22-Nov-2024

WithSecure Corp. (FSC1V.FI)

Investor Day

CORPORATE PARTICIPANTS

Laura Viita
Vice President Controlling, Investor Relations & Sustainability, WithSecure Corp.

Antti Koskela
President & Chief Executive Officer, WithSecure Corp.

Lasse Gerdt
Chief Customer Officer

Artturi Lehtiö
VP-Product & Portfolio Management

Tom Jansson
Chief Financial Officer, WithSecure Corp.

Juhana Autio
General Manager, VP-Cloud Protection, Salesforce

OTHER PARTICIPANTS

Felix Henriksson
Analyst, Nordea Bank Abp

Waltteri Rossi
Analyst, Danske Bank A/S (Finland)

Atte Riikola
Analyst, Inderes Oyj (Research Firm)

MANAGEMENT DISCUSSION SECTION

Laura Viita

Vice President Controlling, Investor Relations & Sustainability, WithSecure Corp.

Good morning. We are WithSecure and this is our Investor Day of 2024. My name is Laura Viita, I'm responsible for the Investor Relations in WithSecure and have the honor of wishing you all welcome and hosting this event today. We are today at Wood City, Helsinki, our new office. And this is actually the first time that we are welcoming our analysts and investors to this beautiful office that we find very inspiring ourselves.

So welcome to all of you who are here on site today. Also welcome if you are watching us over the live or recorded webcast. Great to have you with us today. It has been quite a ride since we last held a Capital Markets Day in June 2022. We have completed the demerger of F-Secure. We've had some ups and downs. We've launched new products. We have gone through some cost savings. We've had a sudden change of CEO. We've arranged some magnificent events. And most importantly, we have taken some important decisions of refocusing our strategy. Today, we are here to talk about why we focus on the mid-market, how we create value to the end customers through our network of partners, how we create value to the investors, and what it means to be a European cybersecurity company.

So today's agenda looks like this. After me, I'm welcoming our CEO, Antti, on stage. And he will go through what we do, how we do it, why we do it. And after Antti, our Chief Customer Officer, Lasse, will be on stage to talk about how we create value for our customers and partners.

After the coffee break, we will come back for the TED talk, which will be delivered by Artturi, our VP of Product and Portfolio Management. And after that, the obvious star of every Investor Day, our CFO, Tom. After that point,

everything will be elements company only. So whether we talk about ARR, revenue, EBITDA or other, it means the elements company.

But then after Tom, we will welcome on stage Juhana, who's the general manager and VP of the Cloud Protection for Salesforce, and he will share their latest news and what their plans are for the future.

After Antti's disclosing words, we will welcome all presenters back on stage for a Q&A session. So note down your questions or keep them in mind. We will have them answered at the end. If you are watching us over the live webcast, you can put in questions any time, I will take them up with the presenters at the end as part of the Q&A session.

So now with that, we are ready to move on. So I'm welcoming on stage the President and CEO of WithSecure, Antti Koskela.

Antti Koskela

President & Chief Executive Officer, WithSecure Corp.

So thank you, Laura, and great to have many people here.

So, thank you, Laura. And great to have many people here on site. And thank you, everybody over the line for joining as well.

So, my name is Antti Koskela, I'm the CEO of WithSecure. And I have a pleasure welcoming you for my part to this session. It's great to have you here.

I'll talk about why we do the things we do. I'll talk about what are the assumptions and the core beliefs underneath our strategy. And then, I'll dive deeper into our ideal customer profile in mid-market. What are their needs, why we have chosen that. And then, we end this first part by going through the four strategic pillars of WithSecure.

WithSecure is a purpose-driven company. So, we exist to build and sustain digital trust, confidence and equity. And with that purpose in mind, when we have designed our strategy, we base it on three core beliefs.

The first belief is that we believe the mid-market playbook is broken, and it's broken because the existing playbook is built for the needs of large enterprises who have built over the years more products, more technology, more controls, more everything. That has made them incrementally safer. But we have left behind the small to midsize companies without viable choices. So, our fundamental belief is that we need a new playbook for cybersecurity, and that's at the heart what WithSecure does.

Secondly, we need diversity and optionality. This current large enterprise cybersecurity environment is dominated by few, mainly North American cybersecurity players.

Meeting mid-market and small to midsize company requirements is a different policy ballgame. We need security outcomes that meet their needs. So, we believe we need diversity and optionality. We need genuine choice. And we need a European alternative for the digitally driven world. So, which secure aims to be the European flagship in cybersecurity for the digitally driven world worldwide and bring the European principles of privacy, respect and responsibility.

And finally, this is not just having the right products and technology. We believe addressing mid-market needs, it requires a platform of capabilities, not just product. So, we need to combine technology, artificial intelligence, and

human expertise for in one place. And that's what we do with the elements cloud. So, we're going to talk about that more during today.

And in this strategy round, we look until 2027, and by then our vision is to be the Europe's flagship in cybersecurity. So, many of you who have been listening to our talks recently, we have talked about a lot about the mid-market. And I would like to go through why we care so much about this segment. Why are they so important?

Growth and innovation in the world is very much driven by It's very much driven by the small and medium sized companies, especially here in Europe. And yet, they are the most underserved. And they are increasingly at risk in today's digital threat landscape. They are losing their digital confidence faster than the others like you see in this World Economic Forum chart. And when these companies start losing their trust in technology, losing their confidence in technology, they start falling behind. So that's what we want to solve.

At the same time, these cyber criminals, they are not losing confidence, and they operate at an industrial scale. Many of these criminal groups have incorporated actually into companies. They have CFO, HRs and structures in place to run their operations. And all of us, we have been advised what these actions from these criminal actors look like, that you are advised not to click on a file, not to click on a URL. But I wish it – world would be that easy.

So what these criminal companies do, they scan the entire Internet against all the many vulnerabilities we have in our digital footprint. And for them, it doesn't matter whether you are small, whether you are a large company. So we all possess valuable information, and we are often part of wider digital supply chains. And for WithSecure, solving this is a matter of fairness and equity. So we need to make sure that we bring minimum effective security for these companies so that the societies and these digital supply chains and the digital supply chains can thrive. And we need to play that level the playing field here.

So, looking then at the levelling the playing field, a European Union is driving a lot of good regulation in the area of cybersecurity and they have this levelling their playing field in mind. So, with the recent introduction of the needs to, which is Network and Information Security Direct the version 2. So, they brought many new industry sectors under this regulation. And overnight, 100,000 more companies came under this regulation.

So, what this regulation does, it increased the requirement for minimum effective security. So, a few things that we have in our platform of capabilities elements are required now by the law. That's a requirement to manage your digital risks proactively. That's a requirement to manage incidents properly. And it is complemented by bringing a personal responsibility for management in case of failure to comply. There are criminal consequences and also fines associated similar to GDPR.

But not only the regulation brought this many hefty security to the companies in scope, but also to the companies that provide products and services associated with these needs to regulated entities. So, this is quite much changing the environment.

So, we have found our sweet spot. Our sweet spot of customers, our shots that are overwhelmed, they are feeling overwhelmed, they are under-resourced, and they are underserved. They are typically 50,000 to 2,000 people inside the companies and they don't have security capability or knowledge in-house like large companies often would do. They realize they need to act either by wanting to be progressive or they are required to be progressive because of regulation.

And then these companies as they don't have security capability in-house, they prefer to trust a local partner to deliver the service for them. So we actually found some interesting statistics here. We look at the Eurostat 2022

report, and 68% of the companies buy security services from managed services provider or that provides the IT services or other services to them. It's a big number.

And we have been talking about how the playbook is different in the same report, only 40% of the large companies do the same because they want to build things in-house. They trust on their own ability to do things. Like what typically large banks would do, for instance, I think I know many of you work in those. So we think our sweet spot is increasing. It's increasing because this regulation brought hundred thousand new entities under the regulation. And also it's causing some of our existing customers needing to act. So we believe there's an opportunity to grow new customers and expand on existing ones. And lastly, we'll talk about how do we concretely do that together with our partners.

Mid-market playbook is broken and we need a new playbook. So, the creation of that playbook start by asking what security outcomes these companies need? So, we talk in SPHERE24 this year is that we researched 1,500 cybersecurity professionals advice, and we researched these companies. And their answers came in three categories. It was, they need resilience. They need trust and compliance. And then, they need efficiency. So, these are the security outcomes they want.

We also found, like we say in our sweet spot, these people are feeling, they are feeling overwhelmed. Not they don't often know what to do. Because they are underserved and understaffed. So, that's how these small companies, small and midsize companies often look like. Artturi will talk about that in his part, what's the reality we see in cybersecurity in the field?

So, what we have now done in WithSecure? So, we have launched a – the mid-market playbook, and we have built elements for it. So, the core of that one builds on the protection, detection and response strategy, and we complemented that in the recent Sphere launch with Identity Security, making it extended detection and response. So, that's the basis for your incident management. But we didn't stop there and we brought this proactive way to manage digital risks, exposure management into the mix, the very thing required now by these two. And we built these ones for the needs of the midmarket. And we have also the human expertise part here in the offer that we are able to simply by elevating a single problem to us co-monitoring the estate go all the way up to managed detection and response on Elements cloud. So that's what we have now and under the general availability and that's what something we also released back in SPHERE. And finally the efficiency so we have been doing machine learning for decades, but now we brought generative AI as an integral part of our Elements user experience is enabled to all our customers currently, and the ambition with that one is of course to bring the productivity. And that's something we very much look forward to developing further as we go with the road map. So we have now Elements for the mid-market playbook.

So I would like to end by summarizing what are our strategic choices. So we first focus in winning. We focus in winning the mid-market by providing them this minimum effective security. And we do that together with our partners serving them. Secondly we want to make an impact. We want to be the most trusted, respected and innovative cybersecurity vendor that is a European alternative for the digitally driven world. That's what we want to be. And then we will stand out by making the Elements cloud a platform of capabilities, not just products. So connecting these technologies, artificial intelligence and human expertise from one place.

And finally, we'll run this company with the precision and accuracy of a world-class company. And Tom will be sharing where we are in our transition to the SaaS company.

So with this one, I would like to close my part and Lasse will next talk about how do we win. Artturi will then talk about how do we stand out. And Tom will talk about how do we run, run this business. So thank you very much for listening for my part, and over to Lasse.

Lasse Gerdt

Chief Customer Officer

Thank you, Antti, and a very warm morning and welcome also from my behalf, people in the room, people also watching online. My morning started actually flying from London last night and being late for 4 hours. I landed in my hotel at 4 AM. So my excuse is if there is some visible effects of that one, but I had to create days in London as well, actually spending time with AWS and working on our partnership forward with them. And that's something I want to highlight as well today and how we are shaping our go-to-market strategy as WithSecure aligning what Antti was telling you. The mid-market being the European alternative as well as then moving forward with the strategy of the Elements platform and the capabilities it's giving us. I joined the company starting this year. In my role as a Chief Customer Officer, I'm obviously in charge of our global sales and partner organization, our revenue and customer operations.

I want to start with the customer value, a little bit different angle what Antti had, but I think still important to echo that one. Why are we aiming to this market segment especially is important to echo that one. Why are we aiming to this market segment especially is because of first of all, we are looking at the small companies. They are looking for no compromise security. These are usually customers and companies that drive most of the backbone of several economies. It's not just a European phenomenon. The same applies, for example, to one of our key markets, Japan.

These are companies that don't have usually IT at all or they have very little IT. And they struggle with just finding the right IT solution, not to mention then actually being capable of providing what is required for cybersecurity. For WithSecure and F-Secure in the past, this has been one of the sweet spots of the strategy, we have more than 140,000 customers still on the segment.

At the same time, these companies are actually the future mid-sized companies. Some of those companies do have an intention to grow, and our value proposition is to grow with them. And while we are providing those capabilities now much more from a platform perspective. It gives them the possibility to actually apply new elements in capabilities when the complexity of their environments and the requirements for cybersecurity are increasing.

In the middle, the mid-sized companies we talk about companies with from 200 to several thousands of employees. Usually they are already in an industry play. They have complexity and they write these systems. But it's also good to remember that Europe is one of the most outsourced markets in IT, meaning that for ages these companies have been trying to find an optimal way on what do they invest in their in-house resources as well as what they then provide – being provided. And as we have been learning and you will hear a little bit more about today, it is really now the moment in cybersecurity and especially the demand from the regulation, the likes of NIS2 that we see an increase of the cybersecurity budget for these type of companies across the markets.

And why are these important? First of all, obviously, we always look at the enterprise market quite often from an IT perspective. But if you just look at the IT spend across these sectors, it doesn't shy away. The market opportunity from that perspective is definitely there. The supply chains, if you look at it, and I already mentioned, if you look at many of the economies where WithSecure operates today on our global remit, more than 98% of the companies in these regions will fit into these categories, and the rest obviously in these than the bigger enterprises.

At the same time, these are the companies that contribute heavily on the TDPs and the backbones of these economies, as well as they employ up to 80% actually of the people and create most of the new positions and employment opportunities. This applies also to Finland actually. If you look at the statistics, we are very close to the same numbers.

What does that mean from a cybersecurity perspective is while the enterprises are becoming more secured, for somebody that is willing to cause harm, this is actually a way to attack the supply chain. And we have seen already in the news how easy it is actually to bring down something that is unprotected. When it might be smaller, it might have a bigger impact. And one of the key reasons for the European Union coming with NIS2 is also to make sure that we are securing by law the supply chains of our critical economy, the supplies to healthcare, of critical infrastructures and so forth which is not necessarily about big companies. It is about the supply chain.

So how is that impacting then? I'll go to market strategy and how we are evolving towards, first of all, how we organize ourselves and how we leverage the platform and the automation, bringing more options and capabilities for our customers depending on what they are willing to use and also how they are buying these solutions moving forward.

We have evidence, the cloud transformation that will continue and more and more the customers are looking for us as service providers for different type of technologies. So if you look at on the horizontal lines, we talk about these different customer segments with specific needs and we are approaching that with the elements platform.

How we are organized in our cells is more on the vertical axis. So throughout this year we have been implementing a global sales engine and a partner sales engine that fosters and automates a low touch and long tail partnerships. We have still more than 5,000 partners transacting with that one I'm not saying that all of them are in the business with us necessarily moving forward, but with that one, we keep the doors open and we want to help them to automate and digitalize and provide the platform for better scale.

This also helps us across the different markets to find, recruit and nurture new partnerships and that especially building the capability to serve the mid-market in the regions where we operate. Moving towards the right is the sweet spot of our partner strategy and we are moving from resell to cross-sell. We are moving from transactional license based channels to actually co-selling. And this has been the journey already for the couple of years. And we are putting more effort on it. So on the top you see the sweet spot for the mid-market on those partnerships where we are doubling down on managed service providers really value adding security, capable sellers and integrators and we are also building on the Cloud Marketplace offerings to provide more alternatives for our customers to deploy and deliver on the Elements platform.

On the latter part, we are also putting a lot of emphasis on the digital and automated journey. So, we have implemented a new global distributive strategy and we are taxing – we have more than 70 distributors today. That's quite a lot actually for the size of the company we have. We are addressing now five or six global and EMEA-based and Japan-based distributors building different capabilities and working really on the backbone that we are actually capable of putting scale in place.

In some markets, we continue to work with telecom operators and with them, we are obviously happy to provide a wider portfolio and more revenue per user as the Elements platform has been growing. Let's talk a minute about how we are addressing the top right corner. There are some key elements that have obviously changed in the couple of past years, one of them being our ability to serve the partners with the SaaS-based offering and the Elements platform. It gives them the opportunity to actually mix and match the different solutions and capabilities.

We are bringing more integrated practices and not just product-only. And we also supporting a variety of business models depending where the partner is willing to engage with the customers from consulting to delivering security solutions to providing managed services at scale.

In order to drive a faster time to market, we have a lot of partners that are still looking at how are they going to build their security practice.

security practice. And that's where the importance of the code security element comes in. It's not just providing the extended capabilities for 24/7 security. It is at the same time giving the partners possibility to ramp up practices quicker and starting gates on cybersecurity offerings on a faster pace. And this is in a very high demand as we speak.

Then, as I said, we are moving from reselling, which is a little bit always not that intimate to cold selling. We have pivoted our regional teams and strategy to work with the local set of hybrid partners that we really invest in for marketing, selling and securing. And in the past months, we have seen a great uptake on this motion, we are bringing more on the partner to sell. And the same time, we are actually approaching bigger customers and bigger deals on that approach.

And this is just based on the partner offering from the platform perspective. Our crew will dive deeper into the pieces of the technology and the capabilities that we provide. I wanted to, from a seller perspective, to open up a couple of things, why do we feel that the new platform strategy is playing in advance.

Number one is that is the solution tailoring, we used to have different products, different commercial models, different capabilities. Now, all that innovation coming into one platform and the partners can pick and choose what is the moment that they want to try. And we try this with the size model of operation. This, obviously, is just a simple thing, there is more readily available on the table because we – what we can sell for a customer together with a partner there is just absolutely more. And also our [indiscernible] 00:29:17 Bill and Tom will talk a little bit more about that one.

Co-Security Services has said it's not just extending the capabilities and skill sets. It's also the time to market and the solution. Cybersecurity never sleeps. The criminals never sleep. So, having a platform-based approach, cloud-native platform, we are driving innovation to the market on what's fast in the space and maybe in the past.

This also enables us to build on the digital experience and automation. So, first of all, I said distribution has evolved in the IT market quite a lot. It used to be built on big facilities and warehouses to stock, even for cybersecurity, the CDs and other media to actually let them be shipped to the customer premises. Now, we are digitalizing the whole end game and that provides some level of scale.

In the next year, we are providing the API support from our platforms to really integrate with some of the largest distributors in the market and to provide with secure elements on their platforms. And to support that, we have built up a global SMB sales engine that is helping and working alongside with these partners.

The digital experience prevails pretty much in the back end, especially when it comes to order, invoicing, those kind of processes. We have evolved also not just the product capabilities but also the platform, providing the partners a 360 view on how they are dealing and what they are selling to their customers, what are the capabilities from them to grow the business, but at the same time, having reports and capabilities so that they can have a constant dialogue with the customer, how are we doing with our security? How are we doing with our compliance? These are the biggest demands that we have today, and as Antti explained, with NIS-2, security is

coming aboard in sea level topic. They are in charge, by law, they are in charge. And with the platform we can provide, the data sources and capabilities for them to match the compliance requirements and report out.

And as I said to that last days with Amazon in London, we are bringing our Elements platform to the AWS global marketplace. We just actually recently also acquired the capability to start globally reselling and cross-selling with AWS across their ecosystem. We will talk this a little bit more in the beginning of next year. But what I was really, really happy about was the reaction from Amazon also for us being a European-based provider, providing our technology and services from Europe because they are also building on their storyline on the sovereignty of data, security, and cloud. And actually in their ecosystem, at the moment, we are the only player that can provide a European-only approach. And it's resonating extremely well with their customers and partners. We just need to execute still in that.

I want to close and to talk very briefly about what is the underlying fundament. Being the leading European alternative or the European security company requires us to be the most admired ecosystem for the cybersecurity as well. And that's why we are evolving our existing global partner program to address the different capabilities, commercial models, and scale models for our partners. It's all about delivering skills and capabilities. It's about delivering incentives and other capabilities so that our partners are doing a great business.

As I said, on the left-hand side, you'll see the structure of our program. These are stages of revenue growth, customer retention, other capabilities, and we will be launching those capabilities towards 2025, evolving towards 2027 with the revisited approach based on the feedback that we have been getting from the market and our partners.

On the top, we are building the specialized programs for MSPs and the like so that we are matching the capabilities and the commercial models to work with that one. We are really enabling our regional teams to work with the more strategic partners that are betting on us, and we have a more goal focused approach across marketing, co-building the solutions and co-selling, and presenting ourselves together at the customer's site.

This place on a new type of market place ecosystem, the SaaS capability is in the background, but we believe that this will be a key element of us driving forward. And just yesterday, I got the number that in the past two months we have been our partners, seeing our partners to certificate or certify more skilled people, both for the with secure technology as well as sales than ever before. So, we are really seeing good uptake on that side as partners are embracing the new platform approach and the broader portfolio.

I could talk for hours about this, but it's easier and maybe more interesting if I invite somebody that actually is working with us as a partner. And we have been actually co-creating a lot of things together with the company called Ictivity. And I would like to welcome Wilbert van Beek on the stage. He's the managing director of Ictivity, a Netherlands based company, which I think is one of those examples that we wanted to bring up to highlight what does a good partner look like and what does a good partnership look like.

So, we'll welcome, Wilbert, as well. Good to have you on stage.

Unverified Participant

Thanks for having me.

Unverified Participant

So, let's get started. Maybe the first question, obviously if you would like to introduce yourself and introduce activity.

Unverified Participant

Okay. My name is [indiscernible] 00:35:33. I'm the Managing Director of Activity. We are a Dutch MSP managed services provider, active in the markets for about 26 years and the last 15 years on managed services especially. We focus on the mid-market and for us the mid-market is somewhere in between 103,000 end users and about 60% of our customers are in the non-profit.

Unverified Participant

So with that one, can you elaborate a little bit the journey that you have had so far with F-Secure? I think you started with F-Secure.

Unverified Participant

We started I think about 14 or 15 years ago with F-Secure and we were – at first we were a system integrator. We evolved to a managed services provider. And for the last years, we're working – are working more intensively together with WithSecure to build our complete offering. And when you look at our company, security is a very important part but I can't do it by myself because I have about 10, 12 people on my SOC, but I can't deliver state of the art very free security services, 24/7 by my own. And I think also our company is evolving from a managed services party to – a provider to what's a services integrator. Because when I want to deliver best in class security services, I need more skilled professionals and I don't have them. And when I have them, I won't hold them in the company.

So I've got a team to do everything what needs to be done every hour, every day, every week, every month. But then I will want to be best in class I need a good service behind our team. And in our case that's with Secure because you don't only provide products to us but a complete solution offering. And I'm not capable of delivering best-in-class European. That's very important for our non-profit customers, a European service 24/7. So it helps us a lot to be secure. And I sleep better at night because we are a target as well as a services provider.

Unverified Participant

Yeah, very good. So if you turn that a little bit around, Netherlands is obviously a very competitive market, the very advanced market in terms of technology, technology adoption as well. Is there anything else that you would like to highlight from what other customers are after today, especially in the mid-sized?

Unverified Participant

In the mid-sized markets? I see two types of customers, those ones who are already outsourced parts of their IT. And those who didn't yet. But they will come in the next year, that's for sure. But they're not there yet. And the easiest ones are the ones that outsource the business because they're not into all the details of products. And they don't want point solutions. They want to get it done by us so we can make the choice of the products that we deliver and the service that we deliver.

And the other end, where the companies that do their own IT management, that's a little bit harder because then there are a lot of tech guys in the company involved and they try to opt for sim their own SOC and point solutions. And nowadays they still rely on a few tech guys that make the decisions. And there we have a, yeah, the playing field is a bit harder for us to get in there, but this do helps us because when I look at NIS2, it will have the most impact of the companies that don't have a strategy of outsourcing yet and it wakes up the board. And when I look at non-profit, the board is already waking up because they have to comply to several regulations for years and they tend to invest in security. When I look at the commercial companies, there's a lot to win on the outsourcing part, but for sure on the security path. So they will come in the next months, year, and they will go for a complete solution.

Unverified Participant

Yes. So we can always look at certain trends and capabilities. But I think what we appreciate with the partnership is you engage very early also to actually work with us to bring new solutions and capabilities to the market, especially when it comes to exposure management. Can you elaborate that [indiscernible] 00:40:12 a little bit?

Unverified Participant

Yeah. I think it's not even a year ago that we spoke about bundling the products, and especially around exposure management and identity protection and things like that, because there are a lot of products and services also in your catalog and when we looked at your vision of minimum effective security, we wanted to provide a minimum effective bundle towards our customers. And the bundle consists of a lot of WithSecure Solutions, go services, security services, but also we add our services to the bundle and we have a bundle with the [indiscernible] 00:40:51 service in there phishing services in there end exposure management from WithSecure. And that's why we bundle the products. We have a basic bundle and let's say a silver and a gold one. No one wants basic. So that's the good news. So everyone is going for the silver or the gold one. And the way we work together with you is that in a few months, we were able to create an effective bundle together. We did go selling on that co-marketing on that we had the cybertruck and visited a lot of customers.

And nowadays, we already have the first, I think, 10, 12 customers in place that bought the complete bundle in there. And we don't have to upsell every month and ask for extra euros. We created the bundle together, what really is good for the mid-market in the Netherlands.

A

Yes. And if you look at now, you know, a lot of things getting started, looking forward next year. These two you mentioned are the other driving forces for you in the market from your perspective as well as from the market perspective.

A

Yeah. These two is going to help us because when you click on your e-mail, it's full of security next to an AI. Now the good news is everything is in the solution the bundle we provide at the moment. AI is going to help us. It's going to help you as a managed services or for as a security services party, as a managed services party is going to help AI. And there is some pressure on pricing in the markets, our pricing as a managed services party. And the only way to respond to that is to have automation and tooling with AI underneath to it. And for me as a managed services provider, it becomes more and more important that I are less dependent on people and skills of people, but more on automation, AI and getting things done in a reliable way and at a cost effectively. And that will be our main target for 2025, 2026.

A

Yes. I think you're tapping into an important point that we see as well is these are also companies that are very quick in terms of show me the outcome, get me secured and so forth. There is a lot of market pivoting as well now to heavyweight services and consultancy type of things and other things from what we call the managed security service providers.

services and consultancy type of things and other things from what we call the managed security service providers.

A

Yeah.

A

How do you see that market versus the approach that you have taken?

A

I think they are going to have a hard time. And maybe they will still do business with the big ones, the enterprises in the market, with the mid-market, they want an out of the box solution, and fast to deploy and fast results and not a lot of hassle with it. And they're not waiting for a sim implementation or complex implementation with point solutions and connecting all the dots together because that's not cost effective and you're always behind the reality. So, I think the typical large security providers will – will get a hard time.

A

I know we didn't discuss this next question beforehand. But I will throw it in anyway. So, there is a lot of noise, obviously for the right reasons for IA and GenAI. And quite often there is an angle about that one that people are, you know, looking for from the security and compliance perspective. What can we do? What cannot we do? How about the data? We are saying now that it's actually one of the key tools to help to provide state-of-the-art cybersecurity and automation. How do you see the markets reacting on that?

A

I don't think when you look at security, we should talk too much about AI and things like that. We have to deliver a service, and we will use underneath AI technology to make it less complex for us and cost effective for us. And we don't, should talk to the customer about all the AI stuff and things like that. We deliver a cost effective service and that's AI is underneath, but not, I don't discuss that with the customer because AI is going to help us in the future. But there's also a bit of fear because AI is very big and we talk a lot about fear in the press and in the market and not on to less. I think we look at the upside and it's more or less the unknown why people are maybe a little bit afraid of AI, but I think we shouldn't talk about AI, but just use it the outcome. That's what counts.

Unverified Participant

Thank you. We are entering the time of end of the year, Christmas, New Year's. All those things coming if you would have two wishes with secure for next year. What would that be?

Unverified Participant

Not for sure. Please keep doing what you are doing at the moment, because the way we work together is an example for a lot of other vendors in the markets. And that's not because I'm here at this moment, but it's really true. I can really say that the partnership is for a lot of value for our company, so please keep doing that. And the way we co-create solutions, yeah, is perfect for us. And please keep up to the security market and keep us secure and keep also our customers secure. But I'm very satisfied in the way we are working together. So I don't have a specific wish, please keep doing what you're doing, because you're doing very well.

Fair enough. All right. Thank you so much, Wilbert.

Unverified Participant

Thank you, son. And thanks for being with us. I think we are a little bit ahead of time.

Unverified Participant

I'll come to the stage. So actually, if you have questions for Wilbert, we could take them up right now.

Unverified Participant

Yeah. No problem.

Unverified Participant

Since we have for once, we have a real partner with us today. And also, if you have questions for Wilbert, please post them on the webcast. We will take them up.

Unverified Participant

Feel free. There we go.

Q

Yeah. It's Kimmo Stenvall from OP Markets. One question on the partner channel or the channel in general, that how crowded is this space? Do you offer any other partner services also besides...

A

Competitors of WithSecure, you mean? Yeah. How do I say this nicely? Fortunately, sometimes, I have to deliver Microsoft. But that's not our first choice. Our first choice, because I want to be the best player in the market together with WithSecure. But sometimes I need to adapt to Microsoft. And that's in the case when there's a specific bundle bought by a customer from Microsoft and there are security in there. And we try to get them through WithSecure. But they already paid for the Microsoft part. So, that's where we sometimes have a hard time.

But I think when I look at our landscape, about 90% of our customers are standardized on the WithSecure portfolio and about 10% on the Microsoft. But I don't deliver any other products because I think a customer should ask me a functional question about the outcome, and that's for our products. And I often tell my customers, when you have a new, get a new kitchen in your house, you don't ask the supplier, are you going to mount it with a Black and Decker or Makita? Because it's my profession to deliver a secure service. And we do that with WithSecure. So, in many cases, we can make the choice for the customer.

Q

Okay. Thank you.

Q

Hi. It's Atte Riikola from Inderes. I would continue on the Microsoft topic basically because we have seen that Microsoft has been growing very fast in the cybersecurity market. So, how do you see their offering from the partners? When are they able to offer a better solution or wider solution with lower price or how they look at the market from your point of view?

A

Microsoft is doing well and their products are not bad. So that's the good news. But it's – for us as a MSP, it's quite hard to partner with Microsoft. And Microsoft provides us with a one size fits all solution for the enterprise and for the small business, medium business, everything. And that means you hit everything for a bit and they

don't deliver the cosecurity services as with Securitas. So I should build my own stack with the Microsoft products, and that's not what I'd prefer because I need to match people in there to deliver a 24/7 good security service. That's why we opt for the WithSecure. And the Microsoft products are not bad but it's more time-consuming to deliver a good service.

Q

All right. Thanks. That's helpful.

Felix Henriksson
Analyst, Nordea Bank Abp

Q

Hi. Felix Henriksson from Nordea. We touched the Microsoft quite a bit, but what do you think – in your view, what differentiates WithSecure from the sort of endpoint protection market leaders like CrowdStrike and SentinelOne? I'm sure they also have like some good – pretty good service capability and that type of stuff but...

A

Yeah. Those are also good players in the markets, global players. That's a difference. And as I just mentioned, about 60%, 65% of my turnover comes from nonprofit and healthcare and local government. And I think a few years ago, they didn't mind where does the product come from. And nowadays, they are more and more looking at a sovereign or European cloud but also European solutions. And when you look towards privacy and things like that, it's a USB that we can sell a European solution, especially on the security part.

So, that works for us.

And yeah, I think that's one of the main advantages. But there are a lot of players in the field and I think when you look at the mid-market and especially the European mid-market, you have to make a decent choice and you can bet on all the players in the market. And yeah, we feel very comfortable towards WithSecure and also the vision they have connects to our company and also the focus on the mid-market connects very well and that's why we made the choice years ago for the WithSecure suite. Yeah.

Q

That's clear. And then on NIS2, I think it's interesting to hear you talk about that bundle that you have with the combination of your own solutions as well as the way to grow stuff. But how would you – how already are your end customers for NIS2 to at this point and what specifically in the WithSecure portfolio addresses the need for minimum viable security?

A

Yeah. And how are ready are my customers? Not ready enough yet. And the pressure from NIS2 helps, especially as I mentioned, the commercials are not that security aware yet. They rely on a few tech guys in the company and – but now, it opens the door to the sea level. Then, we can have the right discussion about security, where it should be. And so that helps. And when you look at the bundles we created together with WithSecure is

when you look at exposure management, a lot of response detection action you should take, logging that should be done. What is part of NIS2 is in the solution they provide.

On the other end, we add like cyber awareness training programs from our end to the bundle and we add a CISO as a service because a lot of my customers our end to the bundle and we add a CSO as a service, because a lot of my customers are not big enough to have a CSO in place, 40 hours a week, and when they have one, they're going to lose him in a few months. And that's why we provide CSO as a service for one two days a week at the beginning, and then we maintain the NIS2 compliancy for the customer. So, we bundle our services and we secure offering together to be and to stay NIS2 compliant and we address that on the right level in the in the customer organization.

Q

Got it. Thanks for the presentation.

Jaakko Tyrväinen

Q

Jaakko Tyrväinen from SEB. I will continue on that, on NIS. Are you already seeing the demand boosts coming from this directive and, or have you already seen that or are you expecting to see that? And could you elaborate a bit on there on the magnitude that you are expecting to, it boost your demand?

A

We see a little demand from the market and we have now some sea level trainings in place and we're really working on that. And I think the big demand will come at the beginning of 2025 because it was, in the Netherlands, it was postponed for about seven or eight months again. So the pressure went down a bit. But we see demand growing at this moment. And I think that the real outcome work and business will come at the beginning of 2025 because they have to be ready by next summer.

A

Yeah.

Q

Good. Thanks.

A

Welcome.

Unverified Participant

All right.

Unverified Participant

So, thank you, Lasse. Thank you, Wilbert.

Unverified Participant

You're welcome.

Unverified Participant

It was great to have you here and especially for a headquarter girl like me. You know, it's so inspiring to hear what's and especially for a headquarter girl like me, you know, it's so inspiring to hear what's actually happening in the real life so thank you.

Unverified Participant

Thank you, the Netherlands.

Unverified Participant

Thank you.

Unverified Participant

Thank you.

Unverified Participant

So next on the agenda is coffee break so we will be back at 10:20 Finnish time so 20 past the hour. If you are on another time zone and then continue with our tech talk. The webcast will go on break as well. Thank you.

[Break] 00:55:33- [Break] (01:04:52-01:06:55) [Break] (01:12:44-01:14:45) [Break] (01:14:44 – 01:16:44]

Laura Viita

Vice President Controlling, Investor Relations & Sustainability, WithSecure Corp.

Welcome back to the WithSecure Investor Day. Next, I'm welcoming to the stage Artturi Lehtiö, our VP of Product and Portfolio Management.

Artturi Lehtiö

VP-Product & Portfolio Management

Thanks, Laura. Hi, everyone. Hopefully, you all had a good coffee break both here and also online. I am Artturi Lehtiö. I'm responsible for Product and Portfolio Management here at WithSecure. Before the break, you heard Antti explain how the cybersecurity playbook for the midmarket is broken. He talked about those overwhelmed, underserved and under-resourced midsized companies, those CISOs and CIOs and IT managers, who are expected to deliver the same security outcomes as their Fortune 500 colleagues, but with a fraction of the budget and a fraction of the resources. They truly are overwhelmed, underserved and under-resourced. And they need to work with trusted partners who can help them with the capabilities they need for a minimum effective security.

And so we've designed our portfolio of software and services really around a strategy of three pillars. Firstly, it's a portfolio of software and services, a portfolio of capabilities that are the fundamental building blocks for our partners, cybersecurity business. Secondly, it's about enabling both us and our partners to do good business. It needs to be efficient, needs to be effective. It needs to be scalable. And ultimately, it needs to be profitable for both us and our partners. And thirdly, it's about enabling our partners to stay at the cutting edge of cybersecurity, enabling them to stay at the forefront of both what customers are asking for and what new things the threat actors are coming up with.

These midsize companies are overwhelmed. They're underresourced, they're underserved. And at the same time, they're being bombarded with best practices. While well intentioned, these best practices are often far detached from their reality. Best practices like zero trust, it's a great idea that by default you shouldn't trust anything even if it's on your IT network, that every user, every device, every service should be separately authorized. It's a great best practice and highly recommended. Zero trust is generally considered to have been invented by Google for their own internal cybersecurity needs.

But in practice, zero trust is very complicated to do right, and Google is not your typical midsize company. The reality is most SMBs aren't even using multifactor authentication. Us, for example, here in Finland might take that a bit for granted. We're used to multifactor authentication in our everyday lives. We're used to multifactor authentication. For example, when logging into online banking, it's been there for over a decade. But not everywhere, not even today, not even in Europe. Two-thirds of SMBs haven't yet found the time and resources to even implement multifactor authentication. So, telling them what they really need is zero trust. That's like telling someone who's trying to buy new shoes that what they really need is a BMW.

On the endpoint, we've been talking of extended detection and response for over five years. The idea that it's not enough to just prevent on endpoints, but that also you need to expand to detect and respond across endpoints and also cloud and identities. At the same time, reality is less than half of companies in Europe even have the capability to detect on endpoints. Never mind extending that across cloud and identity.

Our network and data centers. We've been talking about cloud. We've been talking about hyperscalers like AWS and Azure and Google Cloud. We've been talking about Cloud Native for over a decade. Reality is, 45% of EU companies report buying cloud computing services delivered over the Internet. Over half of the companies in Europe don't yet use software as a service. Over half the companies in Europe don't yet use their browser for e-mail or use their browser for productivity software, or use file sharing over the internet. They don't use Office 365 or Google Docs or Dropbox, things we might take for granted. And it's considered best practice to regularly validate your cybersecurity approach with breach and attack simulation and red teaming exercises, so you know where your weaknesses are and how to prioritize those. Reality is barely a third of companies in Europe managed to do some security testing how to prioritize those. Realities, barely a third of companies in Europe managed to do some security testing in the first place. Now, NIS2 will dramatically accelerate that, but it's only a starting point. It

used to be enough for a minimum effective security for and SME to have an IT manager or systems administrator working as a part-time cybersecurity manager. And then maybe endpoint protection on your corporate devices.

Today, that's no longer enough in today's world, driven by both compliance requirements like NIS2 and driven by the expanding digital attack surface. In today's world, minimum effective security for mid-sized companies is at least their ability to protect, detect and respond on endpoints for security. Exposure management so you know where your weaknesses are and how to prioritize those. And either a full time cybersecurity person or more likely working with a trusted partner who takes care of that for you.

We see this in our own customer base as well. Most of our customers, especially our long time customers, are still using only endpoint protection, but increasingly both new and existing customers are expanding that to detection and response are expanding that across their end points, their code and their identities.

They are turning to augment with additional software like exposure management and our services, like managed detection and response. We firmly believe that tomorrow, even SMEs will need to be able to protect, detect and respond across endpoint and cloud and identities and their collaboration and workspace solutions. They will need to understand the risks and exposures, whether driven directly by compliance or because their own customers are demanding that from them. And usually they will need to augment with services from a trusted partner. That's why we've designed our elements cloud offering, around those fundamental building blocks of that middle market cybersecurity playbook.

We believe that exposure management and extended detection and response are those fundamental capabilities of minimum effective security. At the same time, most of our customers lack the skills or the resources to do everything themselves. And even our partners struggle with the cybersecurity skills shortage. They need to turn to someone who can help them augment. That's why co-security services is so important. It's a key add-on for our software, but it's a true difference maker for our partners, and we've designed our co-security services offering so that our partners and end customers can get just the right amount of augmentation that they need.

If they have their own security operations, they can turn to elevate our unique paper use on-demand security assistance. They'll get our threat hunters, our security experts, giving them that crucial second opinion or that additional insight. But in today's world, most companies, they don't come to the office at 9:00 in the morning and then switch on their computers, and then at 5:00 they shut down all their computers when they go home. In today's world, people work flexible hours, flexible locations. In today's world, it's more 24/7.

And for a lot of our partners, they don't have the scale, they don't have the resources for their own 24/7 by 365 security operations. And often that's limiting their growth, their customers are demanding that 24/7. And again, we can help with, for example, call monitoring. We can either handle the 24/7 for them or we can handle out-of-office hours co-monitoring. We can be there in the evenings and the weekends for them. That way, our partners can focus on acquiring more business for both them and us. And one day, if they reach that scale where it makes sense for them to bring it in-house, that's wonderful. They've achieved that scale on the Elements cloud software. We're more than happy to let them move that in-house and continue to grow their business on Elements software and grow their revenue with us.

We have a truly unique and differentiated approach in this competed market. There are the big three [indiscernible] 01:31:28 players: Palo Alto Networks, CrowdStrike, Microsoft. They're trying to build that one platform to rule them all. They're trying to build that one platform for the enterprise, but it only works for an enterprise who can manage with that complexity and can have the required resources for it. It's a one size fits all solution built for enterprise needs. And then there are the product focused specialists for example, Bitdefender.

They focus mainly on enterprise, sometimes the upper end of the mid-market. Some of them are former point solutions, trying to become platforms like Rapid7 or Qualisource, SentinelOne.

Some of them are former platforms relegated to competing legacy niches like [ph] Credex 01:32:23 or Sophos or ESET. But no one else is focusing on building a platform for the midsize company Cybersecurity Playbook. We have a unique approach, a differentiated platform for the midsize playbook, not an enterprise playbook, not an assemble it yourself set of point solutions, a unique platform for the midsized cybersecurity playbook and from a truly European vendor.

So now that you've gotten an overview of what we do, let's dive a bit deeper into how we do things differently.

Earlier this year, we launched Elements Exposure Management as a completely new area of our offering, enabling our partners to expand their security business and enabling our partners to be ahead of the curve when it comes to compliance requirements for their end customers. It's also about enabling our partners to bring closer together their security business with their broader IT business, because most of our partners, they aren't just in the security business. Their business is IT and we need to be there to enable them to do good business overall. Exposure management is fundamentally about simulating how attacks would actually happen and using that to help prioritize. It's fundamentally a risk management tool. It brings visibility and prioritization into risks. We built our exposure management around our unique path and pending heuristic attack path engine. We don't just look at the list of vulnerabilities, our attack path engine things like a real attacker would think. It all start from how would an attacker gain access. Maybe there is some device open to the internet then that device is running outdated software and there is a vulnerability. Maybe. Maybe not. For a real attacker it's just as interesting. Maybe one of your users has been – one of your employees has been using the same password in their personal life and at work and that password has been leaked. Maybe instead of credentials or using them for one of your employees has previously been leaked online. A real attacker would just use those to walk in through the digital front door. And that's how our attack path engine starts. And then, like a real attacker, they'll think, how can I gain the next step? How do I get from the starting point to that next step, and that next step, and that next step like a real attacker would? And this approach enables us to not just find obvious problems, but also the non-obvious problems and then prioritize those for our partners and customers based on what a real attacker would do.

But staying at the cutting edge isn't just about product innovation. It's also about keeping up with the threat landscape. Today, stolen credentials, stolen usernames and passwords are the single most common entry point in data breaches. And those data breaches are the most resource consuming, the most expensive to fix. In today's world, identities are crucial.

Earlier this year, we also launched Elements Identity Security, really taking our extended detection and response, making it more competitive, ensuring it fulfills today's needs. In today's cloud-based and connected world, increasingly, work doesn't happen on devices. Work happens in the cloud services and applications you're using, and breaches happen in those cloud services and applications where identity is key.

We've also continued to bring new technological advances. We brought large language models, LLMs or so-called generative AI, into Elements Security Center. Now, we've been doing machine learning, we've been using machine learning in our products for almost two decades. We launched the first machine learning-based protection capabilities in 2006. But for the first time, our customers are able to so directly interact with the AI, directly see the output of the AI.

Luminen already has many skills. It can summarize what's going on in your IT environment, and it will summarize it like an actual human would in simple human understandable terms. It can also make recommendations. It's like

having WithSecure's threat hunters and WithSecure's security experts always at the fingertips of our partners and our customers but with the scalability of software, not people. It's really about both keeping our partners and customers on the cutting edge, but also enabling both us and our partners to work more efficiently, upskilling the IT specialists and security teams at our partners, enabling us and our partners to do good business.

We continue to differentiate, we continue to bring new technological advances so that our partners stay at the cutting edge. And this is something we are also consistently getting recognized for. In this very competed industry, we are regularly recognized as one of, if not the leading provider, especially in our strategic focus. My favorite example of this is Gardner's latest EPP magic quadrant where, again, we were included on a very short list of vendors in a large industry.

But more importantly, Gartner's biggest critique. Their biggest criticism, their biggest weakness that they identified for us was, and I quote, most of the vendors customers are in Europe. How is that a weakness? That's exactly our strategic focus. So, I take it as a compliment that if that's the biggest criticism Gartner can come up with, then I think we're doing things quite well.

So, summing it up, we have a unique differentiated portfolio of products and services, a portfolio of capabilities that are the building blocks for our partners, security business and the building blocks for our customers to build that midsize cybersecurity playbook. And we enable us and our partners to do good, profitable business. And we keep our partners and customers at the cutting edge, so that they don't need to worry about falling behind. They don't need to worry about suddenly being uncompetitive. They don't need to worry about falling behind the threat landscape and the threat actors because WithSecure keeps them at the cutting edge.

That's how we stand out. And now there's just two questions remaining. How do we run this business with the efficiency and precision of a world-class SaaS company? And just how good and profitable can that business be? So, with those, I'll hand you over to our CFO, Tom Jansson.

Tom Jansson

Chief Financial Officer, WithSecure Corp.

Thank you, Artturi. It's always great to be introduced as a CFO when there's mention of profit. So, thank you very much. But my name is Tom Jansson, I'm the chief financial officer for WithSecure. And I will talk a little bit about how our updated strategy will take us to the targets that we have set ourselves in terms of market and earnings logic and so on.

So, hopefully we can provide you a roadmap on how to get to the targets that we are in, in terms of our ambition for the next three years.

But let's start first with our – what we want to become in the next few years. So as we launched yesterday to the market, we want to become a rule of 30 plus in 2027. And that means that minimum in 2027, we want to be a rule of 30 company. For those who this expression might not be familiar, the rule of something works the way that you count the revenue growth and the your EBITDA percentage of revenue and combine them together, count them together. That's how you come to a rule of something. For in our case, we are targeting rule of 30 plus, and our new strategy, our updated strategy will take us there.

But let's spend a little bit of time first, kind of where we are from a starting point of perspective. So here, you can see the longer term view of how this company, has Elements company has evolved and transformed to a cloud-based SaaS company. You can see that when we started the journey pretty much in 2020, the Elements Cloud and the on-premise was pretty similar sized. Since then we have evolved and the cloud side has grown exactly as

we have planned, and that's where we also see our future. The on-premise have been planned to decline and that will continue to decline in the future. Our future is in the cloud and our customers' and partners' future are in the cloud. Of course, we are not forgetting those who still want to use an on-premise, but our future still will be on the cloud side of this company.

Then if we look a little bit and I would first like pay attention to the second bar from the left, which is saying 81.8, which is our cloud-based ARR at the end of Q3. Here, we have opened it up into two categories, the managed services and co-security as well as the Elements Cloud software. And then the first bar on the left is the comparison 12 months ago. If we start with the Elements Cloud software, you can see that it's growing quite nicely, a little over 16% year-over-year.

The gross margin is around 87%. So it's a decent software gross margin. The top 10 partners in this category represents about €13.2 million ARR. Of course, behind them there's a number of end customers. So our total number of end customers in the users in the Elements Cloud software is around – a little over 140,000. So in some cases, there is quite small revenue streams.

But the net revenue retention, meaning we are developing our current customers quite nicely. And that at the moment is 110%. Of course, we strive for more. But already our starting point is decent, I would say, over the next three years, our aim is to cross-sell, upsell to the existing customers that we have already. And we will talk about that a little bit later.

Of course, we also want to win new customers, as you have heard today. Important is also that we continue to manage churn. And one of our key strategic initiatives also is customer success going forward and automation, optimizing the digital sales channel. Those are very – also very important ingredients in this category.

Then if you look at the managed services and call security, Historically managed services has been quite dominated by a counter set solution. However, as we have heard today, we are bringing in Elements, MDR and a lot of core security capabilities into this. But at Q3 this year, our gross margin here is 55% – 59% at the moment. Of course, that means that there is a labor component into this revenue stream. Our top 10 customers here represents about $7.8 million ARR at this point. So a little bit more customer concentration in the managed services area.

A number of customers today is around 270. And here you can see also that we have, as we have discussed before, have had some churn with the large enterprise customers who have moved on to their point solutions and bigger enterprise solutions, as has been previously mentioned here, also as an alternative for this. At the same time, though, as you can see, the total ARR development has been flattish, so we have and we will continue to focus our many services offering to mid-market customers. And we have seen already some initial traction quite well on that in terms of the last 12 to 18 months. But of course, there has been a little bit of delay in terms of getting this to growth as we have had some bigger churn enterprise churn customers. But we have at the same time, we are rapidly increasing our number of our co-security customers. And as we have heard, that is one of our focus areas in the next three years. So we will see it is also turning into growth over the next three years.

Then, if we move a little bit to the market size and what is the kind of potential for WithSecure going forward. First you can see that the XDR market, this is based on Gartner information based on Gartner information will continue to grow double digit.

Then the exposure management here, I want to emphasize that this current market is a lot about vulnerability by incident response and attack surface management. So, the exposure management that we have been talking

about is a new market that is developing underneath this number. And that, of course, will rapidly grow as the way we see it and Gartner see it over the next three years. So, we – the expectation is to see the market grow close to 20% over the next three years. And then we will continue to see a strong market growth in the MDR area.

We have also here given you a little bit of flavor on our estimate of what is the total addressable market for WithSecure already today. And you can see the breakdown of it to different – the different areas in terms of market. And, today, that already comes to about $7.5 billion for the product portfolio that we are addressing in the market.

Then we have talked a lot about Europe. We, of course, as you have also heard, we are going to deliver the Europe [indiscernible] 01:47:41 Way to the world. So, we don't limit ourselves to Europe only. But if you look at only the European opportunity and where we stand and what it looks like today, if we start with the left side of the market segment, today, based on Eurostat, there is about 36 million small customers in Europe only. 36 million. That's a pretty staggering amount – number of companies. And our position there today is we have around 95,000 customers That's a pretty staggering amount, number of companies. And our position there today is we have around 95,000 customers in this segment. So, of course, that is a quite a small amount in terms of the total for us, so which represents about 0.3% in terms of market share.

However, this is a very also, going forward, a very important segment for us in terms of developing and key items in this market segment for us is automation, efficient business models, and good customer automated customer success. So, it's not that we are well, our sweet spot and our focused key customers in different segments. This will continue to be an important segment for us also in the future through partners and so on. So, we will see also growth in this area.

Then if we move up a little bit in terms of the set of employees of the companies. In the category of 50,000 to 250,000 today, there's about 275,000 customers in Europe. There, they already have 8,800 customers approximately in our being our customers, which represents about 3.2% of the total market today. And then over 250 employee companies in Europe, there's about 58,000 companies today. Out of those, about 3,300 companies are already today our customers. So, in this key segment for us, which is exactly not the 200 to 2,000, but very close, we already have a quite solid base to work from with our partners going forward.

And we expect this to accelerate the growth in all of these areas.

Then if we look just in the key customer segment today and looking at how many modules our current customers are actually using for us in our outlook. So two modules, 29%. Many times it's EDR, EPP, and so on. But there's also different variations as we heard. The three modules about 10% today and then four modules are more only about 4% as of today. So there's a huge upside also for us to accelerate our growth through just selling to our existing customer base and execute so to say, land and expand strategies that we have been doing already for a while. But of course, a key point for us is also to win new customers together with our partners in this segment. And why we say this is a key segment for us is, of course, as you saw from Artturi's presentation, they are in most need of the complete portfolio that we have.

And if we look at then what is our earnings logic and how do we get our share of the revenue from these customers, we can see it here where we have tried to demonstrate to you approximately how this works from a earnings logic point of view for us. We haven't given you the specific numbers because they vary very much in terms of market segment and customer. So we got – and average would give – not give you a good representation of how much we can earn on a different modules. But as you can see, if you start from the traditional where we are coming from in terms of the elements endpoint, if we had a EDR that usually is about 3X

to our customer value Then if we look at the Elements collaboration protection, adding that, that's another 1x. And then when we move to the newer portfolio items, then we're already talking about 9x and 12x in terms of our earnings potential and earnings logic, how we are monetizing our portfolio with our customers. So there is a significant upside from cross-selling and selling to the full portfolio to our customers.

Then if you move up a little bit on to our company level and what is our ambitions in terms of the next three years when we run a efficient SaaS company. Today, our gross margins is around 80%, which is an okay-ish percentage, where we are today. But of course, we expect this to continue to evolve and we will more and more be a software company-based gross margin. Therefore, we see that in the next three years, we are going to be somewhere around between 80% and 85% in terms of our gross margin in the future.

Sales and marketing today is around 36% at the Q3. We see a lot of opportunity here in terms of efficiency, scaling effect, and working with our partners as we are accelerating our growth. We're probably going to – our ambition is to be around 30% or so in terms of our sales and marketing spend in the future.

R&D, as you heard, we are focusing on R&D even more.

We are focusing R&D even more. I think on the whole picture, we have a pretty complete portfolio today on a high level. However, we, of course, need to continue to invest in capabilities, making sure that we are up to date with our portfolio and so on. But we will see a focused effect also on our R&D spend going forward. So our ambition is to run the company in the future between around 25% of revenue in terms of R&D spend.

Then on the G&A, we see that scaling with the growth very much so we expect that to be continue to have a lean G&A and also in the future. And today, we are at 11%. So 10% and a few percentage points. Hopefully, we can even improve that in the best case. With this combination and the double-digit growth that we are expecting over the next three years, we expect also to make the rule of 30 plus that we have guided yesterday also to the market and launching today.

So if we sum up our target and how we're going to run this company efficiently. So of course, an efficient, SaaS business models, EBITDA, of course, thinking about the different segments and how we serve them, as you also heard from Lasse. But we see a lot of improvement in this area over the next three years, and that's what we're going to do.

Automation. Efficient business models are key things here. As mentioned, we are also going to spend – scale the sales and marketing spend. We see that the way to be scaling quite nicely over the next three years. And then a focused R&D to the current portfolio on its capabilities. We will see an effect of that as well.

and a Lean G&A. Today, we are at 8% in terms of rule of eight. And then the other part that we, of course, will want to do is accelerate our growth. That will come, as you heard from new customers, cross-sell and upsell some new capabilities, partner development, very important going forward, as you heard from Lasse and customer's success is another key area where we are going to get growth through improved NRR and so on. With this, we will decisively take this company to a company of rule of 30 plus by 2027.

With that, I think we'll end the Elements part and I will call Laura back to the stage. Thank you.

Laura Viita

Vice President Controlling, Investor Relations & Sustainability, WithSecure Corp.

Thank you, Tom and Artturi. So up to this point, it was all about Elements company. Now, we will hop to another world for a while and look at our cloud protection for Salesforce business, which has been, as you know, under a strategic review since the end of last year. So I'm inviting Juhana Autio who's General Manager and VP for Cloud Protection for Salesforce on stage.

Juhana Autio

General Manager, VP-Cloud Protection, Salesforce

Thank you, Laura. So hello, everybody in the room and online. So my name is Juhana Autio, General Manager of Cloud Protection for Salesforce. So today, I'm going to talk about protecting Salesforce environments and why we find this to be a very, very interesting area. This are probably a bit less known business area in WithSecure. So hopefully, we can open this up a bit more for you guys today.

One of the biggest transitions in the One of the biggest transitions in the IT world today is the move to SaaS and cloud platforms. So, I mean, the biggest ones are obviously AWS, Office 365 and Salesforce. But in addition to this, there's a large amount of others as well.

So, as a natural result of this, attackers are moving from the traditional vectors of email and other traditional techniques into attacking these platforms. And these attack vectors are a bit special in the sense that they're not covered really by traditional security measures and can be a bit blind spot for many organizations, especially because the responsibility model is a bit different in these platforms. So, if you think about like if you've heard the concept of shared responsibility model that underpins these platforms. And there's a bit of dangerous assumption often for the customers as well on these that these SaaS platforms are 100% secure by default and the vendor does all the work related to the security.

Specifically about Salesforce, Salesforce is much more than CRM. And this is perhaps the thing that we all see a lot. The customers are – customers and the ecosystem broadly thinks that Salesforce is only a CRM. A lot of large enterprises and public sector is building their digital operations on top of Salesforce. So, they're doing stuff like customer support, workforce management, different digital experiences and all sorts of things in addition to the traditional sales and marketing part. A large enterprise can typically have tens of different Salesforce clouds and different units for different use cases. So, it's not like if you are a large enterprise that you have one Salesforce instance and that's it.

And a big part that's driving the risk – and I'm going to talk quite a bit about this more today – is they are also kind of opening the platform up to external users.

So, you're going to have customers, you're going to have partners, you're going to have subcontractors directly interacting with your sales -salesforce platform. It's not an internal tool any longer in these large enterprises.

For outside users, this is – this often quite invisible. So, when you do, for example, a loan application to a bank so you won't go to something that's view is a Web page or a portal, and you submit the necessary documents and you write the information. So, the interesting aspect is that typically you as a customer are interacting directly with the customer Salesforce platform. All the information goes directly into the Salesforce platform.

Same goes for, perhaps my favorite example is that when you're chatting with an airline customer support unit through WhatsApp, that's actually feeding directly into Salesforce support case because Salesforce integrate that with that WhatsApp functionality. So, of course, this gives a direct vector for attackers to put in malicious files, phishing URLs and other attack techniques to get access to your – to the employer – employees of the company.

And of course, Salesforce clouds in themselves are a very interesting at that target because they, of course, contain a lot of sensitive information.

But often, this also can be just a kind of stepping stone into the infrastructure after he was talking about getting these credentials, that's the critical first step. So, this is often a good way of kind of for the attacker to get that first access, get that first breach, those first credentials.

No single security layer will ever catch everything. But a key principle in security is that you scan at the point of entry. And today, more and more often, that first point of entry is the Salesforce platform. So, whose responsibility is it then to security source and cloud platforms, the answer to secure the SaaS and cloud platforms. The answer varies a bit by platform, but here we're going to look at the Salesforce Share Responsibility model. So the vendor is, of course, responsible for securing the core platform infrastructure, network, software and the platform. And they are typically very, very good at this. They have the knowledge, they have the resources, and they definitely have the incentive to protect their platform.

But that still leaves a lot of responsibility to the end customer. So for example, areas such as configuring the platform, identity and access management and content. That's the responsibility of the end customer. So in the Salesforce Shared Responsibility model, the customer's responsible for the content and protecting that content from malware. So the platform does not take care of that for you. So we all know the risks that what can happen with this – with getting malware, phishing links and kind of the cost of breaches.

But this way, kind of Salesforce provides a new vector for attackers. And something that's a bit special in this SaaS world and for Salesforce, so there's a disconnect between IT and security teams and Salesforce administrators. So quite often when we talk to customers, we're going to ask them that who's responsible for your Salesforce security? The Salesforce admins are going to typically say that IT and security and when we asked the IT and security team, they tell that it's the Salesforce guys because this is quite often managed a bit separately from a traditional and from the company. So I quite often there's a bit of a gap that it's a bit unclear who's actually responsible for Salesforce security or then that the team assumes that it's Salesforce. It's a cloud platform. I don't need to do anything about it. It's 100% secure. That's the promise of the platform. So many customers, which is a bit surprising. But even in large enterprises, many customers are not that familiar with the shared responsibility model, and they haven't really thought through what that means, what they need to do.

The threat of an attack vector through Salesforce is real. So this year, we saw a spike of almost 4x in malicious file detection ratio in the Salesforce environments of our customers. We also saw the attacks become more of advanced. A few years back, we saw a more kind of typical traditional malware. Now, we start to see a bit more complex things such as nested attacks. So, instead of getting a phishing link, you actually get the nicely crafted word file and then the link is inside that file, perhaps in a shortened format, and that leads to the phishing page. So, there's these kind of more advanced attacks that are being done.

We also know that there is a fair bit of malicious URLs in Salesforce ecosystems, of course, like getting the credentials, it's all about phishing often. So, there's a fair bit of malicious URLs as well, there as well, we see really interesting kind of developments in in link shorteners or things that make it kind of make it more believable for the end user to click on those links. And of course, we've talked about breaches, and I think Artturi was also talking about this earlier. We know from both research and public breaches that many attacks start from the public-facing apps. So, and often when you if you actually go and research into these breaches, you will notice that the reason for the breach was kind of in the shared responsibility model, the root cause wasn't the kind of customer's part of what they should have done.

Many of you might remember a couple of years ago there was a lot of information leaks from AWS S3 buckets because those storage buckets were just wrongly configured so that they were open to the whole Internet. So, that's a good example of where the responsibility model kind of comes into play.

Couple of real life incident stories So for example, we have an energy company in the UK. So this was a web-to-case submission, web-to-case submission meaning that it's a web portal that looks like a normal web page to you, but that feeds directly into the salesforce platform. So there was a malicious QR code submitted to it. QR code being an image with an embedded URL link. That customer support agent kind of clicked on that link, got forwarded to a fraudulent Microsoft Authentication page and then not noticing that gave away their credentials, thus allowing the attacker the first step into the structure. This was a very interesting example because QR codes are – they're used quite a lot in certain markets around the globe and they're very interesting from the point of typically when you get one on your computer, you're going to scan it with your phone to get that link out so you're kind of – from the attacker's perspective, you're nicely bypassing the software security stack on the actual desktop that you are using.

Another example, a manufacturing company in the US so here again, this is a phishing e-mail to an e-mail-to-case, e-mail-to-case meaning again, salesforce functionality where the customer thought, I'm just sending a normal e-mail but actually instead of there being an inbox where that the e-mail lands, it goes directly onto the salesforce platform where a customer support agent open that. Again, a bit of multi-step attack in a sense, but there was a malicious link there that went to a Google page, which actually then immediately redirected into a fake Microsoft Authenticator page and again customer support page and not noticing this, giving away their credentials. In this case, it actually led to a breach and this was only figured out in hindsight by WithSecure incident response team who then figured out that hey, where did this – where was the point of entry for this app that can then identify that came from the salesforce platform and from there.

So, we talked about cloud platforms and attack vector. We talked a bit about the shared responsibility model. We talked about the increasing malware attacks through Salesforce platforms. So, what can be done about this? So, currently, we have the category-leading product for securing Salesforce content from malicious URLs [indiscernible] 02:08:14 fully native solution runs without middleware, i.e., runs on actual Salesforce servers available from the AppExchange which makes installation very easy. We've got excellent feedback from customers, both public and non-public. For example, like perfect five-star rating on the AppExchange.

We have a really quickly growing customer base, both in terms of ARR and number of customers. So, the moment we have more than 270 customers, of which 30 are in the – on the global Fortune 500 list. Last 12 months based on Q3, we grew our ARR by 38% and new customers by 28%.

And we're focused on large enterprises and public sector. We do have mid-market customers and even some SMB or small customers. But when working together with these large enterprise and public sector, a great product alone is not enough. So, we're, of course, supported by the long history and brand equity WithSecure. We are a long term credible cybersecurity company, and we also have certain key certifications that are a must if you're going to play with these large enterprises. So, not going to walk through all of those, but these are 27001 and ISAE 3000 Type 2 AR some of the most critical ones.

Also, these large enterprises really require great customer support and technical post-sales. For example, with many of our customers we talk like in quarterly business reviews with some of them even in weekly business reviews. So, just how is going everything working?

We talk like in quarterly business reviews with some of them even in weekly business reviews. So just how is going everything working? Do you need some help with something? Also, one thing that was mentioned earlier is this local data processing and us working with these large enterprises. this is something that we see as a hard requirement. So, we already do local processing in Europe, US, we have also instances in Singapore and Australia and from Q4 onwards in Japan, because these large enterprises are not content with any longer with processing only in the EU or in the US, you need to be where the customer is processing. And this is something you have seen earlier with AWS as another going to country specific instances and so on, and now that requirement is coming to the big platforms and even the add-ons of those big platform.

We think Salesforce ecosystem offers a massive opportunity. So Salesforce has more than 150,000 customers. For us, each and every one of them is a potential customer of ours. The ecosystem spans all industries and all regions globally. And of course, Salesforce is not staying still. They're expanding the platform continuously. The biggest thing that they launched a couple of months ago is Native AI capabilities on the platform. So they are, of course, wanting to grow with their customers and become even more sticky with their customers.

We have a clear go-to-market globally with Salesforce. So there is global demand across all industries, but especially in large companies. We've got good sales and marketing collaboration together with Salesforce, and of course the ecosystem of potential customer is very clear. And I think there's a lot of talk about ecosystems and platforms and whatnot, but I think like the Salesforce is a very special one in that Salesforce actually provides really a lot of support to the participants in that ecosystem. So you actually really get the support. It's not just something on a PowerPoint somewhere. But you really get to work together with them and they help you if you need that support.

AppExchange, very important part. Nobody wants, especially in large enterprises, yet another portal or another back end or some middleware. They want it to be easy and work very natively. We also have this independent business unit that I'm heading dedicated to this market. And this is a very important aspect that we've tailored our approach and ways of working to the Salesforce ecosystem fully.

So, the buyer group here is very focused. These are people and teams that only work with Salesforce platforms. So, you need to be fully native. You need to understand the platform from a technical perspective. You need to talk the Salesforce language and use the correct terms. So, if you're not an expert in Salesforce trying to sell to this crowd, you will stick out like a sore thumb. So, this is not the generalist game to sell to these Salesforce teams and platform owners who run this.

We believe there's much more to do within the product than what we have now. So far, we've mostly worked into content security, meaning malicious URLs and file. But we have a lot of other ideas that we want to get to. Two areas that we've identified already as key in the future is identity protection. Artturi talked about that need in general space, we think there's definitely work we can do on the Salesforce platform there as well. And integration and connections. As we talked about, Salesforce is getting integrated. A typical Salesforce instance for large enterprises connected with tens of different systems, whether that's WhatsApp or some AWS storage or something else. So, of course, there's a massive amount of data moving back and forth here, users working across this. And obviously, these same integrations are some of the integrations that attackers want to use to move from system to system So hence, in the future, we're going to focus more also on these areas. During early next year, we will introduce our first identity protection feature and cloud protection for Salesforce. And we're also already working with the first features within that, the integration and connections to make.

So what do we want to do? Our mission is to become the number one security solution within the Salesforce ecosystem. We want to complement Salesforce's all native and premium security offerings. Nothing more, nothing

less. We think we are in a really good position here. We currently have the category-leading product. We've got excellent customer feedback and a really good product market fit. You don't get to these customer names and logos and growth numbers if you don't have a good product market fit. We are a credible cybersecurity vendor, and we've got both the market success and certifications to support the product. And we have a lot of road map and a lot of additional things that we can do in this area, either within the existing products or even within like new products within the Salesforce ecosystem.

Solid go-to-market, competitive positioning. We've got a very fully aligned and native sales process tailored to the Salesforce ecosystem. We work heavily – really heavily on the cases with customer success, marketing and sales, and alliances, which is our unit and team that works with the Salesforce together. We've got really good cooperation with Salesforce in sales, marketing, and technical domains.

We've got a high performing team. So we did a lot last – a lot of changes 12 months ago as did WithSecure, and we pretty much completely revamped how we run the whole business unit during the past 12 months. And I think one of the key thing to note here is that this is very different from Elements. We are not running a midmarket playbook here. We are running a very different like enterprise-focused, mid-market playbook here. We are running a very different like enterprise focused, Salesforce dedicated playbook. So, all the things we do need to work for this with the maximum efficiency. So, we are not trying to cover at the moment other ecosystems or do something like that. We are kind of all-in on making it work the best way it can for this product and this ecosystem.

We are currently recruiting to, with the focus we want to accelerate our ARR growth and deepen the product. Those are the key imperatives that we have. The independence within WithSecure will allow us going forward to focus even more with the aim of increasing execution speed for different. And I think we have a massive market and growth opportunity. I mean, we got the large untapped market that's emerging in the Salesforce ecosystem. I think we've got a good balance between new sales and expansions and low churn at the moment. And there is global demand across different regions and industries.

So, hopefully that gives you a better picture of where we are with cloud protection for Salesforce at the moment and what we're thinking about and where we want to be. So, with that, I'm going to hand over back to Antti.

Unverified Participant

So, hey, thank you, Juhana, so much. And it was a good example how the enterprise playbook is different and it's a good business, Juhana and the team are running and we are running it as an independent operation of WithSecure like we have talked about.

But I – what I would like to do before we move to the G&A, just to recap what we talk about elements company part of the day. So, ambition is to become a rule of 30 plus company by 2027. And our mission is to be Europe's flagship for cybersecurity. Maybe not the biggest, but the best this continent can provide.

And we do that first by winning, so we are bringing the minimum effective security to the mid-market together with the partners, like Ictivity. Because they are the companies, the local market trusts. And we want to make an impact. We want to be the most trusted, innovative and influential European alternative for the digitally driven world. And then we want to stand out with our offering. We are making Elements Cloud truly a platform of capabilities, not just tech and individual point products, but a platform of capabilities combining technology, human expertise and artificial intelligence from one place.

And finally, we'll be running our company with the precision of a world class SaaS company. So that was the Investor Day presentation part for today. And I'd really like to thank you everybody here in the room and within the line for listening and maybe over to Laura next.

Laura Viita

Vice President Controlling, Investor Relations & Sustainability, WithSecure Corp.

Thanks, Antti. And actually stay here, please.

Antti Koskela

President & Chief Executive Officer, WithSecure Corp.

I can stay. Thank you.

Laura Viita

Vice President Controlling, Investor Relations & Sustainability, WithSecure Corp.

Yes. And I would like to invite all of our presenters back to the stage for the questions and answers.

QUESTION AND ANSWER SECTION

A

All right. Here they are. And who wants to start?

Felix Henriksson

Analyst, Nordea Bank Abp

Q

Felix Henriksson from Nordea. Thank you for the presentations. Very comprehensive package. Three questions. Firstly on the financial target, the Rule of 30. So you mentioned you seek for both double-digit top line growth and a double-digit EBITDA margin, but in a scenario where your top line growth doesn't achieve double-digit level. What will happen to the margin? Will it also not get to double digit level or will you start optimizing cost at that point?

A

Our ambition, we have made a very sort of clear guidance to the market with the rule of 30 plus. And, of course, that caters for all the potential scenarios for the faster growth and the slower growth.

Q

Right. And in terms of the margin so you mentioned on gross margin that there's still potential for uplift to 80% to 85% level. What's the driving force behind that in particular?

A

Well, I think you saw our software already exceeding that target. And we do see that our core security services are also quite good margins already today. Obviously some efficiencies there so we can improve on many fronts there. And of course, it's a continuous work on our cost of goods sold also in terms of hosting costs and so on that we have done for many years already.

Q

Right. And then you mentioned the managed services customer account. Now it was 270 if I recall correctly.

A

A little bit less than 300.

Q

Yeah. How many have you lost recently with the customers turning out? Can you give any ballpark figure on how that number has developed?

A

So we are saying there that just on the – because there's been a lot of questions on this topic so the top 10 customers in the ARR was today represent around €7 million to €7.8 million so that in a way could indicate to the large enterprise customers that we have over there. And then, yes, and there has been churn but I think we haven't opened open that up specifically in terms of numbers, but that has impacted, you maybe can look at it what has been the net revenue retention of 87, that gives you your perspective of what's the amount of the churn as well in that one?

Q

Right. And then actually want one more regarding cloud protection for Salesforce, obviously, you've excluded that from your financial targets. So what's the thinking regarding that part of the business as your, you know, future part of the portfolio?

A

Well, I think there's a great opportunity like Juhana said and so on, but we are not publishing any separate target at this point for them.

Q

Okay. So is it still that you're either looking for a divestment of a minority stake or a bigger one in that regard?

A

So we have a patience to develop the business independently and I think that strategic logic to look for investors for that business has not changed.

Q

Great. Thank you.

A

As we are now in no hurry.

Waltteri Rossi
Analyst, Danske Bank A/S (Finland)

Q

Hi. Waltteri Rossi from Danske Bank. Thanks for the presentation. I could continue on the financial targets. You shows specifically that the R&D spend is expected to decrease. Do you see that impacting your competitive kind of ability and ability to keep up with new threats? Do you see that as an issue?

A

I think these are for the 27th scenario. Of course, we expect healthy growth as well to solve because these are in percentage to the revenues so that and I think towards the reaching rule of 30, I think growth will take care of some of that one. But I think there's always a need to find efficiencies everywhere.

Waltteri Rossi
Analyst, Danske Bank A/S (Finland)

Q

All right. But in a case that the growth kind of wouldn't come through, kind of wouldn't come true, then in that case, the relative share of the R&D spend wouldn't decrease. So, or if in that, sorry, if in that case you would still decrease the R&D spend, then obviously it could impact your kind of competitive abilities.

A

So, then not – not to speculate, but I think we said that about 30 plus is that is the guidance for that in a sort of unlikely case of kind of lower growth. Of course, of course, we would look for efficiency measures in that case as a part of the guidance. I think that's embedded in the guidance. And I think our primary plan is to grow the business and the growth drivers are quite clear, as you see, and the historical evidence also in the elements, elements cloud software points to kind of our higher double-digit growth.

Q

All right. Thank you. Then kind of similar question on the – on the sales and marketing spend. You also plan to decrease that the relative share. Can you give any kind of specific on – specifics on how that will be achieved?

You talked about quite a lot of update, focus in the partner channel is – is there plans to make that efficient in a way that you focus even more on the larger partners and kind of decrease the amount of total partner network?

A

So, yeah, maybe a couple of points on that. I think one big part of this is a little bit looking backwards as well. We have a huge transactional partner space and with the new platform and the capability, this is about automation. It will be less resource incentive also from our side and improve the cost structure from that perspective that is enabled by the digital channels and the capabilities we have the strategy. The other part is then obviously our sales and marketing scaling through partners. So at the moment, how we are presenting and then putting the teams in place is we are investing more in partner development and partner capabilities. So in general terms, if you look at SaaS marketing, we are looking at the efficient trade from 1 to 10 to 20 and how we scale out. And this is something especially also on the managed services side as we are bringing MDR to the channel and more partner-driven business model. It will put less heavy weight on our – how much do we need to add people in the front end to actually support this type of customers. So it's a balancing act from that one and that's why we see but also from a marketing side, we can be much more efficient on the digital channels and maybe some of the more traditional mechanisms. So I think it adds up with the percentage, the growth. So we are a healthy balance.

And the keys to automation of the long tail and focusing on the growth-oriented partners like lots to talk to. And of course, this percentage are in relation to the revenue and the same comment as with R&D.

Q

All right. Thanks, Tom. Question about the on-premise revenue and the transition of that revenues to the cloud sales. How is that being proceeding? Do you see that most of the on-premise decline is actually moving into the cloud or do you – are you losing some of that on premise?

A

So obviously, you're losing somewhat some of that in that one. But I think a big part of that gets transitioned. And of course, we sell the full portfolio in the process of doing that one. But we are kind of continuously have been in a path three years. We continue to do so that we move the on-premise versions to the cloud version to the maximum ability.

A

And just sort of to – so what we also see, which is the benefit of the extended portfolio is a lot of them from customers are coming from the EPP side, so to say. So we now see more evolution that actually when we are migrating, we also take an update on the revenue per user.

Q

All right, thanks. Then one last quite specific question we talk about Microsoft a lot. We also heard today that actually their products are quite okay. Then I've heard also that, you know, obviously, they I guess they're a lot cheaper so how much cheaper are they – are there? Okay. All right.

A

Quite the contrary. What makes them cheap is that when you bundle everything together and then you increase prices 25% next year like what happened this year.

A

I think building on what Antti said, like thing there is if you're using all of the products you're getting in the bundle and the price for a product is, of course, low. But then that means you have a lot of people and a lot of experts and you have different experts for different parts of that bundle. It's not just security products and not just one type of security product so essentially the total cost of ownership gets very high. And we've had those comments as well from end customers where they have tried to go to Microsoft and they say they have to start hiring a lot more people compared to running on our platform.

A

I don't want to talk specifically about Microsoft, but there was a recent LinkedIn post from [Foreign Language] 02:29:10 apologies for the Finnish world – Finnish word, but it was that they were quite shocked on the sudden price increase of 25% like that.

Q

All right. Thanks for the answer.

A

But I think we want to have a partner friendly, customer friendly mode customer-friendly mode on that and work in a European way also in those matters.

Q

All right. Thanks a lot.

Jaakko Tyrväinen

Q

Jaakko Tyrväinen from SEB. Thanks for the presentation and especially giving some color on the managed service and cloud sales split. On the managed services where you have seen some churn, could you elaborate a bit more in details what is the size or number of customers being at risk of churn currently?

A

Yeah. So we quoted this number, that we have 10 large customers representing €7.8 million. So that – so we are not saying is that full but that gives you a sort of a number of customers where the biggest revenue concentration

is. And some of these customers continue with the managed option, but it's a fact that in the large enterprise, people opt for this build-it-yourself model like it was talked many, many times here.

Q

Okay. Perhaps a follow-up on that one. How much larger the top 10 customer sales were a year ago or two years ago in that managed risk category?

A

We are not submitting that number.

A

Yeah.

Q

Was it larger or smaller?

A

So – but it's sort of – I think in a way, it's obvious that – in our managed service number that the 270 customers, we are winning these cosecurity customers. You heard from Ictivity how that motion works so that we expect the number of cosecurity services together with Elements Cloud, of course, to grow within that one. And then some enterprise customers may transition. Of course, we want to serve them as to the best of our abilities.

Q

Thanks. Then the up – to the upsales potential our abilities.

Q

Thanks, then to the upsells potential, which looks kind of amazing. However, what is the key reason for customers declining your up sales pitch and you're not being able to kind of deliver to those that potential?

A

That's a very good question I think of what good could get from [indiscernible] 02:31:49 comments so that but if I sort of a start that is this compelling reason to act. And security has been often a very techie thing in the companies, but now it's becoming a board topic and the CEO topic, which is a very different situation. So, so we expect that in a way, the sales speech to the sea level has not all, when you say that we need a system to work

on the vulnerabilities and to get this one, it may might not speak, but even you say that you will be faced with a 2% penalty and a potential jail time that they will listen to.

A

Yeah, maybe I – this sounds very basic, but at the moment I think it's a budget skills and lacking of the forcing factor. But the forcing factor is now coming back to the game and we start to see an uptick on the budget. For us, the opportunity a little bit of the challenge as well is how we pivot our partner ecosystem. But also it's up to speed with partners like activity that they can actually, from the customer perspective, represent the full portfolio. But as we'll still have a lot of product transaction based partners by the legacy.

Q

Then on the slide provided there, that multimodal customers and their share of the total. Is it fair to assume that the remaining 60% of single product customers are mainly EPP or only EPP basically?

A

It is fair.

Q

Yeah. Then, sorry, changing the subject to consulting. What is the update with that strategic review, any words on that? So as you know, we disclosed in Q3 that we are in active discussions regarding consulting.

Q

Fair enough. Thank you.

Atte Riikola
Analyst, Inderes Oyj (Research Firm)

Q

Hi, it's Atte Riikola from Inderes. May we now continuing with the consulting still, now we know that the divestment process has been going on for a pretty long time already. So do you see that it's affecting the development of the consulting business or is there a like do we see like churn in customers or churn in employees there?

A

We have not seen any signs that that process would have affected the business.

Q

Okay, good. And then let's go back to the upselling, because I remember it was your – then it was, of course, F-Secure's Capital Markets Day like six or seven years ago. And I think then there was the one key topic was that

you have so many small customers or customers using only one product. And now we see that still the number of customers using only one or two product is pretty, pretty low. So, you know, a little bit longer term, what has been like the key challenge to get that number higher?

A

I think a lot of it comes to the minimum effective security. Like I said, for a long time, it's not even minimum effective. It's been more minimum viable security or bare minimum security that that organizations have been focused on. I think the other thing there is, we talk quite a bit about where SMBs both in Europe and globally, where they actually are on that technological transition. It's easy for us working in the tech industry or following the tech industry, us living, for example, in Finland. For us it feels like everything is in the cloud and everything's very digital and modern and high speed.

But if you look at the numbers, especially in the mid-market and the smaller companies, they are still on that transition. And it's natural that it also goes a bit hand in hand. As you digitalize your business, as you digitalize your operations, then you also are able to take new capabilities into use or, in some cases, you start to have more of the need and the demand.

So, I think that's maybe on the much longer term, more macro trend, but similarly compliance. The world has changed dramatically in the past 5 to 10 years. And for example, compliance requirements have really started to emerge in a very different way in the past 5 years versus where they were, 6, 7, 10 years ago.

A

Yeah, probably, two additional things. What we see if I look at some of the markets, let's say Japan, Southern Europe, still very heavily focused on not really on the services side of the equation, but just the mainly technology component. So, the privilege that we now have with the cloud security services and what we are discussing with some of these partners in the market, they have now the capability to come up with the kind of the upsell. So, putting more resources and capabilities from the product side, but being also able to serve because that's by the end of the day is the requirement for a smaller company. You don't buy products. You want that service. And while we were missing that cloud security service component, that was quite often the hindering factor because we cannot sell the internal value for the common customer.

A

Also thinking about them like huge upsell potential with the exposure managed from your point of view, but from customers point of view, it might mean that they have to double their investments in their cybersecurity products and services. So, that's like the key sales pitch to convince customers to do that because it can see on paper pretty, pretty big investment for them.

A

But still, the investment is – it's for all these companies is a lot less than hiring a one person. I think you need to give it another perspective it's for all these companies is a lot less than hiring a one person. I think [indiscernible] 02:37:23 give it that in perspective.

A

I think that's a great point. And then the other thing is, obviously, we don't see SMB customers buying exports management, but we see partners providing a different level of service for them, which somewhat dilutes the investment from that side as well. Whereas then the meet market might be equipped to actually acquire such a solution and use it for the right reason.

Q

And maybe about exposure management still, what kind of expectations you have for that if you think about your new financial targets, is it like meaningful in your growth target?

A

It is a meaningful and it's a key part of our elements cloud ARR growth ambition. And we firmly believe that proactively managing digital risk as it's written as text in NIS2 is the requirement companies need to fulfil in addition to the XDR.

Q

All right, then, about that new identity security module that you have. So, could you just briefly explain how it – how it compares to, because we know that there are some vendors that are purely focused on the identity security or identity and access management. So, how is this different kind of product compared to those vendors?

A

So, it – identity and access management is a different thing. It's more, you know, making sure you have the right number of keys and giving keys to the people who need the keys versus identity security, and similar point solutions is more about, you know, noticing if someone stolen a key off of someone or someone's made an extra copy. I guess that's the difference there. But what we do compared to point solutions, again, the key thing is enabling our partners and the end customers to build their mid-market playbook and operate efficiently and effectively. They can't afford to buy yet another point solution to solve yet another separate use case and then having to find people to manage that then upscale on that separately from what else they're doing. And we can all understand how ineffective it is if you need to have a human looking at one product and then turning to look at another product and manually copy pasting with their fingers on the keyboard between those versus having it in an integrated platform where it solves your key needs and doesn't do too much and isn't separated from those.

Q

All right, then last question about cloud protection for Salesforce. It seems it's like a very niche market but how's the competitive landscape nowadays? Is there any like meaningful competitors for the product or a good place?

A

So obviously, like emerging markets are a kind of new category. There is some competition. I think clearly, we see ourselves as the category leader and kind of – it's not that mature that we encounter competition in all cases at all. And when we encounter typically, we've had really good success so far. Obviously in all fields and IT competitor if I'm not standing still. So I mean, we need to press ahead. Yes. But at the moment, the position is very nice against the limited competition there is.

Q

All right. Thanks for the presentation.

Q

Kim?

Q

It's Kim Stenvall continued on the property protection for Salesforce. As long as you have been reporting the business, it has been quite flattish. But now the Q3, I remember it was growing quite light and so, any kind of thoughts a little bit on the big picture on the longer term? What was the reason on the sluggish growth? And now, how do you see the future going on?

A

Well, I think it's a new area. So for us also, operationally, it's like a bit of a learning journey. So like I would say that the improvement now is more from our like internal actions improvement now is more from our like internal actions, like how we restructured the teams, how we develop like a new sales process and how we approach customers and in a way making it work better in all aspects internally. I think that's the core thing that happened in a way. I don't think there has been a super big shift in the market in a way. I think like if we would have executed as we are doing now, just internally, we would have had a lot better last year as well. So I think that's the key on operational efficiency in a way.

A

And we have these few charter cases more than a year ago that impacted quite a lot, these ones. But I think a [audio gap] 02:41:56-02:42:04 increasing the number of customers.

Q

Okay. Thank you.

Q

I still have one question. You mentioned that new products in Elements portfolios like referring to basically the exposure management or is are you planning or is there – is the Elements for missing some bigger products or are you developing any new products with?

A

I don't think we're missing anything big right now, but it's something where we need to also keep our eyes and ears open. And we work a lot with our partners to understand what you know I feel about was talking, what's the overall bundle that their customers demand and what are the parts where it makes sense for the partner to do that either build that capability in-house. Now see, so as a service, for example, having a local person, local language makes a lot of sense for both us and the partner and the customer. And then there might be some specific used cases where they might be using, you know, a very long term point solution, for example, because that works in the local market or for the partner. But we're constantly monitoring those and seeing what would be those capabilities that we see There would be sufficient demand. They make sense for us, us to add those. But I think we have a competitive portfolio right now. So there isn't any clear big gap in the [indiscernible] 02:43:26 front.

A

If I can be like maybe increase maybe some of the scope of the cloud systems and things like that obviously. And – but the key thing is that if you look at our business model that we are moving to an API economy so that how do we connect with APIs also to the backend and how we connect with APIs to the other systems MSPs are using. There are different, different systems. If we make it easier and smoother for the MSPs to put everything together in a pre-integrated fashion, of course we make their life a lot easier to take our products into use.

Q

Thanks.

A

All right. I will go to the chat. There are a couple of questions here. So Erik Karlsson from CapeView Capital says hi, thanks for the presentation, on the channel for us. How difficult is it to retain or sign up new partners given the intense competitive situation, especially for Microsoft?

A

It's not easy. But if I just look at the last six months, the uptake on new partners, we have added I think roughly 10% on that side. This is coming back into a lot of partners like the MSPs looking now how they're entering the cybersecurity market. And that said, there is also a lot of competition already for the traditional Microsoft channel. So it's also for the question for them, do they follow that path or do they differentiate?

The other thing that we see is when we are looking at the distributor market and also working very closely with AWS, that opens a different angle to the ecosystem as well. They obviously do look for solutions and capabilities that are challenging Microsoft. So it's not an easy thing. But at the moment, you know, our value proposition is working quite nicely, and we will see some more consolidation on the strategic side as well. Good news will follow.

Laura Viita
Vice President Controlling, Investor Relations & Sustainability, WithSecure Corp.

A

Thanks, Lasse. Then, Eric, I hope we answered your question regarding consulting. So I'm moving on to a question from [indiscernible] 02:45:44. How many partners do you currently have offering co-security and managed services if the amount of those customers is 270? And what kind of growth are you currently getting in amount of co-security and managed services partners and what is your three-year growth target with these kind of partners?

A

So like Tom pointed out. So we are not disclosing how the managed service growth specifically work. We are guiding on the rule of 30 plus for the whole company. So I think that's for one. But maybe Lasse, you could talk about how with this focused approach with the high touch partners, how the co-security motion works once again.

A

Yeah. The co-security motion and also related loop to the managed services, so we'd just released our Elements MDR product just a couple of weeks back. And we are already seeing a lot of interest and uptake that's partially driven by the NIS and the, you know, ability to provide what the customers are after. It is also again providing the ability for partners that don't have the full extended practices yet to step in into this concept of managed services.

So we do start to see an uptake and that is really if I look at our partner landscape today, we have roughly hundred partners that have this MSP competency, we have roughly 100 partners that have this MSP competency which differentiates them from more the reseller type of activities and so forth, and we see those partners at the moment being the most active in training and then certifying their people, especially on the Co-Security Services side and exposure management. So, it's still early stage we have been with in the market for a couple of months now, but if we follow and look back year-over-year, [ph] it updates us 02:47:39 from when we're following the training figures, we're actually executing, I think, on the highest than ever before on people getting certified and it's on [indiscernible] 02:47:49 solutions.

Q

Thanks.

A

Any more questions in the room? Looks like chat has gone silent.

Unverified Participant

So, if no more questions are coming in, I would like to thank you all. This will end the Investor Day 2024 of WithSecure. I hope we have answered some questions. If you have questions left, please get in touch. If it's about the heuristic attack path engine, go to Artturi directly. But if you want to discuss WithSecure as investment, come to me or any of the other team members.

Thank you very much for participating today. Our journey continues. And thank you to the webcast audience. We are closing the webcast now, so have a nice day and a lovely weekend.

Unverified Participant

Thank you so much.

Unverified Participant

Thank you.

Unverified Participant

Thank you.