

# AI-Directed Troubleshooting for 3-Tier Applications

**cisco** Live !

Eliminate the Guesswork - Let AI Pinpoint the Problem!

Michael Raich  
Product Manager

Gatha Sehgal  
Product Manager

# Cisco Webex App

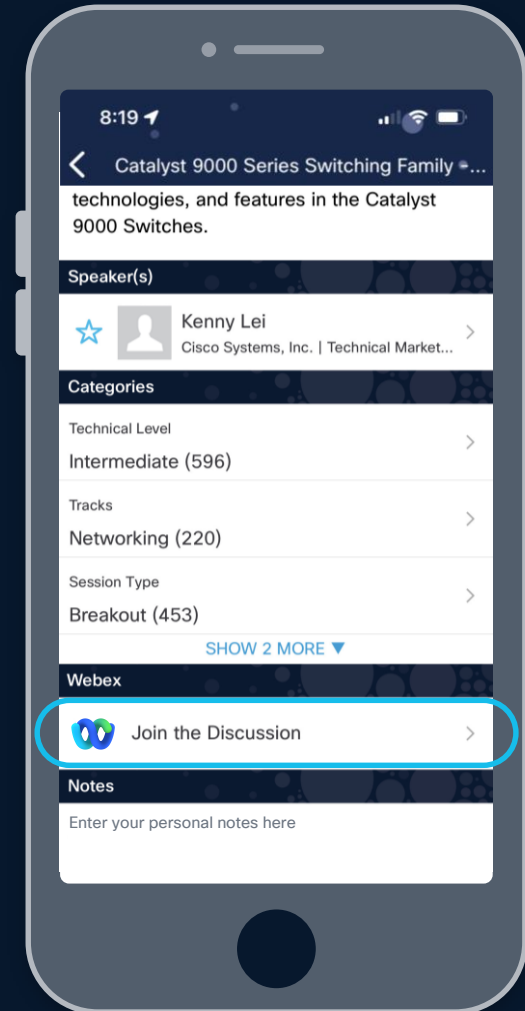
## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

**Webex spaces will be moderated by the speaker until June 13, 2025.**



# Agenda

- 01 **Welcome & Introductions**  
Get to know your speakers
- 02 **The Troubleshooting Challenges**  
Why traditional tools fall short in 3-tier applications
- 03 **AI as a Force Multiplier**  
AI's Impact on Troubleshooting
- 04 **Feature Preview & Demo #1**  
See how AI-Directed Troubleshooting helps pinpoint root causes
- 05 **Feature Preview & Demo #2**  
Walkthrough of AI Insights and how it reduces MTTx
- 06 **Key Takeaways & What's Next**  
How these innovations impact teams
- 07 **Q&A**  
Ask us anything!

# Welcome & Introductions

Get to know your speakers



Gatha Sehgal  
Product Manager



Driving Alerting, Cognition Engine (Powering AI Capabilities), Log Observer Connect and Business IQ (BiQ) areas.



Engineer Turned Product Manager with 7+ years in the observability space.



Passionate about solving complex challenges and thrive at the intersection of technology, data and customer needs.



Always up for Adventure – whether it's sports or road trips!



Michael Raich  
Product Manager



Driving roadmap for AI Troubleshooting and SAP Monitoring areas.



Product Manager with 5 years in the observability space; ex PMO and Tech Partner Ecosystem Lead.



Love to collaborate with partners and customers to 'observe what matters.'

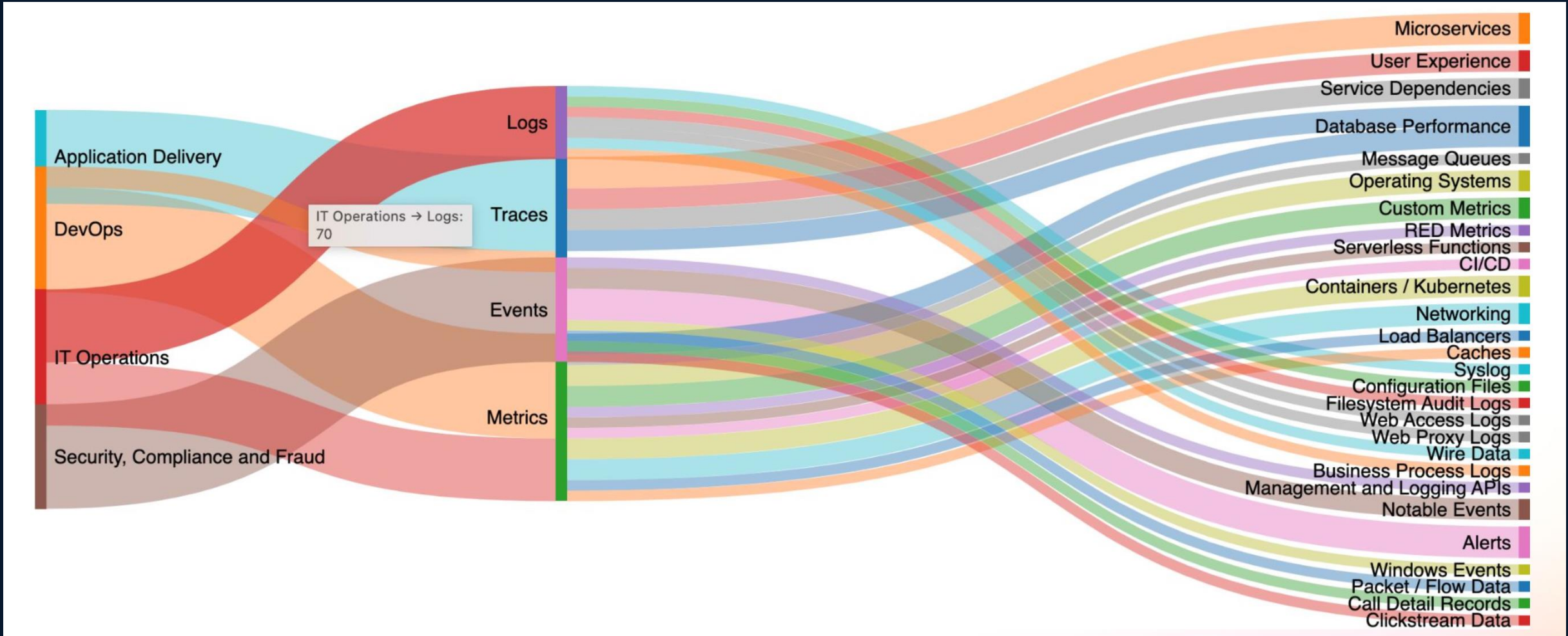


Ready to roll...into sports, music, and road trips! Did I just copy Gatha? 😊



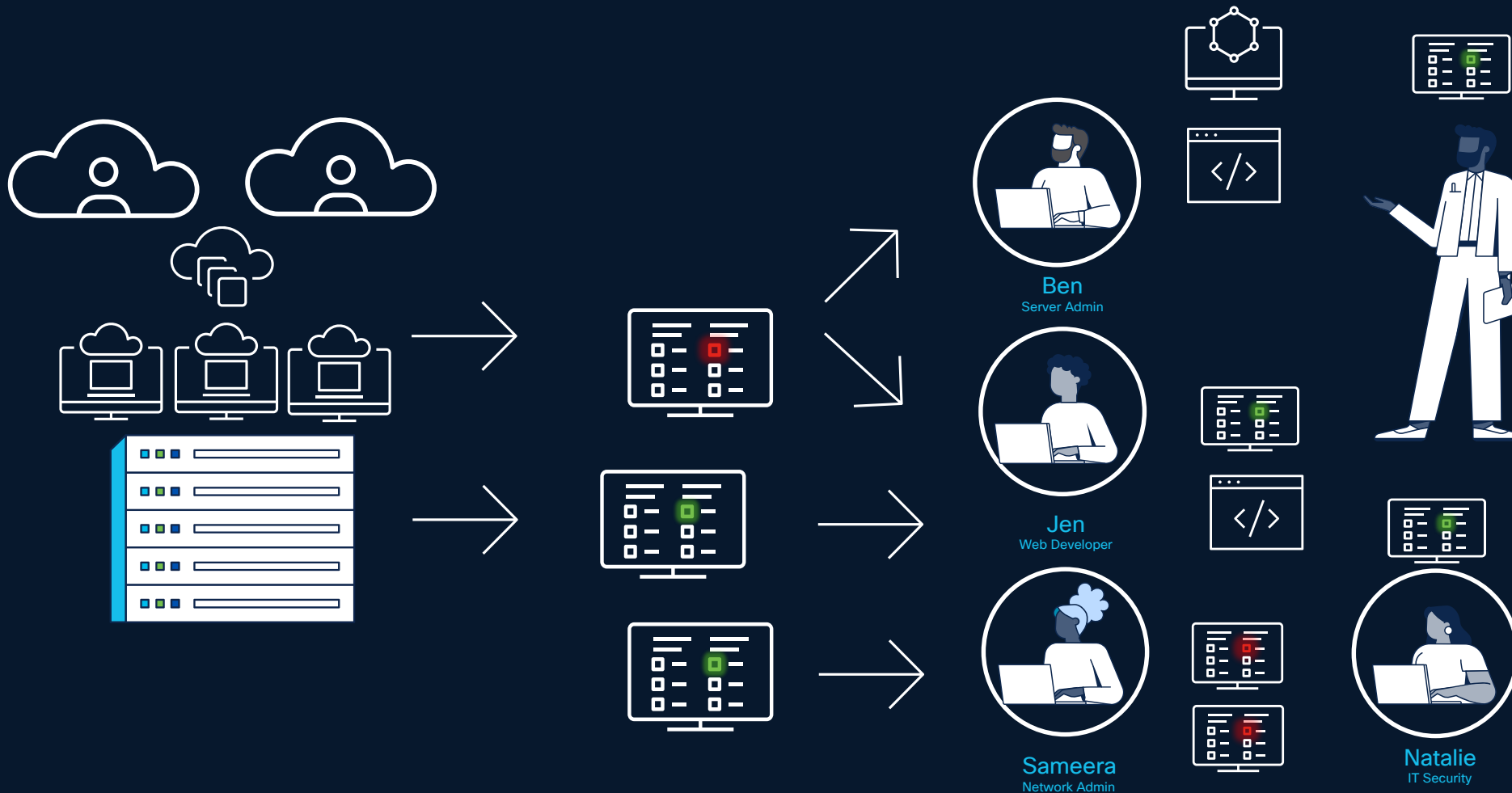
# The Troubleshooting Challenges

# As Tech Stacks and Data Grow, the Big Picture gets Blurry





# Too Many Tools, Too Little Insight



# Data is Moving Faster Than Human Insight can Follow





# The Troubleshooting Challenge

**“Correlating data across the stack requires multiple engineers to spend time on a single issue”**



More Stacks & Data → Less Clarity



Too Many Tools, Too Little Insight



Data Outpaces Humans Insights

# AI in Troubleshooting: Why Now?



# AI's Impact on Troubleshooting

**67%**

Faster RCA

**70%**

Faster MTTD

**90%**

Downtime Reduction



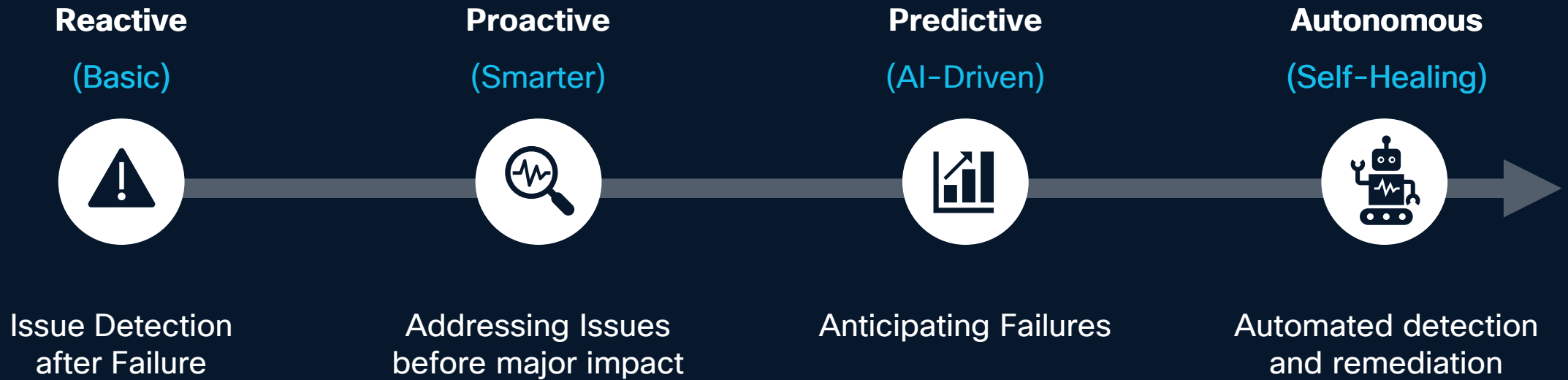
The background of the slide is a dark blue field filled with dynamic, flowing light streaks. These streaks are primarily in shades of bright blue and cyan, with some warmer orange and pinkish tones visible in the upper right quadrant. The lines are curved and layered, creating a sense of depth and movement, reminiscent of light trails or data flow in a digital environment.

**Where are you in your  
Observability Journey?**



# The Evolution of Monitoring and Observability

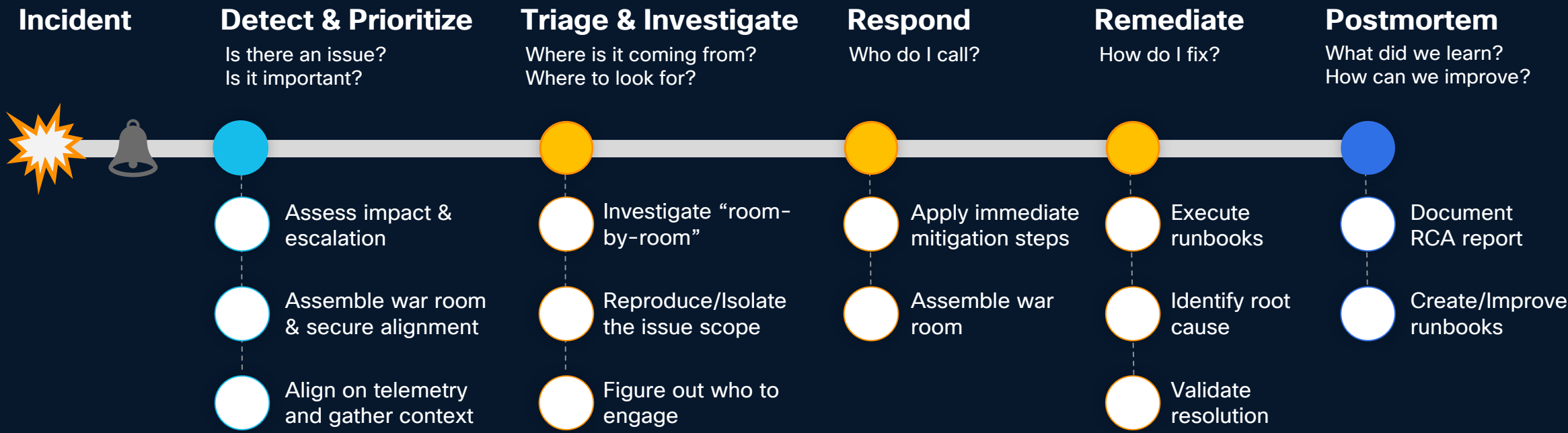
From Reactive to Autonomous: Tracing the Journey to AI-Directed Troubleshooting



# Where AI Fits in your troubleshooting Journey

# The Incident Management Workflow

The Workflow That AI is About to Transform



# What's Available Today: AI/ML in Splunk AppDynamics

Troubleshoot Smarter and Faster with our current AI/ML Capabilities



## Dynamic Baselines

Baseline applications normal behavior every hour and account for seasonality.



## Anomaly Detection

Detect anomalies across Business Transactions, Browser & Mobile Applications, Infrastructure and Databases.



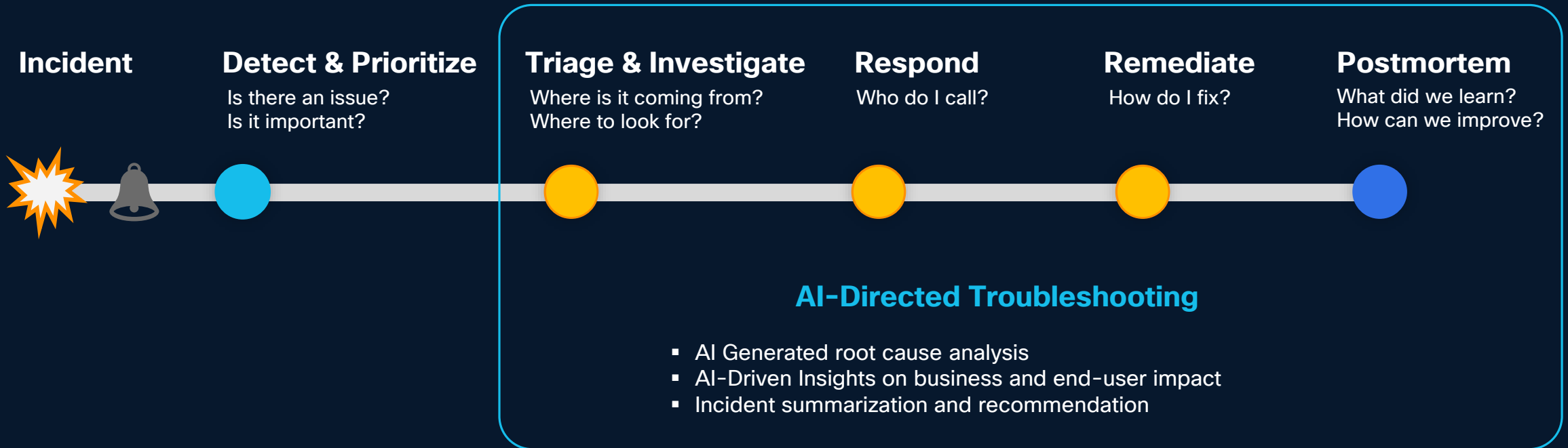
## Suspected Cause

Pinpoint the Top Suspected Cause behind the detected anomalies.



# Rethink Troubleshooting in the Age of AI

Let AI surface causes and suggest next steps – before your team even asks.



# AI-Directed Troubleshooting for Health Rule Violations

# The Event triggering the AI-Directed Troubleshooting

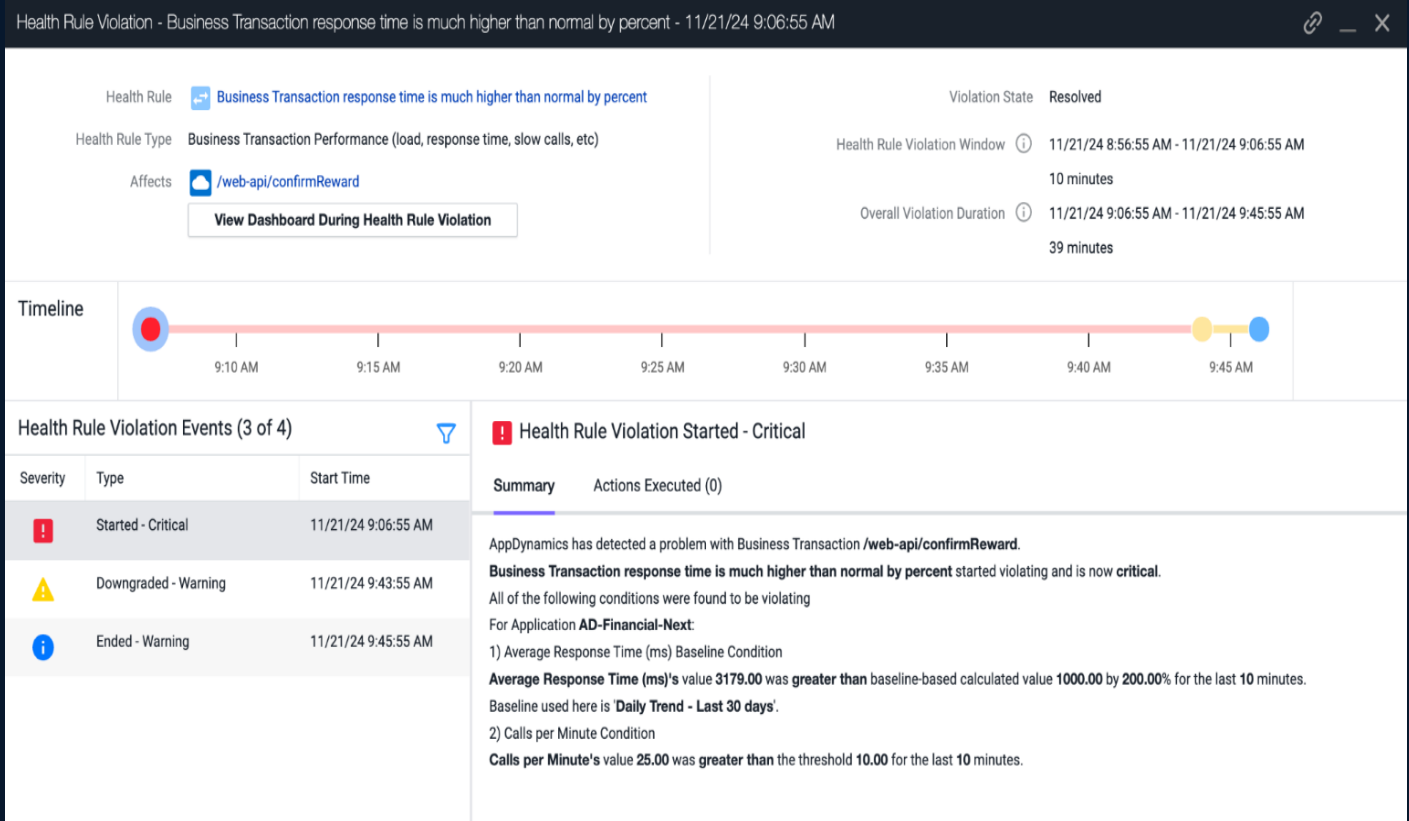
Outcome: Reduced MTTR with AI Driven Suspected Root Cause Analysis

Anomaly Detection and Health Rules complement each other

	Anomaly Detection	Health Rules
How it works	Uses Machine Learning to discover the normal ranges of key Business Transaction metrics and alerts you when these metrics deviate significantly from expected values.	Applies logical conditions that one or more metrics must satisfy. They are perfect for capturing clear-cut logic of SLAs; as well as complex conditional expression.
Configuration	No configuration except when you want to limit Anomaly alerting.	Some default sets provided by AppDynamics, but generally manually configured as desired, including Time Periods, Trends, and schedules.
Events	An Anomaly is a series of Anomaly events.	A Violation is a series of Health Rule violating events.
Entity Coverage	Anomalies are associated with Business Transactions.	Health Rules can apply to any entity.

# AppD Troubleshooting Journey for Health Rule Violations

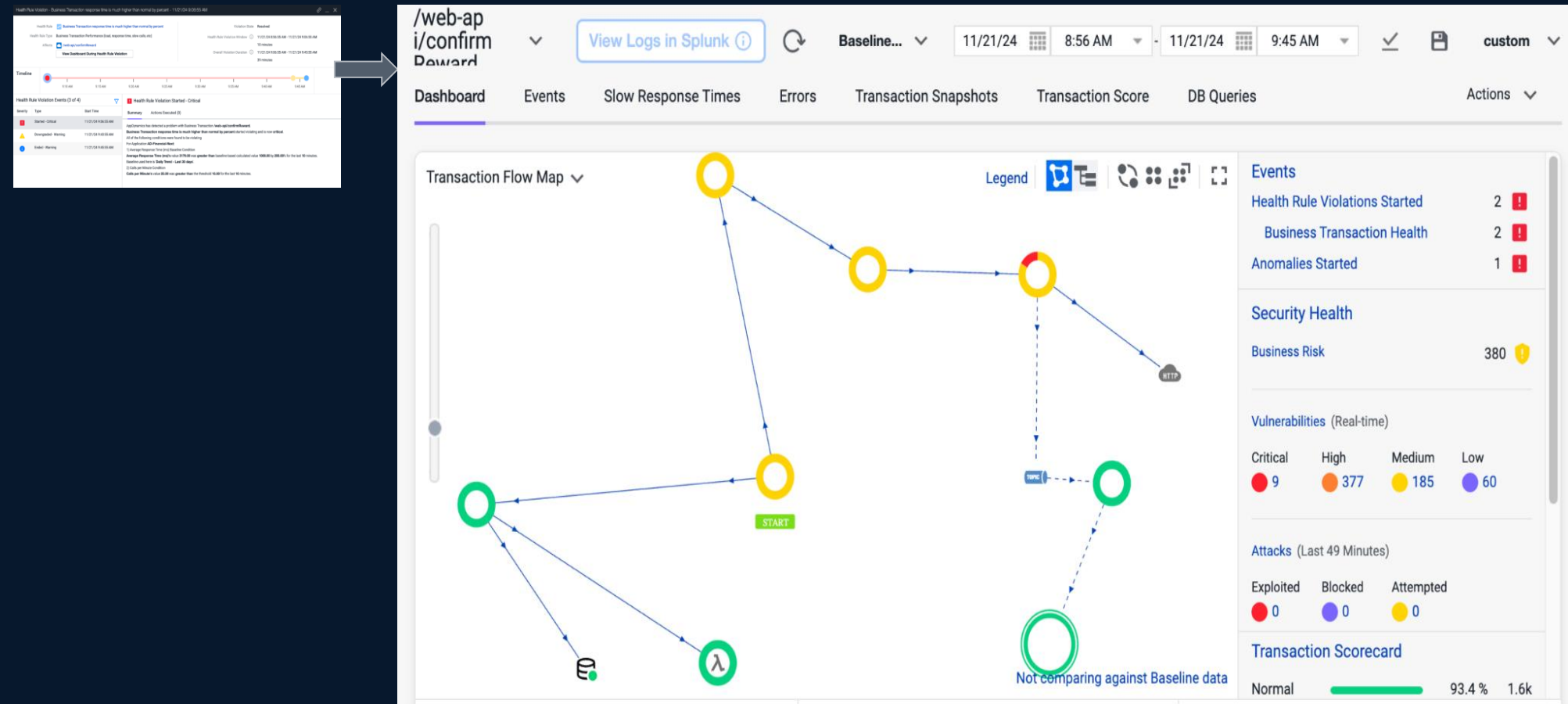
## Detect and Prioritize





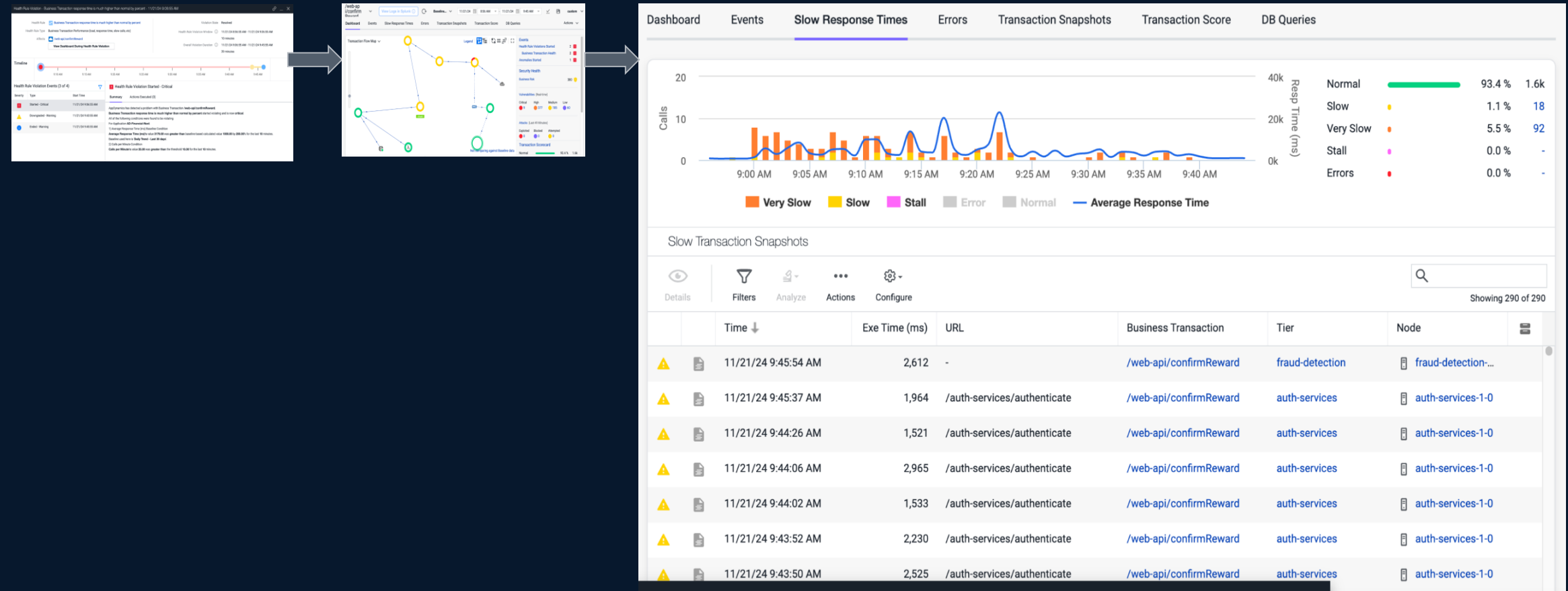
# AppD Troubleshooting Journey for Health Rule Violations

Triage: where is it from?



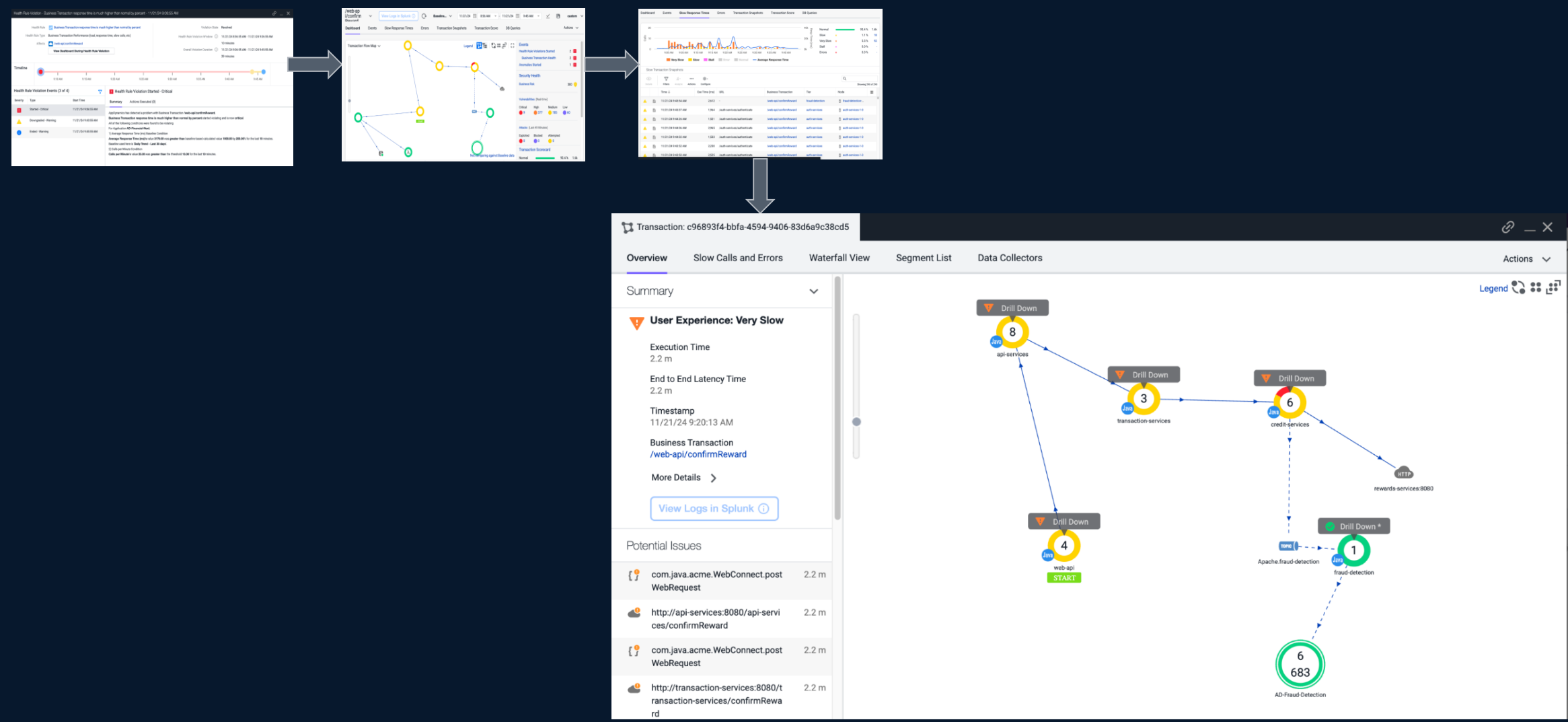
# AppD Troubleshooting Journey for Health Rule Violations

Investigate: where to look for?



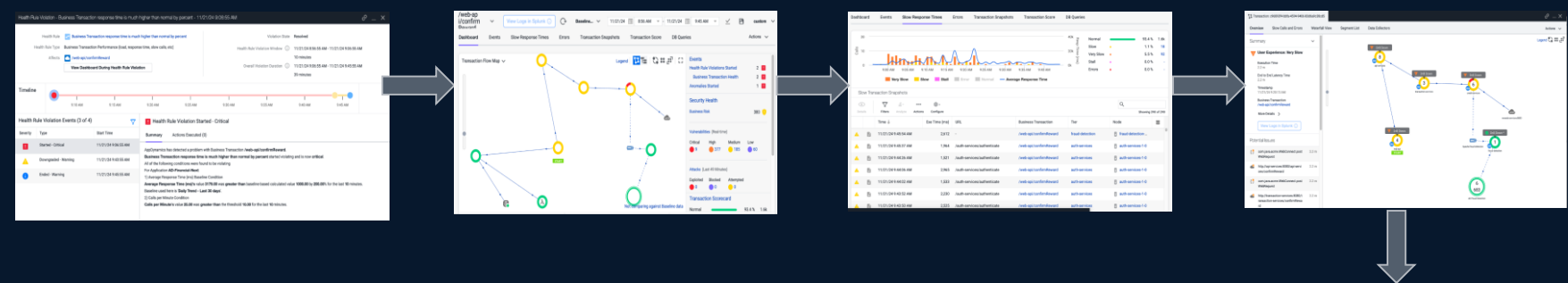
# AppD Troubleshooting Journey for Health Rule Violations

Investigate: where to look for? And more.



# AppD Troubleshooting Journey for Health Rule Violations

Investigate: where to look for? And more. And more.



Overview Partial Call Graph Slow Calls & Errors DB & Remote Service Calls Server Network More Actions				
Execution Time 2.2 m Wait Time 0 ms Block Time 0 ms Node web-api-Node--10 Timestamp 11/21/24 9:20:13 AM This is a Partial Call Graph				
Details Filters Set Root Reset Root Export				
Showing 10 of 10				
Name	Time (ms)	Percent %	Thread State	Exit Calls / Threads *
java.lang.Thread:run:748	0 ms (self)	0%		
HTTPServlet:service:742	0 ms (self)	0%		
HTTPServlet:service:661	0 ms (self)	0%		
Servlet - dispatcherServlet.doService:925	0 ms (self)	0%		
Servlet - dispatcherServlet.doDispatch:991	0 ms (self)	0%		
...	0 ms (self)	0%		
...	0 ms (self)	0%		
Spring Bean - webApiController.confirmReward:130	0 ms (self)	0%		
com.java.acme.WebConnect.postWebRequest:83	0 ms (self)	0%		
com.java.acme.WebConnect.postWebRequest:126	130,387 ms (...)	100%		HTTP



# AppD Troubleshooting Journey for Health Rule Violations

Investigate: where to look for? And more. And more. And more.

Health Rule Violation: Business Transaction response time is much higher than normal (last 10 minutes)

Health Rule Violation Details: Critical

Summary: AppD has detected a problem with Business Transaction response time. The response time is much higher than normal (last 10 minutes) and is not within the expected range.

Transaction Flow Map

Transaction Details

Step	Start Time	End Time	URL	Method	Status	Response Time (ms)	Response Size (bytes)
1	1732198813746	1732198813746	GET /api-services/confirmReward	GET	200	130386	130386
2	1732198813746	1732198813746	POST /api-services/confirmReward	POST	200	130386	130386
3	1732198813746	1732198813746	GET /api-services/confirmReward	GET	200	130386	130386
4	1732198813746	1732198813746	POST /api-services/confirmReward	POST	200	130386	130386
5	1732198813746	1732198813746	GET /api-services/confirmReward	GET	200	130386	130386
6	1732198813746	1732198813746	POST /api-services/confirmReward	POST	200	130386	130386
7	1732198813746	1732198813746	GET /api-services/confirmReward	GET	200	130386	130386
8	1732198813746	1732198813746	POST /api-services/confirmReward	POST	200	130386	130386
9	1732198813746	1732198813746	GET /api-services/confirmReward	GET	200	130386	130386
10	1732198813746	1732198813746	POST /api-services/confirmReward	POST	200	130386	130386

Transaction Details

Self Time: 130,387ms (100%)

Total Time: 130,387ms (100%)

Details: Block: 0 ms, Wait: 0 ms

Exit Calls

Type	Details	Count	Time (ms)	% Time	From	To
HTTP	http://api-services:8080/api-services/confirmRe...	1	130386	100%	web-api	api-services

HTTP Exit Call

Time: 130,386ms

From: web-api

To: api-services

Details: http://api-services:8080/api-services/confirmReward

Properties

Start Time: 1732198813746

postWebRequest: 126

Name: com.java.acme.WebConnect:postWebRequest

Type: POJO

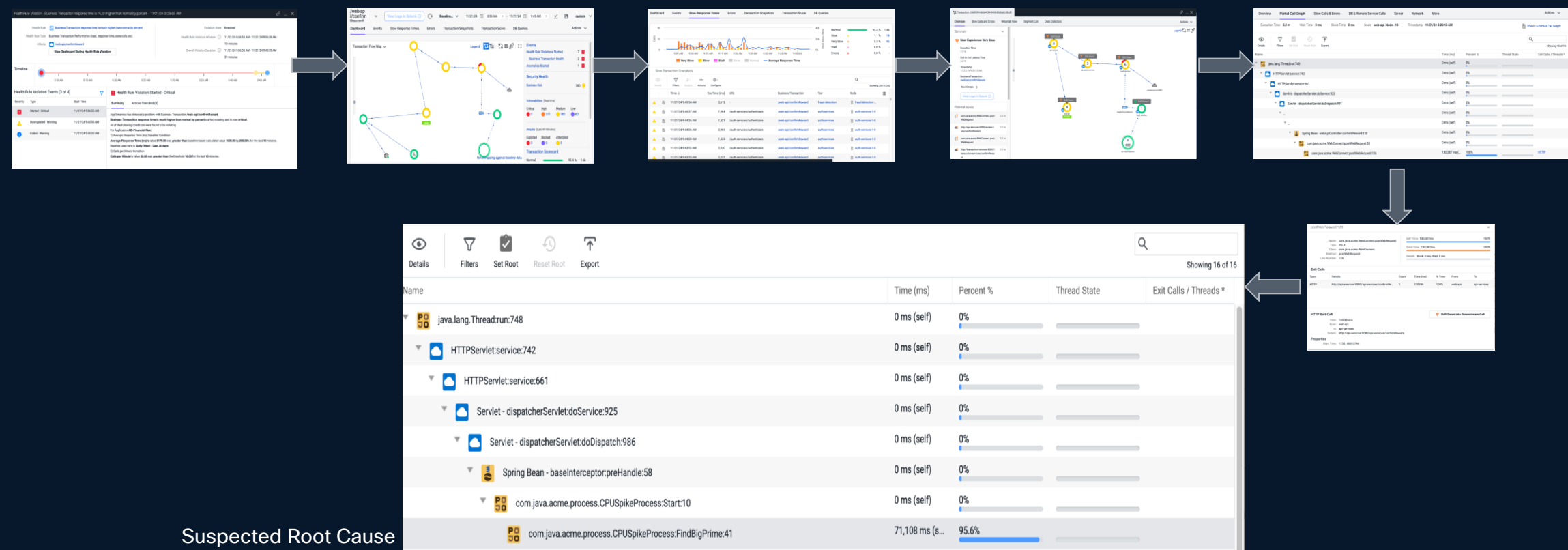
Class: com.java.acme.WebConnect

Method: postWebRequest

Line Number: 126

# AppD Troubleshooting Journey for Health Rule Violations

Investigate: where to look for? And more. And more. And more. And more.



# New: AppD Troubleshooting Journey for Health Rule Violations

## Detect and Prioritize

AI Root Cause Analysis: Health Rule Violation - Business Transaction Health - 04/24/25 12:41:55 PM

Violation Details

Health Rule

Business Transaction Health

View Dashboard During Health Rule Violation

Health Rule Type

Business Transaction Performance (load, response time, slow calls, etc)

Affects

/payments/1232

The health rule violation occurred in the 'payment-service' application component, specifically affecting the '/payments/1232' business transaction. The issue was detected between '04/24/25 03:26:55 PM' and '04/24/25 03:42:40 PM', with the severity escalating to 'CRITICAL' at '04/24/25 03:41:55 PM'. The violation was triggered by performance degradation in key metrics, indicating potential bottlenecks in transaction processing.

Violated Metrics:

Average Response Time (ms): Observed value '106.00' exceeded the threshold '100.00' for the last 15 minutes.

Calls per Minute: Observed value '51.00' exceeded the threshold '1.00' for the last 15 minutes.

The violation is classified as 'CRITICAL', suggesting significant performance impact on the '/payments/1232' transaction. The issue persisted for 15 minutes, with no indication of resolution or downgrade during the monitored period. Immediate investigation into transaction load and response time bottlenecks is recommended to prevent further degradation.

Suspected Root Causes

Violation Events

How are these ranked?

Transaction-Level Bottleneck Identified

A delay in execution was observed in the 'payment-service' application component, specifically affecting the '/payments/1232' transaction. Key delays include 5.598 seconds in 'EpoSelector::select' and 931 milliseconds in '(request)'. These delays contributed to degraded user experience, with multiple nodes reporting 'VERY\_SLOW' performance. The issue is classified as a 'TIER'-level bottleneck, indicating potential inefficiencies in transaction processing within the application tier.

JVM and Hardware Analysis Unavailable

Analysis for JVM and hardware metrics could not be retrieved due to errors in fetching deviating node metrics data. This limits further insights into potential infrastructure-level causes.

Summary

The primary issue lies at the transaction level, with significant delays in execution impacting response times and user experience. While the transaction bottleneck is evident, the absence of JVM and hardware metrics restricts a comprehensive root cause analysis. Further investigation into application-tier processing and supporting infrastructure is recommended.

Sources

1. Snapshot: 7159475b97a540bf96e9d29aa354c6ac

2. Snapshot: eb38483663b0476b9b3593d0a43c5dbf

3. Snapshot: 08e6043625a84c3ba2e6654f13d0ae59

4. Snapshot: 08e6043625a84c3ba2e6654f13d0ae59

5. Snapshot: b4fc3aeb1df346219af8c633be7d94bc

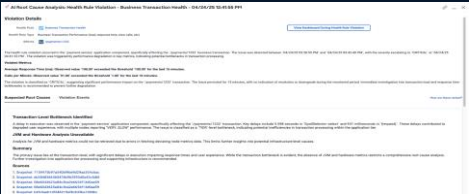
© 2025 Cisco and/or its affiliates. All rights reserved.

BRKOB5-1023

27

# New: AppD Troubleshooting Journey for Health Rule Violations

## Next: 1-click RCA

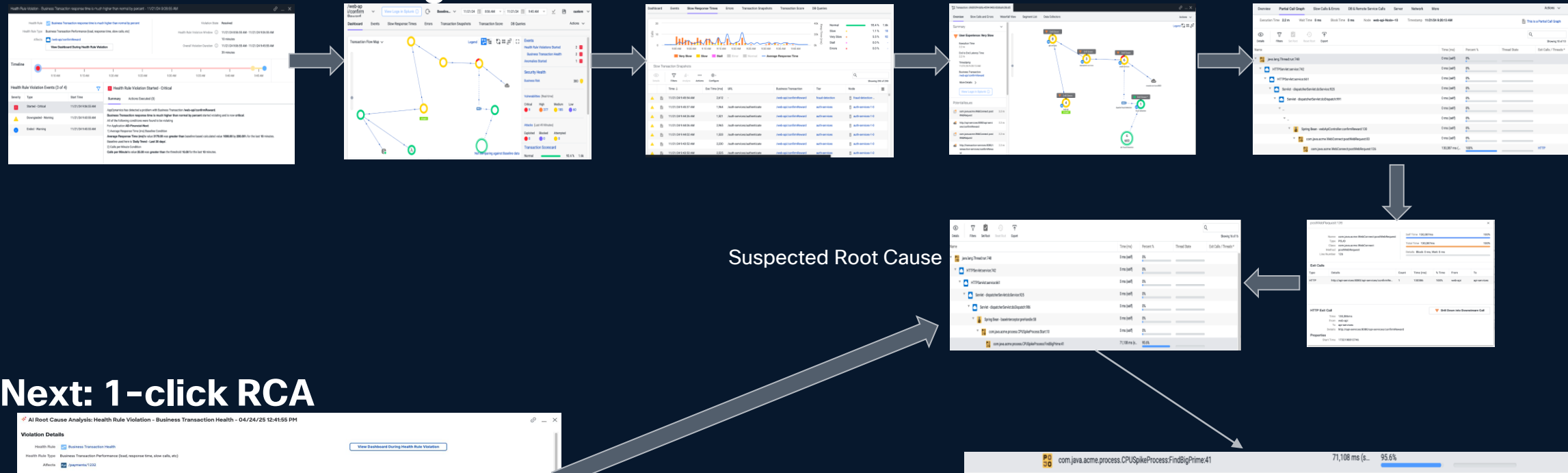


Details   Filters   Set Root   Reset Root   Export					Showing 16 of 16	
Name	Time (ms)	Percent %	Thread State	Exit Calls / Threads *		
java.lang.Thread.run:748	0 ms (self)	0%				
HTTPServlet.service:742	0 ms (self)	0%				
HTTPServlet.service:661	0 ms (self)	0%				
Servlet - dispatcherServlet.doService:925	0 ms (self)	0%				
Servlet - dispatcherServlet.doDispatch:986	0 ms (self)	0%				
Spring Bean - baseInterceptor.preHandle:58	0 ms (self)	0%				
com.java.acme.process.CPUSpikeProcess.Start:10	0 ms (self)	0%				
com.java.acme.process.CPUSpikeProcess.FindBigPrime:41	71,108 ms (s...	95.6%				



# Basic AppD Troubleshooting Journey for Health Rule Violations

## Now: Detect and Investigate



## Next: 1-click RCA

**AI Root Cause Analysis: Health Rule Violation - Business Transaction Health - 04/24/25 12:41:55 PM**

**Violation Details**

Health Rule: Business Transaction Health  
Health Rule Type: Business Transaction Performance (slow, response time, slow calls, etc)  
Alert: [Critical] [View Dashboard During Health Rule Violation]

The health rule violation occurred in the 'payment-service' application component, specifically affecting the 'payments/1232' business transaction. The issue was detected between '04/24/25 03:26:55 PM' and '04/24/25 03:42:40 PM', with the severity escalating to 'CRITICAL' at '04/24/25 03:41:55 PM'. The violation was triggered by performance degradation in key metrics, indicating potential bottlenecks in transaction processing.

**Violated Metrics**

Average Response Time (ms): Observed value '100.00' exceeded the threshold '100.00' for the last 15 minutes.  
Calls per Minute: Observed value '31.40' exceeded the threshold '1.00' for the last 15 minutes.

The violation is classified as 'CRITICAL', suggesting significant performance impact on the 'payments/1232' transaction. The issue persisted for 15 minutes, with no indication of resolution or downgrade during the monitored period. Immediate investigation into transaction load and response time bottlenecks is recommended to prevent further degradation.

**Suspected Root Causes**

**Violation Events**

**Transaction-Level Bottleneck Identified**

A delay in execution was observed in the 'payment-service' application component, specifically affecting the 'payments/1232' transaction. Key delays include 5.598 seconds in 'EpicSelector:series' and 531 milliseconds in 'Inquiries'. These delays contributed to degraded user experience, with multiple nodes reporting 'VERY\_BAD' performance. The issue is classified as a 'TIER' level bottleneck, indicating potential inefficiencies in transaction processing within the application tier.

**JVM and Hardware Analysis Unavailable**

Analysis for JVM and hardware metrics could not be retrieved due to errors in fetching deviating node metrics data. This limits further insights into potential infrastructure-level causes.

**Summary**

The primary issue lies at the transaction level, with significant delays in execution impacting response times and user experience. While the transaction bottleneck is evident, the absence of JVM and hardware metrics restricts a comprehensive root cause analysis. Further investigation into application-tier processing and supporting infrastructure is recommended.

**Sources**

- Snapshot: 7159472671654026f6e9d29a354dc6
- Snapshot: d038485843804768593990d45c5d6f
- Snapshot: d06640423a84c3b2d46454f13d5a09
- Snapshot: d06640423a84c3b2d46454f13d5a09
- Snapshot: 84015a6b10f160317e4f6b13b0e79f6c

# AI-Directed Troubleshooting for Health Rule Violations

Reduce MTTR and supercharge RCA with Generative AI capabilities



## Faster Investigations

1-click RCA; more context on your incidents; guided troubleshooting



## Insight-driven decision making

Surface and summarize suspected root cause(s) for Health Rule Violations



## Lower the learning curve

Remove knowledge barriers; Democratize observability

Health Rule Violation - Business Transaction Slow User Experience - 06/05/25 5:04:55 AM - 06/05/25 6:05:55 AM

Summary | AI-generated

The health rule violation pertains to the "Inventory Admin" business transaction within the "Inventory-Admin" application component of "AD-Ecommerce." The issue, categorized as "Business Transaction Slow User Experience," was flagged as critical from 06/05/25 08:04:55 AM to 06/05/25 09:05:55 AM. The violation is linked to a high percentage of slow transactions and sustained call activity exceeding defined thresholds.

**Violated Metrics:**

**Slow Transaction Percentage:**

- Threshold: >5.00%
- Observed Values: 10.00% (08:04:55 AM - 08:34:55 AM), 17.10% (08:34:55 AM - 09:04:55 AM), 11.80% (09:04:55 AM - 09:05:55 AM)

**Calls per Minute:**

- Threshold: >0.00
- Observed Values: 10.00 (08:04:55 AM - 08:34:55 AM), 4.00 (08:34:55 AM - 09:04:55 AM), 1.00 (09:04:55 AM - 09:05:55 AM)

The violation remained critical throughout the monitoring period, with no signs of improvement or downgrade. The slow transaction percentage consistently exceeded the threshold, peaking at 17.10%, while call activity persisted above the minimum threshold. Immediate investigation into transaction performance and call volume is recommended to mitigate the issue.

Suspected Root Causes

Violation Events

How are these ranked?

Remote Backend Latency Impacting Transactions

The analysis identifies a remote backend issue involving "log4shell:8080" as the primary cause. Transaction snapshots reveal execution times of 11.021 s and 11.019 s on the "ecom-inventory-admin-1" node, leading to a "SLOW" user experience classification. The backend interaction, specifically the query "http://log4shell:8080/search," is a key contributor to the observed delays. This latency likely exacerbates the high percentage of slow transactions (peaking at 17.10%) and impacts response time SLAs for the "Inventory Admin" business transaction.

**Sources**

- Snapshot: 8d7e727f-dfb8-47d1-8174-9e6b95c63434
- Snapshot: ca768398-94ae-498f-85e6-fc4f87c17758
- Snapshot: dfb5ef86-c9e2-4b92-9495-56b2f891da26

Inter-Tier Latency Between Inventory-Admin and Inventory-Services

The suspected cause of the issue is identified as an inter-tier latency anomaly between the "Inventory-Admin" and "Inventory-Services" components. Transaction execution times on the "ecom-inventory-admin-1" node consistently exceeded 11 seconds (e.g., 11.049 s, 11.025 s), resulting in a "Slow" user experience classification. This latency likely contributed to the observed high percentage of slow transactions, peaking at 17.10%. The anomaly is linked to the "Inventory Admin" business transaction, with a specific query to "http://inventory-svc:8080/inventory/stock?itemId=1234" being a potential bottleneck. Further investigation into the inter-tier communication and service dependencies is recommended to address this performance degradation.



# Demonstration: AI Directed Troubleshooting for Health Rule Violations



# AI-Driven Root Cause Analysis & Recommendations



# AI-Driven Root Cause Analysis & Recommendations

Pinpoint the root cause of anomalies and reduce MTTR with guided next steps



## Concise AI Summary

Receive AI generated summary that saves times and helps you focus on what matters most.



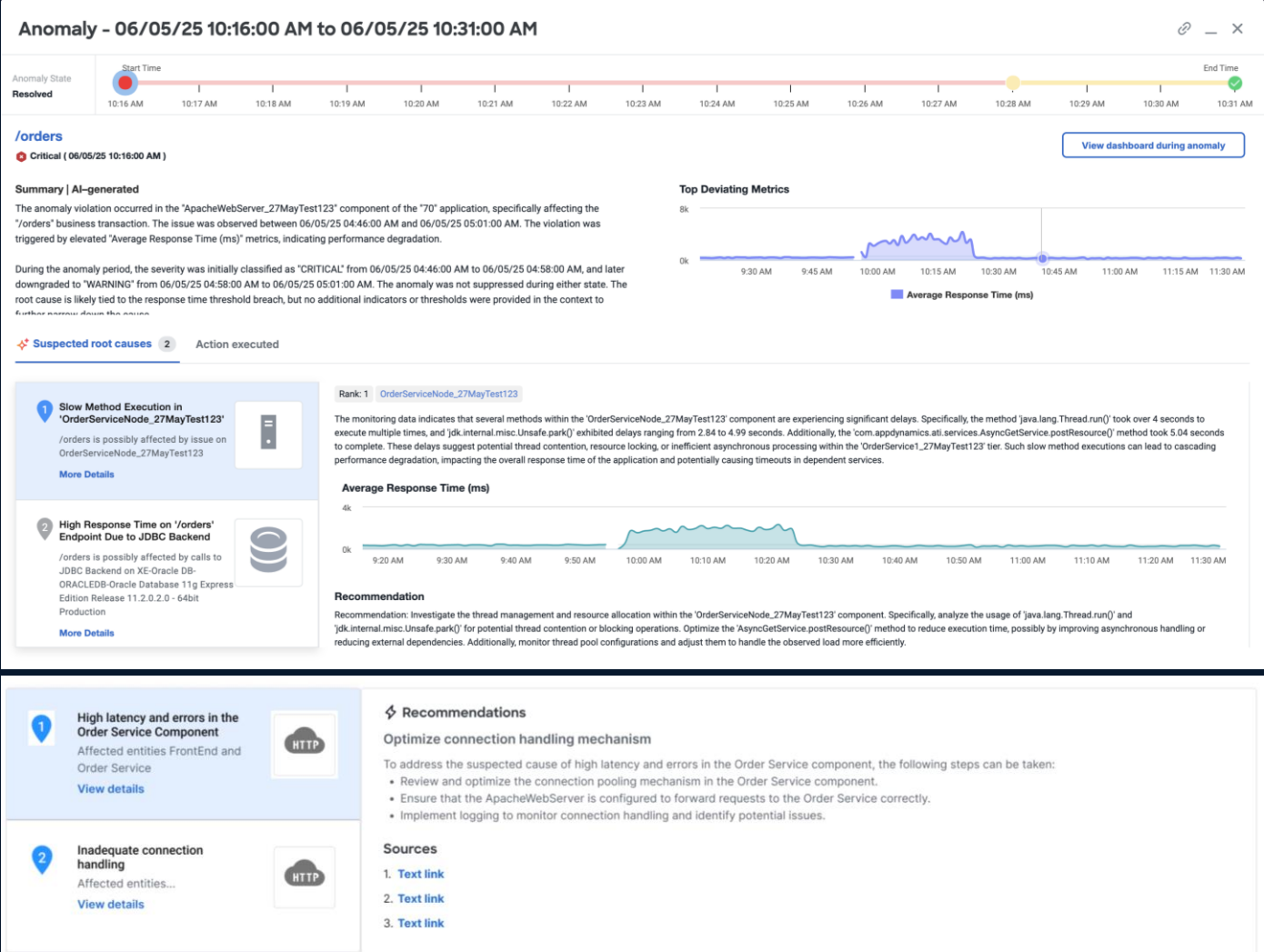
## Root Cause Discovery Made Simple

Identify suspected causes with ease, empowering faster, data-driven decisions.



## Actionable Next Steps

Get relevant recommendations and sources to guide your next steps with confidence.



# Demonstration:

## Anomaly Detection 2.0: AI-Driven Root Cause Analysis & Recommendations

- ☰

Main Menu

Applications

>
- 🔗

Applications

SangrahApp\_27May...

>
- 📊

Application Dashboard
- 🔄

Business Transactions
- 🔗

Service Endpoints
- 🔗

Tiers & Nodes
- 📁

Servers
- 📁

Containers
- 📁

Database Calls
- 🔗

Remote Services
- 🔍

Troubleshoot

>
- ⋮

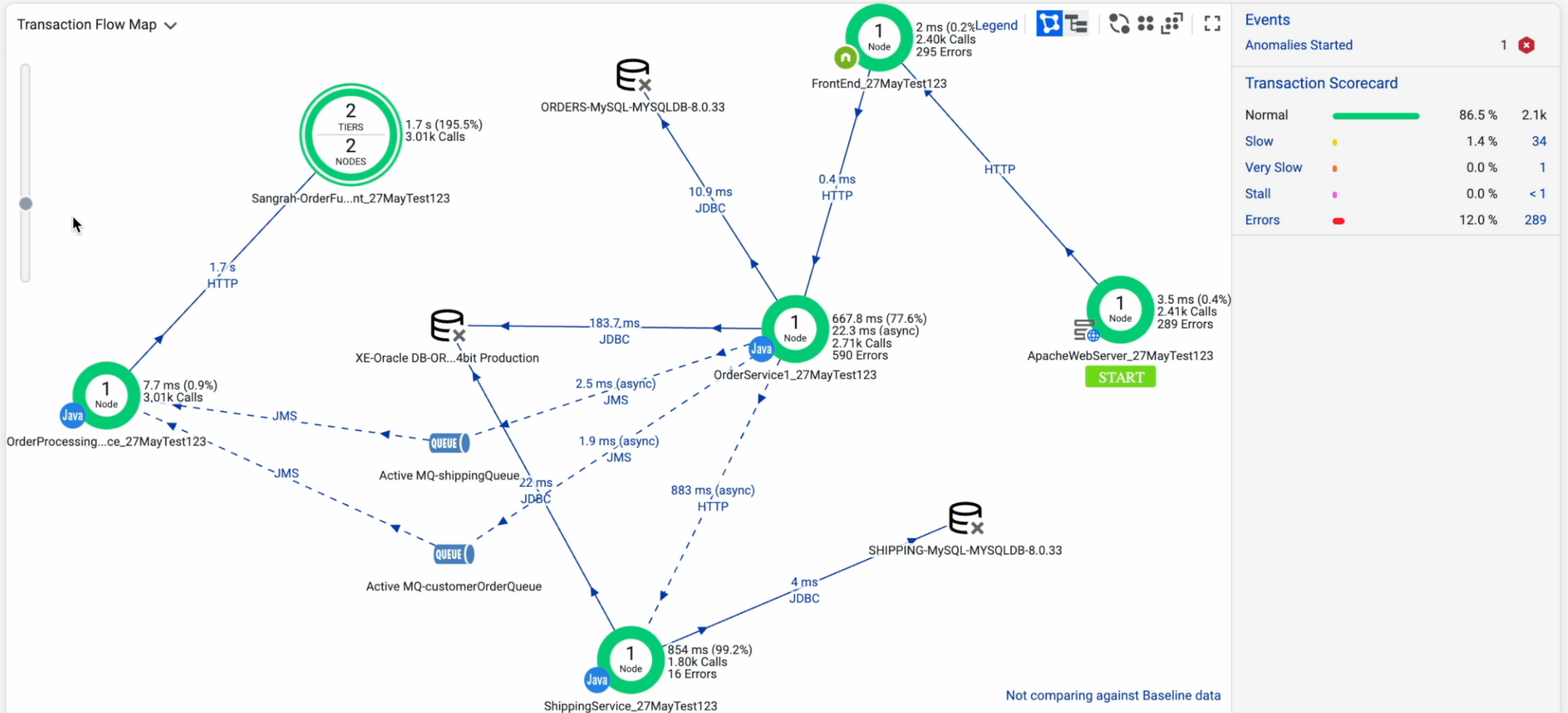
More

>
- 🔔

Alert & Respond
- 📊

Metric Browser
- 🔧

Configuration



Events

Anomalies Started 1

Transaction Scorecard

Normal	86.5 %	2.1k
Slow	1.4 %	34
Very Slow	0.0 %	1
Stall	0.0 %	< 1
Errors	12.0 %	289





# Key Takeaways and What's Next

# AI's Impact in a Nutshell



**Reduce Human Effort**



**Shrink Time**



**Reduce MTTx**



# What's Next in AI for AppDynamics

Now (Available Today)	Next	Later *
<p>Dynamics Baselines</p> <ul style="list-style-type: none"><li>▪ Business Transactions</li></ul> <p>Anomaly Detection</p> <ul style="list-style-type: none"><li>▪ Business Transactions (ART, CPM, EPM)</li><li>▪ User Experience – Browser, Mobile (Page Load Time)</li><li>▪ Infrastructure (Server – CPU, Memory)</li></ul>	<p>Health Rule Violations</p> <ul style="list-style-type: none"><li>▪ 1-click RCA Summarization for Business Transactions</li></ul> <p>Anomaly Detection</p> <ul style="list-style-type: none"><li>• RCA Summarization and Recommendations for Business Transactions</li></ul>	<p>Health Rules Violations</p> <ul style="list-style-type: none"><li>▪ 1-click RCA Summarization for JVM/CLR/HW/Database</li><li>▪ Recommendations &amp; Remediations</li><li>▪ Adaptive Criteria</li></ul> <p>Alert Aggregation / Grouping</p> <p>Chat-based and Embedded Insights (RCA, etc.)</p> <p>EUM Troubleshooting</p> <p>Webex/Slack/Teams AI Agents</p>

\* Items listed here are not formally committed at this point

# Complete Your Session Evaluations



**Complete** a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



**Earn** 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



**Level up** and earn exclusive prizes!



**Complete your surveys** in the Cisco Live mobile app.

# Continue your education



**Visit** the Cisco Showcase for related demos



**Book** your one-on-one Meet the Engineer meeting



**Attend** the interactive education with DevNet, Capture the Flag, and Walk-in Labs



**Visit** the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)

**Contact us at** [mraich@cisco.com](mailto:mraich@cisco.com) or [gatsehga@cisco.com](mailto:gatsehga@cisco.com)

# Join us at .conf!





Thank you

**CISCO** Live !

