Fortinet – Analyst Day 2021
John Maddison, Chief Marketing Officer and Executive Vice President, Products
March 9, 2021

Slide 1: Analyst Day – Peter Salkowski

I'm Peter Salkowski. Fortinet's Vice President of Investor Relations. I'd like to welcome everyone to Fortinet's 2021, Analyst and Investor Day, and thank everyone for attending. Presenters today are John Maddison, Fortinet's Chief Marketing Officer and Executive Vice President of Products, and Keith Jensen, our Chief Financial Officer.

This is a live video presentation that will be available for replay on the investor events section of our Investor Relations website. A copy of the slide presentation, as well as a transcript of the Analyst Day will also be posted on the Investor Relations website later today.

Slide 2: Agenda

Now for today's agenda. John will start off today. He's taking a deeper look into some of the topics he presented earlier today at the Accelerate 2021. A replay link of John's Accelerate 2021 keynote, along with the Accelerate keynotes from CEO Ken Xie, and CRO Patrice Perche, along with all three presentation slide deck and transcripts are posted on the Investor Events section of the Investor Relations website.

After John, we'll host a brief Q&A session with our sell side research analysts. Keith will then review Fortinet's growth drivers, summarize the company's consistent financial performance over the last several years, and provide our 2023 financial targets. We will then conclude a longer Q&A session where Keith will be joined by Ken, Patrice, and John. During both Q&A sessions, we ask that you please limit yourself to one question.

Slide 3: Safe Harbor Statement

Before I turn the day over to John, I'd like to remind everyone that during today's Analyst Day, 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 review or refer to our SEC filings, in particular the risk factors in our most recent Form 10-K and Form 10-Q for more information. All forward looking statements reflect our opinions only as of the data in this presentation and we undertake no obligation and specifically disclaim any obligation to update forward looking statements. Lastly, I'd like to remind the analysts that if you want to proceed in the Q&A session that you need to access the Analyst Day using the Zoom link, that I sent you earlier.

We'll now turn the presentation over to John.

Slide 4: John Maddison – Investor Discussion

Thanks Peter. Let me see if I can share my screen here. Alrighty. So, Peter has given me 20 minutes to get through this conversation, so I'll make sure I focus in on the relevant points.

Two main points. One was, although we announced FortiOS 7.0 about a month ago, it's going to be available at the end of this month. It's really expanded what we call our platform of fabric approach across the endpoint, across the network, and across the cloud. There's not many vendors who can support that platform across all three of those areas, and we also deliver it via our appliances, software, virtual, and SaaS delivery as well. I think the main topics I'm going to talk about in terms of product will be a SASE, although by definition seems to change depending on who you're speaking to, but also a Zero Trust, and across those two things... I'll just see if I can share my video. It doesn't seem like I can share my video, but there you go. All right. SASE across, and Zero Trust are use cases that span across multiple products, and one of the issues customers are finding is that, because I've got point product A, point product B, point product C, making those use cases work across all those different vendors is almost impossible for themselves. Further evidence that a platform that's going to be the solution going forward.

The second point is our partners, and today we announced AT&T from a SASE partnership perspective, been working on this for a while, they will... Taking SASE and implementing it through the network is absolutely the best way. SASE consisting of SD-WAN and secure web gateway. For sure, SASE and implementation with the service providers, we do find that there's a lot of conflicts with SASE only companies or SaaS only companies, a lot of channel conflicts. Our strategy is to partner with our channel, including inside that will be our large service providers as well.

Slide 5: Vision, Mission…Who is Fortinet?

Now, from a vision and mission perspective, and who is Fortinet? As you know, and as you speak to customers, this digital innovation is just accelerating, and as they accelerate that it just expands the attack surface, and they really, really want to make sure that they secure both the people, devices, data, and infrastructure. What we're seeing is greater collaboration between the CIO and CISO teams, as we go forward. Who is Fortinet? We're definitely, as you know, one of the top cyber security brands, and we really focus on delivering a platform that covers that entire attack surface.

Slide 6: One Opportunity - TAM

Now, the TAM, it's always interesting to me when I see companies put up TAMs and sometimes now I don't know where they get their information from, because they claim TAM that I've never seen them operate in, but this is our TAM. It's backed up by a lot of Gartner information. Obviously, we do that through Magic Quadrants and market guides, and I'll talk a bit about that briefly, but our TAM, it stretches from users and devices, across the network, across cloud, and security operators. We operate both in the network security world, the networking world, as well as the cyber security world.

Slide 6: Market Growth Drivers

Well, what trends are we seeing? What's driving the marketplace across endpoint, network, cloud, and cyber security, security operations. Well, at the endpoint, obviously, there was work from home, we're still seeing factories IP enabled, and I'm going to zoom in on the Zero Trust architecture for that, which is a migration from VPN. Network security, what we're seeing is a lot more edges appear. It used to be a very well-defined perimeter, now we're seeing a lot of edges appear, and so I'll talk about SASE, which is a component of that. Now, cloud security, continue to see the rollout across hybrid, across cloud, and we're seeing it migrate all the way back into distributed or edge compute, and so adaptive cloud security and security operation. I'm not going to have time to probably go through much else than zero trust, and cloud edge SASE. There just won't be enough time, but let me focus on those two areas.

Slide 7: Security-Driven Networking

Let's zero in on the security-driven networking. Network security, networking, accelerated convergence. We're absolutely seeing the convergence of networking and security. There's no way you can defend and protect all these edges without having a converged solution. It's just too complex and too costly, and so this convergence is starting to happen rapidly.

Slide 8: Network Security Landscape

When I look at the TAM, we looked at the TAM earlier for network security. What Gartner have are Magic Quadrants, and these are well-defined buying centers, a network firewall, secure web gateway, SD-WAN, switching and wireless.

Now, there are some markets like IPS, intrusion prevention, which have gone from a Magic Quadrant to being a market guide, and a static market guide in that it's not really changing much. The longterm destination for such a marketplace will be consolidation inside one of the existing buying centers. We've seen an awful lot of the IPS marketplace get consolidated into the network firewalls and go forward. Then there's new market guides, which are new markets, up and coming markets, which either formed their own Magic Quadrant or do a merger with an existing magic quadrant. There's kind of three of them right now in network security. There is the performance monitoring, and detection diagnostics. There is a digital experience monitoring, and of course SASE, which everyone wants to kind of hear and talk about.

Slide 9: Network Security TAM

When we broke down and looked at the forecast, this is Gartner's forecast for network security, so I'm just focused in here on the network security marketplace. I've not included network performance, monitoring diagnostics, field acquisition or Panopta. We are in that marketplace now, but I've not included it in the TAM right now. You can see there's not a huge amount of change, to be honest, in the size of the pie slices as we go

forward. Yes, secure web gateway increases a bit. SD-WAN increases two points. Switching decreases slightly. Firewall, maybe one point, but the overall percentage of market share or firewall, and SD-WAN, and web gateway, wireless and switching remains pretty much the same. As you know, it's around a 10% growth into 2024.

Slide 10: SASE is a Percentage of Existing Markets

Now Gartner did recently publish, in fact, back in August, another view of this marketplace. This is their SASE definition, Secure Access Services Edge, and what they did, what SASE really is, is a number of those existing marketplaces repackaged into this framework or architecture.

You can see here, that what they've taken is the fundamental components of a SASE company include SD-WAN, includes secure web gateway, include Firewall as a Service, Zero Trust, and CASB, which obviously go across the endpoint, go across into the cloud, and go across the network. How does that change? Again, it doesn't change too much, but you can see, SD-WAN increases a bit more. Secure web gateway decreases, but pretty much the same, but in our minds to be a SAS, a main SASE player going forward, you need all of these components. You need all these components delivered at the edge. Cloud edge, WAN edge and LAN edge.

Slide 11: Network Security Markets

Again, just to kind of show you who's in these marketplaces, we've taken the Magic Quadrant for network security. We've taken the market guides for network security. You can see the different players and the different parts there. The secure web gateway is a marketplace we actually are very active in. Gartner's definition as a bit strange and why they allow certain people into that Magic Quadrant. I think that will change as we go forward.

Slide 12: Security-driven Networking Vision

What's our key strategy here for Security-driven Networking? Well, the first thing is enterprise class networking at all edges. That is the cloud edge, as obviously, at the cloud edge we need to be able to provide that, from our data centers, from our cloud. Also, at the data center edge, very high performance needed and required there. At the LAN edge, either through Wi-Fi and switching. At the WAN edge, through SD-WAN. At the up and coming 5G edge, LT edge, and we're also doing a lot of work on the OT edge. Remember OT used to be air gaped, that's going away and that's created an edge there. One of our key goals is to be able to supply or be able to network, provide enterprise networking at all these edges, whether they be cloud, data center, LAN, WAN, or OT, through hardware, through software, or through SaaS, any one of those can be used across all those edges.

The second component of a security driven networking is enterprise class security, and I often hear people will say, "Oh, I've got security. It's in the cloud. Don't worry about it."

No one's tested it. No one's looked at it, and no one's certified it. We have tested and certified all our security components, whether it be the content, whether it be web security, user security, IOT, OT, device security, our advanced operational and security operations capabilities, as well as the integration of more advanced support services as well. But I definitely feel like this is an area that people are going to look at, at some point, because you can't just say, "Trust me, I've got great security." You need to make sure that that security is tested and certified.

And then we bring all of that together through the fabric and the platform. And so yes, you could have one of these components. Yes, you can have some security. But the key is then to be able to bring that all together in a platform to be able to orchestrate any one of those Edges in terms of networking functionality, to be able to deliver security, any level of security or any part of the security stack at any one of those Edges. And then to be able to make sure that it fits into the ecosystem, the customer. The customers have made some investments in some large platforms, it needs to be a platform that covers the attack surface and all the security components, but also needs to be able to integrate into the ecosystem of that customer.

Slide 13: Need to Protect All Network Edges

And this is why FortiOS is very important to us. I always tell customers it's probably your most important investment from a Fortinet perspective, is that this stack, this full stack of networking and security capability can sit at any one of these Edges. It can sit in an appliance at the WAN Edge. It can sit in our SaaS Delivered Cloud Edge and SASE. It can sit as a powerful perimeter security, next gen firewall in the Data Center Edge. It can apply security to the LTE Edge, the Switch Edge and the WiFi Edge. And so what the customer gets is the ability to switch on any part of the networking capability and then apply security wherever they want to across all these Edges.

And as they go forward, and as they shift different things, maybe there's a shift from work-from-home back to the office, maybe you continue shifting things into the cloud, and it goes into the Edge compute, maybe you continue IP enabling your OT infrastructure. As these shifts happen, you can all take that networking capability and you can increase or decrease the security depending on where the Use Case is. And it's all consistent enterprise class because you're using this enterprise class operating system stack across all those elements. That's why FortiOS is so important, and it can all be applied through a single policy engine across your entire end-to-end endpoint network and cloud security.

Slide 14: FortiSASE Product Offering

And then I'll just kind of highlight the SASE offering that came out with our 7.0 FortiSASE, and again, people take the SASE definition and weld it or mold it to whatever they'd got. The fundamental tenants of SASE are two components. One is the convergence of networking and security and the second one is a platform approach. Not a point solution, a platform approach, or a framework approach to the Edges as you go

forward the services Edge. So from our perspective, there's three really important components. The first one is you absolutely need to be able to apply a flexible Edge access. And that Edge could be a work-from-home user. It could be what we call a thin Edge where the device, in this case for example, is a 4G or 5G device. It doesn't have the footprint to put the security on. And then there's what we a call a Secure Edge. A Secure Edge will be one of our SD-WAN devices. That can put a full security stack, but even if you don't want to put all the security there, you still need some security on SD-WAN.

And so these flexible accesses from the Edge gives the customer the ability to protect all those Edges. Once you hit our cloud, you hit the first thing is Security as a Service. So you may want to apply secure web gateway capabilities, or you may want to apply isolation web browsing, or next gen firewall or firewalls as a service, but we've also integrated Zero Trust. So your Zero Trust network access Use Case can also be derived using the SASE access proxy.

And then the third component, which we think is going to be extremely important going forward is that digital experience monitoring. Yes, I've put all these things in place to make it more flexible and more secure, but all my users and devices, by the way, getting the right experience end-to-end from how they access the network through the network and into the cloud. And so the pairing of our data centers, the monitoring of the experience and the high availability, and then the ability to see via API security into clouds where you can't even provide any of your own security becomes very important. So to us, SASE consists of these three things, Access Edge. Okay, usually an appliance for SD-WAN and apply it to some sort of device for 5G or some sort of client. Then we provide Security as a Service in our cloud, we then provide digital experience monitoring, which provides that glue and that intersection between the user experience and the application. This is all rolled out under our FortiSASE umbrella.

Slide 15: Zero Trust Access

And I'm looking at the time here, I've got a few minutes so I'm going to see if I can squeeze in the Zero Trust.

Slide 16: Zero Trust Access Landscape

Zero Trust Access, this marketplace is dominated by identity actually, although you did have VPN and NAC and [inaudible] and OT security in as well.

Slide 17: Zero Trust Access TAM

From a size perspective, again, Access Management is dominating, but Zero VPN and Zero Trust is also going to be very important as you go forward.

Slide 18: User and Device Security Markets

If you look at the market guides and the magic quadrants, then it's quite fragmented, but a lot of activity around Zero Trust and VPN Migration.

Slide 19: ZTNA Use Case Requires a Platform Approach

And here's the biggest issue with Zero Trust. It's green technology. It's probably technology that we should have been implementing a while ago. It really does upgrade your VPN access big time in terms of giving you specific application access and constantly doing a contextual view of per session on what's going on. And then also providing that user and device continuous identity check as you go forward. So absolutely without a doubt, VPN has served us well over the last 20, 15 years, but it will evolve forward into Zero Trust. We believe, however, we have a lot of customers on our VPN networks obviously, a VPN solution set that is an evolution versus a revolution in terms of you can just wipe the slate clean and start all over again, but you're going to have to make all these different vendors work together.

So from a vendor perspective, what do you really need from a Zero Trust? First of all, obviously you need that Zero Trust agent sitting on the end point. You can use files and stuff, but you really do need an agent to get the best experience. We also believe, obviously you need that authentication of the user and devices, multifactor as you go forward. Then there's the most important piece which are the access proxy. Access proxy provides that granular access to the applications and also connects the user session into the contextual engine. Now as you go forward, once you're on the application, a lot of customers and enterprises also want to apply more advanced endpoint security such as EDR, because once you're on there you've got to keep that behavioral monitoring going on across that end point.

Now, what I find a lot of the times is that across a specific customer, you've got a vendor for Zero Trust agent, and you've got another vendor EDR, another vendor for identity, another vendor for proxy. And it just goes on. It's almost impossible to get a true Zero Trust networking, working across so many different vendors. Now I'm not saying you need one vendor, but I'm saying you can't have five or six vendors, this doesn't work. So for our solution for Zero Trust, one of the key components inside there is FortiOS. That becomes the access proxy. And the flexibility we can have is that that access proxy can be in the cloud through our FortiSASE solution, but it can also sit in the customer data center. Their existing VPN termination point can be the access proxy for our Zero Trust solution set.

And we think there are other marketplaces, on campus marketplaces, which could replace core switching and networking through the Zero Trust architecture and proxy. So the key for us is that we've got our FortiClient, our FortiZTNA, Authenticator, Token, EMS, and FortiOS that provides an end-to-end Zero Trust solution, where the proxy can be in the cloud and the data centers on the campus. We can integrate with other components, so identity systems out there for example, but we believe this is a great

migration from our existing FortiClient and FortiGate customers into a Use Case Zero Trust that works across all these components and we'll arrive in our FortiOS 7.0.

So let me stop there at 21 minutes, I think. Unusually on time and see if I've got any questions.

Peter Salkowski

All right, John, thank you very much. I will point out there's another dozen slides after this, but you're right, we can move on, we've run out of time. So we are going to open up for Q and A. I will remind everyone that John's slides will be posted on the IR website after the presentations, hopefully very quickly after. So just again, a reminder, please raise your hand to ask a question and please do limit yourself to one question. We've got limited time and lots of people want to ask questions. So first one up is going to be Michael Turits from KeyBank. Michael, go ahead. Just un-mute yourself, Michael.

Michael Turits, Key Banc

Take Care. Should be un-muted. Thanks very much. John, you guys announced the partnership with AT&T today for SASE. Can you talk about that decision to partner with service providers for, let's call it the networking services? By contrast, some of your competitors have built their own network of POPs, others are partnering with cloud providers. Do you get enough control over the end product and over the customer if you're partnering this way versus these other strategies?

John Maddison

Well, to be clear, we'll do both. Okay? So I don't think you can supply a platform, a SASE platform or SaaS platform, without experiencing yourselves and understanding it yourself. And so we'll do both, we'll have an offering. But we firmly believe that once we build that technology, transferring or enabling our big service provider partners is the best way into the marketplace. As I said earlier, we absolutely see channel conflict all the time between service providers and some of the pure SaaS vendors, so we believe you have to build it so you know how to build it, and then we can transfer some of that technology to our service providers.

Michael Turits

Thanks, John.

John Maddison

Excellent.

Peter Salkowski

Okay. Next step is a Jonathan Ho from William Blair.

Jonathan Ho, William Blair

Hi, good afternoon. In terms of the breadth of offering that you've just described, can you maybe talk a little bit about how in the SASE and Zero Trust world having that broad of an offering, does that provide an advantage to you relative to some of the deals that you're doing out there? And can you talk about specifically why it's an advantage to be able to offer, I guess, the set of solutions? Thank you.

John Maddison

Thanks. Yeah, so definitely customers have had enough of buying all the different point solutions. And when I speak to them, it's not that they want to go from 30 point solutions down to one. They want to go from 30 point solutions down to seven or eight platforms that interwork and work together. One of the most common ones we have is Microsoft, and we have eight different integrations into different Microsoft. We're not saying it's one, it's seven or eight, but they need to work together. So they go into a platform, they just can't support so many different point products across the network in cyber security.

The advantage for us is that sometimes I see us enter a customer with one of the products. In fact, it could be anything, it could be authentication, it can be our WAF in the cloud. So we always got something that's available to enter a customer. And the advantage long term, though, is that they can then build out that fabric within that architecture they decided on the seven or eight platforms, and truly deliver those use cases. Again, it's not a point product anymore that can deliver zero trust or SASE. It's just impossible. You need that platform approach to be able to deliver that.

Peter Salkowski

Sorry about that. Next up should be Brad Zelnick from Credit Suisse.

Brad Zelnick, Credit Suisse

Awesome. Thank you so much. And John, really appreciate the presentation. Maybe a variation of the last question, you talked about platform and interoperability of solutions in implementing a SASE architecture. And I just wanted to maybe understand competitively and through the lens of the customer journey. Right? What distinguishes Fortinet? Because at this point, many vendors are approaching SASE from different starting points, Zscaler with proxy, Menlo Security with browser isolation. Cato, I think, began with firewall as a service. Palo Alto has a number of assets. Where does the customer journey begin for a typical Fortinet customer? And why is that a better on ramp to SASE versus others? And as you look out on the horizon, is it always going to be patchwork, or do you think there ends up being winners and losers here because you're all swimming in each other's lanes?

John Maddison

I think the losers, long term, are the point solutions. And there's not many vendors like ourselves who have enterprise class security across endpoint, across network, and across cloud. And if you're trying to measure the digital experience, if you trying to provide security across that attack surface, you don't see part of it. How are you going to protect it? So our long term advantage is that we can sit across any of those edges, that we can provide enterprise security across any of those edges, and that we can deliver it via SaaS or appliance, or software or agent. And that's our advantage. There's a lot of people who are just in the cloud. There's a lot of people just in the network or just at endpoint. Our ability long term to sit across all those three is our biggest advantage. Yes, some customers...

I mean, if you look at the... Let's be honest, let's look at the SASE marketplace today. What is it? It's 95%, probably more, secure web gateway as a service. That's what it is. As people have migrated their proxy, more often than not [inaudible] proxy into a cloud proxy. That's where the market is today. However, it's going to expand as people expect the orchestration between their SASE and their SD-WAN, as they expand their integration into the cloud with CASB, or as they expand and make sure that any endpoint through zero trust on and off the network gets that protection per application. So the advantage for us is the use cases, it works across all these different elements, and we have all of them in place. And, we spent the last, I don't know, I'm going to say 10, maybe eight or seven years, building it organically versus trying to bolt it together with acquisitions.

We do acquisitions, and Panopta was the latest one. But they're small, and we buy it for the technology. I think it's really hard to build a platform like ours if you don't do it organically. But coming back to your question, Brad. I think our advantage is though we can sit across any part of the edge. We can deliver clients, software, and SaaS, and that gives us the ability to deliver these use cases like no one else.

Brad Zelnick

Excellent. Thank you so much.

Peter Salkowski

Thank you, Brian. Next up is that Brian Essex from Goldman Sachs.

Brian Essex, Goldman Sachs

Yeah. Thank you, Peter. And John, thank you very much for the presentation. I was wondering if you could maybe touch on, you talked about the convergence of network and security. And from the perspective of legacy, or incumbent network equipment vendors, what are you seeing there in terms of the way that they might be approaching SASE? Particularly given the legacy install base they might have, maybe their presence of the campus edge as a competitive advantage. How are they thinking about this?

John Maddison

Well, I think what networking vendors have done, and I don't think I said this at the beginning, there's a big difference between networking vendors and cyber security vendors. One's hardware and performance and one's software. Well if you listen to my presentation, I go through that a bit. But I think they've been able to buy and bolt on cyber security components over the last 10 years. You just can't do that forever. And it becomes even harder when you've got to do it in the cloud, or SaaS delivered. So I think they're really struggling.

And we see that in the marketplace, and when the customer says, "Hey, I want this converged solution. And I want to be able to put security on the one edge or the cloud edge or the data center edge. And I want it to be consistent. And I want to be enterprise class," they just can't deliver that. Which is just impossible, because they're trying to bolt things together. That's what I've seen. And it gets harder and harder because the customers get frustrated because they've been promised by some PowerPoint that it's all coming together. And years later it's not, and they could be becoming very frustrated.

Brian Essex

Got it. Thank you.

Peter Salkowski

Thanks, Brian. Next step is a Gray Powell from BTIG. And Keith Bachman, you're on deck.

Gray Powell, BTIG

Okay, great. Thanks. Can you hear me okay?

Peter Salkowski

Yep, we can hear you.

Gray Powell

Perfect. Yeah. I just want to follow up on Brad's earlier question, maybe a different angle. So Fortinet's always had some level of secure web gateway capabilities, and I think it's been pretty successful in the small and mid-market. But historically, I'm not sure if Fortinet's really been thought of as a replacement for pure play proxy architectures in larger enterprise. Could you maybe talk about how that's changing, and particularly, as you focus more on the SASE product set?

John Maddison

Yeah. That's a good point. I mean, I think I kind of mentioned it a bit in the Gartner magic quadrant for secure gateway. That for some reason, a couple years ago, they put in that

you have to be a cloud proxy to be in there. Even though we have got substantial revenues of secure web gateway, whether it be proxy or whether it be through our FortiProxy or through our FortiGate, we can do that. For us, I think, and as we go forward, we now have that capability in the cloud. And so I think we'll get access to the magic quadrant, and then I think you'll see us accessing the enterprise marketplace through there. When you look across cyber security, you look across networking, and I didn't show you. If you can look at my presentation from Accelerate this morning, I flash a slide with all our different products across all these different areas. It's substantial. I probably would say that one of them that wasn't quite enterprise class was the proxy capability, but that would be fixed in our FortiSASE offering.

Gray Powell

Got it. Okay, thank you.

Peter Salkowski

And just as a reminder, those slides are up on the website, as is the replay for the analysts who didn't get a chance to see this morning. Next up I believe is Keith Bachman. If you do have a question, please do raise your hand. We've got about nine more minutes left from the Q&A. I think we'll get a few more in here. Keith, you're up.

Keith Bachman, BMO

All right. Thank you very much. Thank you, John and Peter. My question is going to do the market slides where you had growth rates. And I just wanted to see if you could flush out, A, how you're viewing the growth dimensions surrounding firewalls versus firewalls as a service, versus virtual firewalls. What do you see as a key opportunity as a risk? And then B, to broaden out the question a bit, how do you think Fortinet fits into that as architectures converge surrounding firewalls as a piece of the node, rather than an entire solution of SASE, rather, becomes more prominent? So, just trying to see what the risks are or opportunities for Fortinet, as you think about the growth of the firewalls in those various pockets. Thank you.

John Maddison

Yeah, good question, Keith. Good question. First of all, I think firewalls as a service is a tiny marketplace, and it's just very diff... The secure gateway moving from data centers to cloud makes a lot of sense, and architectural-wise and everything else. And so that will just move into the cloud over the next... It's like email, when I first started doing email security back in 2007 it was all appliance as well as moving to the cloud. It's closer to the application. Web gateway needs to be close to the cloud edge. Firewall is very, very different from an architecture or network perspective. I don't think Gartner could even give you anywhere. That estimate I have there from SASE is a complete guess. They

have no clue what the firewall as a service marketplace. Even if they did get to a detail, I think it would be less than $100 million.

So will it be there eventually? Yes, but it's going to be very small. I think the more powerful components of the firewall marketplaces will go forward. I think it's going to become about 10%, it probably already is about 10% virtual. We have a very strong FortiGate virtual machine offering. Now there's still going to be a need for appliances at these edges, internet facing. There still will be a need for appliances in the core where you need super hyperscale performance. But the other area we think will be very interesting will be the micro-segmentation cross-cloud. And that is, even though you have native cloud firewalls from Azure and AWS, and by the way, we apply management and services sitting on top of a lot of that native security, as we've announced recently. We think a cross-cloud firewalling, micro-segmentation strategy, A, gives you that firewall in the cloud.

And cross-cloud it used to be predominantly an East-West data center technology. I think it's going to migrate to being cross-cloud. But it also gives you that visibility that you can take and transfer back into your North-South or endpoint network WAN capability. So firewall as a service, to me, is just a tiny speck, and will remain that way. It will be there, and we offer it today. But I think the bigger component to us is still making sure we can sit in the middle of the data center, sit at the edge of a network. I don't know anybody yet that really wants to put a virtual machine at the edge of the network facing the internet. The risks are tremendous. But we do see micro-segmentation cross-cloud as being an important part of the firewall marketplace going forward.

Peter Salkowski

Great. Thanks John. Next up is Fatima Boolani from UBS. And Ben Bollin, you're on deck.

Fatima Boolani, UBS

Hi, thanks for taking my questions. And thanks, John, for the presentation. John, I wanted to ask you about the AT&T opportunity and the partnership there, but maybe a bigger picture question around the SASE/SD-WAN market opportunity bifurcated between the service providers and carriers and the enterprise. Because my understanding is that you're able to cater to both in different ways. So I'm wondering if you can talk about those compatible, but still different opportunities.

John Maddison

Yeah, another good question. I think the marketplace is about 50% enterprise DIY, 40% service provider and 10% just cloud SASE or [inaudible 00:36:14] versions. And so we're very strong in the enterprise because a lot of it was just switching it on for us and enterprises like that. Now some enterprise is different in that they need to scale it across multiple customers. They need more sophisticated orchestration. And so we're just kind

of over the last year or so entering that marketplace. It was slightly different for us. And we're starting to provide headway, but we don't think it's going to be isolated SD-WAN. It's going to be more of this SASE. You saw my definition of SASE earlier. It's SD-WAN. It's web gateway, firewall as a service, CASB and zero trust.

What we're going to see is that our customers are going to say, "Yeah, we want to do SD-WAN." This is like AT&T. They said, "Well, we could do SD-WAN with you, but we've got a network only version of that. Why don't we do a SaaS version, which includes SD-WAN, but includes a secure web gateway, will include some of these other applications going forward." And I'm having the same conversation with all the service providers. They're saying, "Let's take our platform approach across our network into the customers." And they're hearing that from the customers as well. That makes sense.

I do think, and I've said this and our service provider customers know this, that they've taken the easy route out over the last five or six years. They've just said, "Oh, let's just OEM something off the marketplace, a SaaS version, because it's easy." But they're realizing now that if they just keep doing that, they're going to get devalued into being just transport, especially since MPLS is getting turned over into SD-WAN and broadband. So they absolutely know they can't just OEM this going forward. They need to have their own solution.

Peter Salkowski

Hey, John. Next up Ben Bollin from Cleveland Research. We've got two after Ben. We're going to have Andy Nowinski and Tal Liani. Andy Nowinski from DA Davidson and Tal Liani from B of A. And then we're going to wrap up the Q&A session. So we're going to try to get all three of them in. So Ben, you're up.

Ben Bollin, Cleveland Research

Thanks, Peter. And hey, John. Bigger picture, interested how you think about the incrementality for Fortinet, either wallet share or cohort expansion as customers evolve into zero trust and SASE. And also interested in any thoughts you have within the customer footprint for the ones who are most prepared to make this transition and already in play versus those who seem to be maybe lagging the most. Thanks.

John Maddison

Yep. Another good question. I split those two up. Zero Trust to me is definitely something that's going to swallow the VPN marketplace. Now we have a certain percent of the VPN marketplace. So A, we want to make sure that all our VPN customers migrate to our Zero Trust versus somebody else's. But we also think that a Zero Trust allows us to go after the new marketplace plus the VPN vendors as well. So to me, that's an incremental increase in market opportunity. SASE, as I keep saying, is 95% skew of gateway where we have a presence, but nowhere near the size some of the larger vendors in that. And so I see that, again, as being an opportunity for us.

I am not worried that it's firewall as a service being such a tiny component of that. It doesn't really affect our firewall business, but we see it as an opportunity to go after the proxy cloud secured gateway marketplace, and again, tie in other things like SD-WAN or CASB integration as we go forward. And again, I keep saying this, there's people who are in the cloud. There's people on the network, the networking vendors, the endpoint vendors. By the way, our Zero Trust, we want to upsell people into our EDR solution and XDR solutions as we go forward. So we think it's a new incremental market opportunity, but even more so to cement our situation in the customers by building a use case across multiple products.

Peter Salkowski

Thanks, John. Our next step is Andy Nowinski from D.A. Davidson. Then we're going to end with Tal Liani from B of A. Andrew, you're open now.

Andrew Nowinski, D.A. Davidson

Thank you very much. I just want to ask a question on your access proxy. I know you said it was essentially FortiOS, but I'm wondering if that's synonymous with the proxy that Zscaler has and now Palo Alto offers as part of their Prisma Access solution. So I was wondering if you could just compare and contrast access proxy versus those two at a high level. Thanks.

John Maddison

Yeah. Well, think about the access proxy and proxy web gateway are different. So the traditional secure web gateway proxy is a certain marketplace and that is protecting users and you apply security to that access to the internet. The access proxy means the ability to apply per session against a contextual engine given a identity based policy of the end users agents. So they are similar from an engine perspective, but very kind of different marketplaces. And so for us, FortiOS could be both. It can be that secure web gateway proxy. And we have quite a few customers actually who use it, our FortiGates as a proxy, the web gateway proxy. But it also will be the Zero Trust Network Access proxy as well. So again, the amount of features and function capability we can put on FortiOS, whether it be the proxy, whether it be the WAN edge, [inaudible 00:41:39] SD-WAN, whether it be a Wi-Fi controller, whether it be a 5G controller, this is what gives us such an advantage that we can play in so many different marketplaces with the same stack.

Peter Salkowski

Great. Thanks, John. Last one up. Tal. And then we're going to move on to the next presentation. Tal, you're there?

Tal Liani, Bank of America

Hey. Can you hear me?

Peter Salkowski

We can hear you.

Tal Liani

There you go. You may get a different name on the computer because of technical issues, but I have two questions. The first one is if I ask your typical customer, historically if I asked them, what's the one benefit of Fortinet the answer is major price advantage, 40% discount. And the question is whether you maintain this kind of price advantage also in a SASE model. And the second question is with other companies, we have seen that SASE is a replacement of appliance revenues, and there's always a decline in product revenues and increasing SASE. And it creates some differences between revenues and ARR. In your case, it looks like your focus is slightly different. Can you talk about cannibalization versus non-cannibalization business that you're forecasting?

John Maddison

Sure. Let me answer those two. So the first one, absolutely. We have such a price performance advantage for core networking, not just firewalling, but also SD-WAN, by the way, that customers obviously talk about that. They should also be talking about that it's not just performance, but it has enterprise security and it has all the networking features. So it's not just the performance. They wouldn't buy it if it wasn't enterprise class. We wouldn't be in the middle of many large financial organizations if it was just cheap. So I always said, yeah, it's great value, but it's absolutely high performance and high effectiveness.

I think the other second part of your question what's happened is SASE, because it's also 95% secure web gateway, has ripped the heart out of blue coat proxy appliances and transferred them into the cloud. Absolutely. A 100% agree with that statement. But as I keep saying, firewall as a service is a tiny cloud. Firewall as a service is tiny. I don't even register it. That's not ripping out our appliances and put them in the cloud. I think the long-term for that marketplace is more around virtual machines, native and micro-segmentation. That's a bigger challenge to traditional hardware appliances. But SASE and firewall as a service is not. That answer your question?

Peter Salkowski

Okay. [crosstalk 00:44:24]-

John Maddison

That answer the question?

Peter Salkowski

He may have gone back on mute during the time. We can always come back to that in the second Q&A after the CFO presentation. So, John, thank you very much.

John Maddison

Thanks.