection, parental controls, and data protection. This evolution of the consumer space is also complicated by the increasing adoption of remote work and distributed work requirements. Enterprises that used to depend on control of the endpoint to ensure corporate cybersecurity now must contend with employees whose work-at-home activities may not utilize the most capable cybersecurity protections. As a result, consumers that wish to work remotely are being forced to adopt endpoint protections that conform to enterprise standards. As Figure 3 illustrates, only 46% of those consumers surveyed indicate that they never work from home.

**FIGURE 3**

**Consumer Days Worked from Home**

Q. How many days do you routinely work from your home?



Base = respondents who indicated employees are employed full time or part time

Notes:

This survey is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Consumer Digital Life Protection Survey*, February 2025

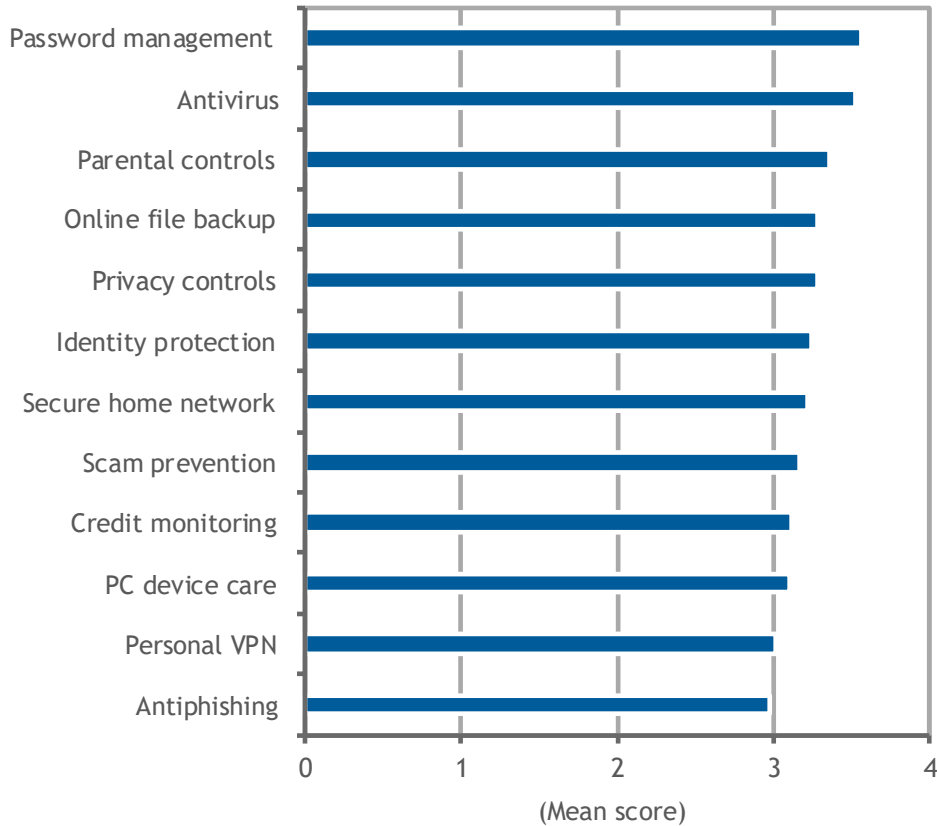
As a result of the increasing consumer needs, cybersecurity vendors are being challenged to upgrade their offerings beyond simple antivirus solutions. As the IDC MarketScape graphic illustrates, the consumer endpoint protection market is characterized by vendors whose value propositions are very similar. The Major Players portion of the market tends to dominate in terms of revenue. Leaders are primarily those that are pushing the innovation and integration capabilities that lead to the delivery of solutions that resonate with small office/home office (SOHO) users.

A war is being waged by vendors for market supremacy; however, their value propositions are often drowned out by marketing noise that is being generated by contending messages that tend to sound the same, especially to relatively unsophisticated consumers. This is reflected in the confusion of survey respondents when asked to rate their familiarity with the various solutions that can be adopted to protect their personal computing environments (see Figure 4).

**FIGURE 4**

**Consumer Familiarity with Cybersecurity Solutions**

Q. How would you rate your familiarity with the following digital life protection technologies?



Unweighted valid n = 1,500

Base = all respondents

Notes:

This survey is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Consumer Digital Life Protection Survey*, February 2025

The challenge for all of the vendors in this study, as a consequence of the background noise, is to find a way to punch their messaging through to reach the consumer.

## IDC MARKETSCOPE VENDOR INCLUSION CRITERIA

---

To be included in this study, vendors must offer a software product or products that deliver endpoint protection platform (EPP) capabilities to the consumer endpoint protection market that may include the following:

- Protecting consumer PCs, tablets, smartphones, and home networks from cyberthreats (e.g., antivirus, secure home network)
- Ensuring online communications are private (e.g., personal VPN)
- Monitoring and resolving theft and abuse of an individual's identity and credit ratings (e.g., credit monitoring, dark web monitoring, identity protection)
- Reviewing and recommending privacy settings for mobile apps, browsers, and/or social media sites (e.g., privacy controls)
- Strengthening online account passwords and simplifying password use (e.g., password management)
- Storing a copy of digital files (e.g., photos, videos, and documents) in an online storage site (e.g., online file back-up)
- Extending parental controls to children's online activities and encouraging appropriate online behaviors
- Scam prevention
- Improving PC performance (e.g., device care)

All products in the previous list must support end-user devices that run the latest version of Windows or macOS.

In addition, each vendor needed to satisfy a minimum 2024 calendar year-earned (based on GAAP reporting) worldwide revenue for the set of products in the preceding list, excluding revenue from products sold in vendor-provided managed services bundles.

## ADVICE FOR TECHNOLOGY BUYERS

---

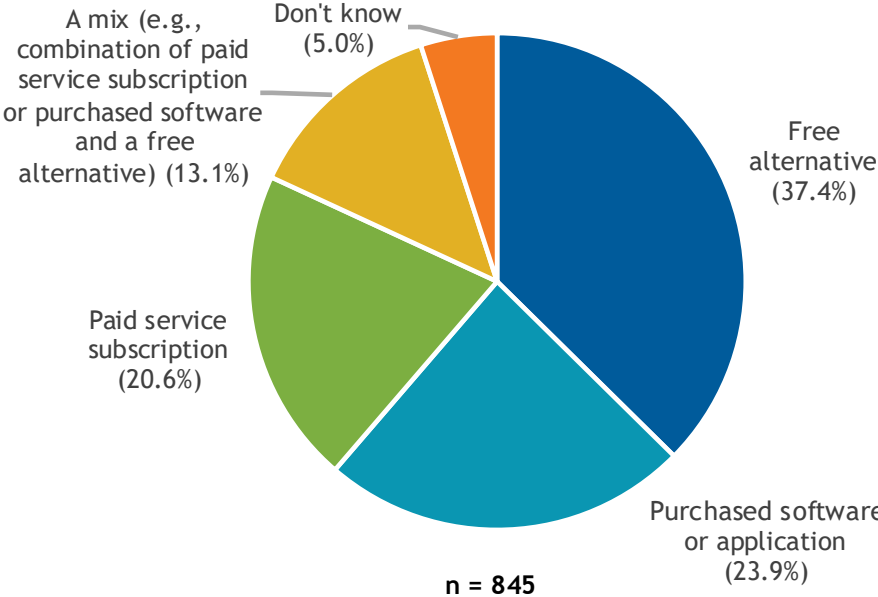
Considering the noisy environment, relatively unsophisticated users, and increasing need for capable solutions that transcend personal use to office use, how will market players achieve success in the consumer digital life protection space? The knee-jerk answer is that effective marketing is increasingly essential. Yet this approach simply leads to even more competing noise. As IDC research discloses, consumers are already overwhelmed with the claims and counterclaims that characterize the current market messaging.

IDC survey data reveals that consumers are primarily driven by tools and technologies with which they are already familiar. As Figure 5 shows, consumers currently depend on free solutions (provided on new hardware), and only 24% are willing to buy solutions.

**FIGURE 5**

**Consumer Cybersecurity Acquisition Strategies**

Q. How did you acquire each of the following technologies you indicated your household uses?



Base = respondents who indicated their organization is currently using a personal VPN

Notes:

This survey is managed by IDC's Global Primary Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's Consumer Digital Life Protection Survey, February 2025

**VENDOR SUMMARY PROFILES**

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

## **Aura**

Aura is positioned in the Major Players category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

Aura is a digital life protection platform designed to address the growing risks of identity theft, financial fraud, and cyberthreats. As reliance on digital tools increases, Aura offers a unified solution to safeguard personal information and digital assets. Its services include identity theft protection, credit monitoring, online privacy tools, and device security, all integrated into a user-friendly platform. Aura's combination of advanced technology and accessible design makes it a practical choice for individuals and families. In addition, Aura's offerings resonate with the SOHO market, where entrepreneurs and small business owners often require straightforward yet effective tools to protect their digital operations and sensitive data.

### **Strengths**

Aura provides a comprehensive suite of services that address multiple aspects of digital security. Its identity theft monitoring, financial fraud alerts, and device security tools work together to offer users a robust defense against a variety of threats. The platform's intuitive design ensures accessibility for users with varying levels of technical expertise, making it easy to navigate and implement. Aura's proactive threat detection capabilities, powered by advanced algorithms and real-time monitoring, help users mitigate risks before they escalate.

The family-oriented plans offered by Aura are particularly appealing to households, allowing multiple members to benefit from its services under a single subscription. This feature also aligns well with the SOHO market, where small business owners often manage both personal and professional digital security needs. Aura's dedicated customer support further enhances its appeal by providing assistance in resolving issues and optimizing the use of its platform. These strengths make Aura a versatile option for consumers and small businesses seeking reliable digital life protection.

### **Challenges**

As the other vendors in this study, Aura operates in a competitive cybersecurity market, where many companies offer similar services. To maintain its position, Aura must continue to innovate and differentiate its offerings. Its premium pricing may deter budget-conscious consumers, even though its services provide significant value. Some users may perceive Aura's solutions as expensive compared to free or lower-cost alternatives, which could limit its appeal to certain segments of the market.

Another challenge is the need for greater consumer awareness about the importance of digital life protection. Many individuals and small business owners remain unaware

of the risks associated with their online presence, requiring Aura to invest in educational campaigns to highlight the value of its services. As cyberthreats evolve, Aura must also stay ahead by updating its technology and expanding its capabilities to address emerging risks effectively.

## **Consider Aura When**

Aura is a suitable choice for individuals, families, and small business owners seeking reliable and comprehensive digital life protection. It is particularly well-suited for users who prioritize proactive security and ease of use. Those concerned about identity theft or financial fraud will benefit from Aura's monitoring and resolution services. Families will find its family-oriented plans appealing, while SOHO users will appreciate its straightforward design and ability to address both personal and professional security needs. For anyone seeking an accessible and versatile cybersecurity solution, Aura provides a practical option.

## **Bitdefender**

Bitdefender is positioned in the Leaders category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

Bitdefender is a cybersecurity provider focused on delivering effective digital protection through technical expertise and innovation. The company offers tools designed to safeguard user privacy, identity, and digital assets, including antivirus software, internet security suites, VPN services, scam prevention, password management and parental controls. These solutions aim to protect personal devices and sensitive information while remaining accessible to a broad range of users. Bitdefender's approach resonates with both individual consumers and the small office/home office market, where small business owners often require reliable yet straightforward tools to secure their operations and data. By combining professional-grade security with user-friendly design, Bitdefender supports users in navigating the digital world securely.

## **Strengths**

Bitdefender's strengths lie in its ability to deliver effective cybersecurity solutions supported by advanced technology and a user-focused design. Its tools consistently perform well in independent testing for detection accuracy, performance, and minimizing false positives. The company's emphasis on research and development has led to the creation of technologies that address digital privacy, identity protection, and asset security.

Bitdefender's threat intelligence system incorporates device-level sensors, cloud honeypots, and network-level sensors, providing comprehensive protection for individual consumers, connected devices within a home or small office network. This

capability is particularly relevant to the SOHO market, where small business owners often manage multiple devices and require seamless security across their operations. In addition, Bitdefender collaborates with law enforcement agencies globally, contributing expertise to investigations and efforts to combat cybercrime.

The company's user-friendly design ensures accessibility for individuals and small businesses with varying levels of technical expertise. Its parental controls and VPN services further enhance its appeal to families and SOHO users who value privacy and control over their digital environments. Finally, its artificial intelligence (AI)-powered chatbot can alert users to potential scams in text messages, emails, social media content, links, or QR codes.

## **Challenges**

While Bitdefender's paid solutions are priced competitively for the value they provide, some consumers may perceive them as costly compared to free or lower-cost alternatives. The variety of product options can also be overwhelming for certain users, requiring clear communication to help them select the appropriate solution for their needs.

As cyberthreats evolve, Bitdefender must continuously update its technology and expand its capabilities to address emerging risks. The company also faces the challenge of educating consumers and small business owners about the importance of digital life protection, which is essential for driving adoption and demonstrating the value of its services.

## **Consider Bitdefender When**

Bitdefender is a practical choice for individuals, families, and small business owners seeking reliable digital life protection. It is particularly suitable for users who prioritize effective threat detection and professional-grade security. Those concerned about malware, ransomware, scams or phishing attacks can benefit from Bitdefender's technology and reputation. Families will find its parental control features useful, while SOHO users will appreciate its ability to secure multiple devices within a network. For anyone seeking accessible and dependable cybersecurity solutions, Bitdefender provides a balanced option that caters to both personal and professional needs.

## **ESET**

ESET is positioned in the Leaders category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

ESET is a cybersecurity company that emphasizes a prevention-first approach to protecting digital lives. By integrating multilayered technology, artificial intelligence,

human expertise, and live cloud protection, ESET aims to shield users from a wide range of cyberthreats. Its solutions are designed to provide security across commonly used platforms, offering tools such as antivirus software, internet security suites, and device protection. ESET's lightweight design ensures that its security solutions minimize the impact on device performance, making them suitable for users who prioritize efficiency. The ESET HOME platform further enhances usability by enabling centralized management of security settings and devices, making it a practical choice for individuals, families, and small office/home office users who require streamlined protection across multiple devices.

## **Strengths**

ESET's focus on prevention allows it to proactively address threats through advanced technologies and real-time cloud protection. Its lightweight solutions are designed to maintain device performance while delivering effective security, which is particularly appealing to SOHO users who often rely on resource-constrained systems. The integration of artificial intelligence and human expertise enables ESET to adapt to evolving threats, ensuring its solutions remain relevant in a dynamic cybersecurity landscape.

The ESET HOME platform simplifies the management of security settings and devices. This centralized control is especially beneficial for SOHO users managing multiple devices, as it reduces complexity and enhances efficiency. ESET's compatibility with multiple platforms ensures that users can protect a diverse range of devices, from smartphones to computers, making it a versatile option for both personal and professional use.

## **Challenges**

While ESET's lightweight design is effective, some users may believe its offerings are less comprehensive. This perception may require ESET to better communicate the value of its prevention-first approach and the practical benefits of its solutions.

The need for greater consumer awareness about cybersecurity remains a challenge, particularly for SOHO users who may underestimate the risks associated with their digital operations. ESET must invest in education and outreach to highlight the importance of digital life protection and the advantages of its offerings.

## **Consider ESET When**

ESET is a suitable choice for individuals, families, and SOHO users seeking reliable and lightweight digital life protection. Its prevention-first approach is ideal for those who value proactive security measures that do not compromise device performance. Not only SOHO users managing multiple devices will benefit from the ESET HOME platform,

which simplifies security management and monitoring. ESET's compatibility across major platforms makes it a practical option for users seeking comprehensive coverage for their digital lives, whether for personal or professional purposes.

## **F-Secure**

F-Secure is positioned in the Major Players category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

F-Secure is a cybersecurity company focused on protecting consumers' digital lives through solutions designed to safeguard privacy, secure devices, and protect online identities. Its offerings combine advanced technology, artificial intelligence, and human expertise to deliver security across multiple platforms. F-Secure emphasizes ease of use and integration, allowing users to manage their digital safety without compromising device performance. The company's solutions are tailored to address the evolving landscape of cyberthreats, making them suitable for individuals, families, and small office/home office users who require practical and efficient protection for their digital environments.

## **Strengths**

F-Secure's approach to cybersecurity leverages artificial intelligence and cloud-based protection to detect and prevent threats in real time. Its focus on lightweight security ensures that users can maintain device performance while benefiting from effective protection. This is particularly relevant to SOHO users, who often rely on resource-constrained systems and require solutions that do not disrupt their workflows.

The company's centralized management platforms simplify the process of monitoring and controlling security settings, making them accessible to users with varying levels of technical expertise. This feature is especially beneficial for SOHO users managing multiple devices, as it provides a streamlined way to oversee security across personal and professional systems. F-Secure's compatibility with a variety of platforms further enhances its appeal, allowing users to secure a diverse range of devices, from smartphones to computers.

F-Secure's adaptability to emerging threats ensures that its solutions remain relevant in a rapidly changing cybersecurity landscape. Its emphasis on user-friendly design and practical functionality makes it a viable option for both individual consumers and small business owners seeking reliable protection.

## **Challenges**

F-Secure operates in a competitive cybersecurity market, where many providers offer feature-rich solutions. While its tools are effective and accessible, some users may

perceive them not as comprehensive. This perception may require F-Secure to better communicate the value of its offerings and the practical benefits they provide.

The need for greater consumer awareness about cybersecurity remains a challenge, particularly for SOHO users who may underestimate the risks associated with their digital operations. F-Secure must invest in education and outreach to highlight the importance of digital life protection and the advantages of its solutions. In addition, as cyberthreats grow more sophisticated, the company must continuously update its technology and expand its capabilities to address emerging risks effectively.

## **Consider F-Secure When**

F-Secure is a practical choice for individuals, families, and SOHO users seeking reliable and easy-to-use digital life protection. Its lightweight design and centralized management features make it particularly suitable for users managing multiple devices, whether for personal or professional purposes. SOHO users who value efficiency and compatibility across mainstream platforms will find F-Secure's solutions appealing. For those seeking accessible cybersecurity tools that balance simplicity with functionality, F-Secure provides a dependable option.

## **Gen Digital**

Gen Digital is positioned in the Major Players category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

Gen Digital is a global provider of cybersecurity solutions designed to protect digital lives in an increasingly connected world. With a portfolio that includes well-known brands such as Norton and Avast, the company offers tools and services aimed at safeguarding personal information, securing devices, and ensuring online privacy. Its offerings include antivirus software, identity theft protection, VPN services, and parental controls, all integrated into user-friendly platforms. Gen Digital emphasizes proactive threat detection and prevention, helping users navigate the digital landscape securely. Beyond individual and family use, Gen Digital's solutions resonate with the small office/home office market, where entrepreneurs and small business owners require accessible and effective tools to protect their operations and sensitive data.

## **Strengths**

Gen Digital's ability to deliver comprehensive cybersecurity solutions tailored to diverse needs is a key strength. Its portfolio of trusted brands provides users with a variety of options, catering to different preferences and requirements. The company leverages advanced technologies to address threats such as malware, phishing, ransomware, and identity theft, ensuring users can protect their digital lives effectively.

The focus on user experience is evident in Gen Digital's intuitive design and accessible platforms, which simplify the management of digital security for individuals, families, and SOHO users. Multidevice protection is particularly relevant to the SOHO market, where small business owners often manage multiple devices across personal and professional use. Gen Digital's global presence also enables it to provide localized support and expertise, further enhancing its appeal to users in different regions.

For SOHO users, the integration of multiple layers of security into a single subscription offers convenience and efficiency, allowing them to focus on their business operations without worrying about cybersecurity complexities.

## **Challenges**

While its solutions are effective, some consumers may perceive them as costly compared to free or lower-cost alternatives. This perception may require the company to better communicate the value of its offerings, particularly to budget-conscious users.

The complexity of Gen Digital's product portfolio can also be overwhelming for some users, including SOHO customers, who may lack the time or expertise to evaluate multiple options. Clear communication and guidance are essential to help users select the right solutions for their needs. In addition, as cyberthreats evolve, Gen Digital must continuously update its technology and expand its capabilities to address emerging risks effectively.

## **Consider Gen Digital When**

Gen Digital is a practical choice for individuals, families, and SOHO users seeking reliable and comprehensive digital life protection. It is particularly suitable for users who value trusted brands and prefer solutions that integrate multiple layers of security. SOHO users managing multiple devices will benefit from its multidevice protection and streamlined subscription options. Those concerned about identity theft, malware, or online privacy will find its tools and services effective for safeguarding their digital environments. For users seeking accessible cybersecurity solutions that balance functionality and ease of use, Gen Digital provides a dependable option.

## **Kaspersky**

Kaspersky is positioned in the Major Players category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

Kaspersky offers a broad suite of solutions that go beyond traditional antivirus and standalone security tools. Its portfolio includes VPN services, password management, parental controls, identity leak checkers, spam and scam call protection, and a recently launched eSIM solution for travelers. These offerings are designed not only to secure

users' digital lives but also to make them simpler, more convenient, and secure by default — enabling users to navigate the connected world with confidence and ease across platforms.

Powered by AI technologies, Kaspersky's solutions proactively detect and neutralize threats — including zero-day vulnerabilities — before they cause harm. The company's integrated approach makes it a practical choice for individuals, families, and small office/home office users who need reliable, streamlined security across multiple devices. For SOHO users, Kaspersky's all-in-one platform combines privacy and security tools offering efficiency and ease of use, which is particularly valuable for small businesses managing limited resources.

## **Strengths**

Kaspersky's ability to deliver a diverse range of security tools tailored to modern needs is a key strength. Its AI-driven technologies enable proactive threat detection and mitigation, addressing risks such as zero-day threats, malware, phishing, and ransomware. Features like unlimited VPN with router support, password manager and data leak checkers, included in most tiers, enhance privacy and identity protection, while parental controls and spam call protection cater to families and individuals seeking comprehensive digital safety. Its intuitive interface and seamless experience across Windows, macOS, Android, and iOS ensure users can manage all devices under one subscription.

For SOHO users, Kaspersky's solutions provide a balance between functionality and accessibility. Its user-friendly design simplifies the management of security settings and devices, which is particularly beneficial for small business owners who may lack dedicated IT support. The ability to secure multiple devices under a single subscription aligns well with the needs of SOHO users, offering comprehensive protection for both personal and professional use.

Kaspersky also maintains a low system footprint, delivering robust protection without degrading device performance — a major advantage for SOHO and older device users. Kaspersky's adaptability to the evolving threat landscape ensures its products remain relevant, while its global presence supports users in diverse regions. However, its resonance with the SOHO market is particularly notable, as its tools address the dual demands of privacy and operational security in small business environments.

Kaspersky's streamlined product portfolio consists of three clearly defined tiers, each offering increasing value and functionality. This structure makes it easier for consumers and small businesses to choose the right solution based on their needs.

## Challenges

Kaspersky faces challenges stemming from its perceived connection to Russia, which has led to restrictions in established markets. These geopolitical concerns limit its ability to compete globally and may deter some consumers from adopting its solutions. For SOHO users operating in restricted regions, this could necessitate exploring alternative providers.

## Consider Kaspersky When

Kaspersky is a practical choice for consumers and SOHO users looking for comprehensive, AI-powered protection with built-in privacy tools and minimal system impact. Its feature-rich plans deliver excellent value — especially for users seeking a single subscription that covers antivirus, VPN, identity protection, and more.

For those not affected by geopolitical restrictions, Kaspersky offers a mature, high-performance security suite in core protection, privacy, and user experience. However, organizations or users in restricted jurisdictions may need to evaluate alternative providers.

## Malwarebytes

Malwarebytes is positioned in the Major Players category in this 2025 IDC MarketScape for the worldwide consumer digital life protection.

Malwarebytes is a global provider of cybersecurity, privacy, and identity protection solutions, offering a suite of consumer-focused products designed to empower users to manage and secure their digital life, regardless of their security knowledge or experience. Its tools address a variety of cybersecurity needs, including malware detection and removal, privacy protection, scam detection, and identity protection. Malwarebytes has also doubled down on mobile, investing in mobile-first features, like Scam Guard, its AI-powered chat companion that offers on-the-go security advice to help users avoid scams. With an emphasis on accessibility, Malwarebytes consumer solutions provide expert guidance and user-friendly products that enable individuals, families, and small, boutique businesses to take control of their personal security, data and identity. The company's solutions cater to diverse lifestyles and budgets, making them suitable for a wide range of users, including small office/home office environments. For SOHO users, Malwarebytes offers straightforward tools that help secure devices and sensitive information without requiring extensive technical expertise or resources.

## Strengths

Malwarebytes focuses on delivering cybersecurity, privacy, and identity solutions via an integrated solution that prioritizes ease of use and accessibility. Its products are designed to detect and remove malware, ransomware, phishing sites, malicious URLs and other online threats, providing users with a reliable defense against cyber-risks alongside actionable guidance to improve their cybersecurity posture. The company's emphasis on privacy and identity protection ensures that users can safeguard their personal information while navigating the digital landscape through additional products such as Identity Theft Protection, Personal Data Remover, and a free digital footprint scan to identify exposed or and breached information. Recognizing that digital lives and their associated threats have largely shifted to mobile devices, Malwarebytes designs all its products with mobile compatibility in mind, aligning with how people now spend their time online.

For SOHO users, Malwarebytes resonates as a practical option due to its intuitive design and straightforward functionality. Small business owners often face resource constraints and limited IT support, making Malwarebytes' user-friendly tools particularly appealing. The ability to manage security settings and protect devices without requiring advanced technical expertise aligns well with the needs of SOHO environments. Malwarebytes' focus on empowering users through expert guidance further enhances its appeal, as it provides small business owners with the knowledge and tools needed to secure their operations effectively.

The company's global reach and ability to cater to diverse budgets make it accessible to a wide range of users, including those in SOHO settings who require cost-effective solutions that balance functionality and simplicity.

## Challenges

To maintain its relevance, Malwarebytes must continue to innovate and differentiate its offerings. While its products are effective and accessible, some users may perceive them as less comprehensive compared to more extensive feature sets. Malwarebytes has taken steps to remedy this and has recently released a variety of new features, including an AI-powered scam detector, Windows Firewall Control, a new in-depth scan option, and Tools to optimize device performance and privacy settings, among others. This perception may require Malwarebytes to better communicate the value of its solutions, particularly to SOHO users who may be evaluating multiple options.

The need for greater consumer awareness about cybersecurity remains a challenge, especially for small business owners who may underestimate the risks associated with their digital operations. Malwarebytes must invest in education and outreach to highlight the importance of its offerings and drive adoption. In addition, as cyberthreats

evolve, the company must continuously update its technology and expand its capabilities to address emerging risks effectively. Recently, Malwarebytes added additional security and detection layers for infostealers that emphasize how this silent threat is targeting consumers.

## **Consider Malwarebytes When**

Malwarebytes is a practical choice for individuals, families, and SOHO users seeking accessible and effective digital life protection. Its straightforward solutions are particularly suitable for small business owners who value simplicity and need tools that prioritize malware detection and privacy protection. SOHO users looking to take control of their data and identity without relying on extensive IT resources will benefit from Malwarebytes' user-friendly products and expert guidance. For those seeking reliable cybersecurity solutions that cater to diverse needs and budgets, Malwarebytes provides an option that focuses on functionality and ease of use.

## **McAfee**

McAfee is positioned in the Major Players category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

McAfee is a recognized provider of cybersecurity solutions, offering tools designed to protect digital lives by safeguarding devices, personal data, and online privacy. Its products cater to the needs of individuals, families, and small office/home office users in an increasingly connected world. McAfee's offerings include antivirus software, identity theft protection, VPN services, Scam Detection and parental controls, all integrated into user-friendly platforms. The company's focus on delivering accessible and reliable security solutions helps users navigate the digital landscape securely. For SOHO users, McAfee's ability to provide multidevice protection and privacy tools within a single subscription aligns well with the operational needs of small businesses, where simplicity and efficiency are critical.

## **Strengths**

McAfee's ability to deliver comprehensive security solutions tailored to diverse needs is a key strength. Its antivirus software is designed to detect and neutralize malware, ransomware, and other online threats, providing users with effective protection against cyber-risks. Features such as VPN services and identity theft protection enhance privacy and security, while parental controls address the needs of families managing their children's online activities. Their AI-powered scam detection is included in their core consumer security plans and covers text, email and deepfake detection. McAfee's multidevice protection is particularly relevant, allowing users to secure smartphones, tablets, and computers under a single subscription. This flexibility simplifies security

management across devices, which is essential for both individuals and small businesses operating with limited IT resources. McAfee's intuitive design and accessible platforms further enhance its appeal, enabling users to manage security settings and monitor devices without requiring advanced technical expertise.

The company's global presence supports users in diverse regions, while its focus on delivering practical solutions ensures that its tools remain relevant to consumers.

## **Challenges**

While McAfee's solutions are effective, some users may perceive them as costly compared to free or lower-cost alternatives. This perception may require McAfee to better communicate the value of its offerings, particularly to budget-conscious small office/home office users.

The complexity of McAfee's product portfolio can also be overwhelming for some users who may lack the time or expertise to evaluate multiple options. Clear communication and guidance are essential to help users select the appropriate solutions for their needs. In addition, as cyberthreats evolve, McAfee must continuously update its technology and expand its capabilities to address emerging risks effectively.

## **Consider McAfee When**

McAfee is a practical choice for individuals and families seeking reliable and comprehensive digital life protection. Its multidevice protection and privacy tools make it particularly suitable for small business owners who need to secure both personal and professional devices efficiently. Those concerned about malware, identity theft, or online privacy will benefit from McAfee's tools and services. Families will find its parental control features useful, while SOHO users will appreciate its ability to streamline security management across multiple devices. For users seeking accessible cybersecurity solutions that balance functionality and ease of use, McAfee provides a dependable option.

## **Microsoft**

Microsoft is positioned in the Major Players category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

Microsoft provides consumer-focused digital life protection solutions that are integrated into its broader ecosystem of software and services. With tools such as Microsoft Defender, the company offers security features designed to protect devices, data, and online activities. Microsoft's approach emphasizes seamless integration with its Windows operating system and other products, allowing users to access protection without additional complexity. Its offerings include antivirus and anti-malware

capabilities, phishing protection, and parental controls, all aimed at safeguarding personal information and enhancing digital safety. For small office/home office users, Microsoft's integration of security tools within its existing ecosystem offers convenience and efficiency, making it a practical choice for those managing both personal and professional digital devices.

## **Strengths**

Microsoft's integration of its security solutions within its existing ecosystem is a key strength. Microsoft Defender, embedded directly into the Windows operating system, provides users with real-time protection without requiring additional software installation. This approach simplifies cybersecurity for SOHO users, who often prioritize ease of use and efficiency in managing their digital operations.

The company's security tools address common threats such as malware, phishing, and ransomware, offering a foundational level of protection that aligns well with the needs of SOHO environments. Features like parental controls and phishing protection further enhance its appeal to families and small business owners concerned about online safety. Microsoft's global presence and extensive resources enable it to continuously update and improve its security offerings, ensuring they remain relevant in a rapidly evolving threat landscape.

For SOHO users, Microsoft's focus on user experience is particularly beneficial. Its intuitive design makes security tools accessible to individuals with varying levels of technical expertise, reducing the need for dedicated IT support. The integration of security features within the Windows ecosystem also allows SOHO users to streamline their operations, combining productivity tools with cybersecurity in a single platform.

## **Challenges**

Although Microsoft Defender is effective for basic protection, some SOHO users may find it lacking compared to standalone security products with more extensive capabilities. This perception may require Microsoft to better communicate the value of its integrated approach to cybersecurity.

In addition, the company's reputation as primarily a software and operating system provider may lead some consumers, including SOHO users, to overlook its cybersecurity offerings. Microsoft must address this challenge by educating users about the capabilities of its built-in security tools, which are often underutilized despite their effectiveness. As cyberthreats grow more sophisticated, the company must also continue to innovate and expand its security features to meet the evolving needs of its users.

## Consider Microsoft When

Microsoft is a practical choice for individuals, families, and SOHO users seeking straightforward and integrated digital life protection. Its built-in security tools, such as Microsoft Defender, are particularly suitable for users who rely on the Windows operating system and prefer solutions that are seamlessly integrated into their devices. SOHO users looking for basic protection against malware, phishing, and ransomware will benefit from Microsoft's offerings, which combine accessibility with efficiency. For those seeking reliable cybersecurity within the Microsoft ecosystem, the company's solutions provide a balanced option that supports both personal and professional needs.

## Trend Micro

Trend Micro is positioned in the Leaders category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

Trend Micro is one of the established global cybersecurity companies focused on protecting digital lives by ensuring the safe exchange of information across connected devices and online activities. Its consumer-focused solutions are designed to safeguard personal information, identity, and privacy but also to proactively protect from scam tactics employed by cybercriminals. The first cybersecurity vendor to deliver a dedicated anti-scam solution, Trend Micro's offerings include features such as threat detection and scam prevention powered by real-time AI, proactive privacy protection, and tools for securing multiple devices under a unified platform. The company emphasizes delivering effective protection at a value that appeals to a broad range of users, including small office/home office environments. For SOHO users, Trend Micro's ability to integrate security across devices and provide straightforward tools aligns well with the operational needs of small businesses that prioritize simplicity and efficiency.

## Strengths

Trend Micro's ability to deliver protection through advanced technologies and through its deep and long-standing threat research operations are its key strengths. Its real-time AI-powered threat detection and anti-scam capabilities enable the identification and mitigation of cyber-risks as they emerge and have been the foundation to its ability to address threats such as malware, phishing, ransomware, and the proliferation of scams hitting the market. The company's focus on proactive privacy protection ensures that users' personal information and online activities remain secure from unauthorized access, which is particularly relevant for SOHO users handling sensitive business data.

Trend Micro's solutions are designed to be user-friendly, making them accessible to individuals, families, and small business owners with varying levels of technical

expertise. The integration of its tools across connected devices provides seamless protection, allowing SOHO users to secure smartphones, tablets, and computers under a single subscription. This unified approach simplifies security management, which is essential for small businesses operating with limited IT resources.

For SOHO users, Trend Micro's emphasis on balancing functionality with ease of use makes it a practical option for addressing both personal and professional cybersecurity needs.

## **Challenges**

While Trend Micro's solutions are effective and extensive, some users may perceive them as less feature rich than others in the market. This perception may require Trend Micro to better communicate the value of its offerings, particularly to SOHO users who may be evaluating multiple options.

The need for greater consumer awareness about the importance of digital life protection remains a challenge, especially for small business owners who may underestimate the risks associated with their digital operations. Trend Micro must invest in outreach to highlight the relevance of its solutions and drive adoption. In addition, as cyberthreats evolve, the company must continuously update its technology and expand its capabilities to address emerging risks effectively.

## **Consider Trend Micro When**

Trend Micro is a practical choice for individuals, families, and SOHO users seeking accessible and effective digital life protection. Its real-time AI-powered threat detection and proactive privacy safeguards — including modern anti-scam protection — make it particularly suitable for consumers and SOHO users who value straightforward solutions that protect sensitive data and devices while lowering their risk of becoming victims of scams. SOHO users looking to secure multiple connected devices under a unified platform will benefit from Trend Micro's integrated approach, which simplifies security management. For those seeking cybersecurity solutions that balance functionality with ease of use, Trend Micro provides an option that aligns with both personal and professional needs.

## **Webroot**

Webroot is positioned in the Major Players category in this 2025 IDC MarketScape for worldwide consumer digital life protection.

OpenText, Webroot's parent company, is a global provider of information management solutions that also extends its expertise into consumer digital life protection. The company offers tools designed to safeguard personal data, secure devices, and protect

online privacy. OpenText's approach to cybersecurity emphasizes the integration of advanced technologies with user-friendly platforms, delivering protection against evolving digital threats. Its offerings include endpoint security, data encryption, and identity management solutions, catering to individuals, families, and small office/home office users seeking effective ways to secure their digital lives.

## **Strengths**

Webroot offers high-performance cybersecurity solutions for home and SOHO users, built on a cloud-native AI- and machine learning–driven threat architecture that enables real-time threat detection with minimal system impact.

Webroot's lightweight design ensures efficient protection without compromising device speed. Its multilayered security suite includes antivirus, secure VPN, identity monitoring, dark web surveillance, text scam detection, unlimited cloud backup, and financial protection features such as \$1 million fraud expense and stolen funds reimbursement.

Strategic integrations with Allstate Identity Protection, LastPass, and Carbonite Backup (also part of OpenText) extend Webroot's capabilities across key consumer digital life protection (CDLP) pillars, including identity, personal data protection, and data resilience. This makes Webroot particularly relevant for SOHO users managing sensitive operational and client data across multiple devices.

## **Challenges**

Webroot operates in a highly competitive consumer cybersecurity market, where global players often have extensive international reach, substantial marketing investments, and deeply integrated security ecosystems. In contrast, Webroot's market presence remains more concentrated in North America and select regions such as the U.K., Australia, and Japan.

Although Webroot has been a player in the cybersecurity market for nearly three decades, its CDLP offerings — branded as Webroot Premium and Webroot Total Protection — are relatively new. This lack of name recognition presents a challenge when competing in a crowded market with many competing product offerings.

As a result, despite its technical strengths and strategic partnerships, Webroot faces the challenge of increasing competitive pressure to address home and small office users. A targeted, go-to-market strategy with the right investments in awareness campaigns is essential to communicate the value of its CDLP capabilities and differentiate its offering in a crowded and brand-driven landscape.

## Consider Webroot When

Webroot is a practical choice for individuals, families, and SOHO users seeking reliable digital life protection. It is particularly suitable for users who value performance advanced threat protection, data and identity protection for individuals or families. For those seeking cybersecurity solutions that align with operational efficiency, Webroot provides a balanced option that caters to both personal and professional needs.

## APPENDIX

---

### Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies. In the case of this IDC MarketScape, capabilities are rated higher than strategies since IDC survey data indicates that consumers value functionality over a vendor's market strategy. For this reason, capabilities are weighted at 60% over strategies, at 40%.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor builds/delivers capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

### IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the

vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior and capability.

## **Market Definition**

Consumer digital life protection (CDLP) captures the broader set of technologies that vendors offer to consumers to address a range of consumers' cybersecurity and digital protection needs. Currently, CDLP technologies include personal device security (i.e., antivirus), device care, connected home security, identity privacy, parental controls, consumer VPN, identity monitoring, password management, multifactor authentication, and cloud file backup. CDLP vendors can offer each technology as a separate product or in packages of CDLP technologies and features.

The number of vendors participating in the CDLP market is considerable and is not limited to independent software vendors (ISVs). Prominent platform providers (e.g., Apple, Google, and Microsoft) also offer CDLP technologies as embedded platform capabilities for free or subscription cloud services or as a combination of both.

ISVs sell to consumers through a variety of channels. Prominent among those are direct to the consumer and through OEMs (device manufacturers and communication services providers). Less prominent but still relevant are the CDLP products offered to employees as part of or an option in their employee benefit packages.

IDC's estimate and forecast of the CDLP market is limited to the subset of ISVs that sell paid-for personal device security products. For these ISVs, all their CDLP product revenue (i.e., personal) and device security (i.e., antivirus, device care, connected home security, identity privacy, parental controls, consumer VPN, identity monitoring, password management, multifactor authentication, and cloud file backup) are included in IDC's market estimate and forecast.

## **Strategies and Capabilities Criteria**

As noted previously, this analysis assessed a vendor's strategies and capabilities with respect to market needs. Each axis was based on various significant variables, which when multiplied by weighting factors based on survey data, generated an overall assessment.

The key measures for success are outlined in Tables 1 and 2.

**TABLE 1****Key Strategy Measures for Success: Worldwide Consumer Digital Life Protection**

Strategies Criteria	Definition	Weight (%)
Innovation	R&D investment and staffing to support R&D activities	15.00
Delivery	Plans for expansion or improvement of deliver channel	15.00
Financial/funding	Degree to which the vendor is financially viable or will be in the future	10.00
Longevity in market	First introduced date	10.00
Value proposition	Consumer and SOHO offerings	10.00
AI strategy	Plans for AI	10.00
Consumer growth	Percentage of consumer growth	10.00
Distribution of revenue	Percentage of revenue dependent on the US market	10.00
SOHO strategy	Plans for delivering SOHO solutions	10.00
Total		100.00

Source: IDC, 2025

**TABLE 2****Key Capability Measures for Success: Worldwide Consumer Digital Life Protection**

Capabilities Criteria	Definition	Weight (%)
Availability	Methods to obtain solution	10.00
Brand recognition	Market leading or market following	5.00
Customer satisfaction	NPS or other metrics showing consumer approval	10.00
Customer service delivery	Multiple options for acquiring vendor solutions	10.00
	Guarantees	
Functionality or offering capabilities	Ability to work with enterprise offerings	65.00
	Portfolio offerings	
Total		100.00

Source: IDC, 2025

### Related Research

- *IDC MarketScape Criteria: Worldwide High-Speed Inkjet Press 2025 Vendor Assessment* (IDC #US53766025, September 2025)
- *Next-Gen Document Services* (IDC #IDC\_P26350, September 2025)
- *IDC MarketScape Criteria: Worldwide Document Scanner 2025 Vendor Assessment* (IDC #US53670825, July 2025)
- *IDC MarketScape Criteria: Worldwide Print Security Solutions and Services Hardcopy 2025 Vendor Assessment* (IDC #US52334025, May 2025)
- *Worldwide Consumer Digital Life Protection Software Forecast, 2025–2029: Evolution Driving Growth* (IDC #US53184925, March 2025)

### Synopsis

This IDC study highlights the evolution of consumer cybersecurity needs beyond traditional antivirus, driven by rising threats to identity, privacy, and data. The study evaluates major vendors' capabilities and strategies, emphasizing innovation, integration, and user-centric design for individuals, families, and SOHO users. Success hinges on clear messaging, comprehensive protection, and adaptability to emerging risks in a crowded, rapidly changing market.

"As digital threats evolve, consumers and small businesses will need to rise above the marketing noise to truly protect their digital lives — or remain vulnerable in a crowded market. The challenge to vendors in this space is to address user needs while delivering a compelling value message that rises above the background noise in this competitive market." — Mike Jude, research director for Endpoint Protection at IDC

## ABOUT IDC

---

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

### Global Headquarters

140 Kendrick Street  
Building B  
Needham, MA 02494  
USA  
508.872.8200  
Twitter: @IDC  
blogs.idc.com  
www.idc.com

---

#### Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit [www.idc.com/about/worldwideoffices](http://www.idc.com/about/worldwideoffices). Please contact IDC at [customerservice@idc.com](mailto:customerservice@idc.com) for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2025 IDC. Reproduction is forbidden unless authorized. All rights reserved.