THE CONNECTED HOME'S NEXT WAVE

A new breed of early adopters is driving the growth of functional smart homes, with security and privacy risks in mind

F-Secure.

CONTENTS

EXECUTIVE SUMMARY 3

HOW BILLIONS OF HOMES GOT CONNECTED.................................... 4

THE SMART HOME REVOLUTION IS INCREASINGLY FOCUSED ON FUNCTIONALITY.. 6

WHO'S LOOKING TO MAKE THEIR HOMES SMARTER? 8

A NEW BREED OF FAMILY-DRIVEN EARLY ADOPTERS IS LEADING THE CONNECTED HOME REVOLUTION 9

CONSUMERS MOST INTERESTED IN THE CONNECTED HOME ARE MOST AWARE OF THE RISKS – AND CRAVE PROTECTION 10

CONCLUSION: WILL SMART SPEAKERS BE THE SMART TV OF THIS DECADE?... 14

REFERENCES 15

ABOUT F-SECURE 16

EXECUTIVE SUMMARY

The smart device revolution is increasingly focused on functionality

Our research shows significant growth in smart home devices since 2018. While entertainment-focused devices—such as smart TVs, gaming consoles and streaming devices—drove early connected home adoption, second wave of more functional smart technology—such as voice assistants, home automation and smart security devices—is now being led by a maturing segment of early adopters with families.

An new breed of family-minded early adopters is leading the connected home revolution

Consumers with lots of smart devices and a large digital footprint tend to be early adopters, a maturing group of tech aficionados with families who act as self-appointed tech experts for their friends and family. These early adopters will continue to update their entertainment devices but are also seeking more function from their smart appliance. Their awareness of smart home security and privacy risks also make them most likely consumers to seek connected home security and they're willing to pay more for it.

Customers most interested in the connected home are most aware of the risks—and crave protection for their families

The vast accumulation of data on ever more intimate aspects of consumers lives presents massive security challenges and potential risks that will only grow as criminals seize any opportunity; around the world, consumers with more devices tend to be more aware of the risks associated with their connected home devices and their worries have increased since 2018 as the adoption of more functional connected devices has grown.

HOW BILLIONS OF HOMES GOT CONNECTED

The connected home is the most personal aspect of the explosion of the internet of things (IoT), the driving force behind what some have called "the fourth industrial revolution."[1]

Internet connectivity has quickly become a norm in many popular consumer electronics devices and appliances. It offers unique value for both the consumer and the manufacturer. Consumers appreciate the interactive features and convenience of so-called "smart" devices. Manufacturers benefit from the growing market and new opportunities to capture consumer data.

The shelter-in-place orders that have followed the spread of Covid-19 have reminded people all over the world how crucial a fast, reliable internet connection in the home can be for every member of the family. Online homeschooling and Zoom conference calls became essential to billions of people around the world within a matter of weeks. And protecting everything under the roof that connects to the internet is key to maintaining some semblance of everyday life.

Relentless, massive growth

The growth of the connected home has been relentless over the last decade. It's a trend that's likely to continue for the foreseeable future.

According to the International Data Corporation (IDC) Worldwide Internet of Things Spending Guide consumer-driven smart home spending is the second largest use case in IoT. According to the IDC, IoT spending is expected to reach $742 billion total spending worldwide in 2020.[2]

With this sort of massive adoption, the types of smart home devices that consumers purchase are likely to evolve and become ever-more intwined in consumers' lives.

IoT Asbestos

Many connected home devices are are cheap because cost and function are main drivers of manufacturers, not security.

F-Secure's Mikko Hyppönen—known for his eponymous law that posits, "If it's 'smart,' it's vulnerable"[3]—sees parallels between the connected home revolution and last century's proliferation of asbestos.[4]

"Asbestos was such a great innovation. It looked like a miracle material, originally. Cheap, easy to manufacture, perfect in every way. You can mold it into any shape you want, it's great for insulation. It's great for fireproofing. And it's also lethal."

The rational desire to fireproof as much as possible led to a disaster that society is still cleaning up. And a similar thing looks to be happening with the desire to connect as many things as possible to the internet.

"As connectivity becomes cheaper and cheaper, eventually, it's not going to be just smart things going online, it's going to be stupid things," explains Hyppönen. "And I'm actually much more worried about stupid things online than smart things.

He believes the more connectivity we add to our homes, the more vulnerability we create.[5]

"This is going to be the IT asbestos of the future. This is what our kids will hate us for."

Millions of insecure devices

Millions and millions of insecure devices that are rushed to market every year without proper security considerations, many with default passwords that cannot be changed and unpatched vulnerabilities, are still in use. Most of the attack traffic detected by F-Secure's network of decoy honeypots is generated by Linux-based malware like Mirai, which targets these unpatched IoT gadgets.[6] A January 2018 F-Secure IoT Threat Landscape report found that threats targeting weak/default credentials, unpatched vulnerabilities, or both, made up 87% of observed IoT threats.[7]

That same report quoted F-Secure's Mark Barnes—the man behind the first hack of an Amazon Echo device, turning the voice assistant from the world's largest retailer into "an expensive microphone." Barnes noted that millions of connected devices from lesser-known manufacturers, including webcams and routers, remain vulnerable due to basic security weaknesses in their design.

A swelling privacy and security conundrum

The ever-expanding number of internet-connected devices increases the probability of attackers targeting connected homes. In December of 2019, the FBI offered connected home security advice that included a warning that "Your fridge and your laptop should not be on the same network. Keep your most private, sensitive data on a separate system from your other IoT devices."[8] This followed a 2018 FBI security warning that noted," Each connected device represents an opportunity for hackers to break into a network."[9]

Traditional endpoint security cannot help when it comes to protecting the smart home, as it cannot be installed on smart devices. Meanwhile, smart home devices generate massive amounts of data — including voice and video recordings — that may be stored by consumers, manufacturers of the devices, and makers of applications that run on these devices.[10] This expansion of the surveillance culture of the internet is now invading the most intimate areas of our lives.

The question of how this data will be used raises serious privacy concerns. And where data goes, attackers follow. The prospect of someone stealing this personal data and leaking it holding it for ransom, or using it to blackmail individuals, could lead to serious security problems for smart home users in the future.

Surging beyond the screen

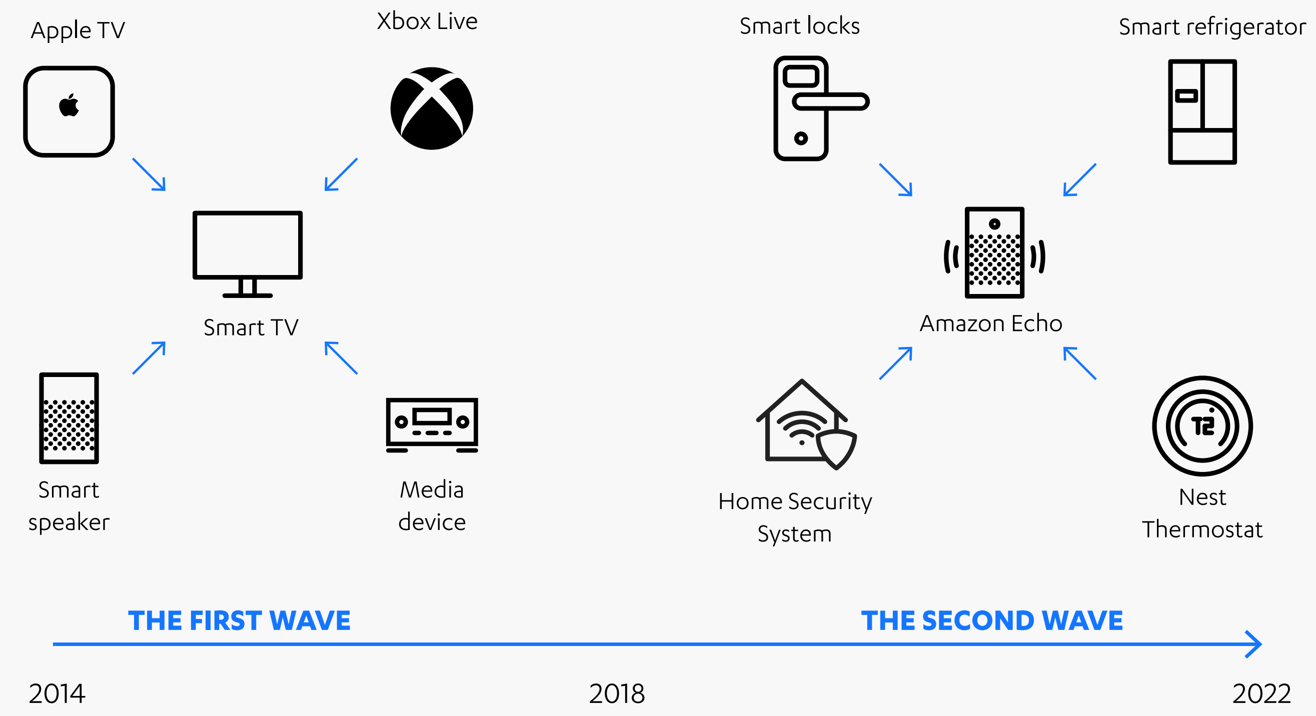
So far entertainment has been the "killer app" that has driven much of the adoption of the connected home.

The rapid adoption of smart TVs and connected devices that work with them will likely continue. F-Secure survey data suggests general consumers tend to follow early adopters, who have now begun purchasing connected devices that facilitate more than entertainment.[11] Thus, the largest relative growth in the market in the next few years is likely to come from more functional devices, including voice assistants, smart security appliances and home automation devices.

These devices invite increasing security and privacy concerns for early adopters. However, early adopters tend to be more worried about the risks to their data, and express a greater willingness to invest in securing their home networks. And these early adopters carry significant influence. Unlike the cliché of past tech addicts, these influencers are young professionals with families and a budget that supports their aggressive adoption of the latest devices and software.

THE SMART HOME REVOLUTION IS INCREASINGLY FOCUSED ON FUNCTIONALITY

THE CONNECTED HOME REVOLUTION



Smart TVs led the first wave

Finding a non-internet connected TV has grown increasingly challenging over the last decade. Soon they may be as hard to find as a rotary phone or a fax machine.

A full two out of three homes now have a so-called smart TV. This places smart TV adoption just behind social media use, which hit 77 % adoption in 2018. For context, that same year, 42 % of US consumers reported having a landline and 28 % said they have an ebook reader.[12]

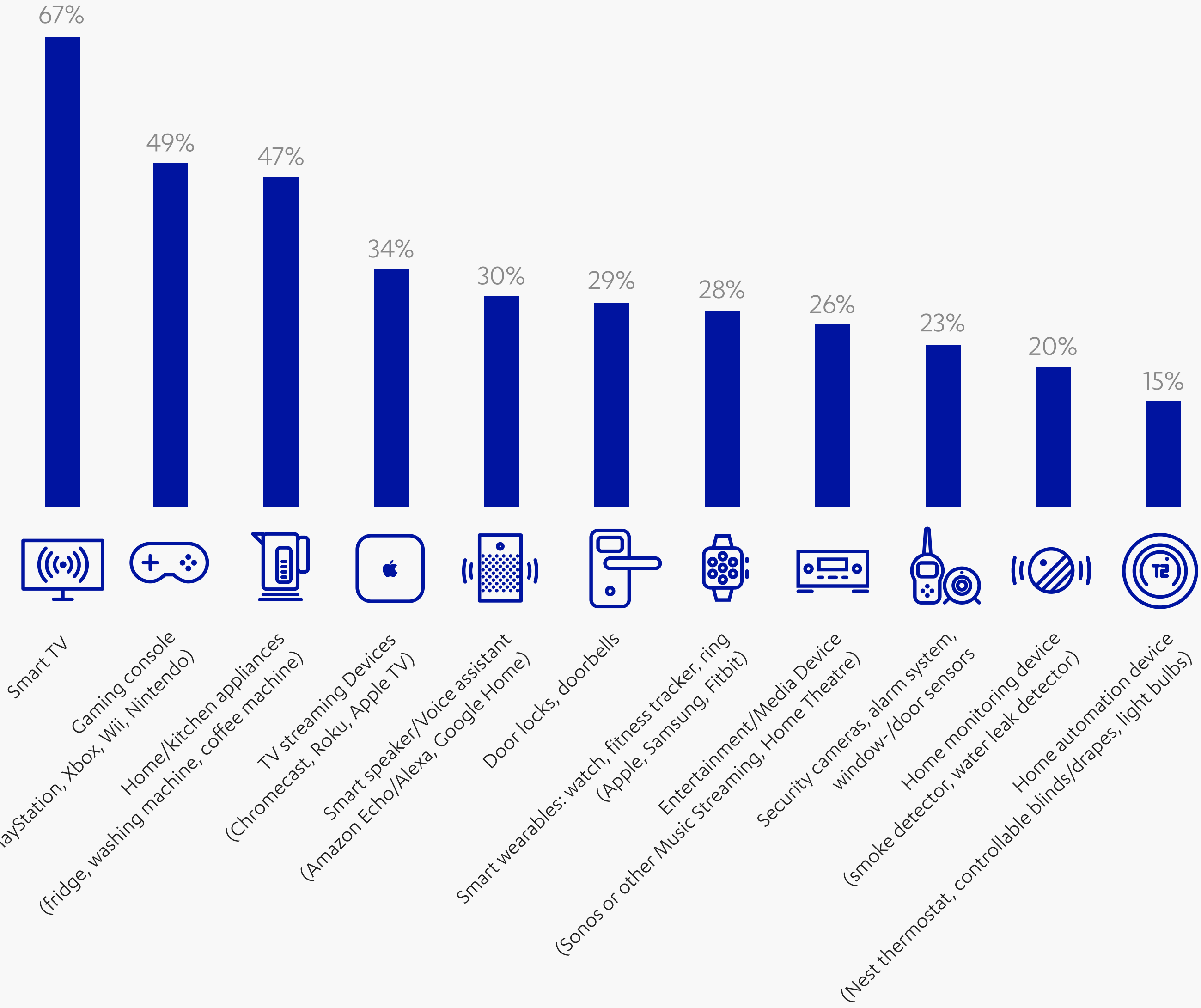
Entertainment, in general, has proven to be the biggest lure to get people to try out new connected devices, with gaming consoles at 49% adoption and TV streaming devices, such as Chromecast and Apple TV, reaching 34% adoption as home music systems like Sonos or home theaters hit 26%.

Too much connectivity to keep track

Survey respondents have an average of 5.3 internet-connected devices in their homes. Brazil, 6.15, and Mexico, 6.03, report having the most connected devices joining the United Kingdom, 5.82, Italy, 5.7, Sweden, 5.66, South Africa, 5.51, and the Netherlands,5.46, as countries where consumers all report having more connected devices than the United States at 5.37.

Cisco recently found that the average American home has 8.4 connected home devices, far more than what respondents reported.[13] Consumers' much-lower estimate of their "smart" devices suggests that "smart" devices are now so common that people may not even recognize all the things in their homes that go online, from the router to the TV to the thermostat to a smart basinet that comforts sleeping babies. In place of a cable-connected television, many homes have an

WHICH OF THESE INTERNET CONNECTED DEVICES DO YOU HAVE AT HOME?

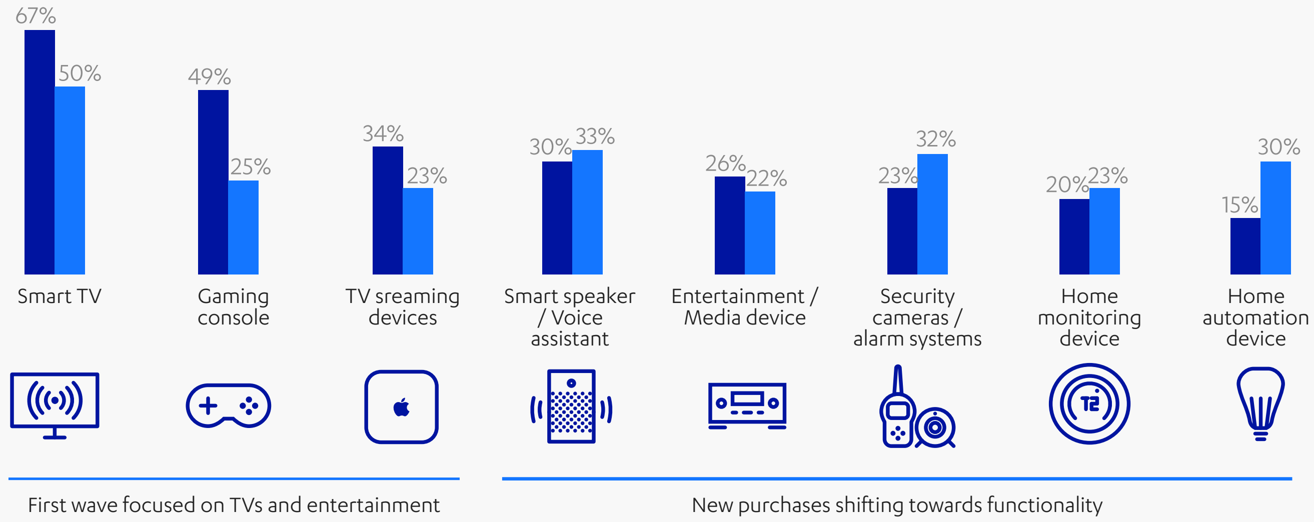


internet-connected entertainment center consisting of a smart TV, TV streaming device, internet-connected gaming console and smart speakers.

A functional smart home wave rising

Kitchen devices are found in 47 % of homes followed by smart speakers, which did not even exist a decade ago, at 30 %. Nearly a third of consumers — 29 % for smart door locks and doorbells and 23 % for security systems — have connected devices that help protect their home. New smart device purchases are generally shifting towards toward functionality — such as smart speakers, security systems and home automation devices.

SMART DEVICE OWNERSHIP vs. PLAN TO BUY IN 12 MONTHS



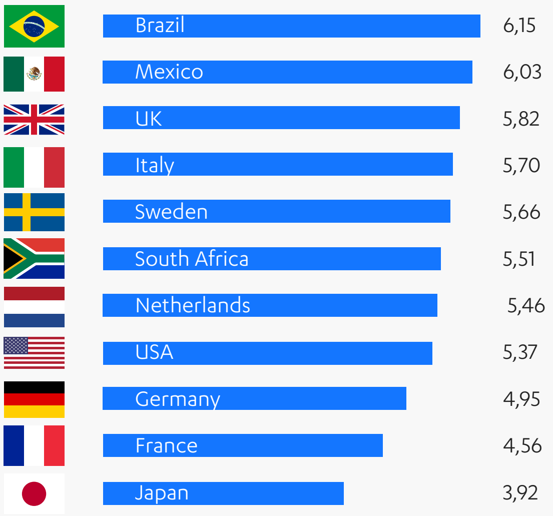
WHO'S LOOKING TO MAKE THEIR HOMES SMARTER?

When asked if they're planning to purchase internet-connected smart home devices in the coming 12 months, 65 % of consumers said they were. And current use of connected home devices looks somewhat correlate with the intent to buy to more

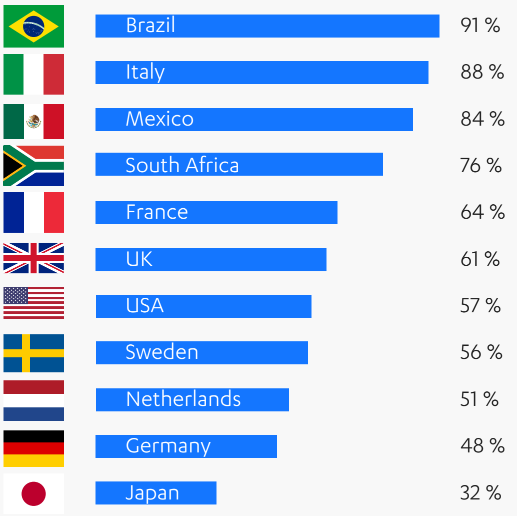
But there's an even better predictor of intent to buy new smart home devices. While an impressive 65% of consumers say they intend to purchase a smart home device, 93 % of early adopters say the same, likely because they have more devices they can update in addition to an inclination to delve into newer devices.

And what's even more interesting is who these early adopters are.

HOW MANY INTERNET CONNECTED DEVICES DO YOU HAVE AT HOME?



INTENT TO PURCHASE DEVICES IN THE NEXT 12 MONTHS



A NEW BREED OF FAMILY-DRIVEN EARLY ADOPTERS IS LEADING THE CONNECTED HOME REVOLUTION

BASIC INFORMATION

AGE	35
OCCUPATION	Senior Product Manager
INCOME	$85,000
EDUCATION	BA, Psychology
STATUS	Married for 8 years

17 connected home devices, including 3 Roombas

Configures his own router

Loves Apple for himself and his kids but uses Windows at work and Android to keep up with the tech

Security solutions and parental controls activated on all devices

Eager to share experiences with friends and family and likely to post reviews

FOR EARLY ADOPTERS, SMART MEANS "AUTOMATION" – AND VULNERABLE

In 1962, Everett M. Rogers coined the term "early adopter" in his book Diffusion of Innovations. "The early adopter is respected by his or her peers, and is the embodiment of successful, discrete use of new ideas," Rogers wrote. In 2010, The New York Times, described this market segment as "ardent consumers [who] will stand in long lines, if that's what it takes, to get an overpriced gadget ahead of everyone else they know."[15]

Not your father's early adopters

With their willingness to embrace new technologies, early adopters invest their time and money to act as authorities on technology for friends and family, helping the early majority in crossing the technological gap by sharing tips and tricks and even aiding in device setup.

But the stereotype of an early adopter as a single male with thick glasses and spare time to fill with silicon toys is outdated.

Extensive F-Secure surveys conducted over several years finds that today's early adopters tend to be married millennials in their 30s with college degrees, young children, and a passion for filling their new homes with internet-connected devices of all sorts.

These consumers tend to be better informed than their peers, explorative, and in search of new technology offerings to try. They are willing to invest and try new products and serve their friends and family by weeding out technology they find lacking, providing feedback to vendors, and sharing what they learn.

More from their smart home, now

While all consumers have increased their purchases of smart home devices, early adopters bought more. And what they bought is increasingly focused on devices that have some functional use for the home.

General consumers are following early adopters into more functional devices, though smart TVs continue to be the top item they and early adopters are looking to purchase. However, early adopters may be purchasing their second, fourth or sixth smart TV in an effort to stay ahead of the curve.

CONSUMERS MOST INTERESTED IN THE CONNECTED HOME ARE MOST AWARE OF THE RISKS – AND CRAVE PROTECTION

In 2018, F-Secure noted there was an "early adopter paradox" that saw the consumers who are most excited about the connected home were also more concerned about the potential risks. This continues to be true in 2020, but the prediction that these concerns might hinder that adoption of smart home appliances has not been realized. Early adopters have embraced connected home devices fully and rely on it more and more for functional use. But that doesn't mean they've overcome their concerns. Instead, they're the consumers most likely to invest more in protection.

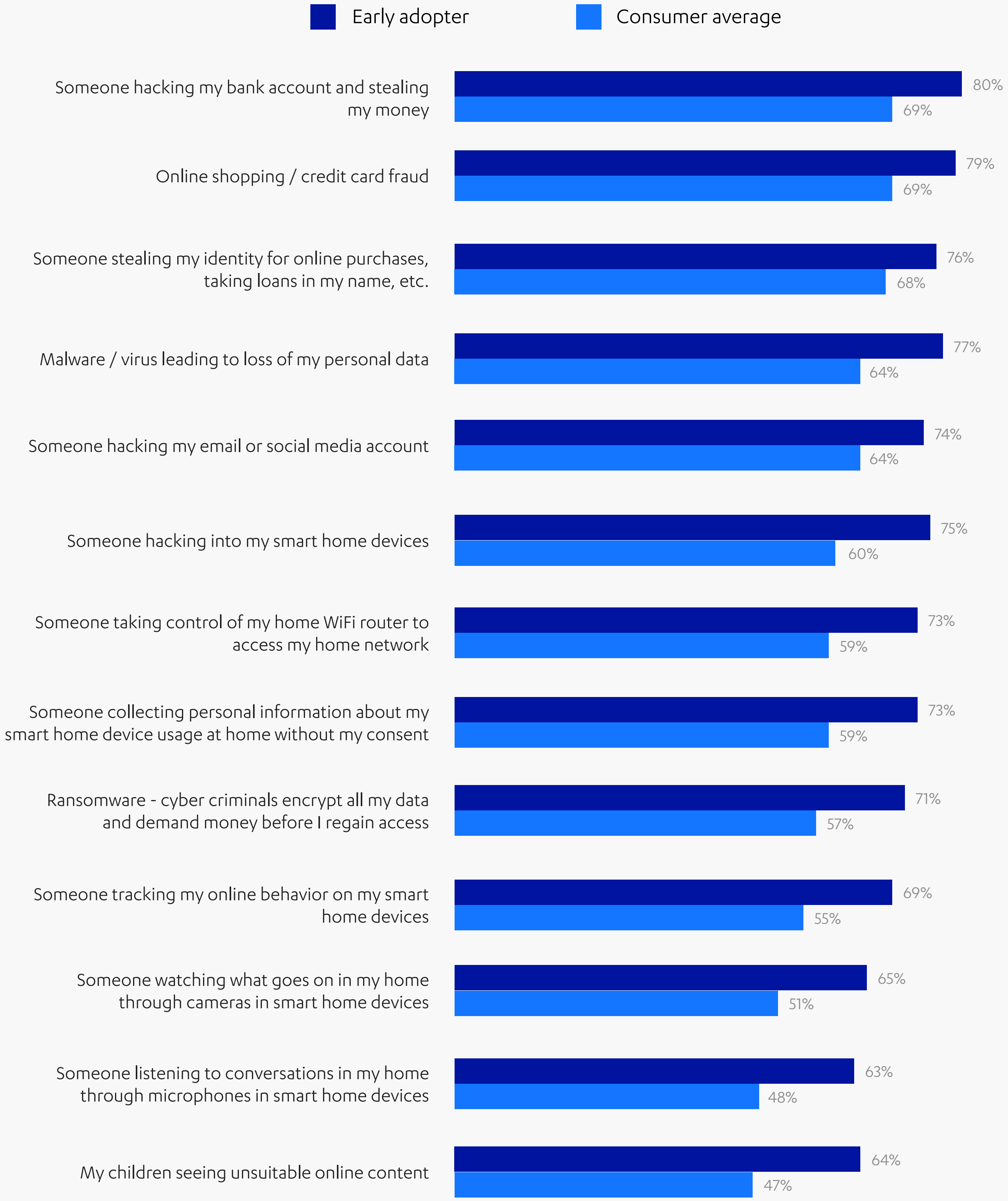
Consumers get the risks

Decades of dealing with online security concerns seem to have informed consumers views of the risks that come from connecting numerous home appliances and devices to the internet. Well over half, 60% of consumers worry about an attacker hacking into their smart home devices. That percentage reaches 75% for early adopters.

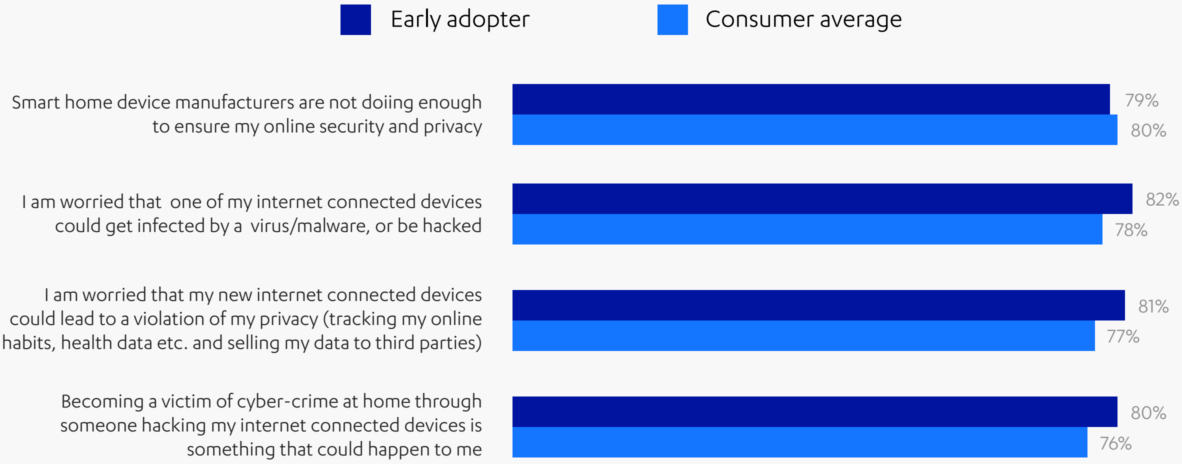
Privacy concerns also haunt smart home owners: 59 % fear someone collecting their personal information, 55% worry about someone tracking my online behavior, 51 % expressed concern about someone watching what goes on in my home, and 48% have anxiety about someone listening to them through their smart home devices.

Consumers with kids aged 0-15 reported significant worry about these threats, with 73% overall expressing fear about their children seeing unsuitable online content. That percentage rises to 79% of early adopters with kids in that more impressionable range.

CONSUMERS WORRY ABOUT ONLINE THREATS



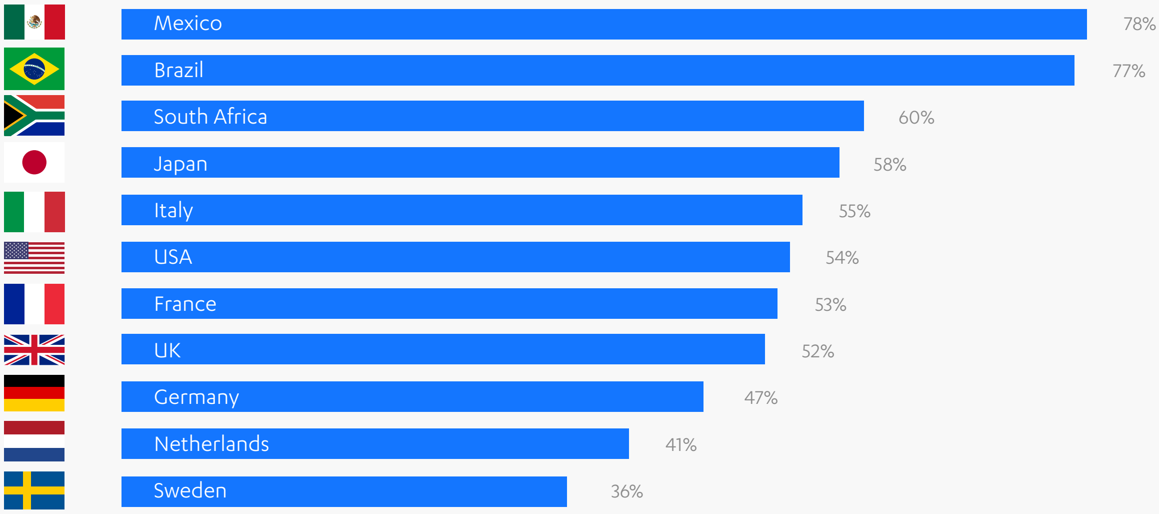
SECURITY AND PRIVACY WORRIES



One thing general consumers, 80%, and early adopters, 79%, agree on is the sense that smart home device manufacturers are not doing enough to ensure their online security and privacy. And the feeling seems closely correlated to the 76% of consumers feel they could easily become a victim of smart home cyber crime

Worries that internet-connected smart home devices could get infected by a virus/malware, or be hacked, vary widely by country, with just over three out of four respondents reporting that they are worried or very worried in Mexico and Brazil, while just one out of three expressed similar concerns in Sweden.

WORRY ABOUT INTERNET-CONNECTED DEVICES COULD GET INFECTED BY MALWARE/VIRUS OR BE HACKED

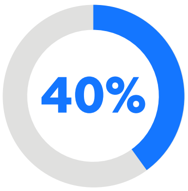


Protecting their kids and their smart homes

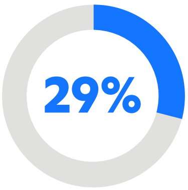
Consumers appear ready to secure all the devices in their homes. It's another area where early adopters are leading the way.

Connected home security is the number one benefit respondents said they are willing to pay for. And early adopters expressed a higher willingness to pay for almost all security benefits compared to general consumers, including parental controls, the ability to manage security and privacy by themselves through one app, and the ability to see smart home threats and scan for vulnerabilities.

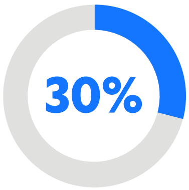
Early adopters' security and privacy concerns for their families are shown in their willingness to pay for parental controls to prevent their children from accessing unsuitable online content, 40 %, versus all families with children, 33 %. They're also more interested in monitoring their child's activity online, 29 % compared to 25 %, and limiting their internet activity, 30 % versus 24 %.



Parental controls for unsuitable content



Monitoring online activity



Limiting online time

CONCLUSION: WILL SMART SPEAKERS BE THE SMART TV OF THIS DECADE?

Smart home devices have been around in some commercial form since the turn of the millennium. But the invention of the smart TV in 2008 led to a decade when billions of homes got their first internet connected device without a keyboard.

Early adopters, with growing families, have helped make the widespread adoption of smart entertainment devices mainstream. And now they're leading the way in the functional connected home wave that kicked off with the launch of voice activated smart speakers, which went from almost zero adoption in the middle of the last decade to now being in almost one in four homes. Like the smart TV, smart speakers are gateway devices that play well with other smart appliances, including thermostats, security cameras and home entertainment systems.

As the data collected from these devices grows and vulnerabilities provide criminals new opportunities, the worries early adopters and most consumers express about smart home security and privacy may be substantiated. Having lived through the revolution that saw every computer get connected to the internet, early adopters recognized that smart means vulnerable. And they're ready to act now to make their homes more functional, while protecting their families.

REFERENCES

[1] How IoT will drive the fourth industrial revolution https://www.zdnet.com/article/how-iot-will-drive-the-fourth-industrial-revolution/

[2] Worldwide Spending on the Internet of Things Will Slow in 2020 Then Return to Double-Digit Growth, According to a New IDC Spending Guide https://www.telecomtv.com/content/iot/worldwide-spending-on-the-internet-of-things-will-slow-in-2020-then-return-to-double-digit-growth-according-to-a-new-idc-spending-guide-38983/

[3] Hypponen's Law: If it's smart, it's vulnerable https://blog.f-secure.com/hypponens-law-smart-vulnerable/

[4] Mikko Hypponen: Smart devices are "IT asbestos" https://www.verdict.co.uk/mikko-hypponen-smart-devices-it-asbestos/

[5] The Internet of Things: how safe are your smart devices? https://life.spectator.co.uk/articles/the-internet-of-things-how-safe-are-your-smart-devices/

[6] F-Secure Attack Landscape H2 2019 https://blog.f-secure.com/attack-landscape-h2-2019-an-unprecedented-year-cyber-attacks/

[7] IoT Threat Landscape: Old hacks, new devices https://blog-assets.f-secure.com/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf

[8] Tech Tuesday: Internet of Things (IoT) https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot

[9] FBI: IoT security warning https://cybersecurity.wa.gov/news/fbi-iot-security-warning

[10] When smart devices watch you, what do they do with the data? https://www.usatoday.com/story/tech/columnist/2019/06/20/what-do-smart-devices-do-data-they-collect-you/1483051001/

[11] F-Secure Survey, May 2020, 11 countries (Brazil, France, Germany, Italy, Japan, Mexico, the Netherlands, Sweden, South Africa, UK, USA), 400 respondents per country = 4400 respondents (+25years)

[12] Technology adoption in US households, 1860 to 2019 https://ourworldindata.org/grapher/technology-adoption-by-households-in-the-united-states

[13] Cisco Annual Internet Report https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/air-highlights.html#

[14] Rogers, Everett M.. Diffusion of Innovations, 5th Edition. United Kingdom, Free Press, 2003. https://www.google.com/books/edition/Diffusion_of_Innovations_5th_Edition/9U1K5LjUOwEC?hl=en&gbpv=1&dq=early+adopter+respected+by+his&pg=PA283&printsec=frontcover

[15] Applause, Please, for Early Adopters https://www.nytimes.com/2010/05/09/business/09every.html

[16] Early adopter paradox: Consumers most excited about IoT are also most aware of privacy risks https://www.helpnetsecurity.com/2018/10/25/early-adopter-paradox/

ABOUT F-SECURE

Nobody knows cyber security like F-Secure. For three decades, F-Secure has driven innovations in cyber security, defending tens of thousands of office, homes, and millions of people. F-Secure shields enterprises and consumers against everything from advanced cyber attacks and data breaches to widespread ransomware infections. F-Secure's AI-driven solutions also help to protect the connected devices and homes of your customers The unique combination of technology and world-class Business Services supporting the entire customer lifecycle is what makes F-Secure an excellent fit for the service provider channel. F-Secure's products are sold globally by more than 200 service providers and thousands of resellers.

f-secure.com/connected-home-security

F-Secure.