

From Monitoring to Observability

Dave McAllister

Sr. Technical Evangelist

Stephane Estevez

Product Marketing Director EMEA, IT Markets



Forward-Looking Statements




During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2020 Splunk Inc. All rights reserved

New Names, Same Great Technologies

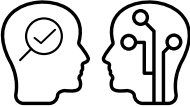

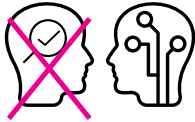

VictorOps  is now **Splunk On-Call**

SignalFx
Infrastructure Monitoring  is now **Splunk Infrastructure Monitoring**

SignalFx
Microservices APM  is now **Splunk APM**

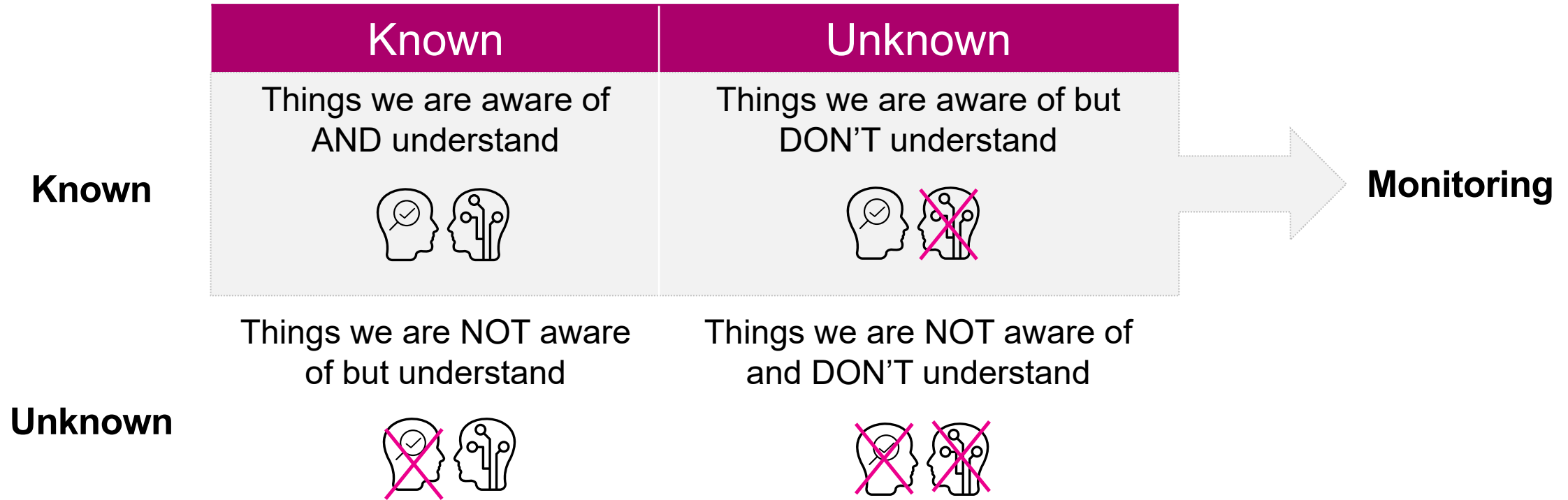
Observability Allows Us to Monitor For the Unknown Unknowns

Today's knowns are yesterday unknowns

	Known	Unknown
Known	Things we are aware of AND understand 	Things we are aware of but DON'T understand 
Unknown	Things we are NOT aware of but understand 	Things we are NOT aware of and DON'T understand 

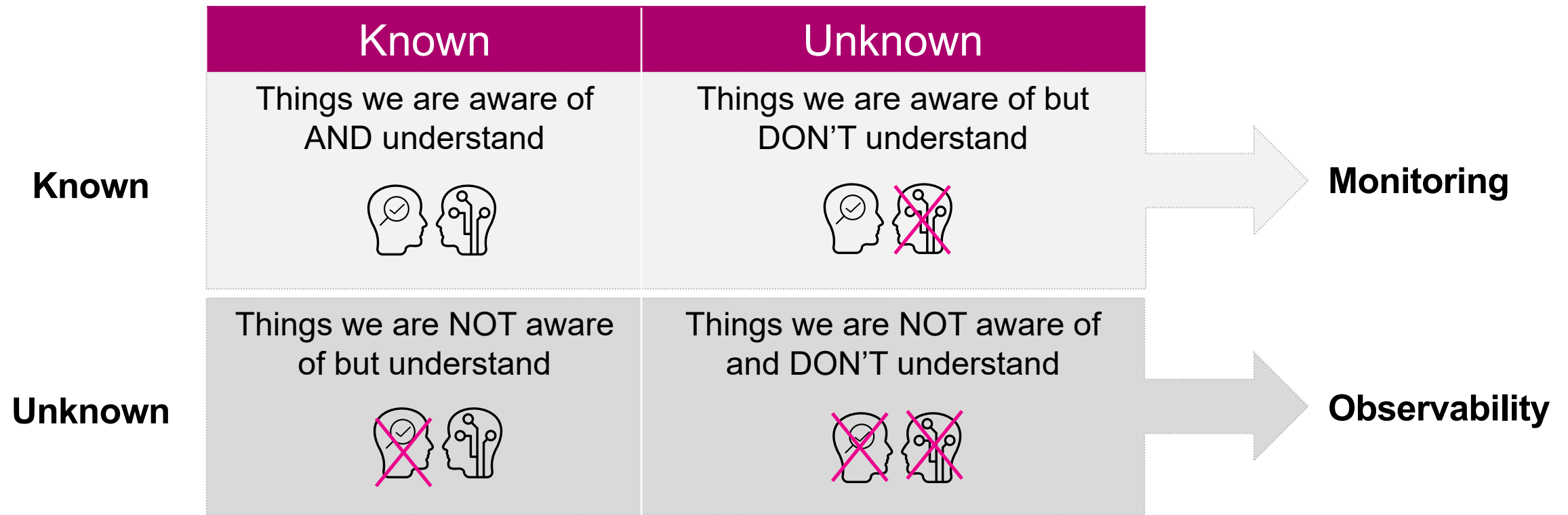
Observability Allows Us to Monitor For the Unknown Unknowns

Today's knowns are yesterday unknowns



Observability Allows Us to Monitor For the Unknown Unknowns

Today's knowns are yesterday unknowns



Monitoring

Looking for expected problems, e.g.:

- Applications
- Overloaded CPU
- High Memory Utilization
- Disk Space
- High Response Latency
- High Error Rate
- Service Availability

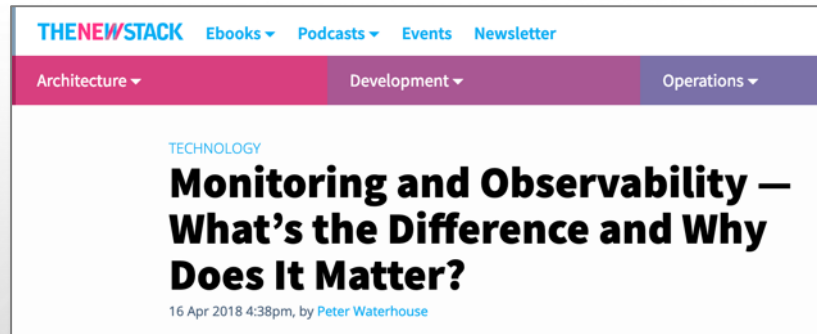
Observability

Looking for new and missing data to enhance monitoring

- Existing Environments
- Containers
- Serverless
- Microservices
- Multi-clouds
- Anything else that can fail, but hasn't (yet)

Observability... The Word Starts Spreading

Because failure is shifting to application code and into production system behavior



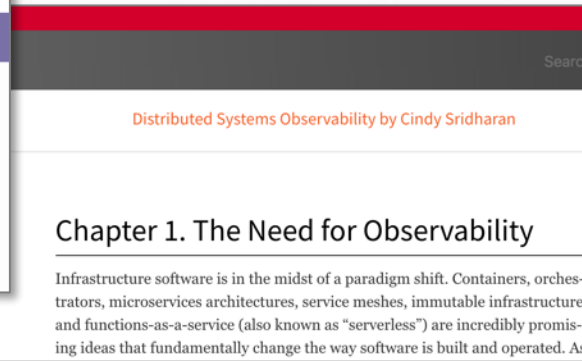
THE NEW STACK Ebooks ▾ Podcasts ▾ Events Newsletter

Architecture ▾ Development ▾ Operations ▾

TECHNOLOGY

Monitoring and Observability – What’s the Difference and Why Does It Matter?

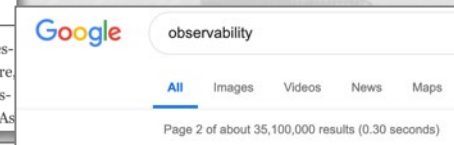
16 Apr 2018 4:38pm, by Peter Waterhouse



Distributed Systems Observability by Cindy Sridharan

Chapter 1. The Need for Observability

Infrastructure software is in the midst of a paradigm shift. Containers, orchestrators, microservices architectures, service meshes, immutable infrastructure, and functions-as-a-service (also known as “serverless”) are incredibly promising ideas that fundamentally change the way software is built and operated. As



Google observability

All Images Videos News Maps

Page 2 of about 35,100,000 results (0.30 seconds)



Salesforce Engineering Follow

TECHNOLOGY ARCHITECTURE FILES OPEN SOURCE DEVOPS CUI

What is Observability?

 Dmitry Melanchenko Follow

May 30, 2018 · 6 min read



VividCortex Product Solutions

Monitoring Isn't Observability

Posted by Baron Schwartz on Sep 14, 2017 4:56:32 PM

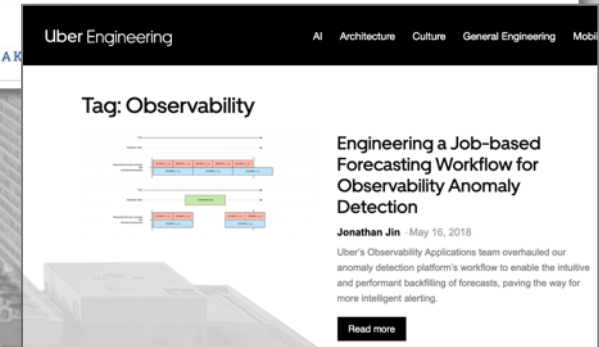
Observability is all the rage, an emerging term that's trending up very quickly in certain circles even while it remains unknown in others. As such, there isn't a single widely understood meaning for the term, and much confusion is inevitably following. What is observability? What does it mean? Perhaps just as importantly, what is observability NOT?

TL;DR: Monitoring tells you whether a system is working, observability lets you ask why it isn't working. [Tweet this](#)




Observability: the new wave or another buzzword?

BY DOUG BREAK



Uber Engineering AI Architecture Culture General Engineering Mobil

Tag: Observability



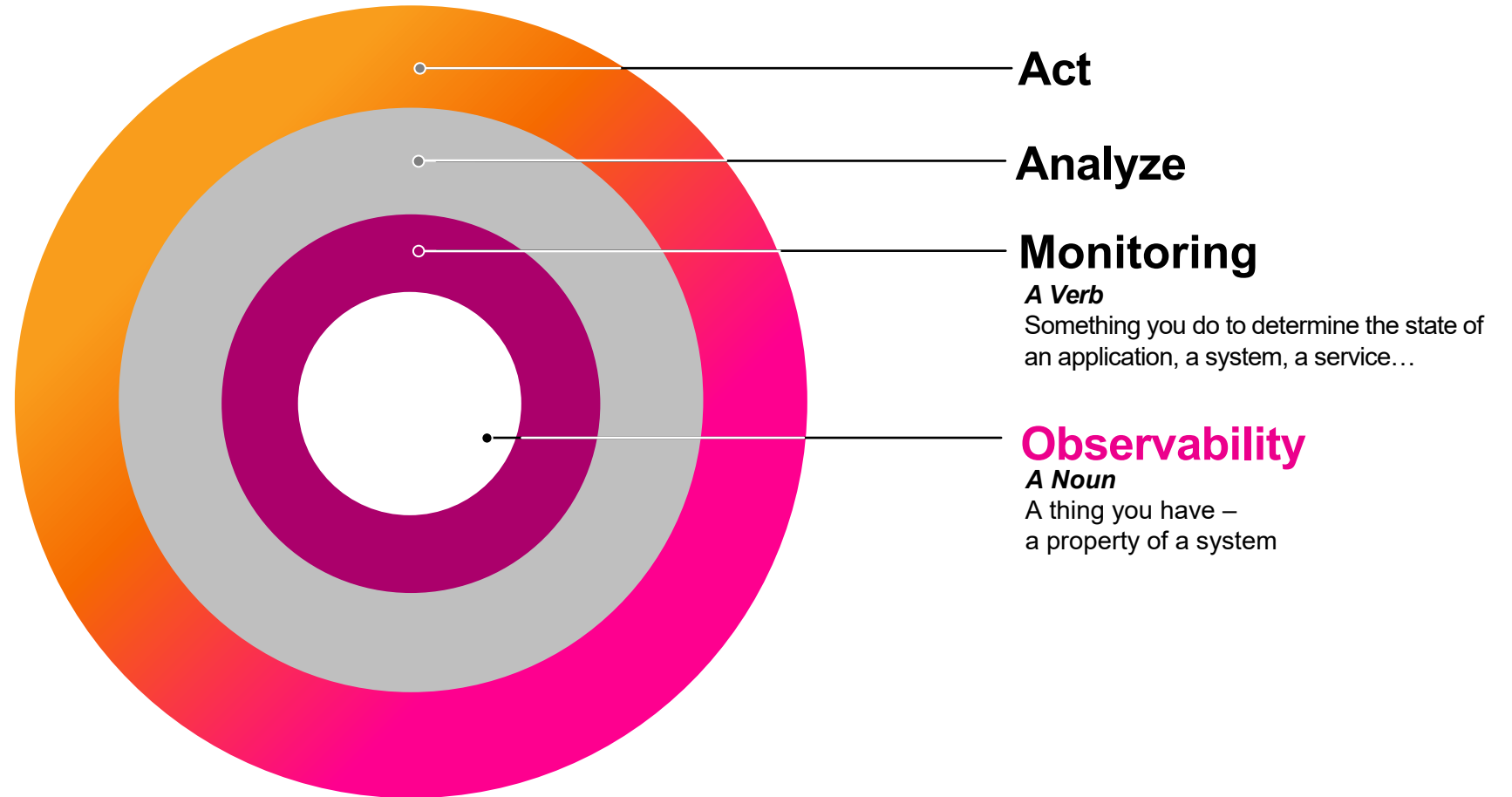
Engineering a Job-based Forecasting Workflow for Observability Anomaly Detection

Jonathan Jin May 16, 2018

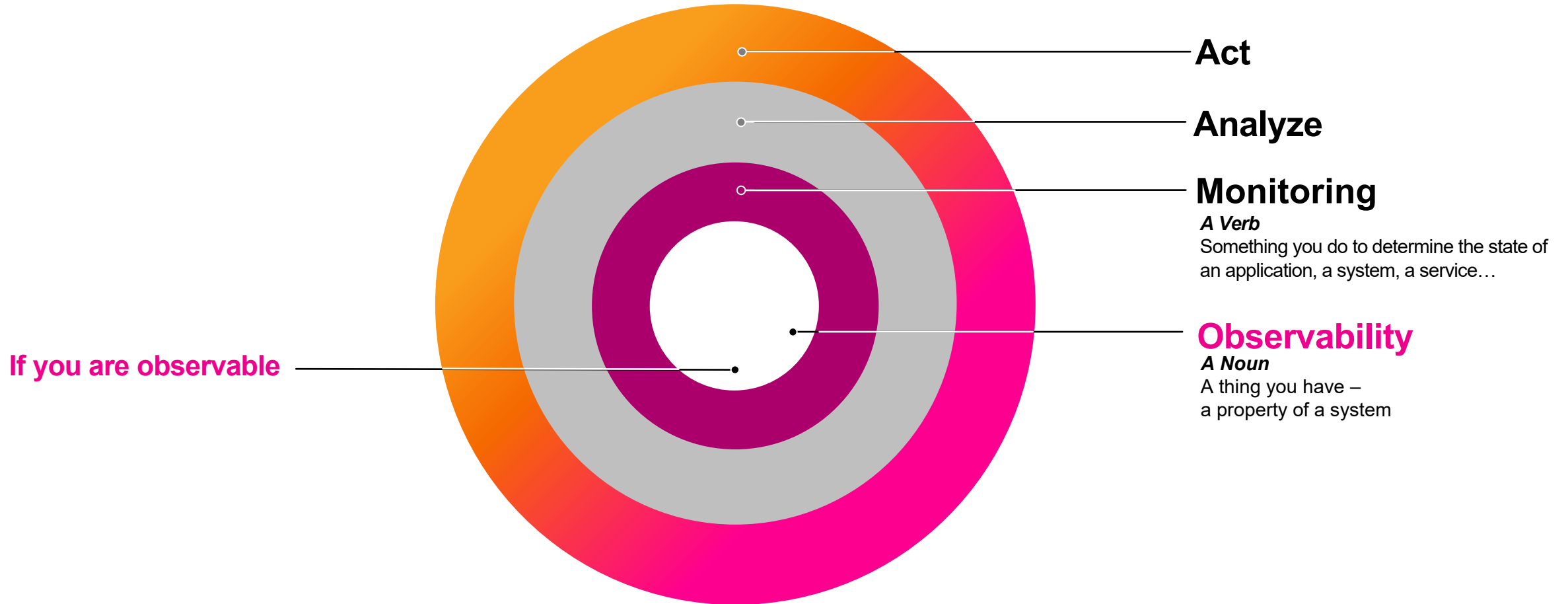
Uber's Observability Applications team overhauled our anomaly detection platform's workflow to enable the intuitive and performant backfilling of forecasts, paving the way for more intelligent alerting.

[Read more](#)

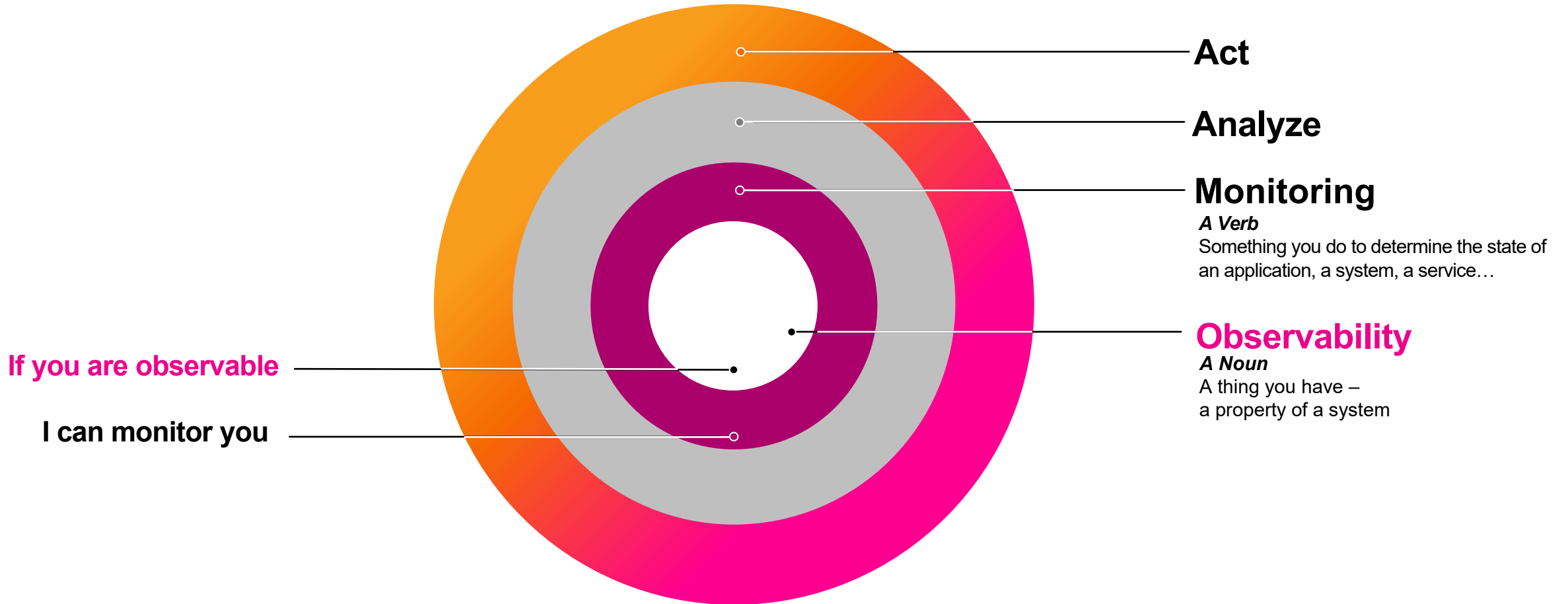
Turning Observability into Action



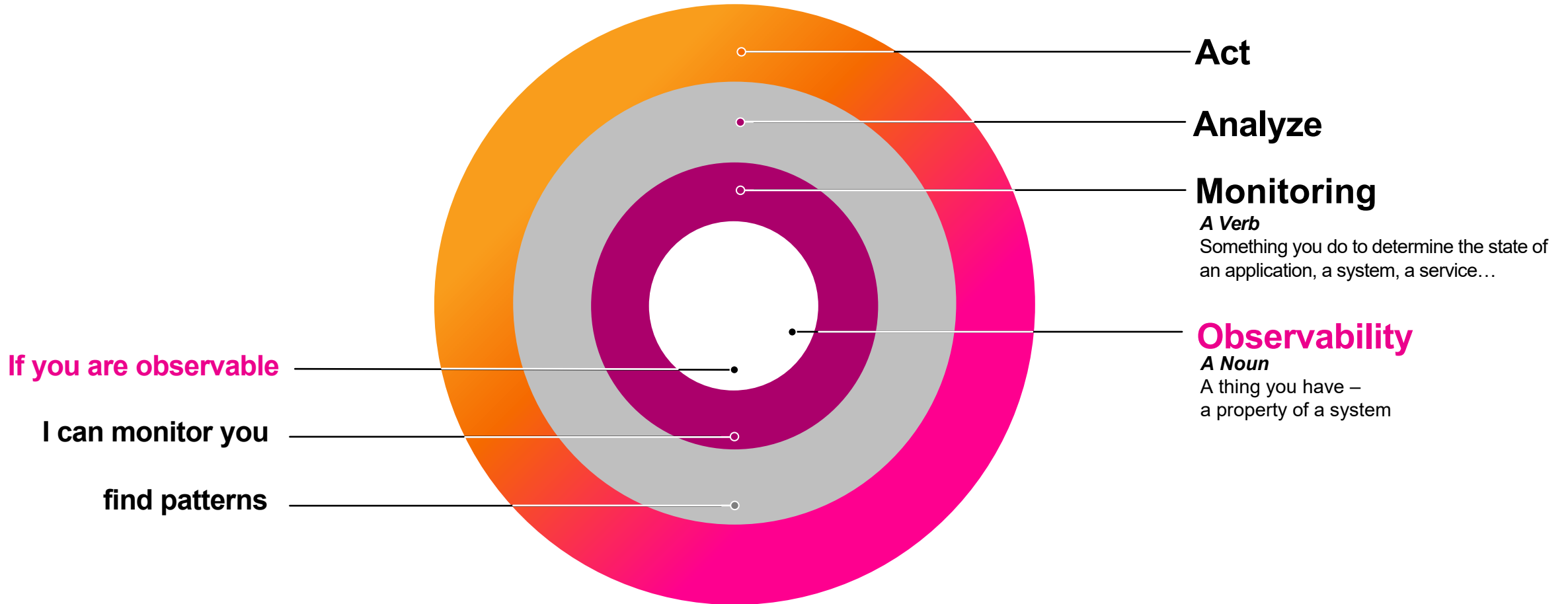
Turning Observability into Action



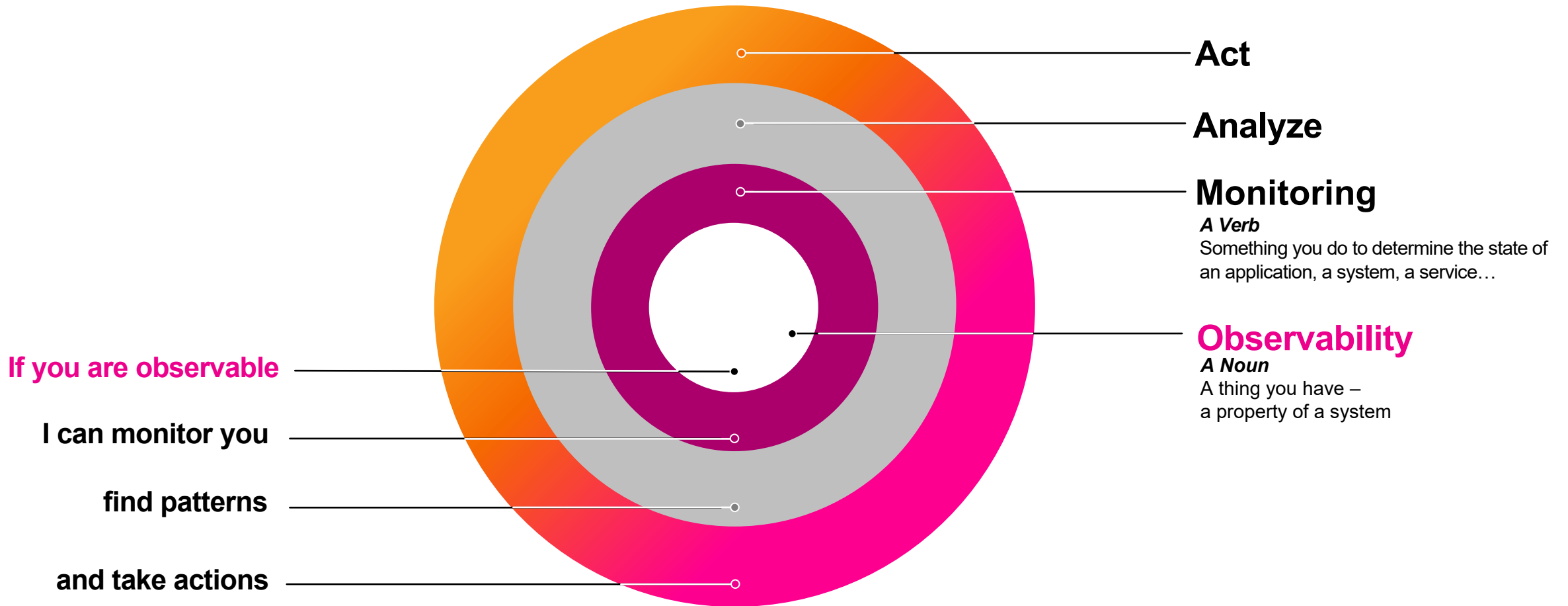
Turning Observability into Action



Turning Observability into Action

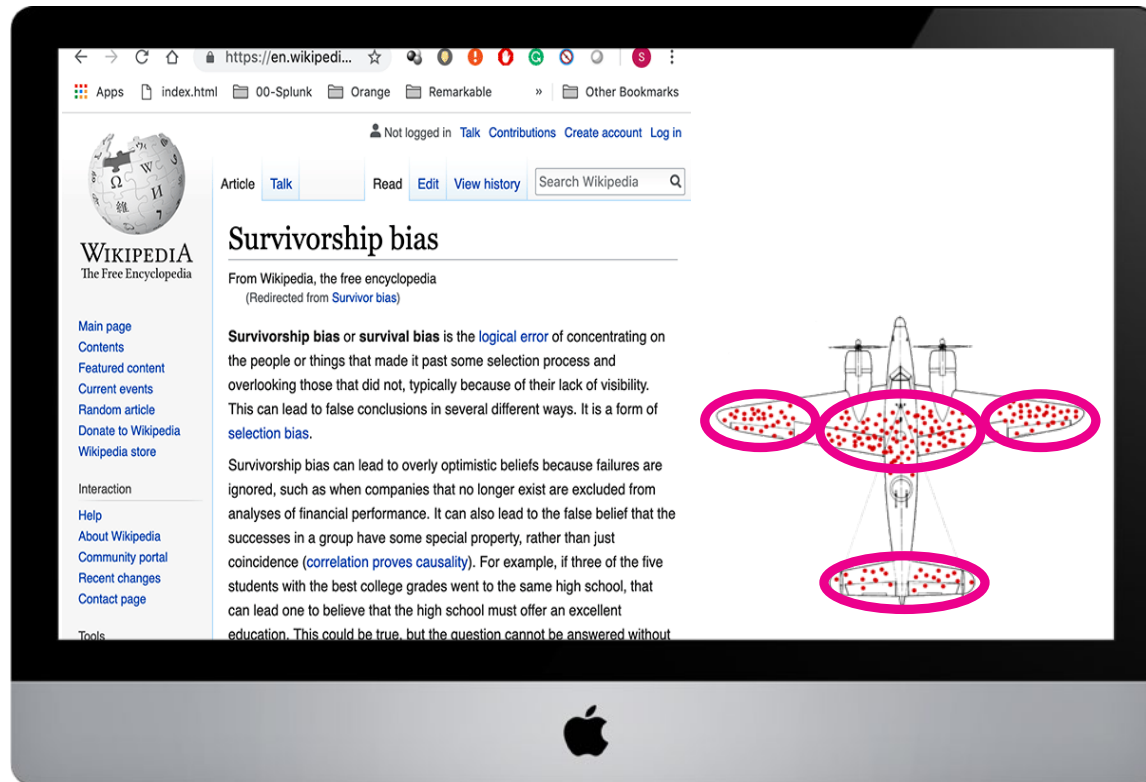


Turning Observability into Action



Understanding Observability Mindset

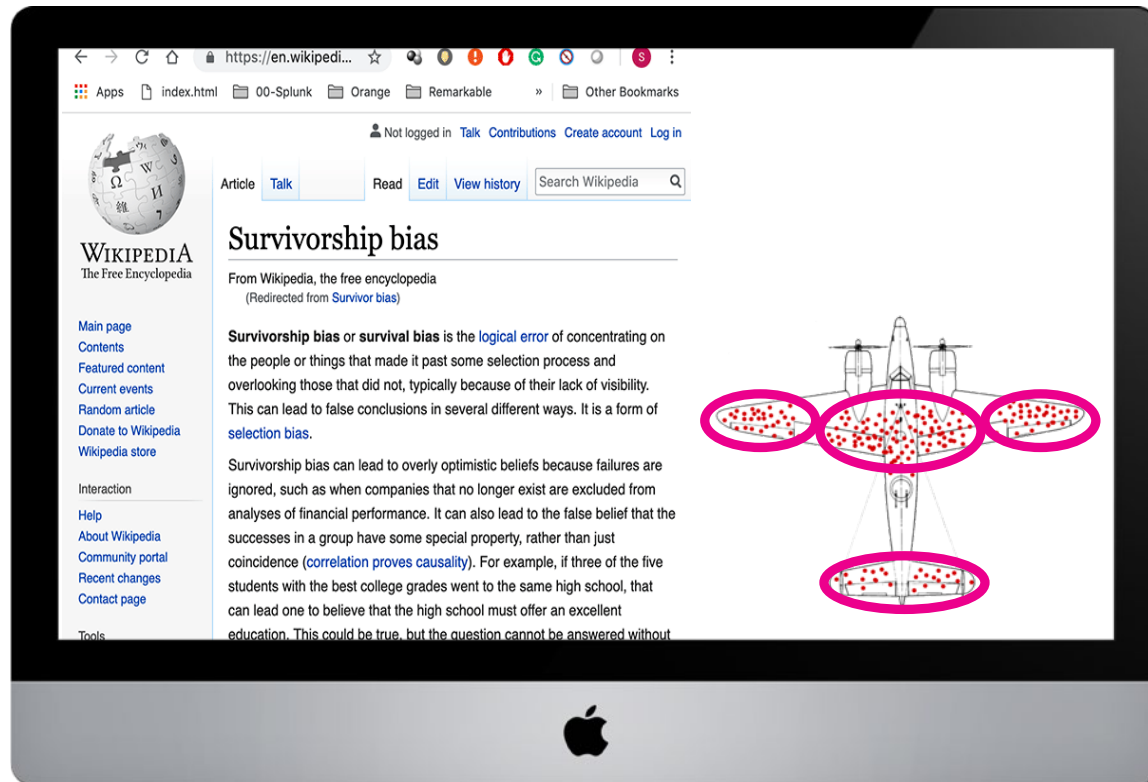
Survivorship bias or survival bias is the **logical error of concentrating on the people or things that made it past some selection process, and overlooking those that did not**, typically because of their **lack of visibility**. This can lead to false conclusions in several different ways.



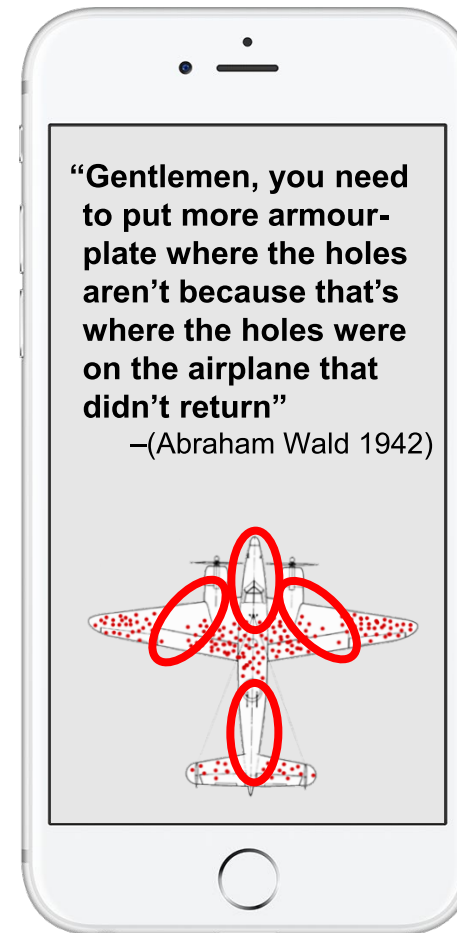
Source: Wikipedia

Understanding Observability Mindset

Survivorship bias or survival bias is the **logical error of concentrating on the people or things that made it past some selection process, and overlooking those that did not**, typically because of their **lack of visibility**. This can lead to false conclusions in several different ways.



Source: Wikipedia



A shot down aircraft doesn't externalize its state

So What is Observability?

“Focus on what you can’t see, the unknowns. If the root cause of a failure stays invisible (the bullet holes) your IT-plane will be shot down again.”

Observability

The Three Pillars

WHAT'S HAPPENING?

METRICS
Detect

Observability

The Three Pillars

WHAT'S HAPPENING?

METRICS
Detect

WHERE IS IT HAPPENING?

TRACES
Troubleshoot

Observability

The Three Pillars

WHAT'S HAPPENING?

METRICS
Detect

WHERE IS IT HAPPENING?

TRACES
Troubleshoot

WHY IS IT HAPPENING?

EVENTS / LOGS
Pinpoint

Observability

The Three Pillars

WHAT'S HAPPENING?

METRICS
Detect



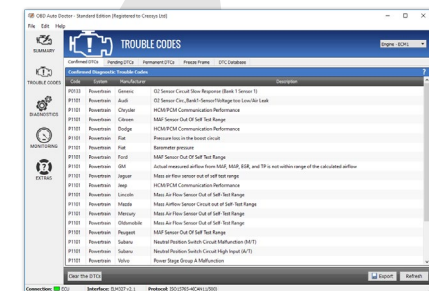
WHERE IS IT HAPPENING?

TRACES
Troubleshoot



WHY IS IT HAPPENING?

EVENTS / LOGS
Pinpoint



Observability Drives Evidence-based Debugging

Debugging for complex systems is iterative

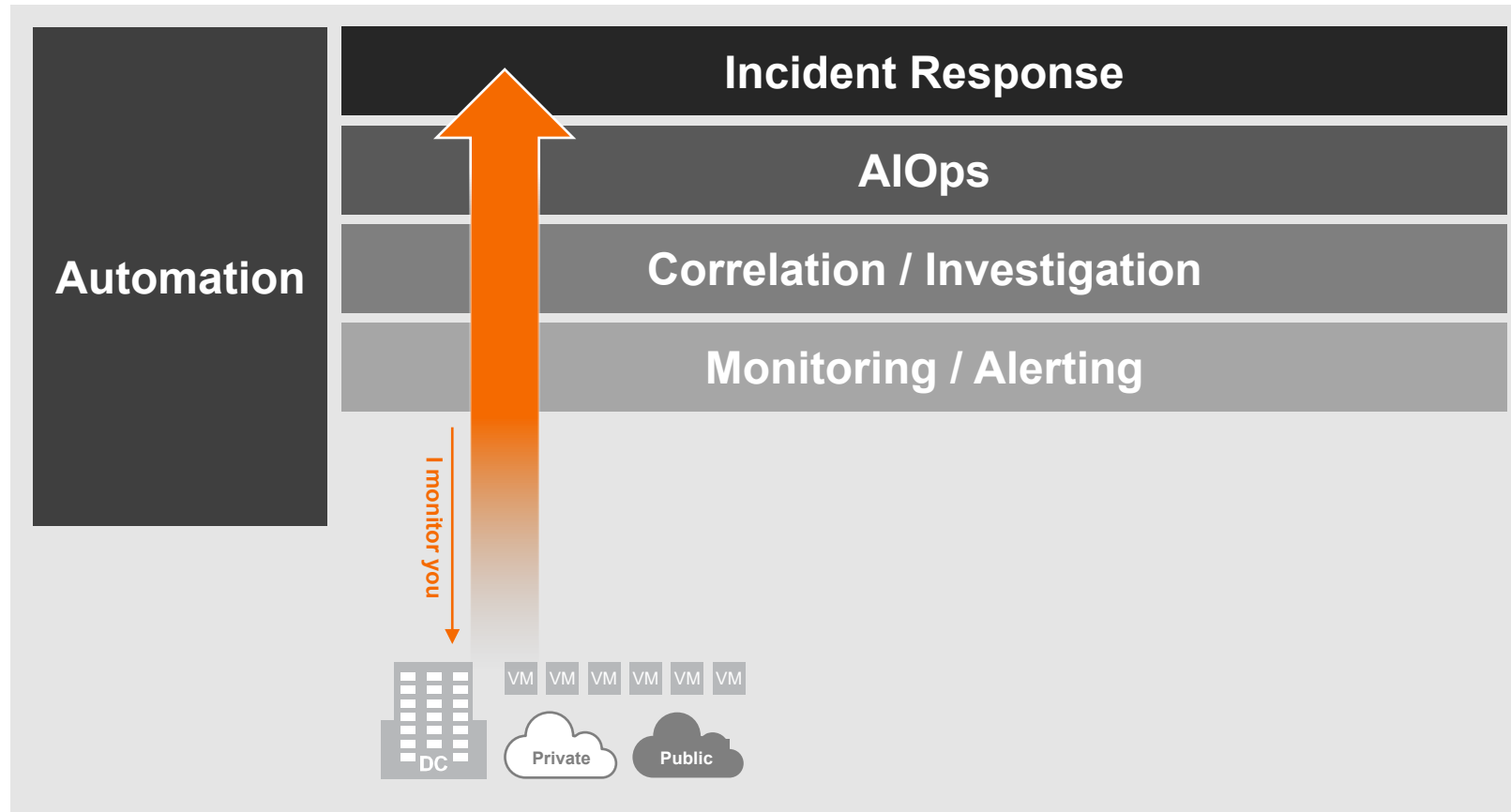
Start with a high-level metric

Drill down and detangle based on fine-grained data/observations

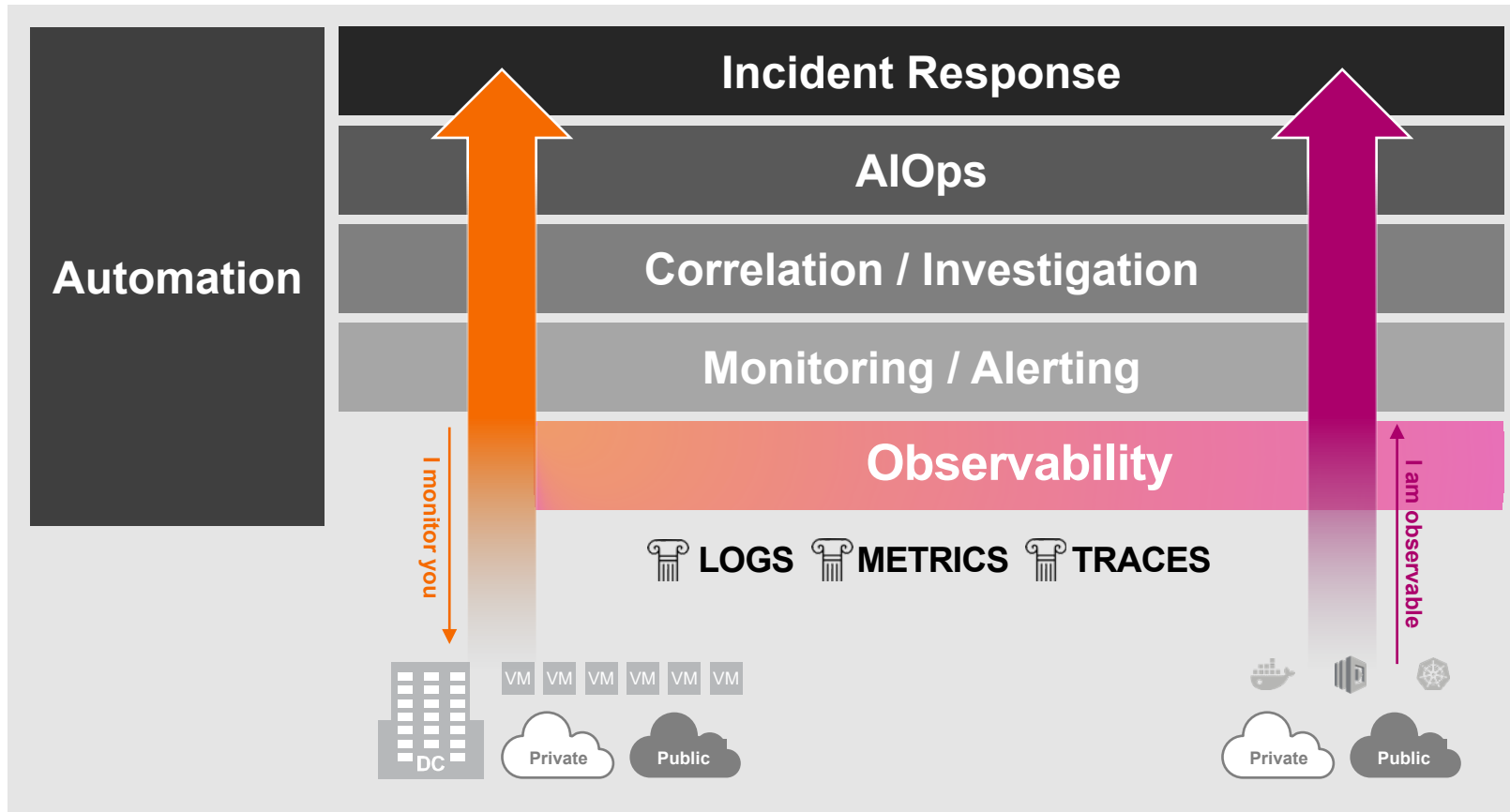
Make the right deductions based on the evidence



Enhancing Incident / Problem Management



Enhancing Incident / Problem Management





Connect



Search



Add to cart



Checkout



Payment

Tracing



Dev



Connect



Search



Add to cart



Checkout



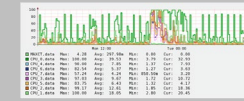
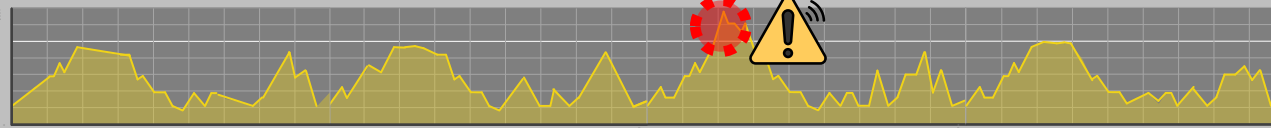
Payment

Tracing



Dev

Metrics Monitoring



Ops



Connect



Search



Add to cart



Checkout



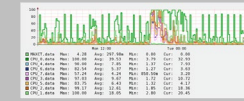
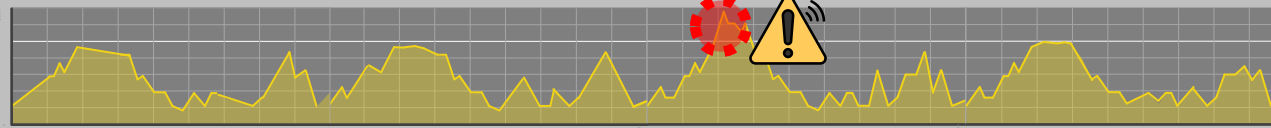
Payment

Tracing



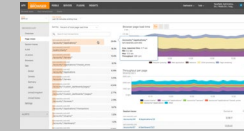
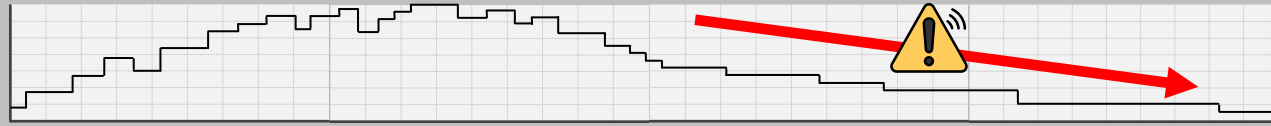
Dev

Metrics Monitoring



Ops

Sessions Monitoring



Business



Connect



Search



Add to cart



Checkout



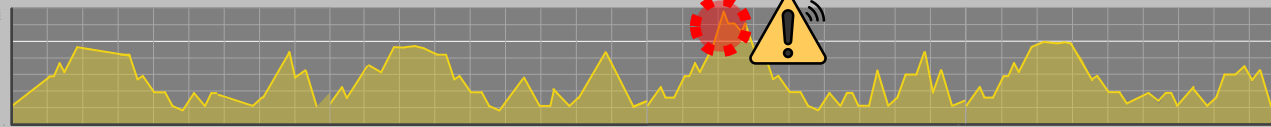
Payment

Tracing



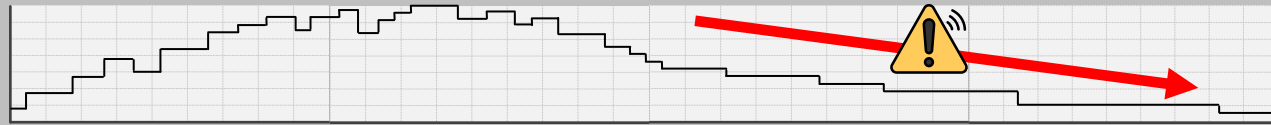
Dev

Metrics Monitoring



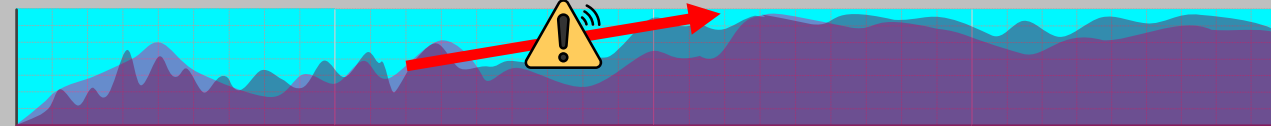
Ops

Sessions Monitoring



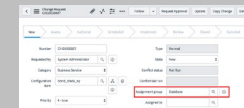
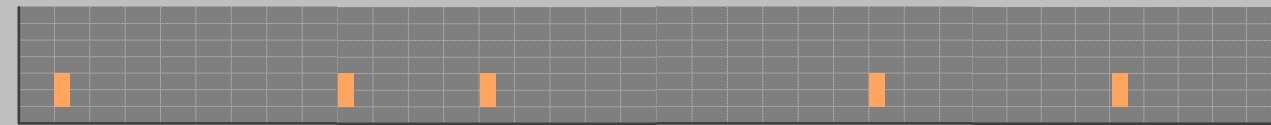
Business

DB Monitoring



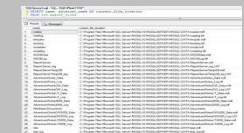
DBA

Change mgnt



Service Mgnt

Log analysis



Problem Mgnt



Connect



Search



Add to cart



Checkout



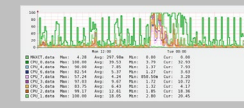
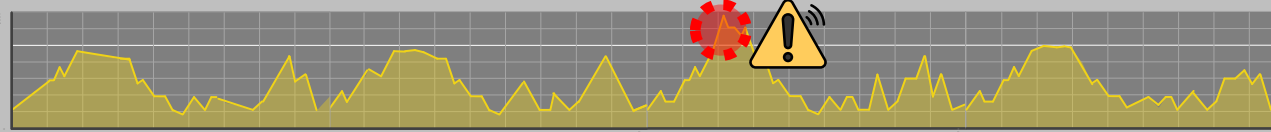
Payment

Tracing



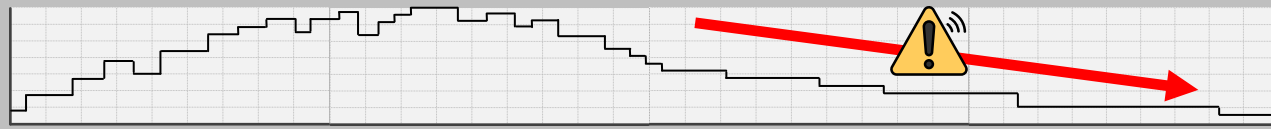
Dev

Metrics Monitoring



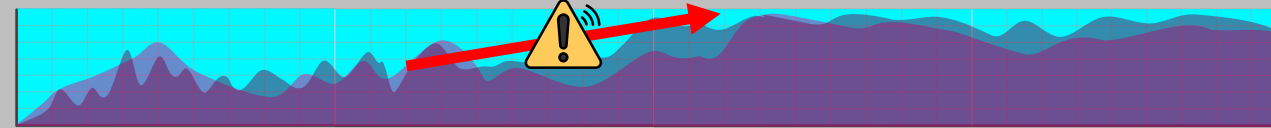
Ops

Sessions Monitoring

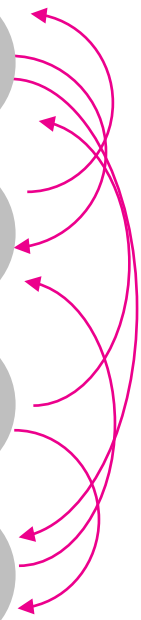


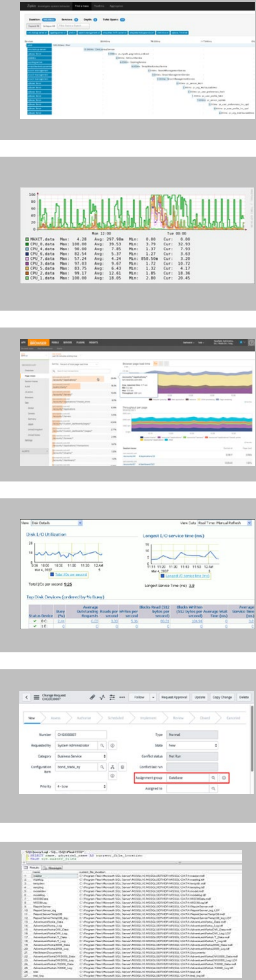
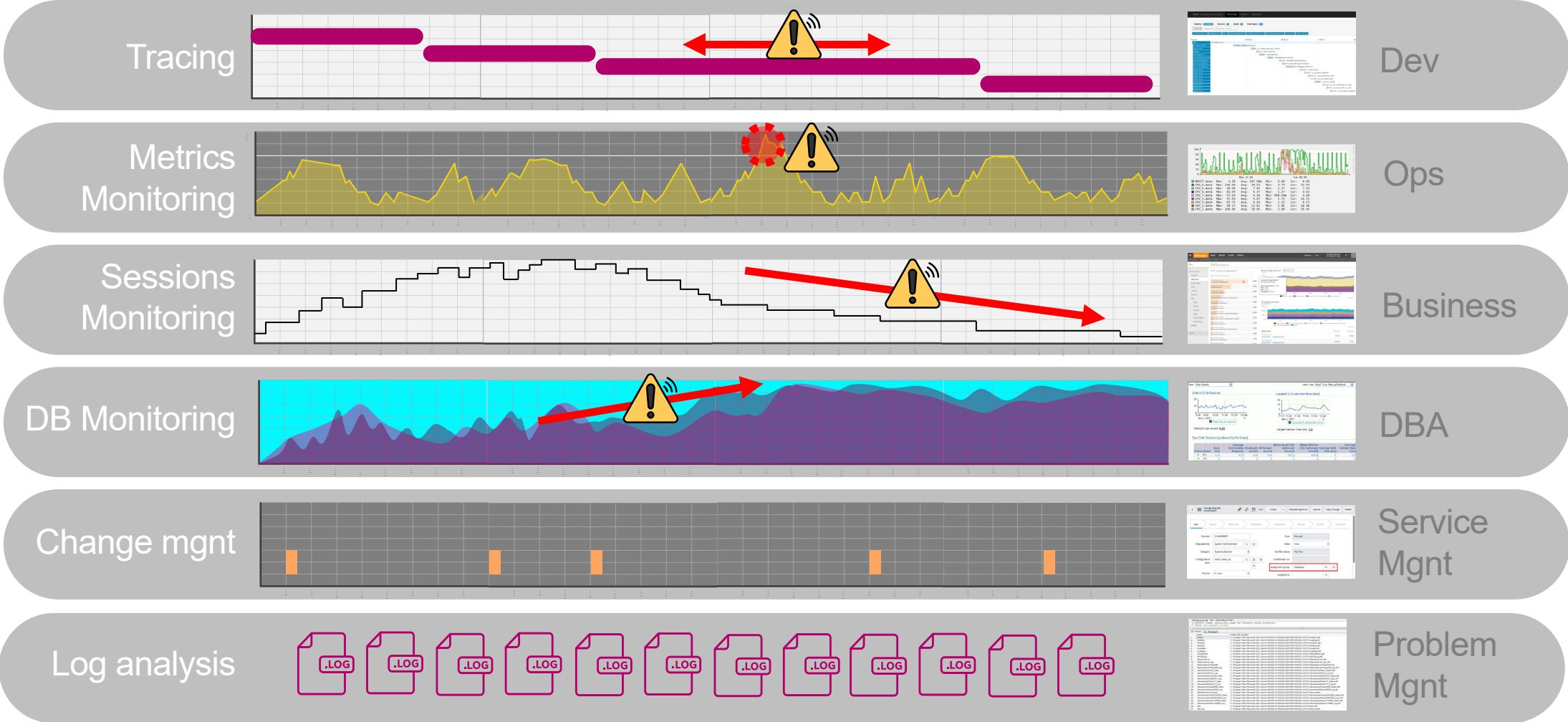
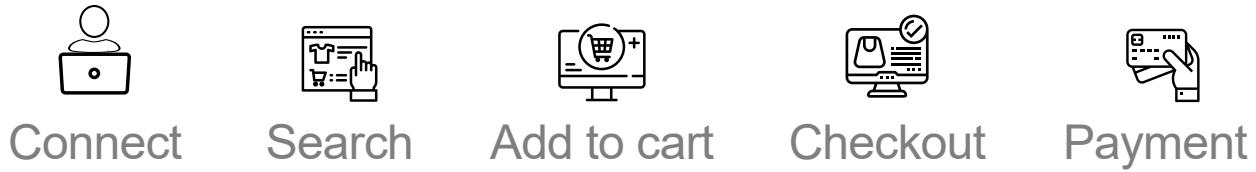
Business

DB Monitoring

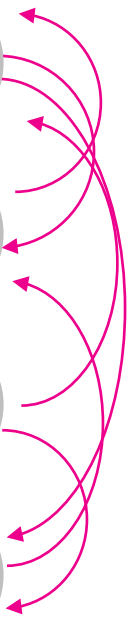


DBA





Dev
Ops
Business
DBA
Service Mgnt
Problem Mgnt





Connect



Search



Add to cart



Checkout



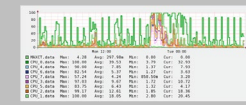
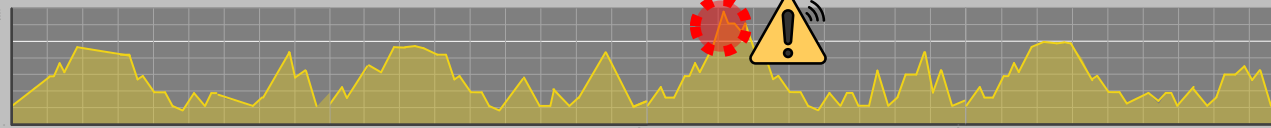
Payment

Tracing



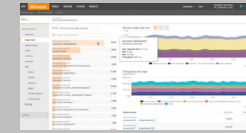
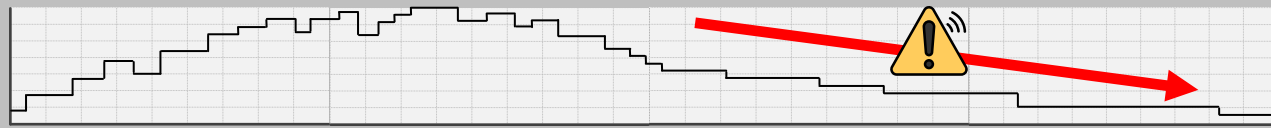
Dev

Metrics Monitoring



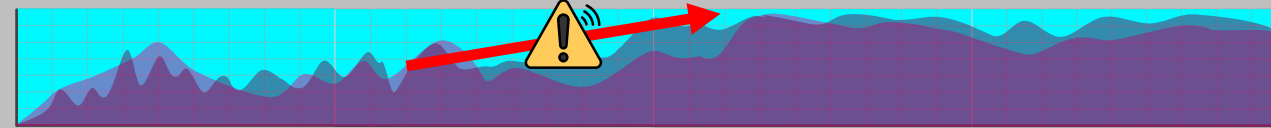
Ops

Sessions Monitoring



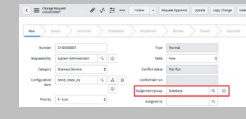
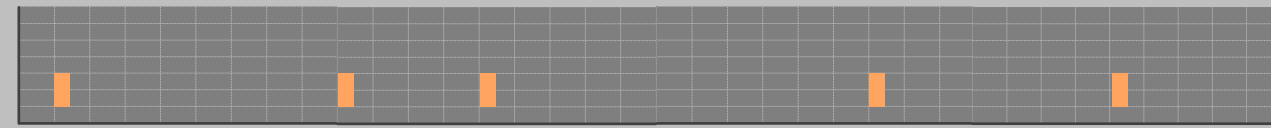
Business

DB Monitoring



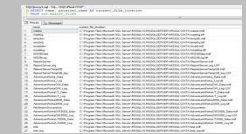
DBA

Change mgnt



Service Mgnt

Log analysis



Problem Mgnt





Connect



Search



Add to cart

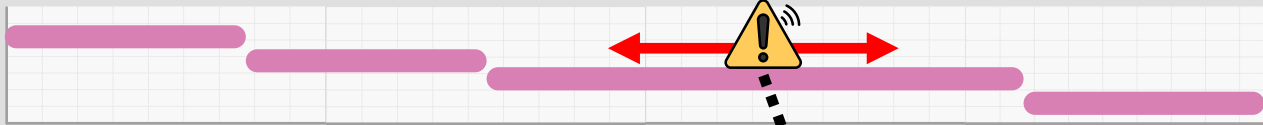


Checkout



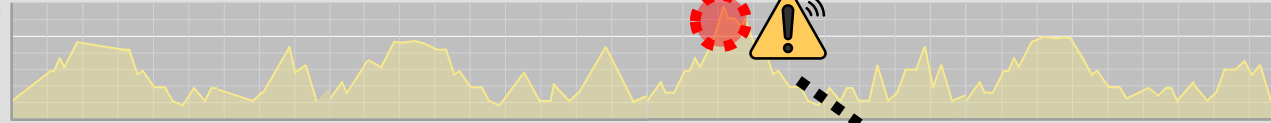
Payment

Tracing



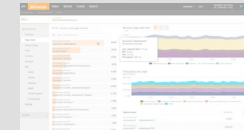
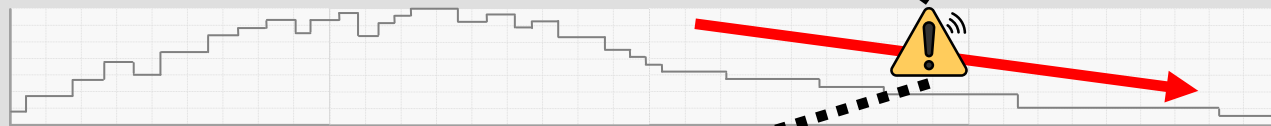
Dev

Metrics Monitoring



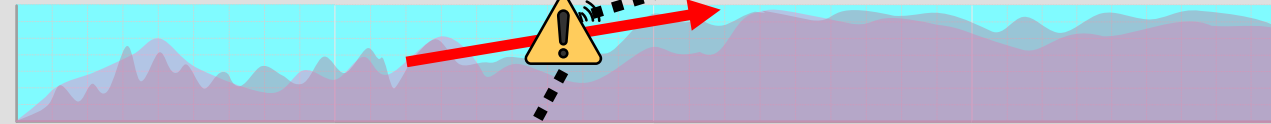
Ops

Sessions Monitoring

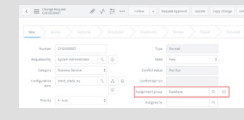
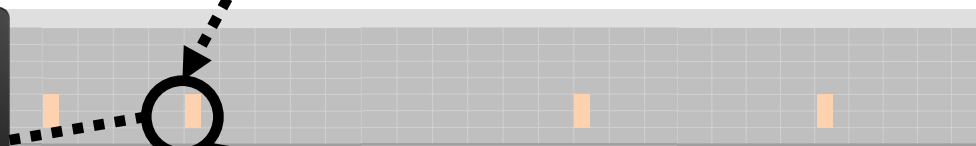
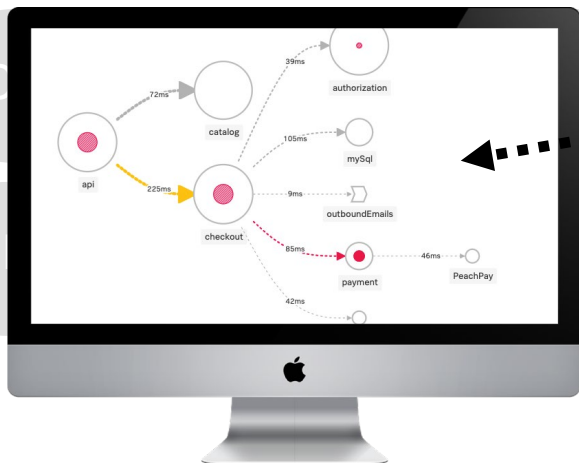


Business

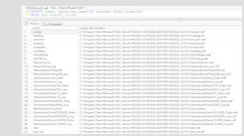
DB Monitoring



DBA

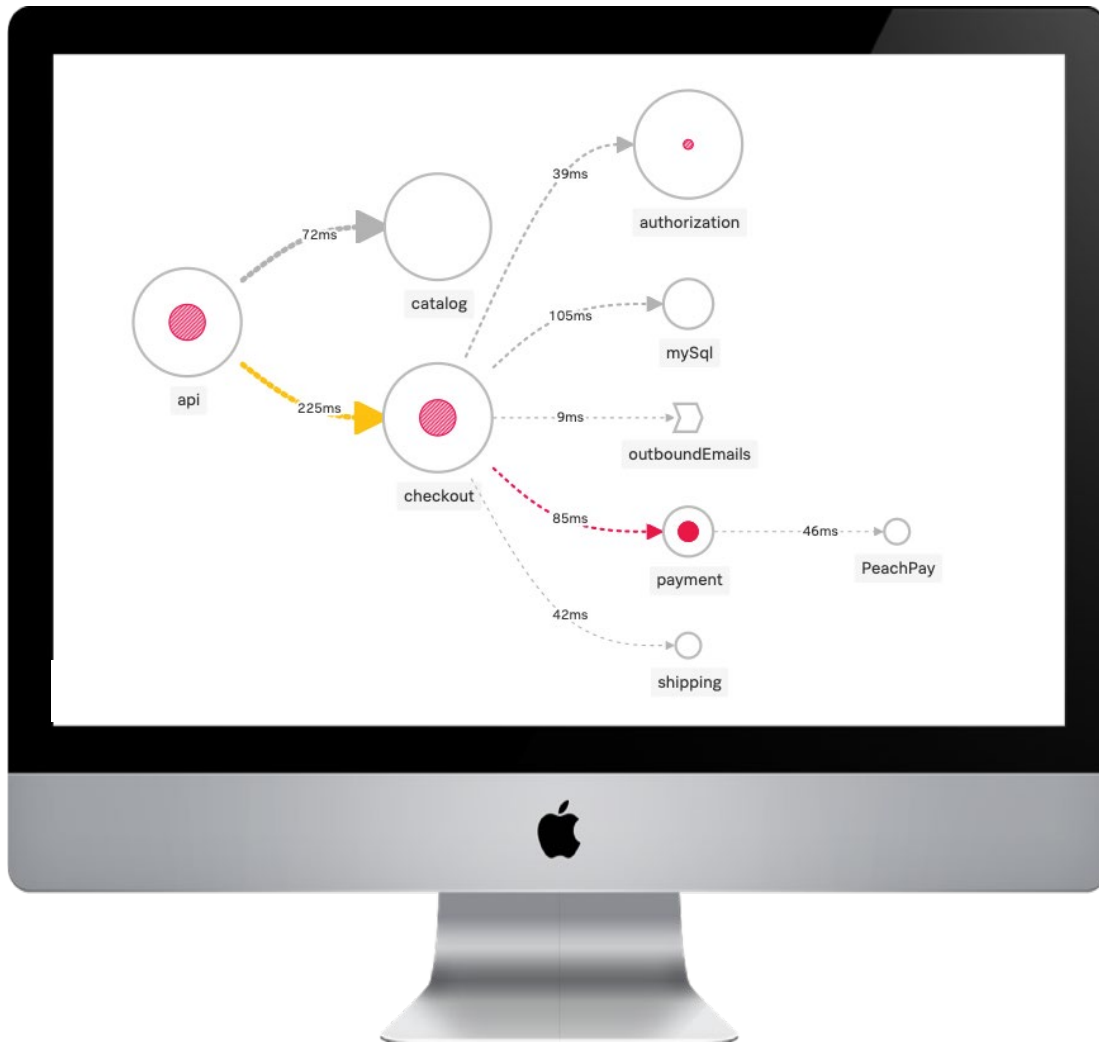


Service Mgnt



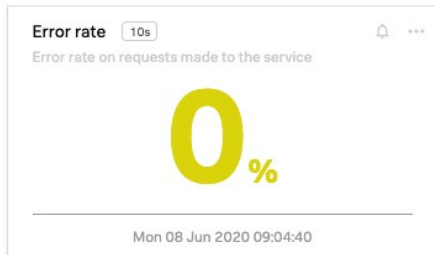
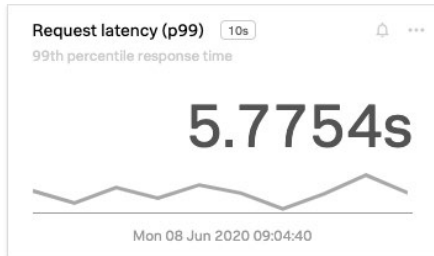
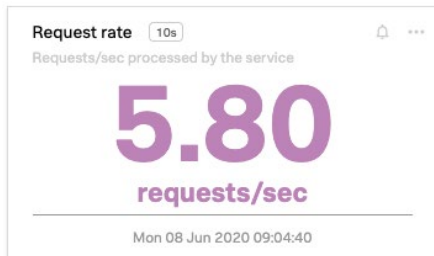
Problem Mgnt

Debug the Unforeseen



- An alert on one service (Monitoring)
- Leads to a timeout error (Tracing)
- Leads to an infrastructure problem (Monitoring)
- Leads to a configuration issue (Monitoring)
- Leads to a memory leak in an app (Logs)

A Customer Happiness Proxy



External (customer's) view is singular

- Request, and its latency and success

Operator's view is over a workload

- Requests latency, rates, and concurrency
- System resources/components



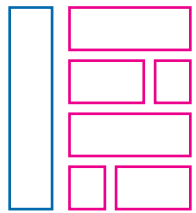
.conf20
splunk>



Why Now?

Cloud-Native Journey Increases Operating Complexity

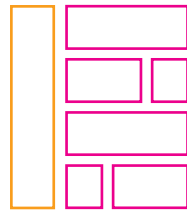
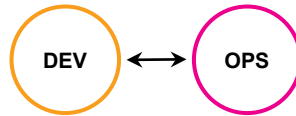
Retain & Optimize



Tightly Coupled Apps,
Slow Deployment Cycles



Lift & Shift



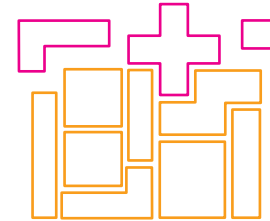
Primarily using
Cloud IaaS



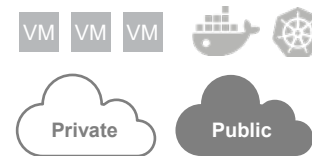
Re-Factor



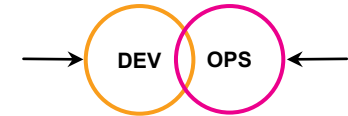
Cloud Managed e.g. RDS,
DynamoDB, SaaS



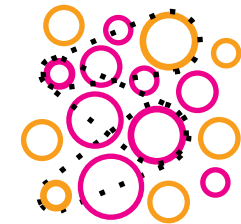
More Modular, but
Dependent App
Components



Re-Architect/ Cloud-Native



Cloud First Architecture



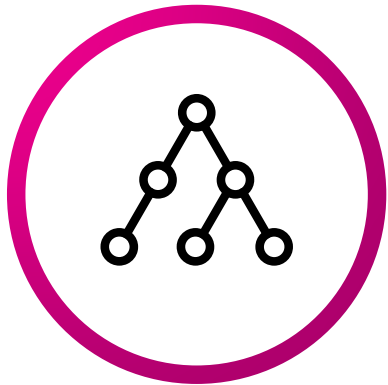
Loosely Coupled
Microservices, and
Serverless Functions



What's Different?

Cloud-native boosts velocity, but also increases complexity

Complex Interdependencies



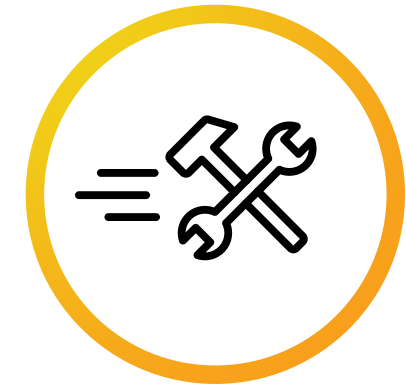
- 10s or even 100s of loosely coupled, polyglot services
- System behavior is unpredictable and changes over time

Elastic, Short-Lived Infrastructure



- Multi-cloud, abstracted infrastructure is extremely dynamic
- Volume of objects and metrics to monitor skyrockets

“You Build It, You Run It”



- Monitoring is not limited to Ops – developers are key users
- No single user has an accurate mental model – troubleshooting is a team sport

“Observability is not the microscope. It’s the clarity of the slide under the microscope.”

Baron Schwartz

Data is the Driving Factor For Observability

AI/ML driven Directed Troubleshooting

Unlimited Cardinality

Streaming/RT data, incl. Monitoring and Alerting

Full-fidelity metrics and traces

Open standards, open source data ingest

Data Collection

Standards-based agents, cloud-integration

Automated code instrumentation

Support for developer frameworks

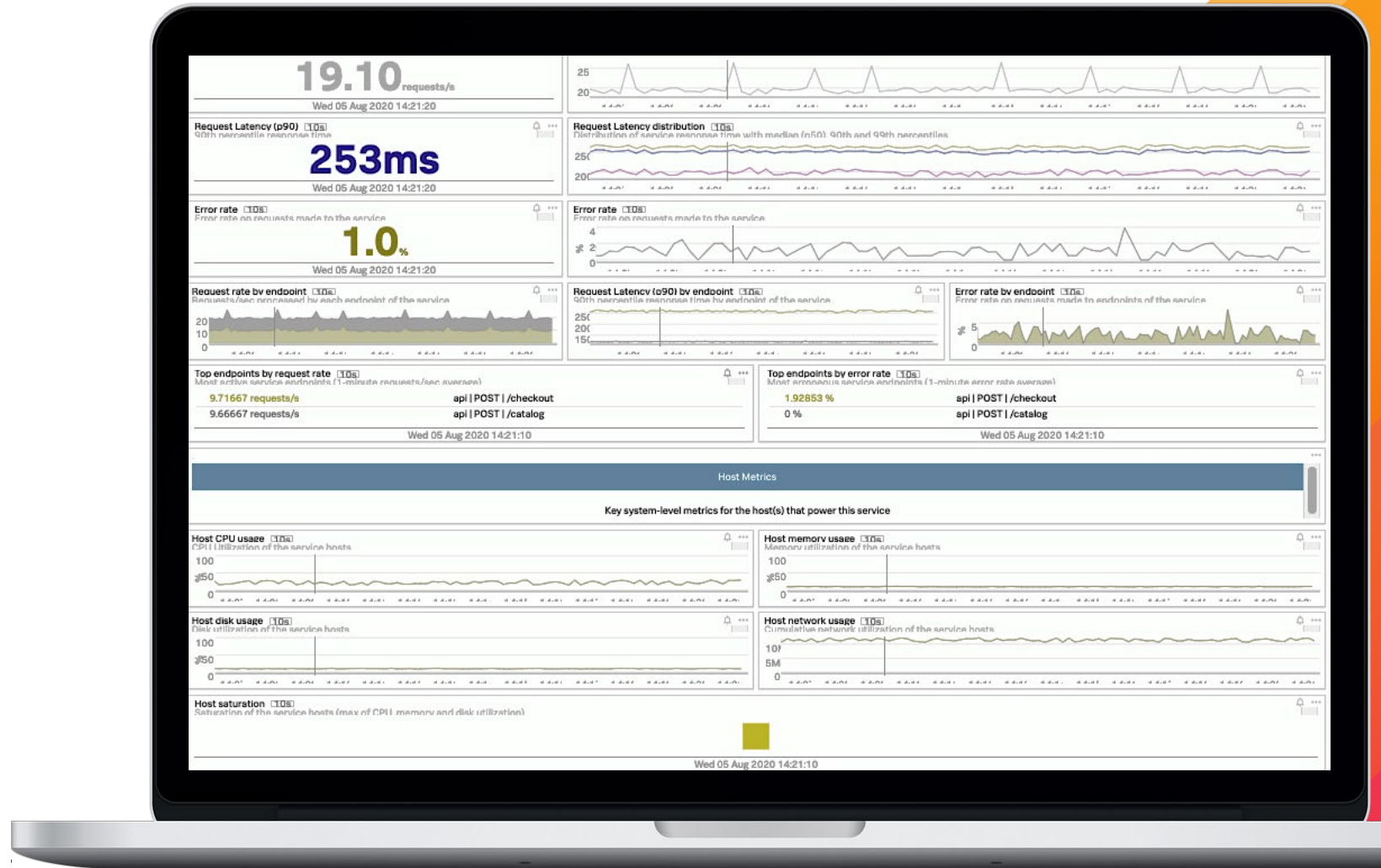
Any code, any time

No cardinality limits



Data Visualization

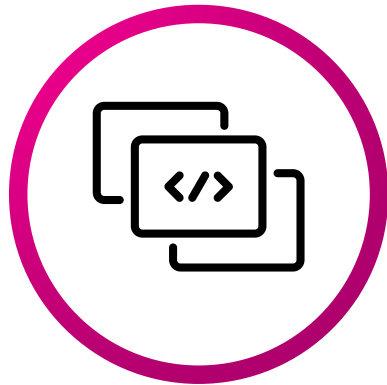
- Monitoring, Analytics, Response tooling
- OOTB and customizable dashboards
- Real-time feeds
- Real-time smart alerting
- No lost data
- And more



Why Splunk Observability

Use all your data and leave no question unanswered

**ALL your data,
any scale**



- Unlimited cardinality metrics
- NoSample™ full-fidelity traces
- No schema, streaming logs

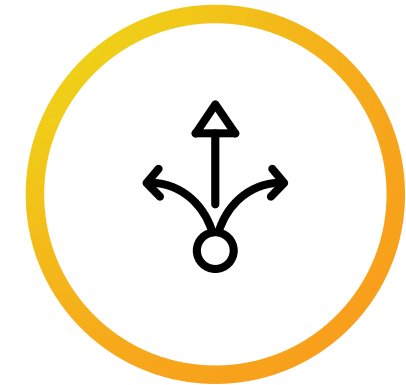
**Open standards
data collection**



- Founder & leading contributor



**Answers & action,
not just data**



- AI-driven directed troubleshooting
- Intelligent & automated response

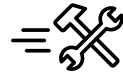
Real-Time, Enterprise-Grade Observability



Monitoring



Analytics



Troubleshooting



Closed-Loop Automation

Service Bureau & Cloud Cost Management

Teams & Permissions | Usage Report | APIs | Mirrored Dashboards

Instant Visualization Real-Time Alerts Deep Business Insights Directed Troubleshooting

Real-Time Streaming Metrics Analytics NoSample™ Distributed Tracing Real-Time Streaming Log Analytics

Open Instrumentation

Metrics Agents | Cloud APIs | Function Wrappers | Tracing Auto-Instrumentation

ON-PREM | PRIVATE CLOUD | PUBLIC CLOUD | CLOUD SERVICES | MICROSERVICES

Fastest Time to Value on Your Data Journey

Real-time streaming analytics for instant insights

Open, Flexible Collection

Open source- and open standards-based instrumentation and data collection

Analyze Data in Flight

Streaming architecture applies advanced analytics to correlate data and find patterns all in real time

AI-driven Insights

Recommendations and directed troubleshooting to accelerate investigation and issue resolution



OBSERVABILITY

All Data, Any Source, Any Scale

Unlimited cardinality metrics, NoSample™ full-fidelity traces and unstructured logs from infrastructure, apps/services and business processes

Immediate Detection

Discover unknown unknowns, catch all outliers and anomalies, alert in seconds

“The most effective debugging tool is still careful thought, coupled with judiciously placed print statements.”

Brian Kernighan
Unix for Beginners 1979

Observability Use Cases

For SREs, platform operators, DevOps teams and developers

Cloud Migration



- Hybrid cloud monitoring
- Cloud cost management
- Cloud capacity planning

Cloud Monitoring



- Cloud services monitoring
- Kubernetes & container monitoring
- Serverless monitoring
- KPI monitoring w/ custom metrics
- Observability-as-a-Service

App Optimization

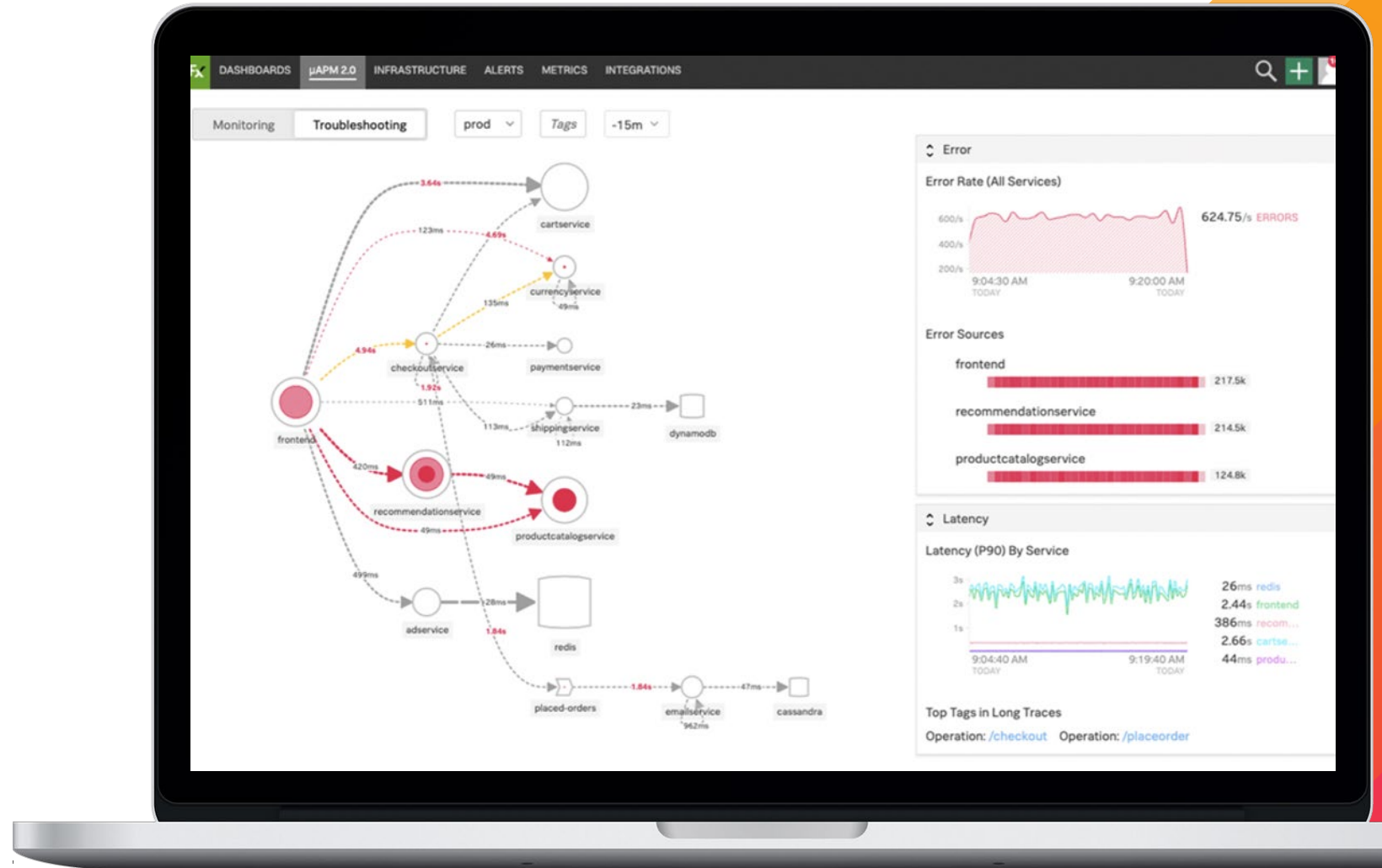


- Application modernization
- Microservices monitoring & troubleshooting
- Business SLx monitoring
- DevOps application lifecycle monitoring

Drive Rapid Innovation

50-70% improvement in developer efficiency

- Detect and pinpoint problems in your applications 60-80% faster with real-time anomaly detection and AI-driven directed troubleshooting
- Identify performance bottlenecks and outages in cloud infrastructure
- Enable your teams to adopt DevOps practices and collaborative workflows no matter where they are in the world



What is Observability Really About?

More productive developers and happier customers

8X

Faster code releases

100X

More visibility
Never miss outliers or anomalies

80%

Reduction in MTTD
Faster detection with alerts in seconds

80%

Reduction in MTTA & MTTR

Key Takeaways

- Observability is based on the acquisition of data that allows you to **ask questions you didn't know** you have and **solve problems that you never thought of**
- Observability is all about data:
At **scale**, at **speed** and **analytics-driven**
- Observability drives new approaches to **monitoring**, **analytics** and **response**
- Start now with the **right tools** to grow with your needs





Thank You

Please provide feedback via the

SESSION SURVEY

