

Automating the Enterprise Cloud

Observability at scale for Red Hat OpenShift providing answer-driven Automation with Event-Driven Ansible

Kristof Renders

Global Director, Innovation Services





Automating the Enterprise Cloud

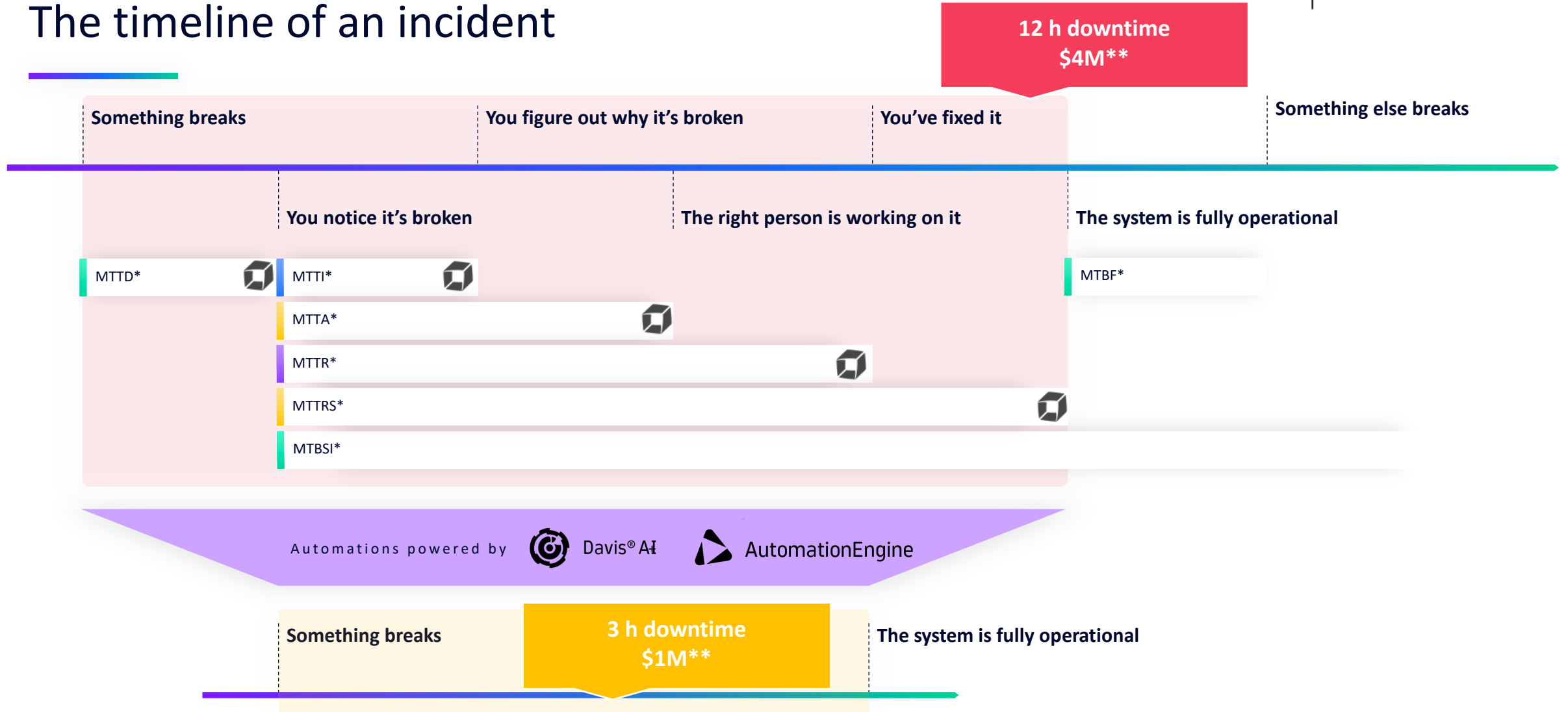
Observability at scale for Red Hat OpenShift providing answer-driven Automation with Event-Driven Ansible

Kristof Renders

Global Director, Innovation Services



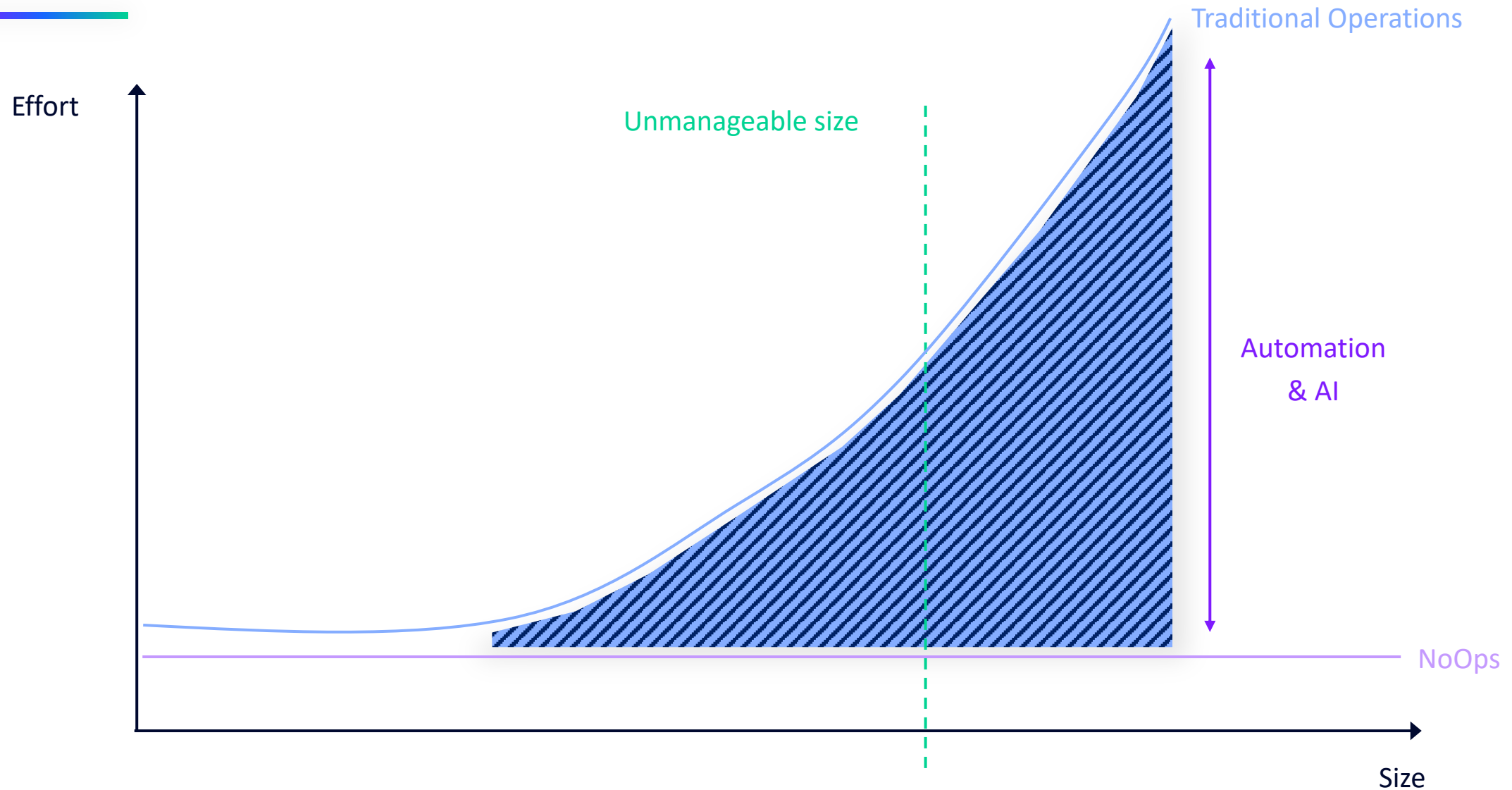
The timeline of an incident



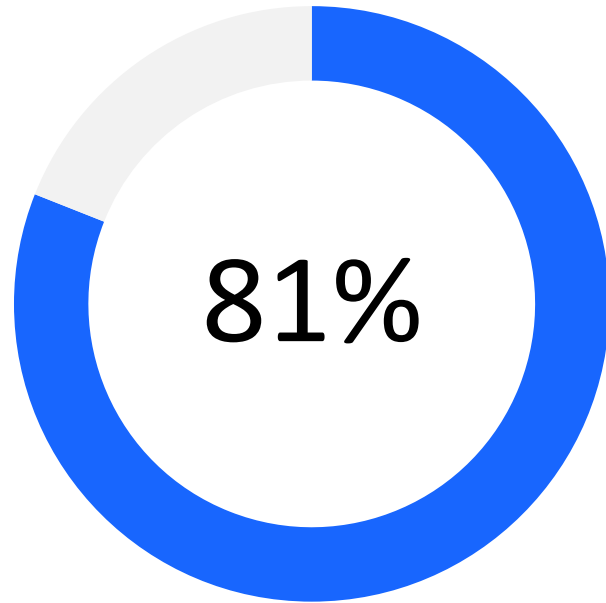
*) **MTTD**: Mean Time to Detect **MTBI**: Mean Time to Investigate **MTTA**: Mean Time to Action **MTTR**: Mean Time to Repair **MTTRS**: Mean Time to Restore Service **MTBF**: Mean Time Between Failures **MTBSI**: Mean Time Between Service Incidents

***) The average cost of downtime is \$5,600 per minute, according to a 2014 study by Gartner. <https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/>

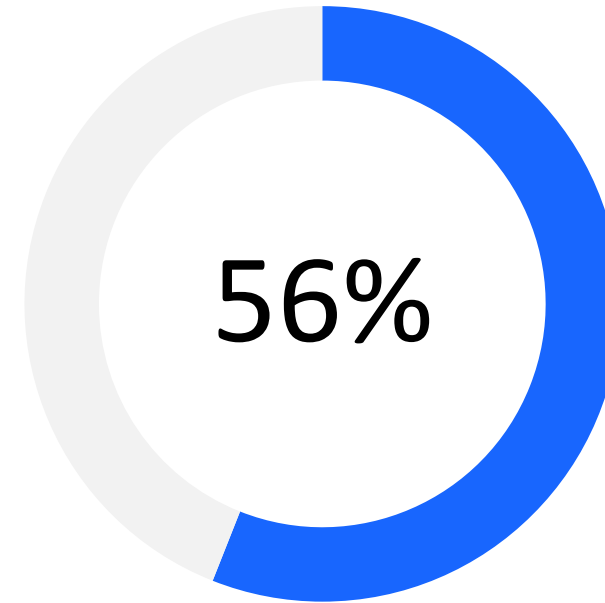
How Many Apps Can You Manage?



Traditional Monitoring Methods are Unable to Keep Up

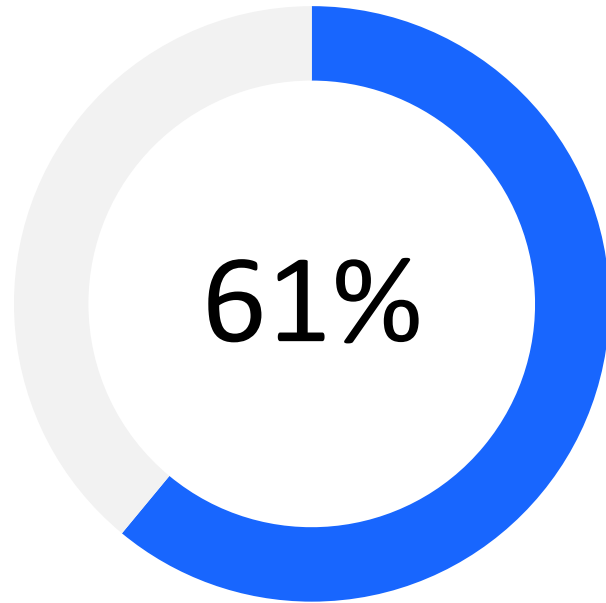


of IT leaders say their use of **Kubernetes** has made their infrastructure more **dynamic and difficult to manage** with existing solutions and approaches

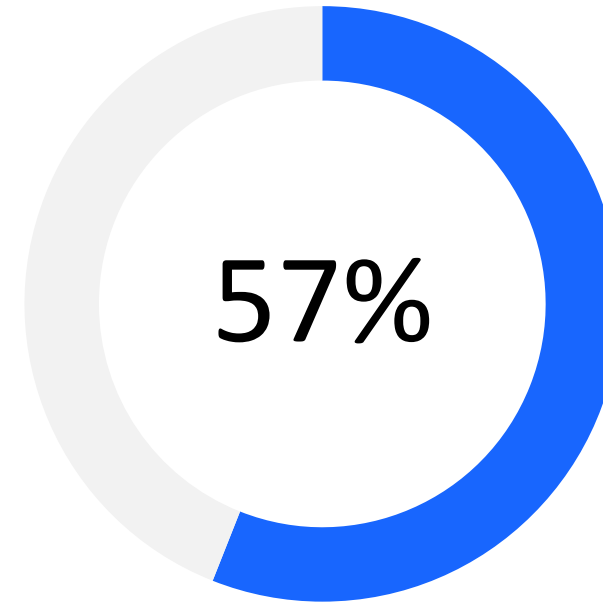


of IT leaders say **traditional infrastructure monitoring solutions are no longer fit for purpose** in a world of cloud and Kubernetes, and they must be replaced with a platform that can provide end-to-end observability across their multicloud environments

Inefficient DIY-Monitoring Create Data Overload

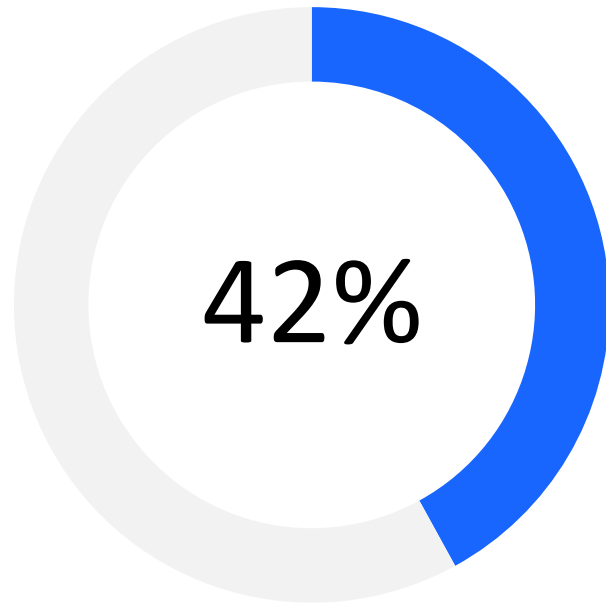


of IT leaders say **observability blind spots in their environments are becoming a greater risk to digital transformation** as teams are finding themselves without an easy way to monitor their technologies end-to-end

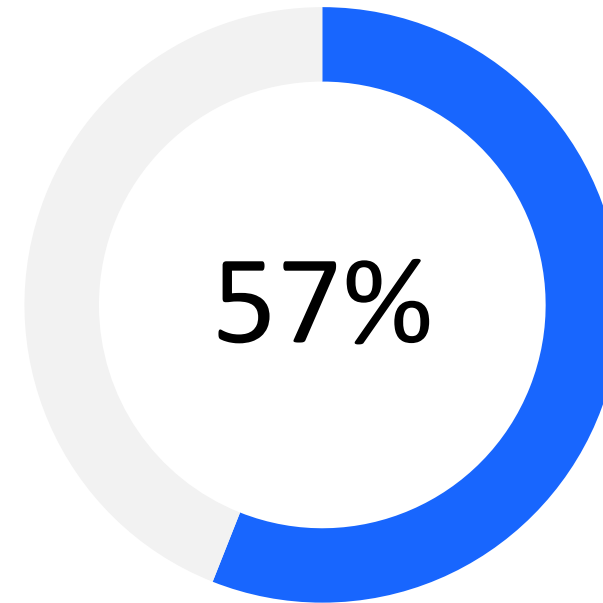


of IT leaders say **multiple monitoring solutions across multicloud environments are making it difficult** to optimize infrastructure performance and resource consumption

Unified Observability and AIOps Drive Success

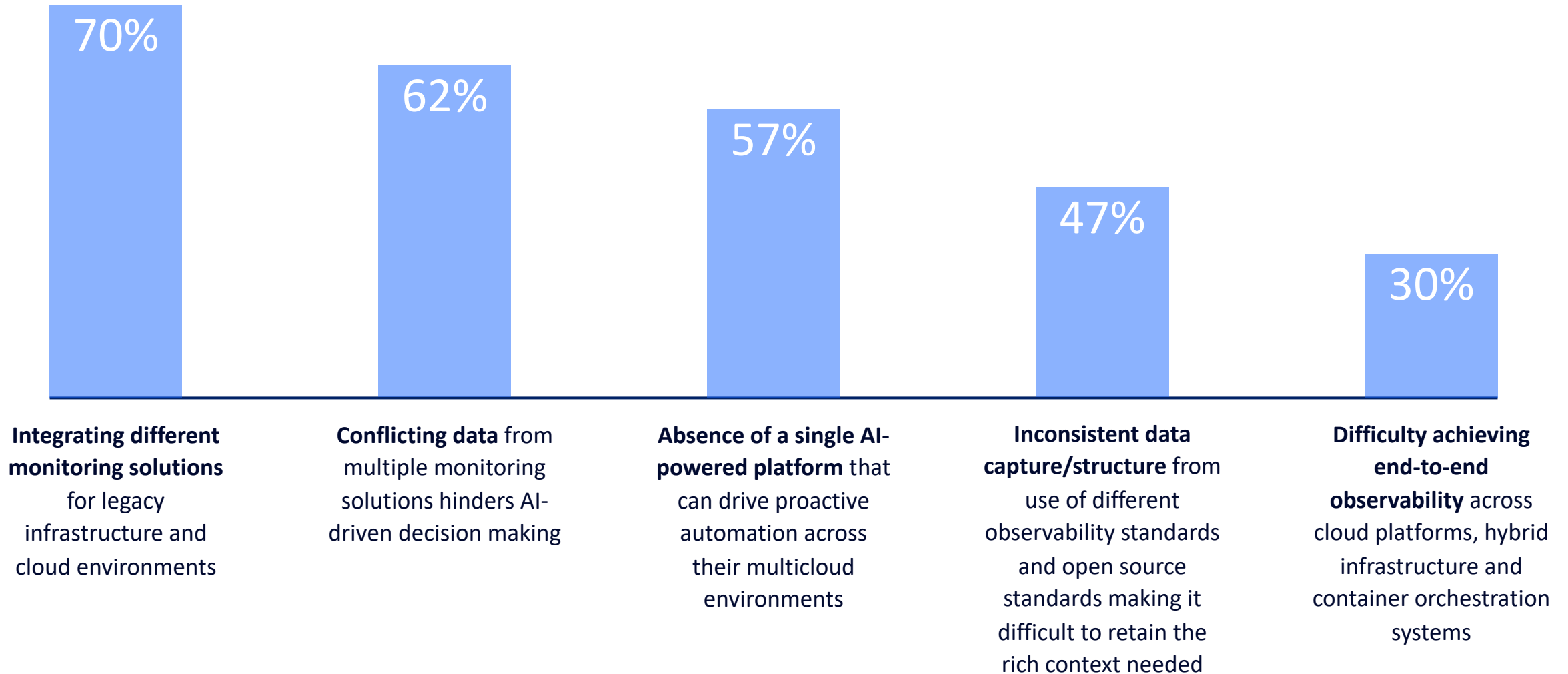


Nearly half of IT team's time is spent on manual, routine work to “keep the lights on” across their environments, creating a major productivity drain and leading to missed revenue opportunities due to delays in innovation

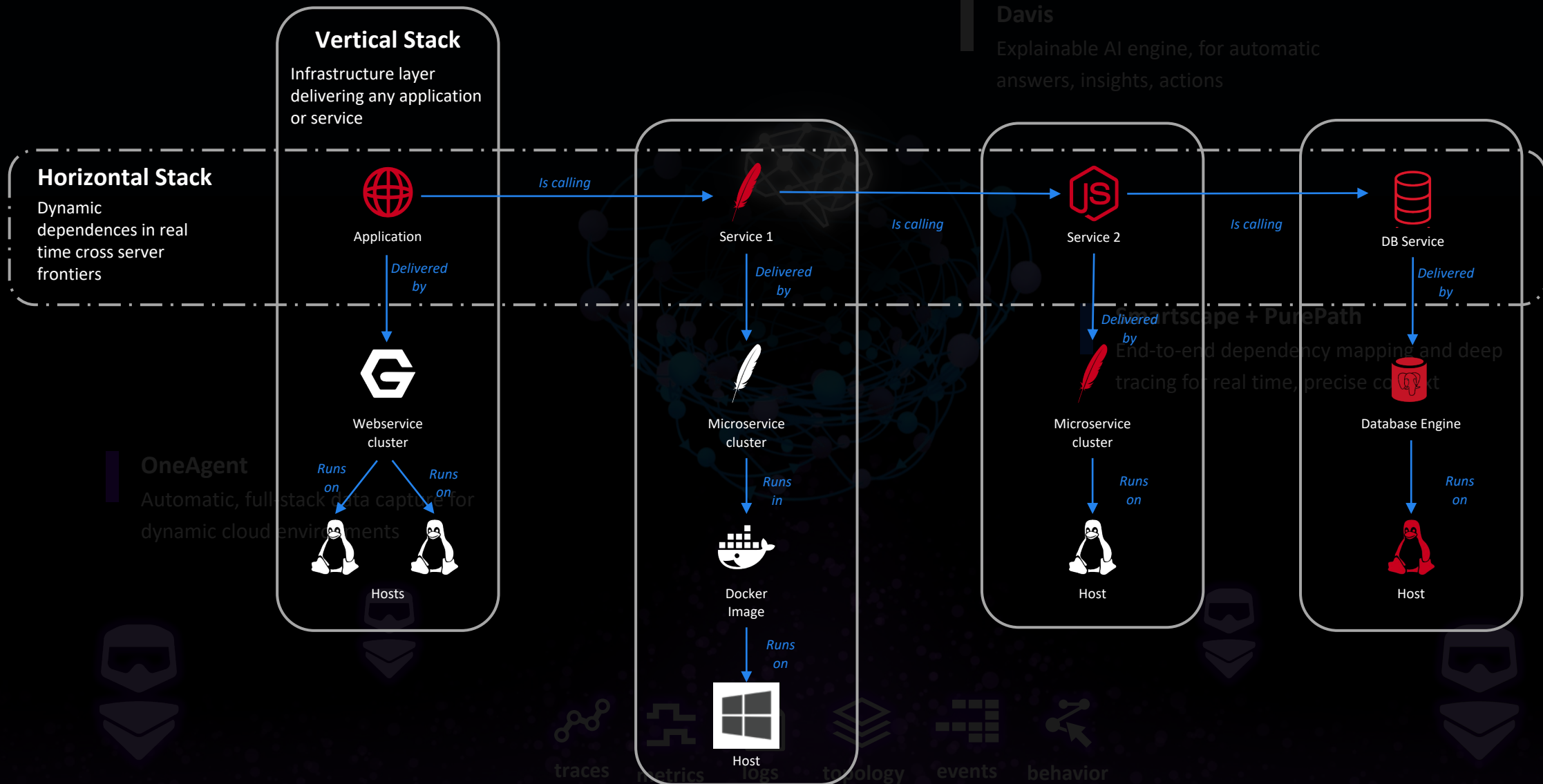


of IT leaders say **manual instrumentation and configuration of monitoring tools is unsustainable** in dynamic multicloud and Kubernetes environments, and teams increasingly struggle to keep up

Biggest Barriers to Achieving Large-scale Automation

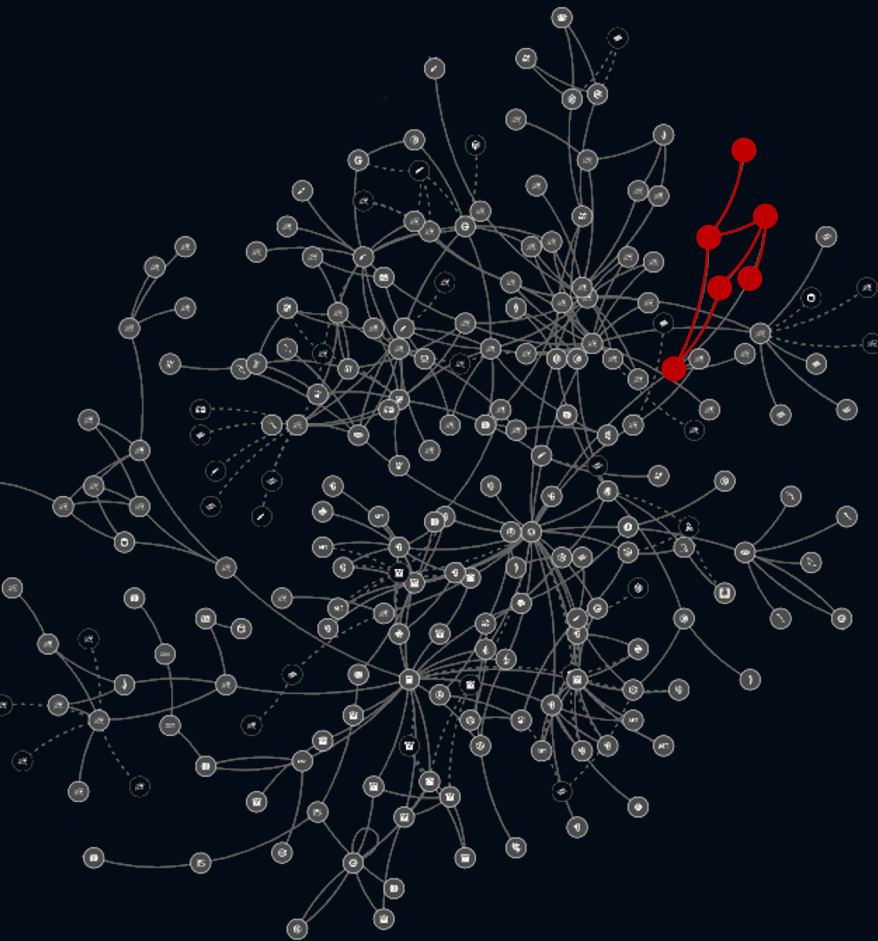


The Diagnostics of the unknowns



Enterprise complexity...

DAVIS[®]
analyzed 186,363,877,025,090,560 dependencies



Problems Problem P-211073888

Global_Servicing_Portal_Prod_US: User action duration degradation

Problem P-211073888 detected at 10:49 (open for 5 hours 11 minutes). This problem affects real users.

Affected applications 1 Affected services 141 Affected infrastructure 1

Business impact analysis
An analysis of all affected service calls and impacted real users during the first 1 hour 16 minutes of the problem shows the following potential impact.

5.06k Users observed 13.3mil Affected service calls

1 impacted application
1.6k+ User actions per minute impacted

Global_Servicing_Portal_Prod_US
Web application / Healthy again for 4 hours 1 minute

User action duration degradation
The current response time (6.86 s) exceeds the auto-detected baseline (2.94 s) by 133 %

Affected user actions	User action	OS
1.6k+ /min	5 User actions	
Browser	Geolocation	All
All	All	All

Root cause
Based on our dependency analysis all incidents have the same root cause

enterprise-comms-platform_registration-b_e3_ipc1
Web request service

Metric anomalies detected
Review the metrics which show abnormal or outlying behavior.

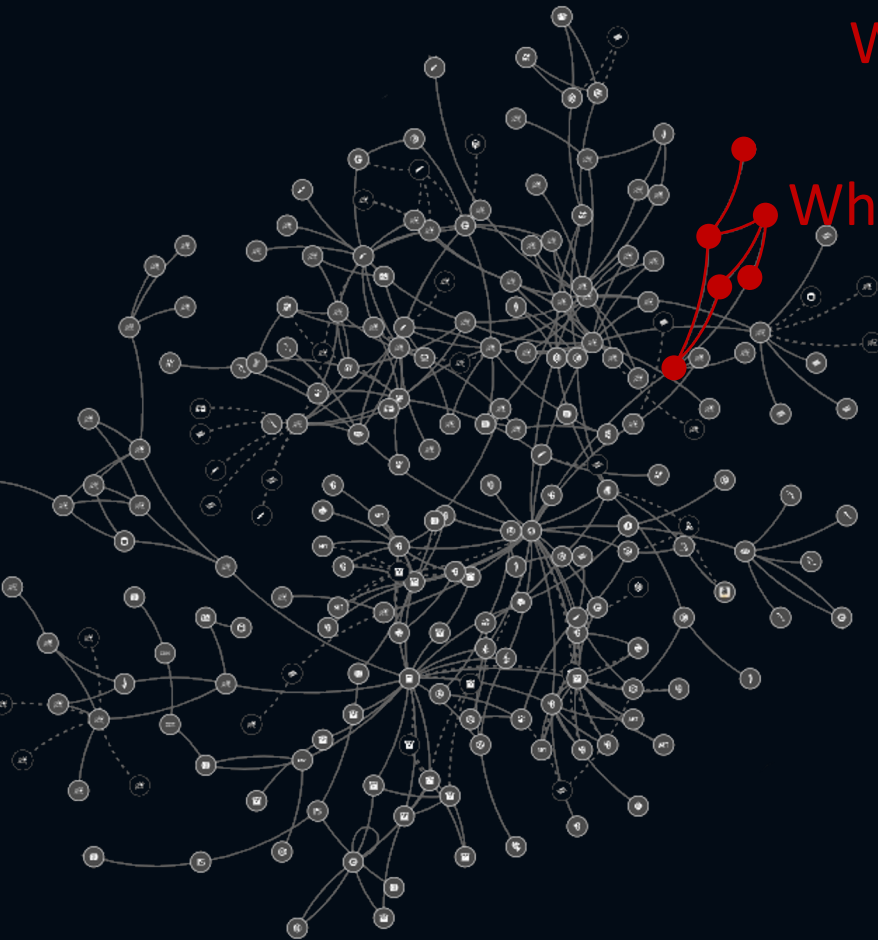
Client failure rate
+ 100 %
Now
Before

Analyze metric anomalies

Close problem

... cannot rely on humans

When something goes wrong, you need to act fast!



What caused it?

What broke?

Who do I need to inform?

Which services are impacted?

How do I remediate it?



Simplifying OpenShift requires unified observability at scale

1

Continuously discover Kubernetes nodes and pods to keep pace with changes

2

Automatically map all components to understand their impact on your environment

3

A common data model to improve collaboration between Ops and Apps teams

4

Precise root cause analysis to reduce MTTR and spend more time on strategic projects

5

Business impact analysis to understand how changes to your environment impact end users

How easy is it? Really?

Run 1 command for:

- Complete visibility of entire Kubernetes cluster:
 - Every node
 - Every pod/container
 - Every process
 - Every transaction, at method-level detail
- Connection to Kubernetes API for:
 - Insight into overall cluster health
 - Defined workloads
 - Kubernetes events
- Connection to Prometheus exporters
 - Full visibility of every exposed Prometheus metric
- Full Dynatrace traffic routing



Native Full-stack Visibility

INSTANT, CONTINUOUS, REAL-TIME
VISIBILITY OF ALL OPENSIFT
COMPONENTS, INCLUDING THEIR
RELATIONSHIPS.

ALL DATA CONTEXTUALISED AGAINST
THESE COMPONENTS

Smartscape topology > Hosts > ip-10-0-142-174.ec2.internal

Applications

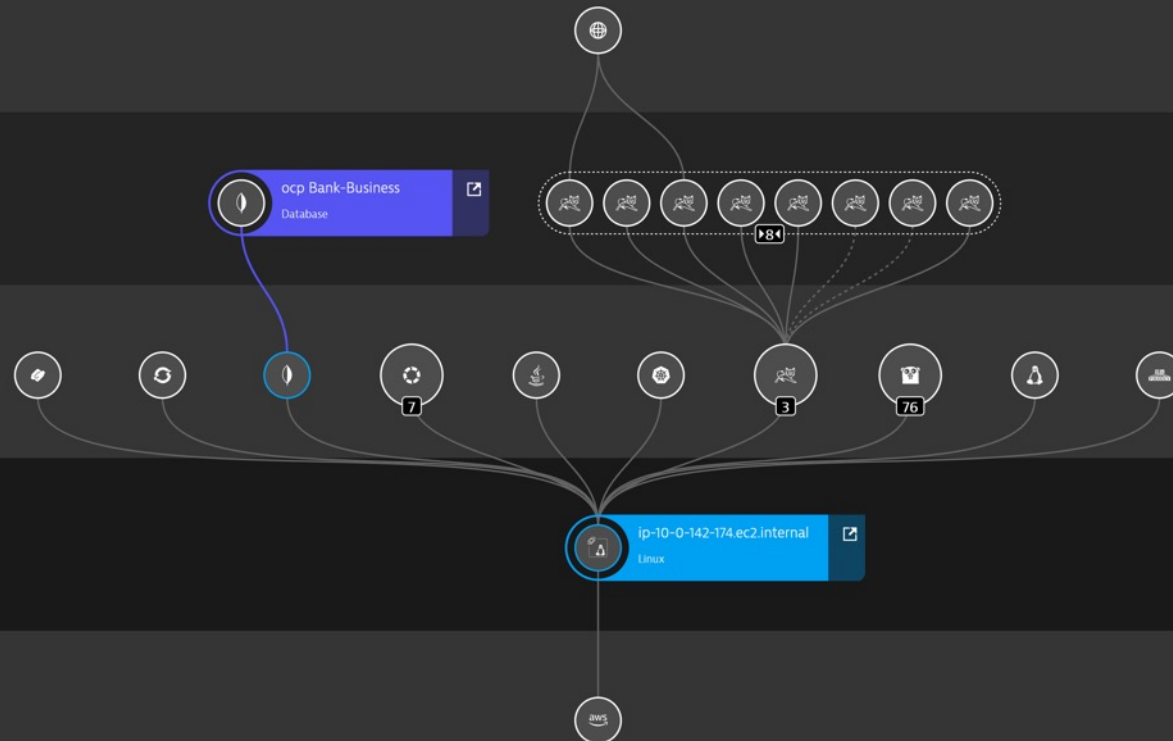
Services

Processes

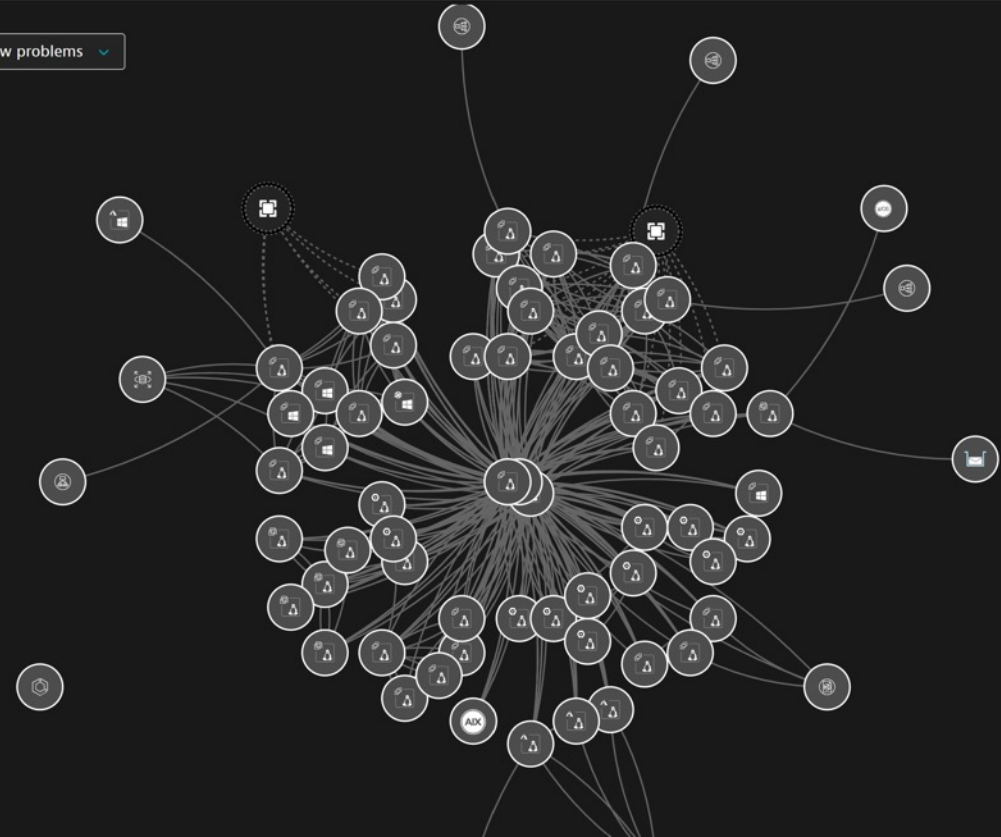
Hosts

283

Data centers



Show problems



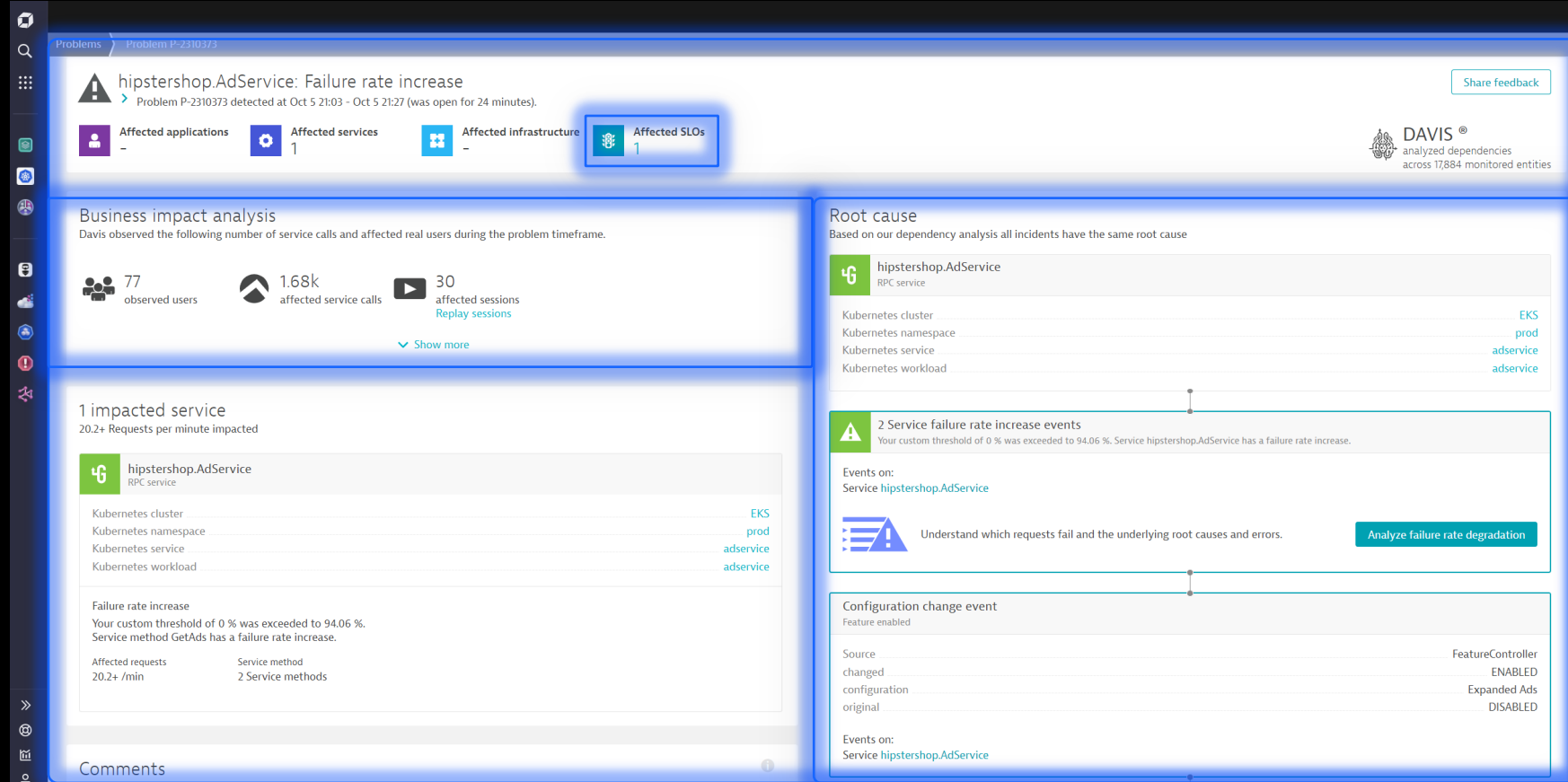
AUTOMATIC PROBLEM DETECTION

AUTOMATIC BUSINESS IMPACT ANALYSIS

AUTOMATIC ROOT CAUSE ANALYSIS,
UTILIZING CAUSAL AI

AUTOMATIC TOPOLOGY TRAVERSAL AND
ANALYSIS OF ALL DATA TYPES

AUTOMATIC SLO ASSOCIATION



Problems Problem P-2310373

hipstershop.AdService: Failure rate increase
 Problem P-2310373 detected at Oct 5 21:03 - Oct 5 21:27 (was open for 24 minutes).

Affected applications - **Affected services** 1 **Affected infrastructure** - **Affected SLOs** 1

Business impact analysis
 Davis observed the following number of service calls and affected real users during the problem timeframe.

77 observed users | 1.68k affected service calls | 30 affected sessions
[Replay sessions](#) | [Show more](#)

1 impacted service
 20.2+ Requests per minute impacted

hipstershop.AdService
 RPC service

Kubernetes cluster: EKS
 Kubernetes namespace: prod
 Kubernetes service: adservice
 Kubernetes workload: adservice

Failure rate increase
 Your custom threshold of 0 % was exceeded to 94.06 %. Service method GetAds has a failure rate increase.

Affected requests	Service method
20.2+ /min	2 Service methods

Root cause
 Based on our dependency analysis all incidents have the same root cause

hipstershop.AdService
 RPC service

Kubernetes cluster: EKS
 Kubernetes namespace: prod
 Kubernetes service: adservice
 Kubernetes workload: adservice

2 Service failure rate increase events
 Your custom threshold of 0 % was exceeded to 94.06 %. Service hipstershop.AdService has a failure rate increase.

Events on: Service hipstershop.AdService

[Analyze failure rate degradation](#)

Configuration change event
 Feature enabled

Source	FeatureController
changed configuration original	ENABLED
original	DISABLED

Events on: Service hipstershop.AdService

Comments



OpenShift Workloads



Use the power of Grail to bring context to OneAgent and OpenTel data

UNIFIED VIEW TO LEVERAGE KEY KUBERNETES WORKLOAD METRICS

IN CONTEXT DATA TO HELP DETECT UNHEALTHY OR SUSPICIOUS BEHAVIOR

KEEP YOUR KUBERNETES CLUSTER SECURE WITH ADVANCED SECURITY ANALYSIS

The screenshot shows the OpenShift Workloads dashboard for the 'adservice' workload. The dashboard includes a navigation bar with 'Kubernetes', 'eks', 'Namespaces', 'prod', 'Workloads', and 'adservice'. Below the navigation bar, there are tabs for 'Properties and tags', 'No problems', '11 Vulnerabilities', '0 SLOs', '2 Conditions', and 'Owners'. The main content area is divided into three sections: 'Events', 'Logs', and 'Vulnerabilities'. The 'Events' section contains a bar chart showing event counts over time and a table of events. The 'Logs' section contains a bar chart showing log counts over time and a table of logs. The 'Vulnerabilities' section contains a list of vulnerabilities, including Denial of Service (DoS) and CVE-2022-21541.

11 vulnerabilities

11 third-party vulnerabilities | No code-level vulnerabilities

Most severe third-party vulnerabilities
Showing the 5 most critical of 11 in total.

- S-188: Denial of Service (DoS)
Vulnerable component: com.google.protobuf:protobuf-java
- S-51: Incorrect Conversion between Numeric Types
Vulnerable component: Java runtime
- S-187: Denial of Service (DoS)
Vulnerable component: com.google.protobuf:protobuf-java
- S-239: Denial of Service (DoS)
Vulnerable component: io.netty:netty-handler
- S-50: CVE-2022-21541
Vulnerable component: Java runtime

[View all third-party vulnerabilities](#)



Quality and security gates

Site Reliability Guardian helps ensure better code rollout

VALIDATE THE HEALTH OF COMPONENTS
ACROSS ANY DATA IN GRAIL

USE GATES TO ENSURE VULNERABILITIES
CAN'T ENTER PRODUCTION

WORKFLOWS ARE ENFORCED IN CORE
PLATFORM CAPABILITIES

The screenshot shows the workflow editor for 'Carts Reliability Validation'. The workflow consists of the following steps:

- Event trigger:** tag.service == "carts" and tag.stage == "production" and event.type == ...
- run_validation:** Automation action to start a Site Reliability Guardian validation
- traverse_smartscape:** Build a custom task running js Code
- get_owner:** Retrieves entity and extracts ownership data from it.
- get_contact_details:** Extracts a list of contact details from teams that are returned by the...

The right-hand panel shows the configuration for the 'Event trigger' step:

- Event type:** bzevents
- Filter query:**

```
1 tag.service == "carts" and
2 tag.stage == "production" and
3 event.type == "DEPLOYMENT"
```

Below the filter query, there is a note: "The workflow is triggered when an event matching the criteria above is ingested. The filter supports a subset of the DQL filter syntax, including ==, and, or, and grouping with brackets (). For more options, see the documentation [?]."

At the bottom of the right panel, there is a button labeled "Query past events".

AUTOMATED REMEDIATION CUSTOMER EXAMPLE

U.S. GOVERNMENT INSTITUTION

MANUAL
REMEDATION



60 minutes

AUTOMATED
REMEDATION

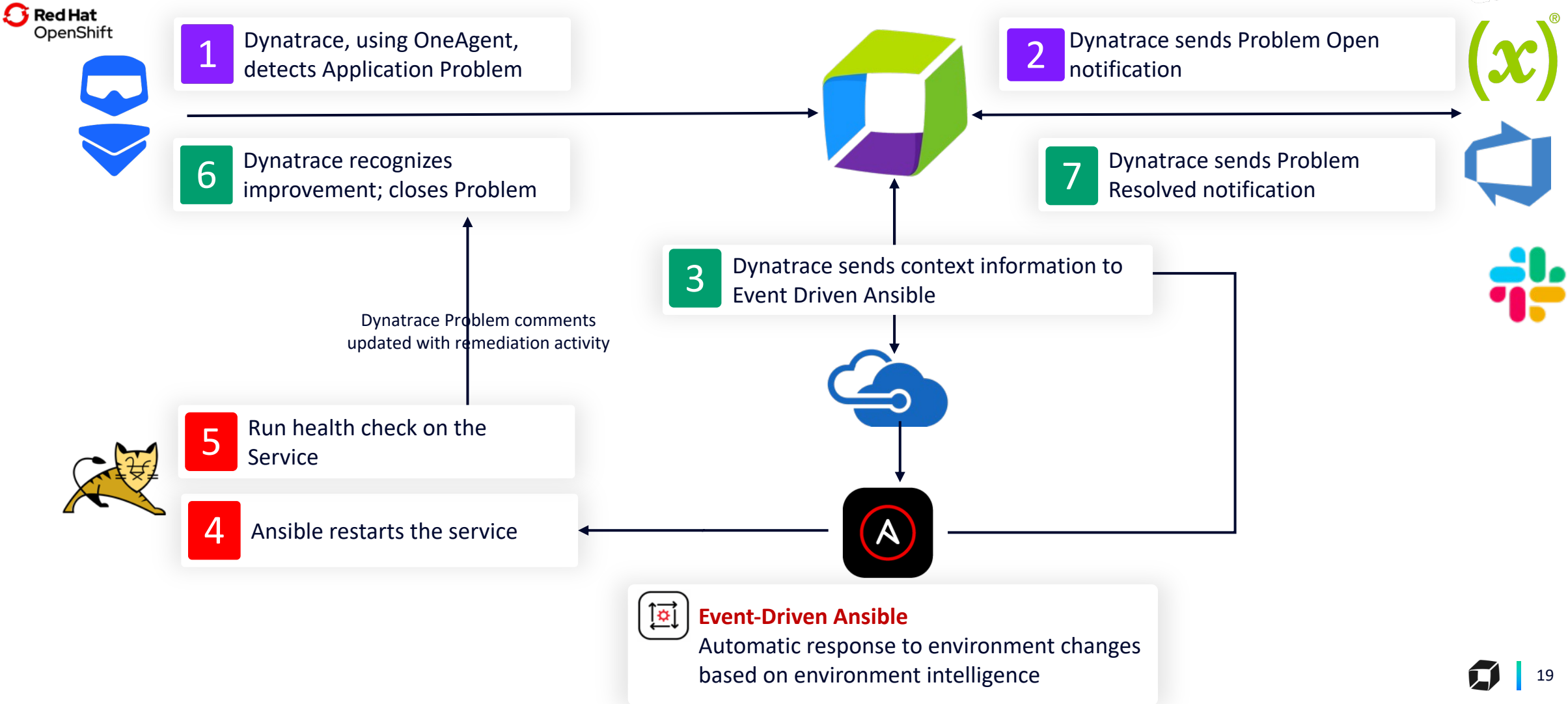


99% reduction in MTTR

9 seconds



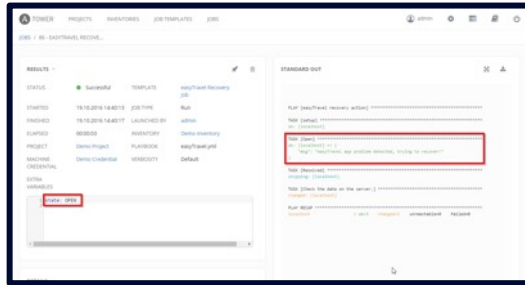
Solution Architecture for AI Operations



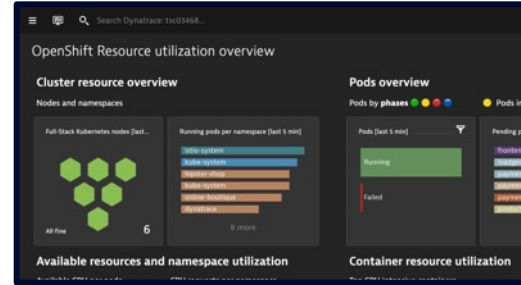
What Automation means for our customers



Dynatrace and Red Hat Partnership



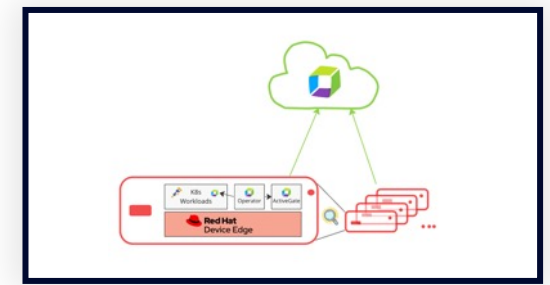
May 2017
Dynatrace executes self-healing with Ansible Tower



May 2018
Dynatrace OneAgent Operator for Red Hat OpenShift



Feb 2020
Dynatrace Managed is certified for Red Hat Enterprise Linux (RHEL) 8.x distributions



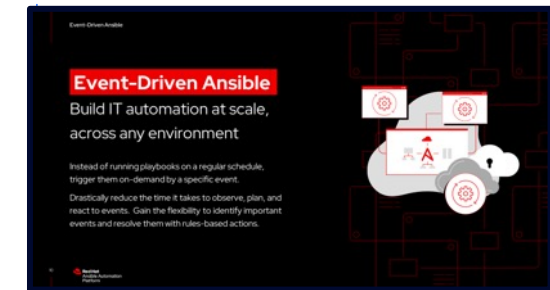
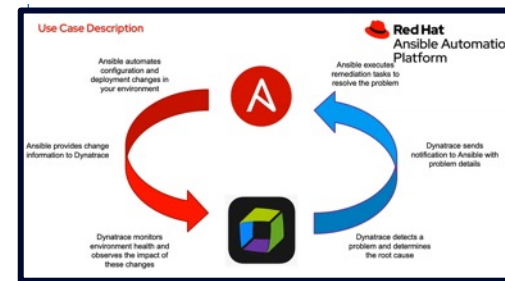
Nov 2023
Dynatrace and Red Hat expand enterprise observability to edge computing

2016
Dynatrace becomes Red Hat Certified Partner, enabling insight into deployed applications

June 2017
Only APM Red Hat OpenShift Primed partner and Red Hat Container Technology Certified partner

May 2019
Dynatrace integrates with Red Hat Ansible to deliver a self-driving cloud ecosystem

Oct 2022
Dynatrace and Red Hat Ansible kick-off next chapter with EDA



For detailed information
Please visit our booth G1 or contact us via:
marcom@asseco-see.com.tr

Thank You



Breakout Session Feedback



<https://forms.gle/thDhJnogZwRp77iAA>

