

6 reasons to migrate from New Relic to IBM Instana



Contents

01 →

Introduction

02 →

Reason 01:

IBM Instana understands your most complex cloud-native and hybrid cloud applications

03 →

Reason 02:

IBM Instana captures and stores every trace for every user—at no additional charge

04 →

Reason 03:

IBM Instana automates the entire application monitoring process

05 →

Reason 04:

IBM Instana helps predict issues and service incidents before they occur

06 →

Reason 05:

IBM Instana is the application silo-buster, providing real-time observability data with context

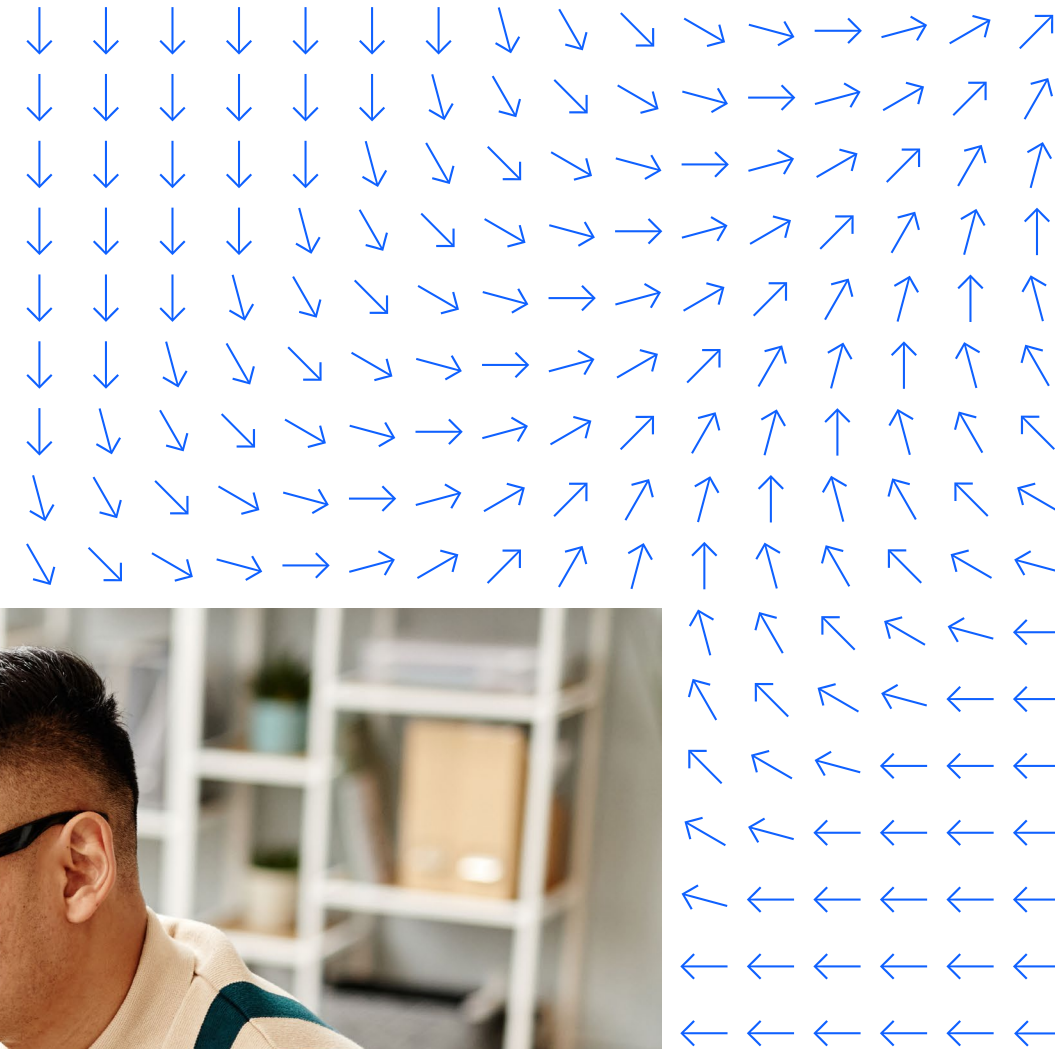
07 →

Reason 06:

IBM Instana pricing has no surprise costs and is simple, transparent, and all-inclusive

08 →

Conclusion



Introduction

You've relied on New Relic application monitoring for years but managing cloud-native applications requires a different approach.

In our view, to effectively monitor cloud-native applications, you must have high granularity and cardinality, complete correlated full-stack visibility, and end-to-end distributed tracing. These capabilities help ensure that you can see issues in real-time and rapidly resolve them using Instana's AI-driven automated or semiautomated remediation capabilities.

Founded in 2008, much of New Relic's monitoring solutions were designed and built before technologies for cloud-native applications—such as microservices, containers and Kubernetes—even existed.

Even hybrid and multicloud architectures didn't come around until years later. These legacy monitoring tools revolved around the ability to see production code. That was a fine strategy back when the entire application structure centered around custom code and application servers.

When cloud-native technology emerged, the world of applications changed—their make-up shifted to distributed microservices, orchestrated containers, serverless workloads, polyglot development, and so on. In distributed microservice applications, individual pieces of custom code are no longer the focal point of applications.

Now is the time to make the switch. This ebook explains 6 reasons why IBM Instana should be your future observability solution.

IBM Instana: observability and monitoring for modern applications

Meet IBM® Instana™, the enterprise observability platform that simplifies cloud-native application monitoring for DevOps and site reliability engineering (SRE) teams. Instead of piecemeal monitoring focused on custom code, IBM Instana collects data up and down the technology stack including infrastructure, cloud, containers, orchestration, code, data flow and more, to provide a precise understanding of how all the pieces fit together. Real-time service maps identify and show every dependency, and end-to-end distributed traces are captured for every request, for every user, while every code-driven process is profiled automatically. Automation even extends to troubleshooting—IBM Instana not only marks hotspots, but also identifies the event that triggered the problem.

The IBM Instana user experience is designed to give every application stakeholder—Dev, ITOps, DevOps, SRE, IT decision makers, line of business and business executives—the observability data they need to understand how applications impact them in a way that makes sense to them. Our philosophy is that observability should be democratized for all—all the data, with all the context for all your teams.

That's why organizations that rely on critical applications use IBM Instana. Are you next?

This e-book explains the 6 reasons the IBM Instana enterprise observability platform should be your future observability solution.

Reason 01: IBM Instana understands your most complex cloud-native and hybrid cloud applications



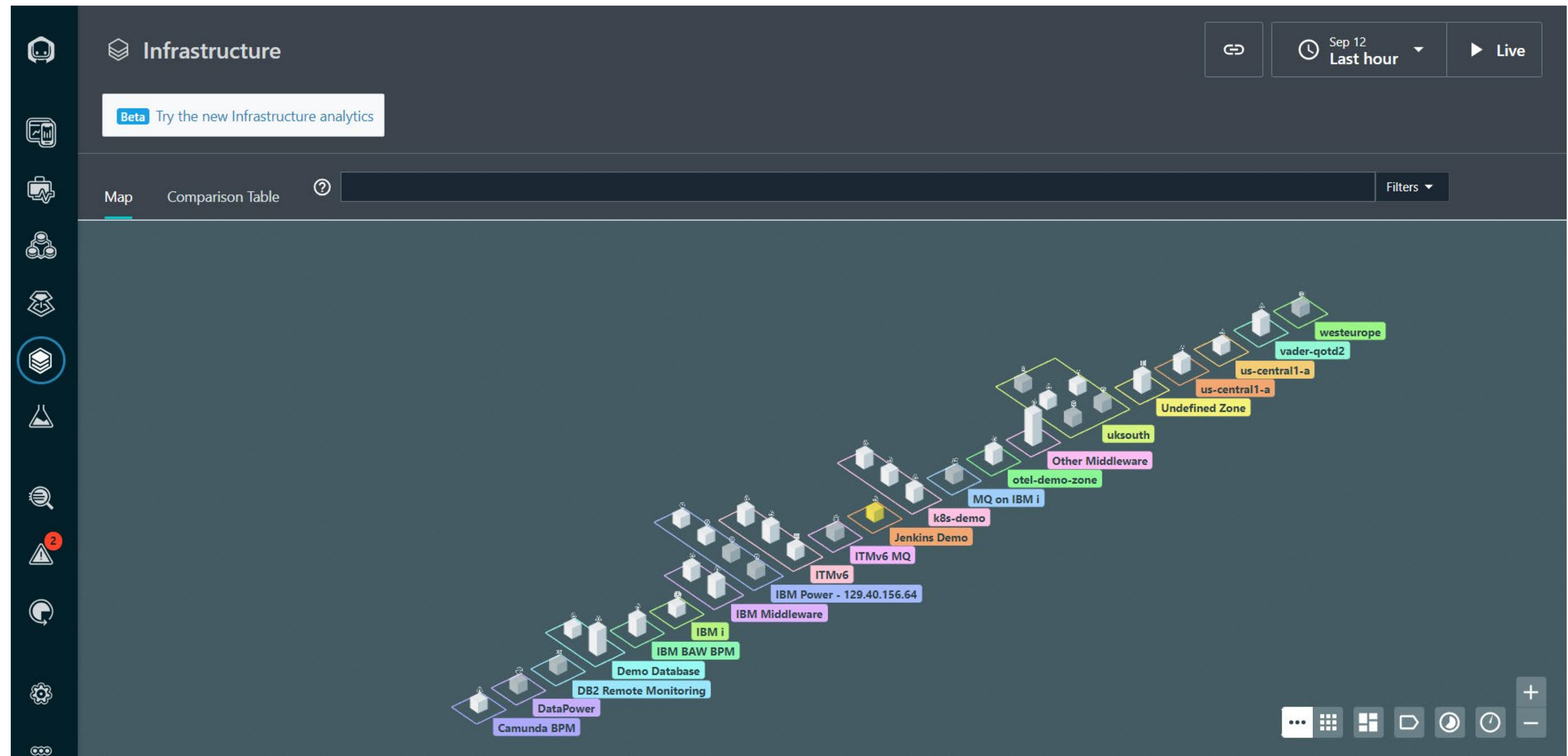
IBM Instana is the enterprise observability platform built to deal with cloud-native applications. IBM Instana leads the way for monitoring in the world of distributed microservices:

- The first APM solution to automatically monitor application services running on Docker with no code manipulation
- The first observability platform to automatically monitor applications running on Kubernetes infrastructure—and correlate it with the performance metrics and traces of applications running on top of it
- The only application monitoring tool to deliver mainframe-native transaction tracing

IBM Instana works automatically, out of the box, with full-stack visibility no matter how your applications are built or where they run—on public or private cloud, hybrid and multicloud, virtualized or containerized, Kubernetes or OpenShift, and so on.

IBM Instana automatically discovers and maps the entire infrastructure and application services, breaking through any architectural barriers like Kubernetes, multicloud or serverless workloads, to deliver real-time performance monitoring at one-second intervals, trace every request end-to-end, and profile every piece of custom code.

We believe that for monitoring tools originally designed to be code-focused, such as New Relic and AppDynamics, the presence of complex cloud-native infrastructure components like Kubernetes can create visibility gaps. And because of the constant changes in these environments, manual configuration and monitoring requirements can worsen these gaps. That's why we think the automated full-stack approach of IBM Instana with real-time observability is a better solution.



Without full-stack observability, real-time change detection and contextual understanding of cloud-native applications, DevOps teams are at risk of experiencing performance issues, surprise outages and disruptions to their software pipeline.

Reason 02: IBM Instana captures and stores every trace for every user—at no additional charge



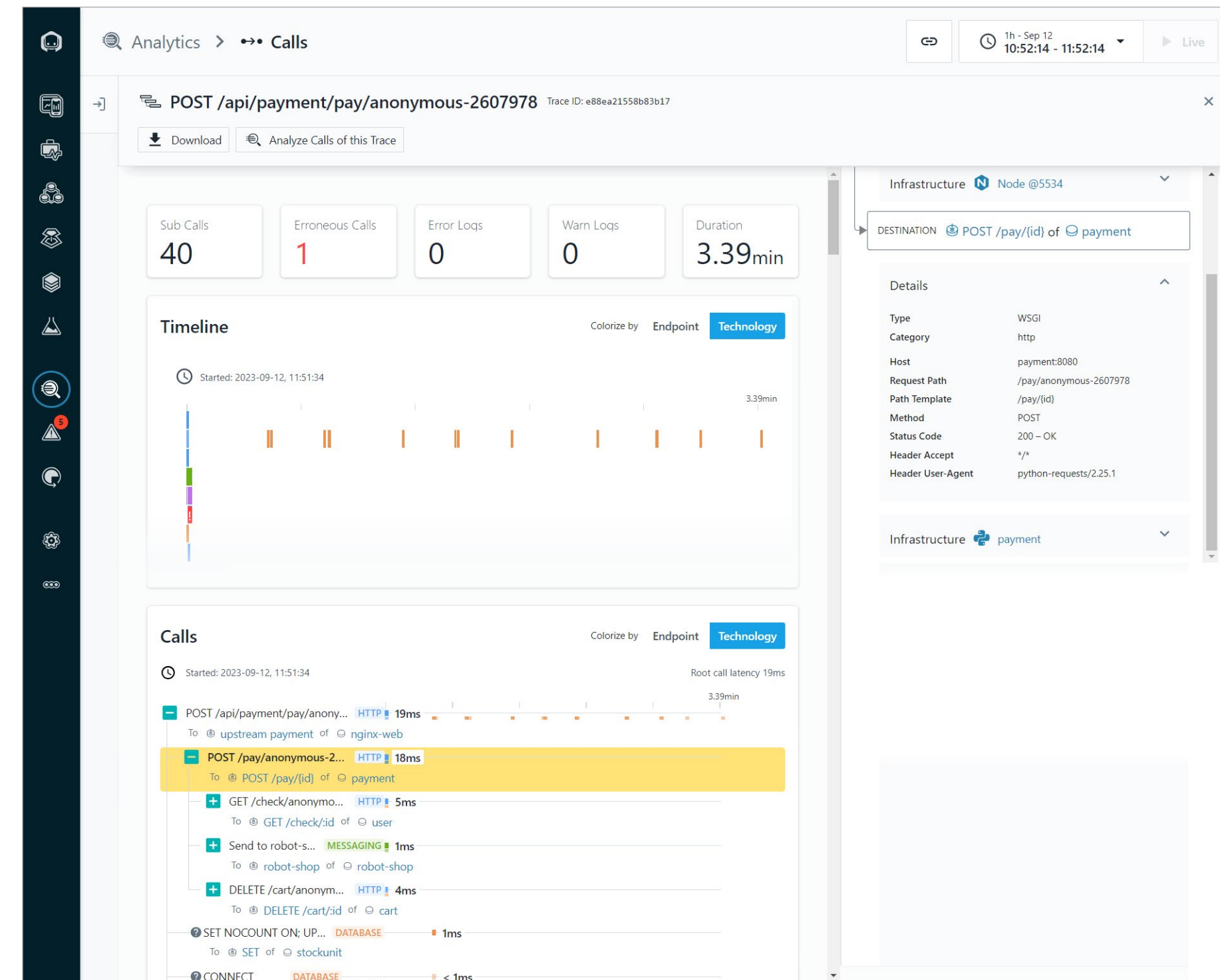
Instana captures an end-to-end distributed trace for every request, for every user—period. This happens automatically out of the box, with one-liner installation and no setup required. If developers have used an OSS tracing API like OpenTracing or Zipkin, IBM Instana not only accepts the trace as input, but integrates the information with the automated traces.

Many legacy monitoring tools sample traces or depending on what infrastructure and platforms a request crosses, truncate the trace to just the pieces visible to the tool. Others trace every request but have a standard operating procedure to perform what's called tail-end sampling—where traces are discarded instead of stored for later use.

IBM Instana tracing capture and storage are included for no additional charge. That helps keep costs predictable ([see Reason 6](#)) and also means you don't have to choose which traces to keep and which ones to throw away. For troubleshooting, all traces are also ingested by IBM Instana's Unbounded Analytics™ deep analysis engine—along with infrastructure, cloud, service, application and profiling data.

There are sometimes options to pay for full trace storage—if you are operating in a North American cloud and are willing to pay the extra licensing costs. But without long-term trace storage available to every user—all the time—for no additional cost, we believe DevOps teams would have to make a tradeoff between full visibility and keeping costs down—and that’s if retaining their traces is an option. It is our belief that sampling traces at any point could lead to skewed data and creates a risk that the exact trace needed to help an end user won’t be available.

New Relic samples every trace by default but it only keeps the one slowest trace per agent per minute. For microservices applications, which are combinations of services that span numerous microservices, this leaves visibility gaps in the telemetry provided to users.



With traces as a cornerstone of modern observability, having every trace is important to analytics, troubleshooting and high-level customer support. If you’re sampling traces, Murphy’s Law almost guarantees that when you need a specific trace, you won’t have it.

Reason 03: IBM Instana automates the entire application monitoring process



IBM Instana automates every aspect of the performance monitoring cycle including application discovery, monitoring configuration, dashboards, alerts and troubleshooting.

IBM Instana breaks through the typical barriers associated with monitoring applications.

- Setup, configuration and ongoing maintenance of monitoring agents
- Operational monitoring setup—dashboards, alerts, incident detection and troubleshooting
- Mapping, change detection and feedback

IBM Instana leverages a single agent, initiating infrastructure monitoring, application performance monitoring, website monitoring, distributed tracing, continuous production profiling, database monitoring and more from a single deployment. IBM Instana can work across all types of environments so that the automated monitoring installation and configuration occur no matter where application components reside or what infrastructure they're running on—even crossing between different clouds and on-prem systems.

By automatically deploying correlated monitoring everywhere within the application infrastructure, IBM Instana delivers immediate value to all stakeholders—Ops, Development, SRE, DevOps, and application business owners—providing the data each needs in a way that makes sense to them.

Often, legacy monitoring tools require manual instrumentation or configuration. In fact, New Relic requires a custom “application” to be deployed to optimize the use of their insights platform. At IBM Instana, we believe that requiring manual instrumentation and configuration—especially coupled with the traditional

application centric focus on code—can lead to longer roll-outs of all monitoring capabilities. That can create a challenge in identifying the interdependencies between application services and infrastructure components since each component requires a different monitoring agent, which in turn requires unique configuration. Additionally, non-automated monitoring setup can require additional continuous human configuration such as alerting thresholds, dashboards and framework interaction.

Dynamic cloud-native and hybrid cloud environments require an automated monitoring solution to keep up with development velocity. The inherent

complexity of these systems also requires automation throughout the typical use cases DevOps teams find while dealing with production application performance.

Not only does IBM Instana capture every performance metric, but it also automates tracing every single request and, for key languages, profiles every process. Regardless of the data type—metric, trace, event, profile—it is all combined by IBM Instana automatically, available for analysis and completely correlated. The result is that whenever a problem occurs, IBM Instana automatically identifies the slow service and component and tags the causal event.

We believe the automated correlated approach provides a more streamlined experience than manually sifting through data from several unique data sources and trying to determine how they’re related. If you’re troubleshooting inside a piece of code and need to reach the infrastructure level, you don’t want to have to open a different workbench and look for the entity you remember from the other screen. That’s a time-consuming task, and you’d probably lose the context of the relationship between the disparate entities.

Reason 04: IBM Instana helps predict issues and service incidents before they occur



If automation is how you get your speed to real-time, predictive alerting is how you take time to the next level. Pick your cliché—slow down time, time travel, see the future—no matter how you like to think about it, even the best monitoring tools still have to wait for a problem to occur before helping you fix it.

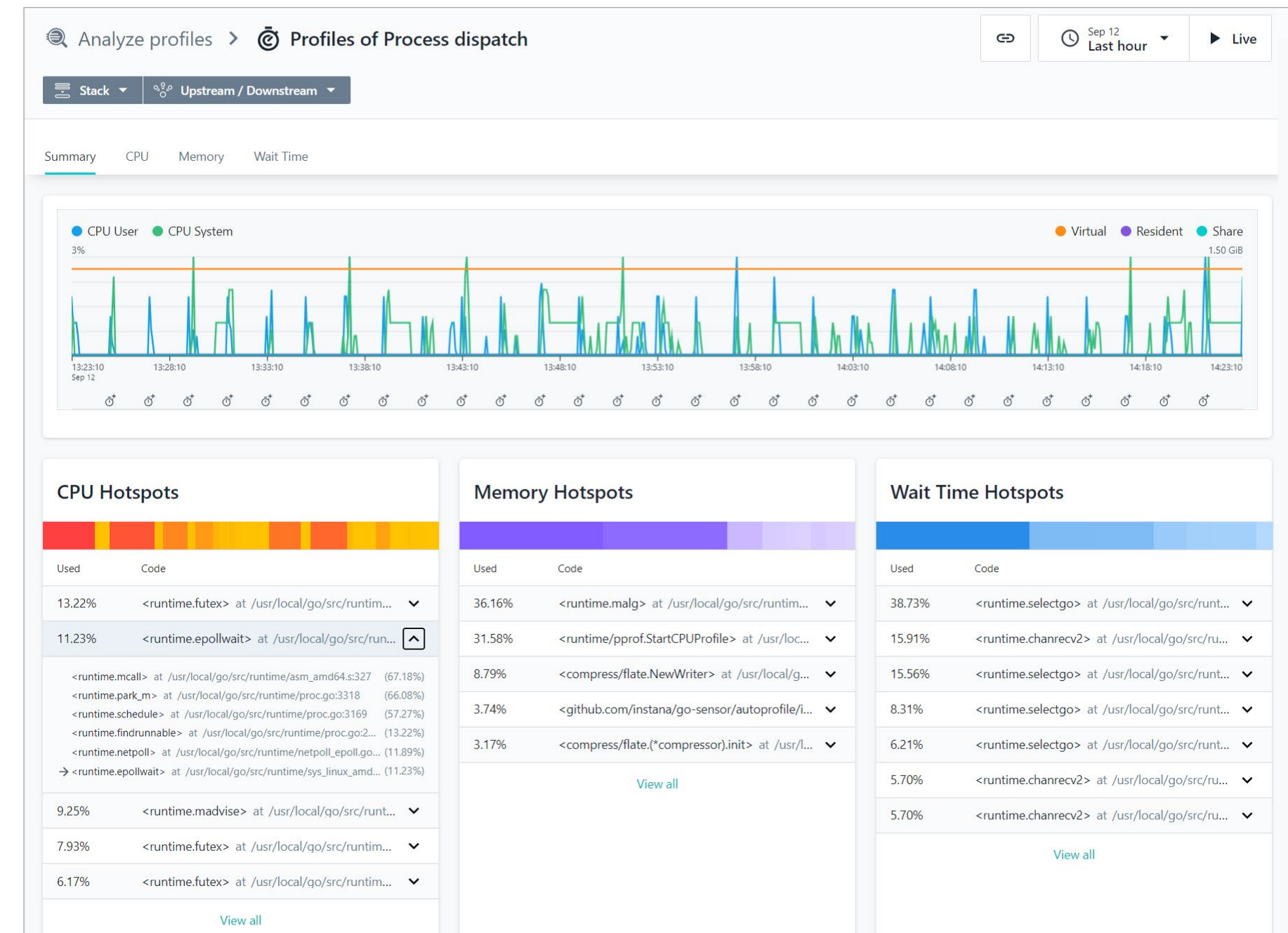
Enter Instana Smart Alerts™.

With Smart Alerts, Instana can help predict when problems will occur. Built on Instana's machine learning engine, the Smart Alerts system automates monitoring for conditions and behaviors that indicate the presence of a problem. This is part of the automatic alerting aspect of Instana discussed in Reason #2.

What sets Smart Alerts apart, though, is that after learning more about your environment (say 7 days of traffic), Instana can identify situations that will potentially lead to that anomaly condition, allowing you to prepare, manage or even correct the situation before it even occurs.

There are many parts of the Instana philosophy at work in Smart Alerts including the Dynamic Graph, machine learning, anomaly detection, single agent monitoring of applications, infrastructure and end users, tiered incident or issue management, and intuitive UI.

Remembering that legacy tools like New Relic were built before the line between applications and infrastructure was blurred, it's difficult for these tools to understand the relationship between disparate pieces of data. In some cases, there may be an available partner AIOps solution for predictive alerting, but that means using yet another tool (installation, configuration, user training, system training and more).



Automating the advanced use cases of observability, such as root cause analysis and advanced analytics, helps reduce the impact of application issues, empowers every team member to troubleshoot problems and allows organizations to bypass costly bridge calls or war rooms.

Reason 05: IBM Instana is the application silo-buster, providing real-time observability data with context



Cloud-native, hybrid cloud and multicloud applications are exponentially more complex than legacy applications. Built on ephemeral containerized environments and typically made up of dozens, hundreds or thousands of microservices, these applications contain a massive number of interdependencies, which are constantly changing.

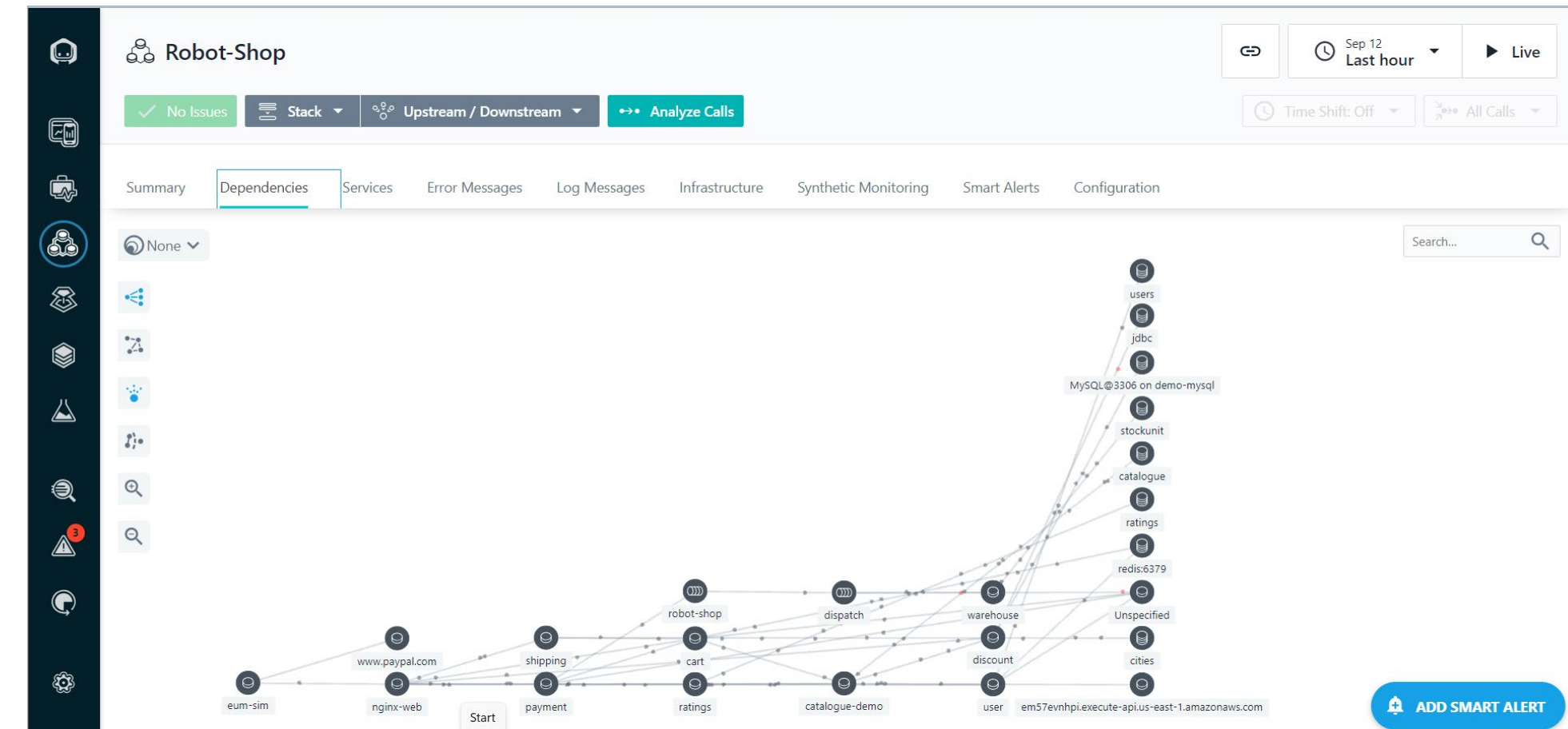
Managing these complex applications effectively requires observability that goes beyond simple measurements—discovering, modeling and mapping dependencies. Instana’s automation drives the gathering of appropriate information, but the platform’s unique Dynamic Graph real-time modeling adds full context to

the mix—all of the time. With the Dynamic Graph, Instana understands how every component, metric, trace and profile is related to infrastructure, cloud, services, applications, and to each other.

We believe that the full context of the application created by the single agent architecture and Dynamic Graph is an easier and more effective way for users to understand what they see, compared to the silos of data created by deploying multiple agent types. If the application architecture and structure aren’t known up front, we believe that silos can lead to confusion and prevent users from solving problems quickly.

For observability, especially in AIOps environments, the ability to understand what the data means depends on the contextual understanding of each piece of information, which also helps any AIOps tooling make better decisions.

In conclusion, New Relic provides 5–15 second granularity to IBM Instana's <1 second. They also fully sample traces out of the box while Instana never samples traces. Instana captures every transaction trace, all the time. New Relic also uses multiple agents for different environments all of which require a degree of manual installation and configuration. Instana's installation is fully automated. IBM now has a fair usage policy putting a data cap. And Instana never charges for users.



IBM Instana provides a complete understanding of all service dependencies. This helps DevOps move between layers and across transaction spans so that they can remediate issues rapidly—before clients are impacted—to help eliminate frustration.

Reason 06: IBM Instana pricing has no surprise costs and is simple, transparent, and all-inclusive



With IBM Instana, pricing is open and simple—you can see it directly on the website—and based on the number of hosts you run. The size of those hosts has no impact. Neither does the number of users, your application load, or storage. IBM Instana licensing also includes infrastructure monitoring, application monitoring, production profiling, and website monitoring, all for one inclusive price.

There are, of course, many different licensing types on the market. For example, according to their website, New Relic licensing costs are based on what is used, not what is being managed—charging for metrics or checks, the number of non-free

users and the amount of stored data. In usage models, the more users you have and the more checks you perform, the more you pay.

In our experience, organizations monitoring cloud-native applications want to make observability and monitoring information available to all application stakeholders. It's not uncommon for customers that migrate from a legacy monitoring tool to IBM Instana to see their user count grow from a dozen users to hundreds or thousands of IBM Instana users.

We believe that a host-based pricing model leads to more predictable expenses, while charging for user seat may lead to some users not having the data they need to properly do their job.

“...We’re looking to grow per-customer spend with this model.”

New Relic Quarterly Earnings Call:
4 August, 2020

\$75 per host / per month / billed annually

Deployment	SaaS or self-hosted (on-prem or cloud)
Users	Unlimited
Supported technologies	200+
Open standards	Prometheus, StatsD, OpenTracing, OpenCensus, Jaeger, W3C Trace Context, DropWizard, and more

Simple, transparent, all-inclusive pricing provides maximum value along with a no-surprises monthly cost. By not charging for usage, storage, or seats, IBM Instana empowers you to apply enterprise observability anywhere you need it.

Conclusion

IBM Instana meets your application performance management and observability needs today and in the future.

One great advantage of IBM Instana's full lifecycle automation is the ease of migration from another monitoring solution, including New Relic. After installing Instana, you will quickly see all services and dependencies across your environment. Between the auto-generated maps—which include infrastructure, containers and services—end-to-end traces and continuous production profiling, Instana goes beyond traditional monitoring solutions, democratizing observability across IT Ops, DevOps, SREs, developers

and IT decision-makers to provide your teams with the data they want and the context they need. Some of the benefits that IBM Instana brings to cloud-native monitoring include:

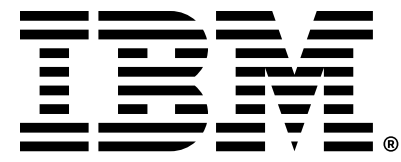
- Automatic infrastructure and application discovery, mapping, monitoring deployment, tracing, profiling, alerting and root cause analysis provide the easiest and fastest path to full observability value
- Full-stack monitoring, tracing and correlation, which work together to provide complete context for services and infrastructure

- Built-in AI and a full analytics engine help drive intelligent actions and predictive alerting, optimizing performance and accelerating application pipelines
- Single pane of glass enables you to monitor hybrid cloud and infrastructure environments

If you want to deliver higher quality, increase your development velocity, and accelerate your CI/CD pipelines, now is the perfect time to add IBM Instana into your operations and development tools.

[Explore IBM Instana](#) →

[Request a quote](#) →



© Copyright IBM Corporation 2024

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2024

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.