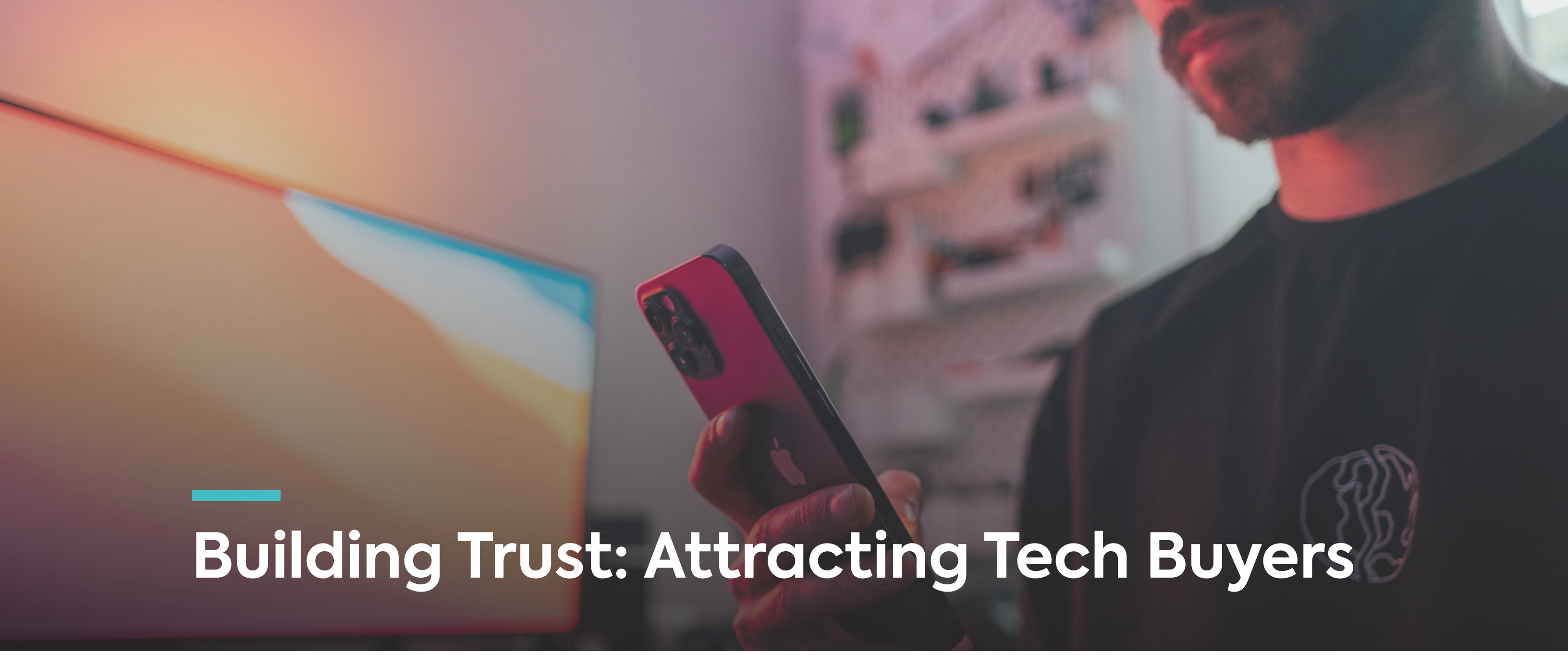
PARKS ASSOCIATES

Data Privacy and Security in the Connected Home

DEVELOPED FOR:

Iris

Powered by Generali



Building Trust: Attracting Tech Buyers

Consumers' homes are growing evermore complicated as an increasing number of internet-connected products are purchased and used regularly. However, consumers are oftentimes unaware of how to properly manage and secure these products to prevent possible data and privacy loss. Certain products are not designed to promote end users' security and privacy and require special handling on the part of consumers to ensure data is protected.

With identity theft, fraud, and invasive data collection growing, smart home platforms and their customers are increasingly at risk. Parks Associates' research has found that some 72% of smart home product owners are concerned with the security of the personal data that is collected and transmitted by their smart home products. Public events such as hacking incidents, data breaches, and overly broad data collection by technology companies further heighten consumer concerns.

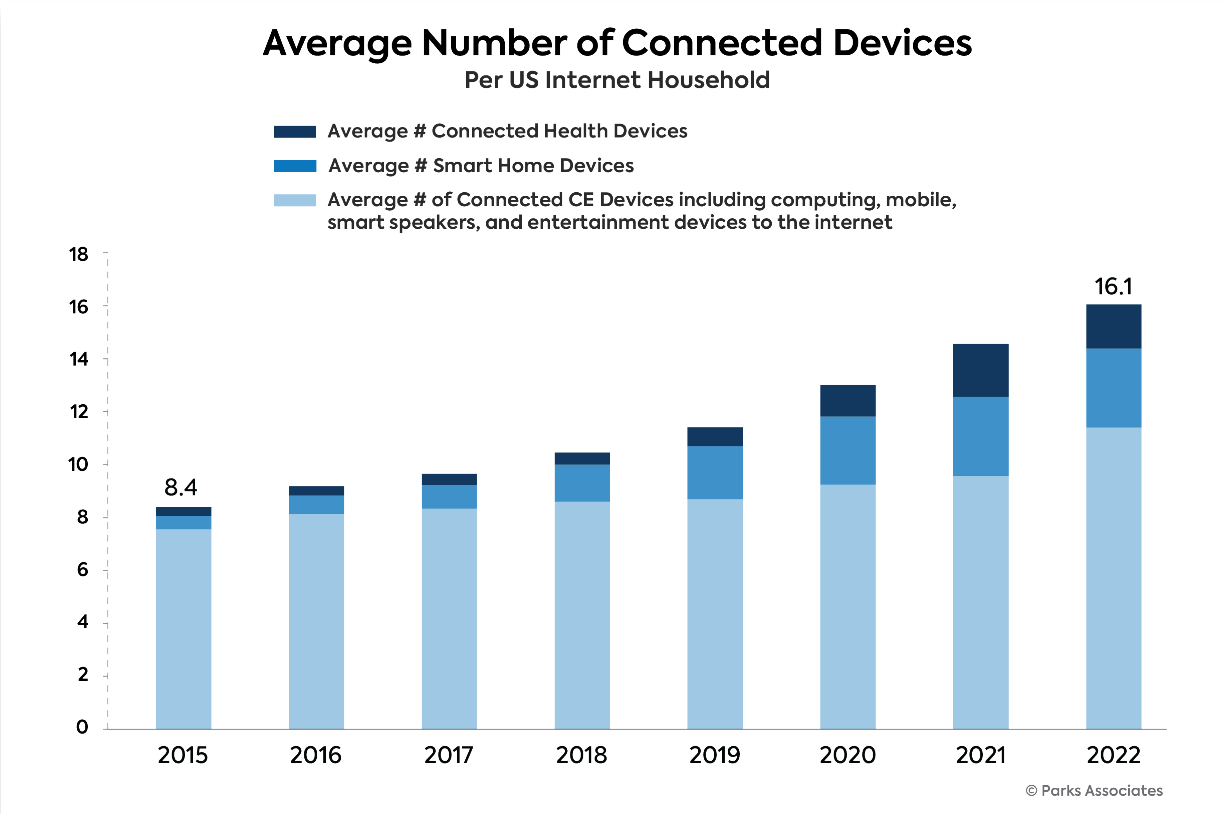
Smart home device owners and those who are most likely to adopt these products report much higher rates of data privacy and security incidents than other consumers. This segment is concerned about hackers and others with bad intentions, but also concerned about technology companies and criminals. Consumer trust is acting as a key differentiator for players in the connected home space, helping them to attract increasingly savvy consumers.

This white paper by Parks Associates highlights the data privacy and security risks posed by the connected home, how consumers perceive these risks, and the role smart home platforms play in mitigating threats. It explores the risks to consumers' identity and data and the opportunity for players in this space – including platforms, internet service providers, home security providers, hardware companies, and home subscription service providers – to help educate and protect their customers against potential harm.

The Connected Home and Data Privacy and Security

Internet-connected products are now commonplace in consumer households. Since 2015, the average number of these products in a home has nearly doubled, rising to over 16 per household in 2022. Some segments of the market, including smart device owners, report owning many more products.

> Smart home households report owning and using an average of 25 internet-connected products in total.



Average Number of Connected Devices

Per US Internet Household

© Parks Associates

Today's consumer reports owning and using a wide mix of product types, including not just traditional computing products with web browsers and apps, but also many varieties of headless IoT devices that interact with the internet in automatic and oftentimes invisible ways (or so it seems to the consumer). These devices typically rely on other devices or systems in the network to receive and process data.

Headless IoT devices are Internet of Things (IoT) products that do not have a user interface or display screen. Unlike more typical devices, such as smartphones or laptops, which have a graphical user interface (GUI) that allows users to interact with them, headless IoT devices are designed to operate autonomously and communicate with other devices or systems in the network.

These products range from browserless consumer electronic devices, such as internet-enabled printers, smart speakers, and robotic vacuum cleaners, to new smart home products, including smart thermostats, video doorbells, and even appliances. Each internet-connected device and accompanying service has its own unique privacy policies, data collection practices, and underlying vulnerabilities.

As the landscape of consumer-connected products grows more complex, the attack surface of the connected household grows, and the likelihood of an adverse event rises. While many consumers are aware that internet-connected products and services have potential risks, they lack a deep understanding of these risks and are unsure of how to mitigate them.

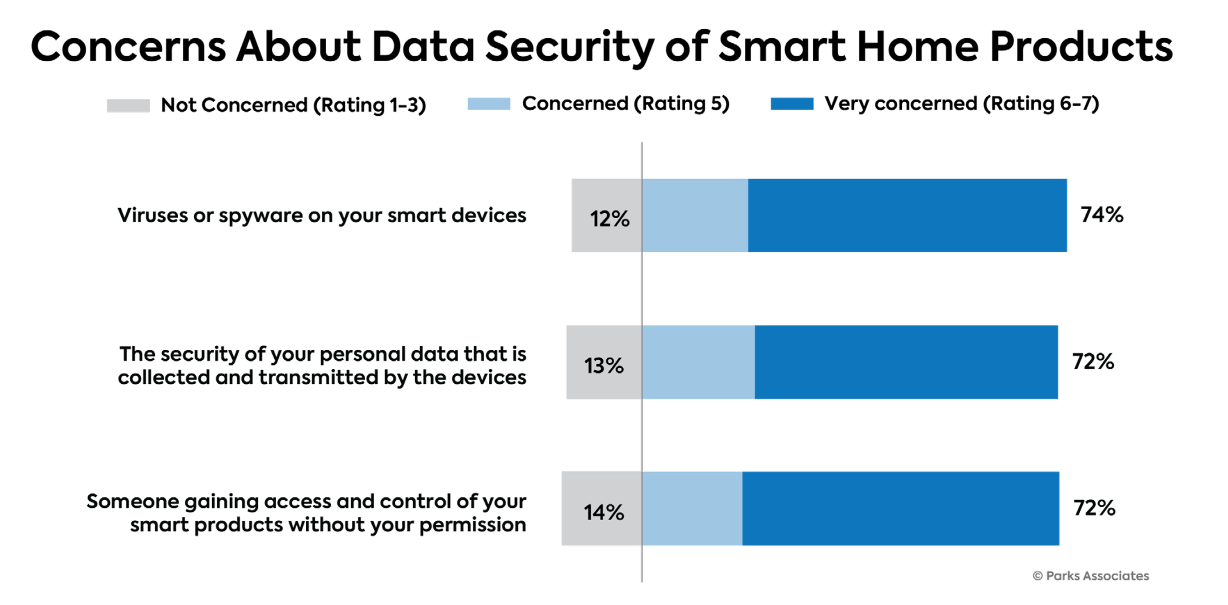
> Some 74% of heads of US internet households report being 'concerned' about the security of their personal data, rating their concern a 5-7 on a 7pt scale. These concerns are largely founded: nearly half of consumers reported experiencing at least one tested privacy or security issue in the past year.

Tested data privacy and security issues:

1. Identity theft
2. Data theft over home networks
3. Data theft over public Wi-Fi
4. Infection by viruses or spyware
5. Private information being made public
6. Companies selling personal data to other companies
7. Companies tracking online activities
8. Hackers gaining access to the respondent's device
9. Unwanted recordings of video or audio data by devices
10. Device theft
11. Loss of a device with personal data.

Consumer Perspectives on Data Privacy and Security

While consumers overall are concerned about the security and privacy of their personal data, smart home product owners in particular report concerns over the data security of their internet-connected products. These worries include viruses or spyware, unauthorized access into products by third parties or even product or platform providers, and the security of the personal data that is collected and transmitted by their devices.



Concerns About Data Security of Smart Home Products

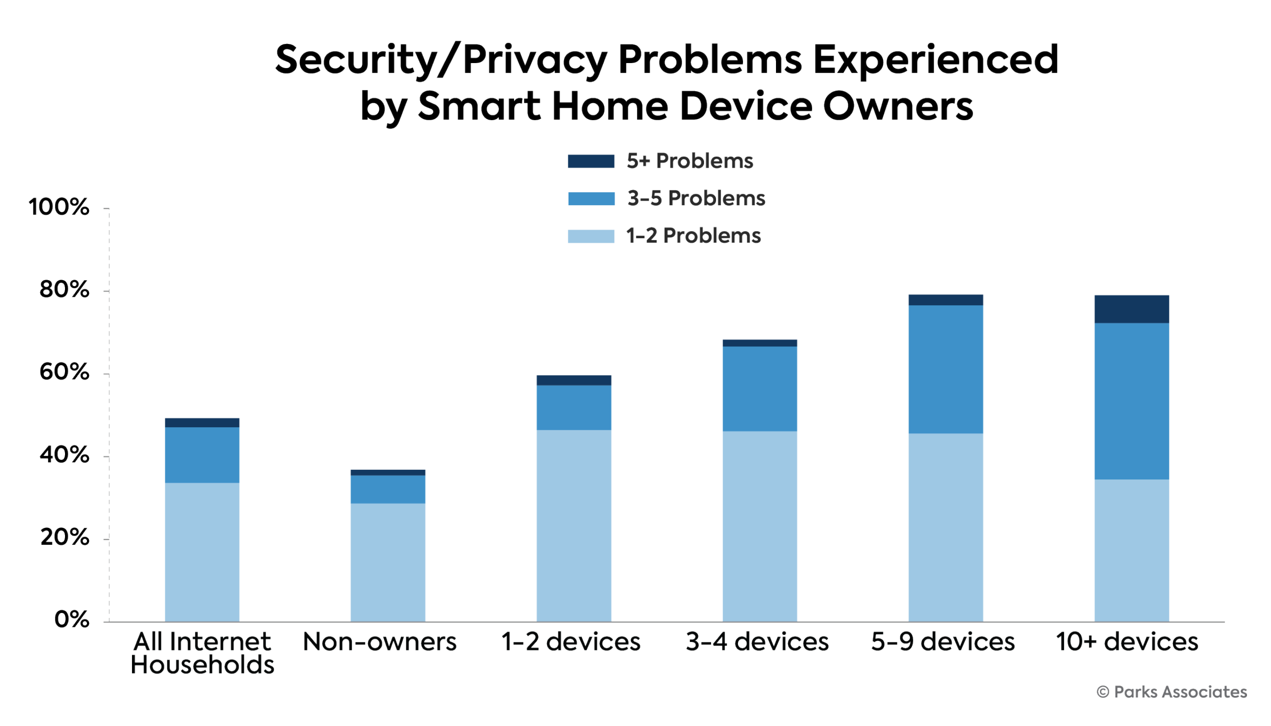
© Parks Associates

Consumer concern over the personal data collected and transmitted by internet-connected products is highly correlated with overall concern about personal data security. Concern is higher among those who own more products, and greater still among savvy adopters who are on the cutting edge of technology. Notably, owners of video security devices report lower levels of concern than owners of other product types; however, they also tend to own fewer devices overall, reflecting that they may be newer to smart home adoption.

Awareness of data and privacy threats and concern over data privacy and security are generally higher among young consumers with strong tech affinities. Consumers who have knowingly experienced data privacy and security problems are more likely to be concerned – and the level of concern is correlated with the number of problems they have experienced. Among smart home households, the number of products owned and used is directly correlated with the number of problems they report.

> Parks Associates research shows 30M households in the US now have at least one video doorbell or networked camera

> Roughly 17% of US internet households own and use networked cameras, making this one of the fastest-growing product categories.



Security/Privacy Problems Experienced by Smart Home Device Owners

© Parks Associates

Privacy and Security Concerns as a Barrier to Smart Device Adoption

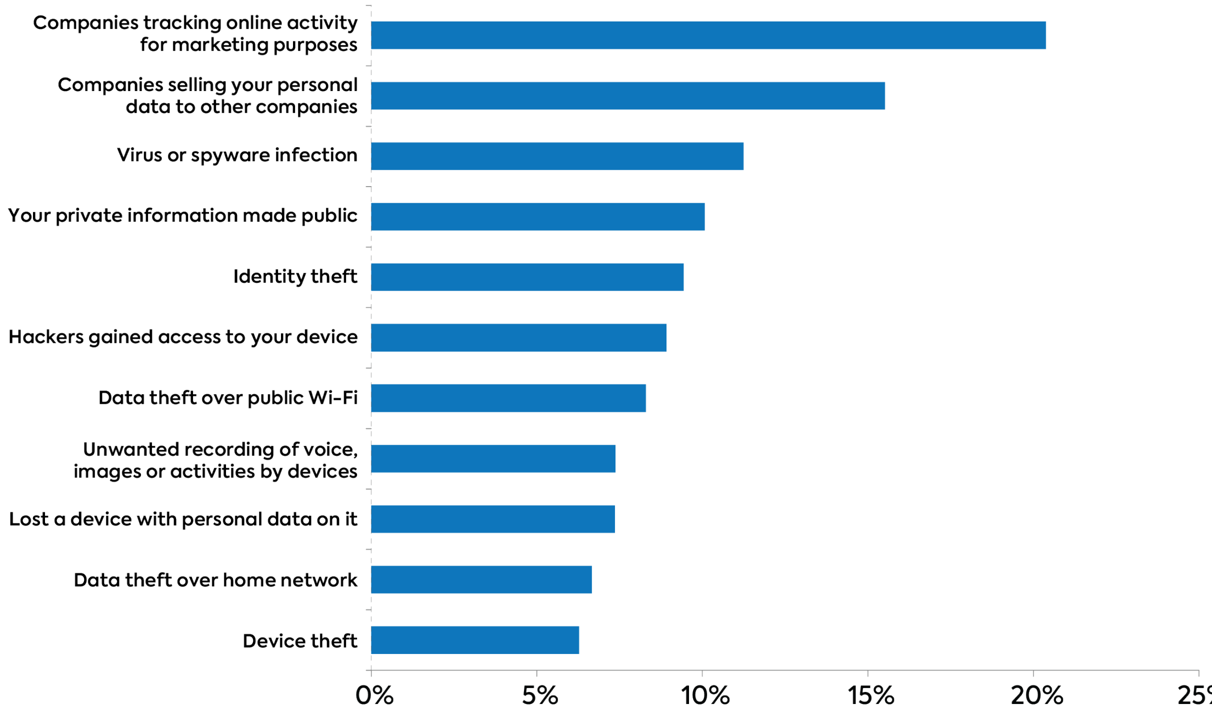
Data privacy and security is one of the top barriers to smart product adoption, coming in third behind cost and lack of perceived value. Nearly one-third of those who don't own or intend to buy smart home products state that the reason is because "I have data privacy and security concerns about having smart devices in my home."

Consumers who have experienced privacy and security problems personally are more likely to report high levels of concern about data privacy and security. Roughly two-thirds of those who have experienced at least one listed problem rated their level of concern "high" (rating 6-7 on a 7pt scale) compared to 44% of those who have not knowingly experienced a problem.

Those who have experienced serious tech-related issues such as data theft, device theft, or virus or spyware infection are particularly likely to report significant concerns compared to those who have not experienced issues.

Notably, those that report experiencing the more common practice of companies selling personal data to other companies have similarly high levels of concern as those that have experienced serious problems. Doubts around whether smart home products or platforms resell their own customers' data for marketing or other purposes harm the perception of these products by consumers.

Security/Privacy-Related Problems Experienced in Past 12 Months



© Parks Associates

Addressing Data Privacy and Security

Addressing the issue of data privacy and security in the connected home offers many benefits to consumers, product makers, and those serving these markets. For consumers, it prevents potential harm and eases concerns, allowing them to adopt valuable technologies more readily without needing to consider trade-offs. For product makers, it reduces potential liability issues and helps to increase customer confidence and product sales.

For those serving these markets, it unlocks new revenue streams and enhances customer satisfaction, while also offering the benefits of greater smart home appeal and uptake. Players in this space have many ways to help improve data privacy and security for end users, beginning with increasing awareness and adoption of existing and widely available tools and methods. Companies offering smart home products and solutions must be prepared to protect their customers.

> 28% of smart home devices are purchased in-store at retail and 46% through online retailers.

Consumers are buying more and more smart products at retail, compared to other channels such as professional installers or service providers; educating the consumer at this point in the purchase journey can help with brand differentiation and trust.

Education and Training

There are several basic steps that consumers may take to protect their own privacy. Product makers and solutions providers benefit from educating consumers on the steps they can take to protect themselves, and from aligning their products and services with these practices.

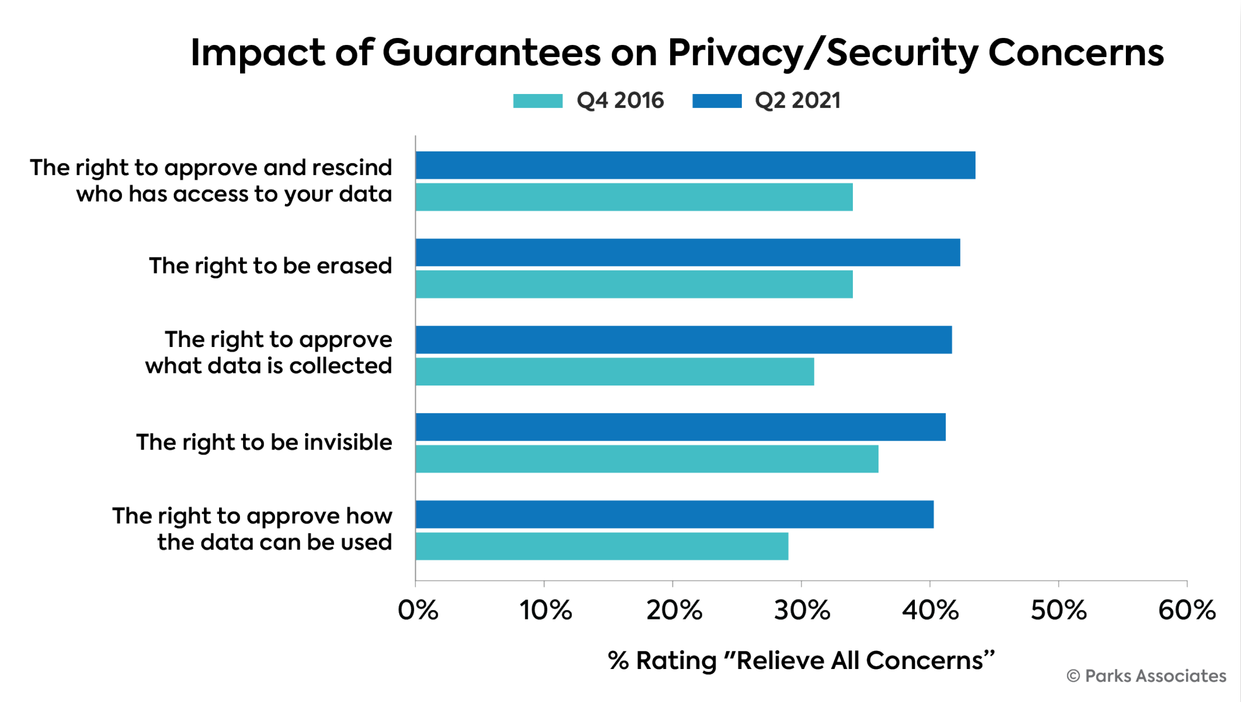
1. Review privacy policies and settings for the devices they plan on purchasing, and only buy devices with robust security/privacy measures.
2. Register with the manufacturer to regularly update software, change the default name and password, and disable remote access.
3. Segregate headless devices onto a separate Wi-Fi network or SSID from computers and cellphones.
4. Enable two-factor authentication and password managers for accounts and credentials when possible.
5. Enroll in identity theft and personal cyber protection to be alerted of suspicious activity and receive resolution services should identity fraud occur.

Smart home product owners are aware of the potential data privacy and security risks that come with owning these products, and they have made the decision that the risk is worth the reward. However, data privacy and security still matter to them, and among product manufacturers and solutions providers, offering these services acts as a differentiator, helping them gain an edge over their competitors. Companies can provide customers with easy-to-use tools to identify risks and protect their identities and their data.

> Product manufacturers and service providers must design their products and platforms with security and privacy in mind.

Consumers who have taken steps to protect themselves are better protected than those who have not. However, consumer action alone is not enough to guarantee data safety and security, given the natural complexities of the connected home's technology landscape.

Parks Associates asked consumers which guarantees from companies would increase their level of confidence or relieve privacy or security concerns about smart products or systems. Nearly 60% of survey respondents rated at least one of the solutions below between 6-7 on a 7-point scale, indicating that a solution tested would relieve all concerns.


Impact of Guarantees on Privacy/Security Concerns

© Parks Associates

The impact of these guarantees to the consumer segments who express the greatest concerns is high – those who are 'highly concerned' about data privacy and security are more than twice as likely to be relieved with a listed guarantee than those who are not concerned.

Technologists, smart home households, professional security monitoring households, and those who have experienced identity theft also express elevated levels of relief when offered a list of rights regarding their data. Making and keeping data privacy and security guarantees help companies expand their appeal among target markets.

One additional factor for companies to consider is that of artificial intelligence: while AI offers additional services and functionalities to end users, consumers are increasingly cautious and pessimistic about its use. This is particularly true for young adults, typically the heaviest users and most rapid adopters of technology. For some specific applications of AI, such as facial recognition, sentiment is more positive than negative; however, approval drops as consumers become more aware of the technology, its uses, and recent developments[1]. At the same time, consumers greatly value the applications that AI enables.

Service Opportunities

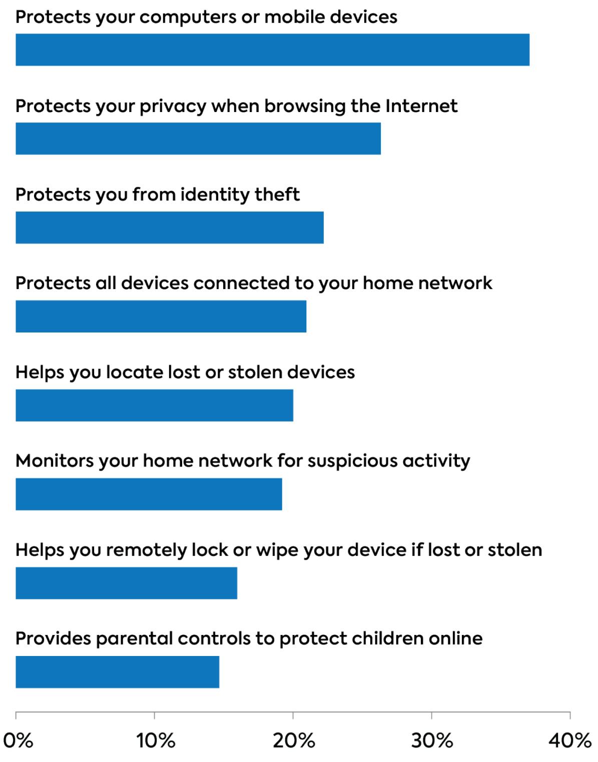
There is a need to educate customers on risks, prevalent scams, and current threats. Many consumers report interest in comprehensive data security services, ranging from traditional antivirus solutions to whole-home protection. Adoption of these services is growing, with new and innovative services increasingly emerging onto the market.

The top services adopted by consumers include traditional antivirus and antimalware applications designed for computers or mobile devices, privacy protection solutions, and identity theft solutions.

One growing area is also that of whole-home cybersecurity, where a solution is embedded in a router or gateway and protects all devices connected to the home network.

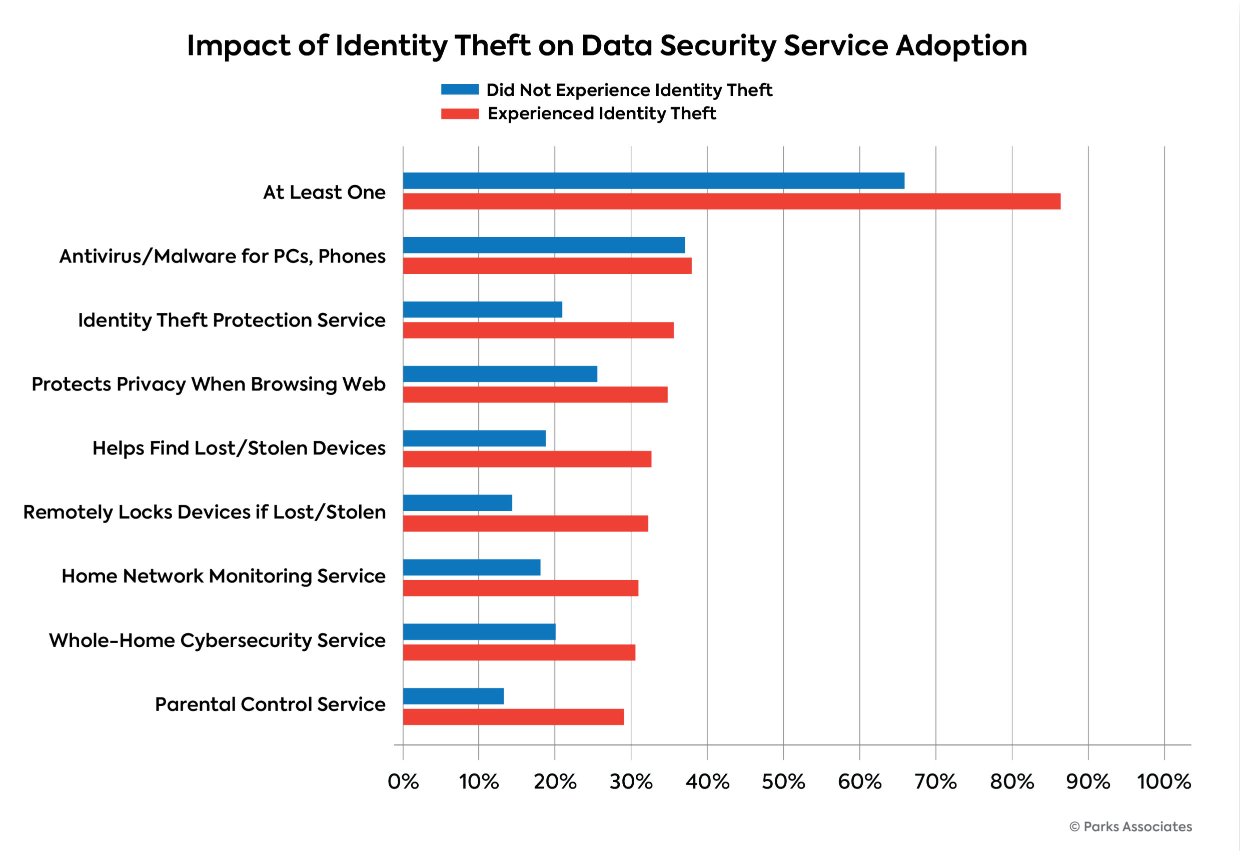
Adoption of data security and privacy solutions is greatest among core smart home customer bases, as well as among those who have experienced issues such as identity theft in the past. This includes not just current smart home device owners, but technologists, high-income households, professional security monitoring subscribers, and others. In particular, those who have experienced identity theft in the past adopt data security solutions at a higher rate than other consumers.

Adoption of Data Security Services



© Parks Associates

[1] Source: Monmouth University: https:/www.monmouth.edu/polling-institute/reports/monmouthpoll_US_021523/



Those who have experienced identity theft have faced direct negative consequences from the loss of their personal data, potentially including financial harm and time spent correcting the issue with credit bureaus, debt collectors, and others.

9% of US internet households report experiencing identity theft in the past 12 months, equating to ~10.5 million households.

The scope of the problem is large, and the risk is rapidly growing. The Identity Theft Resource Center, a non-profit founded to minimize risk and mitigate the impact of identity compromise, reports that in 2022 there were over 1,800 data compromises with an estimated 422M victims[2]. Breaches have occurred in every industry that collects data, including healthcare, education, and government. With breaches so widespread, identity theft may happen to anyone, making identity theft services highly valuable. These services are particularly valuable to those who have been directly impacted by identity theft or are at a high risk of it.

[2] https:/www.idtheftcenter.org/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/

Market Implications

Consumer trust acts as a differentiator for players in the connected home space. In many ways, data privacy and security in a connected home are nebulous, with privacy policies that are either nonexistent or difficult to understand. IoT product makers focused on selling the most feature-complete products for the lowest cost oftentimes sacrifice data privacy and security, creating additional holes and challenges that consumers and service providers must navigate.

Publicized violations of privacy policies and settings undermine consumer confidence in smart home products and services. Companies must be prepared to earn and keep consumer trust, or be prepared to lose prospective customers to rivals. At present, even basic cybersecurity and data privacy measures offer many benefits and improvements for end users. Companies additionally benefit from offering data privacy and security services to their customers, lowering the risk of events, such as data breaches and identity theft, while also raising consumer confidence.

As consumer awareness of smart homes and its risk on data privacy and security grows, so will hesitance to adopt risky products and services. For smart home products and platforms to break through to majority adoption, the issue of data privacy and security in the connected home must be resolved. By educating consumers, implementing security and privacy measures and controls in product and platform design, and delivering new privacy and security solutions, players across this space can help ensure this future.

About Parks Associates

www.parksassociates.com
info@parksassociates.com
972.490.1113

Parks Associates, a woman-founded and certified business, is an internationally recognized market research and consulting company specializing in emerging consumer technology products and services. Founded in 1986, Parks Associates creates research capital for companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, workshops, executive conferences, and annual service subscriptions.

The company's expertise includes new media, digital entertainment and gaming, home networks, internet and television services, digital health, mobile applications and services, consumer apps, advanced advertising, consumer electronics, energy management, and home control systems and security.

About Iris® Powered by Generali

Powered by Generali

IrisIdentityProtection.com
irismarketing@irisidentityprotection.com

At Iris® Powered by Generali, it's not really about us. It's about how identity theft and cybercrime have become a reality for too many. It's about making a person feel whole again, when despite their best efforts, they've still become a victim. It's about understanding that many companies do what we do – just not like we do.

Iris is a B2B2C global identity and cyber protection company owned by the 190-year-old multinational insurance company, Generali, offering always-available identity resolution experts (yes, real people available 24/7/365) and tech-forward solutions that uncomplicate the protection process. We opened our first Washington, DC office in 1983 with a simple mission, bringing customers from distress to relief – anytime, anywhere – and went on to become one of the very first identity theft resolution providers in the U.S. in 2003.

Today, understanding that victimization has no geographical boundaries, we've got a solution no matter what your customers' coordinates are.

About the Author

Kristen Hanich, Director of Research, **Parks Associates**

Kristen Hanich heads Parks Associates' consumer electronics and mobility research, with expertise in other verticals including connected cars, mobile networking, healthcare, wellness, and independent living. She leads a mix of custom and syndicated research projects throughout the year, with a focus on major players and emerging trends. Kristen specializes in bridging the gap between data-driven and narrative approaches to understanding the consumer markets via a mix of qualitative and quantitative research approaches.

Kristen has dual master's degrees in applied anthropology and public health from the Universities of North Texas in Denton and Fort Worth. She earned her BSc in health at the University of Texas at San Antonio and has a graduate certificate in Geographic Information Systems.

ATTRIBUTION

Authored by Kristen Hanich. Published by Parks Associates. Printed in the United States of America.

DISCLAIMER

Parks Associates has made every reasonable effort to ensure that all information in this report is correct. We assume no responsibility for any inadvertent errors.

PARKS ASSOCIATES
International Research Firm

RESEARCH & ANALYSIS

for Emerging Consumer Technologies

With over 35 years of experience, Parks Associates is committed to helping our clients with reliable and insightful consumer and industry research.

- Smart Home Devices and Platforms
- Digital Media and Platforms
- Home Networks
- Digital Health
- Support Services
- Entertainment & Video Services
- Consumer Electronics
- Energy Management
- Home Control Systems
- Home Security

www.parksassociates.com

Provide Protection That Is Smart, Too.

Close to 3 in 4 smart home product owners are concerned that their devices are vulnerable to security breaches.[1]

Your products are changing lives; ensure those changes are for the better with Iris® Powered by Generali. With device protection, data monitoring, 24/7 resolution services, and more, we deliver the full circle of identity & cyber protection. Contact Iris today and get protection for your customers that's built specifically for your products.

Data Collection Point: Smart Lighting
Data Collection Point: Smart HVAC
Data Collection Point: Smart Range Hood
Data Collection Point: Smart Outlet
Data Collection Point: Smart Refridgerator
Data Collection Point: Smart Home Security

Take Smart One Step Further for Your Customers

Your customers are bombarded with alerts and messages all day long – some of which can capture personal data and do serious harm. Offer next-level protection to set your business apart with ScamAssist®: a support service that identifies scams to help keep your customers safe. To learn more, visit **IrisIdentityProtection.com/ScamAssist**.

Iris
Powered by Generali

[1] Parks Associates, Data Privacy and Security in the Connected Home, 2023