

It's 3 AM. The System is Down. And It's Your Fault.



For Site Reliability Engineers (SREs), this is the nightmare scenario. A critical failure in a massive online system.

Empirical studies show over 40% of cloud incidents are directly correlated to software changes.

The ‘Usual Suspects’ Are Screaming, But Are They the Real Culprits?



Existing Abnormal Change Detection (ACD) methods are noisy. They flag services with obvious symptoms but often miss the true source.

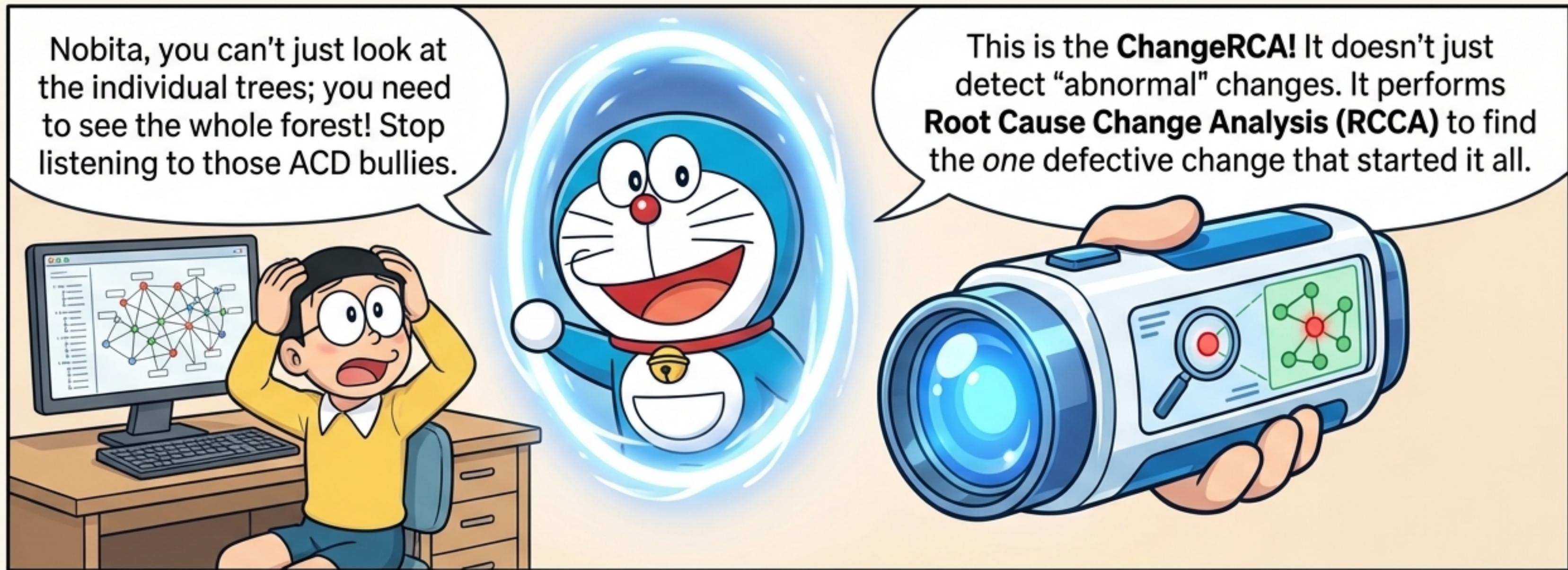
TECHNICAL EXPLANATION: This is **fault propagation**. A 'silent defective change' in one service (the root cause) can create a cascade of failures in other, dependent services (the symptoms). ACD tools often mistake the symptoms for the cause.

Drowning in Data, Lost in the Noise.



Manually identifying the root cause in a system with thousands of services and daily deployments is time-consuming and prone to error. SREs need a better way.

A Better Way to See: The Root Cause Change Analyzer



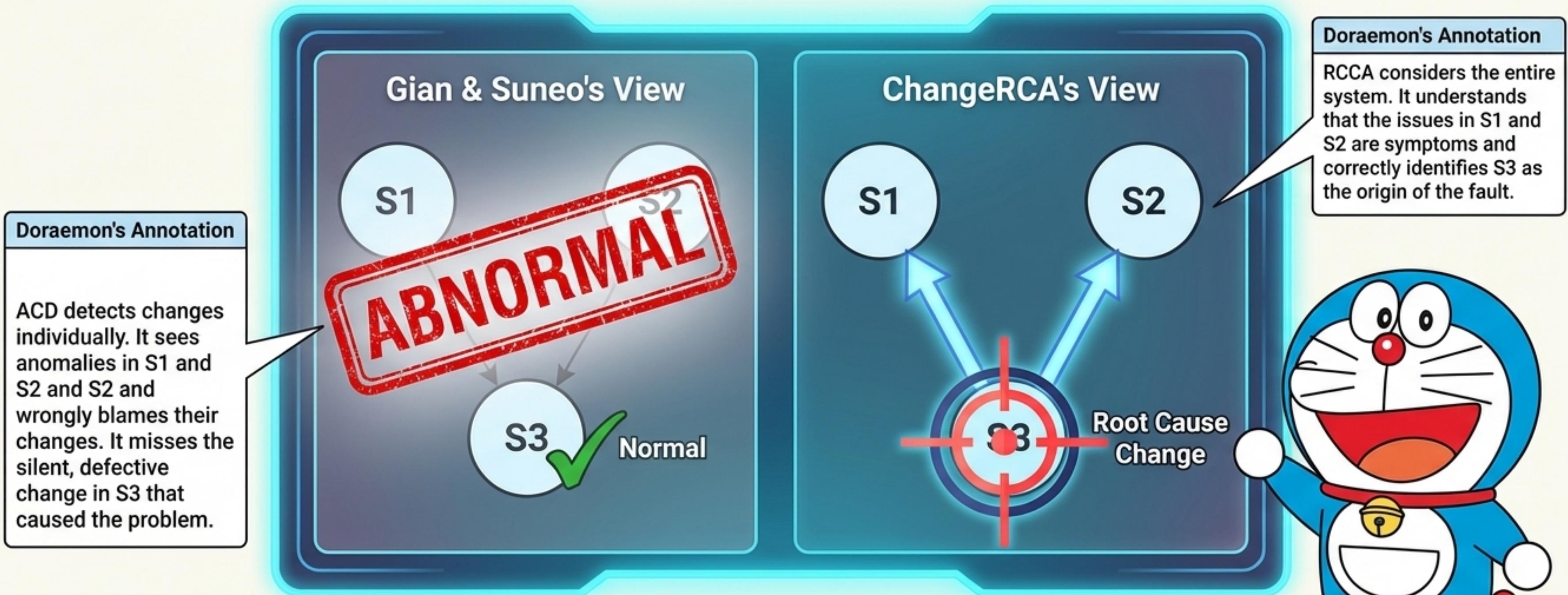
The Old Way (ACD)

Looks at each change in isolation. Prone to false positives from fault propagation.

The New Way (RCCA)

Takes a holistic view. Analyzes interdependencies between changes to pinpoint the true root cause.

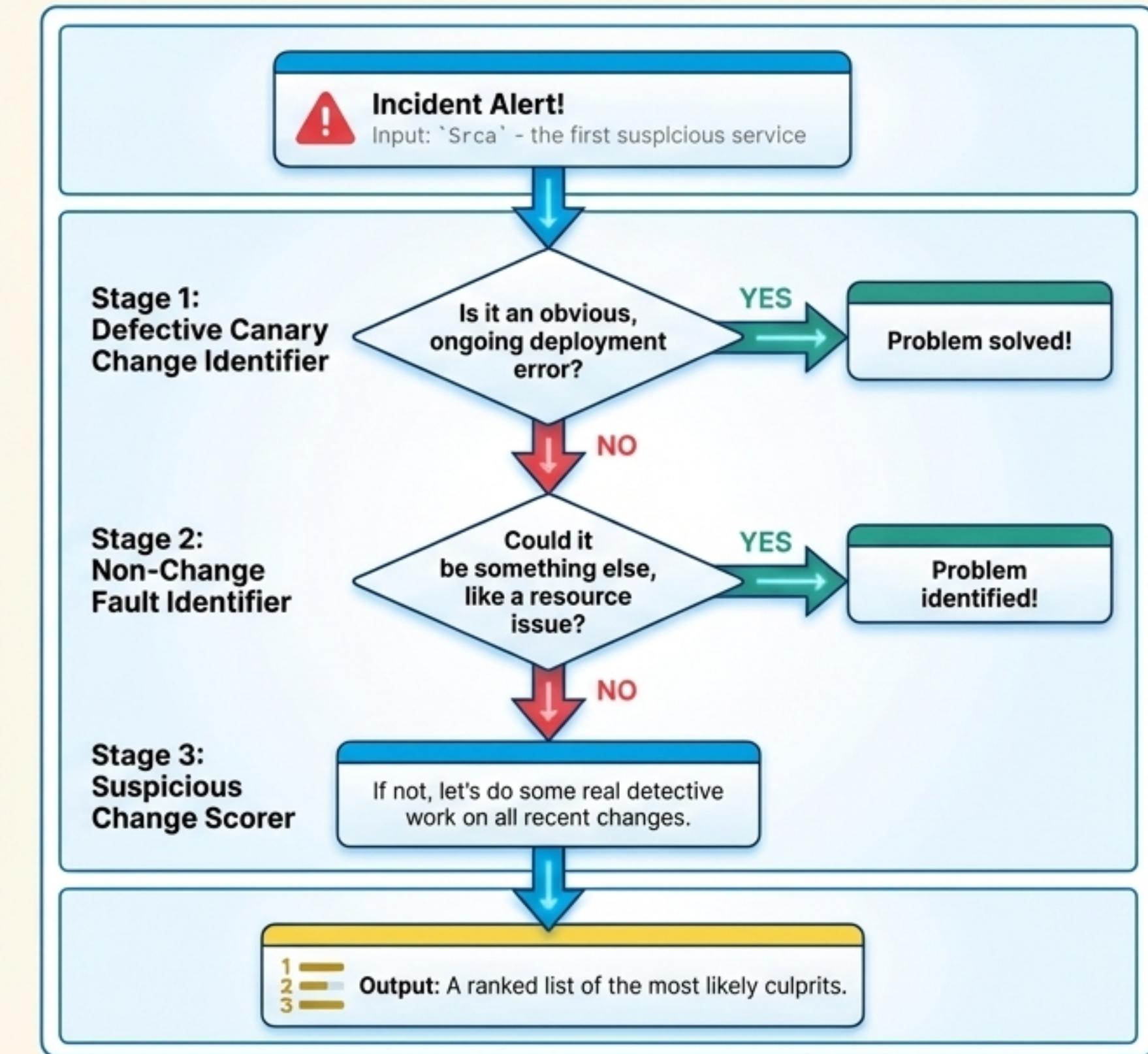
Why Traditional Methods Fail: They Can't See the Connections.



How ChangeRCA Finds the Needle in the Haystack.

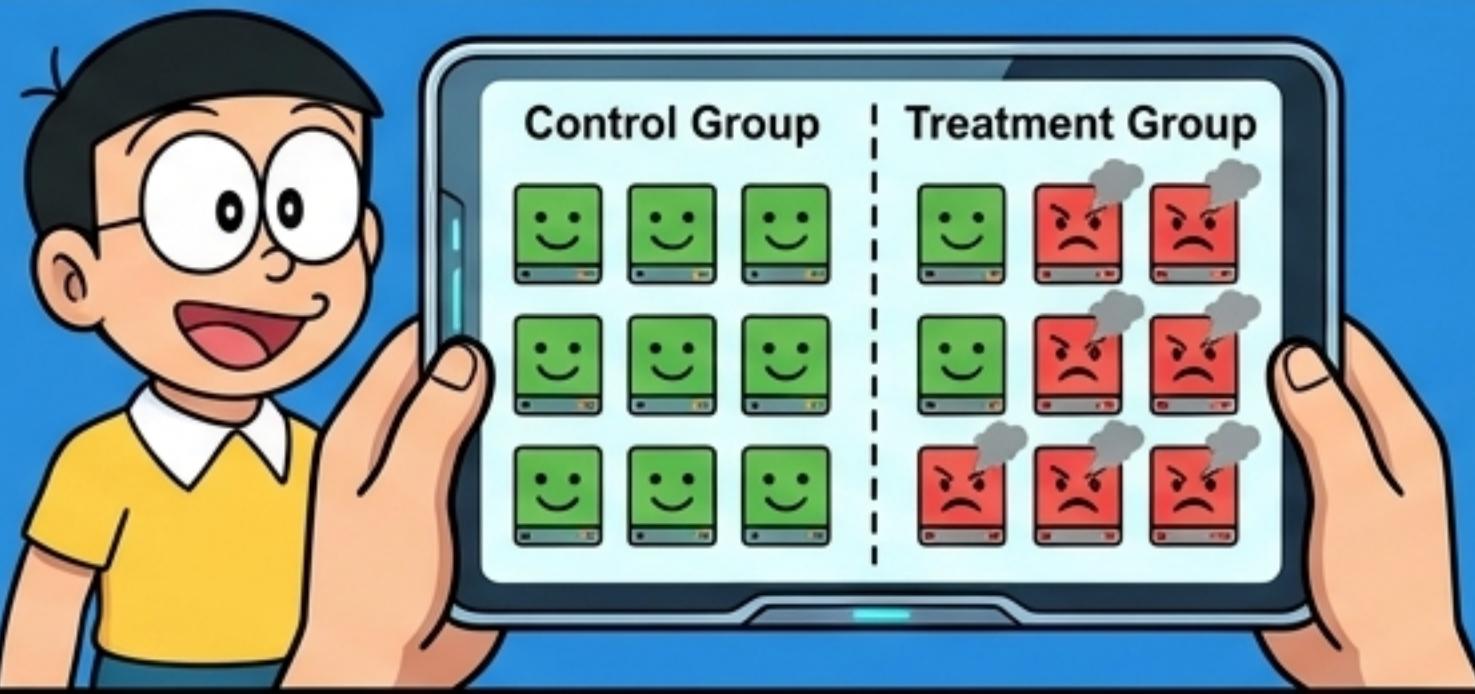


ChangeRCA works like a master detective. First, it checks for the most obvious clues. If those don't solve it, it digs deeper to uncover the hidden connections.

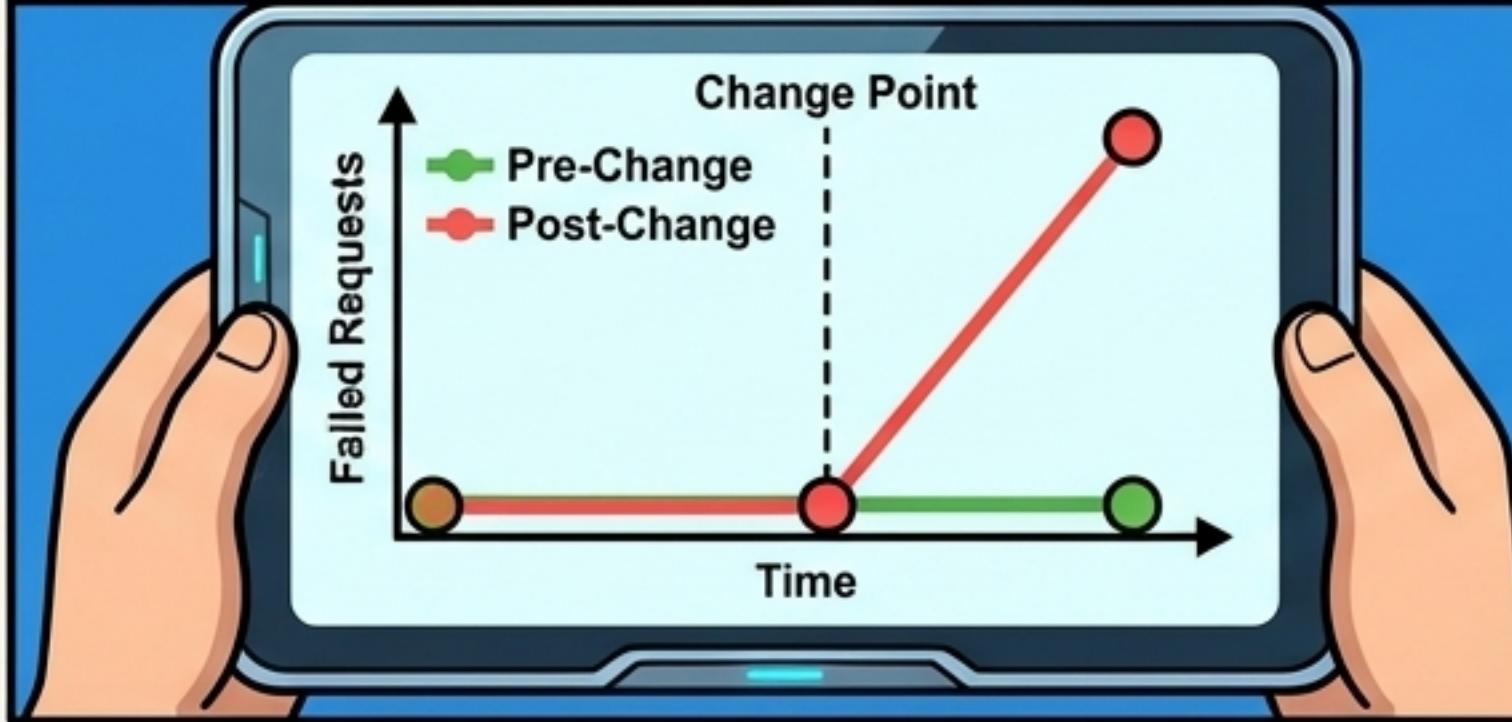


Step 1: Check for a Bad Canary Release

Pre-Change & Post-Change Groups



Failed Requests KPI

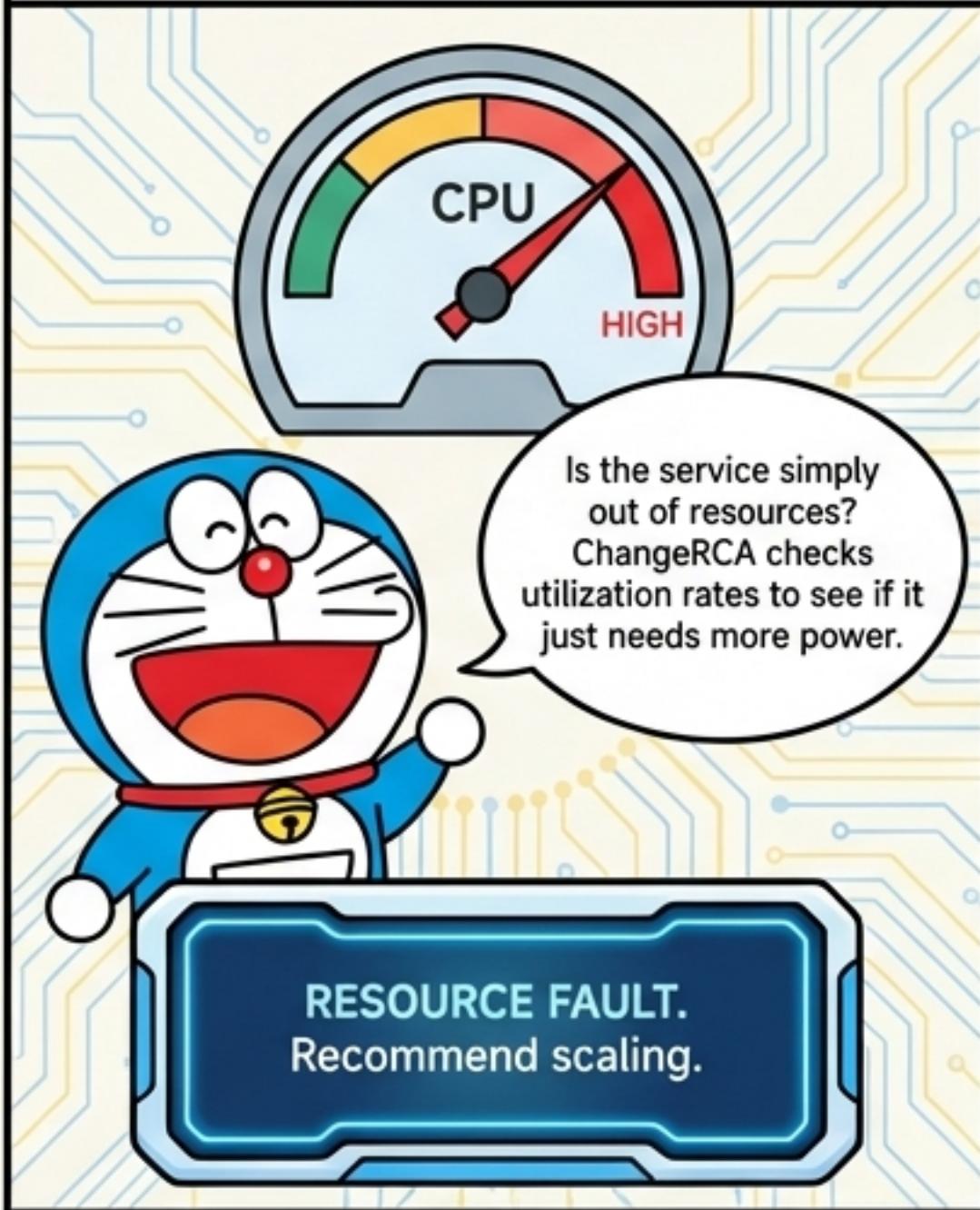


The first thing ChangeRCA does is simple but powerful. It uses a method called **Difference-in-Differences (DiD)** to compare the behavior of instances with the new code (post-change) to those without it (pre-change). A huge difference means we've ~~even~~ likely found our culprit!

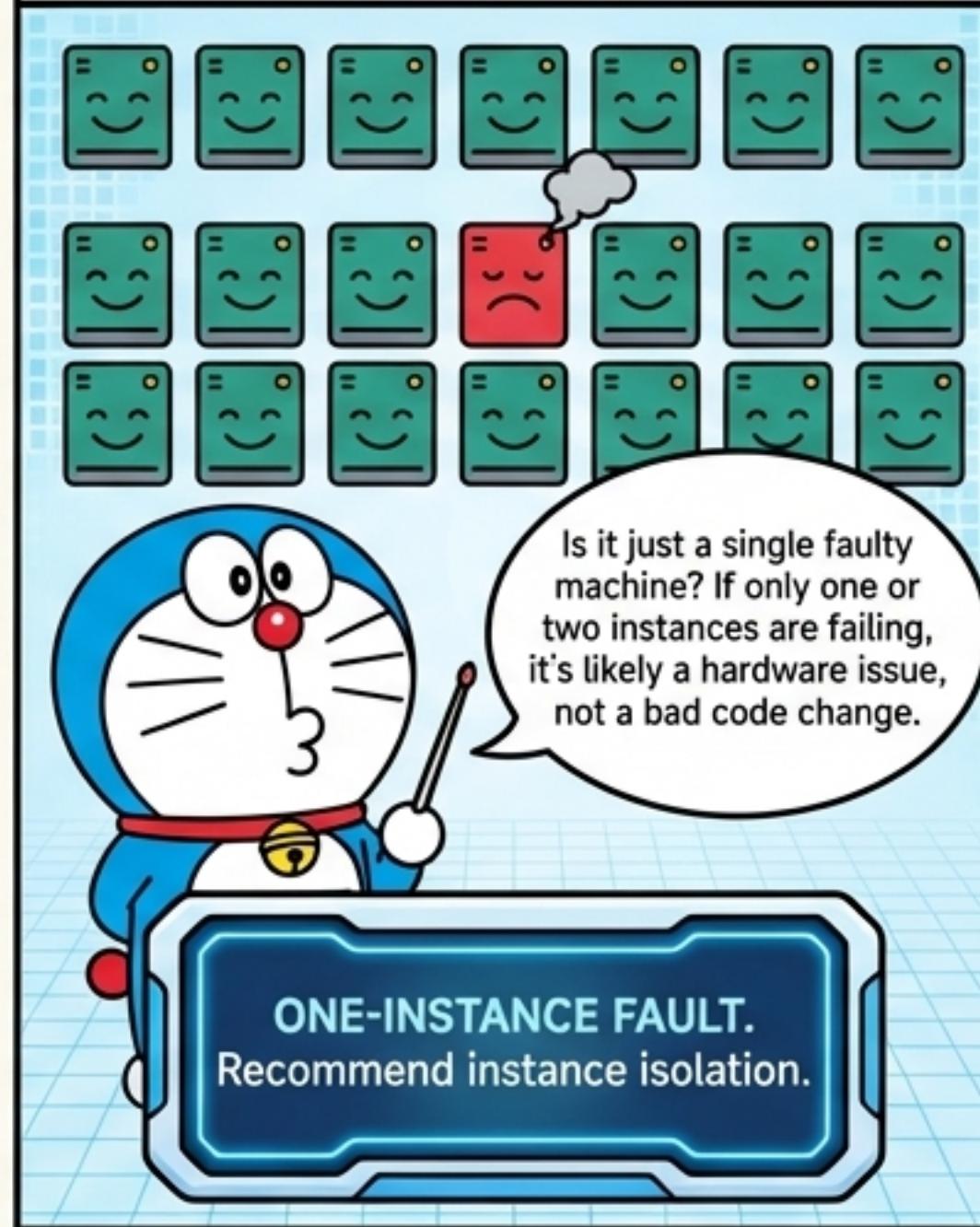


Step 2: Rule Out Common Red Herrings

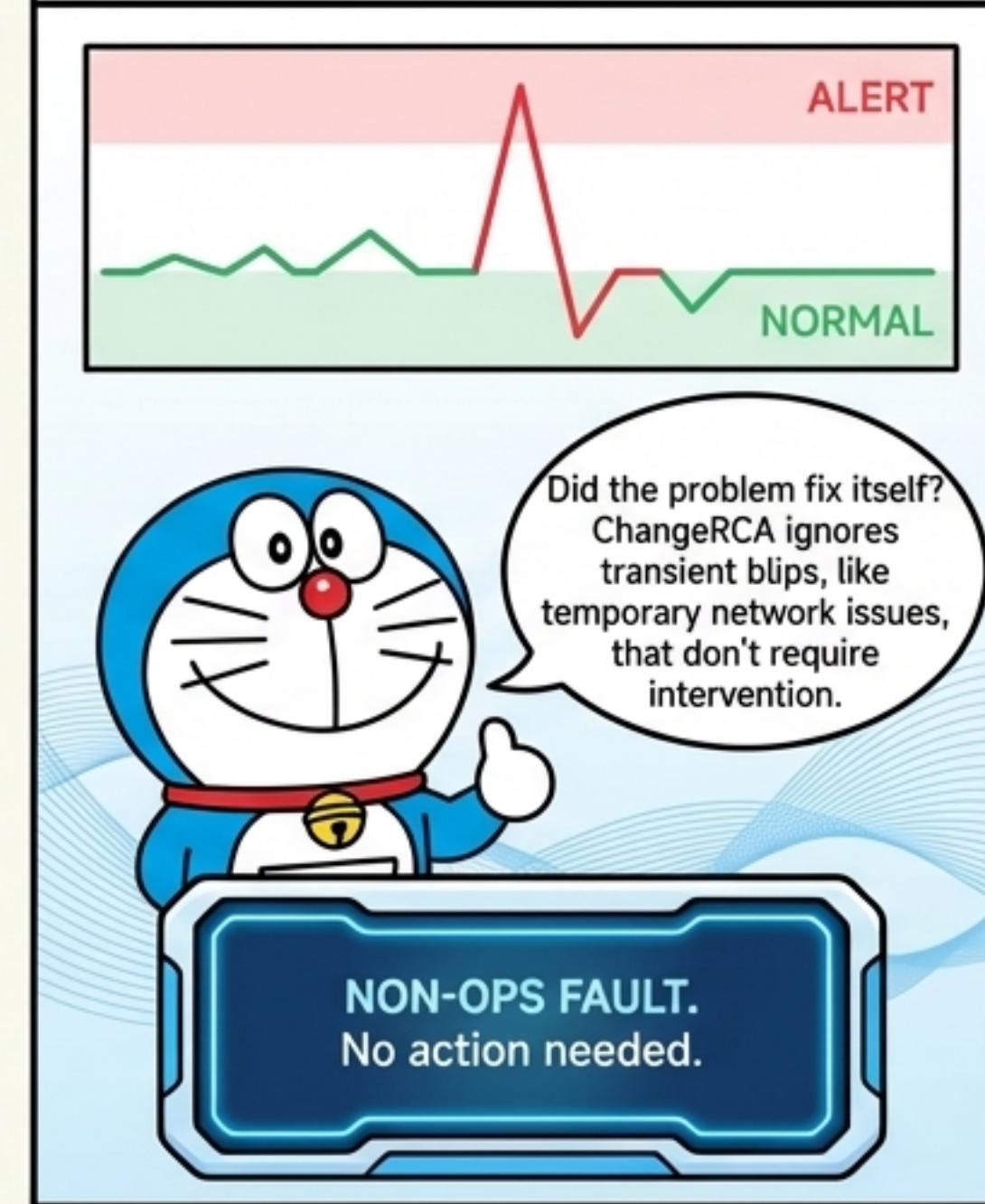
Resource Faults



One-Instance Faults



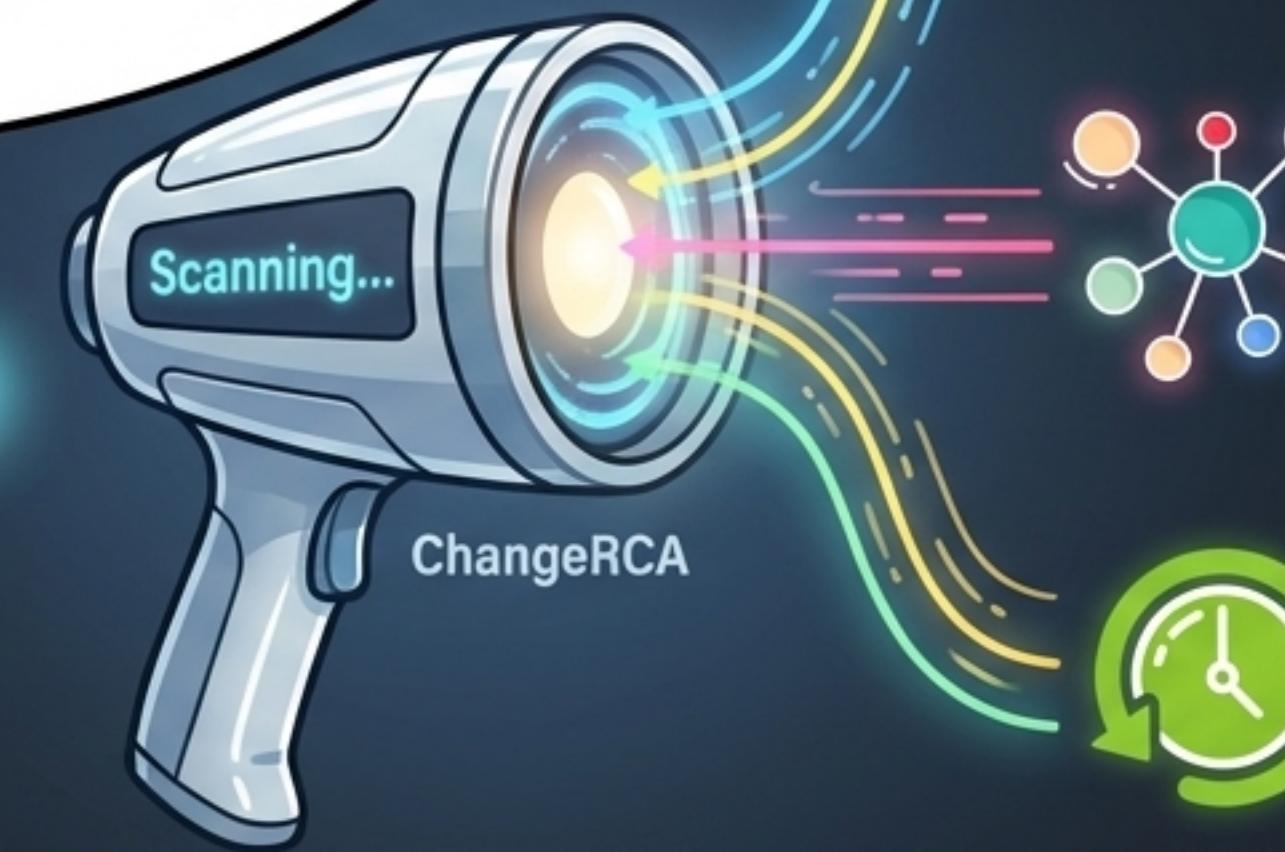
Non-Ops (Transient) Faults



Before hunting for a defective change, ChangeRCA quickly eliminates these common non-change faults, saving SREs from chasing ghosts.

Step 3: The Real Detective Work—Scoring the Suspects.

When the problem is a “silent” defective change, it’s time for the **Suspicious Change Scorer**. It analyzes every recent change in the system’s dependency graph and scores them based on three critical clues.



KPI Score

How abnormal are the service's metrics?



Dependency Score

How closely is the change connected to the failing service?

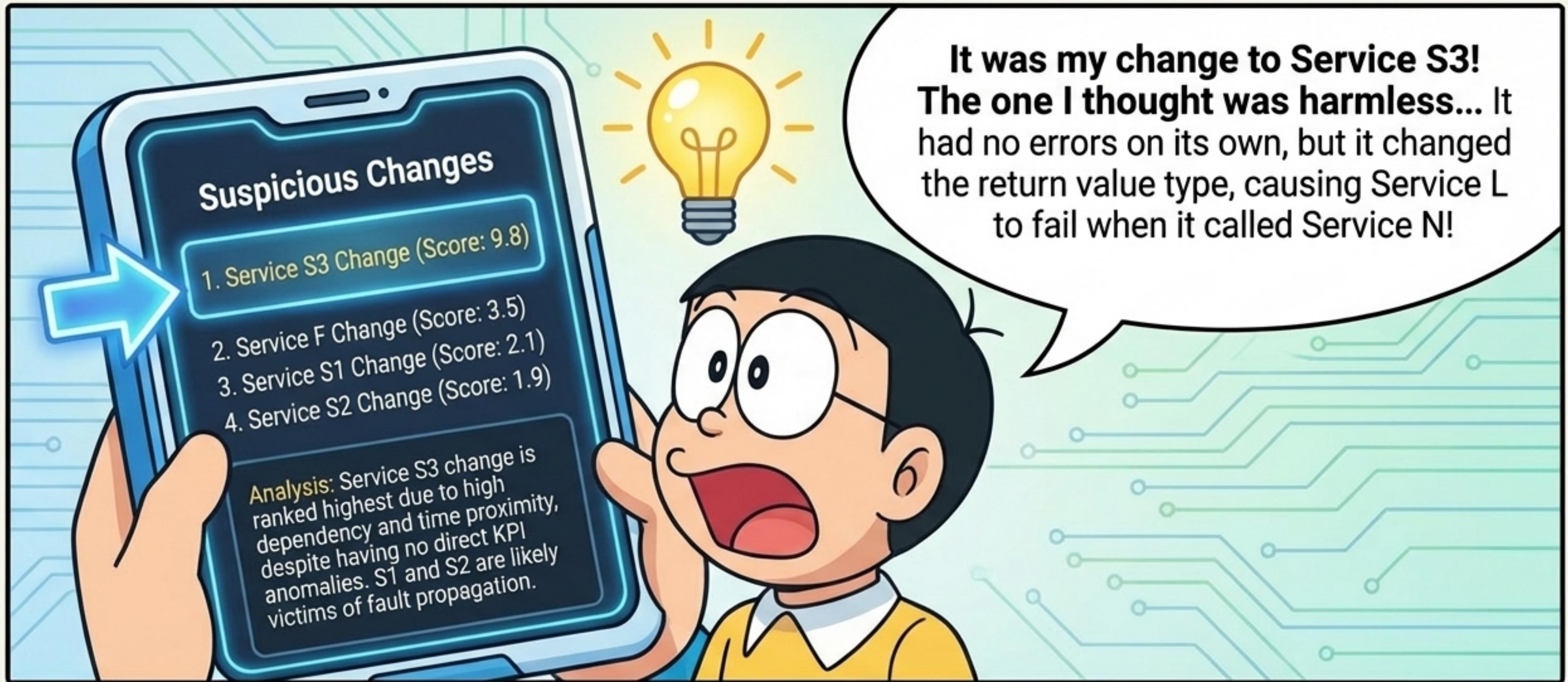


Time Score

How recently did the change occur relative to the incident?

By combining these three scores, ChangeRCA creates a prioritized list of suspects, putting the most likely root cause right at the top.

The "Aha!" Moment: Finding the Silent Defect.



ChangeRCA successfully identified the "silent defective change" that all the other tools missed.

From Crisis to Calm in Minutes

Before ChangeRCA



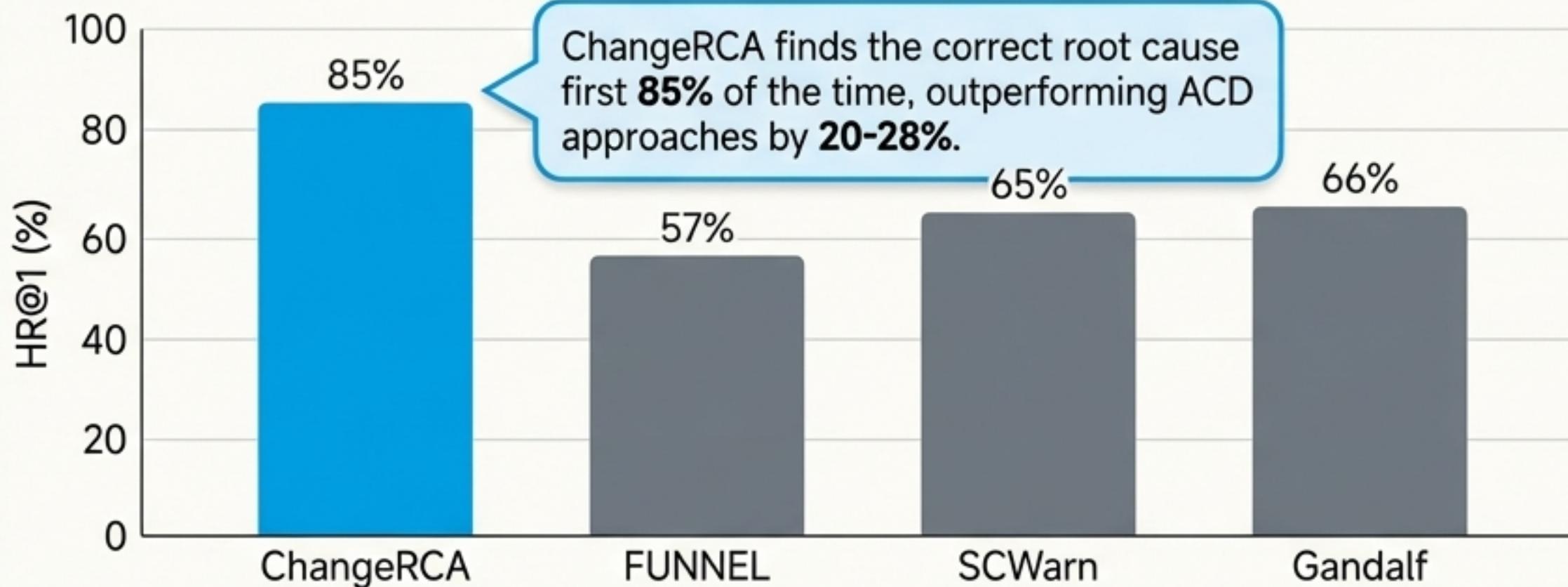
After ChangeRCA



By pinpointing the exact root cause change, SREs can resolve incidents faster, minimizing downtime and improving user experience.

The Story is Great. The Results Are Better.

Top-1 Hit Rate (HR@1) Comparison



96% HR@3

The root cause is in the top 3 results 96% of the time.



90% TTI Reduction

Reduces Time to Identify (TTI) by over 90%, locating 90% of defects in less than 3 minutes.

65% Fewer False Positives

Reduces the average number of false positives SREs must examine by up to 65% (Exam Score from 4.33 down to 1.48).

Stop Chasing Symptoms. Start Analyzing Cause.



“The biggest lesson? Don't just react to the loudest alarm. The most dangerous bugs are often the quietest. To find them, you have to understand the connections between your changes.”



Core Message

ChangeRCA represents a fundamental shift from simple Abnormal Change Detection (ACD) to a holistic **Root Cause Change Analysis (RCCA)**, enabling engineering teams to build more resilient systems.

Call to Action / Further Reading

- To dive deeper into the framework and experimental results, read the full paper: "ChangeRCA: Finding Root Causes from Software Changes in Large Online Systems", Proceedings of the ACM on Software Engineering, July 2024.
- Link: [DOI: 10.1145/3643728]