YOUR ROADMAP FOR CYBER SECURITY SERVICE CREATION

F-Secure

The cyber security threat landscape is more complex than ever and customers need a partner who can keep them safe. That's why adding managed security services to your offering is a must if you want to survive and thrive.

Right now, businesses of all sizes across virtually all industries are facing challenging times. With remote work on the rise and employees working from locations outside organizations' security perimeters, businesses are scrambling to stay safe. And in an increasingly complex, active and well-organized threat environment, this is very much a growing challenge.

A portfolio that includes managed cyber security services is the future because it delivers the security and flexibility your customers demand and the constant revenue flow your business needs. But building it can feel like a daunting task, as it requires new skills, deep knowledge and different ways of working. You don't have to face these challenges alone – we can help.

We've put together this guide to share insights from our latest market research on market demand and what you need to consider when building a managed cyber security services offering. At the end of the paper, we'll invite you to take the first step and book a free service design workshop.

SERVICES ARE THE ONLY WAY FORWARD – FOR YOUR CUSTOMERS' BUSINESS AND FOR YOURS

Today, cyber security is a priority not only for IT teams but for C-level business leaders. Where organizations used to think of cyber security more as a form of insurance, having the right security measures in place is now seen by business leaders as a way to actually increase the value of their organization. And the pandemic and its many ramifications have made the demand for top-quality and comprehensive cyber security even more urgent.

The biggest driver behind this trend is the threat landscape, which is now changing and evolving even faster due to Covid-19. Our research shows a clear increase in demand for security personnel due to the uptick in cyber attacks against organizations of all sizes and across industries[1]. The problem, however, is that many organizations are finding it difficult to acquire and retain the highly-skilled talent they need to effectively manage their cyber security, evidenced by the fact that there are currently over four million security job vacancies and very few experts to fill them. While most companies have IT teams working on cyber security, most don't have advanced teams capable of detecting and – more importantly – responding to attacks. In short, organizations need increasingly flexible and specialized help – fast.

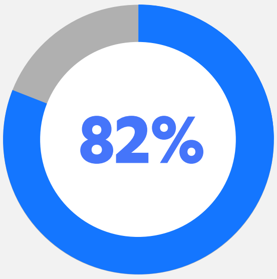
Outsourcing part or all of their cyber security to a managed service provider (MSP) or managed security service provider (MSSP) gives organizations access to security experts with a wider view of the threat landscape due to their experience working with a wide range of customers and threats. It's also a faster and more affordable option than building an in-house team.

It's no wonder, then, that our latest research shows that 65% of midmarket and enterprise customers already outsource at least some part of their security operations. And 82% are looking for a security partner able to deliver all of the solutions, expertise and services they need. According to Gartner, endpoint protection platforms and detection and remediation solutions that are delivered as SaaS or cloud-native services will be the primary choice for 75% of new deployments by 2025[2].

Digitalization, cloudification, regulatory compliance and the global pandemic are all leading organizations to look for new tools, new insights, and new ways of working. And organizations are responding to this new norm by using a wide range of vendor solutions.

In this constantly changing world, the traditional licensed-based cyber security model is quickly becoming outdated. For one thing, it requires companies to purchase the number of licenses they would need at peak consumption up front, which also means having to pay up front. In the midst of a global pandemic, this is a challenge for many organizations. In addition, software licenses don't easily allow for incremental improvement of cyber security resilience.

Clearly, a more agile subscription-based approach is needed. Adding services to your offering is key to both serving the needs of your customers and ensuring the health of your own business. That said, it's understandable that pivoting to a more service-oriented model can feel daunting. But you don't have to do it alone. F-Secure is here to help.

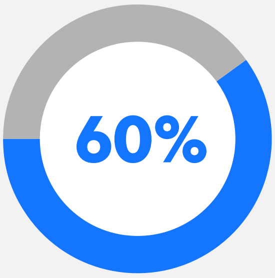


of organizations are looking for a one-stop-shop security solution.

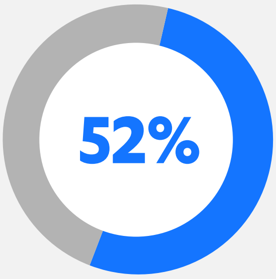
43% would prefer to use a core security system or service provider covering most needs, but still maintain some best-in-class solutions for specific functions.

39% would prefer an all-in-one security system or service provider that covers all their IT/network security needs.

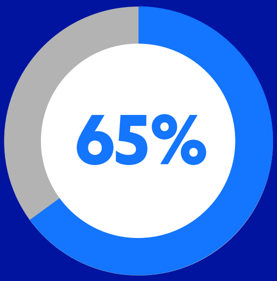
12% prefer to use multiple best-in-class security solutions.



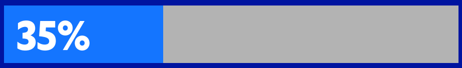
of companies see their service provider or reseller as a key security partner.



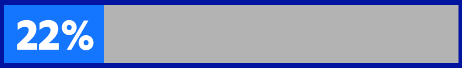
of companies have an in-house IT/security team.



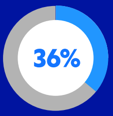
use some services in their security solution mix.



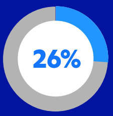
use only internally managed products



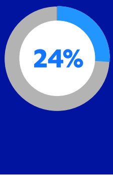
use only managed or outsourced products



cite the availability of 24/7 service



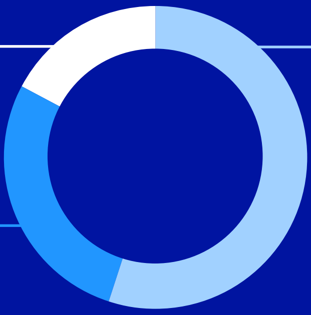
cite organizational strategy to use services



cite a lack of enough internal expertise

17%
We work directly with a security solution vendor (security brand) who provides these services

28%
We work with an IT managed service provider/MSP

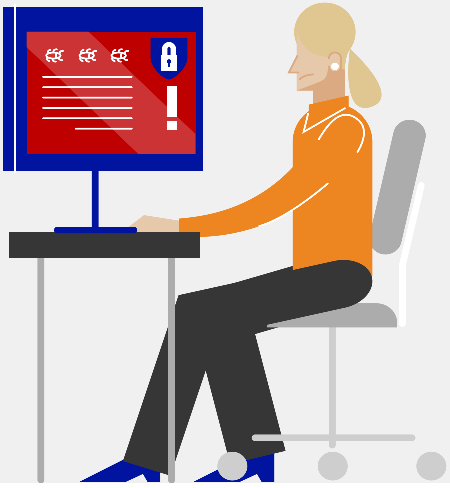


55%
We work with a managed security service provider/ MSSP

5 INGREDIENTS OF A SUCCESSFUL CYBER SECURITY SERVICE OFFERING

1. MARKET MATURITY, CUSTOMER AWARENESS

At least half of companies currently either want to buy cyber security as a service or add services to their product mix. For customers, the main drivers are access to top specialized expertise, flexibility, and the ability to increase their own skills. When choosing a partner, customers tend to look for clear contracts, flexible product options and a partner with security know-how and expertise with the ability to tailor services to their specific needs. Protection against malware and ransomware is key, but customers are also looking for services that ensure the security of cloud-based solutions and that help ensure the early detection and mitigation of attacks.



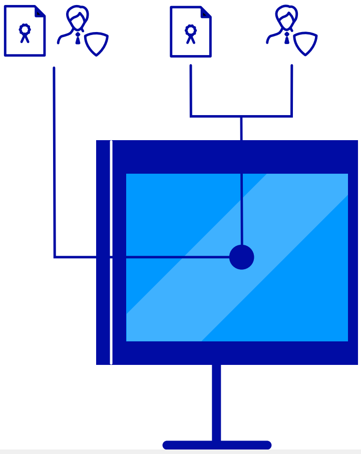
2. YOUR SERVICE DEFINITION AND SLA – WHAT DOES YOUR CUSTOMER GET

The typical SLA and service content in the midmarket segment is a service purchased with a monthly fee that includes detection, reporting (whether an attack has happened or not), and technology maintenance and updates. Mitigation is invoiced separately based on time and material, as it’s impossible to anticipate how much work and resources mitigating an attack will require. The typical midmarket SLA is currently a business-hour SLA with a two-hour response time. There is also growing interest, particularly among larger companies, in 24/7 SLA models.

3. RESOURCES, SKILLS, DELIVERY PROCESS

Running the service requires resources. If you have both service desk and security experts in house, the service desk team can handle basic IT security and things like detecting false positives. When more challenging cases are detected by the service desk, a ticket is created and the case moves to a security expert with deep knowledge around both cyber security and the products in use. Our partner competence development program with specialized career paths helps you train your staff to become security experts. When it comes to a business-hour SLA, the amount of resources needed is surprisingly low, even when handling large environments. A team of just two experts can handle an average of 45,000 incident hosts per month. And if your team needs extra support with deeper threat analysis and guidance by specialized cyber security experts, we are here for you. For tough incidents, our solution has a unique built-in "Elevate to F-Secure" service. It offers professional incident analysis of methods and technologies, network routes, traffic origins, and timelines of Broad Context Detection™ to provide expert advice and further response guidance whenever under attack.

Read more about the Elevate to F-Secure service

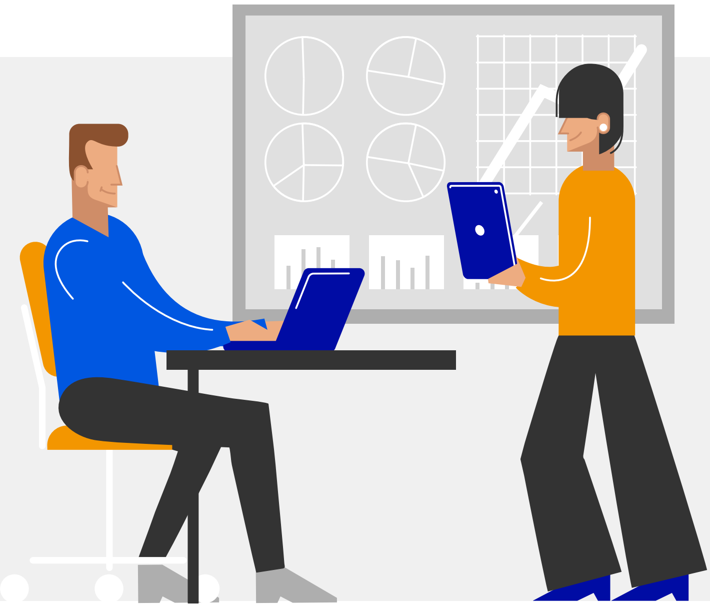


4. PRICING MODELS

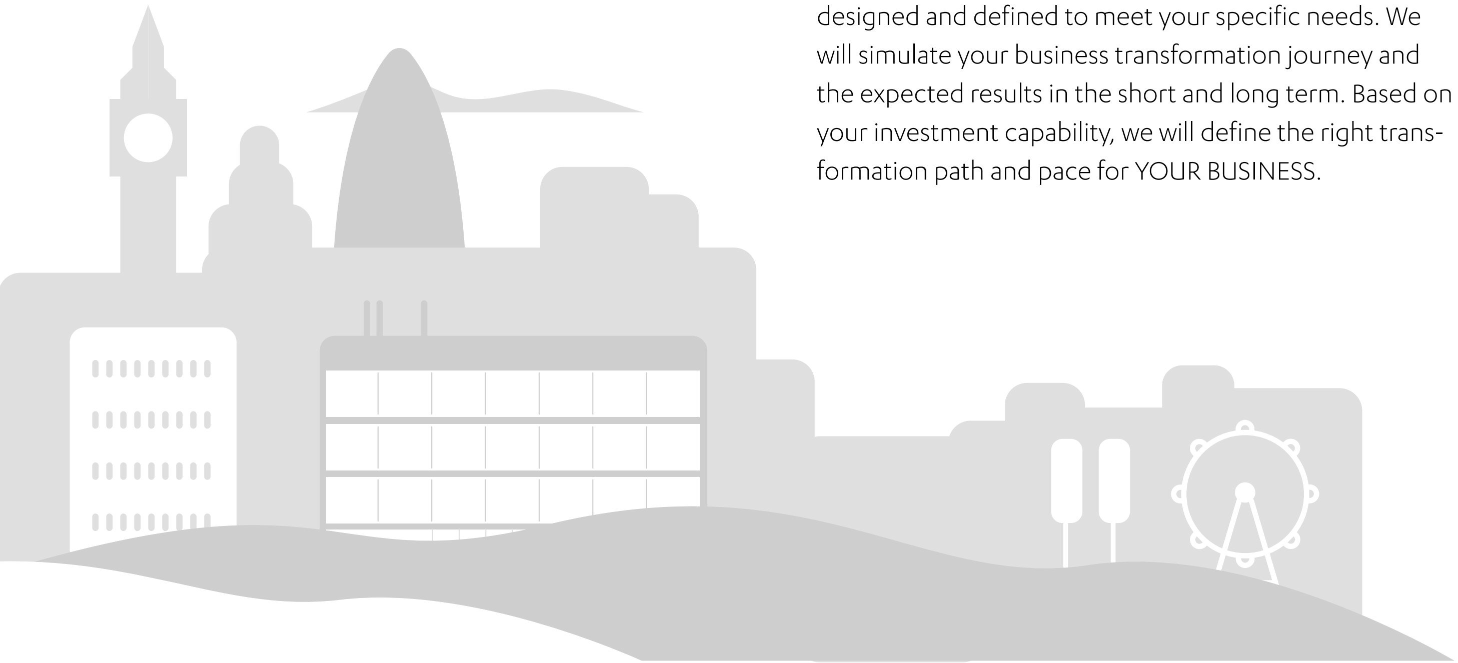
There are basically two options. The most common is one fee per monitored host, which includes both the license and service aspect. This SaaS-like model makes it clear and easy for the customer to understand what they get for whatever monthly fee they pay. The second model is to separate the licensing and service fees, which is preferred, for example, by customers who choose to manage their solutions themselves and by hybrid partners who mix and match selling licenses, services and the combination of both.

5. SALES AND MARKETING

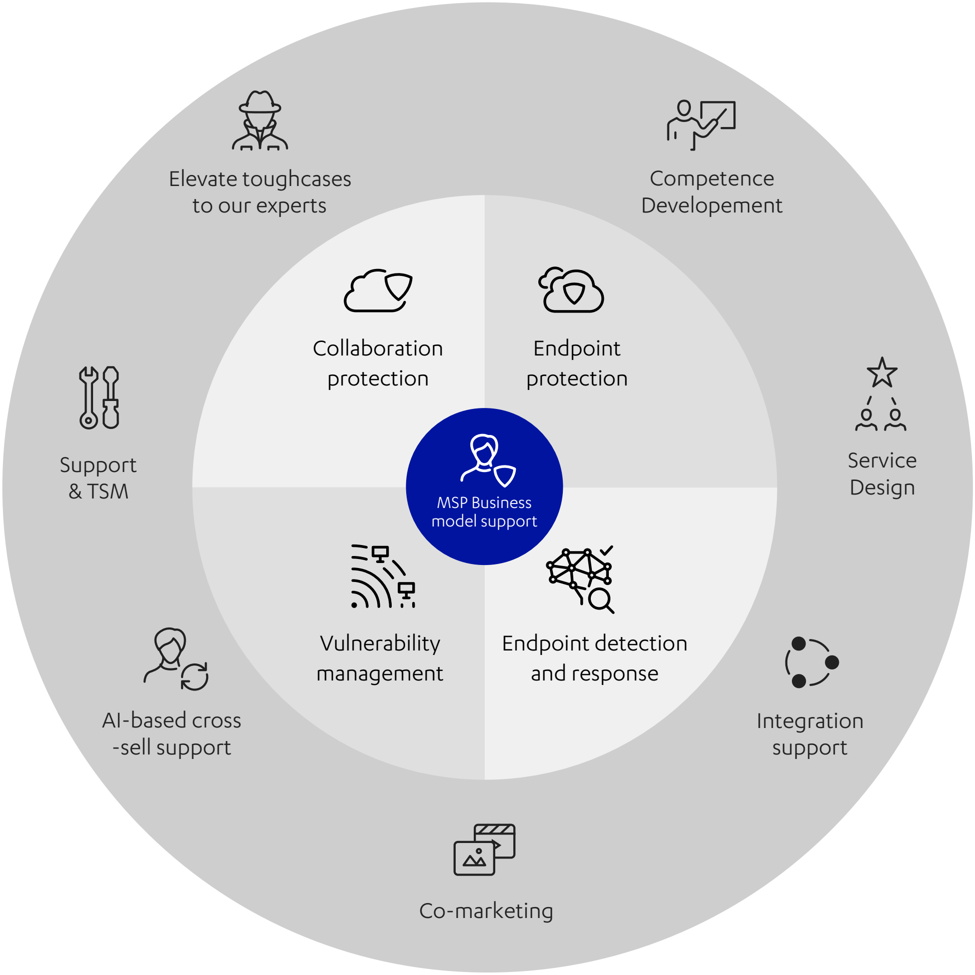
F-Secure is here to help you build a successful service offering. We provide market data and valuable insights on market and threat landscape trends. And we can also help by providing customer insights, ready-made marketing assets, face-to-face marketing planning and multi-channel campaigns ready to be launched for your lead generation. We can also do co-selling with you as well as train your sales team to sell as a service.



Our service design workshop will walk you through these steps and what they mean for your business. Together we will create a service concept in which each step is designed and defined to meet your specific needs. We will simulate your business transformation journey and the expected results in the short and long term. Based on your investment capability, we will define the right transformation path and pace for YOUR BUSINESS.



This is our unique offering designed to support your business. An award-winning solution portfolio combined with supportive partner services.



LET'S BUILD YOUR CYBER SECURITY SERVICE OFFERING TOGETHER

Challenging times like the ones we've all been in this year tend to compel organizations to focus more strongly on their core business and optimize in every way possible. For many, that means outsourcing non-strategic processes. And that's good news for businesses like yours.

The trend is clear, the transformation is underway, and the need is urgent – customers need help with digitalization, cloudification and – in particular – cyber security. Offering cyber security services elevates resellers like you to the role of a trusted advisor, increasing stickiness, loyalty and customer lifetime value. Those who seize this opportunity will be better able to differentiate themselves from the rest of the pack. Those who don't provide the services and security models their customers need and demand will soon find themselves out of the game.

According to the Wells Fargo Small Business 2020 Index, up to 82% of small and medium-sized IT resellers say that acquiring new customers is a bigger challenge than retaining existing ones. At the same time, the margins for software licenses and IT hardware are getting slimmer all the time. The commoditization of typical SKUs makes it hard to increase the average customer lifetime value. But expanding your product portfolio or offering your customers new and value-adding services can help you gain new customers and strengthen your relationship with existing ones.

Based on our research and industry insights, it is clear that MSPs and MSSPs are growing fast. In fact, accelerated by customer demand resulting from Covid-19, 50% of MSPs say that they are currently looking to expand from a more IT and product focused offering towards a portfolio that includes managed security services.

F-Secure can help you not only survive but thrive in the cyber security transformation with the right technology, the right business models and the right services.

With F-Secure's modular cyber security solutions, you can deliver the right products, valuable insights, and services that will enable your customers to concentrate on their core business with the peace of mind that their cyber security is being handled and their digital assets protected by a trusted partner.

Adding scalable ways of providing cyber security services to your customers is also likely to improve your own productivity and profitability. Holistic cyber security, including endpoint protection, detection and response, vulnerability management and cloud collaboration protection managed from a single integrated portal that provides a range of insights, whether into a single endpoint or over the company-wide estate, allows you to allocate and scale you resources as efficiently as possible.

Not all partners possess competencies that put them on the level of cyber security consultants. But with F-Secure, selling cyber security services is a joint effort. Our in-product automation simplifies incident handling, and with our Elevate to F-Secure feature, partners can escalate the toughest cases to our elite cyber security experts for threat analysis and investigation. Selection of the appropriate customer segment (small and mid-sized businesses) also plays a role in a manageable caseload. And with F-Secure's service design assistance, partners get everything they need right from the beginning: service definition, resource planning, SLA and pricing strategies, and sales and marketing strategies.

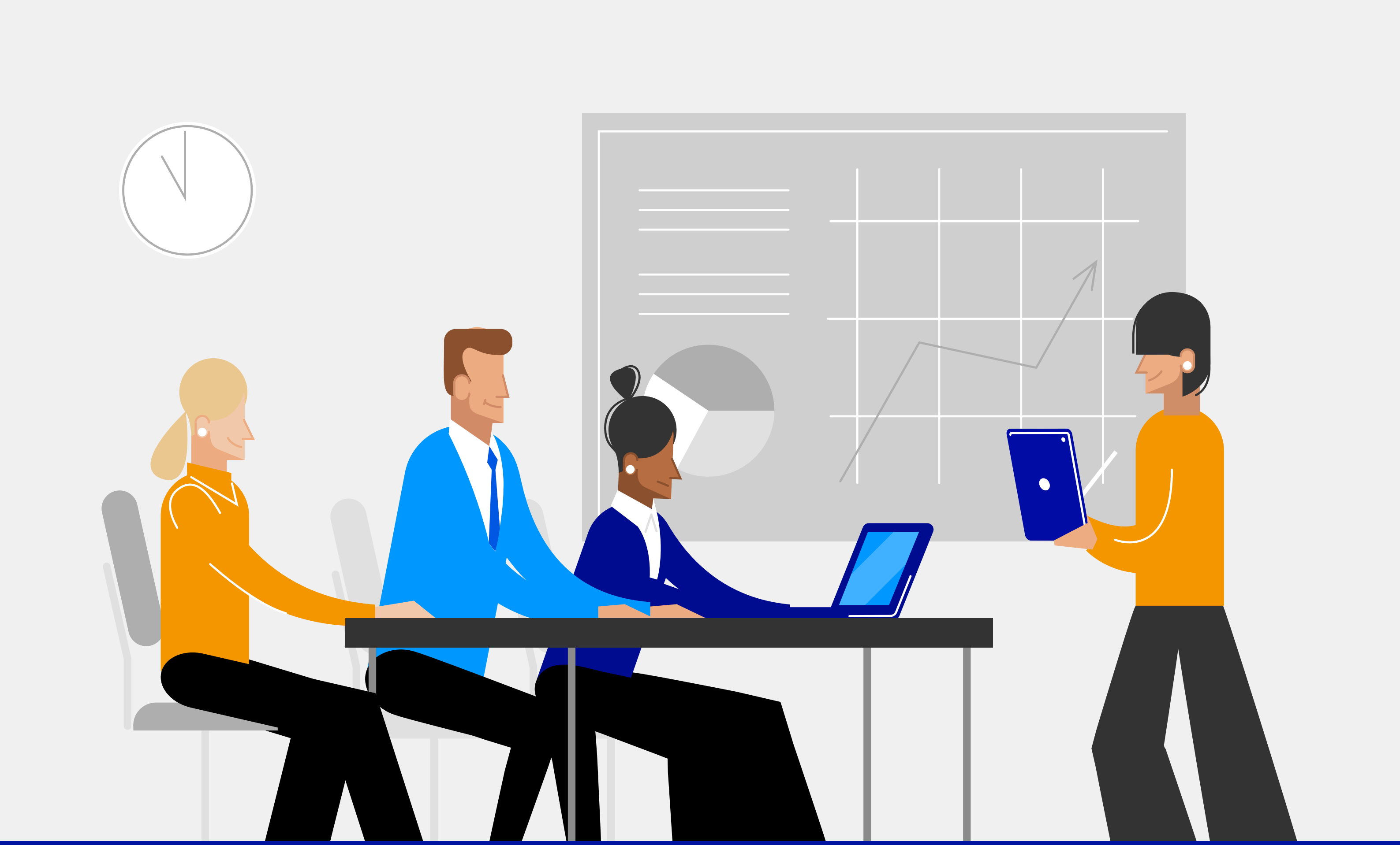
The time to act is now. The bottom line is that cyber threats are evolving too fast for organizations to keep up. Your customers are looking for a trusted partner who understands the threat landscape, their needs, and how to meet them. Extending your existing product and solution offering to include security services will help ensure that you are that partner, now and in the future.

And as your partner, F-Secure will be there to support you as you grow your business to meet the new challenges we all must face – together.

ENDNOTES

[1] F-Secure 2020 B2B Market Research

[2] Gartner Innovation Insight for Cloud Endpoint Protection Platforms, 2019



THE TOP 3 REASONS TO ENHANCE YOUR OFFERING WITH MANAGED SECURITY SERVICES

1. Meet clear and immediate customer demand and respond to the growing threat landscape.

2. Differentiate yourself and be a trusted, value-adding partner there to help your customers stay safe and operate.

3. Scale your services right and increase your profitability.

Book a free service design workshop to start building your new service offering

BOOK NOW

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure.