ESA®
RESEARCH

THE UNION OF PHYSICAL AND CYBER SECURITY SOLUTIONS FOR CONSUMERS:

Security Solutions Coming Together

SPONSORED BY:

resideo

ESA®
RESEARCH

The Union of Physical and Cyber Security Solutions for Consumers:
Security Solutions Coming Together

This report is a Parks Associates Research Report commissioned by ESA and sponsored by Resideo to deliver the latest facts and trends to help you make informed decisions on capturing new customers through careful business strategy evolutions.

PARKS ASSOCIATES

resideo

THE UNION OF PHYSICAL AND CYBER SECURITY SOLUTIONS FOR CONSUMERS:

Security Solutions Coming Together

The home security industry has picked up millions of new households in 2020 and 2021 as consumers' desire for safety and stability has amplified, in part due to the rise of DIY security solutions, the impact of a pandemic, and economic uncertainty. Currently, 36% of all internet households in the US have a home security system, a 14% increase from the 22% just 5 years ago.

However, the security industry is in the midst of major transformation, driven also by the entrance of tech giants, new partnerships, and the rise of interactive services. Paths into the market are changing and provider share is shifting. Companies that provide DIY installation and self-monitoring saw growth from 2020 to 2021. Also, new entrants into the market that offer services at rock-bottom prices have been eating into the industry leaders' market share. The shifting security market and the recent influx of new players will push companies to offer more to their customers.

Adoption of connected devices continues to grow; now more than 1 in 3 households have a smart home device and consumers are adding these devices to security systems for more interactive services. As familiarity and value grow around specific device categories, there is more and more awareness of potential security and data threats.

Data security and privacy have always been a barrier to adoption for connected devices. Tech giants are responding by implementing features that allow users to control when/if audio and video are stored and advanced encryption for that content. New software solutions are available to manufacturers for inclusion with their products or sold directly to consumers. Certifications from groups like UL and ioXt can help put customers at ease, but still, threats exist. Unprotected connected devices can serve as an entryway to the home network and threaten a consumer's most valuable devices and private data. Parks Associates recent data of 10,000 internet households reveals consumer perceptions around privacy and security:

62% of consumers feel that it is impossible to keep data completely private

Only 37% of consumers trust the companies that have access to their personal data

Only 26% feel that they get value in return for sharing access to their personal data

More Connected Devices Brings More Risk

As new connected devices make consumers' homes smarter and more convenient, the consumer is at increasing risk of possible vulnerabilities in the products. With every passing year, more American broadband households are acquiring smart home devices. Parks Associate's data has found a 28% increase in the rate of smart home device ownership from 2014 to 2021 with 37% percent of American broadband households owning at least one smart home device in 2021. In addition, of the households that own smart home devices, the average number of devices owned has more than doubled in the last five years, from 3.5 devices in 2016 to 8.0 devices per household in 2021.

Every device a consumer uses that is connected to a network stores and/or transmits the user's data, which can be accessed or shared by other connected devices on the network. This connectivity can create new exploits for cybercriminals. With consumers increasing their ownership of connected devices every year, the risk of cyber security vulnerabilities rises, making cyber security services essential for the connected consumer. For example, a recent cyber security vulnerability in one particular brand of smart cameras allowed hackers to bypass the account log-in process and access the user's camera, install their software in the camera, and access footage on cameras that were saved to SD cards. The most unfortunate component of this company's security vulnerabilities was that the company was aware of the security issues for three years before notifying their customers and implementing a patch. The lack of quick action taken by the company could generate regular trust issues among consumers and the manufacturers of their smart home devices.

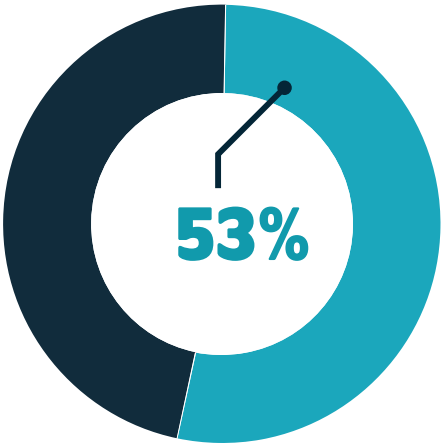
Many smart product manufacturers build in little to no security in their products. According to the cyber security firm Norton, this is due to security not being the manufacturers' primary concern of the product. Cyber security events like what happened to the company mentioned above are not exclusive to them or just smart cameras. For example, white-hat hackers found critical security vulnerabilities in some Android smart TVs, notifying millions of devices were at risk.

According to Norton, some of the most common reasons for smart home devices to be hacked are no system hardening, hardcoded passwords in the devices that are easy to exploit, and no mechanism to update the device's software. These common vulnerabilities in smart home devices have produced a popular mantra among cybersecurity experts "If you connect it, protect it!"

Consumers Have Growing Concerns Over Price and Security

The majority of consumers are no longer just concerned about the physical security of their home, but also the cyber vulnerabilities of their network and smart home devices. Parks Associate's research has found the majority of consumers (72%) are concerned with the security of their smart home products, specifically the security of personal data and someone gaining access and control of their smart home devices.

Home security firms are in a great position to offer cyber security as an add-on service, as the majority of consumers (66%) in 2021 report having an interest in their security provider including a cyber-security add-on service. In addition, earlier data from Parks Associates found that 53% of consumers reported they would prefer the cyber security service be provided by their broadband provider (27%) or home security company (26%).



of consumers reported they would prefer the cyber security service be provided by their

27% **broadband provider**

or

26% **home security company**

Businesses also place a high priority on cyber security. Parks Associates recent study of 1,000 SMBs with under 100 employees found the second most likely product/service among ten options that businesses were likely to spend funds on in the next six months was cyber security services at 37%, just slightly behind Wi-Fi networks (38%).

In contrast, the industry appears to not have caught up with consumers' concerns as only 21% of security companies that offer professional monitoring services are likely to add cyber security services within the next year.

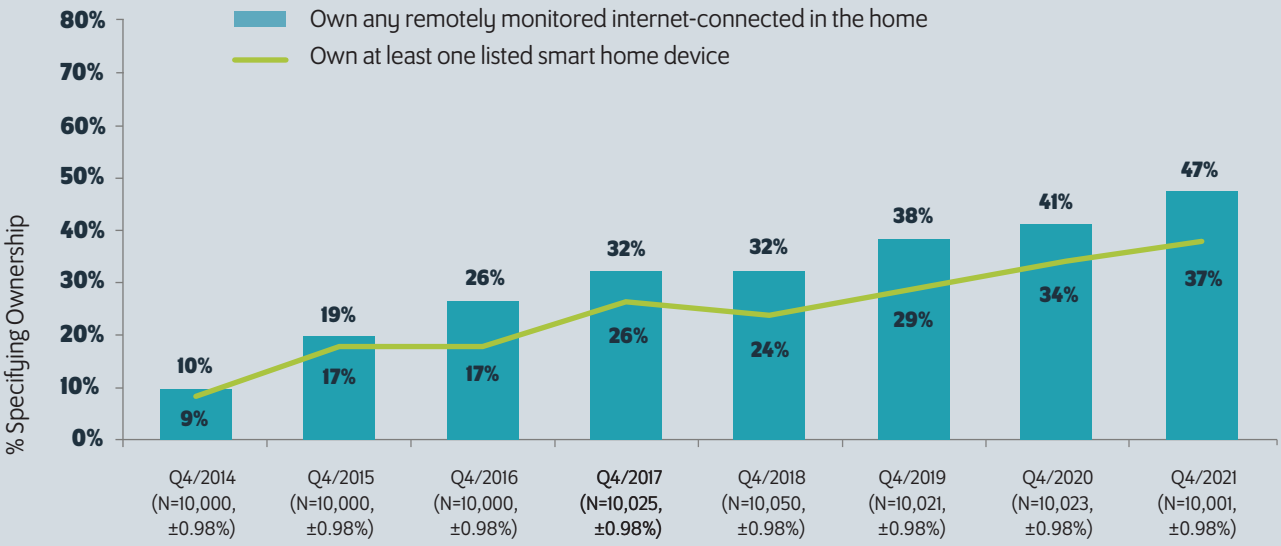
Recommendations and Implications for Security Dealers

Currently, more than 1 in 3 American households have a smart home device. As growth continues, and familiarity and value grow around specific device categories, there will be more consumer awareness of potential security and data threats. Already, nearly half of American broadband households (49%) have experienced at least one data security or privacy problem. There is still minimal regulation applied to smart home devices to ensure their safety, and no standard is used for security in connected devices. Unlike traditional appliances (such as ovens, washers, fridges, etc.) that have to pass strict regulation standards to make sure they are electrically safe and do not consume too much energy, smart home devices do not have such a strenuous regulatory process in place, magnifying fragmentation in the market.

The vast majority of American broadband households are concerned about the security of their smart home devices. Considering that 66% of consumers reported having an interest in their security provider including a cyber-security add-on service, there is a real opportunity for home security retailers to establish a strong presence in the cyber-security space.

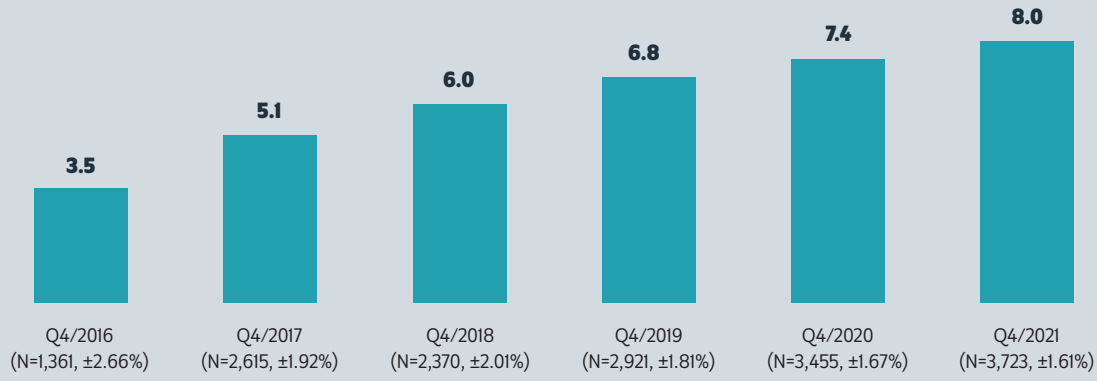
Parks Associates research suggests the opportunity to provide cyber security services for smart home devices is a wide-open market primed to take off based on consumer demand. With many consumers already having familiarity with many home security companies, home security providers have a great opportunity to capitalize and establish a strong presence in the market by offering cyber security services to their current and future customers. Home security providers that innovate and add cyber security services to their current line of products could have a crucial advantage in the unstable shifting home security market and may reap lucrative benefits of establishing dominance in the very immature cyber-security of the IoT market space.

Smart Home Device Ownership



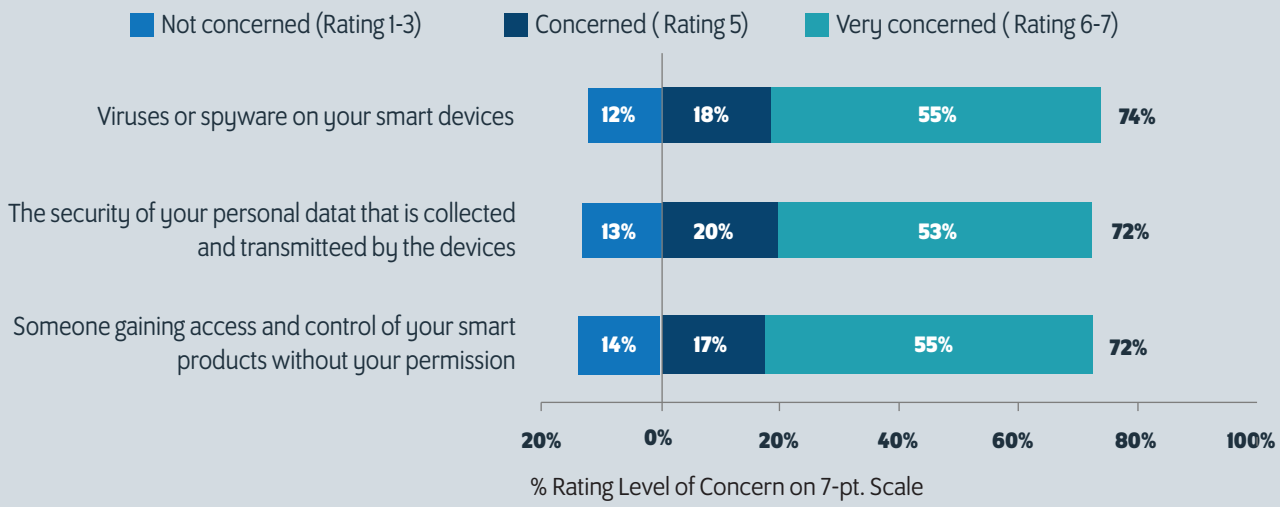
Among All US BB HHs | "Q2600. Can anything in your home... be turned on/off or controlled using a smartphone, tablet, or computer, or ... send you automated alerts by email, text message, or through a smartphone app, or be monitored from outside your home using a smartphone, tablet, or computer?| "ST2601. How many of the following smart home products do you own?"| Source: Multiple Surveys: American Broadband Households and Their Technologies |

Average Smart Home Devices Owned



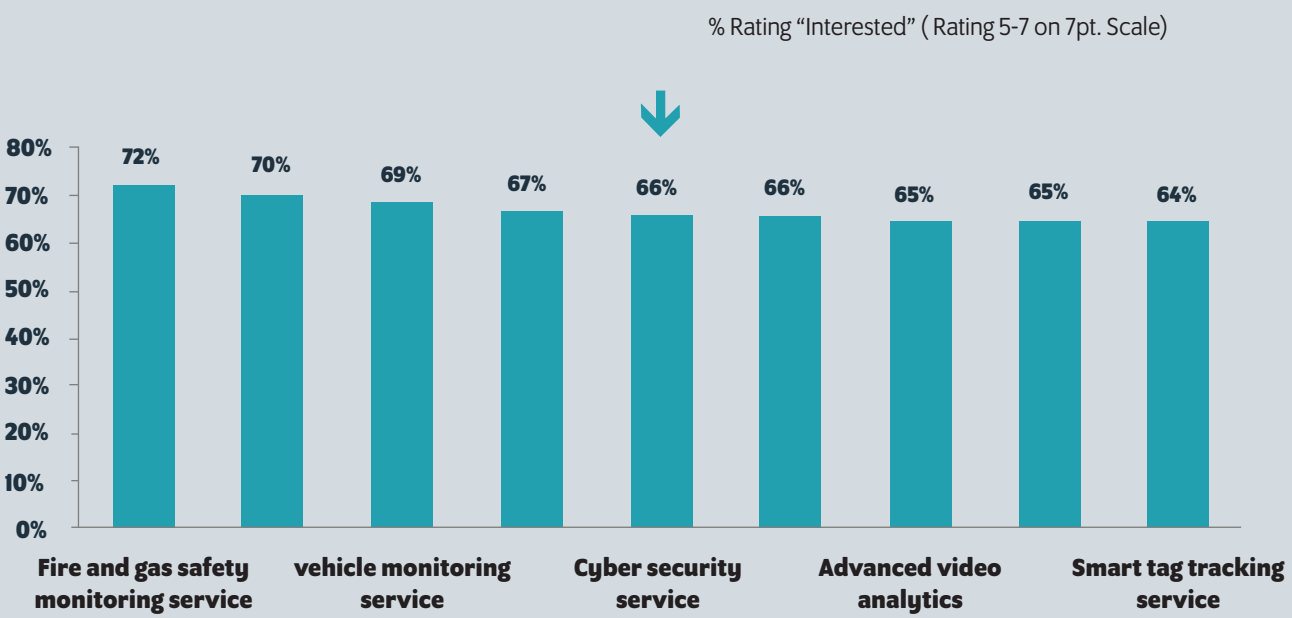
Among US BB HHs That Own At Least One Smart Home Device, Outliers Excluded | "ST2601. Thinking about the devices in your home that can be monitored or controlled using a smartphone, tablet, or computer, how many of the following does your home currently have?"| Source: Multiple Surveys: American Broadband Households and Their Technologies |

Concerns About Data Security of Smart Home Products



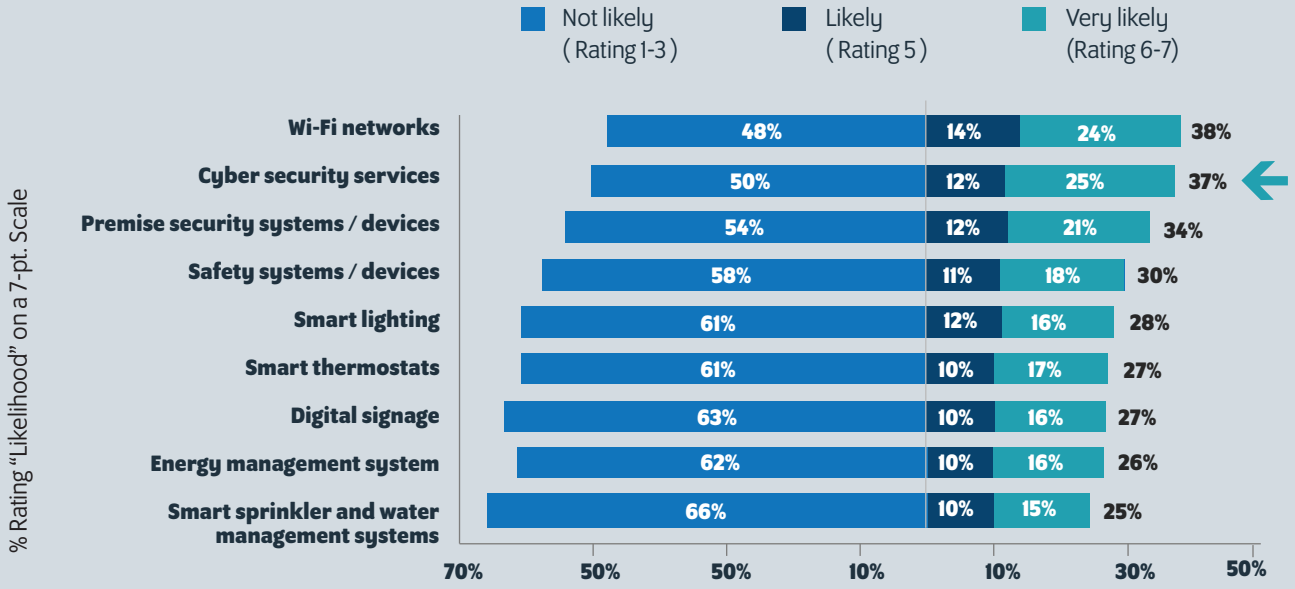
Among Smart Home Device Owners, n=2,209, ±2.09%| "Q7250a. Smart products such as smart thermostats, networked cameras, and smart door locks send data over the internet and allow you to control them using a smartphone app. How concerned are you with the following?" | Source: American Broadband Households and Their Technologies Q2 2021 | © 2021 Parks Associates

Interest in Security System Add-on Service



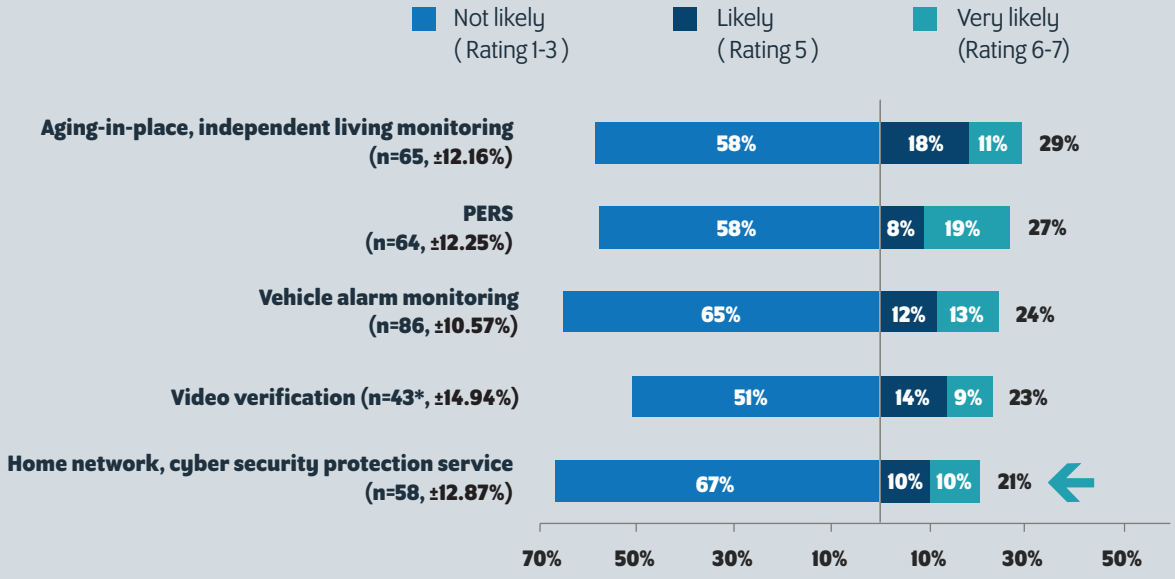
Among Security System Owners, n=1,810, ±2.3% | "S7078.How interested are you adding the following services for your security system?" | Source: American Broadband Households and Their Technologies Q2 2021| © 2021 Parks Associates

Likelihood of Purchasing Smart Devices for Business Locations



Among All Respondents Surveyed, N = 1,002, ±3.10% | "Q4030. Over the next six months, how likely is your business to spend funds on the following?" | Source: New SMB Landscape Q3 2020 | N=1,002, ±3.10% | © 2020 Parks Associates

Likelihood of Offering Add-On Services to Professional Monitoring in the Next 12 Months



% Rating "Likelihood" on a 7-pt. Scale

Note: *Indicate small sample bases, results provide directional information only | Among Security Dealers Not Offering Specified Services |"Q506. What is the likelihood that you will offer the following services in the next 12 months? " | Source: Security Dealer Perspectives: Views from the Front Line| N = 152 Final Completes, ±7.95% | © 2021 Parks Associates