KEY INGREDIENTS OF A PROFITABLE MANAGED SECURITY SERVICE

F-Secure

The corporate cyber security market has been growing fast and is expected to continue expanding at a double-digit growth rate over the next four years.

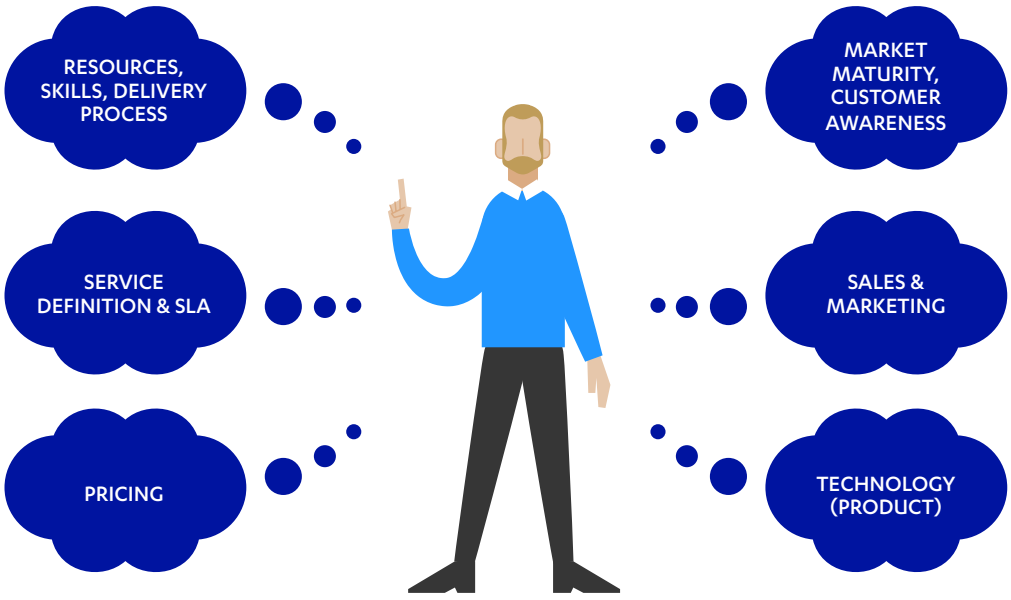
A 2021 Gartner® report predicts a constant currency growth rate in information security end-user spending of above 10% until 2025, resulting in a total market size of around $228bn.

However, not all segments are growing equally and are certainly not equally profitable. The 2021 Gartner® report titled, "Market Opportunity Map: Security and Risk Management Software, Worldwide"[2], highlights the disparity: "Operating profit margins for all security segments were as low as negative 19% and as high as 23% in 2019."

So how should managed security providers design their service offering? Clearly choosing the right services is a key component to ensure maximum profitability. However, there are many other things to consider.

In this whitepaper we will draw on our experience of working with the best managed security providers in the game, as well as running our own managed security services, to highlight the key components behind running a service that is profitable and set up to remain profitable for the long-term.

MANAGED SERVICE CONSIDERATIONS



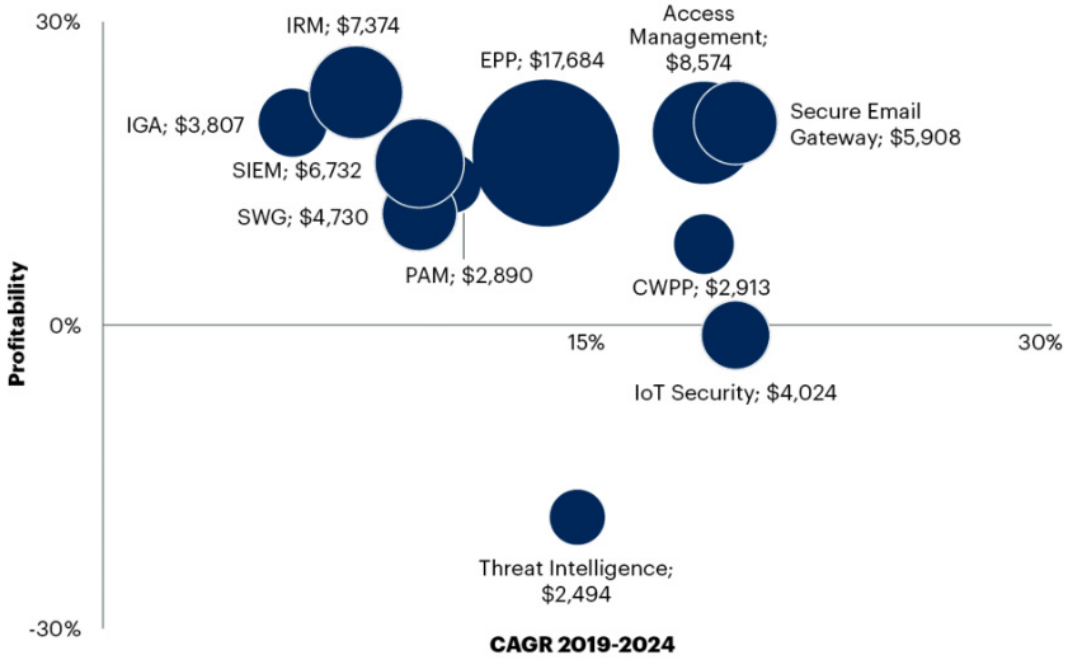
[1]Gartner: Forecast: Information Security and Risk Management, Worldwide, 2019-2025, 2Q21 Update. 24 June 2021 - ID G00752504
[2]Gartner: Market Opportunity Map: Security and Risk Management Software, Worldwide. 10 November 2020 - ID G00731517

MARKET INSIGHTS

The bubble chart below is from Gartner Market Opportunity Map: Security and Risk Management Software, Worldwide report. "The bubble size represents 2024 worldwide security spending for each segment in millions of dollars. The x-axis represents market growth measured as the compound annual growth rate (CAGR) from 2019 through 2024. The y-axis represents the Gartner estimate for an operating profitability percentage for 2019" [2].

This is useful information for security providers that are considering which services to add. But it is the F-Secure view that large disparities within each segment show that knowing your local market will be more important.

MARKET OPPORTUNITY MAP FOR SECURITY AND RISK MANAGEMENT



Source: Gartner
Note: The bubble size represents 2024 worldwide security spending for each segment in millions of dollars.
CWPP = cloud workload protection platform; EPP = endpoint protection platform; IGA = identity governance and administration; IRM = integrated risk management; PAM = privileged account management; SIEM = security information and event management; SWG = secure web gateway
731517_C

In our view, these disparities also highlight that there are certain aspects of running a profitabile service that transcend segment.

WHAT MAKES A PROFITABLE MANAGED SECURITY SERVICE?

At F-Secure we work with over 1,000 partners and have supported many of them in building successful managed security businesses over the past decades. In addition to this we operate our own managed security service through the F-Secure Managed Detection & Response business unit.

Every business has unique characteristics and faces its own set of challenges. However, over the years we have observed certain features that the most successful and profitable have in common and that we also incorporate into our own operating model to achieve maximum efficiency.

These features fall into three broad categories: People, Process and Technology. Clearly there is a lot of overlap between these categories but nonetheless they provide a helpful framework for presenting the findings of our decades long research.

PEOPLE

We talk a lot about how technological advancement is transforming the cyber security industry, but the fact remains: We are a long way off technology replacing the need for investment in staff development and retention. However, best-in-class technology and the support that comes with it will go a long way towards augmenting and developing your in-house expertise.

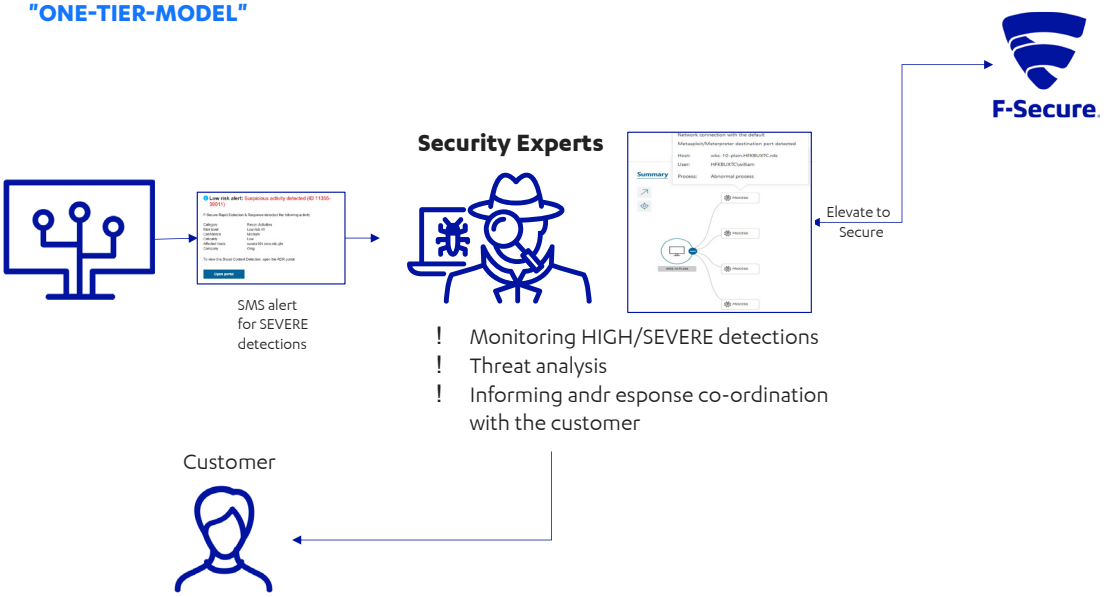
Hiring and retaining cybersecurity experts is still one of the biggest challenges that managed security providers face, because ultimately your people are your product. Here are our top four tips for hiring and retaining the best talent.

- **Make sure you have a sustainable strategy to recruit and grow.** Obviously getting the right talent now is important, but you always need to be prepared for people leaving and the knock-on effect this can have. In order to remain profitable you never want to be overstaffed, but as soon as people start leaving you need to replace them to avoid the service suffering. If the service suffers the job satisfaction of your remaining staff will follow and you can find yourself in a vicious circle.
- **Invest in staff development.** The best cybersecurity vendors will offer extensive online and offline training to ensure that their brand is associated with best-in-class service. Make use of these and take advantage of co-service models where appropriate to complement and eventually expand your own in-house expertise.
- **Build time-off and research time into your processes.** Threat response can be stimulating and rewarding work, but there's no denying the intensity and the toll that can take on your staff. At F-Secure we've adopted a four days on, four days off approach, and two out of those four days on are dedicated to research rather than front line response work. All of our threat hunters report that this research time is what they value most highly.

- **Think carefully before implementing tiers.** We don't have a tiered hierarchy for who responds to what at F-Secure and would advise thinking very carefully about implementing a tiered response system. Obviously, we still have junior and senior team members, but for us it works better if everyone gets experience responding to everything. On the other hand, if you're running a service that deals with a very high volume of low priority requests it can make sense, as long as its implemented carefully with the goal of avoiding alert fatigue and burnout firmly in mind.

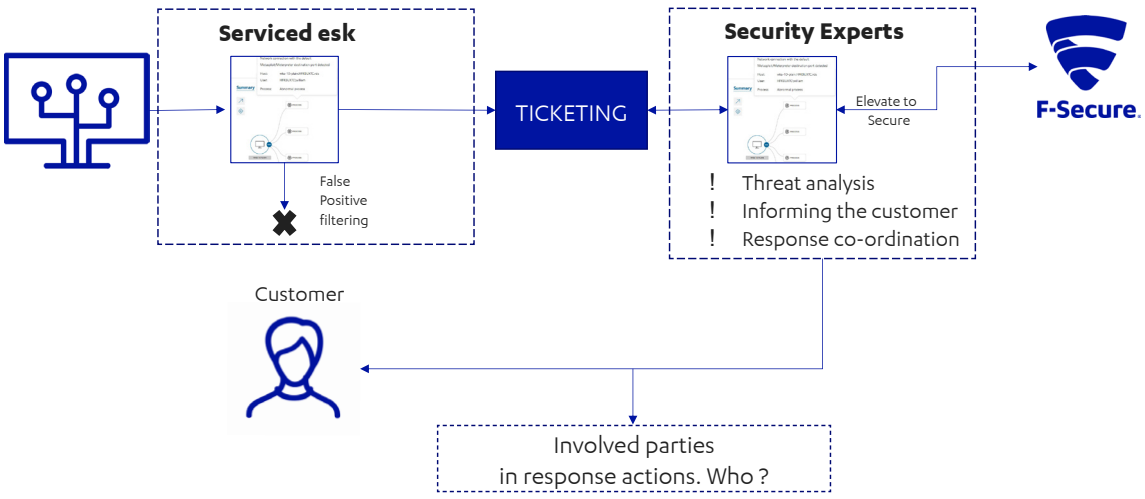
HOW DOES THE SERVICE PROCESS WORK?

"ONE-TIER-MODEL"



HOW DOES THE SERVICE PROCESS WORK?

"TWO-TIER-MODEL"



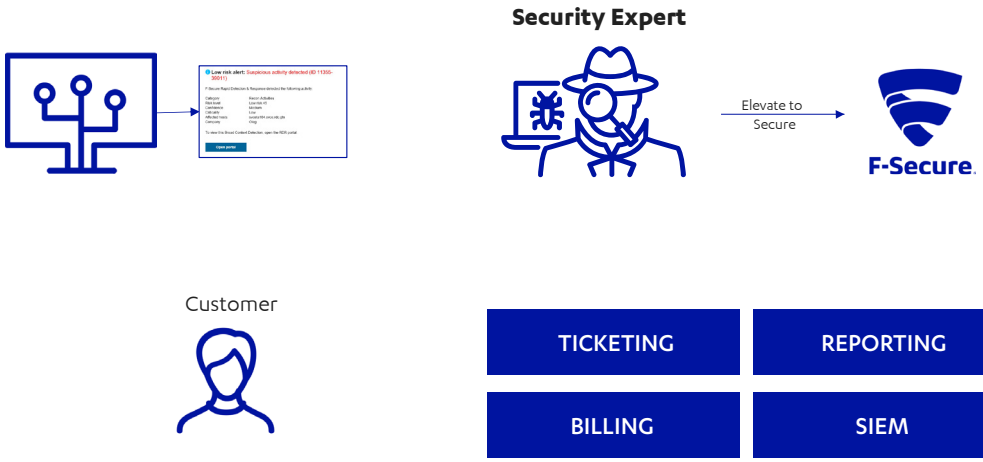
PROCESSES

Getting the right people might well be the most important aspect of building a profitable service but poorly defined processes will not only prevent these people from operating effectively, it will most likely prevent you from recruiting them in the first place.

In the next section we'll give some real-life examples of processes used by our partners, but here are the main principles we recommend you follow:

- **Ensure integration with any other services you offer.** The most important thing when adding a security service to your portfolio is making sure it is well integrated with everything else you offer, whether that's security services from other vendors or other IT or software services that your business provides.
- **Define your SLA.** Business hours SLA (8/9/10-5) is perfectly valid for many customers, possibly backed up by an automatic host isolation in the case of high severity detections. Alternatively - offering 24/7 makes sense if you already have same SLA level for other services you offer.
- **Schedule regular reports.** Reporting is important because it proves the value of the service to the customer. Even if there are no major incidents to report the client should be regularly updated or have access to a dashboard that shows them what the service is doing.
- **Define and document all your decisions.** Whatever you decide on, having well defined and documented processes for alerting the client and delivering remediation guidance is essential.

YOUR PROCESS FLOW



TECHNOLOGY

The third pillar of a profitable managed security service is the technology. Choosing the right technology will enable you to implement the processes that you want to with minimum effort from your staff.

In our experience these are the main things to consider to ensure the technology you choose helps you to maximize operational efficiency and ultimately profitability:

1. Quality of product

This might seem obvious but making sure you are using best-in-class solutions will use AI technology to filter out the noise and decrease the number of support cases, which increases operational efficiency and profitability in the long-term. Independent benchmarks such as AV TEST, Mitre ATT&CK® evaluations are useful sources for comparing vendors.

2. Centralized management system

At F-Secure we strongly believe that the future of cybersecurity is all-in-one solutions. However, that is not the current reality, so making sure that all your solutions can be integrated into one central management system is the next best thing. If your analysts have to split their focus across multiple management systems they are more likely to miss things.

3. User interface

For the same reason, good UI is essential. You need a product that is designed with MSSP analysts as their main target users. From one glance your service experts should know what to do and where to investigate.

4. Data sharing

In addition to choosing technology that can be managed centrally, it is important to choose technology that shares data with your other solutions. For example if you have Endpoint Protection, Vulnerability Management and Email Security solutions all running separately you are missing out on the detection power and efficiency that comes from combining the data they produce together.

5. Licensing options

Depending on your volumes you may benefit from the fixed costs of a long-term contract or the flexibility of a usage-based model. This is important to consider when choosing a vendor.

WHAT TO INCLUDE AND HOW TO RESOURCE IT?

The decision about what services to offer and how to run and resource them is obviously a highly individualized one. In our service design workshops we help partners think this through by looking at local market data, how many detections they can expect on average, their individual capabilities and other unique organizational characteristics.

This experience allows us to demonstrate some "model" process and resourcing designs, although what fits best is highly situational.

One of the first questions we ask is how far the service should go. Typically, we see partners offering three levels of service:

- **Technology management** - Managing basic operational tasks like adding and removing devices and installing updates.
- **Threat monitoring** – Actively monitoring for threats and vulnerabilities and advising the customer on how to address them.
- **Active response and remediation** – Fixing vulnerabilities and actively responding to threats.

Technology management is the lowest value add for the customer and likely the lowest margin business. Most of our successful partners offer something between threat monitoring and active response. However, it's often the first step a customer will take towards improving their security and can be an important service to offer.

Threat monitoring is easier to offer as a productized service since the value proposition is very clear and the scope of the service is easily defined. Active response is harder to define and the service promise and description have to be very clear on what specific response capabilities and/or actions are included.

We have developed a model for assisting our partners with calculating resourcing needs. It takes a range of factors into account including: the level of service offered, the number of detections the average full-time employee can handle per month, and the average number of detections that a specified number of hosts will generate in that period. We are happy to share the specifics of this with our partners.

WE ARE HERE TO HELP

The considerations highlighted above are just a few of the things that should be taken into account when building a new managed security service. But the good news is you are not on your own. F-Secure has decades of experience supporting its partners and has a lot of advice and expertise to share.

SERVICE DESIGN WORKSHOPS

Our service design workshops are designed to support partners that are considering adding new services with building a solid business case. During the workshops our experts will guide you through the steps and decisions that need to be taken to launch a profitable service.

Part of this workshop is introducing partners to our business case calculator designed to help MSSPs estimate their profit margin for different products and services and work out whether their volumes justify switching to a usage-based license.

The calculator takes a range of factors into account including technology costs, personnel and training costs, operational costs and other sales and marketing costs.

Key ingredients of a profitable managed security service

F-SECURE ELEMENTS

Our service design workshops are designed to support partners that are considering adding new services with building a solid business case. During the workshops our experts will guide you through the steps and decisions that need to be taken to launch a profitable service.

Part of this workshop is introducing partners to our business case calculator designed to help MSSPs estimate their profit margin for different products and services and work out whether their volumes justify switching to a usage-based license.

The calculator takes a range of factors into account including technology costs, personnel and training costs, operational costs and other sales and marketing costs.

Centralized management system

When we visited our partners we noticed that their analysts often had several different browser windows open and they were attempting to monitor a different product, through a different management system in each one. We realized there was no way that could be efficient, so we designed Elements to put all of our solutions into one centralized management system.

Comprehensive visibility

This lets your analyst put data from Endpoint Protection, Vulnerability Management and Email protection all together on one screen. Obviously this is instantly more efficient because it focuses their attention in one place, but beyond that it also gives them additional insight and context that simply did not exist before when the solutions were siloed.

Streamlined workflows

The operational efficiency that you gain from this technology enables entirely new ways of working, and ultimately will reduce your personnel costs. We have calculated that a simple detection is more than 10x quicker with Elements than with legacy solutions.

Elevate to F-Secure

F-Secure employs some of the best threat hunters in the industry to run its own managed security services and now with Elevate to F-Secure this expertise is available to our partners.

Not only can you be secure in the knowledge that you can refer your hardest cases to our elite cyber experts, but you can count on their expertise to inform and elevate your own in-house capabilities. We will give you a full incident report which helps you to build your own competences and be ready for similar events in the future.

WANT TO LEARN MORE?

If you want to learn more about anything you've read in this whitepaper please get in touch. Our experts will be happy to speak to you in more detail about how we can support you in building a profitable security service business.

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