AFTER MYTHOS

Patching is never going to be enough.

In April, AI found **thousands of high-severity zero-days** across the software stack almost every enterprise depends on. Things changed, and they are never going back. The findings will keep flowing downstream into every environment, and the backlog is permanent. You already know this. The question is what you do about it.

1,000s
of zero-days discovered autonomously, including a 27-year-old flaw no human ever found

5 weeks
for two more frontier labs to announce the same capability

100%
the odds that someone eventually gets inside. Entry is no longer the variable. It is the constant

THE BOTTOM LINE

You will never patch your way out of this. AI discovers vulnerabilities faster than any team can fix them, and attackers get the same capability. Patch what you can, automate what you can. Necessary. Not sufficient. Never again sufficient.

The game has already moved. It is now two questions: **how fast do I know someone is inside**, and the one that matters more: **what did they have access to?** Which systems, which files, which data. That is the whole game now.

QUERY · THE MORNING AFTER

Someone is now inside. What did they have access to? What did they manage to take? Is it crown-jewel data, or noise? Can you prove it?

ASKED BY · BOARD / REGULATOR / INSURER / COUNSEL

WHERE IT BREAKS TODAY

Your stack tells you something suspicious happened. It does not tell you what happened to your **data**. So when the question comes, the answer is *"we think."* Weeks of forensics, worst-case disclosure, a breach you could not prove was smaller than it looked. That distance between suspicion and certainty is **the Proof Gap**, and it is where programs break.

"Now we know who is accessing our data."

That is the sentence your board wants to hear, and the one almost no security program can say. WireX makes it true: continuous evidence of who touched what data, what they took, and what it contained. Months of history, answers in minutes, proof that stands up to a regulator, an insurer, and a courtroom. **WireX bridges the evidence gap between detection and understanding true impact - on prem or cloud.**

There is board attention on this right now. Use it.

Boards are reading the same headlines and asking for the plan. Attention is budget. Walk in with a two-part answer:

1. **Accelerate remediation.** Automation, prioritization, exposure management. Necessary, and every one of your peers is asking for the same thing.
2. **Fund the assume-breach layer.** The ability to answer, with evidence, what an intruder accessed and took. This is the part most programs cannot do today, and the first thing regulators, insurers, and counsel ask about.

Then you get to end the meeting with one sentence: "Now we know who is accessing our data." Full stop.

One conversation. Thirty minutes, one question: when they get in, what can you prove? If the honest answer is "we think," let's talk.

Evidence, not alerts.
WIREXSYSTEMS.COM