



Elastic Observability

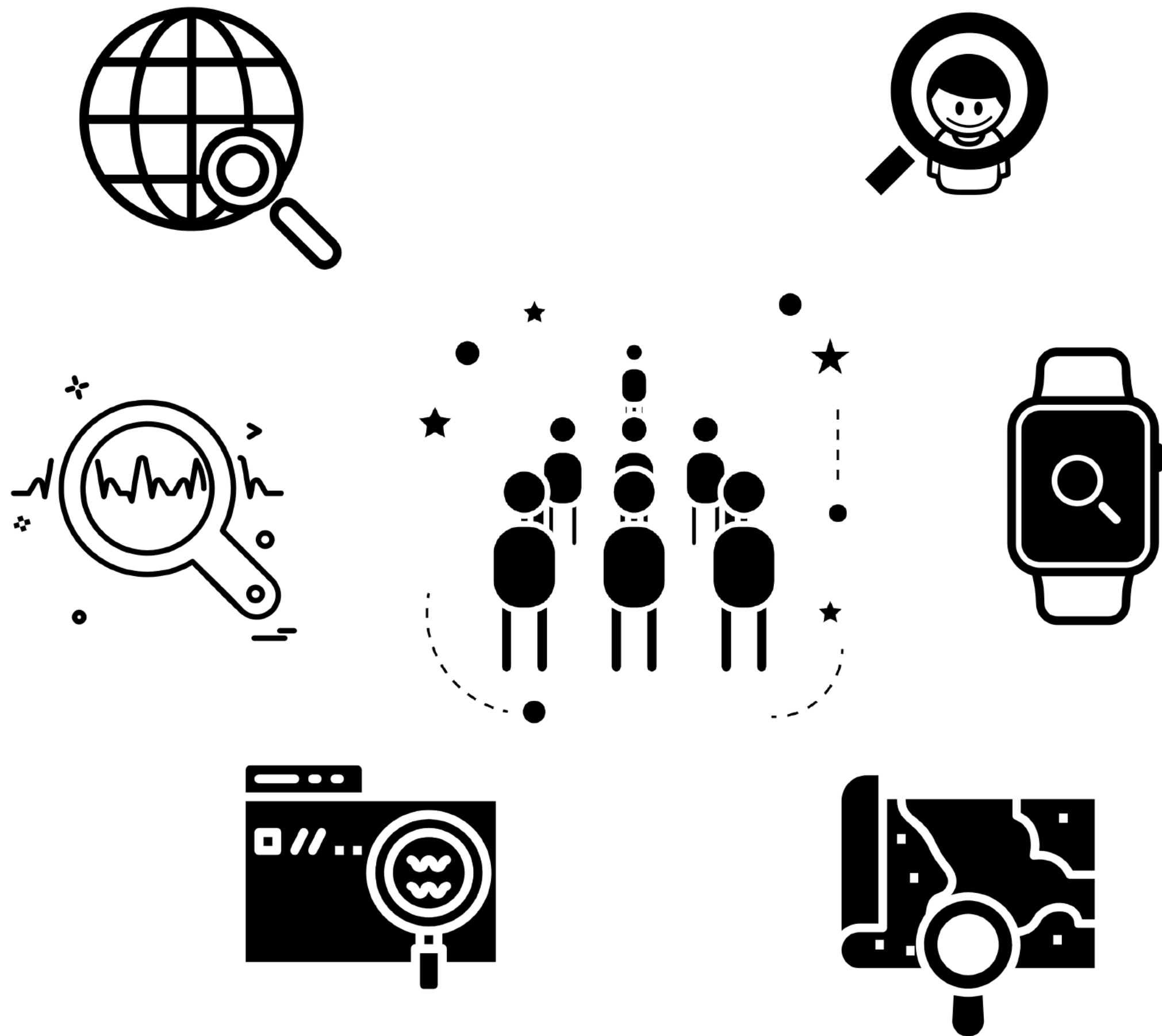
María Bolaños

November 2023

María Bolaños

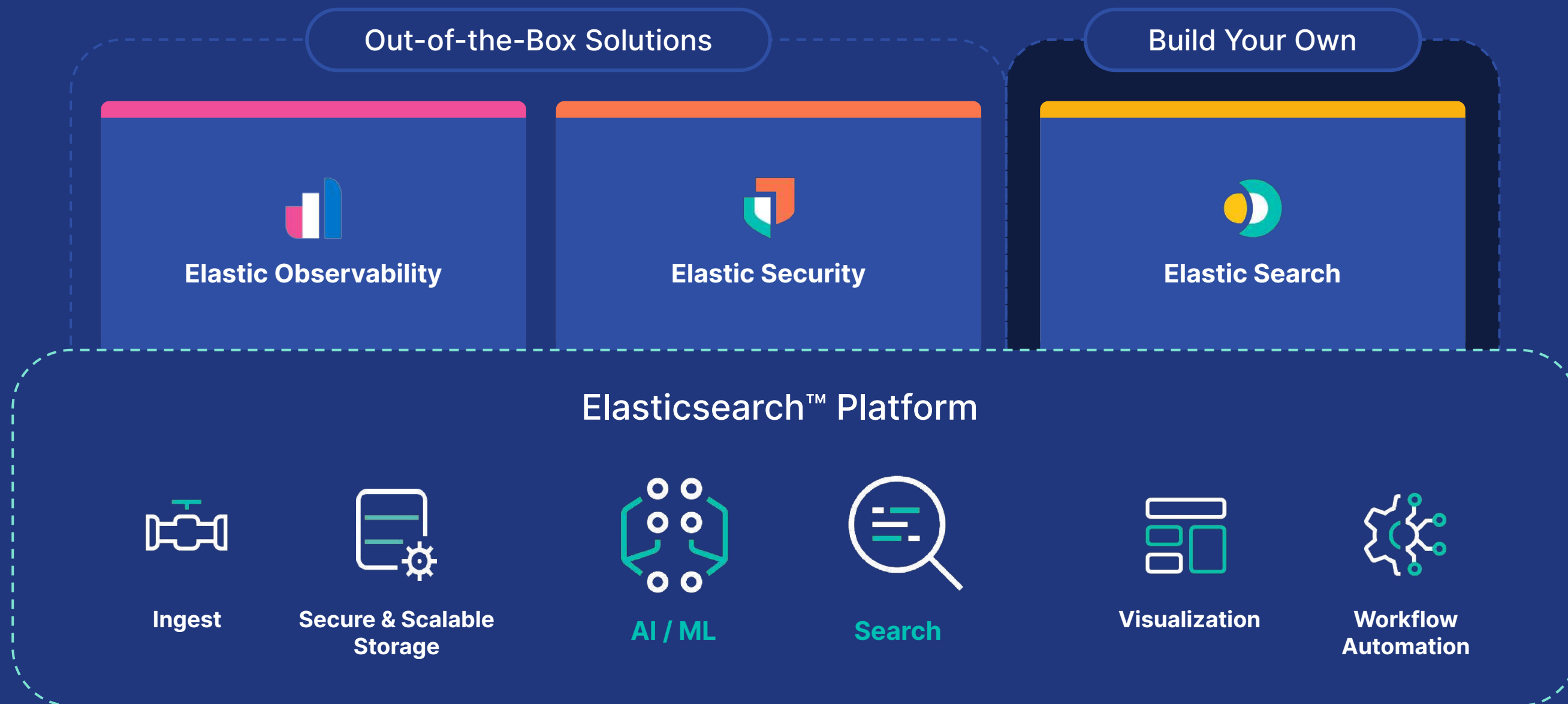
Sr Solutions Architect



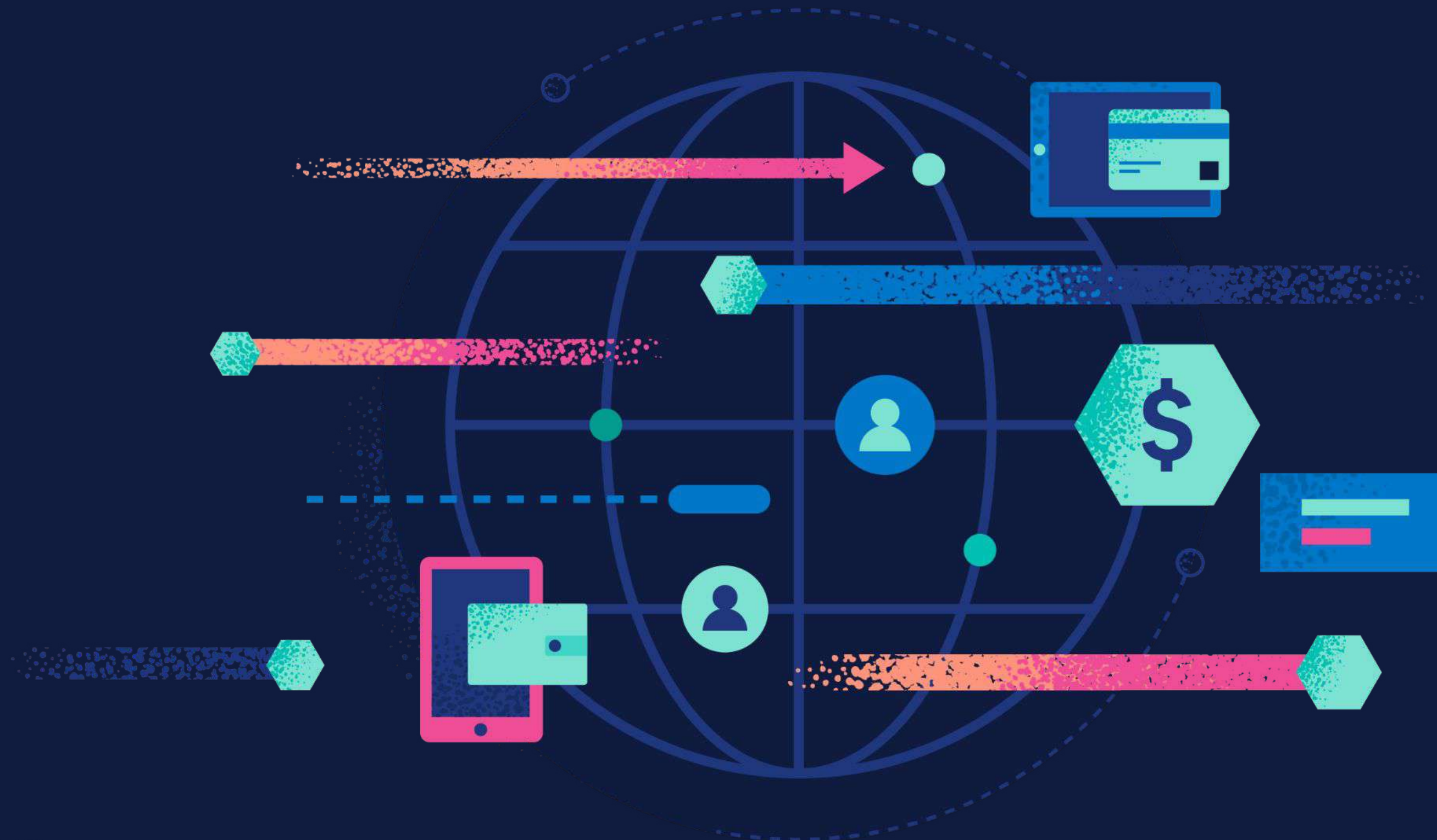


Searching for **Rides**

One **Data** Analytics Platform Two Out-of-the-Box Solutions The Freedom to Build Anything



We live in a world of digital transactions

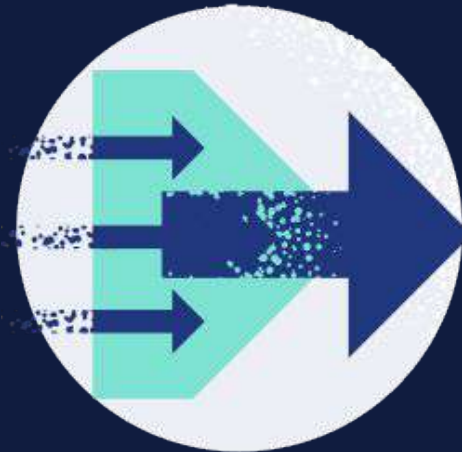


Businesses need to deliver *exceptional* digital experiences to achieve



Revenue growth

62%
improvement in
revenue disruption



Accelerated productivity

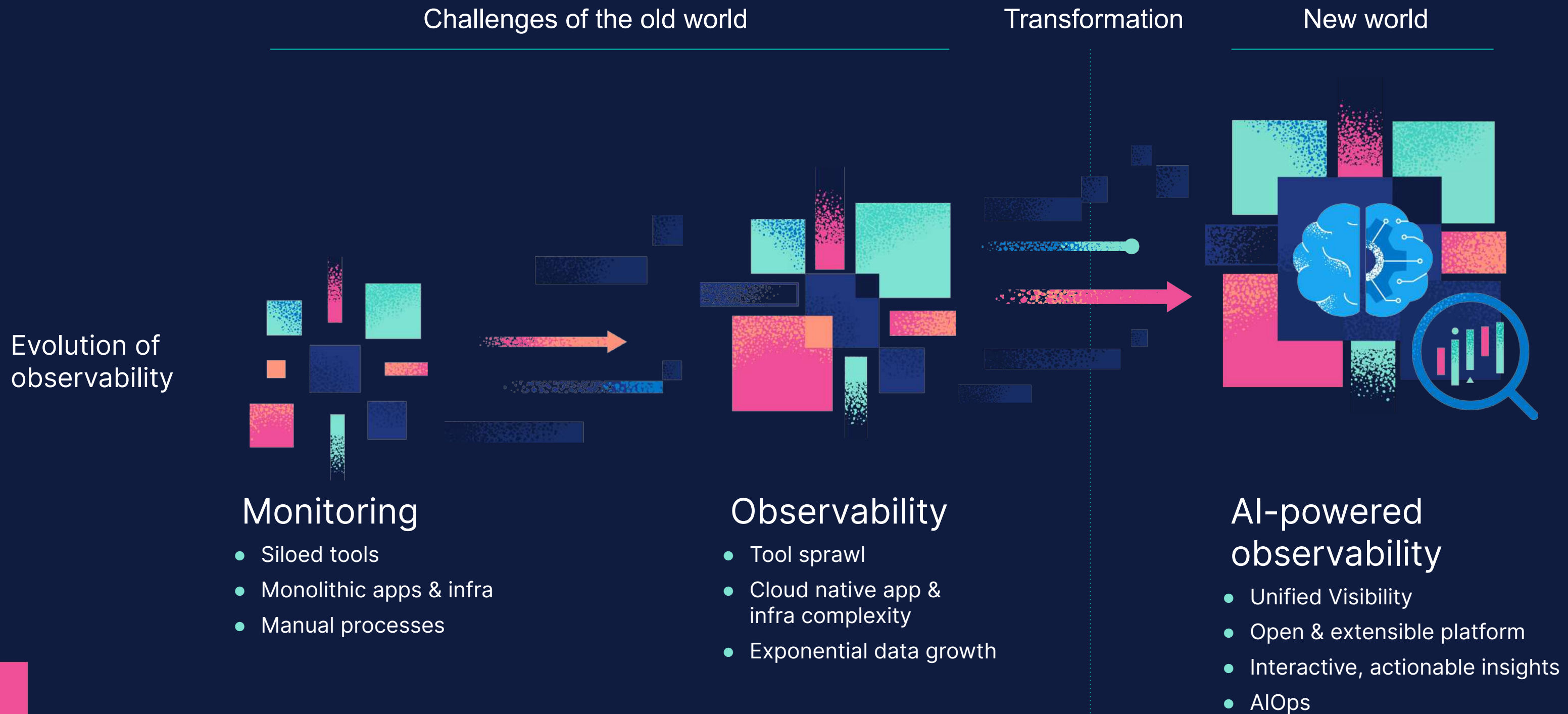
67%
improvement in
dev/IT productivity



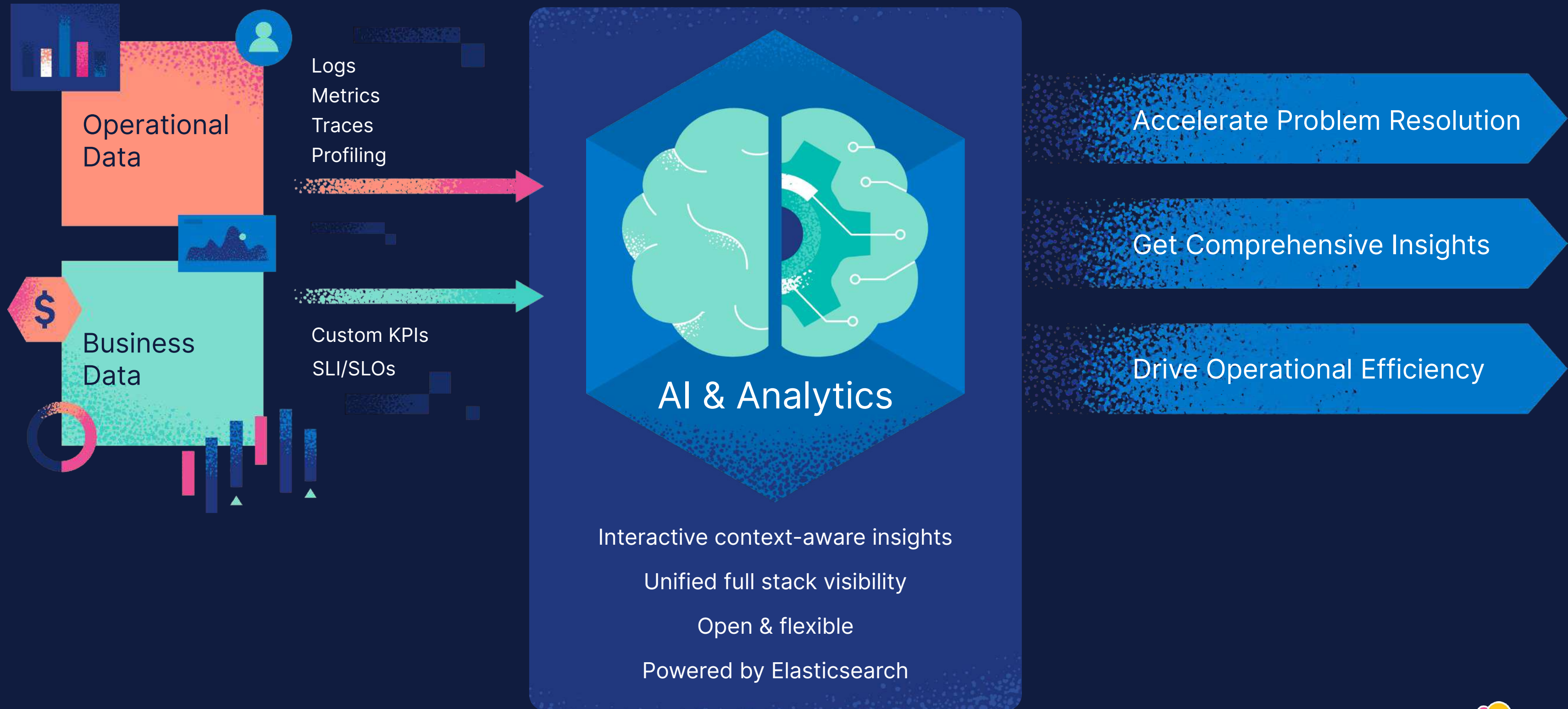
Satisfied customers

69%
improvement in
customer and employee
satisfaction

Teams need AI-powered observability



Meet Elastic Observability



Unified full stack visibility: Context-aware insights

Increase productivity & improve collaboration



Log monitoring & analytics



Cloud & infrastructure monitoring



Application Performance Monitoring

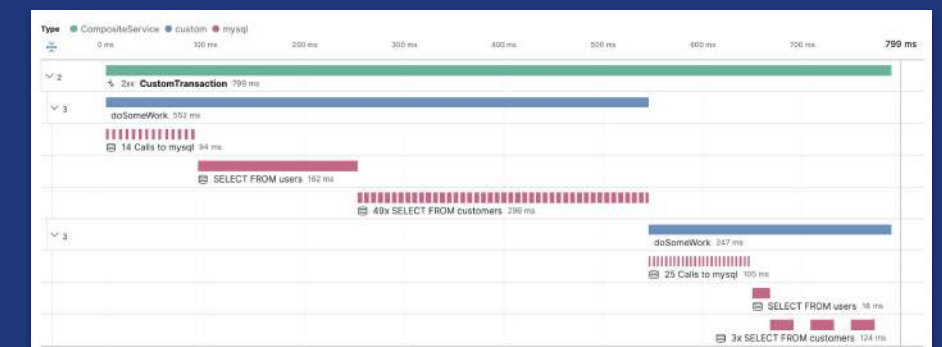
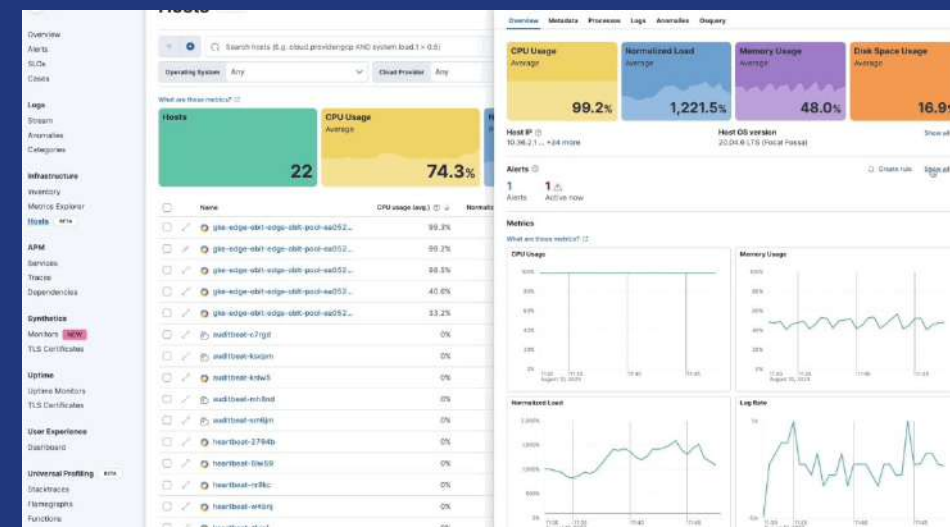
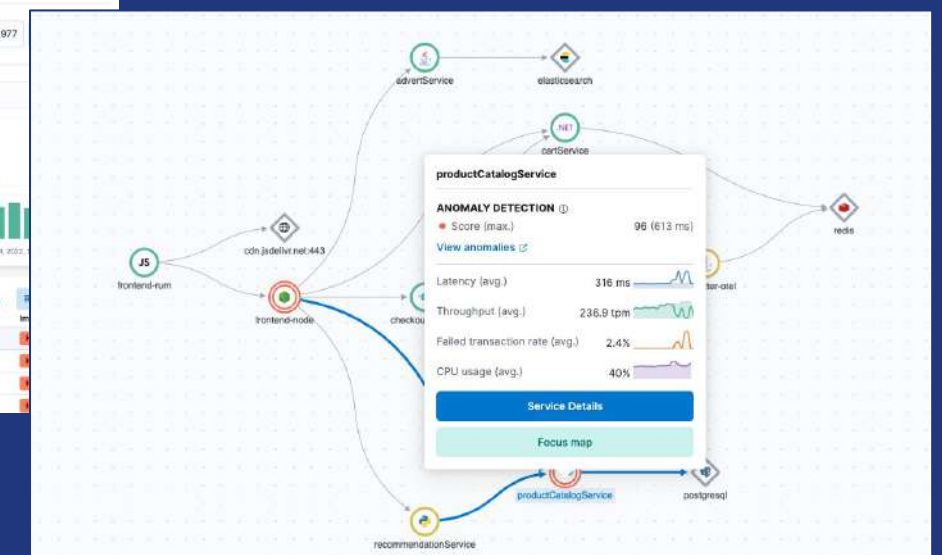
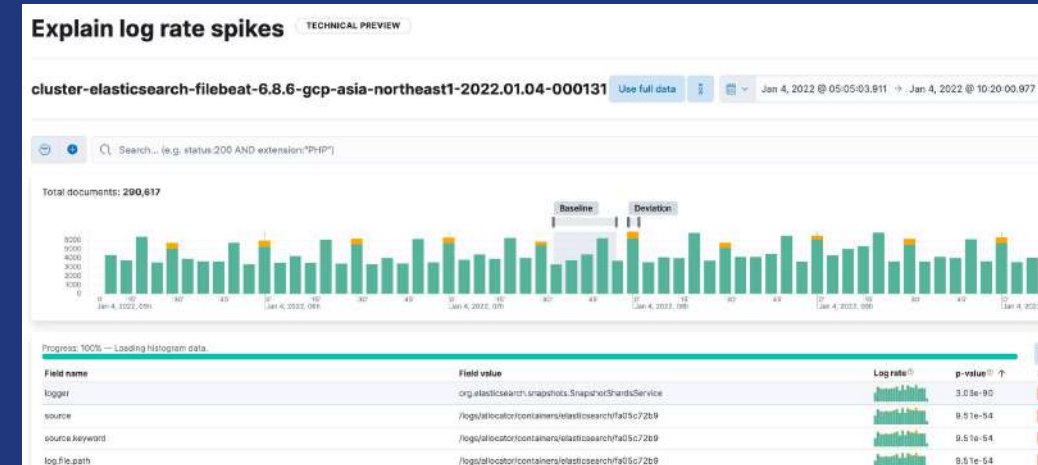


Digital Experience Monitoring



Universal Profiling

Integrated full stack views



Open and flexible: Any data, any source

Integrate with the technology ecosystem you rely on



Data architecture based on OpenTelemetry



Common data model (OTel + ECS)



API-driven,
350+ integrations



Open ML models,
plus bring your own



Future proof your investments

AI & Analytics: Correlate any type of data

Accelerate problem resolution and improve predictability



Anomaly detection & correlations



Log categorization



100+ out-of-the-box customizable ML models



Generative AI powered by ESRE

Democratize data and analytics

There's a spike in hourly revenue

Time	Severity	Detector	Actual	Typical	Description
September 27th 2021	94	sum(taxful_total_price)	\$2,525.91	\$397.49	critical anomaly in sum(taxful_total_price)

Details on highest severity anomaly

Field name	Value
Function	sum
Field name	taxful_total_price
Actual	2525.9
Typical	397.5
Job ID	hourly_revenue
Record score	94.798
Initial record score	65.898
Probability	0.0000746

Typically, we make about \$400, but this hour we made over \$2500

High Latency Incident

You wrote a message

What would you recommend to remediate that issue?

Elastic AI Assistant responded

Analyzing the logs would allow you to better understand what's wrong. Do you want me to run analysis of your logs?

Done

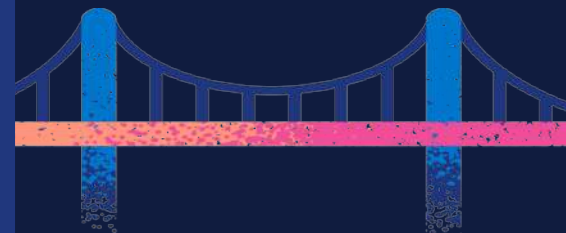
Regenerate

ESRE provides a bridge between private data and generative AI

- Sensitive databases
- Multi-system / cloud information
- Private knowledge bases
- Case histories
- Runbooks



ESRE Elasticsearch
Relevance Engine™



Large
Language
Models

Elastic
Observability Data

Elastic AI Assistant
for Observability

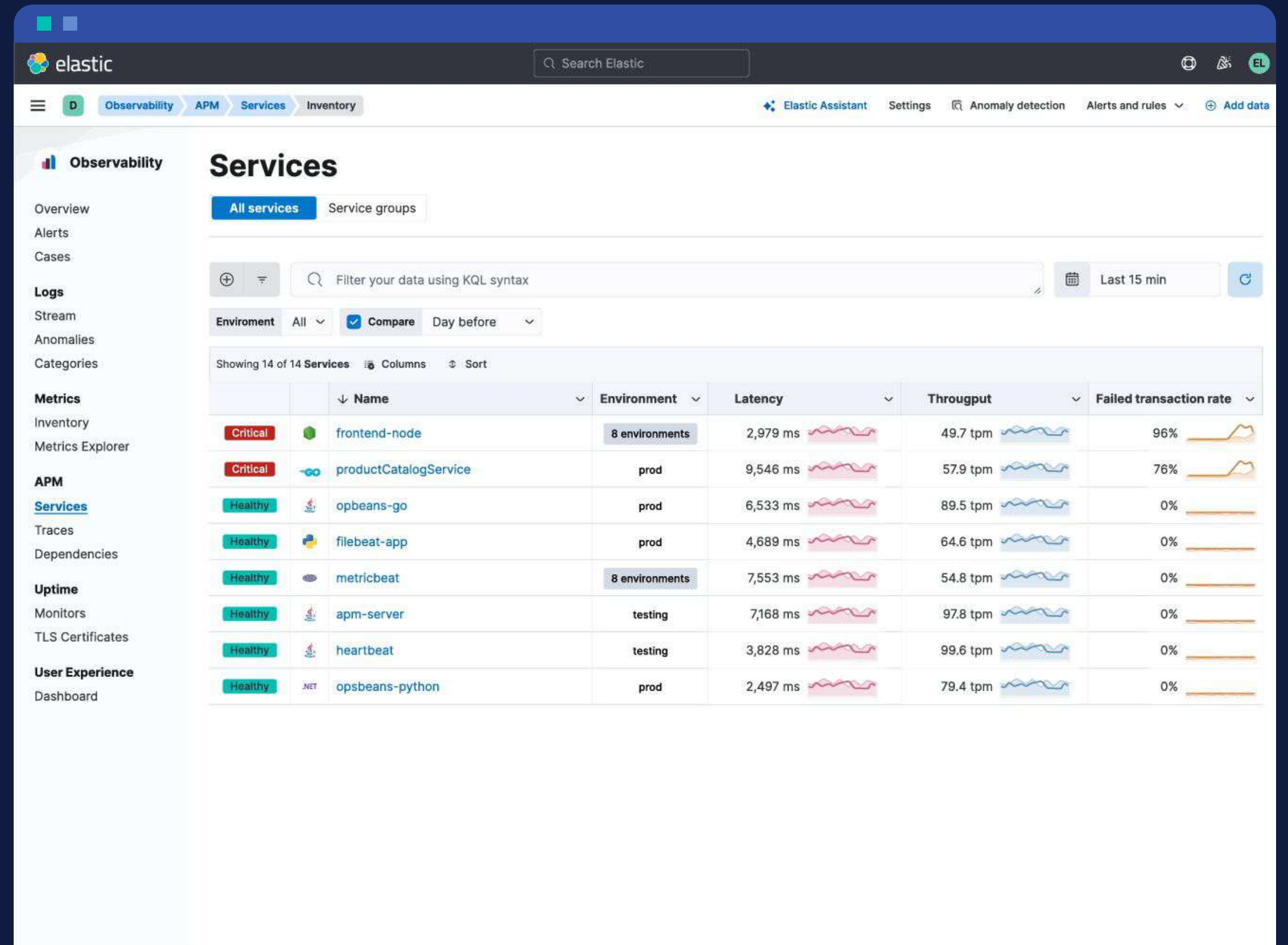


I just got pinged about
an alert - what's wrong?

AI Assistant for Observability

Powered by **ESRE** Elasticsearch Relevance Engine™

- Accelerate incident management and root cause analysis
- Interactively explore problems and execute remedies with generative AI
- Context-aware, business-specific output you can trust
- Based on your proprietary data and runbooks



One solution for all your Observability needs



Cloud Migration

- End-to-end hybrid and multi-cloud visibility
- Operate at scale
- Automated dependency mapping

Cloud Native

- Cloud, cloud-native integrations
- Insights into serverless, Kubernetes, microservices
- Correlate infrastructure and application

DevOps

- Visibility into software delivery chain
- Compare and troubleshoot releases
- Insights into CI/CD pipeline

AIOps

- Automated anomaly detection
- Interactive investigations with gen AI
- Integrated incident management

Digital Experience

- End user experience measurement
- User journey tracking
- Proactive notification and problem resolution

Tool Consolidation

- Eliminate data silos, better team collaboration
- Future proof with native OTEL support
- Low TCO / high ROI

BENEFITS OF Elastic Observability



Accelerate problem resolution

AI-powered capabilities enable you to correlate across all signal types and gain actionable insights



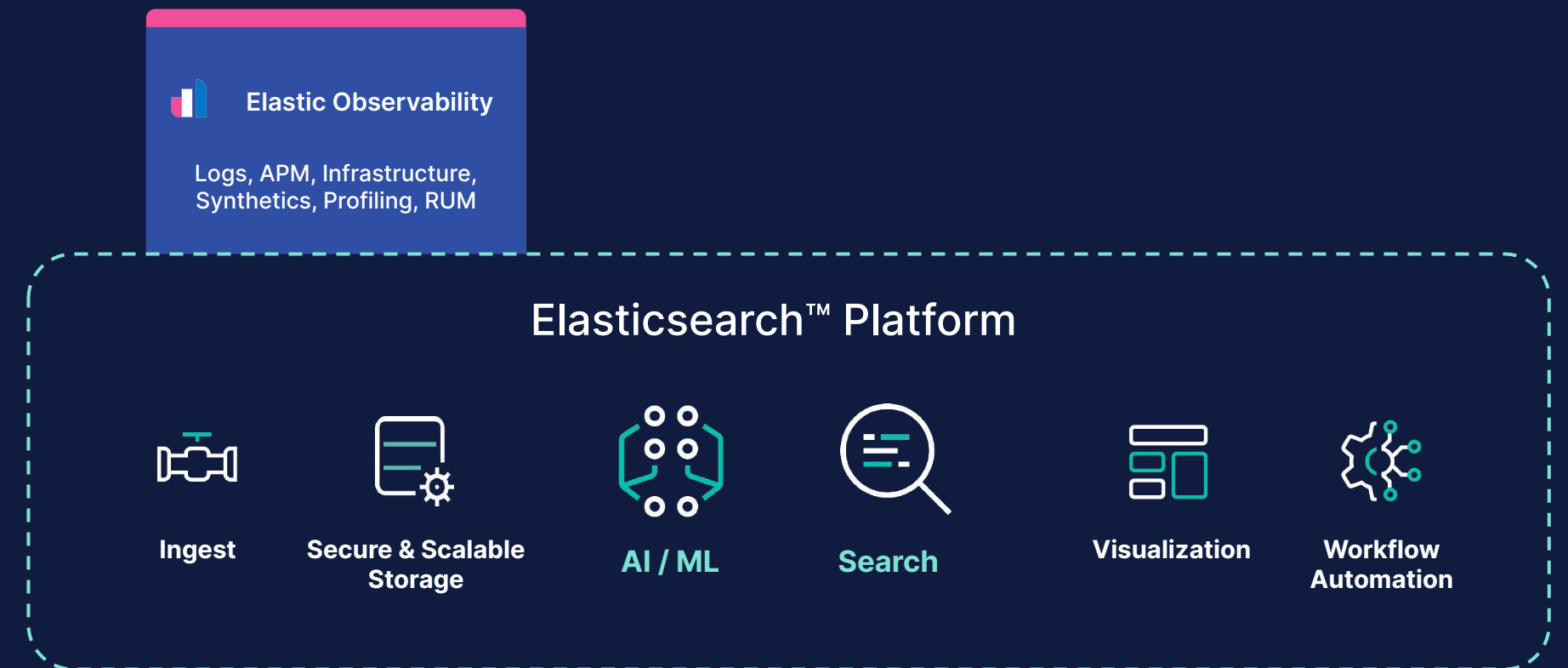
Get comprehensive insights

Open & extensible platform ensures ubiquitous “full stack” coverage of complex environments



Drive operational efficiency

Unified contextual visibility improves dev/IT productivity and collaboration, and drives business growth



Elasticsearch Platform Advantages

Elasticsearch™ Platform

Scalable economics

- Performant & cost-efficient tiered storage
- Predictable consumption billing

On-prem + cloud

- Flexible deployment options, 50+ global cloud locations
- HA & data locality with cross cluster replication

Single platform

- Observability + security in one platform
- Seamless cross-cluster search & analytics

Don't take
— just our —
word for it

Elastic recognized as a top 3 observability vendor

Positive market momentum



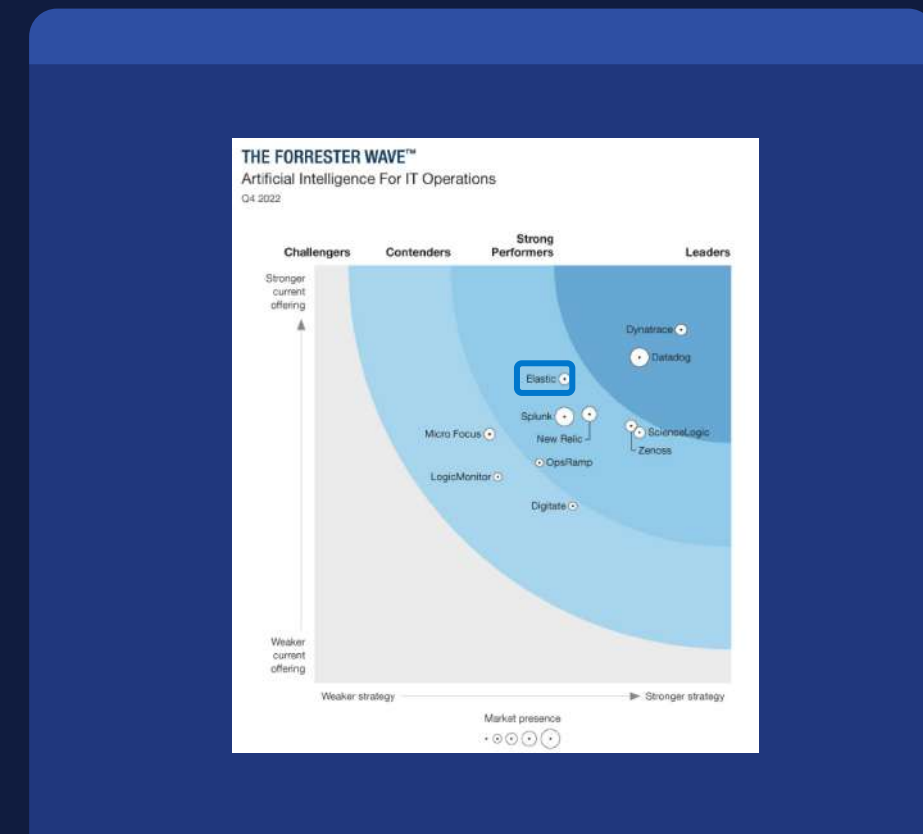
Gartner Critical Capabilities
– Top 3 in:

IT Operations, DevOps/Dev, SRE,
Digital Experience Monitoring



Gartner MQ for APM
and Observability

Visionary



Forrester Wave:
AI Ops

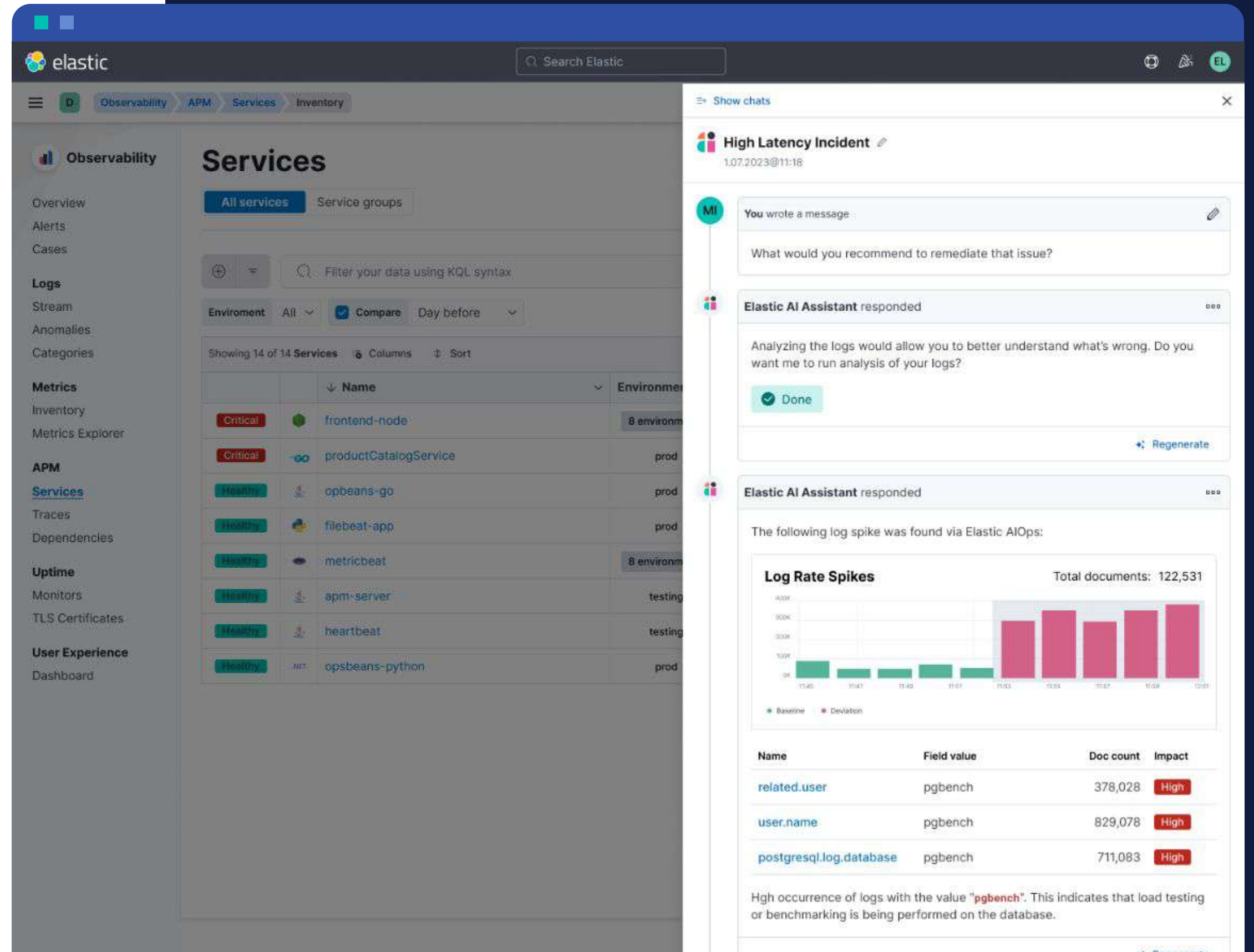
Strong Performer
as first time entrant

Thank You

AI Assistant

Powered by ESRE

- Accelerate incident management and root cause analysis
- Interactively explore problems and execute remedies with generative AI
- Open and agnostic to LLMs
- Context-aware, business-specific output you can trust
- Based on your proprietary data and runbooks



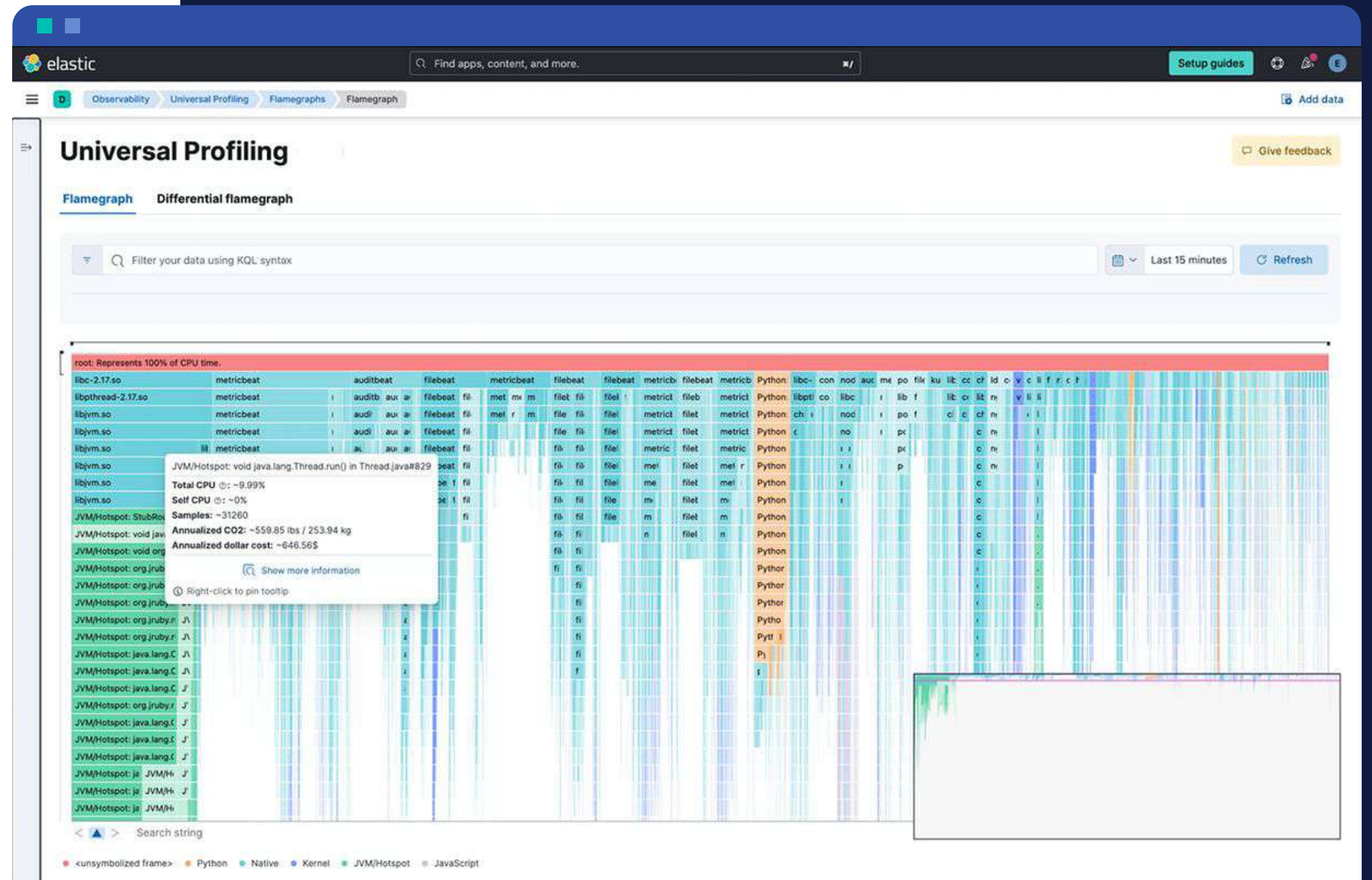
The screenshot displays the Elastic Observability AI Assistant interface. The main panel shows a 'Services' overview with a table of services and their health status. A chat window on the right shows a 'High Latency Incident' and the AI Assistant's response, which includes a 'Log Rate Spikes' bar chart and a table of log field values.

Name	Field value	Doc count	Impact
related.user	pgbench	378,028	High
user.name	pgbench	829,078	High
postgresql.log.database	pgbench	711,083	High

High occurrence of logs with the value "pgbench". This indicates that load testing or benchmarking is being performed on the database.

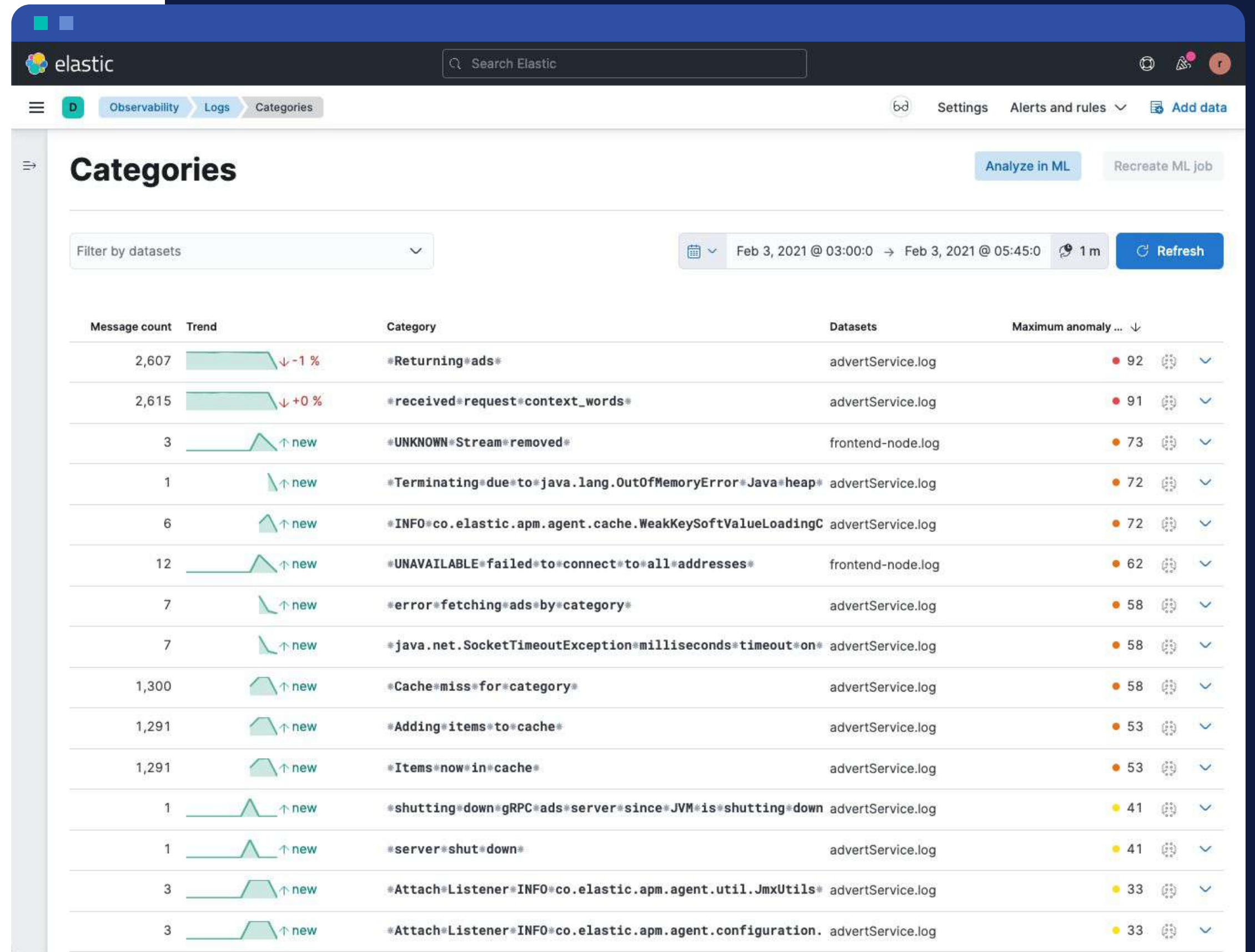
Universal profiling

- Go green with zero-instrumentation whole system visibility across a wide range of languages and containerized environments
- Get “always on” low overhead profiling in production
- Identify inefficiencies and performance regressions in your code and infrastructure
- Eliminate compute waste and reduce carbon footprint



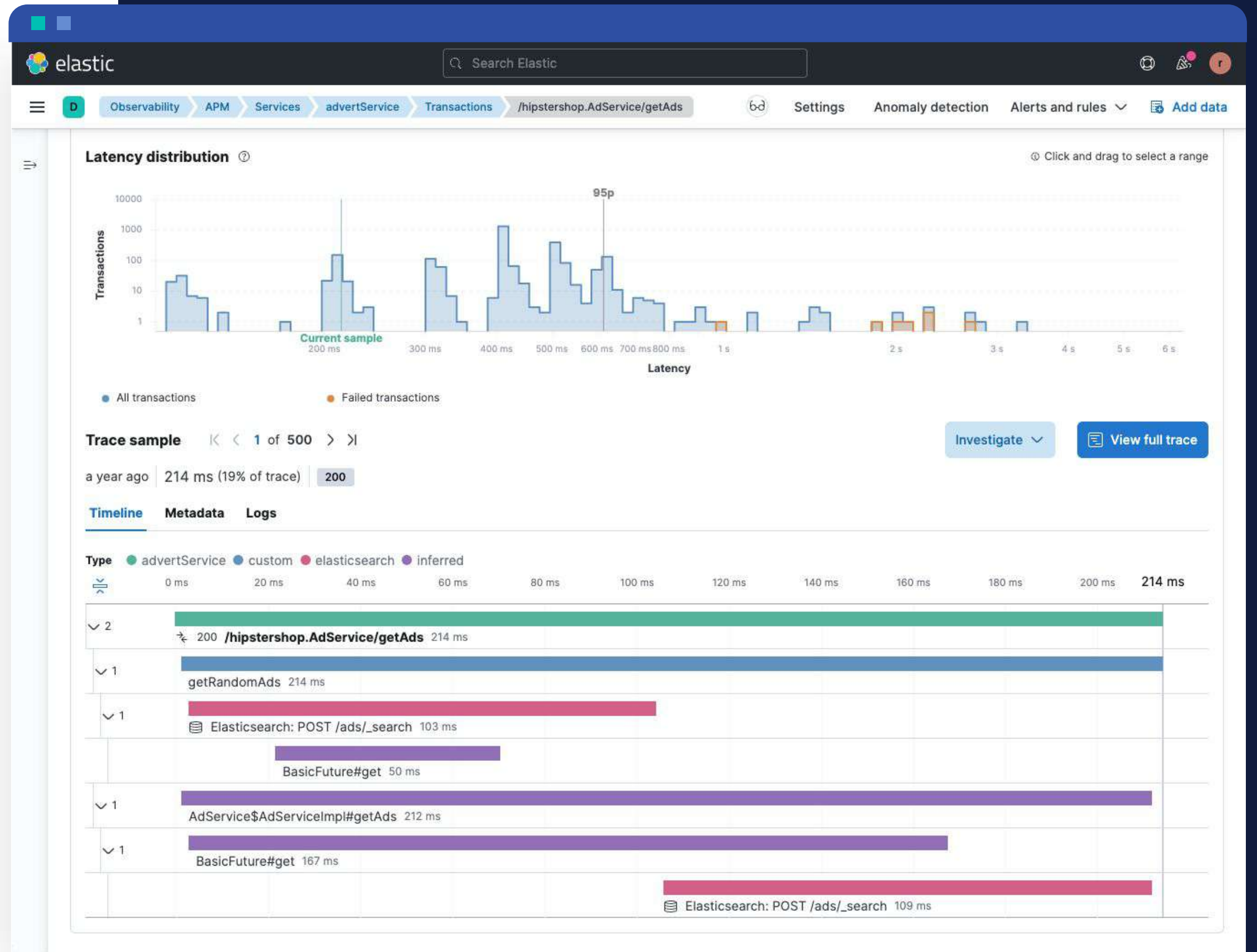
Log analytics

- AI-powered log categorization and anomaly detection to quickly make sense of billions of logs
- Powerful cross cluster search with superior speed, scale and relevance
- Efficient data tiering allowing you to keep all the data you need
- Context and correlation across all signals (logs, metrics, traces & business data)
- Full text search on indexed data - in milliseconds, not minutes!



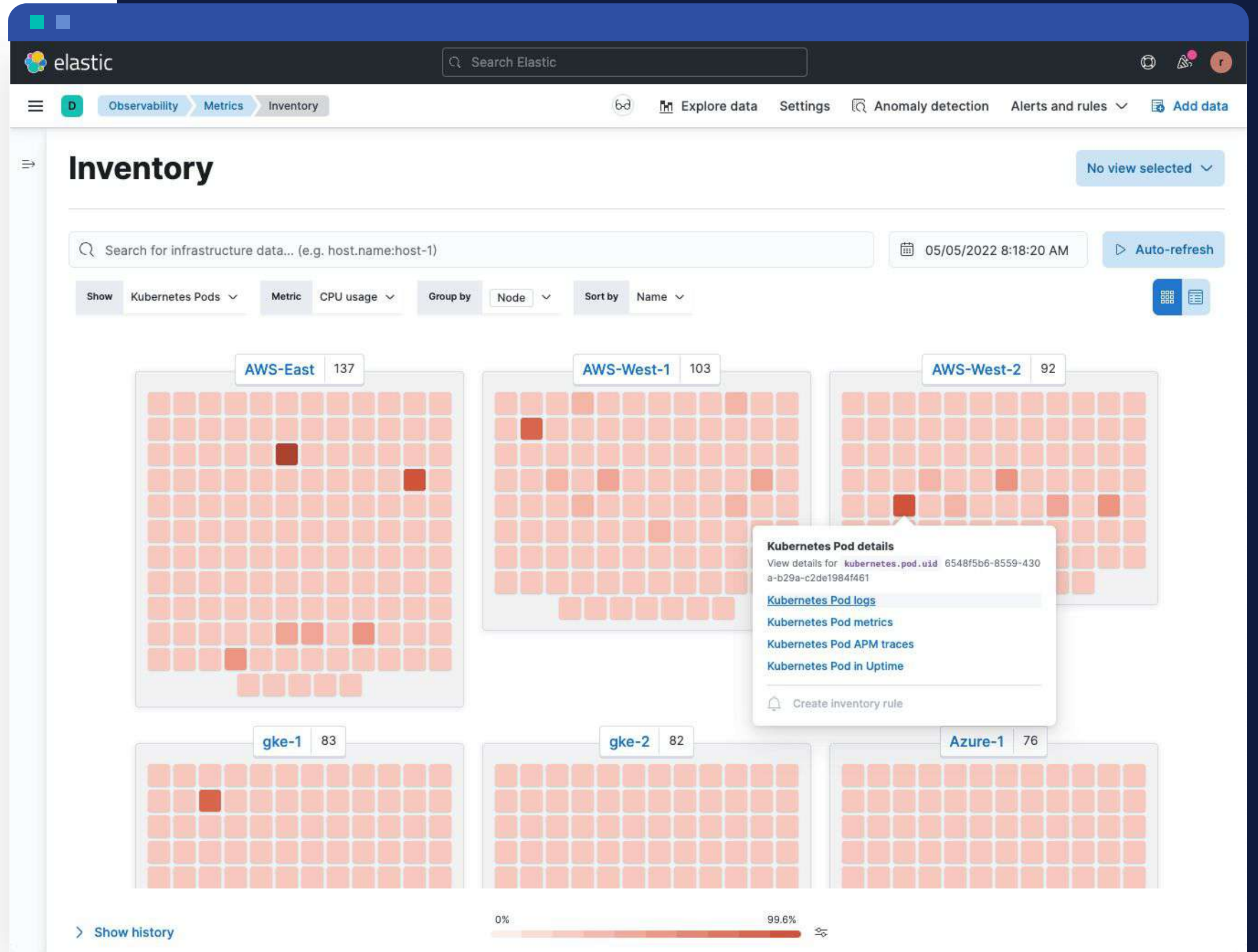
Application performance monitoring

- Improve code quality with end-to-end distributed tracing
- Quickly troubleshoot problems with ML-powered health indicators and anomaly detection
- Identify root cause of slowness and errors with on-demand correlations
- Out-of-the box support for OpenTelemetry and native agents



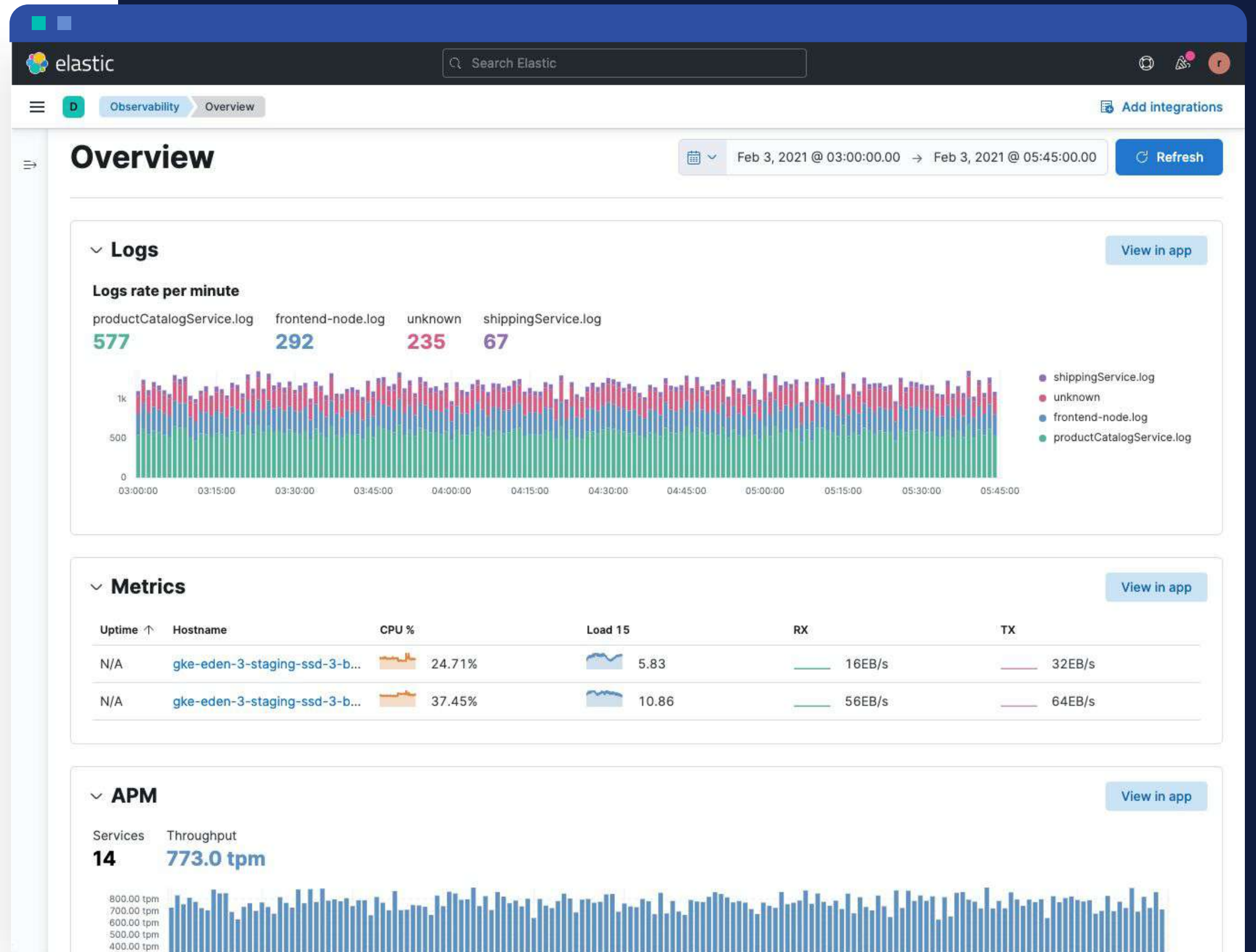
Unified visibility across all environments

- Insights into cloud native and 3-tier architectures
- 350+ deep and growing integrations on AWS, Azure, and Google Cloud
- Kubernetes (native or cloud deployed)
- Isolate problems quickly across complex architectures



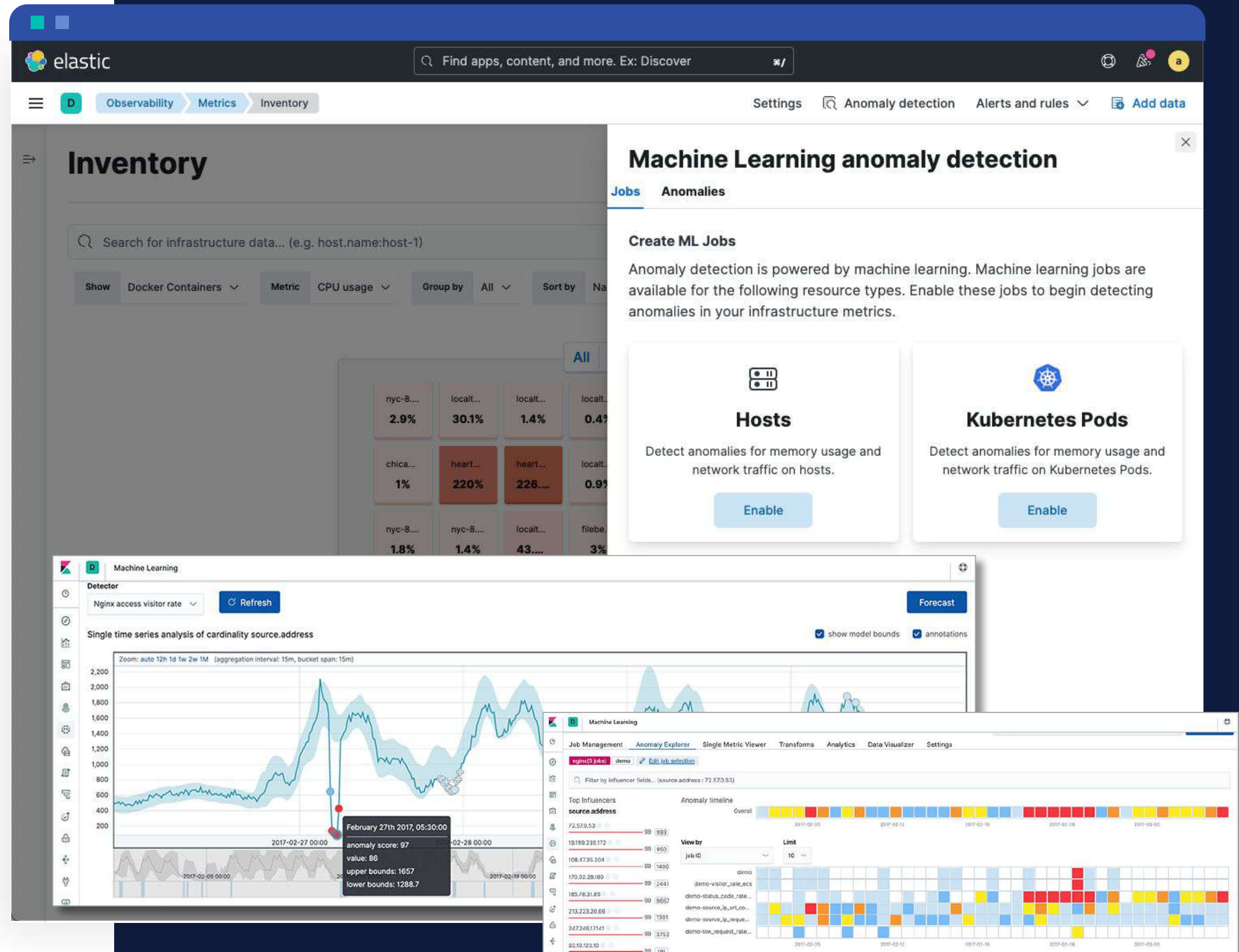
Break down silos with unified observability

- Single platform for all business and operational data
- Correlate metrics, logs, and traces – in context – for faster investigation
- Industry's only open common data model
- Improve cross-team collaboration (ITOps, DevOps, SRE, AppDev)



Actionable insights

- Zero configuration (built-in) machine learning
- AI-driven anomaly detection and root cause analysis across all observability data
- Automatic APM correlations to find root causes
- Powerful search for "unknown unknowns"
- Reduces MTTD and MTTR



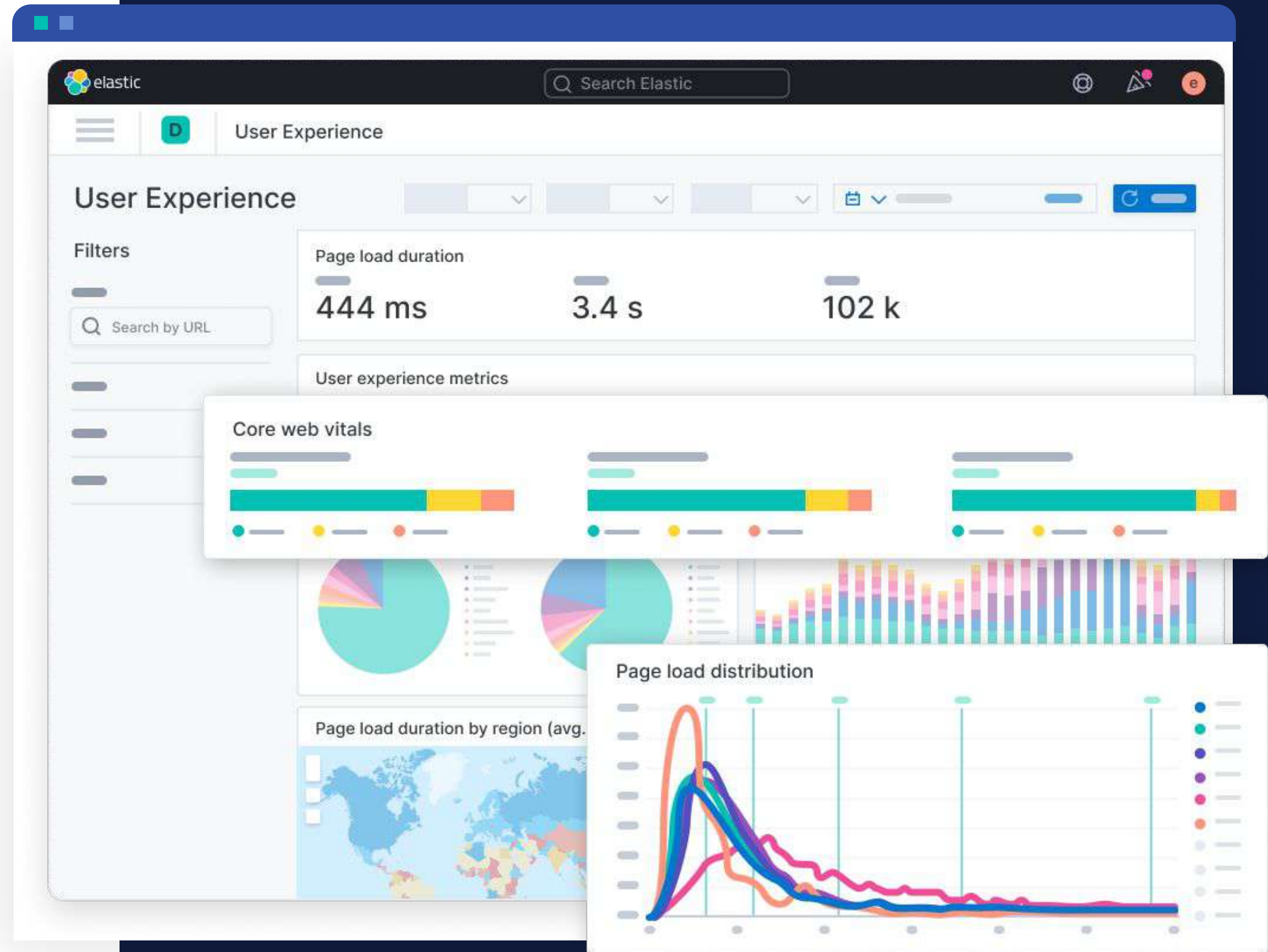
The screenshot displays the Elastic Observability interface. At the top, the 'elastic' logo and a search bar are visible. The main navigation includes 'Observability', 'Metrics', and 'Inventory'. A 'Machine Learning anomaly detection' panel is open, showing options to 'Create ML Jobs' for 'Hosts' and 'Kubernetes Pods'. Below this, a 'Detector' panel shows a 'Single time series analysis of cardinality source.address' with a line graph and a 'Forecast' button. A 'Machine Learning' panel at the bottom shows 'Job Management' and 'Anomaly Explorer' with a heatmap and a list of top influencers.

Host	Metric	Value
nyc-8...	CPU usage	2.9%
chica...	CPU usage	1%
nyc-8...	CPU usage	1.8%
localt...	Memory usage	30.1%
heart...	Memory usage	220%
nyc-8...	Memory usage	1.4%
localt...	Network traffic	1.4%
localt...	Network traffic	43...
localt...	Network traffic	0.4%
localt...	Network traffic	0.9%
filebe...	Network traffic	3%

source address	Score
72.570.53	99 (993)
19199.235.172	99 (950)
108.4735.204	99 (1490)
170.92.28.180	99 (2441)
185.78.31.85	99 (5687)
213.223.20.66	99 (1301)
247.246.171.41	99 (3752)
82.19.123.30	99 (191)

Gauge digital experience

- Track infrastructure, application and business trends over time
- Measure customer experience and proactively verify user journeys
- Resolve problems with tracing from the front end to the back end
- Establish SLOs and measure SLIs and SLAs



Simplify data ingest at scale

- Single agent for logs, metrics, and traces
- Central agent management with Fleet
 - Supports thousands of agents
 - One-click runtime policy changes and upgrades
- 350+ out-of-the-box integrations, many with dashboards and visualizations

