UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

OKLAHOMA FIREFIGHTERS PENSION AND RETIREMENT SYSTEM, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. FORTINET, INC., KEN XIE, MICHAEL XIE, KEITH JENSEN, and CHRISTIANE OHLGART, Defendants.	Case No. 5:25-cv-08037 CLASS ACTION **COMPLAINT FOR VIOLATION OF THE FEDERAL SECURITIES LAWS** **JURY TRIAL DEMANDED**

Plaintiff Oklahoma Firefighters Pension and Retirement System ("Plaintiff"), by and through its counsel, alleges the following upon personal knowledge as to itself and its own acts, and upon information and belief as to all other matters. Plaintiff's information and belief are based on, among other things, the independent investigation of counsel. This investigation includes, but is not limited to, a review and analysis of: (i) public filings by Fortinet, Inc. ("Fortinet" or the "Company") with the Securities and Exchange Commission ("SEC"); (ii) transcripts of Fortinet conferences with investors and analysts; (iii) press releases and media reports issued and disseminated by the Company; (iv) analyst reports concerning Fortinet; and (v) other public information and data regarding the Company.

NATURE OF THE ACTION AND OVERVIEW

1. This is a class action on behalf of all persons and entities that purchased or acquired Fortinet common stock between November 8, 2024 through August 6, 2025, inclusive (the "Class Period"). Plaintiff asserts claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act"), and Rule 10b-5 promulgated thereunder, against: (i) Fortinet; (ii) the Company's Chief Executive Officer ("CEO") Ken Xie; (iii) the Company's Chief Technology Officer ("CTO") Michael Xie; (iv) the Company's former Chief Financial Officer ("CFO") Keith Jensen ("Jensen"); and (v) the Company's current CFO Christiane Ohlgart ("Ohlgart").

2. Fortinet is a cyber security company. Its most important product is its FortiGate firewalls. A firewall is a network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules. The primary purpose of a firewall is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and malicious activity.

3. This case concerns Defendants' misrepresentations regarding the business impact and sustainability of a purportedly "record" round of unit upgrades consisting of approximately 650,000 FortiGate firewalls, or roughly one quarter of the Company's total FortiGate units. During the Class Period, Fortinet told investors that this "refresh cycle" was "by far the largest we've seen probably ever," would generate "around $400 million to $450 million in product revenue" in 2025 and 2026, and would create strong opportunities to cross-sell additional products and services. Defendants also repeatedly represented that the refresh cycle would "gain momentum" in the second half of 2025 and beyond.

4. In truth, Defendants knew that the refresh cycle would never be as lucrative as they represented, nor could it, because it consisted of old products that were a "small percentage" of the Company's business. Moreover, Defendants misrepresented and concealed that they did not have a clear picture of the true number of FortiGate firewalls that could be upgraded. And while telling investors that the refresh would gain momentum over the course of two years,

Fortinet misrepresented and concealed that it had aggressively pushed through roughly half of the refresh in a period of just a few months, by the end of 2Q 2025.

5. On August 6, 2025, after the markets closed, Defendants revealed during the Company's 2Q 2025 earnings call that Fortinet was already "approximately 40% to 50% of the way through the 2026 upgrade cycle at the end of the second quarter [of 2025]." During the call, a Wall Street analyst asked, "why are we not seeing more upside in the numbers this year from the refresh cohort," given "that we are 40% to 50% through" "a really big or larger than normal refresh cohort?" In response, Defendants: (i) admitted that "it's hard[] for us to predict" the total number of FortiGates requiring an upgrade; (ii) suggested customers had "excess [firewall] capacity from [purchasing firewalls in] prior years" and therefore did not need to upgrade; and (iii) revealed that the refresh could not have had "much business impact" as it consisted of only a "small percentage" of the Company's business because the products were "12 to 15 years" old and had been sold at a time when Fortinet's business was 5-10 times smaller, meaning that the total number of FortiGates eligible for an upgrade was inherently limited.

6. On this news, the price of Fortinet common stock fell over 22%, from $96.58 per share on August 6, 2025, to $75.30 per share on August 7, 2025, on unusually high trading volume.

JURISDICTION AND VENUE

7. The claims asserted herein arise under Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. §240.10b-5).

8. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, and Section 27 of the Exchange Act (15 U.S.C. §78aa).

9. Venue is proper in this District pursuant to Section 27 of the Exchange Act and 28 U.S.C. § 1391(b) because Fortinet's headquarters is located within this District and Defendants conducted substantial economic activity in the District. As such, substantial acts in furtherance of the alleged fraud have occurred in this District.

10. In connection with the acts alleged in this complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, and the facilities of the national securities markets.

PARTIES

11. Plaintiff Oklahoma Firefighters Pension and Retirement System is a public pension fund established in 1980 to administer pension benefits for Oklahoma firefighters. Plaintiff purchased Fortinet common stock during the Class Period, as detailed in the Certification attached hereto and incorporated herein, and has been damaged thereby.

12. Defendant Fortinet is a Delaware corporation with its corporate headquarters and principal place of business in Sunnyvale, California. Fortinet's common stock trades on the NASDAQ stock exchange under the ticker symbol "FTNT."

13. Defendant Ken Xie is, and at all relevant times was, Fortinet's CEO and Chairman of the Company's Board of Directors. Ken Xie is a co-Founder of Fortinet.

14. Defendant Michael Xie is, and at all relevant times was, Fortinet's CTO and a Director on the Company's Board of Directors. Michael Xie is a co-Founder of Fortinet.

15. Defendant Jensen served as Fortinet's CFO during the Class Period until May 15, 2025.

16. Defendant Ohlgart has served as Fortinet's CFO since May 15, 2025. During the Class Period until May 15, 2025, she served as Fortinet's Chief Accounting Officer.

17. Defendants Ken Xie, Michael Xie, Jensen, and Ohlgart are collectively referred to herein as the "Individual Defendants." The Individual Defendants, because of their positions with the Company, possessed the power and authority to control the contents of the Company's reports to the SEC, press releases, and presentations to securities analysts, money and portfolio managers, and institutional investors.

18. The Individual Defendants, because of their positions and access to material non-public information available to them, knew the adverse facts and omissions specified herein had

not been disclosed to, and were being concealed from, the public, and that the positive representations and omissions which were being made were then materially false and/or misleading.

SUBSTANTIVE ALLEGATIONS

Background

19. Fortinet is a cybersecurity company best known for its FortiGate firewalls. The Company has two main revenue streams, product revenue and service revenue. Product revenue currently accounts for roughly 30-35% of Fortinet's total revenue and includes the sale of hardware like FortiGates and software licenses. Service revenue accounts for roughly 65-70% of the Company's revenue and includes the sale of subscriptions for intrusion prevention and antivirus protection, technical support, and cloud services.

20. Fortinet sells its FortiGate firewalls bundled with software and support services. The firewalls themselves have a limited support life cycle of roughly ten years depending on the model. After the life cycle ends, the Company stops providing firmware updates and security patches, and hardware support from Fortinet expires. This is referred to as "end-of-support" or "end of service" ("EOS"). When hardware approaches EOS, customers are prompted by the company to "refresh" their hardware with newer models.

21. Periodically, large swaths of older FortiGate models reach EOS at the same time and require a refresh. Fortinet calls this a "refresh cycle." Refresh cycles typically boost Fortinet's product revenue for a time as customers purchase new hardware. A refresh cycle also typically leads to an increase in service revenue, because customers often renew or expand their subscriptions when upgrading their hardware.

22. During the COVID-19 pandemic, many companies shifted employees to remote work which caused a surge in demand for Fortinet's products. Moving employees to remote work meant that companies had to secure all the new remote connections to their networks which often meant buying more or better firewalls. Fortinet experienced strong product revenue growth from 2020 through 2022 during the COVID-19 pandemic.

23. In 2023 and the first half of 2024, Fortinet's product revenue growth slowed for several reasons, including that many customers who upgraded during the pandemic did not need new firewalls and that macroeconomic concerns caused many companies to cut their IT spending.

24. Beginning in the second half of 2024, the Company began to tell investors that it was seeing signs of recovery in the firewall market and that it expected the next refresh cycle to begin in 2025. For instance, during Fortinet's August 6, 2024 2Q 2024 earnings conference call, Defendant Jensen said the Company was seeing "signs of possible improvement in the firewall market" including that "days of registered security service contracts improved . . . and has now returned to 2020 pre-supply chain, pre-COVID crisis levels" and noted that "the sequential increase in hardware sales in the second quarter aligned more closely with historical norms." He added that a "full refresh" was on the horizon, "likely in 2025."

Materially False and Misleading Statements Issued During the Class Period

25. The Class Period begins on November 8, 2024. The day before, November 7, 2024, aftermarket hours, Fortinet held an earnings call to discuss the Company's 3Q 2024 financial results. During the call, Defendant Jensen discussed the FortiGate refresh opportunity in his prepared remarks. He stated:

> I'd like to offer a couple of comments on the firewall recovery and refresh opportunity. During last quarter's remarks, we mentioned that the continued improvement in the days of registered FortiGuard contracts indicated the inventory digestion at end users was returning or had returned to normal.
>
> In the third quarter, this metric was stable, further validating our view that the firewall market is recovering. Today, we'd like to add to this commentary by noting that in 2026, ***a record number of FortiGates will reach the end of their support life cycle, and we expect these customers to start to refresh cycle for these products sometime in 2025.***

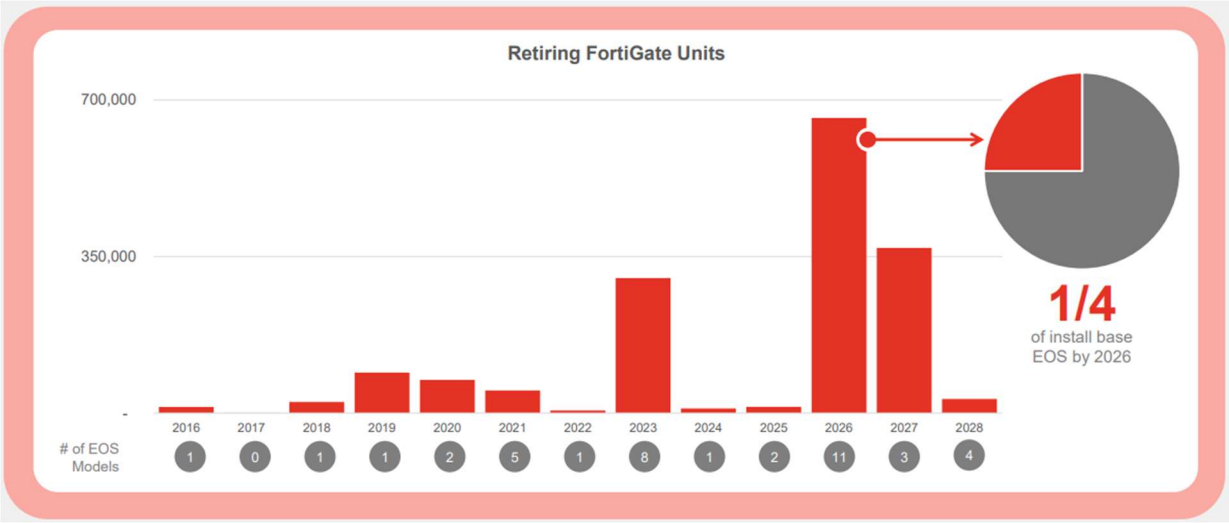
26. Later during the call, JP Morgan analyst Brian Essex asked:

> [C]ould you dig into the commentary around the firewall refresh cycle that you provided? So with respect to conversations you're having with customers, and maybe with a little bit of color what you've seen historically, how far before the renewal point do customers tend to refresh? And do you have any insight into the mix of [types of customers]? And what the timing and the magnitude might be, whether this might be a first-half event, second-half event? Any kind of insight you could provide would really be helpful.

In response, Defendant Jensen indicated certain larger customers would start to methodically upgrade in 2025 and touted the size of the refresh, particularly as compared to its 2023 refresh cycle:

> I think that we see these end-of-life of these products starting in the second half of 2026. We don't expect the customers to wait until the 11[th] hour to make the change. For larger enterprises, they would go through another certification, [proof of concept] project perhaps as part of that before they place them in service.
>
> So we saw a similar -- not similar, we saw a lift, if you will, similarly in 2023, although ***the magnitude in 2026 is much, much larger.*** And why it's relevant to 2023 is that if you go back and look at product revenue growth in 2022, very different world, supply chain, switches, et cetera. But I think in 2022, the product revenue growth was a little bit over 40%. So we do think there's a relationship there. We do think it starts earlier.
>
> To the second part of your comment, as I mentioned, ***the absolute number that we see in 2026 is by far the largest we've seen probably ever,*** but certainly in the last five or six years. It is -- each year is dominated by the entry-level firewalls. However, in 2026, we do see a significant portion of that actually being in the mid-range firewalls as well, and that is a very unusual and positive situation.

27. Less than two weeks later, on November 18, 2024, Fortinet held an "Analyst Day" conference and provided details about the "record" refresh cycle. In conjunction with the Analyst Day, Fortinet published a presentation titled "2024 Analyst Day." The presentation included the following slide, which indicated the refresh included nearly 700,000 FortiGate units, which accounted for one-fourth of the Company's total FortiGate units, dwarfing the 2023 refresh.



Later during the call when referring to the slide, Defendant Jensen stated, "[y]ou can take the units that are up there, call it 650,000 units."

28. Also during the Analyst Day, Defendant Ohlgart discussed the size of the refresh compared to prior refresh cycles. She stated:

> ***Why is it such a steep increase? First of all, it's 11 models and these were high volume models. [S]econd[,] Fortinet has grown over time. So[,] you would expect that with high volume models coming end of support, the number is growing. [T]o put it into perspective[,] [t]he 2026 cohort is about a fourth of all the registered devices, FortiGate devices that we currently have.***

29. Deutsche Bank AG analyst Brad Zelnick asked Fortinet to discuss how much revenue the refresh would bring to the Company. Specifically, he stated and asked:

> I wanted to talk about that refresh slide. So very, very helpful disclosure. I'm curious to understand would it look much different on a dollar basis as opposed to looking at units. And when we think about your midterm guidance, how does the yield that you're assuming on that refresh opportunity compared to prior refresh opportunities that you've seen. Is there an argument that yield can actually be greater because you've got a much broader, more compelling converged offering today to go cross-sell and upsell than maybe you had . . . in the past.

Defendant Ohlgart responded:

> The yield is probably around net to [Fortinet] over the next two years, around ***$400 million to $450 million in product revenue***, if with normal churn and an average price. So that's – if you put it into perspective to the total revenue, and it refreshes over two years [it] is definitely helping product revenue. Total revenue is probably up 4% . . .
>
> From a billings perspective, it's a billings event. It gives us the ability to sell more attached services and have a discussion with the customer about all the other products that may help them.
>
> So I think it's a compelling event for us to go out to the customers.

30. On December 11, 2024, Defendants Jensen and Michael Xie participated in a Barclays Global Technology Conference. During the conference, Defendant Jensen represented that the company had conducted a rigorous analysis of the refresh cycle. He stated:

> As we sat down for the Analyst Day, the 2025 planning session, we were looking at some of our data and Christiane, again, thank you very much for that. What we really saw was something unusual, which is this cohort of refreshes in 2026. And more specifically, it's products that we announced in 2021 that we're going to go

> end of service in 2026. We've done some math on that. ***We look at the unit count, we provided that number, 650,000 units.***
>
> ***And then as we converted units to dollars internally in some of our commentary, we took certain haircuts. We look at those units that are no longer pinging home, as I would call, and we excluded those is part of that conversion. We made certain assumptions around how much of that refresh has already started for a variety of reasons and how much churn we have.***
>
> ***And then we quietly uttered a number of $400 million to $450 million for the 2026 cohort.*** I would encourage everybody in the audience to do your own math.

31. Also during the call, Barclays Capital Inc. analyst Saket Kalia asked Michael Xie, "as [a] founder of the business, I mean, you've seen so many refresh cycles. What's different about this refresh cycle just from your perspective?" In response, Michael Xie stated, "a refresh happens as naturally it needs to occur. And then -- but at some point, it happens in the bulk [more] than some other times." He then indicated that customers are motivated to refresh by Fortinet's "unique technology" because it would "both increase the coverage [of network threats] as well as keeping up [with] the speed needs for the customer."

32. Approximately two months later, on February 6, 2025, Fortinet reported 4Q 2024 financial results and held an earnings conference call to discuss the results. During the call, Defendants told investors that Fortinet was beginning to see the benefits of customers refreshing their products and that the benefits would increase as the refresh cycle continued. For instance, Defendant Jensen told investors, "[i]n the fourth quarter, we saw early upgrade movement with large enterprises, both on buying plans and actual purchases. We expect the momentum to build as we move into the second half of 2025 as we get closer to the 2026 [end of] service dates." Defendant Jensen also touted "significant growth in product revenue" and stated, "when you peel back on that onion, you start to see enterprise companies have actually started their purchasing of the refreshes that we talked about at the Analyst Day."

33. During the scripted portion of the February 6, 2025 call, Defendant Jensen further emphasized that the refresh cycle would benefit the Company as it unfolded through 2026 by describing the initiatives Fortinet would carry out to maximize the refresh opportunity. He stated, "we're implementing several initiatives, including creating sales plays for each customer

segment and key vertical; expanding our account plans for larger enterprises to more specifically target the upgrade and expansion opportunities; and collaborating with our channel partners on SMB [small and medium business] opportunities, incentive programs, end user data, and developing targeted bundle offerings for these customers."

34. Also on the February 6, 2025 call, Oppenheimer & Co. analyst Ittai Kidron asked about the impact of the refresh cycle:

> If you know the devices and you can ping them and you know exactly where they are and when they get retired for the vast majority, can you just be a little bit more specific on what was the contribution of this upgrade to revenue this past quarter? And what is the exact dollar contribution you expect from the upgrade in your '25 guide?

In response, Defendant Jensen did not directly answer the question. Instead, he discussed how Fortinet was working to identify all the units that needed an upgrade, indicating that there was still significant work to be done for Fortinet to maximize the refresh opportunity, and that the Company would improve its ability to identify and upgrade eligible customers as the refresh cycle continued:

> Yes. I think -- it's a great question. And keep in mind the two-tier distribution model. We sell to distributors to sell to resell to sell to end users. And oftentimes, it's also SMB.
>
> ***The quality of the data about the end user gets better and better, the closer you get to the end user, which would be every seller. And that's why you heard a reference in the script about the importance of working with them on data gathering.***
>
> There's a bit of an honor system when they registered the devices. It may be more intuitive to us that, of course, we get a device register like our phone or something like that, but that's not what happens in practice, particularly in the SMB. And really, there's a heavy reliance there on the channel to spend time and energy if you want to get good reporting and tracking on that. So we'll get better at it as we go, and that's probably working closer with the channel partners.
>
> It is easier with the enterprises because we can talk to our sales rep [who] is working in a large enterprise and understand the account plans and what they're seeing, but you're still only getting a partial set of information[.] I think the reporting and the information will get more mature as we go along. ***It's moving pretty quickly right now on us in terms of how we're developing it.***

35. On February 21, 2025, Fortinet filed its Annual Report for 2024 on Form 10-K with the SEC. The 10-K was signed by Defendants Ken Xie, Jensen, and Ohlgart. The 10-K contained the following language: "As organizations continue to modernize their cybersecurity infrastructure, we anticipate a significant firewall refresh and upgrade cycle in the coming years. Given our platform approach, this refresh presents a strategic opportunity to expand our footprint within existing customer environments."

36. The February 21, 2025 10-K also contained a list of purported "Risks Related to Our Business and Financial Position," which included "the purchasing practices and budgeting cycles of our channel partners and end-customers, including the effect of the end of product lifecycles, refresh cycles or price decreases" and "execution risk associated with our efforts to capture opportunities related to our identified growth drivers, such as . . . product refresh cycles."

37. On March 4, 2025, Defendants Ken Xie and Jensen participated in a Morgan Stanley Technology, Media & Telecom Conference. During the conference, Morgan Stanley analyst Keith Weiss asked, "any help you can give us in terms of helping to sort of model investor expectations on how this [refresh] is going to flow through your product revenues when we think about 2025 versus 2026, just to make sure that we stay appropriately conservative, if you will?"

38. In response, Defendant Jensen represented that the refresh would be staggered through 2026 because larger customers would methodically upgrade in 2025 and 2026, while smaller customers were likely to wait until closer to the EOS deadline in 2026 to upgrade. He stated, in part:

> [W]e look at our customer base, our customer types and what our expectations are about when they're likely to start on this upgrade journey. When you look at a larger enterprise that has a more sophisticated IT organization and a more sophisticated purchasing organization and security organization, then say in SMB and they're larger upgrade cycles we believe and we saw some indications of this in the fourth quarter that ***those larger enterprises will purchase and go through the upgrade cycle in a more methodical basis.***
>
> ***It's simply too many units to take down all at once. And so while we got some tailwinds, we think, from the fourth quarter on some of our larger firewalls, we would expect those larger enterprises to continue that purchasing pattern as we get closer and closer to the end of service date.*** If you look at the SMBs, it's quite

> possible that they're more likely to wait until Sunday night to do their homework, shall we say, they may wait until closer and closer to the end of service date before they actually go through that change. And that cohort, that sub cohort could be more of a [20]26 event. You probably have another group of customers or some place in between with the service providers, which oftentimes are selling to the SMBs. But again, they're more sophisticated in their buying behaviors, their security considerations. And they're more apt to start that planning and purchasing processing process earlier than the SMBs.

39. Also on the March 4, 2025 call, Weiss asked about the magnitude of the refresh cycle and whether the refresh would allow Fortinet to cross-sell products and services as customers refreshed their FortiGates. Specifically, Weiss stated and asked:

> I think one of the things investors are excited about is a product refresh coming up within your firewall base. I think you've talked about an unusually large kind of percentage of that base seeing end of life over the next year or so. Can you talk to us about the magnitude of that opportunity? And does that -- is that just a product revenue? Is that just a firewall opportunity? Or does that give you sort of more potential to go in and sell [your] broader solution?

In response, Defendants Jensen and Ken Xie represented that the scale of the refresh cycle, technological advances, and the dramatic evolution of customer security needs would drive cross-selling opportunities, as customers would pursue broader upgrades rather than simply replacing their old "box." Specifically, Defendant Jensen responded:

> Yes. And I think what really to your last comment, we're calling it the upgrade cycle, and they really -- and we'll come back to it, but that really is the opportunity to sell the full suite of products that we have . . .
>
> ***We have an unusually large volume of units that are going end of support in 2026. It's roughly 10x more than our average in the prior 10 years. And [its] followed in 2027 with another cohort that's about half that size. It's just unusual to see the grouping of that.*** I think it has some things to do with some decisions that we made five years ago or four years ago when we announced had the support related to new chips and some other supply chain considerations.
>
> So it's really creating the opportunity. What we don't want it to be is a simple unit swap. I don't want to see something just upgrading from unit to unit.

Defendant Ken Xie replied:

> Yes. ***The customer on average has the box on hand almost 10 years [when it reaches] end of the service. And then we do see the opportunity compared to 10 years ago when they bought the box. First, the speed and then the function has a huge difference, probably average about 10 to 20x better speed. And then on***

> ***the function, probably also 2, 3x more function than the previous half. And also the customers starting to deploy the network security differently than 10 years ago. So before it's more like secure, whatever the infrastructure border, all these kind of things, now they have to expand in supporting work from home.*** They have to do internal like data center kind of eased traffic security there, internal segmentation. So we do see this as like we collaborate opportunity. So we do see the customer so far we work with always kind of come back with much bigger plan infrastructure to upgrade than the premium just replacing the old box.

40. On May 7, 2025, Fortinet reported 1Q 2025 financial results and held a conference call to discuss the results. During the call, Defendant Ohlgart stated: "Regarding the record firewall upgrade cycle that we've spoken about previously, we continue to expect the firewall upgrade to gain momentum in both purchasing and planning activities in the second half of 2025."

41. Also on the call, Morgan Stanley analyst Keith Weiss asked: "What gives you guys confidence that you're still going to be able to perform the stronger second half pickup" from the refresh? In response, Defendant Ohlgart stated:

> What gives us confidence? ***We have a number of products that have been released, the next generation. And our products provide, I think, significant improvement of total cost of ownership and security compared to what customers bought 8, 9, 10 years ago. And we see the activity going on, especially in the enterprise.***
>
> I think we mentioned in the -- in our prepared remarks that FortiGates grew faster than the rest of product revenue, which I think is a testament to the strength that we are seeing.

42. The statements referenced in ¶¶ 25-41 were materially false and/or misleading. In truth, Defendants knew that the refresh cycle would never be as lucrative as they represented, nor could it, because it consisted of old products that were a "small percentage" of the Company's business. Moreover, Defendants misrepresented and concealed that they did not have a clear picture of the true number of FortiGate firewalls that could be upgraded. And while telling investors that the refresh would gain momentum over the course of two years, Fortinet misrepresented and concealed that it had aggressively pushed through roughly half of the refresh in a period of months, by the end of 2Q 2025.

The Truth Is Revealed

43. On August 6, 2025, after market hours, Fortinet released its 2Q 2025 financial results and held an earnings conference call to discuss the results. During the call, Defendant Ohlgart revealed that: "We estimate that we are approximately 40% to 50% of the way through the 2026 upgrade cycle at the end of the second quarter based on the remaining active units and service contracts."

44. Also during the call, Goldman Sachs analyst Gabriela Borges asked, in light of "your prepared remarks that we are 40% to 50% through the 2026 refresh cohort," that "2025 is a really big or larger than normal refresh cohort," and that the Company had a successful refresh in 2023, "why are we not seeing more upside in the numbers this year from the refresh cohort?" Borges then suggested, "[i]s it possible that perhaps customers have excess capacity in their networks from a 2021 COVID-type elevated throughput environment?" In response, Defendant Ohlgart indicated that Fortinet did not have a handle on how many of its smaller customers would refresh. Specifically, she stated, that "where it's harder for us to predict" and where "we can only track registration rates and similar is in the lower end." Defendant Ohlgart also agreed with Borges that "there could be some excess capacity from prior years that has been replaced or that is replacing some of the EOS models."

45. Also in response to Borges's question, Defendant Ken Xie stated that the refresh involves very old firewalls, sold at a time when Fortinet's business was 5-10 times smaller, meaning that the total number of units eligible for upgrade was inherently limited. Ken Xie also noted that the current refresh was not as successful as the 2023 refresh because the 2023 refresh consisted of products that were only four or five years old. Specifically, he stated:

> Yeah. Also the -- the refresh upgrade of the product go out next year is the product[s that are] like 12 to 15 years after we introduced the product. It's not a product like four, five years [old] [during the 2023 refresh]. . . But if you compare [Fortinet now] to like a 10, 12, 15 years ago, the business size probably like current size is probably 5 times, maybe even 10 times larger. So that's where the operate refresh, we do see is very different than the [2023 refresh].
>
> It's a much older product. We really -- after we introduced a new product, they use every selling maybe like seven, eight years. And then after we stop selling

> still supporting five additional year[s] for the service. After five additional year[s] stop shipping, but we do support service, then the customer reach to the end of service. So that's early probably average maybe like 12 to 15 years after the product being introduced.
>
> So that's the sense we kind of try to help customers to upgrade. And so like I said, even we have a large number of products, but that's utilized the business we have like 12, 15 years ago.

46. Later during the August 6, 2025 call, Defendant Ken Xie admitted that "[e]ven [if] all this product" available for the refresh upgraded "within like one or two years [it would] still not [provide] much business impact." He added, "the business impact for the old device is also a much smaller percentage than the total business we have today" and described the refresh as "a pretty small percentage of our total business."

47. As a result of this news, Fortinet's common stock price dropped over 22%, from $96.58 per share on August 6, 2025 to $75.30 per share on August 7, 2025, on unusually high trading volume.

LOSS CAUSATION

48. During the Class Period, as detailed herein, Defendants made materially false and misleading statements and omissions, and engaged in a scheme to deceive the market. This artificially inflated the price of Fortinet common stock and operated as a fraud or deceit on the Class. Later, when Defendants' prior misrepresentations and fraudulent conduct were disclosed to the market on August 6, 2025, as alleged herein, the price of Fortinet common stock fell precipitously, as the prior artificial inflation came out of the price. As a result of their purchases of Fortinet common stock during the Class Period, Plaintiff and other members of the Class suffered economic loss, *i.e.*, damages, under the federal securities laws.

SCIENTER ALLEGATIONS

49. As alleged herein, Defendants acted with scienter because Defendants knew that the public statements issued or disseminated in the name of the Company were materially false and/or misleading; knew that such statements would be issued or disseminated to the investing public; and knowingly and substantially participated or acquiesced in the issuance or dissemination of such statements as primary violators of the federal securities laws. As set forth

elsewhere herein, the Individual Defendants, by virtue of their receipt of information reflecting the true facts regarding Fortinet, their control over allegedly materially misleading misstatements and/or their associations with the Company which made them privy to confidential proprietary information concerning Fortinet, participated in the fraudulent scheme alleged herein.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of all persons who purchased or otherwise acquired Fortinet common stock during the Class Period (the "Class"). Excluded from the Class are Defendants and their families, directors, and officers of Fortinet and their families and affiliates.

51. The members of the Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court. As of August 5, 2025, there were 766,266,033 shares of Fortinet common stock outstanding, owned by at least thousands of investors.

52. There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class which predominate over questions which may affect individual Class members include:

A. Whether Defendants violated the Exchange Act;

B. Whether Defendants omitted and/or misrepresented material facts;

C. Whether Defendants' statements omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading;

D. Whether Defendants knew or recklessly disregarded that their statements and/or omissions were false and misleading;

E. Whether the price of Fortinet's common stock was artificially inflated;

F. Whether Defendants' conduct caused the members of the Class to sustain damages; and

G. The extent of damage sustained by Class members and the appropriate measure of damages.

53. Plaintiff's claims are typical of those of the Class because Plaintiff and the Class sustained damages from Defendants' wrongful conduct.

54. Plaintiff will adequately protect the interests of the Class and has retained counsel experienced in class action securities litigation. Plaintiff has no interests which conflict with those of the Class.

55. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

INAPPLICABILITY OF STATUTORY SAFE HARBOR

56. Fortinet's "Safe Harbor" warnings accompanying its forward-looking statements issued during the Class Period were ineffective and inapplicable, and cannot shield the statements at issue from liability.

57. Defendants are also liable for any false or misleading forward-looking statements pleaded herein because, at the time each such statement was made, the speaker knew the statement was false or misleading and the statement was made by or authorized and/or approved by an executive officer of Fortinet who knew that the statement was false.

PRESUMPTION OF RELIANCE

58. At all relevant times, the market for Fortinet's common stock was an efficient market for the following reasons, among others:

A. The Company's shares met the requirements for listing, and were listed and actively traded on the NASDAQ, a highly efficient and automated market;

B. As a regulated issuer, Fortinet filed periodic public reports with the SEC;

C. Fortinet regularly and publicly communicated with investors via established market communication mechanisms, including through regular disseminations of press releases on the national circuits of major newswire services, and through

other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services; and

D. Fortinet was followed by securities analysts employed by major brokerage firms who wrote reports which were distributed to the sales force and certain customers of their respective brokerage firms. Each of these reports was publicly available and entered the public marketplace.

59. As a result of the foregoing, the market for Fortinet common stock promptly digested current information regarding Fortinet from all publicly available sources and reflected such information in the price. Under these circumstances, all purchasers of Fortinet common stock during the Class Period suffered similar injury through their purchase of Fortinet common stock at artificially inflated prices and the presumption of reliance applies.

60. A Class-wide presumption of reliance is also appropriate in this action under the Supreme Court's holding in *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972), because the Class's claims are grounded on Defendants' material omissions.

COUNT I

For Violation of Section 10(b) of the Exchange Act and Rule 10b-5 Against All Defendants

61. Plaintiff repeats and re-alleges each and every allegation contained above as if fully set forth herein.

62. During the Class Period, Defendants carried out a plan, scheme, and course of conduct which was intended to and, throughout the Class Period, did: (i) deceive the investing public, including Plaintiff and other Class members, as alleged herein; and (ii) cause Plaintiff and other members of the Class to purchase Fortinet common stock at artificially inflated prices.

63. Defendants (i) employed devices, schemes, and artifices to defraud; (ii) made untrue statements of material fact and/or omitted to state material facts necessary to make the statements not misleading; and (iii) engaged in acts, practices, and a course of business which operated as a fraud and deceit upon the purchasers of the Company's common stock in an effort

to maintain artificially high market prices for Fortinet common stock in violation of Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

64. Defendants, individually and in concert, directly and indirectly, by the use, means or instrumentalities of interstate commerce and/or of the mails, engaged and participated in a continuous course of conduct to conceal adverse material information about Fortinet's "record" refresh cycle as specified herein.

65. During the Class Period, Defendants made the false statements specified above which they knew or recklessly disregarded to be false or misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

66. Defendants had actual knowledge of the misrepresentations and omissions of material fact set forth herein, or recklessly disregarded the true facts that were available to them. Defendants engaged in this misconduct to conceal the truth about the Company's "record" refresh cycle as specified herein, from the investing public and to support the artificially inflated prices of the Company's common stock.

67. Plaintiff and the Class have suffered damages in that, in reliance on the integrity of the market, they paid artificially inflated prices for Fortinet's common stock. Plaintiff and the Class would not have purchased the Company's common stock at the prices they paid, or at all, had they been aware that the market prices had been artificially inflated by Defendants' fraudulent course of conduct.

68. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their respective purchases of the Company's common stock during the Class Period.

69. By virtue of the foregoing, Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

COUNT II

For Violation of Section 20(a) of the Exchange Act Against The Individual Defendants

70. Plaintiff repeats, incorporates, and re-alleges each and every allegation set forth above as if fully set forth herein.

71. The Individual Defendants acted as controlling persons of Fortinet within the meaning of Section 20(a) of the Exchange Act. By virtue of their high-level positions, participation in and/or awareness of the Company's operations, direct involvement in the day-to day operations of the Company, and/or intimate knowledge of the Company's actual performance, and their power to control public statements about Fortinet, the Individual Defendants had the power and ability to control the actions of Fortinet and its employees. By reason of such conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act.

PRAYER FOR RELIEF

72. **WHEREFORE**, Plaintiff prays for judgment as follows:

A. Determining that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure;

B. Awarding compensatory damages in favor of Plaintiff and other Class members against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Awarding Plaintiff and the Class their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

D. Awarding such equitable/injunctive or other further relief as the Court may deem just and proper.

JURY DEMAND

73. Plaintiff demands a jury trial.

Dated: September 22, 2025

Respectfully submitted,

/