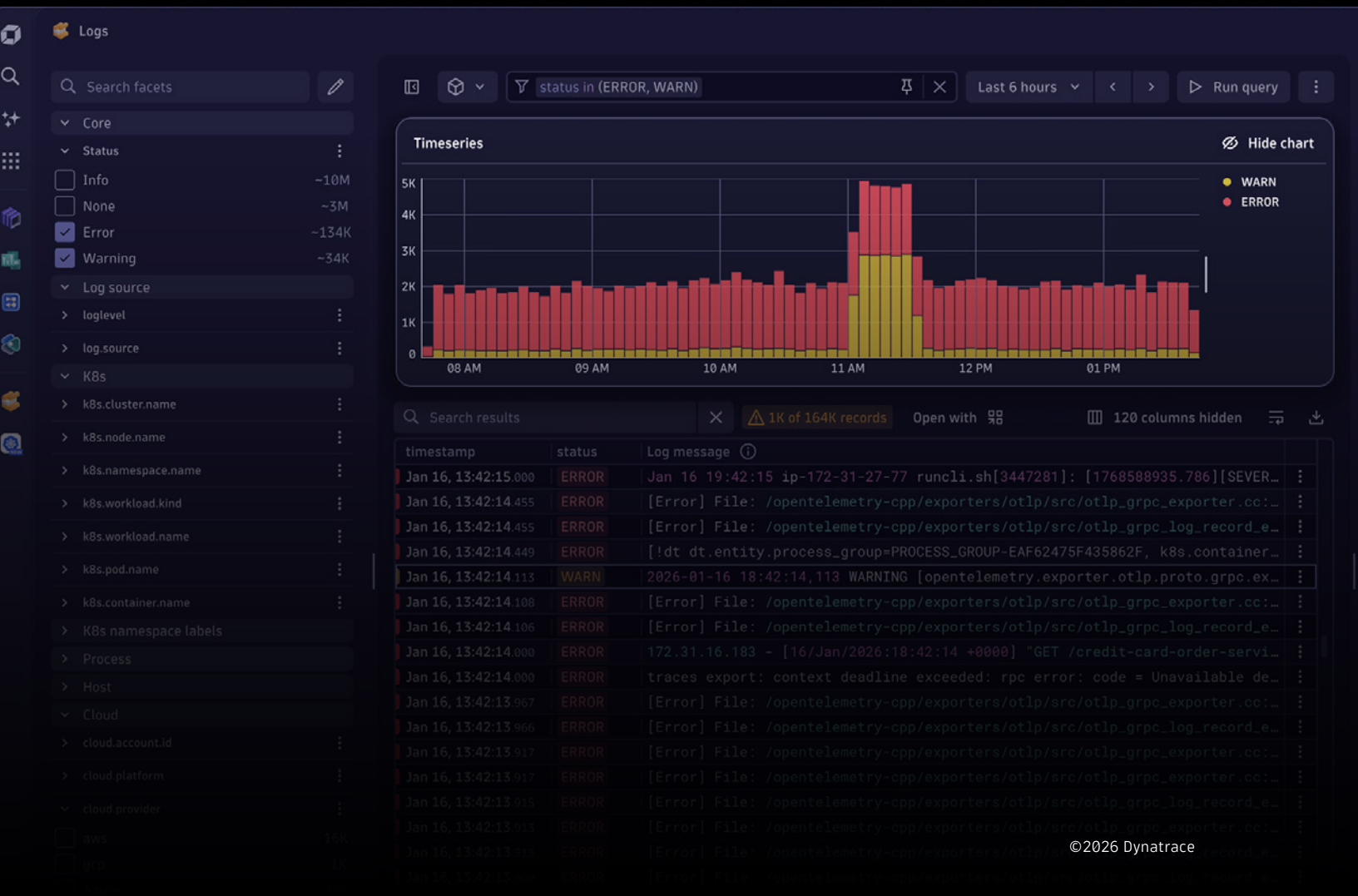
dynatrace

Log management and analytics

Manage every log cost-efficiently and in full context, for faster answers at any scale.



Introduction

Modern applications, cloud-native architectures, and AI-driven systems are creating more telemetry than ever. Logs remain one of the most important signals for understanding what happened, why it happened, and what teams should do next. But as volumes grow, traditional log management approaches force organizations to choose between cost, retention, and visibility.

Increasingly, teams are moving off legacy log platforms — not to get another place to search logs, but to stop trading cost against the visibility they need. Dynatrace removes that tradeoff whether you're replacing a standalone log platform at scale or bringing logs into context with the rest of your observability — and gives you the visibility to understand and control exactly what you're spending, so cost scales transparently with your needs.

Manage every log cost-efficiently, with no sampling or rehydration, and analyze those same logs alongside metrics, traces, events, topology, and business data — high-volume, cost-controlled log management and logs in full context, on one platform.

Built on the Grail data lakehouse and powered by Dynatrace Intelligence, Dynatrace delivers real-time log analytics, insights powered by AI, and automation at enterprise scale. Modern telemetry pipelines help teams collect, route, filter, enrich, and govern telemetry before it reaches storage — improving telemetry quality while controlling cost and complexity.

Dynatrace log management and analytics delivers measurable business results

37%
fewer Sev1 and Sev2 outages
Forrester

40%
reduction in telemetry waste

63%
cost reduction
UWM reduced log management costs after unifying on Grail

90%
faster mean time to reduction
Forrester

451%
ROI over 3 years
IDC

Traditional log management tools require tradeoffs

Traditional monitoring tools and log platforms impose cost, speed, and visibility tradeoffs. As log volumes increase, teams retain less data, sample more aggressively, or move older logs into slower storage tiers to stay within budget.

These approaches reduce cost in the short term but create operational risk. When teams discard or delay access to log data, they lose the context needed for troubleshooting, compliance, security investigations, and AI-driven operations. Rehydration and reindexing can take hours or days, slowing investigations exactly when teams need answers most.

The pressure is real: 67% of executives say their current log management approach costs more than it's worth, and organizations discard 86% of logs on average due to cost constraints. And when costs do spike, most teams can't pinpoint which team, workload, or query is driving them — leaving cost management reactive instead of proactive.

Modern operations require a different approach: cost-efficient access to high-volume telemetry, full context across observability signals, and intelligent automation that turns data into answers instead of more manual analysis.

The pressure to modernize is real

67%

of executiives say their current log management approach costs more than it's worth.

Dynatrace, The State of Log Management 2026

86%

of logs are discarded due to cost constraints, on average.

Dynatrace, The State of Log Management 2026

Introducing Log management and analytics from Dynatrace

Dynatrace breaks the traditional triangle of cost, speed, and insight tradeoffs — whether you're consolidating a high-volume log estate off a standalone platform or bringing logs into context with the rest of your observability. Logs are stored in Grail alongside metrics, traces, events, topology, and business data, giving teams a single source of truth they can query in real time at any scale, with no indexes, rehydration, or sampling to stay on budget.

That means teams keep and analyze all their logs cost-efficiently, and get more from them. Smartscape continuously maps relationships across applications, services, processes, hosts, Kubernetes, cloud platforms, and user journeys, and Dynatrace Intelligence analyzes that context automatically to detect anomalies, identify root cause, explain behavior, and trigger automation when action is needed.

The result is modern log management that goes beyond search — at a scale and cost traditional platforms can't match. Teams understand what happened, why it happened, who or what was affected, and how to respond, without sampling data to control spend, manually stitching telemetry across tools, or waiting for archived logs to be restored.

THE TRADEOFF YOU LIVE WITH TODAY VS. MODERN LOG MANAGEMENT

Legacy log management	Modern log management with Dynatrace
Costs climb with volume, so teams sample telemetry and cut retention to stay on budget.	Ingest and analyze all logs cost-efficiently — no sampling to stay on budget.
Cold and archived tiers mean rehydration and waiting before you can query.	Always-on hot storage with no rehydration, and up to 10 years of retention.
Indexes, schemas, and storage tiers are yours to size, tune, and maintain.	No schema, indexing, or tier management; nothing to maintain.
Logs sit in a silo, manually correlated with metrics and traces in other tools.	Logs are automatically in context with metrics, traces, topology, and business data.
Answers need query expertise, leaving teams dependent on a few specialists.	Natural-language and AI-assisted analysis open answers to the whole team.

Get answers to any question, in real time, at scale, and on budget

Dynatrace turns high-volume logs into answers — analyzed cost-efficiently on their own and in full context with the rest of your observability, security, and business data, with no indexes, rehydration, or complex schema management.

- **Answers at any scale.** Ingest and analyze high-volume logs without sampling, indexes, storage tiers, or rehydration — so you keep every log and query it instantly, on budget.
- **Faster troubleshooting.** Analyze logs on their own or in context with traces, metrics, events, and topology to reduce mean time to repair.
- **Actionable analytics.** Query, parse, and transform logs to identify patterns, create metrics, build dashboards, and prioritize what matters.
- **Situational awareness.** Collaborate securely with live data, reusable notebooks, dashboards, and information-rich visualizations.
- **Answers powered by AI.** Use Dynatrace Intelligence to surface precise, causal answers — from a standalone log investigation to full-stack root cause across every signal.

2 months to 2 minutes

What that looks like in practice

A root-cause investigation that once meant an engineer manually piecing together logs, traces, and metrics for hours now takes seconds.

FreedomPay cut mean time to identify from two months to two minutes and now resolves 99% of issues before customers are affected.

Overview of Log management and analytics features

Each capability below is grounded in what sets Dynatrace apart from standalone log tools: full context, Grail economics, and answers powered by AI.

LOGS APPLICATION

Simplified log management and analytics

- Quickly analyze logs with a log distribution dashboard.
- Use powerful search and customizable filters without requiring a query language.
- Find surrounding logs before and after events with a single click.

INGEST SUPPORT FOR 600+ LOG SOURCES

- Automatically add context to ingested logs with Dynatrace OneAgent.
- Use native OpenTelemetry support for logs, metrics, and traces.
- Ingest from cloud, Kubernetes, infrastructure, applications, APIs, and common log shippers.
- Use native integrations for AWS, Azure, Google Cloud, Fluent Bit, FluentD, Syslog, and other common sources.
- Use modern telemetry pipelines to collect, route, filter, enrich, and govern telemetry before analysis.
- See Dynatrace Hub for a complete list of supported log sources

---

LOG INSIGHTS INCLUDED IN PLATFORM APPS

Infrastructure, Kubernetes, Cloud, Security Investigator, and Database apps include log insights directly in the investigation workflow.

- View log distribution dashboards within platform apps.
- Search and filter logs during investigations.
- Open surrounding logs before and after the log under review.
- Automatically associate distributed traces with relevant logs.
- Support threat detection and incident analysis using logs in Security Investigator.

DYNATRACE QUERY LANGUAGE (DQL) AND NOTEBOOKS INCLUDING LOGS

Deep analytics instantly, with collaborative and repeatable investigations

- Analyze any data in Grail without predefined schemas, indexes, or storage management — with queries up to 10x faster than traditional tools and no indexes to wait on.
- Query across logs, traces, metrics, business events, Dynatrace Intelligence insights, and more.
- Support complex multi-step analysis in real time.
- Share log analysis, operational investigations, and security forensics in dynamic Notebooks.

DYNATRACE INTELLIGENCE PROVIDES PREDICTIVE, CAUSAL, AND GENERATIVE AI FOR LOGS

- Detect anomalies automatically across the full IT and application landscape.
- Identify root cause across logs, metrics, traces, events, topology, and affected entities — automatically, without manual correlation.
- Use predictive insights with workflow automation to respond before issues impact users.
- Use natural language to explain log content, create dashboards, write DQL, generate notebooks, and accelerate analysis.

LOGS, TRACES, EVENTS, AND METRICS IN A UNIFIED VIEW

OneAgent, OpenTelemetry, Smartscape, and Grail work together to provide rich context for logs

- Add context to logs automatically during ingest based on real-time topology and entity relationships.
- Associate traces, events, metrics, and logs with specific problems to decrease MTTI and MTTR.
- Use Grail as a scalable, fast source of truth for logs and all observability signals.
- Use unified context to support troubleshooting, security analytics, business insights, and AI-driven operations.

OUT-OF-THE-BOX DASHBOARDS PROVIDED FOR LOGS

Take advantage of ingest, usage, and cost intelligence dashboards

- Gain transparency into ingest, retention, and query usage.
- Identify high-volume applications, users, sources, buckets, and queries.
- Allocate log costs by team, cost center, or workload — and forecast spend before it hits budget limits.
- Optimize cost by turning high-value log data into metrics for dashboards and alerting.
- Understand ingest volume, source health, and retention usage across environments.

Teams that act on these insights cut real cost: UWM reduced log management costs by 63%, and ADT reduced log monitoring costs by 30–40% after unifying telemetry in Grail.

Benefits of Log management and analytics features

HASSLE-FREE MANAGEMENT

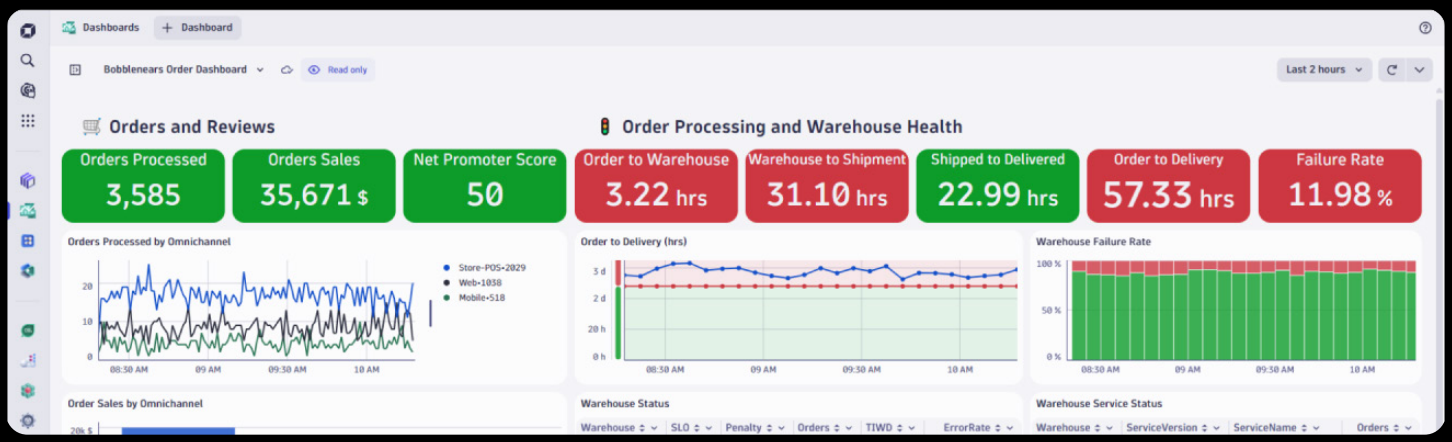
Store petabytes without schemas, indexing, or rehydration

- Access petabytes of data instantly without restoring and reindexing from cold archives.
- Analyze logs without rigid schemas, expensive indexes, or upfront assumptions about future queries.
- Choose retention that fits business, operational, and compliance needs — from debug to audit, up to 10 years.

REAL-TIME ANALYTICS AT SCALE

Analyze de-siloed data sources in full context

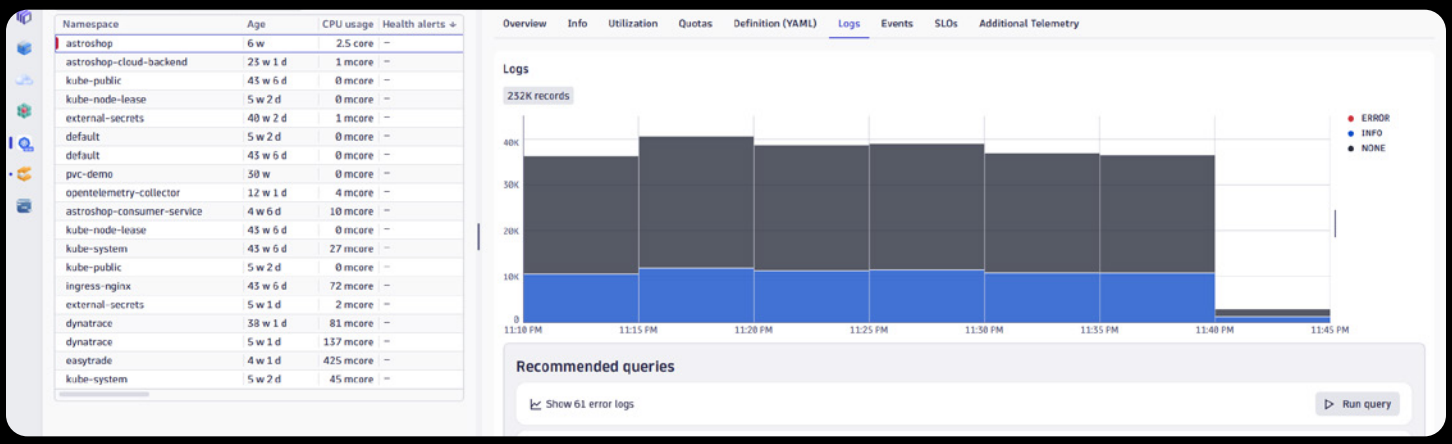
- Consolidate observability data into a purpose-built data lakehouse with one query approach — at up to 90% lower storage cost and up to 100x faster queries than traditional tools.
- Analyze logs in context with traces, user sessions, topology, events, and business data.
- Pinpoint root cause faster by using analysis powered by AI to surface the most relevant context automatically.



ACCELERATE TIME TO VALUE

Turn logs into metrics, dashboards, and operational insight

- Optimize cost by creating metrics from log data and using them in dashboards and alerting.
- Turn any query into a metric or dashboard without rehydrating or reindexing archived data.
- Reduce manual effort and alert noise with auto-baselining, anomaly detection, and root-cause analysis.



PRECISE ANSWERS WITH EMBEDDED EXPERTISE

Explore logs in context of auto-discovered entities, dependencies, and topology

- Quickly focus on relevant application, Kubernetes, cloud, and infrastructure components during live troubleshooting.
- Explore, filter, and search log and event data in context with the systems and services that generated it.
- Use interactive visual queries to navigate investigations and easily pin insights to dashboards.

```
fetch logs, from:now()-3h
| filter dt.process.name=="cartservice cartservice-*"
| filter contains(content, "AddItemAsync")
| fields timestamp, content
| parse content, "LD 'userId=' LD:userId ', productId=' LD:productId ', quantity=' INT:productQuant
| fields productId , productQuantity
| summarize averageProductQuantity = avg(productQuantity), by:{productId}
| sort averageProductQuantity desc
| limit 5
```

TAKE FULL CONTROL

Query, parse, and analyze instantly with Dynatrace Query Language (DQL)

- Use a familiar pipe-based query language built for observability analytics.
- Unlock value across observability, security, and business data without relying only on ingest-time parsing.
- Run flexible analysis across large data volumes with purpose-built, high-speed algorithms and massively parallel processing.

FITS UNIQUE ENVIRONMENTS

Broad ingestion and control across hybrid, multi-cloud, and AI-driven environments

- Use open APIs and native multicloud support for Kubernetes, Red Hat OpenShift, AWS, Microsoft Azure, Google Cloud, and hybrid environments.
- Collect logs across the application stack using Dynatrace OneAgent, OpenTelemetry, APIs, and common log shippers.
- Use Bindplane telemetry pipelines to route data from any source to any destination on open standards, and to filter, enrich, and mask telemetry before storage — reducing telemetry waste by 40% or more while keeping logs available for real-time analysis.

Migration, de-risked

Moving off a legacy log platform sounds daunting — it doesn't have to be. Dynatrace brings proven migration methodologies, AI-assisted onboarding, and dedicated support to make the transition smooth. Many teams start with a single high-value use case to prove the savings fast, then expand on a clear, planned path.

01

PROVE ONE USE CASE

Start with a single high-value use case to prove the savings fast.

02

RUN IN PARALLEL

Bindplane telemetry pipelines route data from any source to any destination—cut over on your own timeline, no rip-and-replace.

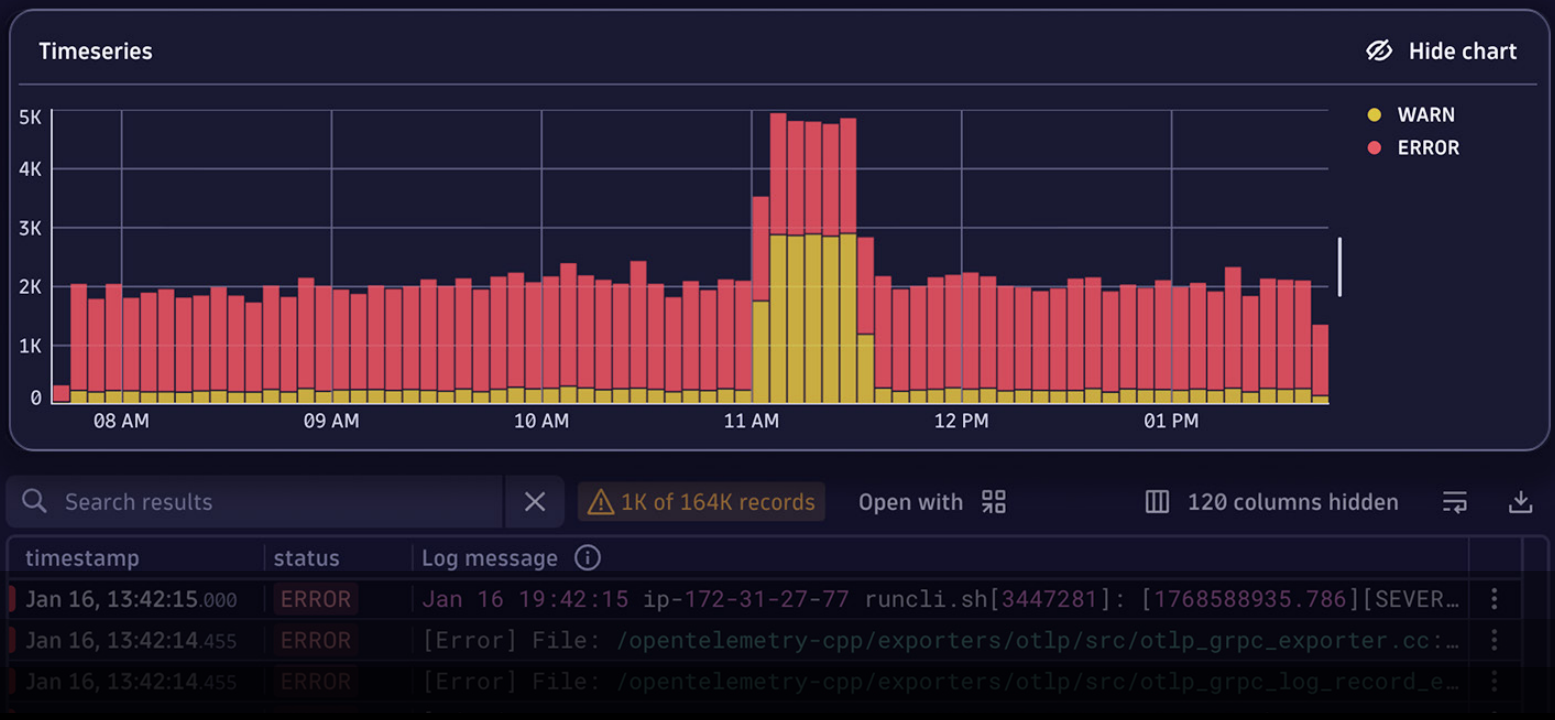
03

EXPAND ON YOUR TIMELINE

Expand on a clear, planned path with proven methodologies and dedicated support.

Why teams replace legacy log platforms with Dynatrace

	Legacy log platforms	Dynatrace
Answers, not just search	Legacy platforms return results you still have to interpret.	Dynatrace Intelligence identifies root cause automatically across logs, traces, metrics, and topology — no manual correlation, no skipped searches.
Predictable economics	Volume-based licensing forces teams to sample and cut retention.	Dynatrace separates ingestion from utilization with transparent, flexible pricing — and built-in cost intelligence lets teams forecast spend, set budget thresholds, and trace any cost spike to its source, so there are no surprises at invoice time.
Nothing to maintain	Clusters, indexes, schemas, and storage tiers to size and tune.	Grail delivers hot-storage access to petabytes without rehydration.
Built for scale and AI	Batch-era indexing and search-first tools struggle to keep pace	A streaming architecture and unified data model handle cloud-native and AI-driven telemetry growth



The Dynatrace difference

Dynatrace is a unified observability platform that turns high-volume telemetry into trusted answers and intelligent automation. Grail stores observability, security, and business data efficiently in context. Smartscape continuously maps dependencies across dynamic environments. Dynatrace Intelligence analyzes that context to detect issues, explain behavior, identify root cause, and support automated remediation.

This combination helps teams move beyond isolated log search. Logs become part of a broader system of insight that connects what happened to the services, users, dependencies, business processes, and outcomes affected. Teams reduce cost and complexity while improving reliability, customer experience, and operational efficiency.

Modern telemetry pipelines extend this value by giving teams greater control over data collection, routing, filtering, enrichment, and governance before telemetry reaches storage. Together, these capabilities help organizations scale log management for modern environments without sacrificing visibility or speed.

Dynatrace modern log management and analytics delivers measurable business results, including:

> LOWER LOG MANAGEMENT COST

Customers reduce log management costs by 30–60% through consolidation and optimized data usage — UWM by 63%, Agos by 50% — with up to 90% lower storage cost than traditional tools.

Teams use Cost Intelligence to surface the highest-impact savings opportunities — from expensive redundant queries to log volume at the source — with Bindplane reducing volume before it reaches Dynatrace and OpenPipeline controlling what gets stored.

> BUSINESS REVENUE RETURNS

IDC reported customers received a 451% return on investment over three years, and large enterprises received $2.6M on average back to the business for every 100 supported applications utilizing the Dynatrace observability platform including logs.

> OPERATIONAL EFFICIENCY

Organizations using Dynatrace identify issues 80% faster and reduce mean time to recovery by 90% (Forrester). FreedomPay resolves 99% of issues before user impact; BT cut incident and outage time by 50% and identified root cause up to 90% faster.

> BETTER CUSTOMER EXPERIENCES

IDC reported customers using Dynatrace had 37% fewer Sev1 and Sev2 outages, spent 56% less time resolving them, and experienced 72% less revenue lost from those outages.

XX.XX.XX BAEXXX_WP_USLet_cs