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

SECTRA COMMUNICATIONS AB, Plaintiff, v. CISCO SYSTEMS, INC. Defendant.	Civil Action No. 2:26-cv-00174-RWS (LEAD CASE) Jury Trial Demanded
SECTRA COMMUNICATIONS AB, Plaintiff, v. FORTINET, INC. Defendant.	Civil Action No. 2:26-cv-00175-RWS Jury Trial Demanded

PLAINTIFF SECTRA COMMUNICATIONS AB'S REPLY IN SUPPORT OF MOTION TO COMPEL COMPLIANCE WITH PROTECTIVE ORDER

Defendants abandon almost every objection raised prior to the motion—including their objections to Python and Node.js, their "read-only" objection, and their reliance on Paragraph 10(e)(iii) of the Protective Order. Defendants now ask the Court to prohibit legitimate source code review tools (which are already being used in another case in this District involving a competitor of Defendants) based on a generalized fear of AI. But the PO does not permit Defendants to withhold approval based on stigma. It requires a reasonable basis. Defendants have none.

I. EVERY CITED AI "BREAKOUT" INVOLVED A NETWORKED COMPUTER.

The thrust of Defendants' response is a generalized fear of AI models "breaking free." ECF 45 at 4. But Defendants fail to mention—and, indeed, actively obscure—that ***in every case Defendants cite, the model had internet access.*** The Claude incident: "a 'misconfiguration' … left the models with live internet access."[1] The OpenAI incident: the models "had very limited internet access"—meaning there *was* internet access.[2] The Gemini incident: "internet access was unintentionally made available."[3] None involved a non-networked environment. And the PO *requires* such an environment, absent Cisco's choice to use a remote thin client. *See* ECF 38, ¶ 10(a).

II. EXISTING SAFTEY MEASURES ARE SUFFICIENT.

Not one time do Defendants contest that disabling or removing network hardware completely mitigates the risk of the tools improperly accessing a network. Defendants instead dance around the issue. They first allege that "AI can work around restrictions placed on such hardware," citing the "breakout" instances. ECF 45 at 5. But none of those instances involved AI working around disabled

[1]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.
[2]Ashley Capoot, *New details in the OpenAI Hugging Face hack show how far agents will go: 'It's now remarkably easy'*, CNBC (July 30, 2026), https://www.cnbc.com/2026/07/30/open-ai-hugging-face-hack-latest.html.
[3]Erin Woo & Robert McMillan, *Gemini Hacked Three Companies in First Known Breakout by Google's AI*, Wall St. J. (Sept. 18, 2026), https://www.wsj.com/tech/ai/gemini-hacked-three-companies-in-first-known-breakout-by-googles-ai-5c0baba2?st=4NcmXo.

or non-existent hardware—every instance involved an AI model using an ***existing network connection***, i.e., ***enabled hardware***. Defendants also raise Bluetooth with no explanation. *See* ECF 45 at 6. But Bluetooth hardware can likewise be disabled or removed. ECF 42-1, ¶ 9. Defendants then accuse Sectra of being "cavalier" and "uncredentialed." ECF 45 at 5. Unwarranted criticisms aside, it doesn't take an AI expert to know that network access is impossible without hardware enabling such access. ECF 42-1, ¶ 9.

Defendants' position is incredible in light Defendants' own use of AI. Defendants advertise that they use AI "daily to accelerate [their] own product development"[4] and have used AI to "augment [their] security analysis for many years."[5] Defendants even advertise air-gapping (i.e., isolating a computer from computer networks) to their own customers in connection with running AI safely.[6] In other words, Defendants publicly proclaim that they use AI to develop and test their own code and instruct their customers on how to use AI safely, but then tell the Court that Sectra's tools are too risky because they are AI. This is unreasonable.

The fact remains: ***a breakout cannot occur if the computer is incapable of accessing a network***. Defendants did not, and cannot, dispute this. Thus, there is a simple, straightforward way to ameliorate Defendants' concerns: ***put "read-only" source code on a computer with no Internet connectivity***. ECF 42-1, ¶ 13. Fortinet is already doing this. And there is no doubt Cisco could do this under the protective order. And where there is no possibility for an Internet connection, then

[4] Travis Sugarbaker, *From an Idea to a Live App on Cisco, in Minutes*, Cisco Blogs (June 2, 2026), https://blogs.cisco.com/ai/from-an-idea-to-a-live-app-on-cisco-in-minutes.
[5] Carl Windsor (declarant from ECF 45-2), *Update on Fortinet Use of Frontier AI*, https://www.fortinet.com/blog/ciso-collective/update-on-fortinet-use-of-frontier-ai.
[6] Fortinet, *Guide To Air Gap Security* https://www.fortinet.com/resources/cyberglossary/what-is-air-gap; Chris Borales, *Sovereign AI Meets Quantum-Ready Defense with FortiNDR* (Sep. 22, 2026), https://www.fortinet.com/blog/security-operations/sovereign-ai-meets-quantum-ready-defense-with-fortindr; Cisco, *Zero-Fial Connectivity for Air-Gapped Networks*, https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/Zero-Fail-Connectivity-for-Air-Gapped-Networks.html.

there is no risk above and beyond that inherent in regular source code review. And the benefit to Sectra is monumental. Proportionality thus requires Defendants to install the tools. [7]

Cisco's choice to produce source code using a thin client does not change the analysis. Cisco argues that AI tools are incompatible with the PO where a party chooses to produce via thin client. ECF 45 at 2-3. But the PO does not give Cisco the right to leverage its optional production method to restrict what tools Sectra may use. Indeed, if Cisco's interpretation were correct, a producing party could deny any software tool that might theoretically interact with a network simply by choosing the thin-client option. In any event, Cisco is no doubt able to ensure that any tools used in connection with a remote thin client stay put—it advertises its prowess on precisely this subject. *Supra* n.6; ECF 42 at 7 n.4. In short, Cisco has two good options. It could choose a standalone computer like Fortinet is doing. Or it could trust in its own ability to secure the environment, as it asks its customers to do.

III. CONCLUSION

Defendants rely on stigma instead of reason. There is no reasonable basis to forbid use of the requested tools. They greatly assist in review and are already in use in this District; the risks are commensurate with those already inherent in source code review; and run-of-the-mill safety measures entirely mitigate any extra, perceived risk. The Court should compel Defendants to install the requested tools.

---

[7] Defendants allege that cases speak against Sectra with "one voice," but then cite just two decisions from the same court. Both are inapposite. In *Philips N. Am. LLC v. Glob. Med. Imaging, LLC*, 343 F.R.D. 59, 66–67 (N.D. Ill. 2022), the court rejected a request to store "unidentified tools and scripts" on the computer—a very different request from installing identified review tools. In *Berkheimer v. Hewlett-Packard Co.*, No. 12 C 9023, 2014 WL 12959469, at *3 (N.D. Ill. Apr. 7, 2014), the court addressed electronic copies of source code produced on disc, not review tools. Neither case involved a request to install software under a PO provision dictating that approval "shall not be unreasonably withheld." And Defendants' later reliance on *Hyles v. New York City*, No. 10 Civ. 3119, 2016 WL 4077114, at *3 (S.D.N.Y. Aug. 1, 2016) is misplaced, because that case only addressed whether a producing party must use technology-assisted review to search its own documents for production. That has nothing to do with this case.

Dated: September 30, 2026

Respectfully submitted,

/s/ Carder W. Brooks
Edward R. Nelson III
State Bar No. 00797142
ed@nelbum.com
Brent N. Bumgardner
State Bar No. 00795272
brent@nelbum.com
Christopher G. Granaghan
State Bar No. 24078585
chris@nelbum.com
Carder W. Brooks
State Bar No. 24105536
carder@nelbum.com
Jinming Zhang
Virginia Bar No. 96210
jinming@nelbum.com
NELSON BUMGARDNER CONROY PC
3131 West 7th Street, Suite 300
Fort Worth, Texas 76107
817.377.9111

Of Counsel:

Andrea L. Fair
State Bar No. 24078488
andrea@millerfairhenry.com
MILLER FAIR HENRY PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
(903) 757-6400 (telephone)
(903) 757-2323 (facsimile)

COUNSEL FOR PLAINTIFF
SECTRA COMMUNICATIONS AB

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing document was filed electronically in compliance with Local Rule CV-5(a). Therefore, this document was served on all counsel on September 30, 2026.

/s/ Carder W. Brooks