Elastic Observability Overview

October 2025

Tim Brophy, Strategic Solutions Architect
International

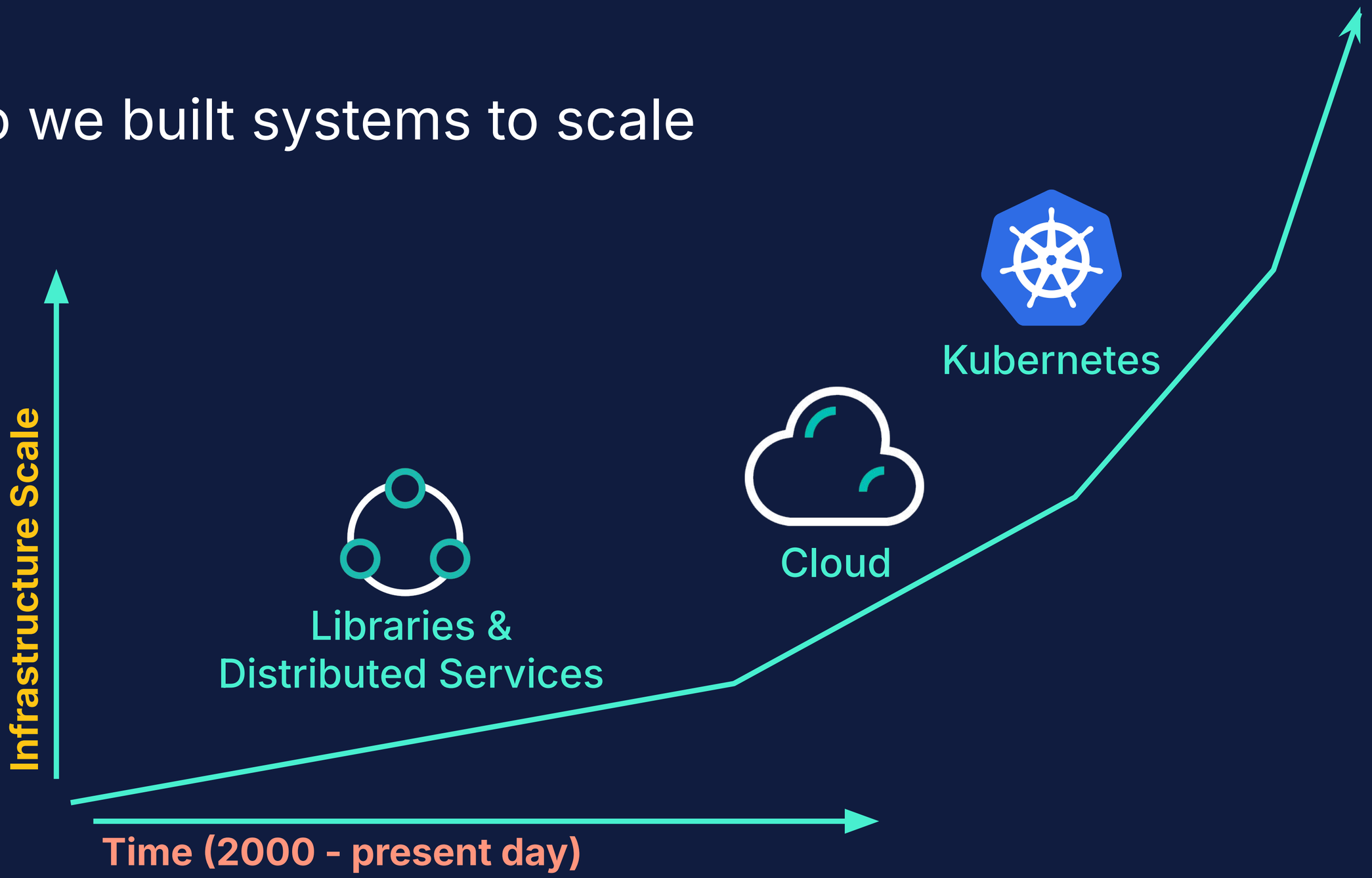
elastic | The Search AI Company


Elastic envisions a world where everyone can unlock new possibilities by harnessing the power of unlimited data.

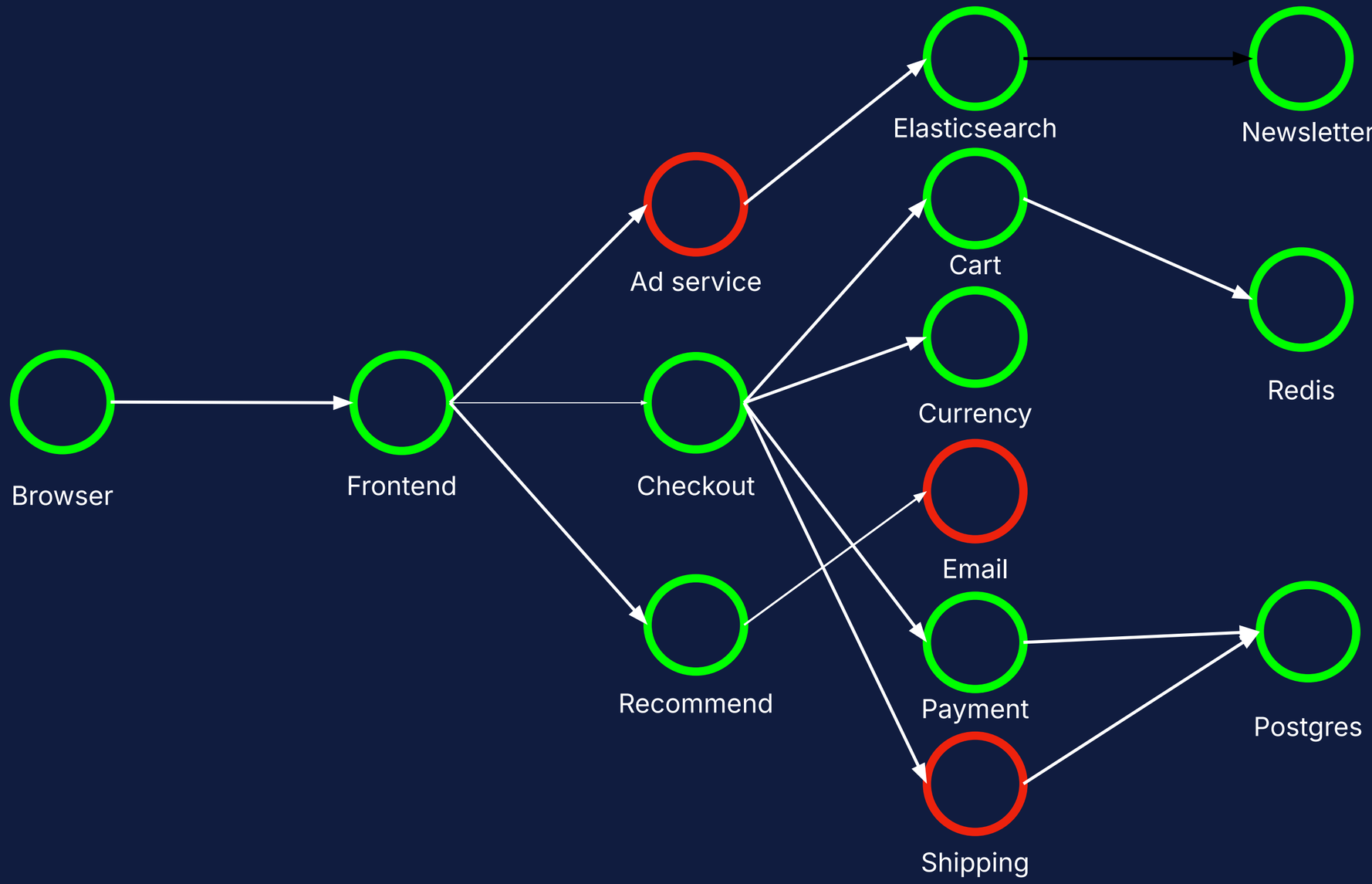
Over the last decade,
the business demands of IT
have outpaced human reach

elastic

So we built systems to scale



Now your applications are complex



Simple questions have become hard to answer

Is my system working?

How do I fix it?

Who was impacted and how much money have we lost?

My customer just told me the website is slow

Who added that column to the database?

Why is my application getting zero traffic?

Towards AI-Driven Open Source Observability

MONITORING - 2000s

Health Monitoring

- Focus on health visibility
- Monitoring “known unknowns”
- Alerting engines
- Manual processes for triage

Legacy

OBSERVABILITY - MID 2010s

Siloed Observability Tools

- Added focus on triage and investigations
- High emphasis on instrumentation
- Black-box tools for apps and infra
- Multi-signal support - as an after-thought

Current

OBSERVABILITY REDEFINED - 2024+

Generative AI and OpenTelemetry

- Solid foundation in logs/wide events
- Low instrumentation w/ OTel and AI
- Convergence with Data Lakes
- AI-driven investigations and insights

Future

Elastic Observability makes it easy for organisations to keep up with rapidly changing applications and expectations

elastic

Elastic Observability

Powered by Search AI

Any data, any source
BUSINESS + OPERATIONAL

Elastic Observability

AI Assistant

Log analytics	**Infra & cloud monitoring**	**APM**
Continuous profiling	**Digital experience monitoring**	**AIOps**

Search AI Platform

OTel-first, 350+ integrations	**Search AI Lake**	**Data exploration**

Deploy anywhere

Public cloud | Hybrid | On-premises

Business outcomes for everyone

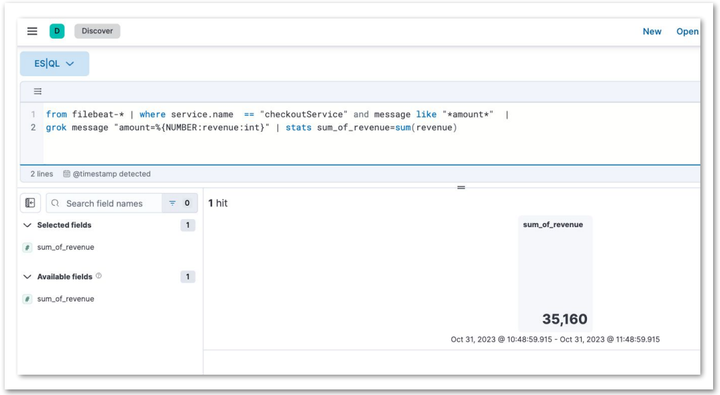
69% improvement in customer and employee satisfaction[1]

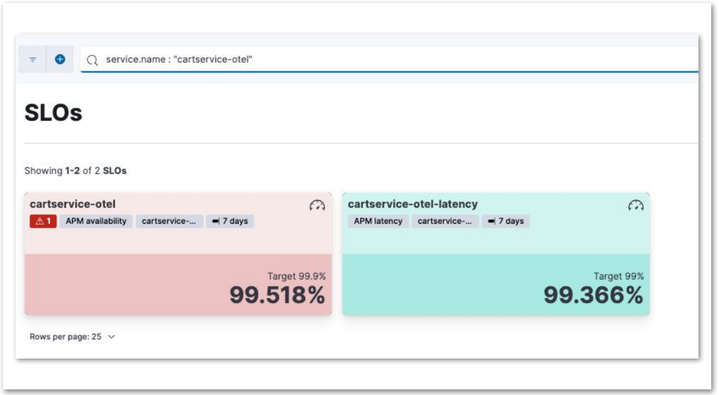
75% gain in dev & SRE productivity[2]

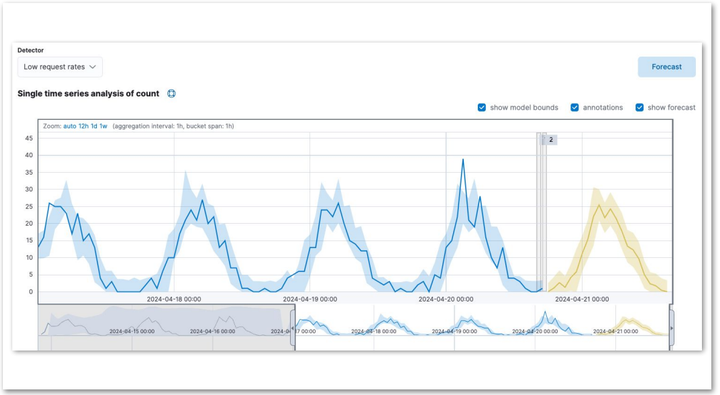
85% reduction in revenue disruption[2]

1: Elastic Survey
2: Forrester TEI

The unified observability journey starts with logs







Business insights from logs

Understand total revenue from successful checkouts

Customer Experience monitoring using logs

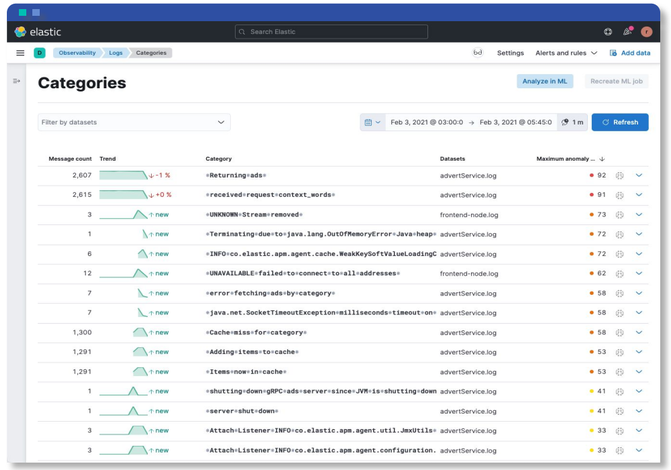
Any availability issues with checkout service?

Proactive log analysis

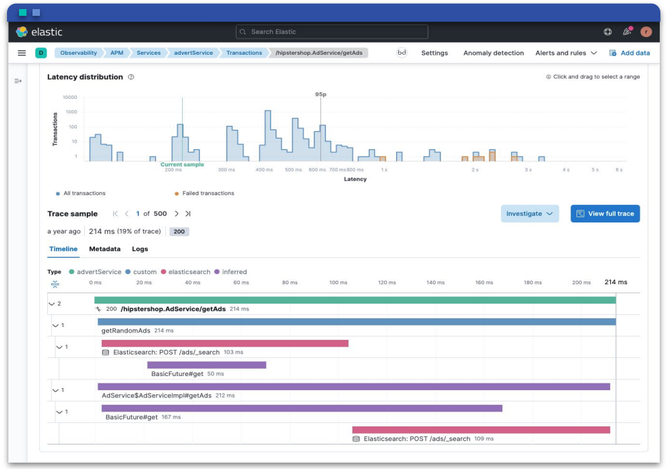
Will we see potential spike in failed transactions?

elastic

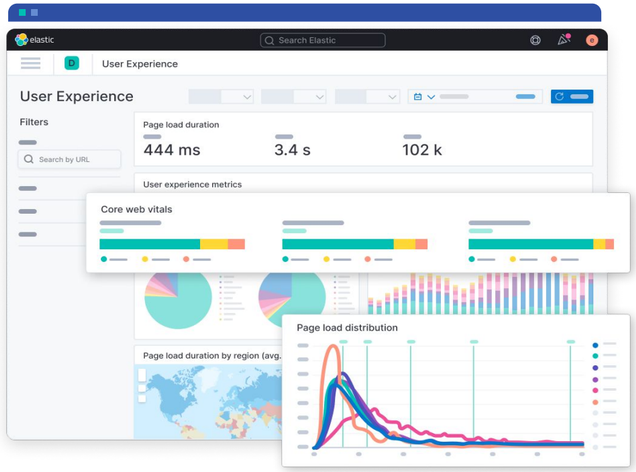
But we need to go beyond logs



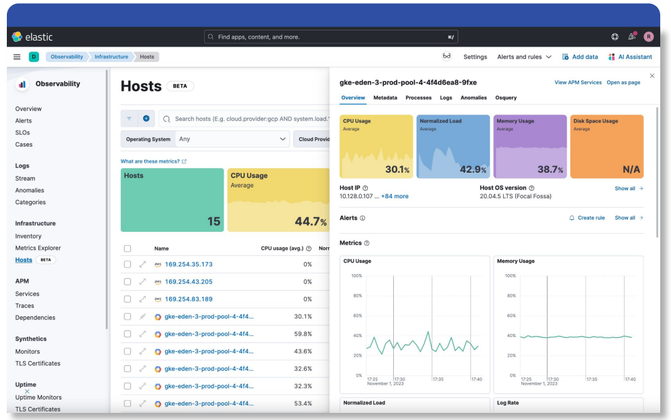
Logging



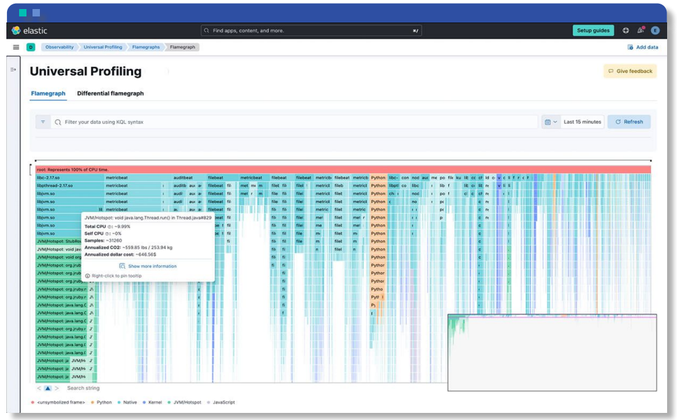
Tracing



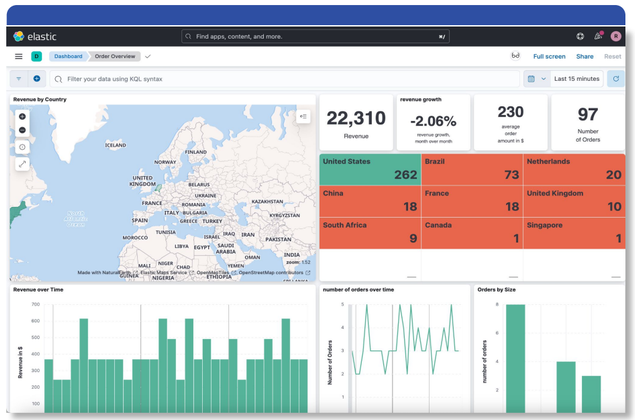
RUM



Infra metrics

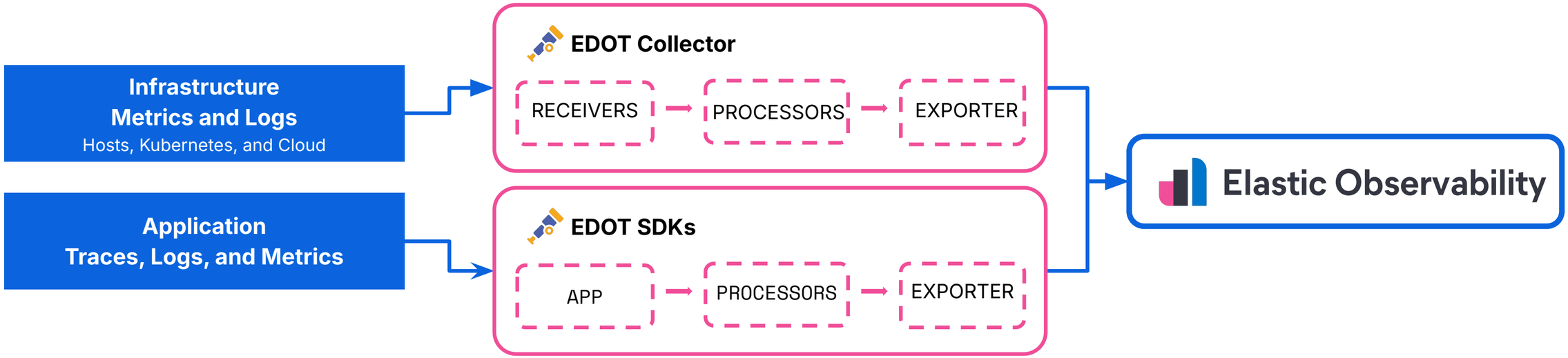


Profiling



KPI metrics

OpenTelemetry makes data collection easier



ECS becomes OTel Semantic Conventions

- Elastic donated Elastic Common Schema (ECS) to OTel
- ECS is now OTel Semantic Conventions
- Significant Schema overlap means data feels familiar

Elastic Distribution of OpenTelemetry (EDOT)

- Elastic distributions of OTel SDK Libraries for Java, Python, Node.js, .NET, iOS/Android
- Elastic distribution of OTel Collector for edge collection
- Fully compatible with OTel Kubernetes Helm Chart and Operator

OpenTelemetry-Native Architecture

- First-class experience with OpenTelemetry
- OTel data is instantly actionable
- Easy retrieval of data in original OTel form
- Portable queries/rules and dashboards

ES|QL makes querying easier

Lightning fast piped queries

- New query engine and query language offering greater speed and flexibility
- Single interface simplifies multi-signal analysis across logs, metrics, and traces
- Define fields on the fly, enrich data with lookups, and process multiple queries concurrently

```
1  from metrics* |
2  stats max_cpu = max(kubernetes.pod.cpu.usage.node.pct),
   avg_mem = max(kubernetes.pod.memory.usage.bytes) by
   kubernetes.pod.name |
3  sort max_cpu desc | limit 10
```

3 lines @timestamp detected Run query ⌘ + Enter

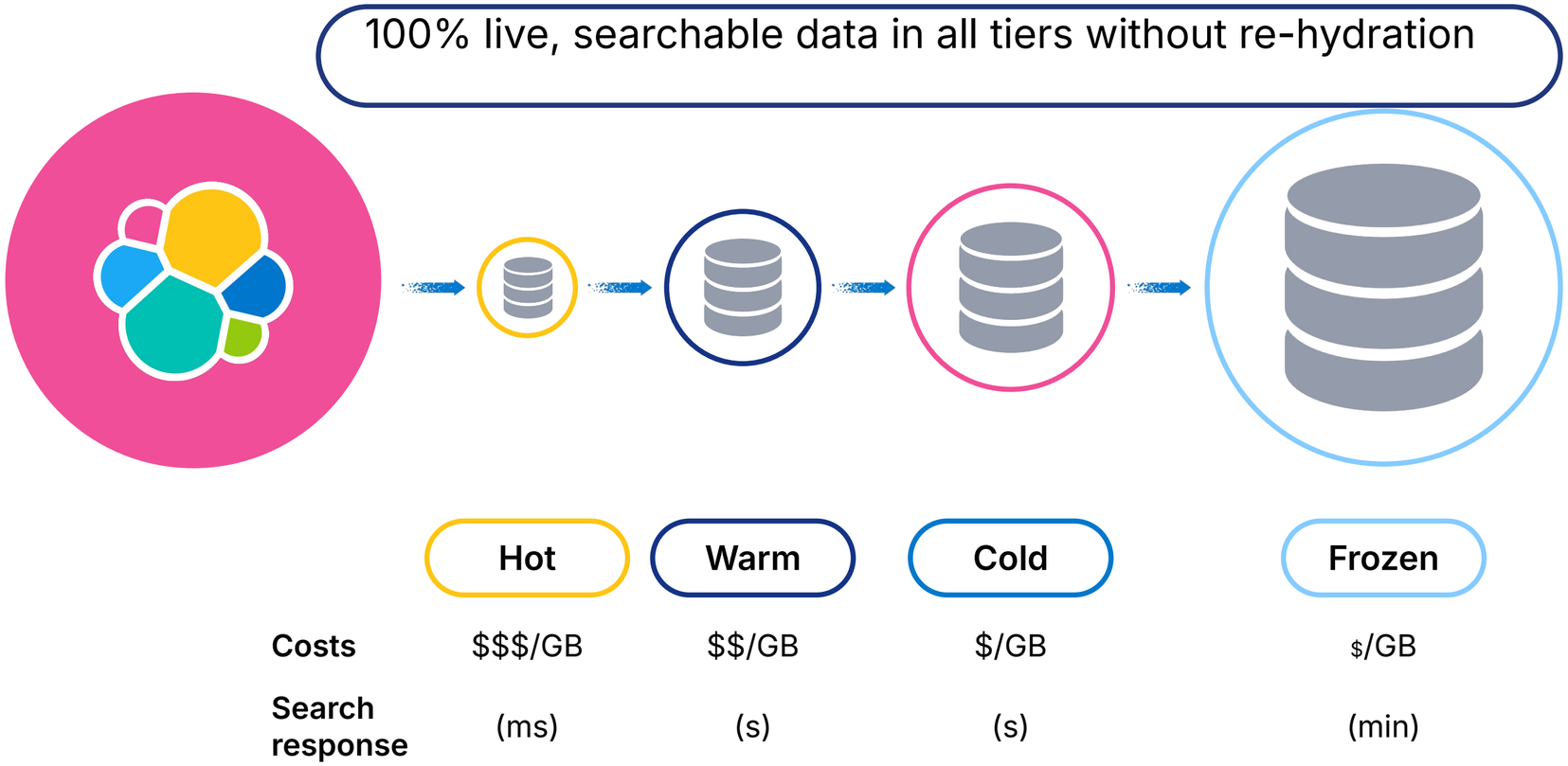
Columns Sort fields

max_cpu	avg_mem	kubernetes.pod.name
-	-	-
0.125	945872896	heartbeat-synthetics-6c9497b68-pljxr
0.117	943742976	heartbeat-synthetics-tokyo-5b9f74dd57-27hlv
0.099	2220580864	relevance-workbench-app-ui-f7cbd657c-dpd7d
0.097	1999900672	elastic-agent-cxjv4
0.09	232505344	kafka-loadgen-deco-green-5cf8cc7988-pxcnp

elastic

Data tiers make data retention more cost efficient

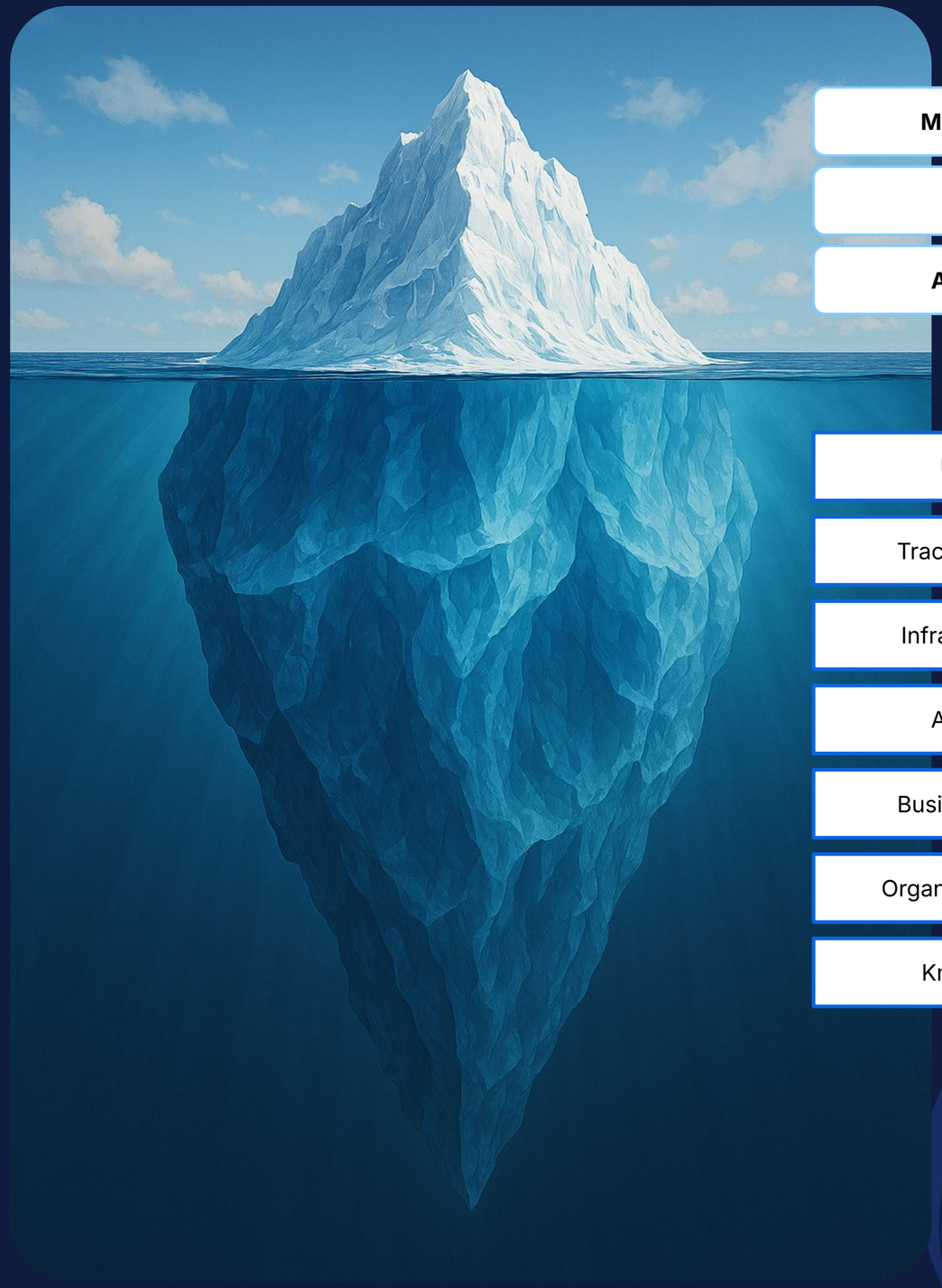
Balanced visibility, retention, performance & budget



Elastic provides automated data lifecycle management (ILM) to manage budget

What about AI?

AI depends on data, Elastic makes it easy to bring them together



Machine learning

Generative AI

Augemented AI

UX monitoring

Traces, spans, latency

Infrastructure metrics

Application logs

Business process logs

Organisational processes

Knowledge bases

elastic

History of AI at Elastic

Foundational technical building blocks within the Elastic Stack

AI-powered features that enhance our solutions

'17

Support for supervised and unsupervised learning

'18

Support for forecasting in Observability

'19

Native support for Vector Search

Support for anomaly detection and AIOps

'20

Support for ML-powered detection rules

'21

Support for ML-powered alerting rules

'22

Support for NLP and BYO Transformer models

'23

ESRE Elasticsearch Relevance Engine

Elastic Observability Assistant powered by ESRE

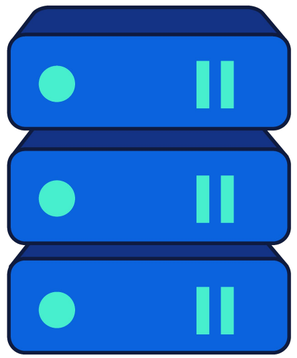
'24

ES|QL & Industry standards for vector search & RAG

Attack Discovery, Auto Ops, Entity Discovery

elastic

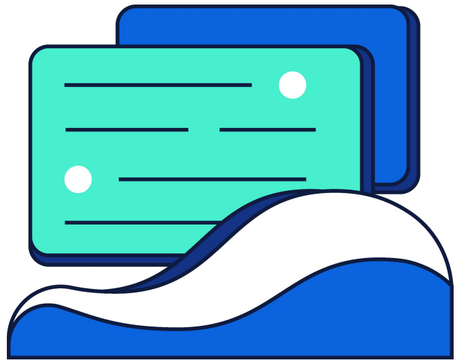
The Search AI Platform features a **novel data architecture**



Data Warehouse

Response time:

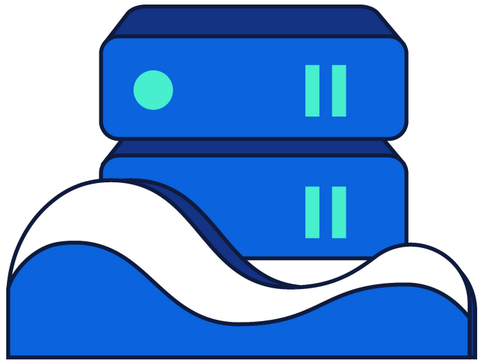
10s of Seconds



Data Lake

Response time:

Minutes



Lakehouse

Response time:

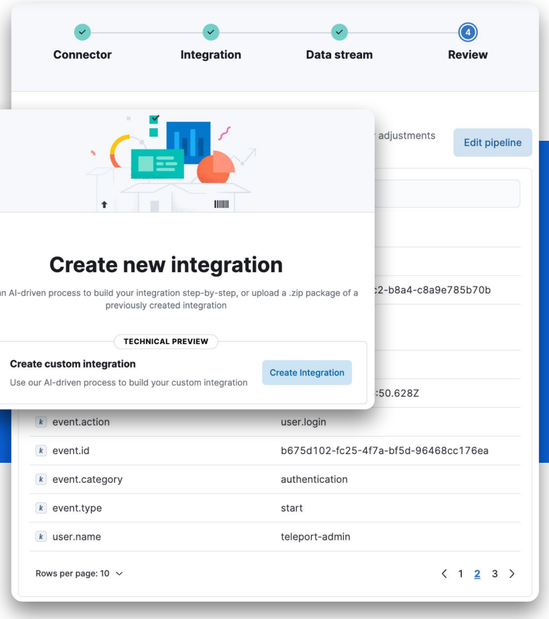
Seconds

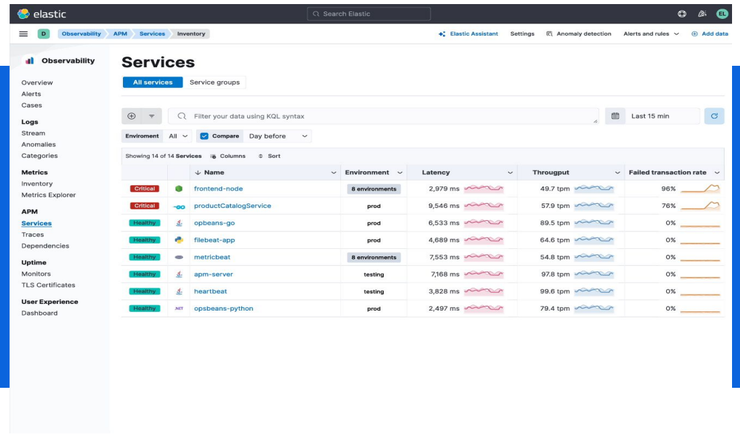
Search AI Lake

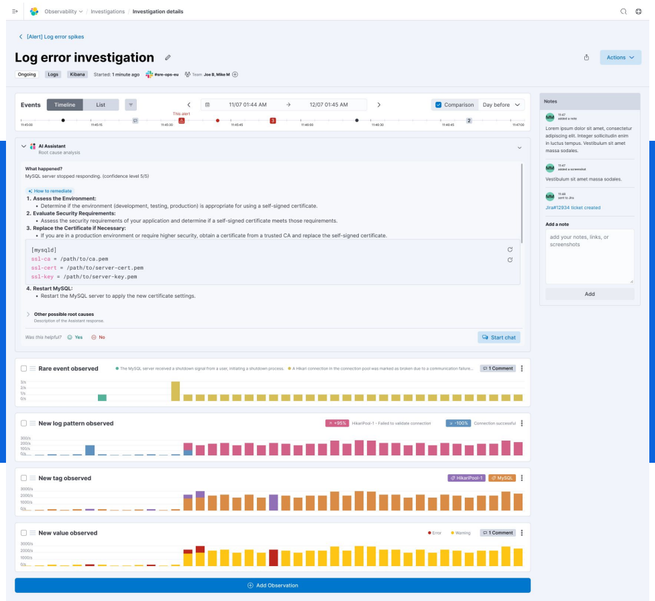
Response time:

Milliseconds

Streamline SRE Teams with AI







ACCELERATE DATA ONBOARDING

Automatic Import

- Create custom data integrations in minutes, not days
- Extend visibility beyond Elastic's 400+ prebuilt data integrations

BOOST SRE TEAMS

AI Assistant

- Make every user a power user w/ insights and guidance
- Guide SREs through rule creation, triage and investigation
- GA today with EIS (out of the box LLM), local LLM support and privacy controls, next - support for custom dashboards

AUTOMATE TRIAGE

AI Investigations (Future)

- Harness multiple events and alerts associated with an entity to get to root cause faster
- Get guidance on what to do next, ask follow-up questions, and take action

elastic

Driving faster RCA: AI-powered zero-config features

Complete set of AIOps features

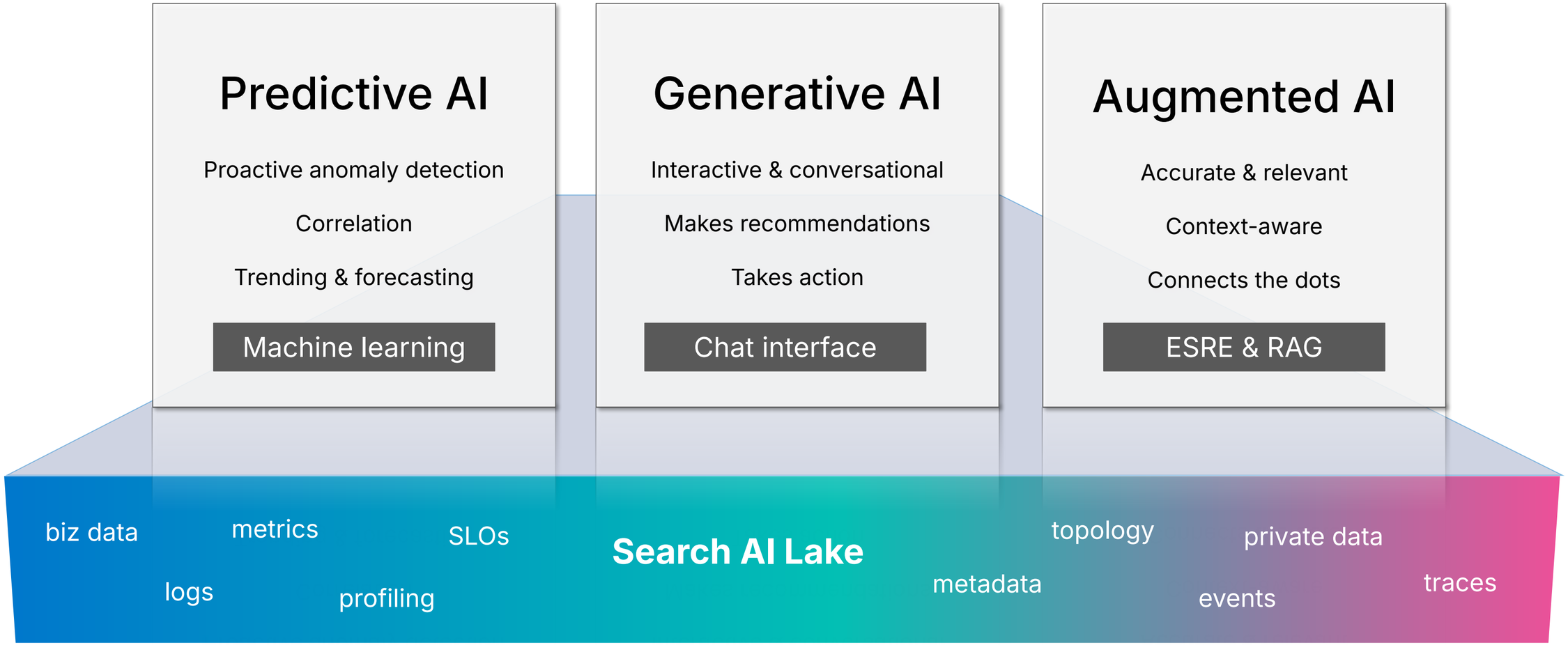
Minimal config – high value

Log categorization & anomaly detection	AI makes sense of billions of logs
Log rate analysis	AI analysis of deviations in logs
Metrics anomaly detection & correlation	AI makes sense of billions of metrics
Multi-signal anomaly detection	AI analyzes logs, metrics, traces, & more
Trace analysis (latency & failure correlation)	AI finds the cause of latency and failures

- AI-driven
- Zero-config
- All signals
- Baseline capability
- Easy to turn on

Elastic Multimodal Search AI

Prevent downtime & improve SRE productivity



Where are we going?

Open standards, efficient onboarding

- Store more data and stay on budget with efficient storage and downsampling
- AI-assisted OpenTelemetry-first onboarding
- Streamlined data onboarding with automated parsing and partitioning

Automated resource and signal insights

- Comprehensive observability with investments in logs, metrics, traces
- Leverage “significant events” detected via Streams to automatically detect problems and notable events

Detect and resolve issues faster

- Act before issues become critical with advanced querying and visualizations
- Identify and resolve issues using advanced AI capabilities with alert groups, correlations and investigations

Elastic Observability Platform

- Logs
- Streams
- Metrics
- APM
- Dashboards and Discover
- ES|QL

elastic

Thank You

elastic