UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SECTRA COMMUNICATIONS AB, *Plaintiff*, v. CISCO SYSTEMS, INC., *Defendant*.	Case No. 2:26-CV-00174-RWS-RSP (Lead Case) **JURY TRIAL DEMANDED**
SECTRA COMMUNICATIONS AB, *Plaintiff*, v. FORTINET, INC., *Defendant*.	Case No. 2:26-CV-00175-RWS-RSP (Member Case) **JURY TRIAL DEMANDED**

RESPONSE BRIEF OF DEFENDANTS CISCO AND FORTINET
IN OPPOSITION TO PLAINTIFF SECTRA'S
MOTION TO COMPEL COMPLIANCE WITH PROTECTIVE ORDER

The parties' only remaining dispute is over the use of ***the AI-based tools*** (Cline, Ollama, and Qwen) to review Defendants' source code. Defendants agree that Plaintiff can use the non-AI tools (Python and Node.js), but they cannot agree to the use of AI-based tools. Plaintiff's request to use AI-based tools poses both known and unknowable risks to the security of Defendants' source code. Plaintiff's request is not based on an allegation that Plaintiff or its expert is unable to fairly assess and review Defendants' source code with non-AI tools. Instead, Plaintiff bases its request on its own convenience and cost savings. *See* Dkt. 42, p. 6.

In doing so, Plaintiff's Motion ignores the recurring headlines about previously unknown risks posed by AI, including AI tools breaking free from restricted environments even though engineers believed there was no Internet connection, as shown below. Plaintiff asks this Court to nonetheless blaze a new trail by endorsing the safety of these AI-based tools—and to do so based on the declaration of an expert who does not purport to have expertise in the creation, architecture, or operation of AI models and tools; his only qualification is as a user of AI. *See* Dkt. 42, Ex. at ¶ 1. Any benefit from these tools is far outweighed by the risks imposed on Defendants' businesses.

To be clear, neither Cisco's nor Fortinet's source code has ever been reviewed by any opposing counsel in any case using AI-based tools (and the same is true even for their own outside counsel). Declaration of Mubashir Hussain ("Hussain Decl."), ¶¶ 8-9; Declaration of Carl Windsor ("Windsor Decl."), ¶ 5. As far as Defendants know, this is the first case in which an opposing party has made this request to either Cisco or Fortinet. And rather than doing so when negotiating the Protective Order, Plaintiff made this request via the Court's expedited process for discovery disputes, limited to a total of 5 pages of attachments (which Plaintiff exceeded). Plaintiff made this request after agreeing to the same terms in the Protective Order with which Defendants have complied in dozens (if not hundreds) of cases without any form of AI review of their source code.

As shown below, the Court should deny Plaintiff's request for two independent bases.

First, there is a straightforward, threshold basis for denial: Plaintiff's request is incompatible with Paragraph 10(a) in the Protective Order (Dkt. 38; hereinafter the "PO").

Second, the Court should deny the request under Rule 26(b)(1) because:

1. Source code is considered to be a company's crown jewels.
2. The use of AI-based review tools poses enormous risks to these crown jewels.
3. These risks are completely unnecessary for Plaintiff to fairly review the source code.

Each basis is discussed below. The statement by Plaintiff's expert that "the requested tools provide a cutting-edge approach to review" captures the issue. PO at ¶ 12. Simply put, the review of an opposing party's source code is the last area in litigation where "cutting edges" should be allowed. Instead, the maxim, "if it ain't broke, don't fix it," is far more appropriate.[1]

I. The Protective Order Cannot Be Reconciled With Plaintiff's Request

Plaintiff all but admits that AI-based tools are not safe for reviewing source code if access is provided over an Internet connection via a "thin client." Dkt. 41, p. 3-4. Plaintiff posits, however, that its proposed AI tools will be safe if the producing party is required to produce code on a non-networked, stand-alone computer. *Id*. Plaintiff then argues that Cisco's decision to produce code on a "thin client" over the Internet (instead of a non-networked stand-alone computer) is so unreasonable that Cisco is in violation of the PO by declining Plaintiff's request to use a standalone computer loaded with AI-based tools. *Id.* at 4 ("Cisco cannot use its own choice of production methodology to deprive Sectra of legitimate review tools."). But Paragraph 10(a) of the PO (to which Plaintiff agreed) says exactly the opposite, giving the producing party the sole decision:

[1]Of course, a day may come when AI-based tools are appropriate for source code review, perhaps based on a long record of safety testing after the underlying technology is better understood. But that time is certainly not now.

> Access to a Party's Source Code Material shall be provided only on (1) "stand-alone" computer(s) (that is, the computer may not be linked to any network, including a local area network ("LAN"), an intranet, or the Internet) or (2) up to two remote thin client computer(s) used to access source code material on a virtual machine maintained behind the producing Party's firewall (collectively, "stand-alone computer(s)" or "Source Code Computer(s)"), where **the decision to use (1) or (2) is solely the decision of the producing Party**.

PO at ¶ 10(a) (bold added).[2] Plaintiff would eliminate the PO's second option altogether. If Plaintiff's position were correct—that the PO gives it the right to use AI tools—then this provision would not exist, as the decision of whether to use option (1) or option (2) would instead be "solely the decision of the [receiving] Party." This basic contradiction undoes Plaintiff's entire position.

Moreover, nothing in the PO even suggests that the producing party must agree to AI-based review tools. The guiding standard is in ¶ 10(e)(i), as follows: "The Source Code Computer(s) shall be reasonably configured to permit the receiving Party to review the Source Code Material…." Plaintiff can review the code without AI-based tools, as Plaintiff does not contend that any of the tools Defendants approved are insufficient. Likewise, the PO's directive that Defendants cannot "unreasonably withhold" permission to install a requested tool does not support this Motion. As shown below, Defendants' position on AI-based tools is eminently reasonable.

II. The Court Should Deny Plaintiff's Request Under Rule 26(b)(1)

A. Defendants' Source Code Is Their Crown Jewels

For companies like Cisco and Fortinet, source code is their crown jewels. This is why there are special protections for source code in Protective Orders. *See* PO at ¶ 10. The source code at issue here unquestionably qualifies for "crown jewel" status. Hussain Decl., ¶ 4; Windsor Decl., ¶

[2] The existence of this second option reflects the extreme risk involved with any source code production. The first option (a "standalone computer") is a physically movable device. If it inadvertently fell into the wrong hands, the harm could be irreparable. As a result, some companies (such as Cisco) produce code via a network-connected "thin client" that allows the reviewer to access the code on the company's network but likewise allows any access to be terminated if the computer inadvertently falls into the wrong hands. Hussain Decl., ¶ 7.

3. Access to this source code is highly restricted even inside each Defendant. Hussain Decl., ¶ 3; Windsor Decl., ¶ 3. The inadvertent disclosure of the code sought in this case would cause enormous, irreparable damage to Defendants. Hussain Decl., ¶¶ 5-6; Windsor Decl., ¶¶ 3, 6.[3]

B. AI Poses Unique Risks To The Security Of Defendants' Crown Jewels

The use of AI by non-employees to review source code poses unique and untested risks to the security of the source code. Plaintiff's description of the meet-and-confer misses the forest for the trees. Defendants' basic point is that the risks of AI are unknowable ahead of time, precisely because AI is not deterministic. The scenarios in Plaintiff's Motion are barely the tip of the iceberg.

The Dangers Are Real. Even in a so-called "sandboxed" environment purportedly cut off from access to anything outside of the controlled environment, recent reports abound of AI tools breaking free. OpenAI and Anthropic both made headlines due to their AI models escaping closed environments and hacking outside organizations.[4] Anthropic's AI was able to take advantage of a misconfiguration of Anthropic's system in order to access the internet, and OpenAI's model similarly escaped its closed environment. Google made headlines just last week, when its model "autonomously" "accessed the internet and hacked other companies" in three separate cases.[5]

---

[3] Courts have long recognized this basic point. *See, e.g., Mod. Font Applications LLC v. Alaska Airlines, Inc.*, 56 F.4th 981, 990 (Fed. Cir. 2022) (Newman, J., dissenting) ("It is well-recognized that source code may be a company's 'crown jewels,' *Unwired Planet LLC v. Apple, Inc.*, 2013 WL 1501489, at *5 (D. Nev. Apr. 11, 2013), and "its secrecy is of enormous commercial value," *Viacom Int'l Inc. v. YouTube Inc*., 253 F.R.D. 256, 259 (S.D.N.Y. 2008).'"

[4] *See* Chia Osmund & Laura Cress, *Anthropic's Claude AI escapes to hack into three organisations*, BBC (July 31, 2026) https://www.bbc.com/news/articles/cz7dl7w8y7po; Joe Tidy, *OpenAI says its rogue AI tried to hack other companies,* BBC (July 29, 2026) https://www.bbc.com/news/articles/c2el319vzr3o.

[5] *See* Erin Woo & Robert McMillan, *Gemini Hacked Three Companies in First Known Breakout by Google's AI*, The Wall Street Journal (September 18, 2026) https://www.wsj.com/tech/ai/gemini-hacked-three-companies-in-first-known-breakout-by-googles-ai-5c0baba2?st=4NcmXo. Not all security breaches have been disclosed by the AI companies themselves; some are only discovered by security researchers. *Id.*

Plaintiff argues that similar incidents would be impossible if Defendants are required to only use option "(1)" in the PO (as Fortinet intends to do) because there is "no network interface (Fortinet's setup)". Dkt. 42, p. 4. Beyond re-writing the PO (as described in Section I), Plaintiff is incorrect. Laptops come with integrated networking hardware such as Bluetooth radios, and it is becoming more apparent that AI can work around restrictions placed on such hardware. For example, OpenAI was conducting an "internal" test in what it believed was a restricted environment for its own AI tool that had no internet access.[6] "The plan was to have it solve a cybersecurity challenge in an environment with no internet access." *Id.* The AI tool, on its own, "found an unknown vulnerability to escape the sandbox and gain[] internet access," and then hacked several different companies. *Id.* In addition to such escapes, OpenAI reported a number of other events that, while less interesting to the mass media, are equally alarming here, such as "Uploading files to the internet in order to cite to them"; "Unsanctioned Artifactory writes and cross-sample communication"; "Unauthorized communication via temporary file hosting services."[7]

Plaintiff's Assurances Are Insufficient. The assurances from Plaintiff's counsel (who do not purport to be AI experts) and its expert (who claims only to be a user of AI) that the AI-based tools will operate the same way as non-AI tools are as cavalier as they are uncredentialed. With AI, the human reviewer does not know exactly what the tool will do. That is a fundamental aspect

---

[6] *See* Lorenzo Franceschi-Bicchierai, TechCrunch (August 27, 2026) https://techcrunch.com/2026/08/27/heres-all-the-times-ai-has-gone-rogue-and-hacked-othercompanies/.

[7] *See* OPENAI ALIGNMENT RESEARCH BLOG (September 16, 2026) https://alignment.openai.com/misalignment-reports/uploading-files-to-the-internet-in-order-to-cite-them/ ; OPENAI ALIGNMENT RESEARCH BLOG (September 16, 2026) https://alignment.openai.com/misalignment-reports/unauthorized-artifactory-writes-and-cross-sample-communication/ ; OPENAI ALIGNMENT RESEARCH BLOG (September 16, 2026) https://alignment.openai.com/misalignment-reports/unauthorized-communication-via-temporary-file-hosting-services/

of AI; there is no human-readable source code to evaluate the ever-evolving capabilities of the tool. Hussain Decl., ¶ 2; Windsor Decl., ¶ 2.

Plaintiff's expert does not purport to have actual expertise in the creation or operation of AI. *See* Dkt. 41, Ex. 1. His only AI-related qualification stated in his declaration is that his "experience includes using large language models to search, analyze, and generate source code." *Id.* at ¶ 1. That's it; he is only a ***user*** of AI. Yet, Plaintiff asserts that this assurance is enough for the Court to re-write the rules of engagement on source code reviews. Like everyone else surprised by the recent headlines, Plaintiff's expert has no way of knowing what a given AI tool might do.

Plaintiff acknowledges that Defendants have extensive experience with the operation of AI and the large language models they employ internally, even referencing Cisco's "prowess" in AI. Dkt. 42, p. 3, 7. This extensive knowledge of both network security and the risks and rewards of AI is precisely why Defendants' position on the review of their source code with AI is so firm.

C. These Risks Are Unnecessary For Plaintiff To Fairly Review The Source Code

Plaintiff's request would impose new burdens and risks on Defendants without a sufficient basis. Plaintiff alleges that the standard practice of reviewing code with non-AI tools is "disproportionately burdensome and inconsistent with the principles of Federal Rule of Civil Procedure 26(b)(1)." Dkt. 42, p. 6. But Plaintiff's burden is no different now than before, and any convenience from AI-based tools is far outweighed by the risks and burdens on Defendants. Plaintiff's proposed path for Cisco highlights the burden. After forcing Cisco to use a stand-alone computer, Plaintiff would require that Cisco "examine the model architecture and verify exactly what is being installed" and then "compare the original code with the reviewed code" to check that its code had not been modified. *Id.* at 4, 5. The only justification is making Plaintiff's job easier—at the cost of increasing Defendants' burden and risking their crown jewels. *Id.* at 6.

Defendants have not located a case in which a court addressed this issue in a contested motion. The analogous case law, however, speaks with one voice. Even without the unique risks of AI, courts reject requests for atypical procedures in reviewing source code, precisely because the risk outweighs any convenience. *See, e.g., Philips N. Am. LLC v. Global Med. Imaging, LLC*, 343 F.R.D. 59, 66 (N.D. Ill. 2022) (rejecting request to store scripts on the source code computer: "the Court is unable to confirm the claim that there is 'no plausible risk' to the source code from adoption of the atypical procedure."). The PO in *Philips* did not limit the experts' ability to review the code, so there was no "sufficient justification for the provision that Defendants seek for the convenience of their expert to speed the review of source code." *Id.* at 67. Likewise, in *Berkheimer v. Hewlett-Packard Co*., 2014 WL 12959469, at *3 (N.D. Ill. Apr. 7, 2014), the court "recognize[d] that it may be more inconvenient for Plaintiffs' expert to have to review the source code in the manner proposed by Defendant, but such inconvenience is not outweighed by the legitimate concerns of Defendant to protect its source code." The court found this was "an unnecessary risk" because "Plaintiffs' convenience-based arguments do not outweigh Defendant's legitimate concerns regarding inadvertent disclosure of its highly confidential and highly valuable source code if electronic copies of Defendant's source code were to be produced." *Id.* at *3.[8]

[8] The assertion that Plaintiff's expert used this "without objection" in one other case (a case not involving either Defendant here) is the exception that proves the rule. Dkt. 41 at 6. Courts have rejected demands that a producing party use AI-based tools to search even its own documents for production. The court's analysis in *Hyles v. New York City*, No. 10 Civ. 3119 (AT) (AJP), 2016 WL 4077114 (S.D.N.Y. Aug. 1, 2016), is equally applicable to the context of Plaintiff's Motion here: "While Hyles may well be correct that production using keywords may not be as complete as it would be if TAR were used [], the standard is not perfection, or using the 'best' tool [], but whether the search results are reasonable and proportional. Cf. Fed. R. Civ. P. 26(g)(1)(B)." *Id.* at *3. As that court summarized the issue, when a party demands the use of a tool over reasonable alternatives, "[t]he short answer is a decisive 'NO.'" *Id.* at *1.

Dated: September 25, 2026

Respectfully submitted,

/s/ Matthew C. Gaudet
Matthew C. Gaudet
mcgaudet@duanemorris.com
David C. Dotson
dcdotson@duanemorris.com
Alice E Snedeker
aesnedeker@duanemorris.com
DUANE MORRIS LLP
1075 Peachtree Street NE, Suite 1700
Atlanta, GA 30309-3929
Telephone: 404.253.6900
Facsimile: 404.253.6901

Melissa R. Smith
Texas State Bar No. 24001351
melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, Texas 75670
Phone: (903) 934-8450
Fax: (903) 934-9257

Counsel for Defendants Cisco Systems, Inc. and Fortinet, Inc.

CERTIFICATE OF SERVICE

The undersigned counsel hereby certifies that on September 25, 2026, a true and correct copy of the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all attorneys of record.

/s/ Melissa R. Smith
Melissa R. Smith