

Connect Application Performance to the Network Path

NetBrain correlates application and trace information from Dynatrace with the underlying network paths and devices, so Deep Diagnosis starts with the full picture.

HOW IT WORKS

Build context before the incident, fetch evidence during it. A plugin keeps application dependencies current inside NetBrain, Skills hold the senior engineer's diagnostic steps, and MCP tools pull point-in-time Dynatrace data when Deep Diagnosis needs it.



BEFORE · CONTINUOUS

API Ingest

A plugin queries Dynatrace over REST and writes the application-to-segment dependency graph into an Automation Data Table (ADT). The data renders on Path Browser and is available to Deep Diagnosis as a context layer.



DURING · DIAGNOSTIC

Skills

Action Plans, Network Intents, and Knowledge Documents codify a senior engineer's steps. The agent executes them, compares results to baseline, and logs every run with evidence.



DURING · ON DEMAND

MCP Tool Calls

Deep Diagnosis calls Dynatrace through the Model Context Protocol and pulls only the data the current step requires: the exact-moment-of-failure view, stitched into the root cause chain.

ONE DIAGNOSTIC FLOW

1

API ingest

Plugin pulls Dynatrace traces on the Benchmark schedule. ADT is populated.

2

Path Browser

App dependencies appear on every live path.

3

Alert triggers

A ServiceNow alert opens Deep Diagnosis with the affected app path.

4

Skill executes

Action Plan runs Smart CLI, Intent checks, and an ADT lookup.

5

MCP fetches evidence

Point-in-time Dynatrace trace joins the RCA.

INCLUDED WITH THE INTEGRATION

Three Dynatrace Skills for Deep Diagnosis

Each skill answers one question and hands off rather than overlapping. The agent picks the matching skill from the wording of the request. No DQL knowledge is required.

dynatrace-path-correlation

Which network segment carries an unhealthy application, joining live Dynatrace health to the recorded NetBrain path.

"Why is this application slow and what network segment is involved?"

dynatrace-shared-tier-attribution

When several applications share a host or backend and only some are failing, whether the shared component is broken or one service instance on it.

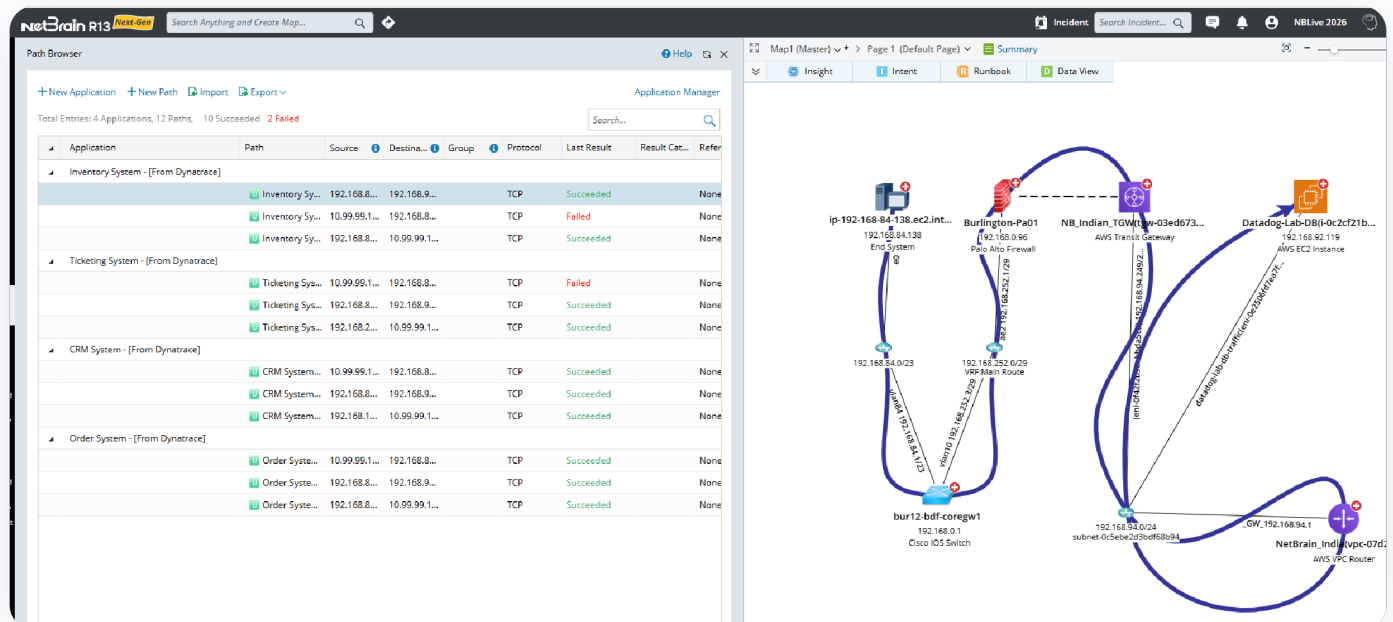
"Why are Inventory and Ticketing both timing out?"

dynatrace-span-data-quality

Whether the span feed is complete enough to support a diagnosis, and what each gap invalidates.

"Is our Dynatrace data complete?"

IN NETBRAIN



Dynatrace-monitored applications in Path Browser, with a path that traverses both the traditional network and AWS Cloud.

PATH AUTOMATION

Application Paths That Maintain Themselves

Each time the plugin retrieves Dynatrace data, it drives the full workflow. Manual Benchmark runs and ADT edits are no longer needed. The resulting mapping feeds Deep Diagnosis, Network Intent, and Map/DataView.

01

Create Applications and Paths

New Application API registers apps and paths in Path Browser/AAM, with no duplicates.

02

Calculate Paths

Batch Calculate Paths API computes real network paths for many apps in one operation.

03

Select in ADT

A condition filter, such as Application Name contains "Dynatrace", includes new apps automatically.

04

Build ADT Mapping

Build ADT API refreshes device and interface-to-application-path relationships and latency.

QUICK SETUP

Two Dynatrace servers

Classic (API token, entities.read) for applications and services. DQL (platform token, storage:spans:read and storage:buckets:read) for source and destination span data.

Automatic ADT creation

The plugin creates the Path AAM, Device Viewer, and Raw Span ADTs on first run. No manual Table Builder setup.

Scheduled path calculation

Paths calculate through a native Benchmark Task on their own schedule, so the plugin run is not blocked.

WITH SERVICENOW

From Incident to Root Cause in One Prompt

A single prompt such as "Troubleshoot INC0013914" starts the investigation. The Deep Diagnosis agent reads your ITSM and observability tools in parallel, then gathers evidence from the network itself.

1

Retrieve the incident

Incident details come from the ServiceNow MCP.

2

Map paths and changes

NetBrain identifies the application paths and related changes, such as an ACL policy change.

3

Correlate Dynatrace alerts

Latency, service degradation, and packet loss are retrieved through the Dynatrace MCP.

4

Gather evidence

CLI commands, automations, and interface and BGP checks run against the live digital twin.

5

Present root cause

Root cause, impacted paths, correlated alerts, and recommended actions.

6

Update ServiceNow

The diagnosis is written back to the incident through MCP.

EXAMPLE RESULT

ACL policy change on a core router is blocking required traffic and degrading the CRM application.

Dynatrace: high latency, service degradation, packet loss on path.
Recommended: review ACL policy on the core router, validate traffic flow, monitor application performance.