F-Secure

Putting a price on smart home protection

How Internet Service Providers can protect customers, increase revenue and enhance their brand with digital security

Key takeaways

Internet security and privacy are now considered as important as high speed when choosing a home gateway/Wi-Fi router

- **33%** of consumers have experienced some form of cybercrime in the last year
- **81%** of consumers either expect their Internet Service Provider (ISP) to keep them safe as a core part of their internet offering or expect some level of protection from online threats but are willing to pay for increased threat protection
- **20%** of an average service provider's internet customer base is at risk if an operator is noncompetitive on providing security

Today's consumer knows the risks of leaving their smart devices unprotected, and this manifests in both a desire for protection from the providers they trust and a willingness to pay for it

- **42%** of consumers believe smart home device manufacturers are not doing enough to ensure their online security and privacy
- **42%** of consumers worry that one of their internet connected smart home devices could become infected by a virus/malware or be hacked
- **62%** would be willing to pay for the protection of all their internet connected devices at home

Protecting smart devices requires a smart approach

Methodology

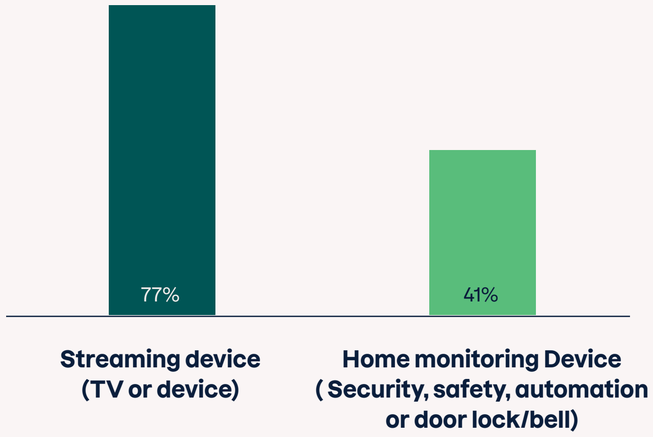
The F-Secure Global Connected Home Survey was undertaken in June 2023. The total number of respondents was 4400. Data in charts selected from 11 countries: Brazil, Germany, Finland, France, Italy, Japan, Netherlands, Norway, Sweden, United Kingdom, United States. (N = 400/country, age 25-74 years). All data refers to this study unless referenced otherwise.

Smart home devices are here to stay, and consumers need protection

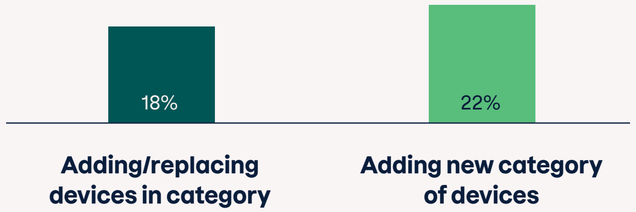
In a world where convenience is the new currency it's no wonder that internet connected smart home devices are so popular. Deloitte has found that there are now 22 connected IoT (Internet of Things) devices in the average home within the United States, and this is expected to rise by 55% by 2025.

But today, it's not just computers and phones that are connected to home Wi-Fi networks. We have found that 77% of consumers have a TV streaming device in their homes, while 41% of consumers have some kind of home monitoring device, and 27% of consumers use smart wearables. Plus, we found that 18% of consumers plan to add or replace a device in the next 12 months, while 22% plan to add a new one in a new category. If this tells us one thing, it is that smart devices are here to stay.

% Owning one or more connected devices



Plan to purchase devices in next 12 months



22

the number of connected IoT (internet of things) devices in the average home within the United States according to Deloitte

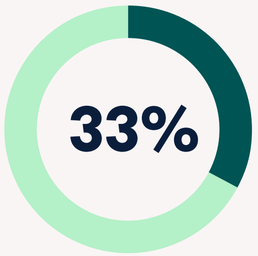
55%

the predicted increase in this figure by 2025, according to Statista

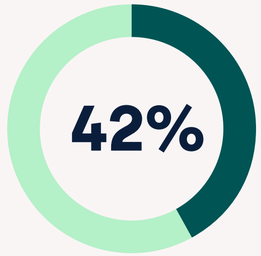
Consumers are worried about their digital security at home

While consumers are fast filling their homes with smart devices, they are no less worried about cyber crime. F-Secure has found that more than half of consumers feel likely to be a victim of cyber crime or identity theft in the future, while 33% of respondents said that they had been a victim in the last 12 months.

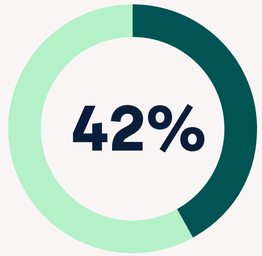
What's more, 42% are worried that one of their internet connected smart home devices could get infected by a virus/malware or be hacked. Perhaps this is driven by a lack of faith in device manufacturers - we found that a further 42% believe that smart home device manufacturers are not doing enough to ensure their online security and privacy.



said they had been a victim of cyber crime in the last 12 months

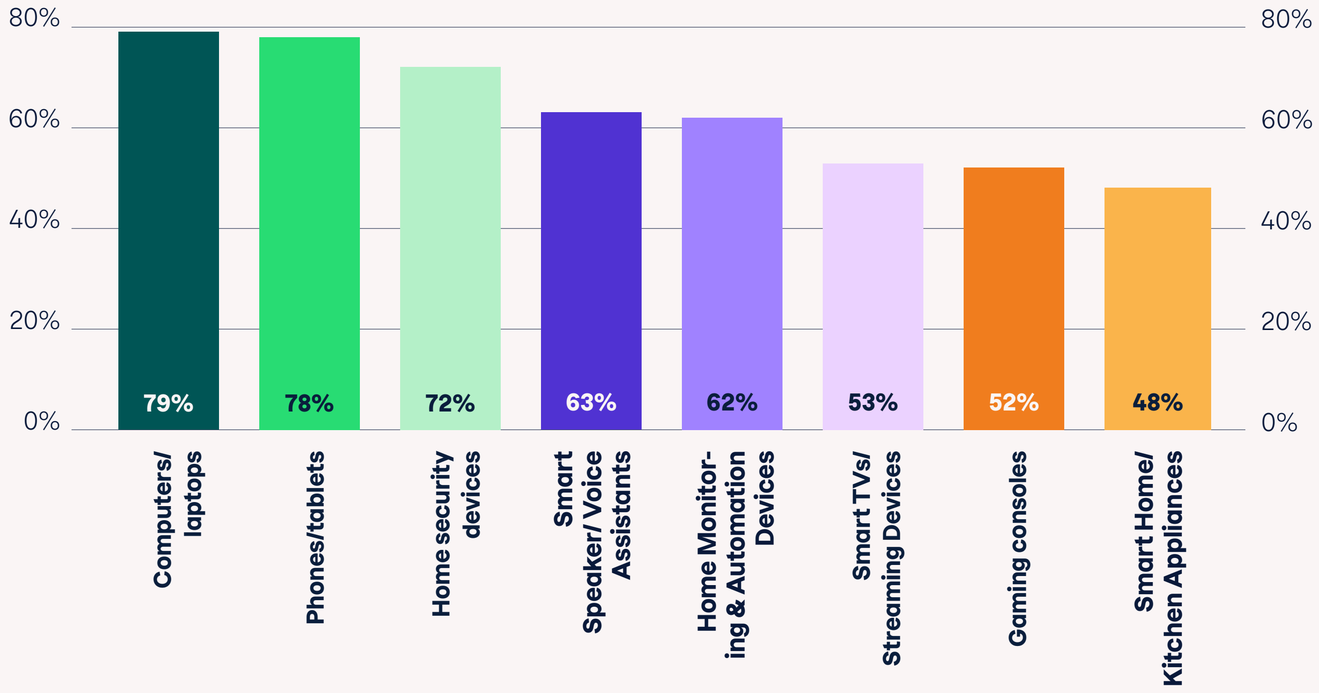


worry that one of their internet connected smart home devices could get infected by a virus/ malware or be hacked



believe smart home device manufacturers are not doing enough to ensure their online security and privacy

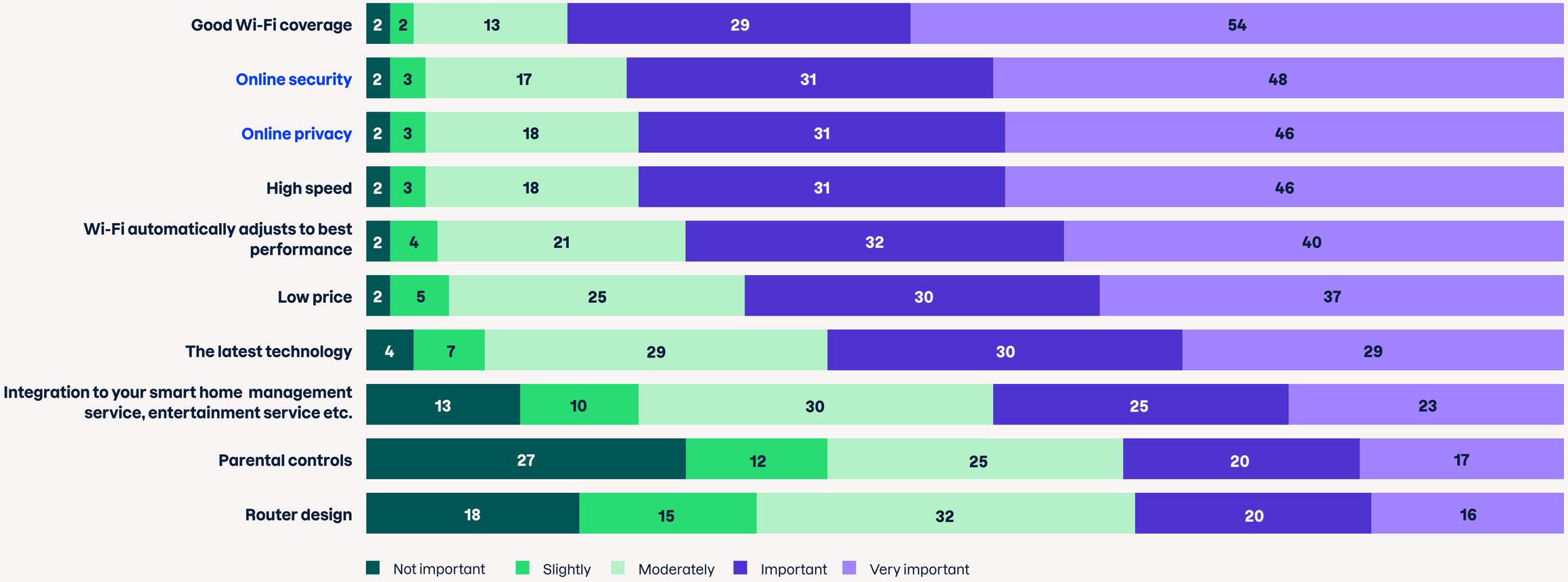
% Saying it is important to protect selected devices



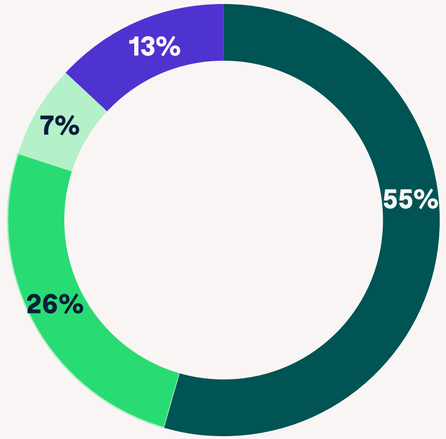
Internet security and privacy are considered as important as speed

There is no doubt that consumers today are recognizing the importance of protecting their devices. Security and privacy are now considered the second and third most important factors when choosing a home gateway/Wi-Fi router.

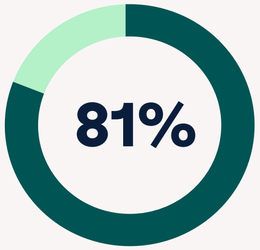
How important are the following factors when choosing your home gateway / Wi-Fi router?



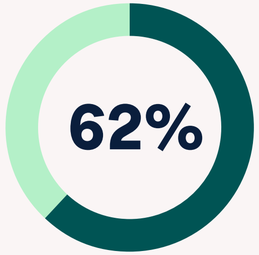
How much do you rely on your internet/Wi-Fi service provider to actively protect you from online threats?



- I expect my internet service provider to keep me safe as a core part of their service offering
- I expect some protection from online threats, but am willing to pay for additional security features and increased threat protection to keep me safe
- I do not rely on my internet service provider to keep me safe and am willing to pay for protection of all my internet connected devices
- I do not worry about online threats



of survey respondents said that they either expect their ISP to keep them safe as a core part of their internet offering or expect some level of protection from online threats, but are willing to pay for increased threat protection



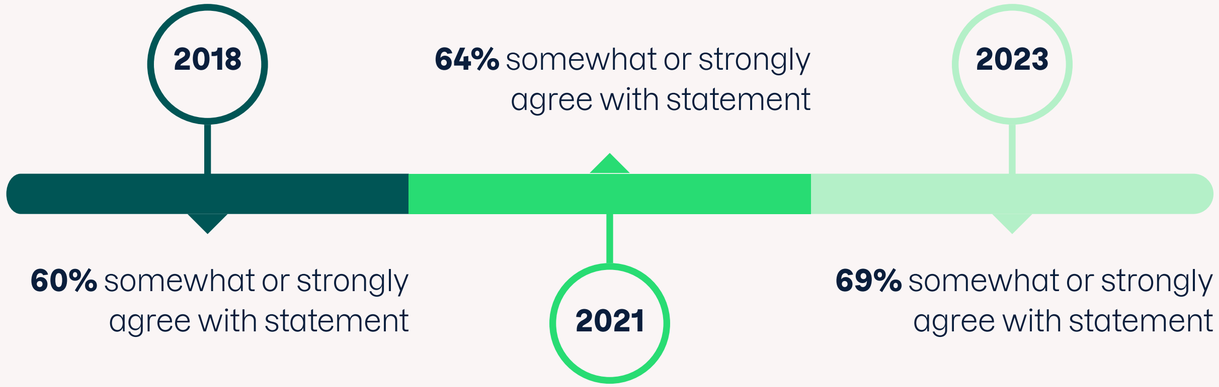
of survey respondents said that they would be willing to pay for the protection of all their internet connected devices at home

Cultivating consumer trust pays off

Not offering internet security may not be a viable option for ISPs for much longer. Of the 55% of consumers that expect their ISP to keep them safe and do not explicitly say they are willing to pay for supplemental protection, a worrying 36% say they are at least somewhat likely to leave for another provider offering better protection at the same price/speed.

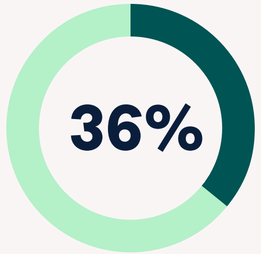
This means that around 20% of an average ISP's internet customer base is at risk if an operator is noncompetitive on providing security. Alternatively, this presents a huge opportunity for an operator that provides security over one that doesn't.

"I would purchase my security and privacy services from my internet service provider."

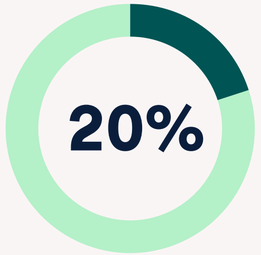


Source(s): 2022 F-Secure Connected Home Whitepaper, F-Secure Global Connected Home Survey, 2023

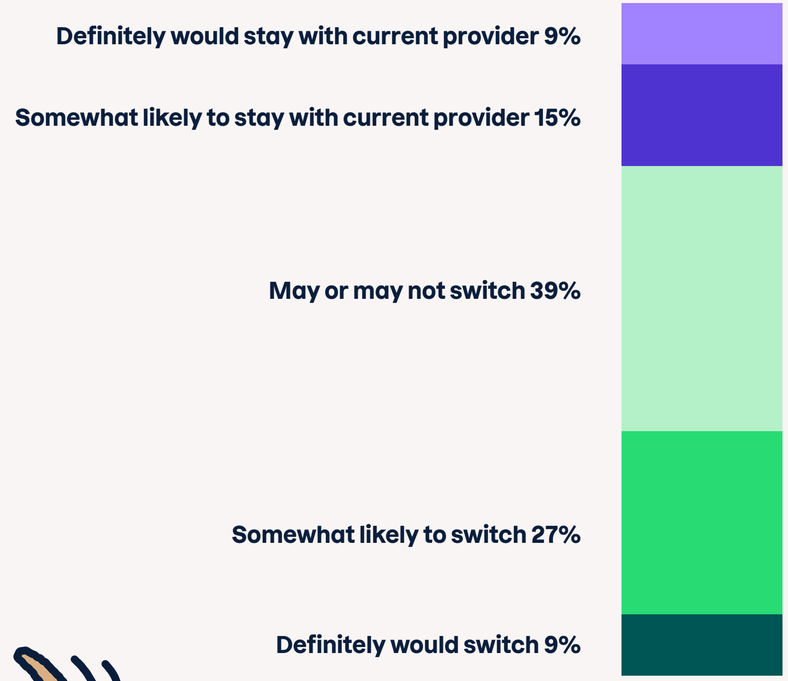
Likelihood to switch providers offering better security at same price/speed*



of consumers say they are at least somewhat likely to leave for another provider offering better protection at the same price/speed



of an average service provider's internet customer base is at risk if an operator is noncompetitive on providing security



*of those that expect their internet service provider to keep them safe as part of their internet service

Protecting smart devices requires a smart approach

Today's consumer knows the risks of leaving their smart devices unprotected, and this manifests in both a desire for protection from providers they trust and a willingness to pay for it. But is protecting these with legacy solutions the security equivalent of putting a square peg in a round hole?

The connected home device category is highly fragmented. There are hundreds of thousands of device types on the market, and this is only growing. This presents two unique issues. Not only is identifying threats for thousands of devices and device models extremely difficult, but there are also no specific endpoint online security solutions provided. In fact, many manufacturers overlook device security for these smart devices altogether.

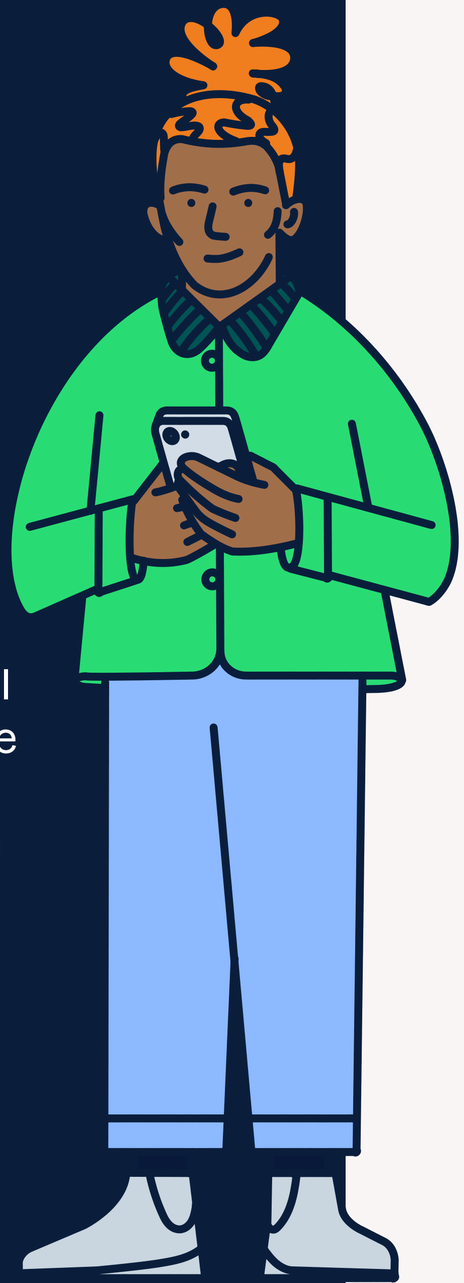
Endpoint protection does a great job of protecting phones and computers against threats, but most smart home devices do not allow installation of endpoint security protection on the device itself. As cyber security expert and author Mikko Hyppönen titled his bestselling book, "if it's smart, it's vulnerable."

"Unfortunately, many of the companies that got into making smart home devices didn't prioritize security. Some devices couldn't be updated at all. Other companies failed to issue fixes in a timely manner. Given how AI tools can encourage even greater intimacy and trust on smart home devices, they will only become more attractive to motivated attackers."

Tom Gaffney,
Director, Business Development, F-Secure

Does artificial intelligence (AI) hold the key to smart device protection?

At F-Secure, we understand that AI is the future, and we are heavily investing in AI technology. This includes using AI to better protect connected home devices. For example, we are currently using machine learning to identify and highlight our F-Secure users' abnormal data traffic from smart home devices.



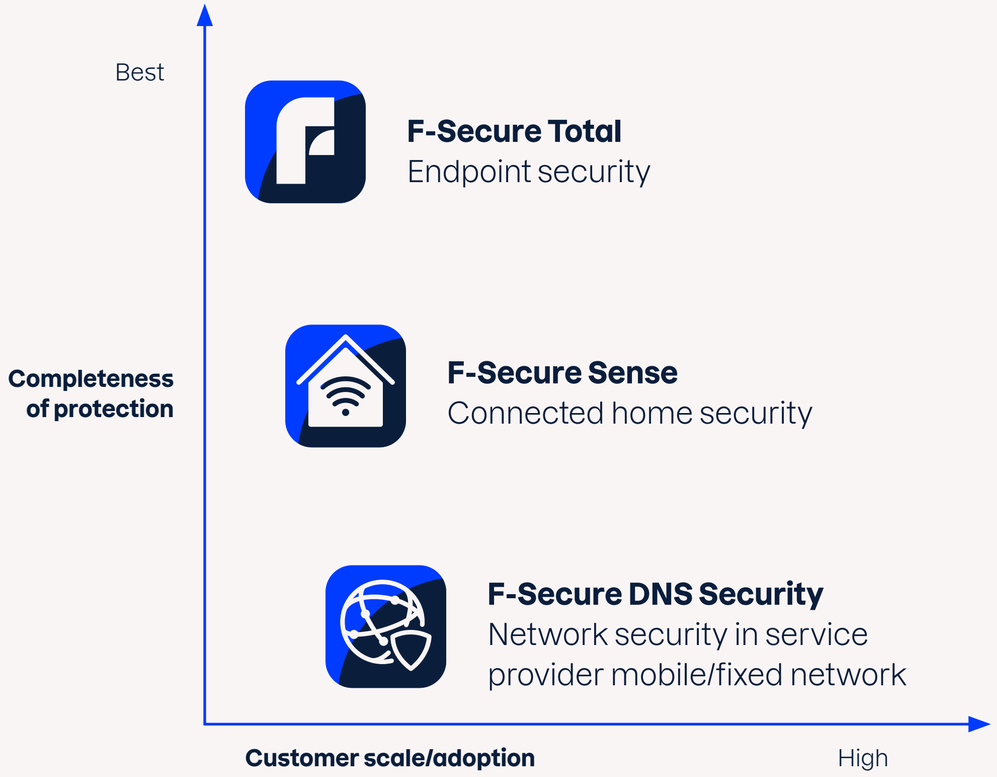
F-Secure provides holistic, seamless and converged protection for your customers

At F-Secure, we recognize that keeping consumers safe requires flexible solutions that meet our partners' business objectives. While we're best known for F-Secure Total, our comprehensive endpoint security solution, we also provide router-based and network-based security solutions that enable Internet Service Providers to offer layers of security protection with flexible business models to best meet customer needs.

Whether your goal is to offer broad, cross-platform protection, drive gateway rentals and services through online protection of all connected devices or drive incremental revenue and lower churn by offering the very best protection for devices, F-Secure can provide the perfect tailored solution for you.

F-Secure’s three layer security solution for maximum protection and ARPU

For best protection and Average Revenue Per User (ARPU) opportunity, F-Secure offers a three-layered security solution with a flexible business model. These can be sold as independent solutions or packaged to best fit your needs and strategy.



F-Secure Total - endpoint security

Offers unparalleled online security, privacy and identity protection for phones, computers, and tablets, ensuring the broadest defense against a wide array of threats.

F-Secure Sense - connected home security

Provides full visibility into home network traffic and extends protection to all devices in the home network. It also encourages the installation of endpoint protection on personal devices.

F-Secure DNS Security - network security

Delivers baseline protection to all devices within the communication service provider's mobile and or fixed network, and caters to devices where users are not activating endpoint security or connected home security.

Keen to find out more about how to drive incremental revenue while protecting your customers?

Fill out the contact from
and let us show you how.

Contact us now

About us

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 180 partners.

For more than 30 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For more information visit F-Secure today.

F-Secure®