PRESENTATION
Peter M. Salkowski - Fortinet, Inc. - VP of IR

Good morning, and good afternoon, everyone. I'm Pete Salkowski, Fortinet's Vice President of Investor Relations. I'd like to welcome everyone to Fortinet's 2022 Analyst and Investor Day.

Before we begin, a few housekeeping items. (Operator Instructions)

For those of you here in the room, please wait for a microphone to ask a question. Aaron and I will walk around and provide that so we can get the questions out of the webcast.

This is a live video presentation that will be available for replay on the Investor Events section of our website. The Analyst Day slide presentations as well as the transcript will be posted on the Investor Day website as well later today.

Now for today's agenda. Our presenters today are John Maddison, Chief Marketing Officer and Executive Vice President of Product and Solutions; and Keith Jensen, our Chief Financial Officer. John will start off by doing a deep dive into Fortinet's core platform and platform extension products. Well, John has a ton of great information to share. He'd like to make the presentation interactive. So as John's speaking, he's going to ask the
audience if you have any questions, and so feel free to do so. If you have one in the room, please raise your hand. If you have one online, type it into the application.

We're going to give John a little bit of time, probably an hour, maybe a little bit longer as he tends to have a lot of information to share, and I think it's really good stuff. So we'll go that. After that, Keith will be following John, doing a financial overview of our consistent financial performance for the last several years and then update our medium-term model. Keith's presentation will be followed by a Q&A session, where Keith will be joined by Ken, Patrice and again, John.

Before we begin, the all-important safe harbor slide. I'd like to remind everyone during today's Analyst Day that we will be making forward-looking statements and that these forward-looking statements are subject to risks and uncertainties, which could cause actual results to differ materially from those projected. Please refer to our SEC filings, in particular the risk factors in our most recent 10-K and Form 10-Q for more information. All forward-looking statements reflect our opinion only as of the date of this presentation, and we undertake no obligation and specifically disclaim any obligation to update forward-looking statements.

With that, I will turn it over to John. But one thing about the room, if you do get up and walk around, please be careful. People have things plugged into things on the floor and they may trip you. Thank you. All you, John.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Thank you, Peter. As Peter said, please don't be shy about asking questions as we go along. So what I thought I'd do is just go through our product portfolio by platform, core platform and platform extension. And then dig into a bit of detail about what products are in those solution sets. And then what's our vision within that strategy set.

I thought I'd start off, though, by just -- I know we saw a lot of TAMs today. By just looking at 2 pieces of the TAM. And so we had -- we talked about this $200 billion by, was it, '25 or '26? More on that. And so one part of that was the network security, and that's about, right now, about $80 billion. And when you look at this marketplace, it's very conservative, and it's -- there's not a huge amount of vendors. You can probably name, I don't know, the top 10, and that would be it, I think, after that for networking. It's somewhat, I wouldn't say commoditized, but what has been focused on over the last 20 years is just getting faster. So we've just got faster switches and faster access points, WiFi 7 here in 2 years' time. And a lot of it -- all these vendors can work together on ethernet switch works with another ethernet switch. And so it's easy to interchange vendors in that environment.

And I would say the biggest innovation that's come in this marketplace in the last 3 or 4 years is SD-WAN, where it started to look at being a bit smarter. So as Ken says, a lot of networking gear has no clue about the application. It has no clue about the content. It has no clue about the user, where the user is and everything else. And so SD-WAN came along and said, "Well, let me start guiding or routing based on application versus some static or dynamic IP address." And you can see what happened pretty quickly over the last 3 or 4 years, it's just eaten into that router marketplace. In fact, the traditional enterprise router marketplace is shrinking, and it's all going into that SD-WAN marketplace there.

I do think this -- the biggest piece of innovation coming, which a lot of these vendors have tried in the last 2 years, you've heard about software-defined networks and those sort of things. But I think the AIOps which gets you to that point where it's operationally more efficient is the next innovation center inside here. And then the other pieces start to embed more security in the networking devices, so that my ports can apply micro segmentation, so that my ports can apply security. So my access points can apply security. So we think SD-WAN's just kind of the start of making networking smarter, more secure. And I think as we go forward and Ken have the graph of the ratio of networking versus network security, you can see network security becoming a larger portion, almost 30% now. We just think that will continue going forward.

So yes, maybe you can look at this marketplace and say somewhat commodity and slow moving in some ways, but we think there's a lot of opportunity to disrupt this marketplace through putting security into networking gear.

This is not going to -- any ASICs inside this would control it, it's very slow. Was there a question there? No? There we go.
And then the other marketplace is cybersecurity. And you can see how fragmented it is. Even within those fragmented segments, there’s sometimes hundreds of vendors doing different things. There’s no standards to interoperate. There’s no standard to share policy. There’s no standards to share threat intelligence. And if you look at the marketplace, there’s different tools at endpoint and all over the kind of infrastructure, a bit faster growing in certain segments, but certain segments have become very static. And so this marketplace, we feel is ripe for consolidation, and it’s a bit different from convergence is consolidation of multiple vendors. So consolidation to us is not saying there’s 3 products here, we get rid of 3 products. It is there’s 3 vendors here, let’s go to 1 vendor for those 3 things. And that’s what we’ve talked about in the keynotes around the mesh and platform fabric and been able to kind of build that capability. And just about every customer I speak to or every CSO has that goal to get to automation.

Okay. And I think Keith has this. Keith will cover this slide as well. I think it’s -- we used to talk about things in this FortiGate and non-FortiGate world. And we just -- we didn’t modify it, but we just -- now talk about it in terms of what we call our core platform, which is FortiOS, as you heard today, which includes hardware and some virtual machine, but really FortiOS is the core there. And our platform extension. So when we extend that FortiOS so that it can talk to networking devices like switches and WiFi when it can implement a zero-trust network architecture, which requires endpoint and policy engines and proxy enforcement capabilities, when it can talk to the cloud capabilities. And I talked a bit about a new announcement there coming in a couple of months’ time around cloud native. And of course, when it can provide all that intelligence back into the SoC and the security operations. So going forward, we’ll talk about it as platform, core platform and platform extension.

And let me just kick off the first component of the core platform, which of course is network security. And the TAM here is I’ve heard 2025 is about [$25 billion] it includes, of course, the biggest part of that is Network Firewall. And I call it Network Firewall that includes staple firewall and next-gen firewall. It also includes a kind of shrinking IPS marketplace. I think in the next 3 years, that will all be assumed by the next-gen firewall. It includes secure web gateway, which is getting some different names as we go forward as some of that makes its way into the cloud. And then it includes network performance monitoring, which is a smaller marketplace. So this is the key network security marketplaces.

From our perspective, what we’re really focused on now and going forward, is making sure that we can deploy our FortiOS, which is the core of network security, the core platform at any edge. So these edges are formed around the 1 edge around the LAN Edge, especially OT Edge, 5G Edge, Cloud Edge, data center as it goes on, there’s edges everywhere. So our key capabilities been able to deploy that networking functionality, so the 1 edge is SD-WAN. You need best-of-breed SD-WAN functionality to deploy there, but then being able to apply security in any places. So I’ve been able to apply that security at the WAN Edge, LAN Edge or Cloud Edge, and maybe you apply different security in different places and then being able to manage all of that from a single console.

One of the hardest things when you’re trying to build a platform and the networking vendors have found us out is if it’s okay, writing big checks for a lot of different companies, then building a single policy console across all those disparate acquisitions is impossible. It’s absolutely impossible. So having a single console, that can provide policy for your WAN Edge, LAN Edge, Cloud Edge, 5G Edge can only be done organically. That’s why it’s taken us a bit of time. We’re still not there. It’s still a journey for us in some ways, but we have a much better shot at doing it.

And then as we go forward, we’ll start adding in some of that AIOps, so that we can measure that experience, digital experience from devices and users all the way through the LAN, into the WAN, into the cloud, measure that and feed that back into our AIOps engine. And then prior initially, we’re providing some information of what the performance is and maybe there’s a problem here and there, long term, providing some ability to self-correct issues that which are happening.

And we believe that you can’t just do that if you’re just in the cloud or you’re just on-premise or endpoint or you’re just in the network, you have to be able to see everything end-to-end, and you have to be able to provide control in the network at the endpoint, in the LAN, in the cloud, etcetera, to change that experience. Because if it’s outside of your realm, your domain, you can’t do anything about it. If you have all those pieces, then you can do something about it. But first of all, you need to know.

So our goal vision as we roll forward in network security, as we said today, is to be able to deploy our FortiOS as an appliance, as a VM, as a container, delivered by us as a cloud, but long term, manage that from a single console and be able to provide the AIOps across everything because the operational capability and the digital experience are going to be really important to the CIO as you go forward.
And this is the portfolio. So each one of these, we call them pillars inside Fortinet. We have a portfolio slide. So inside here is obviously our FortiGate and our FortiOS. We also have our FortiProxy and FortiSASE web gateway, also our digital experience monitoring, and of course, our FortiGuard powered security. And this is pretty impressive numbers for this marketplace. Keith talked about the number of customers we add per quarter per year. So over 565,000 customers, 5,000 to 7,000 per quarter, we're almost -- we're getting towards 40% of the marketplace. We think as the supply chain issues persist, we can get more market penetration beyond that.

And then one of the key things going forward are those security services. And we definitely think there's an opportunity there to add more service components to each of those edges. We continue to add new capabilities. I think the in-line sandboxing is one of the new ones we've introduced recently. Definitely, a lot of customers want to make sure they've got the most appropriate FortiGuard or security stack that they can apply to each of those edges. And of course, our services are recurring revenues applied to that footprint.

All right. Let me stop there to see if I got a question.

QUESTIONS AND ANSWERS

Hamza Fodderwala - Morgan Stanley, Research Division - Equity Analyst

Hamza Fodderwala from Morgan Stanley. I wanted to go back to an earlier slide where you talked a lot about consolidation. I feel like a lot of us have been hearing about consolidation security for a number of years. I'm just curious, what do you think has changed in the last couple of years, particularly post-COVID, where enterprises are finally starting to address some of the technical debt that they have from having all these various point solutions?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. Good question. So I do think sometimes, I speak to quite a few customers each week. Sometimes we get carried away with the huge customers who are still probably going to be a bit of a siloed environment. There's some financial companies who still have 100 security vendors, and that's just the way they're going to be. But there are -- there's a huge amount of enterprises and commercial mid-market customers. You just can't cope with 30, 40 different security vendors. They can't.

So they have got a plan in place. They're putting plans in place to consolidate. And it's a bit of a trade-off between a point solution. And that's why our functionality can have the Magic Quadrants for WAN and for network firewall and then for wireless LAN. It's important for us to not only have that platform functionality but also be almost best-of-breed as a product as well. If you best -- if your functionality is too far off, the customer won't accept it. There's too much of a trade-off between the platform and the functionality. So your functionality needs to be good enough, maybe 80-20 rule to get that platform benefits. So I think what's happened, especially for us over the years that some of those products that weren't core are starting to get to a point where they've got good enough functionality. And then it's an easy choice for customers after that. I want a platform, for sure.

But if we just focus in on the very large customers, I still think they've got a way to go before they decide on platform. I mean I'll see some pieces like IPS systems, for example, they've still got separate IPS systems sitting in their data centers. That will change 1 day, but it seems like it should have changed a while ago.

Michael Turits - KeyBanc Capital Markets Inc., Research Division - MD & Senior Analyst

Michael Turits, KeyBanc. Great to see you again. So you talked a minute ago about visibility and control across cloud and on-prem. And we just saw a great demo at the end of the keynote of an interface that I don't know if that was the FortiCloud or what the interface was or SoC as a Service. But clearly, you're moving in this direction that they were calling service mesh -- security service mesh architecture, and it sounds a lot like what
people are doing in XDR. So what specifically is the road map for building out the data, whether it’s in a data lake or some other fashion? And then exerting that visibility and control over it?

**John Maddison - Fortinet, Inc. - CMO & Executive VP of Products**

Yes. So Robert was showing was FortiOS and our FortiManager. And that has the ability to see everything like the fabric on our fabric topology map, you can see all the firewalls, you can see all the endpoints. You can see SD-WAN. You can now see zero-trust because it’s sitting inside there, so that’s that capability.

I will say though that I think I had a slide that showed you, we probably have 2 or 3 consoles today for some of that functionality, like some of the SASE stuff can be managed in FortiSASE, but we also have built a cloudified FortiSASE portal as well.

And so that is probably, as I said before, that is the hardest thing to do. When you’re building a platform across networking and cybersecurity across LAN and WAN and Cloud and everything else is you’ve got to get all that functionality in that single console.

So right now, it’s our FortiManager. We have a console that does some of the SaaS stuff. We also have a consolidated some of the zero-trust. I think, and we’re going to speak a bit further out here, as we go forward, you’ll see some of those things that come together, either as FortiManager or as some sort of cloud portal as well. But that’s always the hardest thing to do is to get the consult into sync with the functionality and the products.

**Brian Lee Essex - Goldman Sachs Group, Inc., Research Division - Equity Analyst**

Brian Essex from Goldman Sachs. A follow-up on the visibility and control point. When you’re talking enterprise, I guess, when you’re talking to clients, where are you seeing that come up the most? Is that primarily large enterprise clients? And is that a determining factor in terms of them choosing more of a secure networking solution as opposed to a secure web gateway solution with regard to the amount of visibility and control? What are they looking for when you’re comparing like your platform as opposed to like a Secure Gateway solution?

**John Maddison - Fortinet, Inc. - CMO & Executive VP of Products**

Yes. I think that’s still a bit broken. And if we go back to the beginning of this, there was networking and network security and zero-trust access. And so they’re still broken into those what I call buying centers to a certain degree. And even SD-WAN, where everyone said that secure SD-WAN is compulsory really, you’re opening up your network, there’s still a networking team making those decisions.

And then the Cisco will come along and say, “Well, we need to add security components here, either it’s on the SD-WAN device or it’s in the cloud.” So there’s still a bit of siloed thinking going on even within networking, definitely between networking and security. But everyone I speak to, and I speak to quite a few customers each week, absolutely believe they can’t carry on, just keep adding more and more different vendors and different company. There needs to be some consolidation and convergence.

And as I said, the larger customers are going to have a harder time getting there, given that, some of these organizations of 50,000 people in IT, it’s just hard to make the move. But definitely, the enterprises and commercials are starting to say, “Well, I’ll take this vendor to do maybe 3 things, not just the 1 thing.” And it’s easy for me -- a good example for us is SD-WAN, where -- they say, “Well, I’m coming up for the renewal of my WiFi in my retail branch, am I switching?” I could go and get a different vendor, I could stay with the same vendor or I could add Fortinet.

And as the view you saw from Robert today, I can see all my switching, I can see all my APs, my SD-WAN, all my security in 1 view and manage it that way. And that was just 1 use case. There was the work from anywhere as a use case. The cloud will be a use case going forward. The Zero Trust Edge will be a use case. So I think customers will look at use cases and decide, let’s see if I can get to a platform approach within those use cases.
On that note, John, I'm going to let you decide whether or not you want to keep going for a little bit or this audience will keep us on Q&A for the next 1.5 hours.

That's okay. We can have another question. That was my last slide, I think wasn't it?

Yes. Yes, you're on 13. I won't tell you how long it is because I know.

Fatima Boolani from Citi. Actually, just on this slide, I think with the benefit of hindsight, if you look at the middle, shipment chart, notwithstanding the fact that you joined Fortinet in 2012, and that's when your shipments started going up, but maybe...

Everything got better after 2012, to be honest. Every single thing.

So with the benefit of hindsight, what are maybe the 3 things that have transpired between now and then to have your shipment volumes really materially hit escape velocity? And then as a related question, that flies directly in the face of what we would consider to be opposite of cloud adoption, right, because your principal form factor is a hardware plane. So how do you explain that dichotomy with your shipment volumes going up into the right that way?

Yes. Yes, we've had that question -- we got a question for the last 5 years and we're still doing pretty well. So as I said, if I kept saying that, yes, there's going to be some movement of -- there is movement applications from the data center into the cloud, and that means maybe you need less of some core firewalling or some IPS devices there. But there's other markets which have come and taken off. SD-WAN is a really good example. We have to -- it's replacing all the routers around the world in branches and also in campus environments.

We've also seen the need to do OT security. And hopefully, you've got and see where are we on that way, the demo of our OT security when we need to put firewalls and those sort of capabilities inside the OT environment. So there's been a bit of a shift in business, but we always thought and we knew that there's other markets which are expanding and opening up so it's -- yes, some has gone to the cloud. And definitely, we've got a thriving virtual firewall business. I think that will turn to cloud native eventually.

And that definitely, some of the secure gateway business has moved into cloud delivered. And we definitely want to be part of that going forward. We just think markets kind of move, and the security always follows where the application is eventually. One more question here.
Shaul Eyal - Cowen and Company, LLC, Research Division - MD of Communications, Security and Infrastructure Software and Senior Analyst

Shaul Eyal with Cowen. John, looking at this 565,000 firewall customers and adding about 20,000 to 28,000 new customers a year, can you maybe talk to us about maybe the blend of the customers? How are you thinking about it, small customers, mid-customers, large customers? And maybe what is it that you've been seeing over the course of the past few years?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. Well, I think Keith had the slide on the breakdown, it's pretty equal between SMB, enterprise, large enterprise and service provider. They're 25% each probably between those. And of course, the volumes are different between those sort of customers, there could be a large enterprise has got 10,000 sites or it could be a large customer that's building out data centers. So the mix of the product changes obviously with the size of the customer, but it's pretty equal between those customers.

And we've always been a company that served both SMB commercial enterprise and service provider. And if you look at our product sets, they have to scale across those things.

Shaul Eyal - Cowen and Company, LLC, Research Division - MD of Communications, Security and Infrastructure Software and Senior Analyst

Just to follow-up on that. Is the mix in that part, the network firewall customers different to the mix, the overall mix that you talked about in that slide? I mean, because maybe you can imagine that a very small new business is purely operating on the cloud, and therefore, their needs are different.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. It's a good question. Probably, but it's also depends on the product. So we have a broad set of products. Some are more mature, leading in Gartner Magic Quadrants, and some are incubation, have just come out. And so an enterprise customer is not going to probably take an incubation product.

If you've got somebody who just wants to have cloud and that's it, then definitely our cloud portfolio. But even if a cloud-only customer still has a campus, some has a branch office, still has a network.

PRESENTATION

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

And I think as I move to the next section, I think what's important to us is that a lot of people are talking and this is the first component of the platform extension.

Now I do hear some vendors talking about the network is kind of irrelevant. Don't worry about the network. It's just -- we've just got our cloud here and just find a good connection and an agent and we're away, don't worry about anything else. We think nothing could be further from the truth that unless you can have that digital experience and measure that network and make sure that network's up full time and make sure that you can provide that connectivity to devices as well as users you just can't ignore the network. It's so important going forward. So the part of our extension is the network security.

This marketplace, as I talked about it before, is pretty mature, in '25 it's still a $66 billion marketplace. In fact, in 2021, some of the core components of their switching and access points started growing again, if you noticed. And this also includes Unified Communications, which these days is not
just phone systems, it’s Zoom and all those sort of things. But the core components are definitely wireless switching and the highest growth is SD-WAN.

What we’re trying to do here is, from an SD-WAN perspective, and I think I have this slide up there earlier is that we’ve really focused on the left-hand side so far, building that SD-WAN component and making sure that SD-WAN, based on our SoC 4 chip, and as Ken suggested today, we’ll continue evolving those chips out. That was our first SD-WAN chip.

And we’ve done really well in building that out for the SD-WAN functionality as well as, as we go forward, customers are starting to add some security on there as well as zero-trust going forward. And as I also mentioned, A lot of our customers are saying, well, why not -- why don’t I have an SD branch, which includes 5G and switching and almost campus as well.

And on the right-hand side is what we’ve been working on. You saw a couple of acquisitions over the last 12 to 18 months, which gives us that capability in the cloud as well. So this is FortiOS on the left-hand side, sits in our appliance. On the right-hand side, sits in the cloud and capabilities there. We think we focused on secure gateway, CASB and zero-trust. We do think that marketplace is more focused on remote access initially, and maybe FinEdge from 5G. But we do believe those 2 things need to work together. So there’s an intersection between those. And I think Robert talked a bit about that, but you need this single console and ability to manage between your SD-WAN network. And if you want to call it SASE network, call it SASE network, I don’t like that terminology, but that’s the important thing going forward.

And I -- and so again, some vendors think I can just be a cloud, and that’s all there is. We definitely think you need both that on-premise capability and networking to provide a digital experience as well as the cloud component. And then on the pure networking side -- that’s SD-WAN. On the pure networking side, and I don’t think this is well understood by a lot of people. That our goal is not to be a networking vendor and provide fast switches and fast APs. Our goal is to provide secure networking equipment where we can apply security to any switch port.

If you go into our management console today, a FortiGate console, you can see all the switches inside there. You can configure the ports to have security. You can configure micro segmentation across those ports, the same on the AP side. So our goal over the last -- since we started the switching and wireless business is to keep building that security capability inside there at greater speeds and greater capability. And then again, evolve that to what we think the next generation capabilities are around AIOps.

So yes, we have a networking business. But in our mind, it’s a secure networking business, not just a pure networking business. It’s not that often that someone comes and said, “Oh, I just want your switch.” They want a secure switch.

Well, so here’s the -- I’ll come to your question in a second, so here’s the capabilities of our enterprise networking portfolio, which includes access points, switches, NAC. I talked a bit about the Linksys HomeWRK, our FortiVoice, our SD-WAN and our 5G, which round off the complete portfolio.

Question?

QUESTIONS AND ANSWERS

Darren R. Baker - PRIMECAP Management Company - Financial Analyst

Darren Baker with PRIMECAP. I wanted to kind of follow up on this topic, but also related to what Fatima was asking, right? Because when we look across this space, you look at the people who are networking vendors, who are leading vendors in the space and they’re growing maybe single digits, right? And you guys have had a very consistent trajectory of growth. And honestly, some of your best numbers since your IPO -- have been in the last few quarters, right? And product is leading the way there with a lot of hardware sales and things. And so I’d love to just get a little bit more color on kind of what you think is really motivating that?

When you have people who maybe already have networking gear because they need it, are they adding in security in places where it didn’t exist before branch offices or things like that? Are they adding your devices in place of some of the networking because they get all these additional
capabilities on top of it? What other things are motivating those customers that's driving that kind of growth for you guys when a traditional networking vendor is not seeing that kind of new hardware adoption?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. There's a few factors. There's also the -- if you look at the network firewall marketplace, I think long term, there's probably only 2 vendors in that marketplace. So I've seen some of the traditional networking vendors fall so far behind.

I mean some of their platforms are 10 to 15 years old. At some point, the customer goes enough is enough. I got to upgrade. So I see some kind of taking market share from digital marketplaces. I've seen a lot of SD-WAN implementations where they want to put security on there. As I said before, I was starting to see a lot of OT environments because the problem with OT is during the pandemic, they had to open up firmware mode access.

I've spoken to several manufacturing customers where they got infected through their supply chain. One manufacturing customer had 3,000 suppliers that come straight into the network and update their machinery, and they got affected twice for those vendors. So that's a big new marketplace as well.

So yes, as I said before, there's some traditional marketplaces like some maybe core data center that's moved, but there's so much more new opportunity. And I do think that having that built-in security at high performance puts us at such an advantage over a traditional networking vendor or security vendors. And most of the -- 99% of security vendors are software. They don't make any of their own hardware. Even though the claim they've got ASICs inside there, don't have their own ASICs inside there. They're just off-the-shelf stuff. So I think that's where we're winning in both the networking and network security marketplaces.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

Okay. One quick comment for those of you that know that the video wasn't working, it should be working now. For those of you who just got in and missed my presentation, there will be a replay. And so we'll have the first 30 minutes of this as part of the replay. I apologize for you not being able to get in. But...

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

That was my best piece, Peter, though.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

No. Well, you're still going to be in the -- your first 17 slides, and we got another 17 to go. So your first 17 will be in the replay. I apologize for those people virtually who couldn't get in. Also, as a reminder, which I think we made a statement at the beginning of the call, if you have questions, John is doing a more interactive presentation online. If you have questions online, you should be able to type your question into the app, and we'll ask it here on the microphones or you can e-mail me directly, which many of already have. So I know you have my e-mail address.

Andrew James Nowinski - D.A. Davidson & Co., Research Division - Former MD & Senior Research Analyst

Andy Nowinski with Wells Fargo. I just want to follow up on the questions on the networking vendors. If you look at one of the prior slides and one that was presented this morning, it showed, obviously, Fortinet shipping a lot more units than the other vendors, but Cisco seemed to flat line through 2021. Checkpoint obviously lost, had a decline in units. But why do you think -- if everyone talks about taking share from Cisco and the networking vendors not doing well, why do you think Cisco's firewall units have basically flatlined? And that -- it doesn't appear to have [large share].
John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. I can't talk to Cisco specifically. I do think that we've really focused on that price performance, most recently on the supply chain and delivery. I think some of the market stats either from IDC and Gartner, sometimes they're not always accurate per quarter. Eventually, you don't lie, and that catches up over per year. And so we're very confident about taking market share from our competitors, and that will show eventually inside the analyst reports.

Because if you're a big company, I've got lots of buckets of money, I can move around in different places. We can't do that. We show where our network security money is, and I think that's very evident in the market share and we'll continue to gain.

Andrew James Nowinski - D.A. Davidson & Co., Research Division - Former MD & Senior Research Analyst

So it sounds like you're taking share from Cisco, both networking and firewalls, but it doesn't show it yet?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

I don't want to pick on Cisco because they're a big company. They've been a good company for a long time, so I don't want to really pick on competitors. I think we're taking market share from quite a few different networking and network security vendors out there.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

One more, do you want to keep going? Or you want to go back to your thing? I know Saket had a question. I saw his hand up earlier. One more?

Saket Kalia - Barclays Bank PLC, Research Division - Senior Analyst

Saket from Barclays. John, I want to marry together a few of the questions that were asked and just kind of ask this maybe rather bluntly. But can a firewall replace a switch or a router? I mean, when we think about just the convergence of security and networking, is the FortiGate firewall actually taking share from that separate TAM? And -- right, that's the first part of the question.

The second part of the question is, how do you -- how does Fortinet remake that market, right, economically? I mean, do you charge more for something like that because it's got more security in it? Do you charge less for it just to disrupt the market? So maybe just those 2 things.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

All right, just 2 things, 2 questions. Okay. So 1.5, I mean, because but beyond 2 and 3/4.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

So the first part of your question is the FortiGate isn’t a switch, okay? But the FortiGate is a switch controller, okay? So we can control the switch. It can define the policies for the switch. You can define what ports do, access control. So the brains as it with the switch is in the FortiGate. So you still -- that's why I call us an extension -- platform extension because I've got a FortiGate here, and I need to add some access points. You can see some of access point here. It's a physical access point you need to add or as a switch in our IT (inaudible) there. It's a physical switch on it. But that access point and that switch is controlled by the FortiGate software. It defines a policy for it. That's what we call an extension, you're adding capability to it.

Now of course, I've forgotten your second question.
John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. Well, it's addition. So sometimes when we've got an SD-WAN deal and they say, well, we want to make an SD branch, I've got to add switches, I've got to add access points, maybe add 5G connectivity, it's 2, 3, 4x. And that's why you're seeing some of those numbers just dramatically increased. Okay. We scoot along here. And yes, so we've done -- as you know, done extremely well in SD-WAN. We think it's a very important marketplace. We think it's a foundation going forward. And so you've seen our market share numbers, you've seen our growth.

And then what we're starting to see is customers start to add some security to the SD-WAN network. So again, initially, it was a networking decision, networking -- buying center. We're starting to see quite an increase and people say, "Well, I just need to put at least maybe some base security in my SD-WAN, maybe not the full stack but I need some base security inside there." So we're starting to see a service attach because if you think about networking companies, their service attached only is service and support, which is a much lower number.

Our goal going forward is to not only provide civil support but provide security capabilities to networking as well, again, switching access points and SD-WAN.

PRESENTATION

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

All right. So zero trust, which we absolutely think is a really important concept. And so a zero trust marketplace is just dominated by identity and access management. NAC's quite small and OT securities are growing really fast inside there. OT security, now you could put in different places because a bit of it's endpoint, a bit of it's network, a bit of it's policy, a bit of it's identity, but we put it inside here. This is the OT security.

And then what we call traditional VPN and ZTNA. ZTNA right now is probably a small marketplace, probably 0.5 billion, but growing at 30% or 40%. And what is our strategy there? And Michael talked to this on stage, in his mind is one of the more exciting products as we going forward, is to merge this ZTNA and traditional or used to be called endpoint protection, now people refer to as EDR together.

And the reason we're going to do that is that there's a lot of information that can be exchanged that's very valuable. So if you think about a ZTNA solution, it's got an -- it's an agent, you actually -- if you can't get an agent on there, you need NAC, which a lot of people forget about. It needs a policy engine to decide what that user can do and what they can access. And then it needs an enforcement point. And that enforcement point, in our opinion, needs to be in as many places as possible close to the application, not in the cloud somewhere that's not close to the application. So if an application is on-premise, that's where your ZTNA enforcement point needs to be within the data center needs to be there. If it's in the cloud, it needs to be there.

So having that ZTNA architecture in place, then if we can start to say, for example, EDR, if you decide this end point is or has a virus or is compromised, I can immediately tell that ZTNA policy engine change the policy for that user, either don't allow access anywhere or allow Internet access. So the interchange of policy between components is so important going forward. So we truly believe that bringing together EDR as well as ZTNA is the best long-term solution to protect endpoints.

Yes, we can sprinkle in some NAC here and there to maybe for OT security. But making sure EDR at the endpoint, because you speak to a lot of CISOs that go, I'm just tired of having 9 to 10 agents on my endpoints. This is too much. I need to get it down. Now today, let's be honest, we have an EDR agent and we have a ZTNA agent. And rather like the management consoles, our goal is to make sure those agents come together long term. That can't be done in 6 months. That takes a few years to do.
But we believe the convergence of these 2 is very important. And by the way, we have a pretty sophisticated authentication, multifactor token offering that we connect inside there. But I’ll give you an example of -- and this is the ZTNA portfolio, obviously, it consists of our client, our proxy that can sit in the cloud, in the data center, on-premise. It consists of our token of FortiTrust, which is the new licensing system or authenticator on FortiSASE.

And we started this journey internally in IT inside Fortinet almost 18 months ago. And one of the first applications we did was actually obviously the most valuable piece of data and the most valuable people accessing that. What’s that? Our source code.

So we made sure all our developers were on ZTNA. The source code obviously sits in our data center. So when they access the data center, that firewall inside there has in-built ZTNA enforcement that only allows those people protected by ZTNA clients to access that source code. Because ZTNA, in our opinion, isn’t something to switch on with all the complexity of policies or the application movements, it’s something we’ve been doing over the last 12 to 18 months because each person is different and each application is different. And where you deploy that policy is going to be very different.

So I think this as a marketplace, ZTNA, I just say, is small today. Every customer I speak to once they get to ZTNA architecture at some point. They just find it very complex, given all the different pieces in place right now.

And yes, so we’ve already added almost 1,500 ZTNA customers in the last 12 months. All right. Any questions on the ZTNA stuff? No? All clear.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

One second, John, before you go ahead. A reminder for those people who are on virtually, the entire Investor Day slides will be posted on the Investor Relations website -- great time for the wind as well -- on the Investor Relations website after the presentations are done today. So you will get to see all of John’s great slides in the beginning as well as this entire replay of the event will be available later today on the website. So the 30 minutes that you weren’t able to see will be part of the replay.

Lastly, if you do want to ask questions during John’s presentation, you can type them into the app that you have, and we will read them from there. All you, John. Oh, we have a question up front.

QUESTIONS AND ANSWERS

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Thanks, Peter. By the way, that’s our green building. I thought the sun goes around there, the blinds go up and down.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

It wasn’t my mental telepathy is what you’re saying?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Everything is green.
Adam Charles Borg - Stifel, Nicolaus & Company, Incorporated, Research Division - Associate

Adam Borg from Stifel. Just on FortiSASE, right? Maybe talk a little bit more about your own strategy there, building out some POPs internally, relying on service providers and how that should evolve over time?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. Yes, a good question. So our long-term approach, we say long term is 2, 3, 4, 5 years, is that we truly believe our service provider partners are in the best position to provide some of that capability. They have the network. They have their points of presence. They have a local access. And so our goal is to, first of all, build our own FortiSASE as we call it and provide a global footprint, mainly focused on remote access initially as well as FinEdge, but that's able to connect into our SD-WAN network. And so we need to be able to build it and make sure it's working and functional. We've been doing that over the last 12 to 18 months.

But we have many service providers lined up who want to take that functionality at some point, and we'll transfer it across because they suddenly woke up and realized that they've OEMed a lot of other cloud vendors right now and now they compete with them.

They kind of knew that, I think, years ago, they maybe couldn't do and think about it. Now they definitely want to do something about it. And so we'll build our own capabilities out. But we're also, long term, we'll transfer that technology to service providers to allow them to compete as well. It's part of us being very partner-friendly, but maybe 3 or 4 years ago, we started to do that, but if you haven't built it yourself, it's hard to transfer something you haven't built.

So we decided almost when we did the acquisition of OPAQ and some other capabilities is to build it out, and that's in progress right now, it's progressing very well. We added ZTNA to it in Q1, which is a fantastic new feature for our users, and we'll keep building that out.

And to be honest, it's a very different development model as Cloud and SaaS vendors are, we have weekly releases for software because that's what you do in a SaaS environment. So that's why I asked Michael the question about the development developers. We have different development teams who have different skill sets because a SaaS implementation is very, very different. The way you build it, the way you operate it, the way you control it from a 4-, 5-year development around an ASIC, extremely different. Did I answer your question?

Roger Foley Boyd - UBS Investment Bank, Research Division - Associate Analyst

Roger Boyd with UBS. Just going back to the question on AIOps and considering that kind of partner-friendly SASE zero-trust product. How do you think about who owns the data? And can provide that value from looking at data and driving insights from that?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

So when you said the data, you mean the data, not the customers' data or the data from the network and the applications and the security?

Roger Foley Boyd - UBS Investment Bank, Research Division - Associate Analyst

Just collecting like telemetry data, really, you're talking about 100 billion telemetry events a day or something.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Okay. Yes. So there's 2 pieces there. So the first one is that all our customers have the option to -- they opt in to providing data on our FortiGuard services, and that gets sent back into us, into our POPs around the world. And then we apply machine learning. So it could be that I've got a file in
the sandbox, for example, or I've got a hit on an IPS or I've got an AV file, they provide all that telemetry back into our core data centers. And then we provide -- we attach machine learning to each one because each threat act is different.

I've got a file that's very different from a URL. It's very different from a vulnerability. And so each of those threat vectors is very different from a malicious piece of e-mail. We take each threat vector in. We apply machine learning. Machine learning today is very much focused on good or bad. So for example, a file, we'll pass it through 2 billion good files and 4 billion or 5 billion bad files, and we get a pretty accurate view if that's good.

The key long term is taking all those threat vectors. And then applying AI to detect some sort of campaign in the wild. That's the end goal for everybody. If I can detect a campaign in the wild, and I know where it's going to attack you and how it's going to spread and where it's going to go and who is going to go after, that is the key.

Because you're going to tell a customer, by the way, this person is going to try and get in through here. If they get in, they're going to go over here and they're going to do XYZ, and they're going to try and get this information or they're going to try and lock your manufacturing plant down. I think that still evades most companies, especially companies who haven't got all the threat vectors, you need all the threat vectors because a life cycle goes across all of those. I still think it's a bit way off even for us, given the amount of compute and data you need to apply there. But that's our goal in getting a lot of data. But you need all the data. You need it from the endpoint, you need it from the network. You need it from e-mail applications everywhere.

Right now, we're applying a lot of machine learning, but our goal is to provide AI against that eventually to hopefully be able to detect campaigns in the wild. Okay. Question?

Unidentified Participant

Just had one quick question about ZTNA. So it sounds like you're using that proxy predominantly for remote users today. Do you foresee -- or are you already seeing that use case being extended to branch offices? And how do you think about that potentially cannibalizing what's already a really strong branch firewall business?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. It's not a good diagram, to be honest. But the SASE is for remote users today. ZTNA is for everyone on the network and off the network. And so I am -- we have controlled access to some of the product management systems in our data center.

I have some product marketing systems in AWS. When I'm off network, my ZTNA policy provides enforcement of the network and the same enforcement on the network. So if I'm on the network here and my FortiClient isn't talking to our policy engine, I can't access that either.

So ZTNA, I call it a -- that garden have a term called Universal ZTNA, which is ZTNA on the network, off the network for applications in the cloud, in the data center and on-premise. That's the end goal. And so it's SASE -- on the other hand, SASE right now, we've really focused on remote users. Eventually, and that connects into 5G, eventually, that will be universal, but ZTNA is absolutely universal across on-network, off-network and applications in every location. And that's really important. Did that make sense?

Unidentified Participant

Yes. What about the canalization between LAN? Maybe you have appliances at the branch office already? All of a sudden, maybe you're using more of a cloud-enabled SASE model. Does that cause any friction over time between what's already a strong appliance business?
John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

No. I mean you'd still need SD-WAN, so that isn't going away. You still need to have an efficient connectivity. So we still have SD-WAN there. In the future, how much security do put on SD-WAN device versus our own SASE cloud may change. But we always have a presence there. And it's the same -- look at it this way, so 5, 10 years ago, our firewalls provided firewalls, maybe some IPS. Today, they provide SD-WAN SSL inspection. And we just added a new application, ZTNA proxy, that door's loud, come in.

So all our firewalls now can do ZTNA processing, which is another application sitting on the firewall. I've heard some people talk, well, firewalls can't do ZTNA. A firewall's part of the ZTNA, it's not into all the ZTNA, it's the proxy enforcement and you've got policy and then you've got the endpoint. But as I say, our network internally, all our firewalls, both virtual and in the cloud and our SASE have ZTNA enabled to provide that enforcement.

Intiaz Ahmed Koujalgi - Guggenheim Securities, LLC, Research Division - Director of Technology, Media & Telecom and Analyst

John, it's Taz Koujalgi from Guggenheim. I have a question on ZTNA and how you reconcile that with the VPN because one of the things that we've heard from many vendors and many industry analysis as ZTNA is kind of -- ZTNA and VPN. Your approach to remote access is based on getting on the VPN remotely from a remote location. How do you reconcile the zero trust concept with the fact that most of your, I guess, remote access technology still bit in VPN and networking, right?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

No, I think Robert's demo was pretty good showing that. So he actually showed a VPN agent calling -- going into a data center, traditional VPN technology. And by the way, a lot of the zero trust could be done today through firewall technology in the data center, just people didn't get around to it. So they just said, "Oh, just go wherever you want when you get there." And that's one of the issues of VPNs. But we upgrade that client to a ZTNA client. We upgrade the firewall to ZTNA proxy enforcement, ZTNA's there straight away. Now some of the applications have moved into cloud and SASE, so we're going to need more ZTNA enforcement in the cloud and over here. So going always to that firewall in the data center, you can go to the virtual firewall in AWS or Azure or you can go to our SASE firewall, so we've just expanded it, but it's a very easy upgrade for us. It's just an upgrade of the client and the firewall.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

I think that's a common question that we do get is sort of the VPN going away, being replaced by the proxy capabilities for connecting to branches and things like that.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Right. But remember, VPN technology was pretty straightforward. You had a client and you had a data center concentrator, where all the policy was, everyone have the same policy. You just switched the VPN on, you add the IP address and you went to that concentrator in the cloud in the data center.

Going forward, when you upgrade that to ZTNA, you also need to add a policy engine as well because that policy engine is to decide which applications you can access and where you can access them, even how you can access them long term.

And as I said in my presentation and the Gartner mesh, 3, 4 years from now, if we're going to provide context to that as well, that's the key. Because in no way does anybody outside your company know the context of what you're doing, why you're doing it, when you're doing it, where you're doing it. So when you provide that contextual engine to the ZTNA policy engine, the transmission and the interface and the transport is the same technology in a way, encrypted tunnels go into the data center or the cloud or to the SaaS. So to us, it's a very simple upgrade of our existing VPN technology, and that's why you saw those 1,500 customers already upgraded to ZTNA.
Unidentified Participant

(inaudible)

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

It's always hard to tell. I mean, PowerPoint is very powerful. It looks good. I don't really know if they've done it or not. For us, it's at least a 3-year development. For us, it's the policy engine and also making sure that works inside our OS.

Now those traditional vendors who had a VPN, let's say, I've got a networking vendor at a VPN. That's not their firewall. It's something completely different. It was a completely different device doing VPN concentration. It was dedicated to doing that. In fact, we replaced a lot of these VPN concentrators because our performance was so huge on IPSec that we could do -- we want to replace the rack of gear with a 1 new box -- was that big difference. But going forward, that's not just the only thing you need, you need that policy engine to decide where customers can go and the employees can go. So I don't know the answer to that question, to be honest, but I think it's hard to do.

Patrick Edwin Ronald Colville - Deutsche Bank AG, Research Division - Research Analyst

Patrick Colville from Deutsche Bank. So the message today has been all about platform. Platform, platform, platform. Fortinet is clearly seeing a lot of success in platform and with a platform message. I think one of the things that would help us as to how do you conceptualize security platforms today in 2022 versus the security platforms we saw 10 years ago with like Symantec, McAfee and Cisco? What's changed between now and then? And why -- and I guess, how is this platform message going to be durable?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. I think...

Peter M. Salkowski - Fortinet, Inc. - VP of IR

I have one comment to add to that. The 3 companies you listed, how do they put their platforms together?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

If you go back and Ken knows as well, so you go back to 2000. If you go back then, the end -- I mean, I worked for an endpoint vendor before I work for Fortinet because back between 2000 and 2010, the endpoint vendors were the big cybersecurity vendors. You mentioned the McAfee, Trend Micro, all these companies. They were the big -- the network is much smaller than the endpoint marketplace.

And so you had an endpoint platform, and they try to bring more endpoint functions and trying to expand a bit, but they never really got beyond endpoint. And then between 2010 and today, I suppose, the networking vendors came along and said you need a networking platform. So there's us and there's some people down the road there apparently that do networking, network security. And network security overtook endpoint as being a larger marketplace. That's somewhat swung back to endpoint recently an endpoint actually will take a network security game.

But the key for a platform long term is not just endpoint, not just network, not just cloud, it's all 3 of those working together. And that's the key message for us. It's not just network endpoint platform or it's all of those things together as a combined platform with a single policy engine across everything. That's the key. That's the difference, I think.
PRESENTATION

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Keep saying hurry up. All right. So cloud, I’m going to -- cloud is very, very fragmented. This is going to be a very interesting marketplace going forward. No one really knows the size of the cloud security marketplace. I’ve seen guesses all over the place. Always a $500 billion. Oh, no, it’s only 20. We don’t -- no one really knows. And so I don’t think there’s a good estimate of how big it is. These are some of the major marketplaces, which are considered cloud.

You’ve got CASB, which, in fact, if you look at Gartner, their cloud market is based on just CASB, that’s it. You’ve got e-mail security, you’ve got WAF, which is going to be very important going forward to secure API traffic. API traffic now has overtaken HTML traffic inside this environment, and that’s going to be a major attack factor going forward.

For us, this is our portfolio right now. So we have our WAF, which is really growing very fast inside the cloud to protect applications from botnets or attacks and applications and API in the future. We actually have a substantial e-mail security protecting some remaining on-premise e-mail. Most of the e-mail has gone into the cloud now.

We also have a cloud workload protection through an acquisition of FortiDevSec, our CASB solution, some smaller products around ADC. So we have a reasonable-sized cloud portfolio. But as I mentioned on the keynote earlier today, we definitely think going forward, you’re going to need to be very conscious of the cloud-native capabilities and make sure that’s part of your solution. Because in the end, the platform vendors wield a lot of power. My analogy is you go back to when I was at my endpoint company, it was a long time ago, there was a certain company called Microsoft who decided they wanted to get into the game. Now Microsoft own consumer endpoint with Defender. In the end, they’ve got so much power. So you can’t ignore them and say, oh, we’re going to compete head to head.

You’ve got to be able to take advantage of some of the capabilities they’re going to build and they’ve already built some security capabilities. But the one thing they won’t be able to do is to apply that same capability across other clouds. So this multi-cloud, hybrid cloud is with every customer I speak to. It’s got multiple clouds. And even if they signed a $500 billion deal or a $1 million deal to take cloud from a certain vendor, they’re always going to have multi-cloud. So I think this cloud world for us, we’re building our own products, building capabilities to take advantage of cloud-native and bring that together. And that’s the product we’ll announce probably in a couple of months.

And again, some really good numbers here in terms of cloud, in terms of our growth across all the different product areas.

So yes, we do talk a lot about hardware and ASICs and everything else. We do have a thriving cloud business, and we do invest in the cloud business.

All right. And then I think we’re going to finish up on our other -- the fourth part, which was the security operations. So this portfolio or this TAM is pretty large. Obviously, endpoints inside there that makes it very large. But you also have some of the new technologies around SOAR network detection and response and also threat intelligence.

And our portfolio was pretty substantial. And in fact, if you look at the slide that Ken had on acquisitions, maybe half of those were security operation acquisitions. The SIM, the SOAR, most recently is our attack -- enterprise attack surface monitoring tool, just about to announce that’s FortiRecon by the way, that tool there. That was the acquisition of (inaudible).

And so what we’re seeing is if you look at the attack life cycle, we started to implement some more capabilities in the front end, that can see what’s going on. It’s very unknown. It’s stuff like deception or things that look for a lot of behavioral type capabilities.
Now what you can’t do with all of those products is block. You're not 100% sure, you can’t be blocking across that. So what we hope to do is build those tools out and then if we transfer them into what we call our Protect, and the latest change to this was sandboxing, which previously has just been detection. I found this file, it’s bad. It’s already gone. So we just added in-line sandboxing protection. So once you get more certain about that capability, you can add protection in there versus just detection. And again, Kennedy’s slide about the number of detection vendors, protection vendors, it gets harder and harder as you need to do that at high speed and you need to be really sure you detected something bad because you don’t want, of course, false positive inside the network. That’s a disaster.

And then, of course, we have our SOC capability, which ranges from our SIM, our analyzer, analytics, new SOC-as-a-service, incident response. And so this is a very broad portfolio that’s really focused on the SOC and the CISO from a security operations perspective. And I think that could be it.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

John, just a question that came in online. Okay. I’m not exactly sure if it fits right in because I've been jumping around here. But the question is, can you give some more concrete examples of how you can’t coexist with the cloud-native platform vendors and maybe how you delineate their role versus yours?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. A good example is our WAF rule set. So I think what the platform vendors are very good doing is taking some basic function and making it ready and available. And so all the cloud vendors have a WAF, web application firewall. AWS, Azure, GCP. And so what we did inside AWS was if you’d already have an AWS WAF, you can opt in marketplace and click on advanced WAF rule set from Fortinet. And that gives you updates of our bot nets, about attacks, vulnerabilities, and that service is doing extremely well. So for the customer, that have kind of taken a basic cloud-native functionality, but they've added on functionality from us that makes it better and more sophisticated. The same will happen when they introduced -- they've already introduced basic firewalling, they haven't got the capabilities to add that next firewall on top of that.

The other capability, long term, will be, not only am I providing functionality on top of that cloud-native functionality, but I'm also sucking information in, from the cloud-native capabilities. Like all the cloud vendors have got vulnerability scanners, why build your own vulnerability scanner? Just take the information from them and bring it in. So it’s a combination of working on top and with and then alongside the cloud-native capabilities, but you need to do it across all the clouds. You can't just focus on one cloud. All right. I think it might stop there, actually.

Yes. I’m going to, I think I might stop there. There's our management systems. And I think I talked a bit about which we think is really exciting technology is the AIOps and the monitor. Monitor was an acquisition in Chicago of Panopta which is digital experience monitoring. We feel like long term, the network operations teams will want this functionality to be able to provide to their CIOs what the digital experience is.

Once you have that in place, then you start working on AIOps, and AIOps is not one of those things, again, you're going to switch on, it just looks after the network and you go home and that's it. It's going to be a road map and the evolution of functionality across both end point network and the cloud.

Okay. I got to Slide 36. It's pretty good. Some really good question, though. Any other questions from me?

Peter M. Salkowski - Fortinet, Inc. - VP of IR

Yes, we've got a couple of minutes. We can take a couple more questions, and then we're going to turn it over to Keith.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Well, Keith always needs extra time because he talk slow.
Peter M. Salkowski - Fortinet, Inc. - VP of IR

Yes. I have a surprise for you, John.

QUESTIONS AND ANSWERS

Fatima Aslam Boolani - UBS Investment Bank, Research Division - Former Associate Director and Equity Research Associate Technology-Software

Hey, John, Fatima again. In the same way we've seen the convergence of networking proper with security proper, do you anticipate that we -- in the next couple of years as these previously independent disciplines as they fused, we're going to start to see the NOC and the SOC actually become 1 singular entity. Why or why not?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes. We've heard about that for a long time. In fact, the acquisition of -- we acquired a SIM -- what was the company again SIM company? It was on that slide anyway, but they were one of their...

Fatima Aslam Boolani - UBS Investment Bank, Research Division - Former Associate Director and Equity Research Associate Technology-Software

I think it was AccelOps.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Yes, AccelOps. I knew that. I was just testing you, bingo. So I was paying attention. So they actually -- one of the key features was NOC and a SOC combined together. And so -- but I also see a lot of customers the main -- large enterprises for sure, it's just very separate.

But again, I think this convergence and consolidations are 2 different concepts. Convergence is I'll take 2 products, and I'll make it into 1. Consolidation is I've got 3 vendors, and I'll make it 1 vendor. That's kind of different. I think network and security is converging. I think security operations is consolidating, a slightly different concepts. One is a platform approach and one is an OS approach.

Gregg Steven Moskowitz - Mizuho Securities USA LLC, Research Division - MD of Americas Research

John, it's Gregg Moskowitz Mizuho. So a question going back to secure switches and access points because, some have the viewpoint that -- and you sort of alluded to this, that it's a very commoditized area, really not much opportunity to differentiate. Now you talked about naturally the integration to broader portfolio, including FortiGuard and a lot of the intelligence that you're switches have. I guess I'm also curious, since we're talking about some recent M&A what haven't talked about is ALAXALA from last year. And I'm curious, naturally, that has given you more of an inroad into Japan. But I'm kind of wondering if there's any IP from the ALAXALA acquisition that you can actually apply, thereby potentially further strengthening your switching and access point presence in the marketplace.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Good question. I haven't covered that piece. But -- so today, intelligence is in our FortiOS operating system in FortiCare. Yes, we have communication links to the switches and APs so that we can't tell it to provide more security, but the intelligence is not in the switches.
The piece that we've built is the ability for the switches to communicate that intelligence. So ALAXALA, I mean, has built switches in a traditional way. I think our area which we were kind of missing from a coverage perspective was the data center. And so if you look at switching as 2 distinct markets, there's a campus and the data center, very different marketplaces. And so we didn't really play in the data center per se. I think I was going to give us the capability to play in the data center long term, but it also probably means a more integrated architecture.

I'll just leave it at that as we go forward because given the performance criteria of a data center, you probably need things more integrated together versus my AP talk about FortiGate somewhere else, and that's okay because of the speeds are in tens of gigabits versus terabits. Yes, that's definitely part of the strategy long term.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

So I have one follow-up question from online, which the good news is people are online and I can see it now. But Slide 29.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Just now?

Peter M. Salkowski - Fortinet, Inc. - VP of IR

They've been on for 0.5 hour, 40 minutes. But Slide 29 apparently had some good stats, 32% growth in FortiWeb and 52% growth in cloud and virtual, and the question is really just ballpark, how are those businesses in terms of Fortinet and kind of round numbers. I wouldn't necessarily give numbers. Because we don't give to that level, but -- part of our...

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

So Keith is over here.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

Well, kind of get into like...

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

So I think what we're doing right now is we're saying here's our new kind of structure of what used to be FortiGate and non-FortiGate and we split that into core and extension. The extension is networking, zero trust access, security operations and cloud. And that's as far as we're going right now.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

Okay.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

And then we'll give you some stats of growth for the components inside there. Long term, we hope, but we'll be ready, we might break those out to show you some of the components inside there, but not at this point. Is that good answer, Keith?
Keith F. Jensen - Fortinet, Inc. - CFO & CAO

You did very well.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Thanks.

Intiaz Ahmed Koujalgi - Guggenheim Securities, LLC, Research Division - Director of Technology, Media & Telecom and Analyst

John, it’s Taz again. Your -- you've had a lot of success in the last few years converging networking and security, and that made sense because you're the only guys who had both networking and security, while Palo and Check Point were mostly security and firewall vendors. But when you think about the classic network vendors like Juniper and Cisco, they've always had security and networking under the same umbrella, but they never had the convergence that you've got -- you've had in the last couple of years. They never see the success of integrating security and networking like you guys have. Is that more of a product saying that they missed or was the market not there yet? Why did you guys have the success in combining or converging those 2 areas while Juniper and Cisco were not able to.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Because it’s hard to do if you're not innovating, they just won't buy. And I'll give you SD-WAN as an example. We could have gone on bought it and it's why we wouldn't have bought it because there was ridiculous valuation. So let's stop there. But we could have built it on a separate box. It would be much easier for us to do, much faster, maybe some code. Here's a separate box. And even the largest networking vendor in the world couldn't build it internally.

They went and bought something from somewhere else. Then they go, well, can we try and make that work with our firewalls? No. It's really hard to take mature products that's got roadmaps and customers and everything else, and bring them together as a converged solution. You can't do it.

Yes, you can't make it look that way by a console talking to each other. And if you go back even further, IPS and next-gen firewall. Let me go and buy an IPS system instead of a firewall system, let's see if I can't bulit a firewall on top of an IPS system. No, it's really hard to do. And it's really hard to do not only in terms of functionality, but high performance.

Some of our latest firewalls are running 400 gigs per second per port. You can’t do that when you bolted some virtual machines together. It’s impossible. So I just think the strategy is incorrect and that one of the issues is that internal innovation has died. So you’re not building it internally, you’re going and buying pieces all over the place, and then innovation is trying to make it work together, and I think that's really hard to do. Really hard to do.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

On that note. I knew we could do it. I knew we could fill 1 hour in 15 minutes. That wasn't going to be a problem with the Q&A. John, thank you very much for your presentation. You'll be back later for the Q&A in 15, 20 minutes, but thank you very much.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Okay. Very much appreciated.
I told you there were more slides. These will be posted, but I'm just going to fast forward to -- no, not there. Well, I thought you were going to move it. Can you move -- can you take me to Slide 2? Okay. Because I have a surprise for those of you all in the room.

First of all, just to remind you for those people that are online that got in late, there will be a replay of the entire Investor Day presentation. So John Maddison's is our in 15 minutes and soon to be the rest of the presentation, will be webcast, will be replayed, will be available. We will also post a transcript later today as well as all of the slides.

But more importantly, as I wait for my slide to show up. I can, and I'm going to. I know it's a surprise. But for those of you got the sense we didn't have the video playing in the beginning, we've got to review the safe harbor slide as soon as they can't get it up there. There it is. Read it in your -- before I turn the call back over to Keith, I'd like to remind everyone that during today's Analyst Day or during this part of the Analyst Day, we will be making forward-looking statements and those forward-looking statements are subject to risks and uncertainties, which could cause actual results to differ materially from those projected. Please refer to our SEC filings, in particular, the risk factors in our most recent 10-K and 10-Q for more information. All forward-looking statements reflect our opinions only as of the date of this presentation, and we undertake no obligation and specifically disclaim any obligation to update forward-looking statements.

With that, we're going to turn it over to Keith, hopefully, they can't throw -- Jamie. Hopefully, you can't throw Keith's presentation up. Just the agenda items for everybody that knows certainly the people are on line that didn't hear it. After Keith's presentation, we will bring up Ken Xie, my Founder, CEO, Chairman, Patrice, our Head of Sales, John Maddison will come back. And of course, Keith will be here as well. Just wait, Keith, they're going to throw it up there to the beginning yours.

Never stop hitting the button.

Yes, in going to go. I think they just throw it up there.

Okay.

This will give you all time to read it in its entirety. Want me to read it out loud like a poetry reading, wouldn't that be fun, information states and projection came in the presentation. How fast can I read it. Slides concerning Fortinet's business outlook, second quarter and full year guidance. Guidance, 25 -- wait, 2015 financial targets in future there we is -- now it just -- I know I do the safe harbor statement on the earnings call as fast as I can, but anyway, you're welcome. I think you're on about Slide 39 or so for Keith.

The last thing I would offer is that what we have not yet been exposed to is that the windows will actually open and close automatically based upon temperature experience, typically happens about the most important part of this presentation. And the mid-year guidance will be...
Peter M. Salkowski - Fortinet, Inc. - VP of IR

Fortunately, these windows don't open in this room, particularly, but that is true in some other parts of the building. Okay, all yours.

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

Let’s see. Thank you, again for everybody for joining us. Appreciate you being here earlier this morning as well. I'll take about 15 minutes here and then we’ll pivot back to Q&A.

If I take a look at the agenda, I’ll begin by highlighting our investment thesis, discuss several of our industry and company-specific growth drivers, review our financial performance over the past several years and then offer some observations about the supply chain.

I’ll wrap up by highlighting the cash flow generation, capital allocation strategy. And then I’ll conclude by updating our medium-term financial guidance. And then maybe after that, Ken, John, Patrice will join me as well as Peter and we’ll have some more conversation.

As you know, cybersecurity is a very large and fast-growing market with growth being driven by long-term secular tailwinds. Our business is driven by our ASIC and operating system advantage, they combined to form our platform strategy and provide customers a lower total cost of operating operations and a sizable performance advantage.

The highly diversified nature of our business model across customer sizes, industry verticals and geographies has enabled strong and consistent financial performance over the past several years. Doesn’t work with a clicker. All right.

Our financial strategy, as a publicly-traded company, has been balanced growth and profitability, including last week’s 2022 guidance, Fortinet is expected to achieve the Rule of 40 in 8 of 10 years and 11 of the last 14 years as a public company.

In 2021, we hit the Rule of 55 and last week’s guidance indicates we should hit it again this year. In some ways, the Rule of 40 has become easier for Fortinet as it scaled and expanded from its early days as a single product company to the cybersecurity platform company that it is today with product and service offerings that extend well beyond the firewall.

At the core, platform are the high-performance ASIC-powered FortiGates serving a number of different use cases from data centers to branches and from SD-WAN to OT. From this core, the platform extends their products in 7 different Gartner Magic Quadrants and a full product suite that appears in over 20 Gartner research categories. Our suite of platform extension products has grown to be over 30% of our business.

Based on Gartner projections, as we talked about this morning, we estimate the cybersecurity market that we play in will grow at 10% annually over the next 4 years. It will approach $200 billion by 2026. Keep in mind these TAM estimates are products only. They exclude the over 60% of our business related to services, FortiCare and FortiGuard.

Our continued focus on organic innovation means we will continue to add capabilities to our core platform and platform extension, including Zero Trust security, cloud security and fabric operations, the security operations. Our solutions include a complete range of form factors in delivery methods including physical and virtual alliances, cloud, SaaS and perpetual software as well as hosted and non-hosted solutions. Together, they provide security solutions, enabling broad, integrated protection for hybrid environments and the expanding digital attack surface.

Next year, we're going to put a monitor in the back, so I don't have to do this each time I say adjust the slides. Thank you very much.

All right. Fortinet's almost all organic billings growth accelerated from 19% in 2020 to the mid-30% last year, closing 2021 with billings of over $4 billion. Contributing to the 2021 growth, cloud billings grew approximately 40% to $325 million. And last week, we guided 2022 billings to be over $5.5 billion. representing full year growth of 32%. Over the past 4 years, product and service growth has remained balanced at say, 29% to 28%, respectively, and services continue to account for nearly 70% of total billings.
Our revenue is highly diversified across customer services, geographies and industry verticals. The diversification you see on these charts largely contribute to the consistent performance over the past several years.

Illustrating our customer segment diversity over the past 5 years. Again, no single customer has represented more than 2% of our billings in any quarter over that 5-year period.

The geographic diversification you hear is very interesting. Over the last 12 months, we've generated almost half of our billings across more than 100 smaller companies with no single country representing more than 3% of our business.

It’s all of geographic diversity, which provides us the ability to mitigate the impact of country-specific events impacting the local economies, including the rotation of the pandemic, economic downturns and even conflict in Ukraine.

Looking at the industry mix, we see the top 5 are very consistent quarter-over-quarter-over-quarter at about 60% to 65% of our business. While we’ve certainly seen very strong growth in each of these larger industries, what’s interesting, again, is the mix from the other industries, which has increased to 39%. That’s up about 4 points year-over-year.

We've seen extremely strong growth here especially in industries that historically, may have invested have been more constrained with their IT and security budgets. We think that ransomware is changing that. Ransomware is much more industry agnostic.

Over the past year, we have seen significant security investments coming from customers in manufacturing, utilities, services and similar industries.

The diversity you see across the slide drives the need for a broad solution set as our customers are not easily pigeon hold into one size or one type of solution or buying only one form factor or one size of a security offering.

I’ll pivot now to review some of our growth drivers that contributed to our strong performance and that we expect will help to drive our market share gains going forward. As I said earlier, it all starts with adding new customers. Last year, we added over 23,000 new customers. That’s 5,000 more than the year before.

As we earn the trust of our partners and customers, solving use cases, consolidating more technologies and platforms, solving more of their business challenges, the partnership expands.

The bar graph on the right shows that in 2021, we increased the number of $1 million deals by over 60%. And the dollar value year-over-year increased by 70%. And the question was asked earlier. At the same time, we saw the large enterprise mix shift increase by 3 points year-over-year to 37%.

In the SD-WAN Fortinet is at the epicenter and showing dramatic growth. SD-WAN has shown to be the driver for both the networking and security markets and for Fortinet. We offer a unique product to combine security and SD-WAN functionality in a single appliance. And Fortinet is the only SD-WAN vendor in the leadership Quadrant for both SD-WAN and enterprise firewalls with the exact same product the FortiGate.

With these advantages, our SD-WAN bookings increased to 15% of total bookings in 2021 and again from almost 0 in 2018. In 2008 – in OT, we have something, I would say, newer on the scene, younger, it’s driven less by the ROI type model that you see in SD-WAN and more by the current threat environment. And it’s now at scale at 78% bookings growth and follows the earlier comments about ransomware and some of the other industries that we see are investing more in security, manufacturing and services.

Fortinet’s all organic revenue shows a 3-year average growth of about 26% and in 2021 accelerated to 29%. Last year, we guided additional acceleration with 2022 revenue of 31%. With the proliferation of work and study from anywhere, together with the worsening of the threat environment, security investments in spending accelerated as companies reconfigure the network architectures and infrastructures along with the security capabilities to accommodate an increasingly hybrid workforce, partially driven by the accelerated security spending, product revenue increased from 16% in 2020 to over 35% in 2021.
Over the 2-year period ending in 2021. Our higher-margin service revenue grew at a 2-year CAGR of 23%. And for 2022, we are forecasting an acceleration of service revenue growth to 28% as services continue to represent the clear majority of our total revenue.

I think you've seen these before. These 4 graphs illustrate the consistency of Fortinet's operational metrics, despite the COVID shutdowns, supply chain disruptions, conflict in Ukraine, the demand for exceeding supply, whether you're looking at discount rates, average contract term, renewal rates, or the predictability of our service revenue, each of these has consistently tracked within narrow bands over the last 3 years.

As we pivot to the supply chain, I'll come -- I'll offer some commentary about the supply chain, how we're working through information about backlog and the financial impact. Some of you may have seen this chart earlier today.

During our earnings call, we summarized some of the actions we've taken to mitigate the risk, including redesigning products and reprioritizing how we allocate the limited supply of components to finished goods, qualifying additional suppliers, shifting from ocean freight to airfreight and significantly increasing our inventory purchase commitments. That's that bar chart on the left that shows the increased level of commitment we've made to our suppliers from $300 million to $1.4 billion.

The increase reflects longer lead times as well as a read through in how we view the opportunities for growth over a longer period of time. The chart in the middle provides the backlog trend. It also offers a metric that provides sizing context. Specifically, we're seeing the net additions to backlog hovers around 9% of total orders each of the last 2 quarters. And below that, you can see the mix and the trend in backlog.

The last chart highlights the impact of one aspect of the current chain challenges, expedite fees, does not include labor or other component costs fixed rate or freight.

We've agreed to pay expedite fees to our suppliers to facilitate inventory deliveries in certain cases. And as you know, we have a price to performance advantage and like our competitors have taken certain pricing actions to offset a portion of these higher costs.

The key message here as we balance profitability and market share gains is that we have passed through some, but not all, of the higher supplier costs.

While product margins reflect the majority of our pricing actions to date, the tailwind to service revenue will become more noticeable as we progress through 2022 and thereafter.

In 2022, we expect a 25 -- we expect a 75% gross margin to be a headwind to our 25% operating margin, but to be mitigated by the service revenue tailwind and continued leveraging of our operating expenses at these higher topline growth rates.

At the same time, the 25% operating margin guide still provides room for increasing our topline capacity through continued investments in sales and marketing, products and other areas. In the end, sales and marketing accounted for just over 50% of our head down for the year -- at the end of the year.

When it comes to cash flow for the last 20 years since our IPO, free cash flow remains our most important source of capital. In 2021, we generated $1.2 billion of free cash flow and a 36% free cash flow margin.

To put our strong cash flow conversion into context, we've again benchmarked the free cash flow against the S&P 500 constituents. Our top 10 standing as a percentage of total of all S&P companies. We think it's a testament to our business model -- there we go -- our ability to maintain margins and efficient working capital management.

This capital allocation strategy is key to financing our R&D investments and small tuck-in acquisitions. Over the past 5 years, our innovation investment has totaled $1.4 million in R&D, engineers and salaries and $200 million in tuck-in acquisitions.
Our free cash flow generation has not been the result of letting up and innovation investments. We have over 2,300 engineers with software engineers accounting for approximately 2/3 of the total. So again, working on the operating system, working on the cloud and other software products.

As we work to transition to a more efficient balance sheet in 2021, we issued investment-grade bonds, totaling $1 billion with an average annual interest rate of 1.6%. During 2021, we repurchased 2.6 million shares of our stock for a total cost of $743 million.

As for our capital allocation, we have a clear hierarchy for uses of cash and our free cash flow in order, debt reduction, if necessary, reinvesting in the company through R&D, CapEx investments and other organic initiatives, investing in inorganic alternatives, i.e., M&A with a focus on smaller scale acquisitions and minimal execution risk, and returning excess capital to our shareholders.

Here’s a recap of our second quarter and 2022 guidance as we provided it on May 4. In order to achieve service revenue growth of 28% in 2022 for the full year, we expect quarterly service revenue growth to begin to accelerate in the second quarter, reaching the 30% in the second half of this year.

Just a couple of additional modeling points. And as a reminder, the Analyst Day slides we posted on our Investor Relations website later today. And now I’d like to share our medium-term targets. And I’m happy to say that the personal objective that Patrice said earlier today of $10 million in 2025 is consistent with the rest of the company.

All right. Over the past 3 years -- pardon me, over the next 3 years, we expect continued growth looking out at 2025. We expect billings to be at least $10 billion and total revenue of at least $8 billion. At the midpoint of the 2022 guidance that we provided last week, these projections equate to 3-year CAGRs for both billings and revenue of approximately 22% through 2025.

As for margins, we expect our non-GAAP operating margin to average 25% for the period from 2022 to 2025. We expect adjusted free cash flow at the margin to be in the mid-high 30% range -- mid- to high 30% range in 2025.

Okay. All right. And with that, I think it’s time to bring Ken, Patrice, John back, Peter for Q&A.
gross margins may be a little bit light because of the supply chain stuff and -- but OpEx has been very disciplined. I guess, how should we kind of conceptualize the next couple of years and the kind of subcomponents of the operating margin guide?

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

Yes. I think your -- I assume that's a question for me, not John. I think you've seen us guide again this year to -- we widened the range a little bit, I think, 26% in light of what's going on out there in the supply chain. I think we've seen clearly with the model, it is capable of producing increasing operating margins. And as we look forward over the next several years, and we anticipate that the supply chain environment and other factors may not be as challenging as it is today.

We did pull that back a little bit from what we think the model is capable of just to reflect what we are seeing today because we do not know when the supply chain challenges and such will end.

Patrick Edwin Ronald Colville - Deutsche Bank AG, Research Division - Research Analyst

Maybe address the averaging over 3 years.

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

It is an average, as you kind of alluded to. So I'm not necessarily commit -- we're not necessarily committing to 25% as of for each and every year, but we are saying 25% over that period of time.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

Which to remind everyone, if you go back to our 2019 guidance, it was in over a 3-year period, but we did a similar thing we said we'd average 25% over that period back then. So similar to what we did back then.

Brian Lee Essex - Goldman Sachs Group, Inc., Research Division - Equity Analyst

Brian Essex from Goldman Sachs. Maybe for Keith, as we think about some of those longer-term projections, Obviously, one of the ways that you've been able to -- or one of the ways that Ken has been able to differentiate the company is maintaining the hardware focus and the value of that ASIC's performance. How should we think about the contribution of product, service, maintenance as we kind of look out to that 2025 timeframe and the mix that you anticipate from a contribution standpoint?

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

Yes. I think that we've seen some very rich product mixes, particularly over the last -- comparatively speaking, over the last 2 quarters. I would say the model over a longer period of time does not contemplate that same level of richness, if you will. And I think previously, we've kind of been in a 2/3, 1/3 model between product and services, and we expect over time, it's going to revert to norm.

You may have heard the reference to software accelerating and also an inference that the pricing actions that we've taken in November of last year, August of last year and February of this year, but those pricing actions again appear in the product revenue line immediately or comparatively speaking.

In services, it takes a little time. We knew we were not going to get a lot of lift from the services even though the pricing -- the billings went up at the second half of last year and the first half of this year, but it takes a while for that to pull into the service revenue line. And you see that acceleration
that we talk about this year. Part of that comes from you're going to see the impact of the price increases starting to appear in the income statement. And not unlike what you saw with us when we started adding 25/7 support from our, pardon me, 25. Yes, all day support. That was a bit of a journey.

We saw the uptake and it was continual and we saw that our customer are switching over. In the same way, you'll see that here, not only as the new customers are working off a new price list, but our renewal pricing is also based upon the then current pricing. So we should start to see, again, like we did with 24/7, a bit of a tail to these pricing actions.

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

Yes. I think if we're looking at a Q4 to Q1 comparison, if you will, and I think it was 27% growth versus 24% growth. There's a number of factors that go into there, and I'll give some sizing to a few of those. One of those is we actually recognize revenue on a daily basis for services. And here's to think 2 fewer days in the first quarter than they are in the fourth quarter. So that's about 2% of revenue right there.

And I think we've talked in other places that impact on service revenue in the quarter from the attach rate, if you will, not the attach rate, but the registration lag was probably in the mid-7 figures, maybe to the low 7 figures in terms of a dollar amount. If you looked at -- this gets kind of complicated but trying to do the math out loud, the pricing impact on services versus product and how much of an impact it was. I would probably size that pricing difference at, well, the pricing swag, I guess, is probably close to $10 million.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

One way to think about it, if we have an average 27-month contract term in 1 month is — 1 quarter is 3 months, so 1/9 of a service contract is actually being recognized in a quarter over that 27-month period. And on top of that, only the new service contracts that are signed or the renewals that occurred would even be at the new price. All the other service contracts are going to be at the existing prices that were pulling them off the deferred into the income statement.

So to Keith's point, the 24/7 versus 8/5 move that we did a couple of years ago, that's still happening. That's still trickling into the income statement. But it -- we talked about it back then when you look -- go back and look at the comments we made in terms of what the mix shift was over time. And I think we talked about it for 2 years. So it takes a while for that to happen.

Saket Kalia - Barclays Bank PLC, Research Division - Senior Analyst

Saket from Barclays. Keith, maybe for you, just looking at the long-term targets from a different angle. How do you think about the — what are the new names, the core versus platform extension mix, right, sort of the 2/3, 1/3 that we have now. What do you sort of envision that mix looking like down the road from a high level. And then within the platform extension, do you sort of see the splits of switches and access points versus cloud versus all the other stuff sort of changing meaningfully as well?

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

Yes. I’m not going to put a specific number about it, but I do expect that the platform extension will continue to become a larger percentage of the mix of the business. And inside that, John and I have had this conversation, he violated the rule by giving numbers for specific products, which we said we were never going to do.
John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

I didn’t...

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

But I do think the -- we're optimistic there will be something to talk about in those areas in the future. We've talked in the past and if you kind of look at that extension the grouping of products in there. About 1/3 of that is software, about 1/3 of that are these access points and switches and about 1/3 or other products that we offer inside there. And that's been fairly consistent. But keep in mind, ALAXALA -- if you were to add ALAXALA's switches to that part of the business, you would get a little more of a lift on the switches and access points.

Jyhhaw Liu - Evercore ISI Institutional Equities, Research Division - Research Analyst

Irvin Liu from Evercore ISI. I'll leave my question as a jump ball for anyone to answer. So from a product innovation perspective, it sounds like you’ve been gaining traction in SASE as you’ve made several mentions during your keynote today and even featured it as part of your product demo.

So correct me if I’m wrong here, though, this is a bit of a contrast versus recent months where SASE mentions were somewhat sparse. And I don’t recall the term used during the last -- your last 2 earnings calls. So, can you talk about any recent developments here in your SASE offering or if there are any milestones worth calling out?

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products

Sure. So I think it's not -- nothing has changed dramatically. I think at this conference, we just wanted to make sure we cover as much as we could. We can't cover everything. And so we wanted to make sure that the FortiOS everywhere message got across, and that message is that we can deploy FortiOS as an appliance, the VM as a container and as a SASE-delivered. And we just wanted to make sure that message has nothing to do with any changes. We still want to build on our SASE, we still want to build out all of those products and those businesses.

Shaul Eyal - Cowen and Company, LLC, Research Division - MD of Communications, Security and Infrastructure Software and Senior Analyst

Question for Patrice. Shaul from Cowen. As we think about the mid-term targets that you've provided, in the context of your channel partners, the VARs, should we be expecting any change maybe also in the context to supply chain comments that Keith alluded to, anyone or any ones that you have been investing in, whether it’s in the U.S.? Or in Europe or we should think about your partners, your VARs, your channel picture largely intact for the next several years?

Patrice Perche - Fortinet, Inc. - Executive VP of Support & Chief Revenue Officer

So yes, I think the, let's say, the impact on the evolution on the supply chain, especially for the partner. We try to provide the best let's say, visibility if we can. It's always a bit difficult, but -- and we have been able to serve, let's say, slightly better than most of our competitors in this space. So I think we -- here, we're getting a bit of a better traction from the very large size worldwide because we're -- the opening door is this year to be able to deliver and match some customer requirements.

So I've said in one hand, that's helped to create a bit -- I'll say a bit more strategic and long-term engagement with those partners. And we also been able to -- it's a line a bit of our sales strategy with the -- especially for the enterprise segment as we have this direct touch engagement to really make sure we are going a bit more strategically with the partner we want. And before it was more like a bit of a broad -- whatever the choice of our rep. Right now, it's much more strategic to focus on the key partner in the U.S. and Europe.
So the discussion we’re having right now is those very large SI or service provider are becoming much more strategic at much larger -- I would say, larger scale term of projects or it's -- so he's more and more confident. It was a bit more tactical before and becoming more strategic today.

Unidentified Analyst

(inaudible) on guidance on the CAGR to the $10 billion and the $8 billion, this coming year, in the ’23, we will be getting something boost -- not huge, but something that boosts from the runoff of backlog. So how can you help us parse how much of that growth that we're seeing on a long-term basis and in '23 will be from that backlog, granted you know how fast will run off. How can you help us parse it today? And how will you guide us through that as we try to think about what the really sustainable organic growth of the business is post this backlog build?

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

Yes. I think there’s simply too much uncertainty around the backlog and when it’s actually going to turn around into the financial statements. I think when we look at our longer-term guidance setting process, it’s more about starting with, first of all, can I generate enough sales capacity to make those numbers, right? Am I going to be able to give Patrice and John enough dollars, if you will, while maintaining 25% operating margin on average, that he and his sales team maintain their productivity, and John can build the pipeline. I think that’s the first step that we look at.

The next step we will look at is what’s the TAM? How big is our market? And we know that we've gained market share, I don't know how many years in a row now for many, many years. And how much of a market share gain do I have to assume out of that almost $200 billion of TAM that's coming, how much do I have to get to make that number?

The distinction in terms of what may happen with backlog, either the ins and the outs of it, I think we set that aside largely, if we look at it for a longer term modeling purposes in terms of whether it’s going to be a headwind or a tailwind. I think we kind of really assumed as we get into those outer years, it’s more of a neutral proposition. If it accelerates, that would be fantastic.

Unidentified Analyst

Ken, my first question is for you. When I think about the success you’ve had with the secure SD-WAN strategy is the, basically a net new FortiGate use case in the last 4 years. Can you talk to us about the evolution of your relationship with service providers because as we understand it, it’s an ROI game for SD-WAN, and one of the areas where a lot of customers see ROI is from reducing their MPLS spend. So I’ve always found it interesting because your relationship with service providers has been very unique. So just wondering how you see that relationship evolving where you’re basically cannibalizing some of their business?

Ken Xie - Fortinet, Inc. - Founder, Chairman & CEO

It's SD-WAN a little bit different than some other 5G even DoT. A lot of SD-WAN deal driven by the enterprise. And because they see the cost savings. They see they can't offer more reliable, redundant, flexible service. Some bigger service provider, I have to say, they are a little bit hazy in the beginning because they get so much money on NPI service. So that's where some smaller service provider tend to be a little bit more aggressive. So they try to use SD-WAN to gain market share.

I feel 5G is a little bit similar since. So we do see a lot of our 5G requests, especially connect a lot of device, even certain vertical like manufacturer or the health care. So -- but I do believe long term, the service provider because they have the infrastructure, whether later earned the 5G or some other IoT space, they do play quite some important role. Even in some kind of a SASE.

So if we’re working with service providers still one of the key areas. So they are still one of the top 3. They tend to be the #1, if you look by 10 years ago. So that the carrier service provider almost across kind of 30% of our business there. Now they’re probably #2, #3, but I do believe they probably will have a -- I think pointing this way, once the economy stabilizes a little bit, our service provider, they probably can add more value. But when
the economy growing so fast in the last couple of years, some vendors tend to lose money against a market share than the service provider sitting back a little bit. So we feel the service provider carrier probably will keep coming back in the next few years, especially a lot of new infrastructure being deployed and also security like operation goes through service also will be huge potential.

Unidentified Analyst

I appreciate that. Patrice, just a very quick one for you. So Keith has promised us 25% or more operating margin. So what does that mean on average, what does that mean for build-out of your sales capacity? And as you look out over the next 3 years is the growth in the business going to come from adding incremental levels of sales capacity or driving more productivity? And I'm just mindful of the talent environment. So how are you sort of thinking about that in the context of the guidance that was just laid out?

Patrice Perche - Fortinet, Inc. - Executive VP of Support & Chief Revenue Officer

I think will be a combined results. So we definitely look for acquiring new white space, and that's where we're investing in capacity. We have this -- especially for the enterprise segment, as you know, we are very organized within the sales organization by segment from SMB, mid and enterprise.

The enterprise require much more attention for we have this kind of repeat and grow strategy where we're reducing number of company rep. We have a quite high today compared to our peers. And we're expanding, in fact, to, of course, giving less [thought] and each reps to develop, in fact, the value proportion. Our broad portfolio, in fact, allow us to start having some use case of the fabric, so it can't be data center, and then maybe next will be branch refresh or cloud and then as we consolidate this platform.

So there is that we one will be, of course, much more revenue per account that we develop. So a better productivity by rep. So we'll need, of course, to continue to invest in capacity to have this better coverage. And at some point, we will reach the right ratio. And so we have this aspect, which, of course, expand and the new logo, of course, because we mix a bit of an existing account and of course, new white space account for the reps or will be acquired. And we hope that we can continue to gain market share because especially on this enterprise, I'll say even in the U.S., we still have a huge room for getting -- compared to Europe or Asia, where we have already nice but still, of course, a high potential.

If we just cover the ratio, I think we'll have a significant impact and growing in the U.S. So we should have a combined wholesale contribution.

Unidentified Analyst

Yes. I heard a question on SD-WAN and OT, how much headroom do you think these high growth rates have to continue? I think maybe you started to answer that, Ken, a little bit with the service provider comment you made. But I'm just wondering, these are extraordinarily high growth rates. How much longer can they go on that way?

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

You want to talk about SD-WAN in your goal.

Ken Xie - Fortinet, Inc. - Founder, Chairman & CEO

So I think SD-WAN still in fact, I'll say, at the early stage. Service product is a good example. They're quite slow to move. So there was, of course, a bit holding due to the revenue stream that was coming from MPLS. So it was clearly not trying to go ahead. They've been forced by the market adoption and also more independent, I would say, system integrator that was able to provide expertise to deploy, in fact, SD-WAN. So now we see, and it takes, of course, much more time. I mean like 12 months, we enable all the logistics, the connectivity with their system in our PNC to be able to launch the machine. So -- and we do see that the sales part is coming much stronger in terms of volume and contribution.
So -- and the market is, I think there's a very significant refresh, I think, for the next 5 years on this SD-WAN. And OT, it's a bit of a similar situation. Maybe difficult to assume from how much is really adding security right now on this infrastructure, maybe 5 or maybe less than 10%, I think. So still huge, in fact, white space here for protecting those critical infrastructure.

So people are rushing, so it's, I think that's also potentially a longer, I'll say, road. And we're also developing, you see on the road map, a lot of additional feature on this detection for OT. So it will be more on OT will also to expand as we already feature set. So those 2 drivers, I think, should sustain for the next 3, 4 years without any problem.

Keith F. Jensen - Fortinet, Inc. - CFO & CAO
Yes. I think the SD-WAN use case, and I'll ask John to jump in here in a second. I mean early on, it was all about the ROI that came from the MPLS avoidance, if you will, and it was a no-brainer. But I think maybe there's other SD-WAN use cases that are coming on the scene now.

John Maddison - Fortinet, Inc. - CMO & Executive VP of Products
Yes. When you look at the SD-WAN marketplaces had 30% growth last 2 years, which surprised a lot of people with this work from home and say, we're not doing anything else in the branches. We still have 30% growth, that will slow down a bit. And so the total marketplace will slow down a bit. But I think the, as I said before, there's opportunity to add additional services.

One of them is our security services. The other one is the cloud on-ramp, which I think is going to be very important going forward. So we see that building out with just pure SD-WAN is still a great marketplace, but we can keep it growing at a high percentage to add more services on it as we go forward. Rather than, again, just treating it as a piece of networking gear, add service on top.

Peter M. Salkowski - Fortinet, Inc. - VP of IR
A couple of quick clarification, too, by the way. The 30%, John, is talking about is the market not Fortinet, right? Our CAGR for the last 3 years was 85%. Secondly, I think Keith earlier during his presentation, talked about services and products, and I think he switched and when he gave the percentages, 2/3 of our business is services, 1/3 of our business is product. So keep that in mind as you kind of think about the model.

And then thirdly, the executive briefing rooms are across the hall. After we're done in here, if you want to walk through there and take a tour and see the OT lab and the SD-WAN lab and the other teaching labs and the executive briefing capabilities, we certainly can make that happen. Although, I got to check with what meetings are going on and we don't want to disrupt them.

Adam Charles Borg - Stifel, Nicolaus & Company, Incorporated, Research Division - Associate
Great. Adam Borg from Stifel. Just maybe so for Ken or Keith. You talked obviously about the M&A strategy really been more tuck-in in nature. But just given your extensive cash balance, the valuations that potentially will continue to come in on the private side in coming months. Any change to the M&A cadence to think about going forward?

Ken Xie - Fortinet, Inc. - Founder, Chairman & CEO
We -- every week, we evaluate a few opportunities. So far, we still see the more attractive from the smaller company, some startup. I think the market multiple come down a little bit, but for us also we need to consider integration. We need to consider like keeping saying 98% of the individual EBITDA before acquisition and also where before the acquisition, we also tend to make a partner first, make sure how things can work together if there's a chance of acquisition of how this is. So that's where, so far, I don't think we are changing this strategy right now.
Keith F. Jensen - Fortinet, Inc. - CFO & CAO

Yes. I would think -- I would agree and add to that, that we get a weekly report from the biz dev team about the deals are looking out and historically, valuation concerns appears very, very frequently in that weekly report, meaning that their valuation expectations are higher than we’re ready to go for.

Look, as dramatic as the market, the public market has moved over the last month or 2, oftentimes, you’re going to see a correction like this, we’re told, expected to take 6 months for the private companies to really adjust their mutations the reason to think that's not true, but boy, this has been a very quick movement in the market, and so maybe we're going to get some valuations.

Moving through to the private sector a little faster than we've seen in the past. And I guess what I'm really saying by all that is that valuation has always been a filter for us, and it will continue to be, maybe more things will move through the filter from there in the second half of the year in light of current market events.

Unidentified Analyst

Guys. I'll ask one over here. But Keith, I wanted to come back to the operating margin question. I mean you guys have been around that kind of 25% operating margin level for the past couple of years. And you commented you think maybe the model can actually support somewhat higher than that. And I've just wondered like kind of what are the key levers that if you were to actually be able to achieve some margin expansion, even though that's not in the forecast, where would that come from? Because it feels like you guys are already very efficient, certainly with G&A and realistically with R&D as well. And so it feels like you kind of maybe have a couple of points of maybe mix effects to work with in the gross margin, but otherwise, it's just sales and marketing. So how would that play out if you were to be able to find some additional margin opportunity in the business over the next few years?

Keith F. Jensen - Fortinet, Inc. - CFO & CAO

Well, first of all, I want to acknowledge the shout out about the G&A being very, very efficient for everybody's benefit. Second part of the question. I'm sorry. Yes. Look, I think we're trying to be prudent about it. If I get upside or will I get upside, Patrice talked about -- I don't like to assume increases in productivity in the longer-term model. We do get it now because of the price increase. But if I normalize for that, I think the model is still assuming the same. So if I get increased productivity, it will come there. Lower discounting can move things around the edges a little bit. The pipeline growth, thank you, John, has been really, really strong. And so really, he generates the pipeline, he converts it as long as the close rates, and again, I assume they're going to be at normal rates.

The other place would be in that kind of I'm uncomfortable making any real assumptions about when the backlog starts appearing in the income statement. It's just -- there's just too much uncertainty. And it seems that every time we get together, we're always talking about, well, maybe it's a little bit better now in terms of supply chain, but it's going to go for another 6 months. And we get together get in 3 months, and we say the same thing. So I think it would be very imprudent to pick a point in time where that's going to start coming in, but I do think it's going to start coming in.

I do believe that services, we look internally spent a lot of time looking at billings because it's a current indicator as opposed to GAAP revenue, which is more of a lagging indicator. I think that we'll start to see it internally on some of our billings numbers will come up above those numbers would be the thing that we would expect. And then we get the conversion into revenue.

Ken Xie - Fortinet, Inc. - Founder, Chairman & CEO

Yes. Also from my experience, we see the margin tend to be more short term, easy to manage compared to the growth. Sometimes you need to invest to be long term, whether by the region or by the sales. So you probably will see without maybe 6 months or 9 months, 12 months after that.
But margin, if we slow down the hiring or if we probably do some on the pricing side, discount side, the margin can be improving much quicker within months compared to the topline growth, sometimes you need to see a result after a few quarters, even years.

Peter M. Salkowski - Fortinet, Inc. - VP of IR

Excellent. With that, we have made it to the top of the hour, so we’re going to wrap it up at this point. I appreciate, obviously, the management team for all their time in their Q&A. If we can give them a round of applause, I’d appreciate that.

On that you’re free to go. And so are you. At this point, we do have lunch.