

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

_____, 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

19 Plaintiff __ (“Plaintiff”), by and through its counsel, alleges the following upon
20 personal knowledge as to itself and its own acts, and upon information and belief as to all
21 other matters. Plaintiff’s information and belief are based on, among other things, the
22 independent investigation of counsel. This investigation includes, but is not limited to, a
23 review and analysis of: (i) public filings by Fortinet, Inc. (“Fortinet” or the “Company”)
24 with the Securities and Exchange Commission (“SEC”); (ii) transcripts of Fortinet
25 conferences with investors and analysts; (iii) press releases and media reports issued and
26 disseminated by the Company; (iv) analyst reports concerning Fortinet; and (v) other public
27 information and data regarding the Company.
28

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 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

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

4 **SUBSTANTIVE ALLEGATIONS**

5 **Background**

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

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

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

23 22. During the COVID-19 pandemic, many companies shifted employees to remote
24 work which caused a surge in demand for Fortinet's products. Moving employees to remote
25 work meant that companies had to secure all the new remote connections to their networks which
26 often meant buying more or better firewalls. Fortinet experienced strong product revenue growth
27 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.

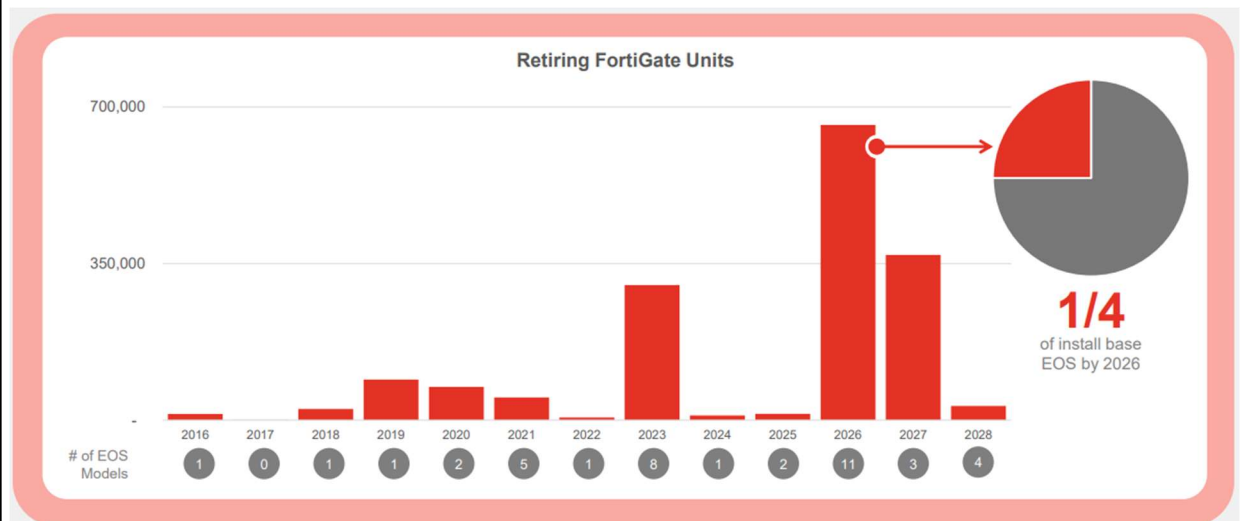
1 In response, Defendant Jensen indicated certain larger customers would start to methodically
2 upgrade in 2025 and touted the size of the refresh, particularly as compared to its 2023 refresh
3 cycle:

4 I think that we see these end-of-life of these products starting in the second half
5 of 2026. We don't expect the customers to wait until the 11[th] hour to make the
6 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.

7 So we saw a similar -- not similar, we saw a lift, if you will, similarly in 2023,
8 although **the magnitude in 2026 is much, much larger**. And why it's relevant to
9 2023 is that if you go back and look at product revenue growth in 2022, very
10 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.

11 To the second part of your comment, as I mentioned, **the absolute number that**
12 **we see in 2026 is by far the largest we've seen probably ever**, but certainly in the
13 last five or six years. It is -- each year is dominated by the entry-level firewalls.
14 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.

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



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

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

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

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

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

19 Defendant Ohlgart responded:

20 The yield is probably around net to [Fortinet] over the next two years, around
21 ***\$400 million to \$450 million in product revenue***, if with normal churn and an
22 average price. So that's – if you put it into perspective to the total revenue, and it
23 refreshes over two years [it] is definitely helping product revenue. Total revenue
24 is probably up 4% . . .

25 From a billings perspective, it's a billings event. It gives us the ability to sell more
26 attached services and have a discussion with the customer about all the other
27 products that may help them.

28 So I think it's a compelling event for us to go out to the customers.

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

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

1 end of service in 2026. We've done some math on that. *We look at the unit count,*
2 *we provided that number, 650,000 units.*

3 *And then as we converted units to dollars internally in some of our commentary,*
4 *we took certain haircuts. We look at those units that are no longer pinging*
5 *home, as I would call, and we excluded those is part of that conversion. We*
6 *made certain assumptions around how much of that refresh has already started*
7 *for a variety of reasons and how much churn we have.*

8 *And then we quietly uttered a number of \$400 million to \$450 million for the*
9 *2026 cohort.* I would encourage everybody in the audience to do your own math.

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

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

27 33. During the scripted portion of the February 6, 2025 call, Defendant Jensen further
28 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

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

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

7 If you know the devices and you can ping them and you know exactly where they
8 are and when they get retired for the vast majority, can you just be a little bit more
9 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?

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

15 Yes. I think -- it’s a great question. And keep in mind the two-tier distribution
16 model. We sell to distributors to sell to resell to sell to end users. And oftentimes,
17 it’s also SMB.

18 ***The quality of the data about the end user gets better and better, the closer you***
19 ***get to the end user, which would be every seller. And that’s why you heard a***
20 ***reference in the script about the importance of working with them on data***
gathering.

21 There’s a bit of an honor system when they registered the devices. It may be more
22 intuitive to us that, of course, we get a device register like our phone or something
23 like that, but that’s not what happens in practice, particularly in the SMB. And
24 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.

25 It is easier with the enterprises because we can talk to our sales rep [who] is
26 working in a large enterprise and understand the account plans and what they’re
27 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.

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

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

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

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

21 [W]e look at our customer base, our customer types and what our expectations are
22 about when they’re likely to start on this upgrade journey. When you look at a
23 larger enterprise that has a more sophisticated IT organization and a more
24 sophisticated purchasing organization and security organization, then say in SMB
25 and they’re larger upgrade cycles we believe and we saw some indications of this
26 in the fourth quarter that ***those larger enterprises will purchase and go through
the upgrade cycle in a more methodical basis.***

26 ***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
27 would expect those larger enterprises to continue that purchasing pattern as we
28 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***

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

9 40. On May 7, 2025, Fortinet reported 1Q 2025 financial results and held a conference
10 call to discuss the results. During the call, Defendant Ohlgart stated: "Regarding the record
11 firewall upgrade cycle that we've spoken about previously, we continue to expect the firewall
12 upgrade to gain momentum in both purchasing and planning activities in the second half of
13 2025."

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

17 What gives us confidence? *We have a number of products that have been*
18 *released, the next generation. And our products provide, I think, significant*
19 *improvement of total cost of ownership and security compared to what*
20 *customers bought 8, 9, 10 years ago. And we see the activity going on, especially*
21 *in the enterprise.*

22 I think we mentioned in the -- in our prepared remarks that FortiGates grew faster
23 than the rest of product revenue, which I think is a testament to the strength that
24 we are seeing.

25 42. The statements referenced in ¶¶ 25-41 were materially false and/or misleading.
26 In truth, Defendants knew that the refresh cycle would never be as lucrative as they represented,
27 nor could it, because it consisted of old products that were a "small percentage" of the Company's
28 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

1 still supporting five additional year[s] for the service. After five additional year[s]
2 stop shipping, but we do support service, then the customer reach to the end of
3 service. So that's early probably average maybe like 12 to 15 years after the
4 product being introduced.

5 So that's the sense we kind of try to help customers to upgrade. And so like I said,
6 even we have a large number of products, but that's utilized the business we have
7 like 12, 15 years ago.

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

13 47. As a result of this news, Fortinet's common stock price dropped over 22%, from
14 \$96.58 per share on August 6, 2025 to \$75.30 per share on August 7, 2025, on unusually high
15 trading volume.

16 **LOSS CAUSATION**

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

25 **SCIENTER ALLEGATIONS**

26 49. As alleged herein, Defendants acted with scienter because Defendants knew that
27 the public statements issued or disseminated in the name of the Company were materially false
28 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

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

5 **CLASS ACTION ALLEGATIONS**

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

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

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

- 17 A. Whether Defendants violated the Exchange Act;
18 B. Whether Defendants omitted and/or misrepresented material facts;
19 C. Whether Defendants’ statements omitted material facts necessary in order to make
20 the statements made, in light of the circumstances under which they were made,
21 not misleading;
22 D. Whether Defendants knew or recklessly disregarded that their statements and/or
23 omissions were false and misleading;
24 E. Whether the price of Fortinet’s common stock was artificially inflated;
25 F. Whether Defendants’ conduct caused the members of the Class to sustain
26 damages; and
27
28

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

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

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

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

10 **INAPPLICABILITY OF STATUTORY SAFE HARBOR**

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

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

18 **PRESUMPTION OF RELIANCE**

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

- 21 A. The Company's shares met the requirements for listing, and were listed and
22 actively traded on the NASDAQ, a highly efficient and automated market;
23 B. As a regulated issuer, Fortinet filed periodic public reports with the SEC;
24 C. Fortinet regularly and publicly communicated with investors via established
25 market communication mechanisms, including through regular disseminations of
26 press releases on the national circuits of major newswire services, and through
27
28

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

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

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

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

15 **COUNT I**

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

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

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

23 63. Defendants (i) employed devices, schemes, and artifices to defraud; (ii) made
24 untrue statements of material fact and/or omitted to state material facts necessary to make the
25 statements not misleading; and (iii) engaged in acts, practices, and a course of business which
26 operated as a fraud and deceit upon the purchasers of the Company's common stock in an effort
27
28

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

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

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

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

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

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

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

1 **COUNT II**

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

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

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

13 **PRAYER FOR RELIEF**

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

- 15 A. Determining that this action is a proper class action under Rule 23 of the Federal
16 Rules of Civil Procedure;
- 17 B. Awarding compensatory damages in favor of Plaintiff and other Class members
18 against all Defendants, jointly and severally, for all damages sustained as a result
19 of Defendants' wrongdoing, in an amount to be proven at trial, including interest
20 thereon;
- 21 C. Awarding Plaintiff and the Class their reasonable costs and expenses incurred in
22 this action, including attorneys' fees and expert fees; and
- 23 D. Awarding such equitable/injunctive or other further relief as the Court may deem
24 just and proper.

25 **JURY DEMAND**

26 73. Plaintiff demands a jury trial.
27
28