Avast Smart Home
Security Report 2019

Key facts

» Two out of five (40.3%) digital households worldwide have five or more devices connected to the internet

» Out of all smart homes worldwide, 40.8% have at least one vulnerable connected device which puts the entire smart home at risk

» 31.8% of these vulnerable devices are at risk due to unpatched software vulnerabilities; 69.2% are vulnerable due to weak security credentials

Executive summary

Smart devices, like security cameras, baby monitors, TV media boxes, smart TVs, printers, and gaming consoles, are entering homes at a rapid pace and with them, vulnerabilities. Avast scanned more than 16 million smart home networks worldwide using Avast Wi-Fi Inspector, and found that two out of five (40.8%) digital homes worldwide contain at least one device that is vulnerable to cyber attacks, which therefore puts the entire home at risk. Despite widespread warnings to consumers to change passwords and pick strong and unique ones for all devices, over 69% of vulnerable devices are still at risk due to default or weak access credentials, which offers hackers easy access and the opportunity to seize control of these devices.

The anonymized, statistical data in this document has been obtained with user consent from scans run by Avast users from their computers using the Avast Wi-Fi Inspector feature during September 2018. All non-home networks have been excluded from this study.

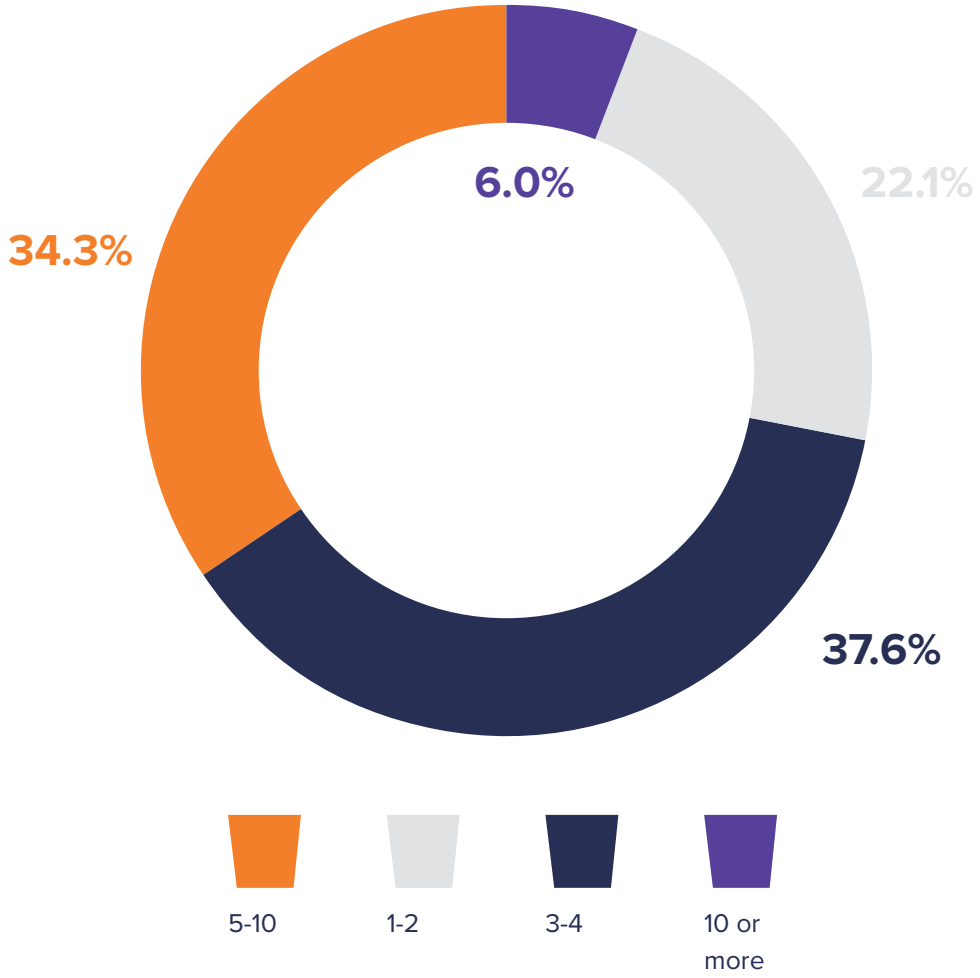
In total, 16 million different home networks worldwide are included in this study from countries all around the world, and in this report we're focusing on 21 countries in North and South America, Europe, and the Asia Pacific region. 56 million devices were scanned.

Connected homes in 2019

Worldwide standard: at least five devices are connected to the internet in the average household

Today, two out of five (40.3%) digital households worldwide have five or more devices connected to the internet, and 6% have more than ten devices connected to the internet. Households in Indonesia have the most devices connected, with 18.2% having ten or more, followed by the United States, where 15.5% have ten or more devices. France registered the least number of smart homes with only 2.1% of households falling into the 10+ devices category.

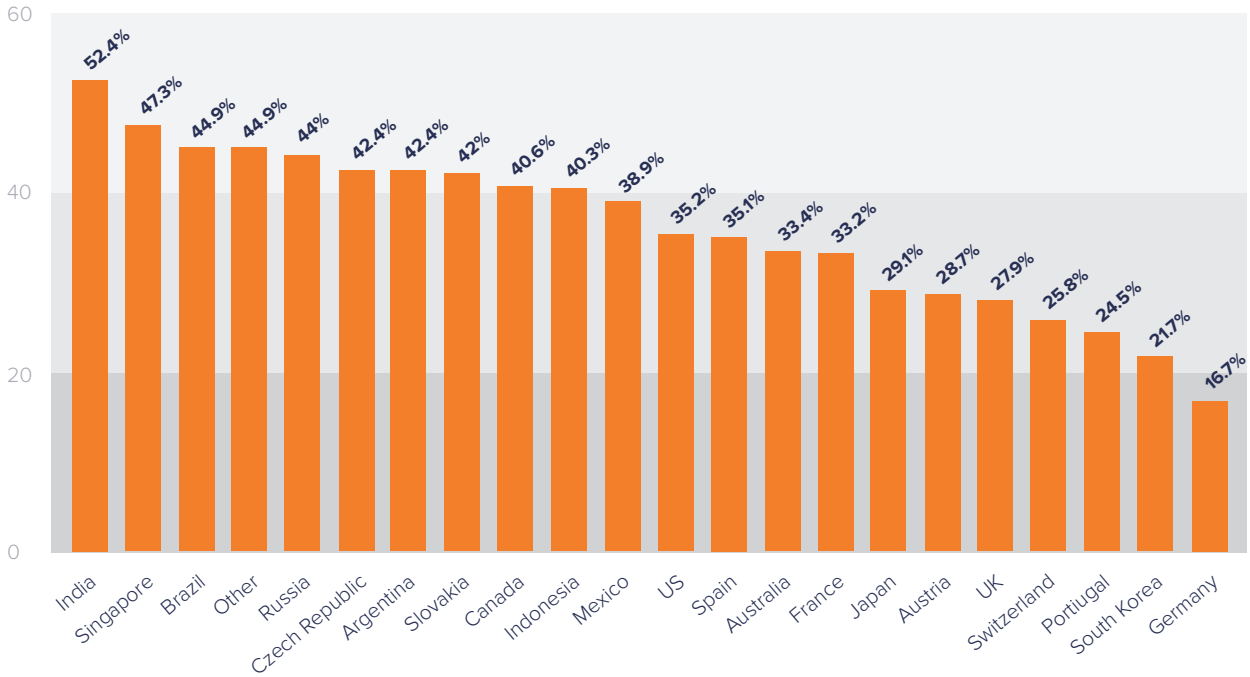
Number of devices per home network worldwide



Over one-third of smart homes worldwide have one or more devices that could be attacked

As users add more devices to their homes, they become more vulnerable. Any device connected to the router can be an entry point for attackers to access other devices on the same network. For example, if a family's baby monitor is accessible using the device's default login credentials, username and password, a cybercriminal can use the baby monitor to gain control of further devices connected to the same network, like the home's smart speakers or smart TV, locking them and demanding a ransom.

Share of connected homes with one or more vulnerable devices per country



Most used smart home devices worldwide

The majority of connected devices users have at home are still computers and smartphones which connect via Wi-Fi through the home router. Excluding these three types of devices, the research shows that, globally, TVs are the next most prevalent IoT device in digital homes worldwide, closely followed by printers, media boxes (e.g. set-top boxes, Chromecasts, TiVos) and security cameras.

Top ten smart home devices per country (excluding PCs, smartphones, and routers)

NORTH AMERICA & AUSTRALIA

No.	U.S.	%	Canada	%	Australia	%
1	Media boxes[1]	31.1%	Printers	26.8%	Media boxes	25.3%
2	Printers	23.7%	Media boxes	20.2%	Printers	23.8%
3	Tablets	10.3%	TVs	11.5	Tablets	14.9%
4	TVs	10.2%	Game consoles	11.3%	TVs	13%
5	Game consoles	8.9%	Tablets	10%	Game consoles	9.8%
6	Voice assistants	5.3%	Network nodes	9.4%	Audio equipment	4.1%
7	Audio equipment[2]	3.1%	Audio equipment	3.7%	Security cameras	3%
8	Security cameras	2.6%	Security cameras	2.7%	Network nodes	2.1%
9	Network nodes	0.7%	Voice assistants	1.3%	NAS	1.7%
10	Lighting	0.8%	NAS[3]	1%	Voice assistants	0.7%

[1] Media boxes refers to set-top boxes, Chromecasts, TiVos

[2] Audio equipment refers to speakers, headphones and amplifiers

[3] NAS refers to Network Attached Storages

It's unsurprising to see the growing popularity of media boxes feature so highly on the list given the growing prevalence of online streaming services and devices such as Google Chromecast and Roku. These devices are great for entertainment purposes, but given they connect to other devices in the home such as speakers, mobile, and TV, they are another gateway into the network — making them a prime target for hackers.

GERMAN SPEAKING COUNTRIES

No.	Germany	%	Austria	%	Switzerland	%
1	Printers	21.4%	Printers	30%	Printers	33.4%
2	Media boxes	18.6%	TVs	19.3%	TVs	16.2%
3	TVs	18.4%	Media boxes	14.8%	Media boxes	11.5%
4	Tablets	11.8%	Network nodes	8.8%	Audio equipment	9.2%
5	Network nodes	11.4%	Tablets	7.9%	Tablets	6.7%
6	Audio equipment	5.2%	Gaming consoles	4.9%	Network nodes	6.0%
7	Game consoles	5%	Audio equipment	4.8%	Gaming consoles	5%
8	Security cameras	2.2%	Security cameras	3.2%	Security cameras	4.4%
9	NAS	2%	NAS	2.5%	Lighting	1.1%
10	Voice assistants	1.8%	Voice assistants	1.5%	IP Phones	0.2%

Printers, smart TVs and media boxes top the list of devices used in German, Austrian and Swiss households. Tablets are also growing in popularity in these countries, featuring in the top five devices.

WESTERN EUROPEAN COUNTRIES

No.	UK	%	France	%	Spain	%
1	Media boxes	21.8%	Media boxes	54.9%	TVs	33.6%
2	TVs	18.29%	Printers	15.2%	Printers	19%
3	Printers	17.45%	TVs	10%	Media boxes	16.4%
4	Tablets	15.2%	Gaming consoles	5.4%	Network nodes	8.7%
5	Game consoles	10.3%	Tablets	4.1%	Games consoles	8.3%
6	Audio equipment	5.1%	Security cameras	4%	Tablets	7.1%
7	Voice assistants	3.73%	Network nodes	2.4%	Security cameras	3.8%
8	Network nodes	32.9%	Audio equipment	1.9%	NAS	1%
9	Security cameras	2.7%	NAS	0.9%	Audio equipment	0.7%
10	NAS	1.2%	Lighting	0.2%	IP Phones	0.2%

Media boxes and smart TVs also dominate the top three most common household IoT devices in the UK, France, and Spain. This is followed by printers which feature in third place for the UK and second place for Spain and France.

CENTRAL EUROPEAN COUNTRIES & RUSSIA

No.	Czech Republic	%	Slovakia	%	Russia	%
1	TVs	43.4%	TVs	40.3%	TVs	46.4%
2	Printers	20%	Security cameras	20%	Printers	15.4%
3	Network nodes	8%	Printers	15.6%	Security cameras	11.2%
4	Media boxes	7.3%	Media boxes	7.4%	Media boxes	8.9%
5	Security cameras	6.8%	Network nodes	6.2%	Tablets	8.3%
6	Game consoles	4.5%	Game consoles	4.4%	Network nodes	4.3%
7	Tablets	4.3%	Tablets	2.7%	Game consoles	3.7%
8	NAS	3.5%	NAS	1.9%	NAS	0.9%
9	–[4]	–	–	–	IP phones	0.5%
10	–	–	–	–	Audio equipment	0.3%

[4] Empty fields: No statistically relevant data available

Smart TVs are the top runner in Czech (43.4%) and Slovak (40.3%) households. In Slovakia, security cameras are one of the top most used connected devices, used by 20% of smart households and which can include baby monitors. Security cameras come fifth in the Czech Republic (6.8%). Media boxes make it into the top four for both countries with 7.3% of Czech and 7.4% of Slovak households having one on their network.

ASIAN COUNTRIES

No.	India	%	Indonesia	%	Singapore	%
1	Security cameras	21.8%	Security cameras	23.2%	Printers	33.6%
2	Printers	18.29%	Printers	22.2%	Tablets	19%
3	TVs	17.45%	Network nodes	17.7%	TVs	16.4%
4	Media boxes	15.2%	Tablets	13%	Network nodes	8.7%
5	Tablets	10.3%	Media boxes	10.9%	Security cameras	8.3%
6	Network nodes	5.1%	TVs	10.2%	Media boxes	7.1%
7	Games consoles	3.73%	Games consoles	1%	NAS	3.8%
8	–	–	–	–	Games consoles	1%
9	–	–	–	–	Audio equipment	0.7%
10	–	–	–	–	Voice assistants	0.2%

No.	South Korea	%	Japan	%
1	Printers	34.4%	Printers	36.6%
2	TVs	20.4%	Media boxes	24.4%
3	Media boxes	19%	Game consoles	9.1%
4	Tablets	9.4%	Tablets	8.8%
5	Security cameras	5.1%	Network nodes	7.3%
6	Game consoles	4.1%	TVs	7.1%
7	Network nodes	3.3%	Security cameras	1.8%
8	NAS	3%	NAS	1.2%
9	–	–	Game handhelds	1.1%
10	–	–	NAS	1%

India is the country that has the most connected security cameras, accounting for a third (34.3%) of all smart home devices in India and nearly one-quarter of smart home devices in Indonesia.

In Japan and South Korea, printers are the number one smart home device, accounting for 34.4% of all smart home devices in Japan, and 36.6% of devices in South Korea

Security risks for smart homes

The greatest security risk for smart homes are weak credentials
The Avast research found that two out of five (40.8%) digital homes worldwide contain at least one device that is vulnerable to cyber attacks. Out of these, 69.2% are vulnerable due to weak credentials, and 31.4% due to software vulnerabilities. Avast Wi-Fi Inspector discovers weak passwords and alerts its users, advising them to fix the issue. Therefore, we could consider that this number might be higher if users were not getting this guidance.

40.8%
contain at least one device that is vulnerable to cyber attacks

Despite the rapid increase in IoT devices entering the home, the security built into these devices isn't always the strongest; with manufacturers rushing to get their great product idea into the market, security is often left as an afterthought.

69.2%
which are vulnerable have weak access credentials

The research shows that we're often our own worst enemies when it comes to keeping our devices safe. Strong passwords and two-factor authentication are a vital part of the security steps we need to take when protecting the devices in our homes.

59.7%
of routers have weak credentials or some vulnerabilities

Additionally, 31% of devices are vulnerable to not being patched. Hackers love to exploit old software, as it's often the weakest link in most people's security. That's why regular software updates are fundamental to keeping the devices in your home secure.

Outdated software lacks the most current security measures and patches, leaving households vulnerable to hackers who know how to exploit these weak spots. To ensure that they're fully protected, people need to update their software regularly.

59.1%
of users worldwide have never logged into their router or have never updated its firmware

The weak entry point to many smart homes: Routers
Routers are the central point in any smart home, acting as the "gateway" to the internet. Therefore, a router that is vulnerable to attack poses a risk for the whole home, much like leaving your front door unlocked. Cybercriminals can redirect compromised routers to access exactly what the they want, including phones, computers or any other connected device.

Avast found that well over half (59.7%) of routers either have vulnerabilities, or weak credentials. On the one hand, weak credentials protecting the router's administrative interface could allow third parties to gain access to easily reconfigure the router. On the other hand, weak Wi-Fi access credentials make it easy for cybercriminals to snoop on their traffic.

An Avast survey among more than 19,000 internet users shows that 59% of users worldwide have either never logged in to their router or have never updated their router's firmware, leaving them potentially vulnerable to fairly simple attacks.

Routers have proven to be simple and fertile targets for a growing wave of attacks. While many attacks against routers use variants based on the Mirai codebase (which was released by the creator shortly after the successful attacks of September 2016), many are far more complex and point to a murky future for home network security.

Not only did we see an increase in router-based malware in 2018, but also changes in the characteristics of those attacks. Where router-based malware has traditionally taken over a device for the purposes of carrying out a DDoS attack, such as the Mirai attacks, today's attacks use malware to infect a device and open up a line of communication to a C&C (command and control) server.

Graphic: A single vulnerable device can be the entry point for a cybercriminal to access the whole network.

The most prevalent vulnerable smart home devices

When it comes to smart household devices, the top of the overall most prevalent vulnerable devices worldwide are printers. Printers have been in homes for many years, perhaps causing users to forget that they pose a threat to the network, or perhaps used less than before and so are less likely to be maintained.

Top vulnerable devices per country (excluding PCs, smartphones, and routers)

NORTH AMERICA & AUSTRALIA

No.	U.S.	%	Canada	%	Australia	%
1	Printers	43.8%	Printers	33.7%	Printers	35.8%
2	NAS	17.7%	NAS	26%	Network nodes	19.7%
3	Security cameras	14.7%	Media boxes	12.9%	NAS	19.4%
4	Network nodes	14.6%	Network nodes	12.4%	Security cameras	11%
5	Media boxes	3.7%	Security cameras	10.8%	Media boxes	8.5%
6	TVs	2.8%	TVs	1.5%	TVs	3.2%
7	DVRs	1.2%	DVRs	0.9%	Gaming consoles	0.5%
8	Tablets	0.3%	–	–	–	–
9	Game consoles	0.2%	–	–	–	–
10	–	–	–	–	–	–

Printers top the list across the U.S., Canada and Australia. NAS devices are also among the top most vulnerable with 17.7% in the U.S., 26% in Canada, and 19.7% in Australia.

As content streaming becomes the new norm for consuming content, media boxes are becoming an increased source of vulnerability, featuring in the top five for the U.S. and Australia, and the top three in Canada.

GERMAN SPEAKING COUNTRIES

No.	Germany	%	Austria	%	Switzerland	%
1	Network nodes	31.2%	Network nodes	36.5%	NAS	30%
2	Printers	29.%	Printers	27.4%	Printers	26%
3	NAS	21%	NAS	15.7%	Network nodes	25%
4	Security cameras	11.6%	Security cameras	14.3%	Security cameras	10.25%
5	Media boxes	2.46%	TVs	2.45%	Media boxes	4.3%
6	Remote controls	0.6%	Media boxes	1.4%	TVs	2.37%
7	Tablets	0.2%	HVAC_Controls	0.8%	Tablets	0.4%
8	Gaming consoles	0.1%	Tablets	0.3%	–	–
9	–	–	–	–	–	–
10	–	–	–	–	–	–

Network nodes are the most vulnerable devices in Germany (31.2%) and Austria (36.5%) with NAS topping the list in Switzerland (30%). In the home, a network node is essentially networking hardware that isn't a router, such as a redistribution point or a communication endpoint. Across all three countries printers come in as the second most vulnerable.

WESTERN EUROPEAN COUNTRIES

No.	UK	%	France	%	Spain	%
1	Network nodes	25.9%	Security cameras	32.7%	Network nodes	55.6%
2	Printers	25.11%	Network nodes	22%	Printers	28.39%
3	NAS	21%	Printers	21%	Security cameras	5.7%
4	Security cameras	20.1%	NAS	12.9%	NAS	5.2%
5	Media boxes	4.6%	Media boxes	8%	Media boxes	2.62%
6	TVs	1.5%	TVs	2.54%	TVs	1.2%
7	DVRs	0.9%	DVRs	0.2%	Tablets	0.5%
8	Tablets	0.3%	Tablets	0.1%	DVRs	0.2%
9	–	–	–	–	–	–
10	–	–	–	–	–	–

Network nodes make up over half (55.6%) of vulnerable devices in Spain – compared to 25% and 22% in the UK where it is also the top vulnerability, and France's 22% where it comes in second on the list. The top vulnerable device in French households are security cameras with 32.7%, making up nearly a third of all vulnerable devices.

CENTRAL EUROPEAN COUNTRIES & RUSSIA

No.	Czech Republic	%	Slovakia	%	Russia	%
1	Network nodes	37%	Network nodes	36.7%	Printers	45.0%
2	Printers	24.4%	Printers	24.2%	Security cameras	22.9%
3	NAS	18%	Security cameras	21.8%	Network nodes	17.3%
4	Security cameras	14%	NAS	10.2%	TVs	6.1%
5	TVs	3.5%	TVs	2.8%	NAS	4.4%
6	Media boxes	1.3%	Media boxes	2.3%	Media boxes	2.5%
7	DVRs	0.7%	DVRs	0.9%	DVRs	1.1%
8	–	–	–	–	Tablets	0.4%
9	–	–	–	–	Home appliances	0.1%
10	–	–	–	–	Game consoles	0.1%

In the Czech Republic and Slovakia, network nodes (37% and 36.7%, respectively) are the most vulnerable connected device followed by printers (24.4% and 25.2% respectively). NAS and security cameras both feature in the top four vulnerable devices for both countries.

ASIAN COUNTRIES

No.	India	%	Indonesia	%	Singapore	%
1	Security cameras	45.6%	Network nodes	36.7%	Printers	37.4%
2	Printers	29.9%	Security cameras	24.4%	Security cameras	19.8%
3	Network nodes	13.3%	Printers	24.3%	Network nodes	17.6%
4	NAS	5.1%	Media boxes	6.5%	NAS	12.9%
5	DVRs	2.8%	NAS	3.4%	Media boxes	7.8%
6	TVs	1%	TVs	2.49%	DVRs	2.9%
7	Media boxes	1%	DVRs	1%	TVs	1%
8	–	–	–	–	–	–
9	–	–	–	–	–	–
10	–	–	–	–	–	–

No.	South Korea	%	Japan	%
1	Printers	61.4%	Printers	42.3%
2	Security cameras	12.2%	Network nodes	36.5%
3	NAS	11.4%	Media boxes	12.6%
4	Network nodes	11.1%	Security cameras	4.9%
5	Media boxes	3.2%	NAS	1.4%
6	TVs	0.5%	TVs	1.1%
7	–	–	Game handhelds	0.3%
8	–	–	–	–
9	–	–	–	–
10	–	–	–	–

Printers make up an overwhelming proportion of the most vulnerable devices in South Korea with 61.4%. Printers also topped the list in Japan and Singapore with 42.3% and 37.4% respectively.

In India, the most vulnerable device was security cameras (45.6%) and network nodes came out on top in Indonesia with 36.6%.

Conclusion

Increased IoT usage needs increased protection
With IoT growth predicted to more than triple by 2025 to over 75 billion connected things, manufacturers are under pressure to deliver smart devices to market quickly and at an affordable price; however, this often means security features are neglected.

As IoT devices, such as a Google Home or an Amazon Alexa, grow in popularity, there needs to be greater consumer awareness to help mitigate the risks they could pose if not properly protected.

The reality is that many smart devices can be compromised, including thermostats, streaming boxes, webcams and digital personal assistants – and consumers and small businesses are among the most vulnerable users. One of the more common types of attack is when cybercriminals hack thousands of IoT devices in unsuspecting households to create networks of infected devices known as botnets to perform attacks on others.

Our research shows how many devices are vulnerable to attack, either because they use weak access credentials, or due to outdated firmware, especially where (in some cases) patches aren't even available.

The current approach to securing IoT devices is to expect the user to take action and understand how to accomplish this — even when the majority of vulnerabilities are caused by unpatched security flaws, which is extremely concerning. This approach creates a security gap — and a massive opportunity for cybercriminals. With a high diversity of IoT devices on the market, it is difficult and complex to provide protection at the device level, and therefore smart home security needs to begin and end at the network level.

That said, there's only so much that consumers, and indeed manufacturers can do. Whether people are using their smart speakers to wake up in time for work, play music, or to buy items online, the truth is that these devices stream valuable personal data about the habits of the household. This makes them a very attractive target for cybercriminals who are constantly finding new ways to attack.

In a perfect world, IoT manufacturers would be working with security experts to ensure a security layer is included in their devices. For now, we can take action to protect the router in a smart home, which is often an overlooked device, capable of more than we might realize – more than just connecting our homes and devices to the internet. Most IoT devices rely on network security, which means that everything and everyone on the same network can gain control or access to them. If a home router, for example, is hacked or poorly configured allowing attackers to get into a network, they can control most of the IoT devices connected to the network, especially as most IoT devices are also vulnerable. Consumers do have the means to change their router password and keep its firmware updated, and these simple steps can ensure their smart home is immediately a safer place.

Methodology

The data in this document has been obtained from scans run by Avast users from their computers using the Avast WiFi Inspector feature during September 2018. In total 16 million different home networks worldwide are included in this study from countries all around the world. 56 million devices were scanned.

This report outlines the specific results from home networks in the following countries (in alphabetical order). All non-home networks have been excluded from this study.

Number of home networks scanned per country for this report

Argentina	**364,933**
Australia	**117,773**
Austria	**54,619**
Brazil	**2,032,447**
Canada	**221,464**
Czech Republic	**248,945**
France	**1,441,545**
Germany	**563,082**
India	**607,844**
Indonesia	**297,881**
Japan	**231,106**
Mexico	**474,075**
Portugal	**106,888**
Russia	**1,119,791**
Singapore	**19,737**
Slovakia	**54,267**
South Korea	**894,10**
Spain	**559,143**
Switzerland	**62,400**
UK	**406,185**
US	**747,396**
Other	**6,478,265**

About Avast Smart Life

Avast's artificial intelligence-based IoT security platform, Smart Life, provides insights into anomalies in smart home network traffic and alerts users if any devices start to behave abnormally, e.g. their fridge starts sending masses of emails for no obvious reason. Avast is currently working on delivering the Smart Life service to mobile users through carrier partnerships, and will also offer a plug and play solution based on Smart Life, directly to consumers.

About Avast

Avast (LSE: AVST) is the global leader in digital security products. With over 400 million users online, Avast offers products under the Avast and AVG brands that protect people from threats on the internet and the evolving IoT threat landscape. The company's threat detection network is among the most advanced in the world, using machine learning and artificial intelligence technologies to detect and stop threats in real time. Avast digital security products for mobile, PC and Mac are top-ranked and certified by VB100, AV-Comparatives, AV-Test, OPSWAT, West Coast Labs and others. Visit: **www.avast.com**.