IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Avast

As consumers' digital connectedness expands, security and privacy risks rise. Network operators are positioned to mitigate these risks by offering Digital Life Protection services delivered in partnership with an experienced technology provider.

A Comprehensive Solution Can Enable Operators' Success in Digital Life Protection

May 2020

Written by: Michael Suby, Research Vice President, Security and Trust

Introduction

Consumers' digital connectedness is ramping upward. IDC projects that annual shipments of smart home devices (e.g., video entertainment, home monitoring and security, speakers, lighting, and thermostats) and wearables will expand by at least a factor of four from 2016 to 2024 (see Figure 1). Additional confirmation of this trend comes from an in-depth home network study conducted by Stanford University and the University of Illinois Urbana-Champaign (*All Things Considered: An Analysis of IoT Devices on Home Networks*) in January 2019. According to this study, two-thirds of homes in North America had at least one smart home device; 25% had three or more smart home devices. When we factor in personal computers and mobile devices, the stay-at-home impact of COVID-19, and increasing bandwidth capacities in home broadband and mobile (4G and 5G) networks, it is clear that household connectedness has transformed from a series of point-in-time sessions to a mesh of continuous, high-bandwidth connections.

AT A GLANCE

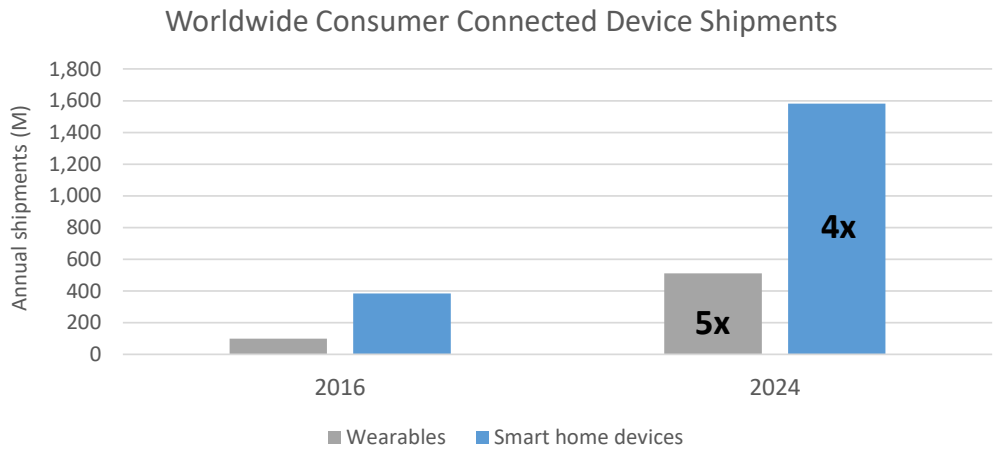
WHAT'S IMPORTANT

Consumers' connectedness is on a continuous upward trajectory as are the risks to consumers' security and privacy. Network operators are strategically positioned to mitigate these risks through Digital Life Protection services.

KEY TAKEAWAYS

To be successful in Digital Life Protection services, the network operator needs a partner that is steeped in security experience and expertise and advanced technologies and that possesses a powerful data lake.

FIGURE 1: ***Digital Connectedness Is on the Rise***



Source: IDC, 2020

The dark side of connectedness is that it presents risks. The potential for malware infection, remote device takeover, privacy violation, and information and identity theft expands with each added device and the accumulation of time online. Compounding the problem is the presence of easily exploitable vulnerabilities in home networks. In the Stanford study, open communication protocols and interfaces and weak administrative credentials were often uncovered during vulnerability scans of smart home devices and home routers.

Parents have additional concerns. How exposed are their children to online predators, cyberbullying, and inappropriate content? How can they instill good online habits when they lack visibility into their children's online activities and the means to define and enforce boundaries?

This dark side, however, presents a silver lining for network operators now and well into the future. As providers of the digital highway with established customer relationships, network operators are positioned to serve their customers with safe and secure connected experiences through Digital Life Protection services. Deployed at scale, these new services can add to both monthly revenues and profits for operators while delivering a superior customer experience.

As consumers' online activities span broadband and mobile networks, a platform delivering Digital Life Protection services must be designed to seamlessly support all network types. Whether the operator's network is exclusively broadband or mobile, or a hybrid, the platform must be inherently flexible.

Cross-network flexibility is just one element operators should weigh in pursuit of this business opportunity. Working with a technology partner that can adapt to changing customer needs, devices, networks, and cyberthreats is another. In this Technology Spotlight, IDC describes the attributes operators should include in successfully bringing a Digital Life Protection solution to market and the criteria they should consider in selecting a technology partner.

Consumers' Views on Security and Privacy in Smart Homes

For a growing number of consumers, Wi-Fi and high-bandwidth internet connectivity have transformed the home into an always-on network hub. Yet despite the convenience and added functionality smart homes offer, consumers harbor security and privacy worries. Data from a recent IDC survey of over 1,500 U.S. consumers highlights these concerns.

- 56% of survey respondents are highly concerned about the security of their smart home devices.
- An additional 20% of survey respondents are somewhat concerned about the security of their smart home devices.
- Older survey respondents expressed higher levels of concerns about the security of their smart home devices.

Smart home concerns span security and privacy as half of security-concerned respondents identified the following as major issues:

- Someone controlling my devices without my permission
- Someone stealing my identity
- Having my password discovered

- Having my conversations recorded
- Having a virus in my device or network

The survey also highlights consumers' incomplete understanding of the personal and financial consequences of an unsecured smart home. When better informed about these consequences and their contributors, consumers are more likely to take actions to strengthen the security of their smart homes and protection of their privacy.

Solution Attributes for Digital Life Protection

Digital Life Protection services must be well aligned with consumer expectations to succeed. IDC identified the following solution attributes as essential to alignment:

- Delivering a unified and holistic consumer experience
- Protecting consumers continuously
- Improving family safety
- Adapting automatically to changing circumstances
- Generating operational insights

Delivering a Unified and Holistic Consumer Experience

In today's rapidly evolving digital world, consumers often pick and stitch together services from a host of sources — frequently with unsatisfactory results. A Digital Life Protection solution eliminates this difficult task and improves the customer experience by uniting multiple services into a single package to meet a range of customer needs, such as:

- Securing all personal devices
- Detecting and mitigating threats in and out of the home network
- Ensuring privacy when connecting through untrusted networks
- Enabling parents to view and oversee their children's online activities
- Lessening password fatigue
- Providing alerts when evidence of identity theft is present
- Protecting personal files through secure backup

Protecting Consumers Continuously

Consumers are online within and outside their homes, so the protective shields of a Digital Life Protection solution must be portable. Moreover, the protection of consumers' portable devices — smartphones, laptops, and wearables — should be equally portable and transparent.

Improving Family Safety

Parenting styles naturally adapt as children age and become more independent. A Digital Life Protection solution must also be adaptable in offering the right amount of visibility and controls for each family. A solution that provides visibility into family members' online activities and defines guidelines is important for families with younger children. For families with older children, location tracking provides assurance to parents, letting them know where their children are and when they enter locations that are off-limits as well as when and where their devices are turned off. Older children can also benefit from parental coaching made possible through visibility into their online activities (e.g., when a child's late-night online gaming interferes with his or her daytime responsibilities). Whether a child is just discovering the online world or is a veteran, digital dangers can be subtle and unnoticed. A Digital Life Protection solution equipped with machine learning (ML) algorithms can surface these dangers and facilitate fact-based discourse between parents and their children.

Adapting Automatically to Changing Circumstances

Today's home networks encompass an expanding number of smart devices. Initially, the consumer may have a good understanding of the home's smart device inventory. But as devices multiply, certainty fades. Of equal concern, built-in security is often secondary to a device's novelty, affordability, and core functionality. A Digital Life Protection solution provides a much-needed safety net. It automatically identifies and granularly classifies each device (e.g., type, model, manufacturer, and firmware and operating system versions) and monitors its behaviors without compromising device or network performance. Also, new devices can be prevented from connecting until approved. If abnormal behaviors are detected from any of the approved devices, automated and consumer-guided remediation can be taken.

The extensiveness of the ML algorithms used in device identification, classification, and threat detection is an important attribute in a solution. Other key attributes are the quality, diversity, and volume of data used to initially build and continuously improve the algorithms. Together, time-tested ML algorithms and a continuous flow of high-quality data strengthen the credibility of the solution in serving the ever-changing device inventory in connected homes.

Generating Operational Insights

Gathering telemetry from consumers' devices and home networks and combining it with information from the operator's network can help with more than parental controls and security issues. Operators can proactively leverage this telemetry to serve their customers in several ways. For example, by gauging the performance of the home network and connected devices, operators are in an improved position to pinpoint and address performance issues before they escalate into customer support incidents. They can also respond with fact-based recommendations tailored to each customer, such as upgrading bandwidth, deploying signal-strengthening Wi-Fi extenders, changing device settings or location, and installing software patches. In so doing, operators enhance the customer experience, strengthen loyalty, and increase upselling opportunities.

Critical Technology Partner Capabilities in Driving Operator Success

This paper has described the attributes a Digital Life Protection solution should have to be successful in the market. But what is success from the operators' perspective, and how do technology partners support that success? Like solution attributes, operator success is not singularly defined. Rather, operators justifiably gravitate to market opportunities that

have robust potential to support multiple business objectives. Those objectives span increasing average revenue per user (ARPU), strengthening customer loyalty, reducing costs, and ensuring budget predictability.

From IDC's perspective, the technology partner should help an operator concentrate on the following:

- Standardizing on a software-based platform architecture
- Expanding market opportunities
- Educating consumers on risk

Standardizing on a Software-Based Platform Architecture

The prevailing trend in information and communication technology is cross-functional integration on a software-based platform architecture. This same trend is present in Digital Life Protection as a platform architecture benefits an operator in several ways:

- **Coverage comprehensiveness.** By using a single platform, the operator can protect home networks, connected devices (independent of location), how users connect (home broadband, 4G, 5G, and public Wi-Fi), and customers' digital lives. The platform can also provide a single portal experience. A platform approach benefits the operator by minimizing the need and incremental expense of engaging with multiple providers to deliver a unified consumer experience.
- **Integrability.** Colocated or deployed in close proximity to a network operator's network, the platform incorporates the operator's real-time telemetry data to create consumer value (e.g., location-aware parental controls and alerting) and support (e.g., preventive behind-the-router visibility into performance issues in the smart home network and connecting devices). The positive outcomes extend to customer loyalty, stability and growth in ARPU, and reduction in customer support calls as issues are resolved.
- **Extensibility.** As a platform, the suite of Digital Life Protection services is plug-in extensible, further contributing to customer loyalty, ARPU, and budget certainty.
- **Modularity.** Modularity is important on two fronts. The first is personalizing the service experience for each customer. With modularity, the network operator can offer services à la carte and through persona-based bundles. The second front is enabling flexibility. Like their customers, network operators also need flexibility to select the service options that suit their needs now and in the future. Modularity based on a software-based platform makes this possible.
- **Lightness.** With computational heavy lifting and data triangulation conducted in a platform off the customer's network and devices, device and router resource requirements (e.g., storage, CPU, battery) are minimized. Customers' concerns about advanced security coming at the expense of performance can be marginalized. The operator benefits by achieving stable ARPU, solidifying customer loyalty, and reducing the number of support calls.
- **Host portability.** As a software-based platform, Digital Life Protection can be hosted at locations optimized for the provider and its customers. A future deployment option is as a virtual network function (VNF) deployed at 5G network edges. This would be a potential ARPU boost for 5G operators.

Expanding Market Opportunities

The extensibility of a Digital Life Protection platform expands operators' market opportunities into services traditionally purchased by consumers as standalone software applications. Endpoint security (i.e., antivirus and web content filtering), consumer VPN, parental control, password management, file backup, and identity protection are examples of security and privacy applications that consumers have directly purchased from independent software vendors (ISVs). Under the umbrella of Digital Life Protection, the operator can become the centralized store for these services and earn a commission from each. Customer experience, leading to increased ARPU and loyalty, is boosted by one-stop shopping, a single portal interface, and confidence in purchasing curated services from a trusted source, the operator.

Extensibility serves all network types, whether one is an exclusive terrestrial broadband provider, a mobile operator, or a converged network provider. The operator is not required to be the owner of the network to gain from market extensibility. Virtual network operators can benefit, too.

Educating Consumers on Risk

According to IDC's survey of smart home consumers, security and privacy concerns vary. Some consumers are only somewhat concerned, while others are not concerned at all. These groups justify their lack of concern in the following ways:

- The chance of someone hacking my smart home device or network is very small.
- The information that someone could obtain by hacking my devices or network is harmless or insignificant.
- If someone obtains my information, there is not much they could do with it anyway.
- I feel comfortable with the protections in place to remedy any security breach.

To IDC, these survey results point to consumers' inadequate understanding of the potential risks. Working with a technology partner can assist operators in bridging this gap in understanding and contribute to a higher take rate of Digital Life Protection services. Partners may also be able to assist with data on cyberthreats and risks in escalating tiers of personalization:

- The first tier is localized data based on anonymized data from other customers residing in the same geographic area.
- The second tier is a tailored risk profile based on consumer-provided input (e.g., family demographics, device inventory, and online activities).
- The third tier is a highly personalized risk profile based on collected data on the consumer's current environment (e.g., through a vulnerability scan and risk assessment of home network and devices).

Considering Avast

Avast has over three decades of experience in serving the consumer segment with security and privacy products and over 15 years of partnering with network operators around the world. This experience has led to product designs that are easy for consumers to purchase, deploy, and use and flexible partnerships with carrier-grade integrations and support. The company was also an early developer of artificial intelligence (AI) models to detect and blunt cyberattacks. Because AI model effectiveness is dependent on data, Avast's lengthy cybersecurity tenure has allowed the company to amass volumes of data to initially train its AI models, and its ongoing data collection from its global customer base drives continuous model refinement.

In addition to extensive data on cyberattacks, Avast has five years of experience in analyzing home Wi-Fi networks for vulnerabilities and compromised connected devices with its Wi-Fi Inspector tool. Demonstrating its extensiveness, Wi-Fi Inspector scanned over 240 million connected devices each month during the past six months. A feature of Avast's endpoint security agent, Wi-Fi Inspector has a 90% accuracy rate in device classification, according to the company. Supporting its operator customers, Avast has been educating consumers on home network risks.

The company has assembled an extensive Digital Life Protection suite. Built for modularity, Avast's product suite includes:

- Endpoint security for PCs and smartphones
- Consumer VPN for PCs and smartphones
- Connected home security
- Parental controls
- Password management

Avast's connected home security technology is available as software for modern home routers and as an appliance to coexist with older router models. For network operators with a mix of routers in their customers' homes, the combination of software and appliance enables the marketing of connected home security across its entire customer base without first requiring router upgrades. Avast's parental control product is available for iOS and Android smartphones. Avast's experience with consumer VPN has produced dividends. IDC estimates that Avast is the second largest consumer VPN provider in this fast-growing global market.

Further, Avast is rapidly accumulating experience with network operators. One of Avast's most recent operator customers is Wind Tre. In June 2019, Wind Tre launched its Smart Life offering using Avast's technology. Aiming for a 5G future, Avast is packaging its solution set as a VNF for deployment in 5G cloud edges.

Challenges

Avast's challenges in the Digital Life Protection market are not unique. Consumer ambivalence toward security and privacy risks and tepid willingness to pay for additional services are the greatest barriers in developing relationships with network operators and growing this market. At the same time, the home broadband market is already competitive and will intensify with the availability of 5G. Consequently, network operators, whether they are terrestrial or mobile, or both, must foster competitive differentiation, and Digital Life Protection is a logical extension of their existing connectivity services.

Separately, there are numerous ISVs in the Digital Life Protection market. However, many have limited product sets and little time in the market, with brand positions that are untested. Conversely, there are formidable ISVs with product sets equal or even greater in number to Avast's, and they are established brands among consumers and network operators. Over time, ISVs with shallow product sets will expand through in-house development, resell, and acquisition. Inevitably, the passage of time will intensify competition among Digital Life Protection ISVs vying for operator partnerships. For all ISVs, including Avast, continuously strengthening their capabilities to serve operators in growing the Digital Life Protection market is an absolute requirement to remain viable.

Conclusion

IDC believes the market for Digital Life Protection services for consumers will grow. The ubiquity and established customer relationships of network operators place them in the pole position to profit by seizing this growing business opportunity. Yet consumers do not fully grasp the risks that are rising in their digital lives and are less sure how to address them. Therefore, network operators must invest in customer education, tailored service offerings, and reliable service delivery to succeed in this market. Selection of an experienced and dedicated technology partner becomes a critical linchpin for success.

The nascent Digital Life Protection services market is too rich for network operators to ignore.

About the Analyst

Michael Suby, *Research Vice President, Security and Trust*

Michael Suby is a Research Vice President in IDC's Security and Trust research practice. In his role, Mr. Suby concentrates on endpoint security and, in collaboration with IDC team members, engages in a wide and evolving spectrum of cybersecurity topics. In the broad endpoint security landscape, Mr. Suby's research focuses on impactful developments in solutions, markets, cyberthreats, and end-user requirements in the following endpoint security categories: endpoint protection, physical and virtual server security, information protection and control, endpoint management, and consumer digital wellness.

MESSAGE FROM THE SPONSOR

Avast has over 15 years of working directly with global network operators and integrating with their network infrastructure. They deploy their solutions at various network perimeters that include white-labeled mobile apps, router firmware, and as 5G virtual networking functions (VNF). Avast extends security, privacy, and family safety to all devices, regardless of how and where they connect.

As an international company, Avast brings together extensive threat and customer research to build solutions that meet the challenges of today and into the future. To learn more about Avast's solutions, partnerships, and research, visit ***avast.com/partners***.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com