

A global AI planning platform hunts across unlimited history on Elastic at 2–3 TB a day

A leading AI planning platform consolidated its security operations on Elastic Security, giving its SOC unlimited threat-hunting retention across 2–3 TB of daily telemetry pulled from Google Cloud, Azure, and AWS.

Unlimited

Threat-hunting retention
vs. 10–20 days

2–3 TB/day

Telemetry ingested
across three clouds

Plain English

Detections authored via
the AI Agent

1 platform

SIEM, hunting, IR, and
observability

The challenge

- ✗ Retention was bound to storage cost, capping useful history at roughly 10–20 days.
- ✗ Threat hunting was limited by how far back the team could look, not by analyst skill.
- ✗ Every new detection meant a ticket to an overloaded engineering queue and a wait.
- ✗ Telemetry was scattered across three clouds, applications, and network devices.

The solution

- ✓ Searchable snapshots hold full history in the frozen tier on low-cost cloud object storage.
- ✓ Any cloud bucket integrates with the frozen tier, so history is set by the object store, not disk.
- ✓ Analysts describe a threat in plain English and the AI Agent returns the exact query.
- ✓ Cloud-agnostic collection lands Google Cloud, Azure, and AWS telemetry in one platform.

How it works

1. Collect

Cloud-agnostic ingest
from three clouds

2. Retain

Searchable snapshots
into the frozen tier

3. Hunt

Unlimited history, no
rehydration wait

4. Detect

Plain-English queries
via the AI Agent

5. Respond

Attack Discovery
across the lifecycle

Before

- Retention capped near 10–20 days by storage cost
- New detections queued to an overloaded engineering team
- Telemetry split across clouds, apps, and network devices

After

- Effectively unlimited history in the frozen tier, backed by object storage
- Analysts author detections in plain English with the AI Agent
- Cloud-agnostic ingest into one platform for security and observability

“To spot a behavior anomaly you have to look across a long period, not 10 or 20 days. **Searchable snapshots** let me hunt across **unlimited data** in the frozen node, and I can point it at any cloud bucket.”

— Senior Director of Security Operations (anonymized)

Why it matters beyond retention

The searchable window is set by object storage, not by disk, so the platform absorbs growth without forcing the retention-versus-cost tradeoff that limited the team before. The same principle holds whether you are bringing together your first data sources or hunting across effectively unlimited history: keep full context, and keep it searchable.

[See how Elastic Security hunts threats across your full history or start a free trial →](#)