Corporate · 4 Min Read

AI era security: Why complete telemetry is now a competitive advantage, not a cost

Security systems previously discarded data due to high storage and compute costs. New AI capabilities now demand complete, high-fidelity telemetry for accurate machine decisions. Advances in object storage and open formats have drastically reduced data retention expenses. This architectural shift allows for comprehensive data collection, unlike past rationing strategies. Organizations embracing full telemetry will gain a significant strategic advantage in security.

Shomiron Das Gupta • ETCISO

Updated On Aug 19, 2026 at 08:00 AM IST

For twenty years we've accepted that security systems must discard most telemetry because storage and compute were too expensive. That

architectural compromise became accepted wisdom. Today, that assumption is no longer true. In the AI era, complete, high-fidelity telemetry is becoming a competitive advantage - not because humans need more dashboards, but because machines need complete context to make accurate, consistent, and auditable decisions. The question is no longer whether enterprises should collect everything. The question is whether their data infrastructure is capable of making that practical.

The compromise we stopped questioning

Ask any security leader why they filter, sample, and age out telemetry, and you'll hear the same answer: cost. SIEM pricing models built on ingest volume made every gigabyte a budget line. Index-everything architectures made every retained event a compute liability. So the industry built an entire discipline around deciding what *not* to keep - filtering pipelines, sampling strategies, 30- and 90-day retention windows, tiered storage that quietly turns "retained" data into "technically present but practically unreachable" data.

We told ourselves this was data hygiene. It was actually rationing. And like all rationing, it was a response to scarcity - scarcity of affordable storage, scarcity of query engines that could scan petabytes without melting the budget, scarcity of anyone who could actually reason over that much signal.

Here's the uncomfortable part: every one of those scarcities has ended, and most security architectures haven't noticed.

What changed underneath us

Three shifts broke the old economics.

Storage stopped being the constraint. Object storage brought the cost of retaining a terabyte of telemetry down by orders of magnitude. Open columnar formats mean that data written once can be read by many engines, forever, without vendor ransom. Keeping everything is no longer an extravagance; it's a rounding error compared to the cost of a single missed breach.

Compute and storage separated. Modern analytical engines query data where it sits. You no longer pay to index everything on arrival just in case someone asks a question later. You pay for the questions you actually ask. That single architectural change inverts the economics that justified two decades of discarding.

The consumer of telemetry changed. This is the shift that matters most. For twenty years, the end consumer of security data was a human

analyst looking at a dashboard, and humans genuinely can't use more data - they drown in it. AI agents are different. An agent investigating an incident doesn't want a summary; it wants the full sequence of events, the ambient context, the six months of baseline behavior that makes an anomaly an anomaly. Give an agent partial data and you get partial conclusions delivered with full confidence. Give it complete data and you get investigations that are accurate, repeatable, and - critically - auditable, because every conclusion traces back to evidence that still exists.

"Collect less" was never a security strategy

The "too much data" argument was always a confession dressed up as a philosophy. When a vendor tells you to reduce ingest, they're telling you their architecture can't afford your reality. When a team samples authentication logs, they're not making a security decision - they're making a procurement decision with security consequences.

Consider what discarding actually costs. Dwell times for sophisticated intrusions routinely exceed the retention window of the average SIEM. That means the evidence of initial compromise is deleted *before the investigation begins*. Threat hunting becomes archaeology in a museum that burned its own archives. Compliance attestations rest on data that no longer exists. And every AI initiative the security team launches inherits the same amputated dataset, faithfully automating decisions made on incomplete evidence.

The adversary, meanwhile, keeps everything. Attackers operating with AI assistance don't sample your environment - they map it completely.

Defending a complete attack surface with a sampled view of your own estate is asymmetry by choice.

The real question for security leaders

None of this means "buy a bigger SIEM." Scaling the old architecture just scales the old cost curve. The shift is architectural: telemetry as a durable, owned system of record - stored in open formats, queryable by any engine, retained for years instead of weeks - with detection, investigation, and AI reasoning layered on top rather than fused into a proprietary ingest pipeline.

That's a different set of evaluation criteria than the industry is used to. Not "how much can we afford to ingest?" but: Do we own our telemetry, or does our vendor? Can an agent reach back eighteen months without a restore ticket? Does adding a data source improve our security or just our bill?

For twenty years, "collect less" was the responsible answer because the infrastructure gave us no other choice. That excuse has expired. Complete telemetry is now economically achievable and strategically decisive. The organizations that internalize this first won't just detect more - they'll hand their AI systems the one thing no model can compensate for lacking: the full picture.

More data *is* better security. It always was. We just couldn't afford to admit it.

The author is Shomiron Das Gupta, Founder and CEO of Bloo.