Moogsoft®
Continuous Assurance

4 Simple Reasons Why Rules-Based Solutions Are Failing IT Operations

How AIOps Liberates IT to Deliver Continuous Service Assurance

EBOOK

SUMMARY

RULES-BASED SOLUTIONS ARE THE PAST. AIOPS IS THE FUTURE.

Managing IT operations is a challenging job that's getting harder. Complexity is growing with exponential speed – especially as enterprises embrace digital transformation via cloud services, virtual/serverless environments, and agile DevOps processes hinging on containers and microservices.

In a large enterprise generating millions of operational events daily, it's clear that enabling continuous service assurance is a task beyond human capability alone. This fact is not new; for decades operations teams have relied on powerful systems

AIOps presents operators only with situations that are meaningful and worthy of human attention. Typically, this eliminates 90% of alerts.

TWEET

and software to manage IT infrastructure. What is new is this universal cry for help by IT professionals swamped with computer-generated alerts whose root cause defies obvious answers.

If humans can no longer effectively process the volumes of data intended to help identify and remediate IT issues, what is a network operator expected to do? This fundamental question leads to another: is your legacy event management tool still up to the job?

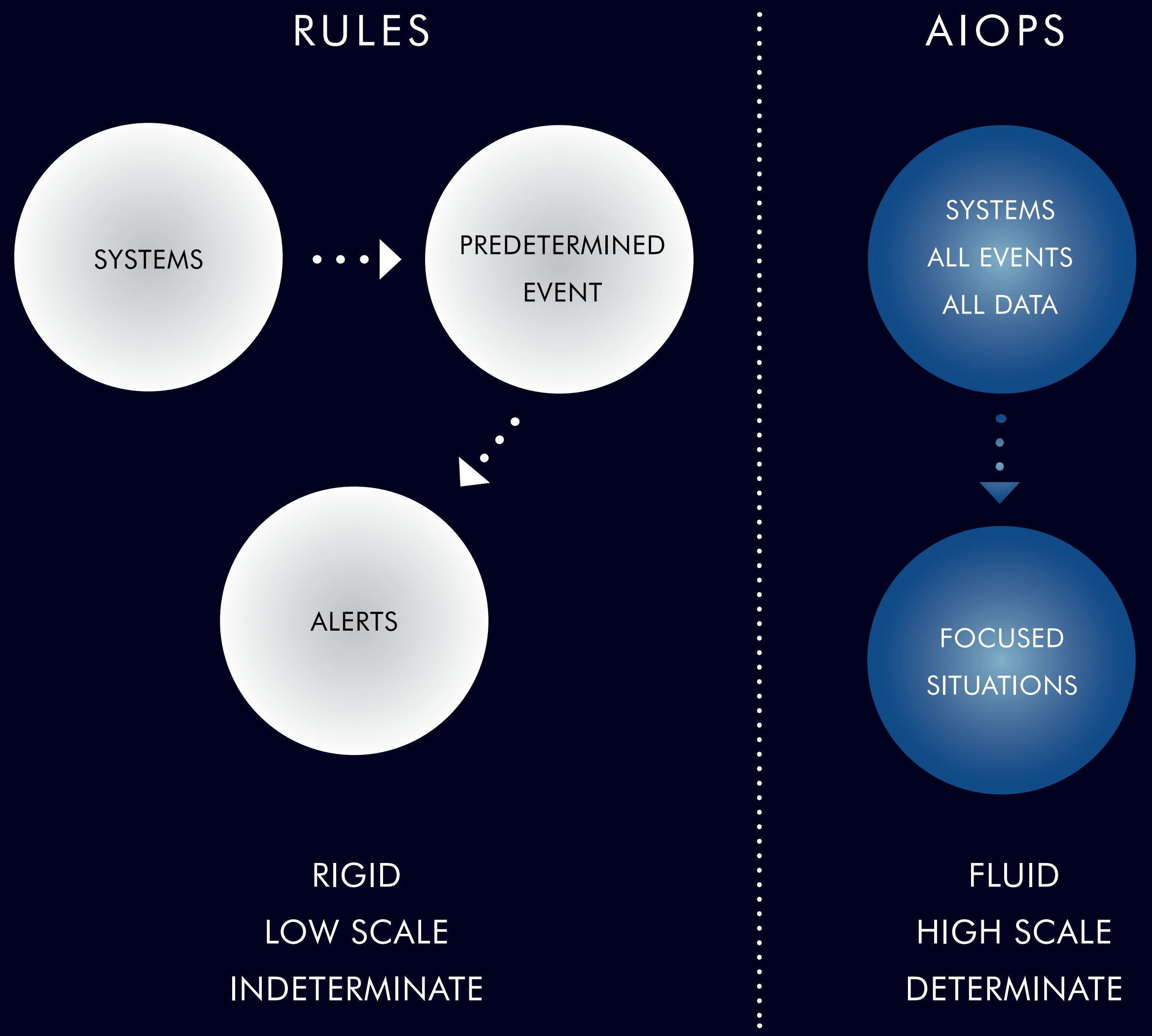
For most enterprises, their legacy tool is based on technology that relies on *rules*.

A rules-based system attempts to assess operational performance with two factors:

(1) pre-determining what the “state” should be for all operational elements at any moment; and (2) “measuring” the state by monitoring operational events, which are used to calculate if the state is correct. If the answer is “no,” the system sends you an alert.

AIOps takes a different approach. Rather than hard-code rules that attempt to identify and predict everything, AIOps simply accepts and enriches all the data for all operational elements at all moments and applies algorithms to automatically gauge state and potential issues. AIOps presents operators *only* with situations that are meaningful and worthy of human attention. Typically, this eliminates up to 90 percent of alerts – and dramatically accelerates spotting root causes for remediation.

This e-book describes the technical limitations of rules-based solutions (some that even attempt to disguise themselves as AI/machine learning) and why AIOps is the intelligent automation of the future.



Rules-based systems separate system state from measurement, complicating root cause analysis. AIOps combines state & measurement, dynamically analyzing situations for cause & effect to speed remediation.

HOW DOES A RULE WORK?

Rules have governed IT operations monitoring and remediation for decades. Seasoned IT Ops professionals probably see a rules-based approach as an old familiar friend. As alerts flow into a traditional monitoring tool, the simple logic of "If this condition exists, then do that..." addresses each issue with ostensibly reliable execution and results.

A rule looks like it what it says. It consists of a fixed input and a fixed output. A set of associated rules attempts to address a black-and-white situation with a binary choice, without ambiguity. Yet what appears to be straightforward is not always the case. The real world is an unpredictable universe of exceptions, which is always the environment in IT Operations.

The tiniest exception to a rule is a deviation from what that rule was designed for. Exceptions mean the rule's logic ceases to work. Any result will be 100 percent wrong – until a new rule is created to address the exception.

One analogy to the way rules operate is the U.S. tax code. On the surface, a law is something for which you either comply or ignore, at risk of penalty. But it's not quite that simple. As with IT Operations, tax laws have many exceptions ("loopholes"). For example, the U.S. Tax Cuts and Jobs Act of 2017 contains 503 pages of new policy. The changes are so big and complex that CPAs are still wondering exactly how they may apply in the real world. The U.S. Treasury Dept. is writing regulations (aka "rules") that will answer some of those questions over several years. By then there will be thousands, possibly tens of thousands of new pages of rules attempting to cover all exceptions under the law.

For IT Ops, a large modern enterprise is getting tens or hundreds of thousands of alerts *every day*. Trying to comprehensively and effectively address all those events with a rules-based approach is quite similar to tax compliance. Gray areas will never disappear with rules.

There are four reasons why rules-based solutions are failing IT Operations.

Let's consider each of them.

REASON 1

BRITTLE RULES FRUSTRATE IT OPS

Rules are becoming brittle, weak and ineffective against the enormous rising tide of operational data in a modern IT infrastructure.

Rules are easy to create. Many are needed to address all known exceptions. This is where managing IT Ops gets tricky. Simply doubling the number of rules from one to two means that those two rules must be 100 percent consistent with each other. Complexity rises exponentially (see chart) as you create more rules within the same set. A typical enterprise architecture can potentially require thousands of rules to manage.

# OF RULES	POSSIBLE COMBINATIONS
5	120
6	740
10	3,628,800
100	n^{157} (157 zeros)

Testing an enterprise portfolio of rules to ensure consistency and accuracy is a major undertaking. Each combination of rules must be verified to avoid false positive alerts or not miss critical incidents. Data scientists call this the NP-complete problem – meaning that no computer exists capable of scaling to this requirement. Let that sink in for a moment.

It's virtually impossible to understand all the effects of alert exceptions in a collection of rules.

Rules are especially weak at finding and predicting the probability of unknown unknowns, which are potentially crippling, unusual IT events the enterprise has never witnessed or experienced before. Enterprise IT Ops teams need as much certainty as possible to take decisive action. Rules-based solutions leave IT infrastructure vulnerable to the unknown.

KEY TAKEAWAYS

- ✓ Rules have illusion of simplicity
- ✓ Rules bring exponential complexity
- ✓ Rules do not address unpredictable events
- ✓ AIOps relies on algorithms, not rules

In IT Operations, It's virtually impossible to understand the effects of alert exceptions in a collection of rules. AIOps effectively identifies anomalous events in a flood of alert data.

TWEET

AIOps Looks for Patterns, not Rules

With AIOps – which combines artificial intelligence with machine learning – IT Operations teams are able to process all incoming event data in a manner that is tolerant to exceptions, without the limitations of rules. AI algorithms analyze the data to know when something is an unusual *feature* of the event. This information is used to automatically create profiles of normal behavior and spot deviations or anomalies that may signal trouble.

The human brain's methodology for processing data provides a scalable model for AIOps, which uses very similar algorithms. No training of the system is required. AIOps algorithms are a sophisticated way of clustering all the individual IT events across monitored infrastructure into a single correlated incident, eliminating the noise of alert storms.

AIOps replaces the uncertainty of brittle rules by quickly and effectively spotting event patterns and flagging critical incidents triaged by priority. The unanticipated is no longer a disruption. More large enterprises are turning to the data science of AIOps for a clearer insights and control over the chaos.

SEE MORE ON BRITTLE RULES

READ NOW ▶

REASON 2

RULES ARE EXPENSIVE

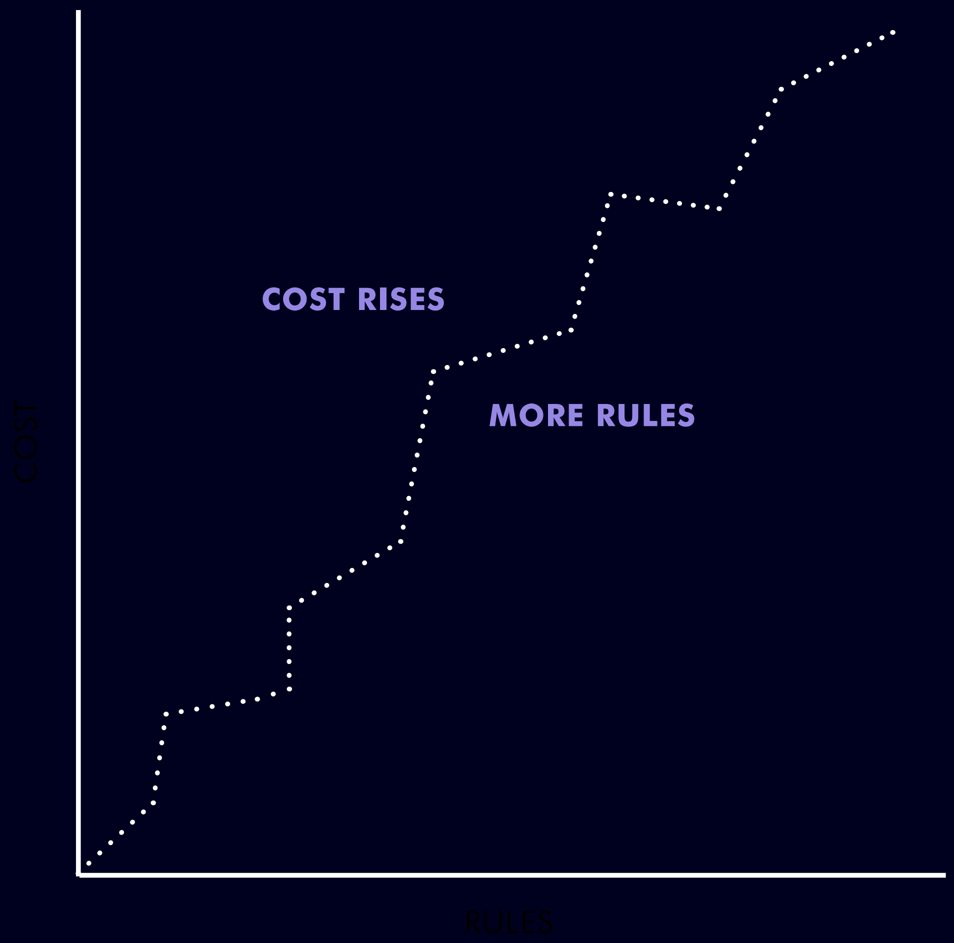
The process of maintaining rules is complex, costly, risky, and may actually impede incident resolution.

Rules punish you with hidden complexity and cost. They look simple, which implies cheap. But the true cost of rules entails a never-ending process of creating, checking, and revising them. A complex enterprise infrastructure requires a large number of rules. Rules-based solutions rapidly become a maintenance problem of gargantuan proportions.

Rule maintenance requires keen insight on the interactions and nuances of a rule set. The technical knowledge and operational experience needed for effective maintenance is beyond Level 1 operators. Be prepared to focus expert consultants (i.e. expensive resources) on this continuous challenge.

There simply is no practical or cost-effective way to reliably maintain all rules. When rules don't work as intended, or when conflicts between rules arise, their accuracy suffers. The IT operations team becomes inundated with irrelevant alerts. To address alert fatigue, well-meaning analysts may even turn some rules off. This action makes them more reactive than proactive to system issues. The result is that costs rise while availability and downtime suffer.

Most severe outages do not begin with a critical alert. So filtering "irrelevant" rules in favor of critical alerts won't work. Major incidents usually start with a low-severity alert. Turning off certain alert rules to tame the problem means issues will go undetected for a longer duration. By the time an incident turns critical, network operators never saw the issue coming. It's too late. Forget rules. The cost of downtime is the worst cost of all.



Maintaining rules is a never-ending process that grows in number, complexity and cost over time – as system experts try to cover every possible scenario.

AIOps Eliminates High Cost of Rules

AIOps is more cost effective than rules. Self-learning algorithms automatically assess all the operational data in your enterprise and tell you which events matter. This approach eliminates the futile treadmill of writing more and more rules trying to cover every potential scenario. A rules creation process is manual, menial, time consuming and expensive – especially when done by Level 2 and 3 domain experts and engineers.

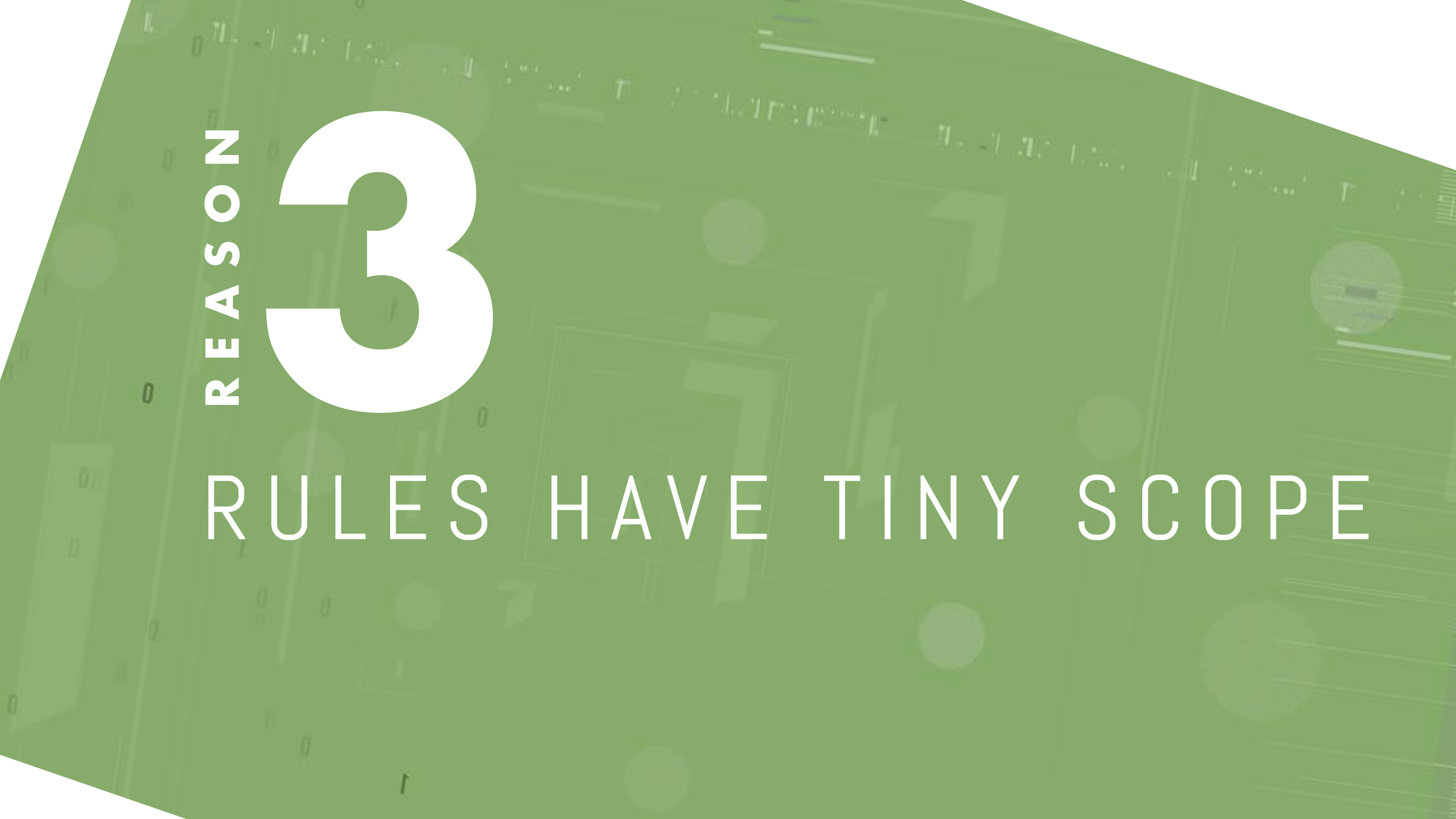
By eliminating the hidden costs of rules, AIOps also does a much better job of safeguarding system performance. Your enterprise saves the unspeakable risk and cost of system outages and downtime. AIOps automates the entire data ingestion and analysis process, quieting the noise to let teams focus on remediating only the most critical incidents. The valuable savings in time, cost and effort allows IT Ops to deliver continuous service assurance.

KEY TAKEAWAYS

- ✓ Rule maintenance is expensive
- ✓ Rules have hidden complexity and cost
- ✓ Rules can hinder detection and remediation
- ✓ AIOps solves these issues

SEE MORE ON THE TRUE COST OF RULES

READ NOW ▶



REASON 3

RULES HAVE TINY SCOPE

Rules-based approaches to managing IT Operations are limited in scope, inaccurate, and unpredictable as complexity grows.

Rules-based approaches to managing IT Operations are limited in scope, inaccurate, and unpredictable as complexity grows. Rules have a fundamental flaw that impedes their predictive accuracy: their tiny scope. “Scope” is defined as the potential range of IT events that may affect system performance.

An analogy useful to understand scope is a daily commute to work. For IT Operations, an individual rule is like a solo commuter. It’s simple to say, “If alert A occurs, then the solution is B.” Conclusive, highly predictable results are only available when the scope of operational variables is small (akin to commuting on empty roads).

But the reality is that a metropolitan area is a large, complex system where the random actions of thousands of independent decision-making drivers produce reliably unpredictable results. In other words: gridlock! Frustration abounds because unpredictable traffic clogs our solo commuter's most efficient route.

The intrinsic chaos of commuting is another example of NP-complete (described in Reason #1). City gridlock is so complex to compute that it can never be solved. If the commuter problem for 10 cars could be worked out on a laptop, solving for 100 cars would take all the available computing power on planet Earth!

Enterprise networks are nothing like empty roads. They easily generate thousands, even millions of alerts every day. The scale, complexity, and potential combination of events generated dwarfs the decision problem posed by our commuting analogy. With rules, scope is so limited that there is no way to ensure accurate results. Hence the peril of relying on rules to guarantee IT service delivery.

KEY TAKEAWAYS

- ✓ Rules have predictable results in simple environments
- ✓ Rules results are unpredictable in complex environment
- ✓ The scope of rules guarantee they will not work in large IT environments
- ✓ AIOps avoids the limits of rule scope for accurate predictions of emergent behavior

AIOps Liberates the Limits of Scope

Using artificial intelligence for IT Ops instead of a rules-based approach avoids the constraining limits of scope. AIOps frees IT Ops teams from the need to create rules for every possible situation. These intelligent solutions apply AI and machine learning to operational data flows from infrastructure monitoring tools, ingest all alert traffic, and automatically apply algorithms that determine which events matter and which don't. Unlike a rules-based approach, AIOps improves incident response over time, without having to account in advance for every input and output.

The result of using AIOps is greater accuracy in detecting and resolving critical incidents before they cause crippling outages or downtime. AIOps keeps IT Ops teams – from Level 1 operators to Level 3 engineers – working efficiently at peak productivity. The unique capability of AIOps to cluster alerts into incidents also helps detect anomalous behavior. This is a big problem that cannot be solved with legacy rules-based tools shackled by limited scope. AIOps provides a reliable, more predictable path to prevent applications and services from operating below service level agreements.

SEE MORE ON THE TINY-SCOPE OF RULES

READ NOW ▶

REASON 4

RULES ARE UNDECIDABLE

Some system failures amount to real-world problems that don't have a clear yes-or-no answer.

In a past of physical data centers and on-premise hardware, a rules-based legacy event management system was adequate. But rules fall flat in today's complex environment of microservices, containers, virtual servers and cloud storage.

The problems that rules try to solve are themselves undecidable. In computational theory, an "undecidable problem" is a decision problem for which it is impossible to construct an algorithm that always leads to a correct yes-or-no answer.

To illustrate, let's consider downstream suppression, a common but important use case for enterprise IT infrastructure monitoring. Ambiguity arises when servers are connected by a switch that fails. Monitoring those servers triggers phantom pings, so rules provide inaccurate information for diagnosis. A rule is then needed to ping switches to distinguish what is really down. This scenario shows how simple rules quickly grow into complex rule sets in order to account for all potential variations of interdependencies.

Now what happens if the whole data center loses power? A rules-based solution has no way to distinguish between false positives and real failure. The situation is ambiguous. It's *undecidable* – because rules cannot guarantee to fully determine the most likely root cause.

In an interconnected enterprise with 1000s of servers, tens of 1000s of apps, and millions of virtual connections – a rules-based system is flooded by undecidable scenarios.

SUMMARY

- ✓ Rules-based solutions cannot guarantee to fully determine or decide the root cause of a system failure.
- ✓ The random circumstances of real-world failures often confuse undecidable rules and delay remediation.
- ✓ Unlike a rules-based system, AIOps teaches itself without having to account in advance for every input and output.

Rules cannot guarantee to fully determine or decide the probable root cause of IT system failures. Only AIOps liberates IT Ops from rules by learning over time using contextual and historical data, patterns and probabilities.

TWEET

AIOps Replaces the Undecidable with the Probable

Painful lessons learned from real-world outages prove that many rules-based solutions are not adequate to maintain continuous service assurance. IT Operations staff need greater visibility, contextual and historical data, incident probabilities, and likelihood of failure. All these insights can be used to determine probable root cause of any incident.

Ironically, most IT Ops managers know this. Teams working with rules-based systems are awash in symptomatic alerts that don’t mean anything. They waste manual effort and suffer added expense, while customers endure poor quality of service. AIOps operates independent of the undecidability of rules.

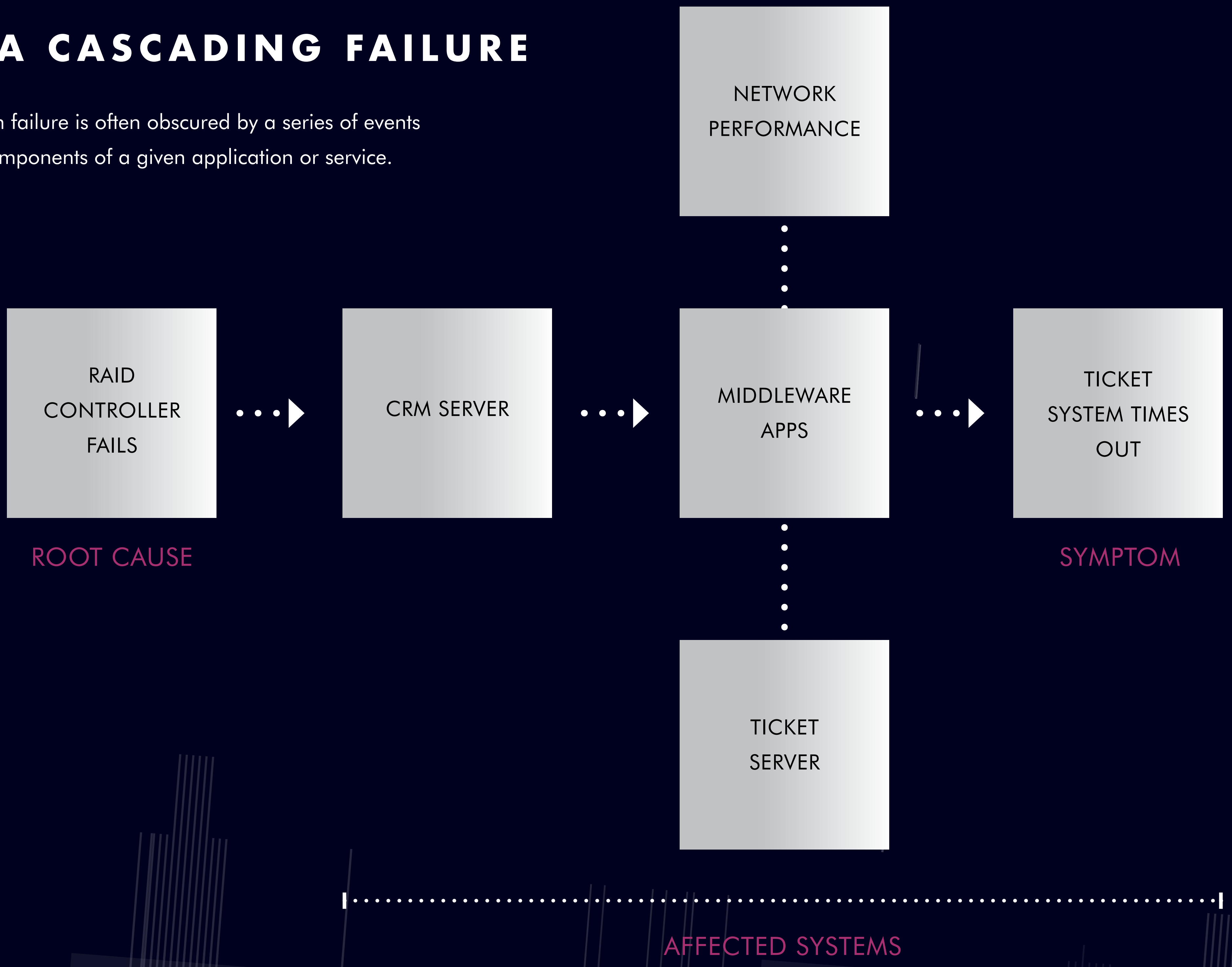
These intelligent solutions ingest all operational data and apply algorithms to automate the detection and triage of important incidents.

SEE MORE ON UNDECIDABLE RULES

READ NOW ▶

ANATOMY OF A CASCADING FAILURE

The root cause of a system failure is often obscured by a series of events that impact multiple components of a given application or service.



AIOps Liberates IT from Rules to Deliver Continuous Service Assurance

Simply put, rules are a thing of the past. AIOps is the intelligent automation of the future.

AIOps allows you to detect incidents that a rules-based system might have missed. AIOps is a mathematical approach of statistical machine learning based on algorithmic logic. One algorithm can replace the logic of hundreds of thousands of rules. Processing incoming event data happens in fractions of a second. Algorithms are deterministic – meaning that they always produce the same output, regardless of input. The same algorithm can infer one type of incident from other types of incidents, contextually or historically. Algorithms themselves are error-resistant and don't need to have all of the data to make reliable conclusions.

Moogsoft has large enterprise IT Ops customers that are already reaping huge benefits from AIOps. The new approach is enabling them to accelerate mean-time-to-resolution of operational incidents, improve service assurance for customers, simplify the management of cloud infrastructure, and more effectively manage digital transformation initiatives.

It's time for IT Operations to move beyond the antiquity of rules-based legacy solutions and put the modern machine-learning of AIOps to work. It is a better approach for delivering continuous service assurance to the enterprise.

AIOps is essential for ensuring the peak performance of modern IT infrastructure. It liberates rules-based legacy solutions and guarantees continuous service assurance for customers.

TWEET

ABOUT MOOGSOFT

Moogsoft is a pioneer and leading provider of AIOps solutions that help IT teams work faster and smarter. With patented AI analyzing billions of events daily across the world's most complex IT environments, the Moogsoft AIOps platform helps the world's top enterprises avoid outages, automate service assurance, and accelerate digital transformation initiatives. Founded in 2011, Moogsoft has more than 120 customers worldwide including SAP SuccessFactors, American Airlines, Fannie Mae, Yahoo!, and HCL Technologies. It has established strategic partnerships with leading managed service providers and out-sourcing organizations including AWS, Cisco, HCL Technologies, TCS and Wipro. Moogsoft® and the Moogsoft logo are proprietary trademarks of Moogsoft Inc. All other products or names may be trademarks of their respective companies.

Moogsoft® and the Moogsoft logo are proprietary trademarks of Moogsoft Inc. All other products or names may be trademarks of their respective companies.

For more information about Moogsoft's AIOps platform and its newest addition of customers, visit www.moogsoft.com, read our Blog or follow us on Twitter and LinkedIn.