EVOLVEN

Prevent Problems Using Four-Dimensional Observability

Reduce Risk, Improve Customer Experience, and Innovate Faster using Evolven with an APM Solution

AUTHOR

CHARLEY RICH
FORMER GARTNER ANALYST &
EVOLVEN TECH STRATEGIST

"There are really four dimensions, three which we call the three planes of Space, and a fourth, Time". –
Albert Einstein

Introduction

Enterprises today face an agonizing paradox. They need to excel at two essential requirements that are often in conflict: speed and control. They need to "go faster"' to innovate but need control to ensure quality and mitigate risk. As a result, most "move slower," become less agile, and opt for quality over innovation. The business, however, demands both.

An APM/observability, full-stack solution (later abbreviated as just "APM") integrated with Evolven can help transcend this paradox and ensure applications deliver the business value they were meant to.

Modern applications, whether in the data center or spanning hybrid clouds, are highly dynamic and composable, regularly changing to continue to capture customer demand. Gartner predicts that "Composable application architecture empowers such adaptability, and those that have adopted a composable approach will outpace the competition by 80% in the speed of new feature implementation".

However, this dynamic, composable architecture adds complexity and new opportunities to fail to deliver the intended value. In concert, APM integrated with Evolven tells the user exactly what's wrong, what's changed in the context of the most probable root cause, and whether the severity indicates they must act immediately to resolve an issue. APM detects something is incorrect, determines where the problem is located, and then passes this information to Evolven to identify the related actual changes that are the most probable root causes of these issues.

APM and Evolven add a fourth dimension to the standard definition of observability which only focuses on the three dimensions of logs, metrics, and traces. Observability, as commonly understood, is limited and utilized to reduce the impact of problems that have already occurred. While a modern concept for monitoring complex systems, it still fits into the "build-fix-repair-repeat" cycle of reactive maintenance.

The Four-Dimensional solution of APM and Evolven adds an aspect that observes and analyzes changes, who made them, when they occurred, if they were authorized, and whether they are the cause of a problem now, or risk being one in the future. The changes provide context for the other three observability dimensions. The awareness of future harm enables IT Ops and DevOps to transcend observability's limited usage in reacting to problems and instead focus on preventing them.

Charley Rich,
Former Gartner Analyst &
Evolven Tech Strategist

About the Author

Charley Rich retired from Gartner as Research Director in the IT Operations Management group as an analyst focusing on providing guidance to users and providers of APM and AIOps solutions.

Mr. Rich comes with almost 40 years of IT experience as a Software Product Management Executive having built many innovative APM, big data analytics, SaaS, and UI solutions. He was a key contributor to four highly successful startups, receiving the General Manager's Award at IBM and the President's Award at Tivoli.

Challenges

- Infrastructure and Operations (I&O) leaders struggle to reconcile the speed of the business with the reliability and control IT needs to ensure a smooth-running production environment.
- I&O leaders' observability strategies leave them blindsided, unaware of changes that lead to failure.
- I&O leaders can become overwhelmed with the task of reconciling planned changes with actual changes.

Recommendations

I&O leaders managing infrastructure, operations and cloud must:

- ***Prevent*** problems by anticipating the risk of change before there is an impact
- ***Improve*** the reliability of production by determining when a change is the root cause of a problem
- ***Innovate*** faster using CICD in a closed-loop, unhampered by unexpected changes and expected changes with unexpected consequences

Anticipate Change Risk and Prevent Customer Impact

To deliver enhanced observability, improved customer experience and facilitate business innovation I&O Leaders need to be able to expect the unexpected, handle uncertainty, and actively manage risk.

AI-driven automation can be used to detect, assess, validate, and reconcile actual changes in manual and automated deployments before there is a problem.

Evolven's patent for Change Reconciliation helps address this. It is used to detect what actually changed in an IT environment and compares this to planned change requests and deployment events using sophisticated correlation. Evolven leverages AI ML and natural language processing to identify the scope or the potential "blast radius" of planned changes defined in a change request.

The detected actual changes are compared to planned changes, producing an authorization score indicating if a particular detected change can be attributed to planned or pre-authorized change activity or not. Evolven's Analytics Engine goes on to provide proactive risk analysis, evaluating all changes and differences to estimate their likelihood to cause issues in the future. The resulting probability is visualized for the user as a color-coded risk level (See Figure 1).

This approach to analysis guides the user from the endless loop of build-break-fix-repair to proactive management that provides prescriptive steps for the IT Ops user to take to prevent problems and avoid business impact. Using AI ML, this Four-Dimensional Observability solution can anticipate that a specific "change" will cause a customer-impacting problem and gives IT the time and opportunity to prevent impact.

If you don't measure risk, you can't manage it, and then you are stuck fixing what might have been avoided.

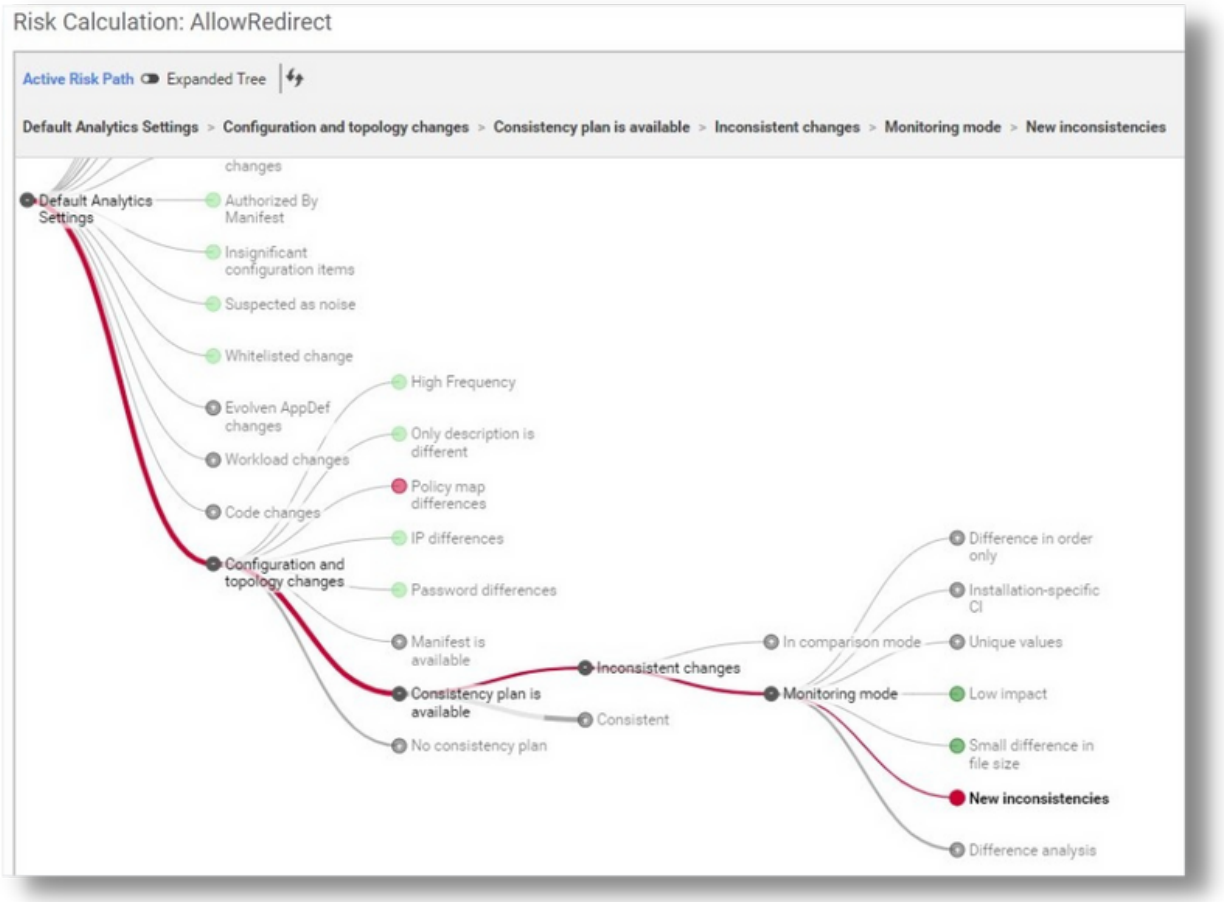

Figure 1: Displaying the CAlculation of Risks in the sample On-Demand Loan Application, Filtered by Technology

Use Change-Aware Root Cause Analysis to Improve Production Reliability

Working together APM and Evolven help prevent impact by providing enhanced root-cause-analysis (RCA) that considers change as a potential root cause.

The APM solution discovers the IT environment by tracing code-level transactions, capturing associated metrics, and logs, and generating alerts when something is wrong.

Evolven captures what has actually changed in that same environment and how that differs from what was expected. Both solutions utilize Machine Learning analytics and when integrated together correlate their analysis to determine risk and deliver actionable insights into the root cause of problems occurring now as well as problems that may happen in the future. (See Figure 2).

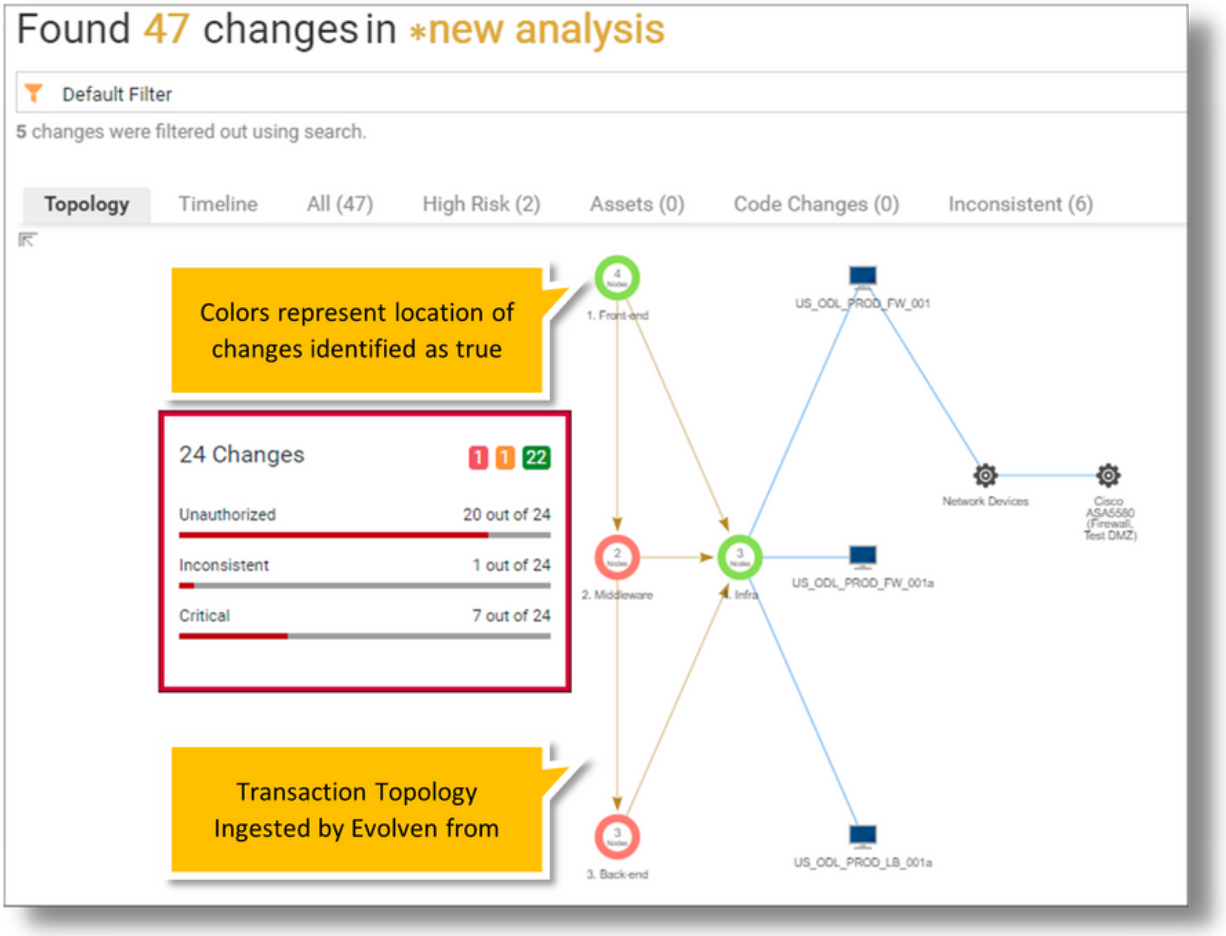

Figure 2: APM Topology within Evolven Highlighting Changes that are Root Causes

Use a CICD in a Closed Loop, Unaffected by Unexpected Change, and Innovate Faster

Evolven and APM both integrate with the CICD pipeline. Evolven's integration scans both the CICD pipeline and pre-production deployments to determine the expected changes that a change request or a deployment will cause, as well as the actual changes.

Evolven employs machine learning analytics to analyze these changes; correlate them with data drawn from DevOps, CICD, and monitoring tools; and assess their risk.

This provides DevOps, CloudOps, IT Ops, and IT Risk & Compliance teams with the insights they require for troubleshooting and prevention of stability, compliance, and security incidents in order to avoid trouble.

Evolven Change Manifests (ECMs) capture expected granular changes for automated reconciliation and validation of actual changes. ECMs are automatically created by Evolven during pre-production deployments.

The ECM is automatically attached to corresponding change requests or automated deployments. Using ECMs, Evolven first analyzes the Operational Risk of the expected changes before the deployment and then reconciles the actual detected changes. This process ensures that the Change Management System's notion of change is correlated with Evolven's detection of actual changes, providing DevOps with accurate information about the actual outcome of the new deployments.

Together APM with Evolven provides DevOps with direct access to the state of new deployments and immediate insight into the root cause of failures and the ability to avoid them and prevent future impact. This closed-loop approach enables DevOps to continuously improve results in an increased cadence of effective new releases (See figure 3)

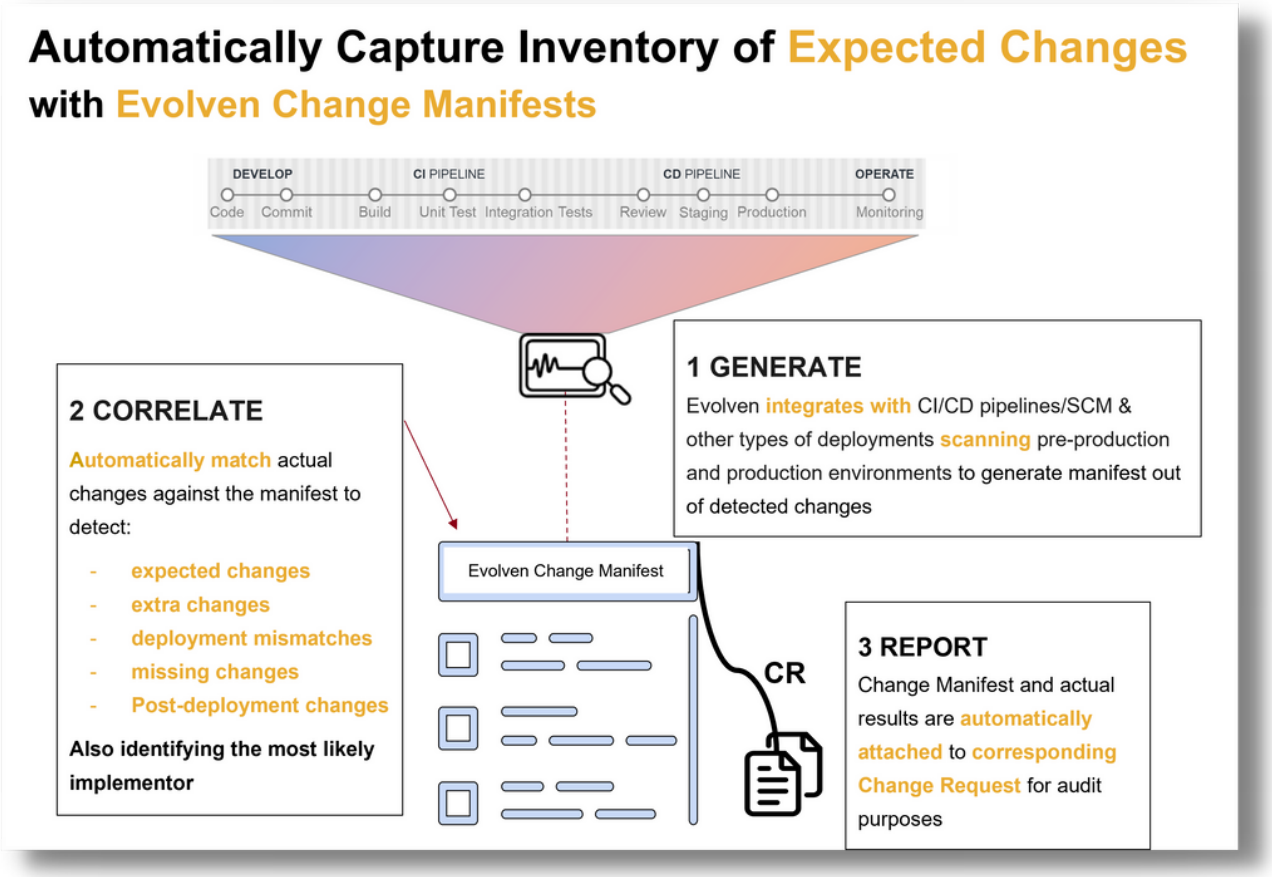

Figure 3: Evolven with APM Prepares DevOps with an Automatically Captured Inventory of Expected Changes

How the APM and Evolven Integration Works

With bi-directional integration to the APM solution, Evolven can request via a REST API the alerts APM health rule exceptions produce. These events are accompanied by the underlying topology (a graph with nodes and edges) including applications, server, and network dependencies that APM discovers.

APM sends to Evolven a snapshot containing the transactions that are running slow or have failed and the paths they have traversed in the underlying topology.

Evolven can correlate its knowledge of change and configuration with the topology it ingests from APM. Evolven displays a flow map from APM in its dashboard overlaid with the Evolven acquired changes to this topology.

The change overlay includes the status of changes such as for example, compliant and authorized, and the risk these changes may incur. AI-based risk analysis looks at many factors including the distance of the issues from nodes on the graph, apriori change risk, the type of issues discovered, time-based impact and more.

When desired, the Evolven dashboard widgets may be encapsulated within the APM solution's dashboard in an iframe. Evolven can also send the detected actual changes back to APM as custom events.

Both APM and Evolven utilize AI machine learning (ML) in their analysis. APM's ML tooling determines among other things application performance deviations, while Evolven uses ML to identify and prioritize risk and determine if a change is the root cause of a current or future problem. (See Figure 4)

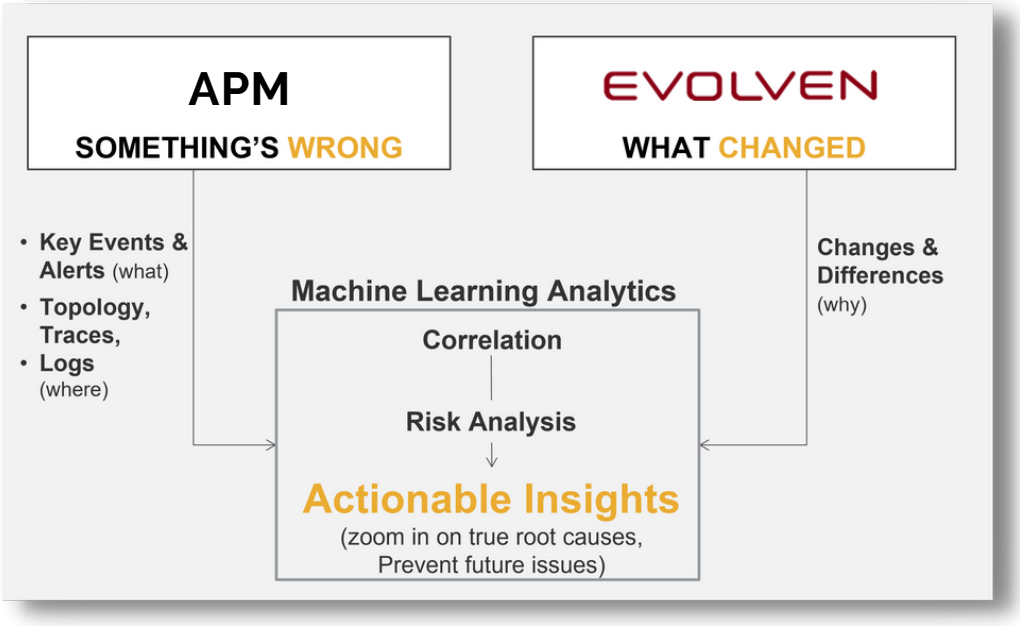

Figure 4: Evolven + APM Reinvent Observability

Customer Case Study

Overview

A large multinational bank realized that many of their Priority 1 (P1) incidents were caused by unexpected changes. These included: changes to applications, configurations, infrastructure, data schema, and content. The IT environment for this bank was deployed in their on-premises datacenter using Pivotal Cloud Foundry (PCF) with applications developed in Node.js, Python, Go, and Java.

The bank was successfully using an APM solution in production for traditional application performance monitoring (APM) and more recently for Observability capabilities now that their newer applications were being architected in microservices. The APM solution has been highly effective at the bank in determining the location of performance slowdowns and failures impacting availability so that service interruptions were kept at a minimum.

Conflicting Truths

However, the bank had the problem of having multiple, conflicting "single sources of truth" on which to base their decisions. An IT single source of truth is the repository, often a CMDB (configuration management database) where the definitions and configurations of IT infrastructure components, as well as other key artifacts such as incidents and change history, are stored. It is used in the change management process to ensure that all planned deployment decisions are based on an accurate reflection of the IT environment.

Unfortunately, their monitoring tools had one version of the topology while their ITSM tools, specifically ServiceNow (SNOW) had another. Their ITSM change management tools had a record of planned changes but did not have an accurate record of what actually changed. The bank's IT Ops team attempted to reconcile these discrepancies manually, but as this was quite laborious, the efforts stayed at a high level and were never up-to-date. They were faced with the enigma that applications behaved normally yesterday, but not today and they struggled to find out why.

Moving to a Single, Single Source of Truth

Initially, in Phase One, Evolven was integrated via API with the current APM implementation and configured to dynamically import the application maps (topology) from APM (See figure 5).

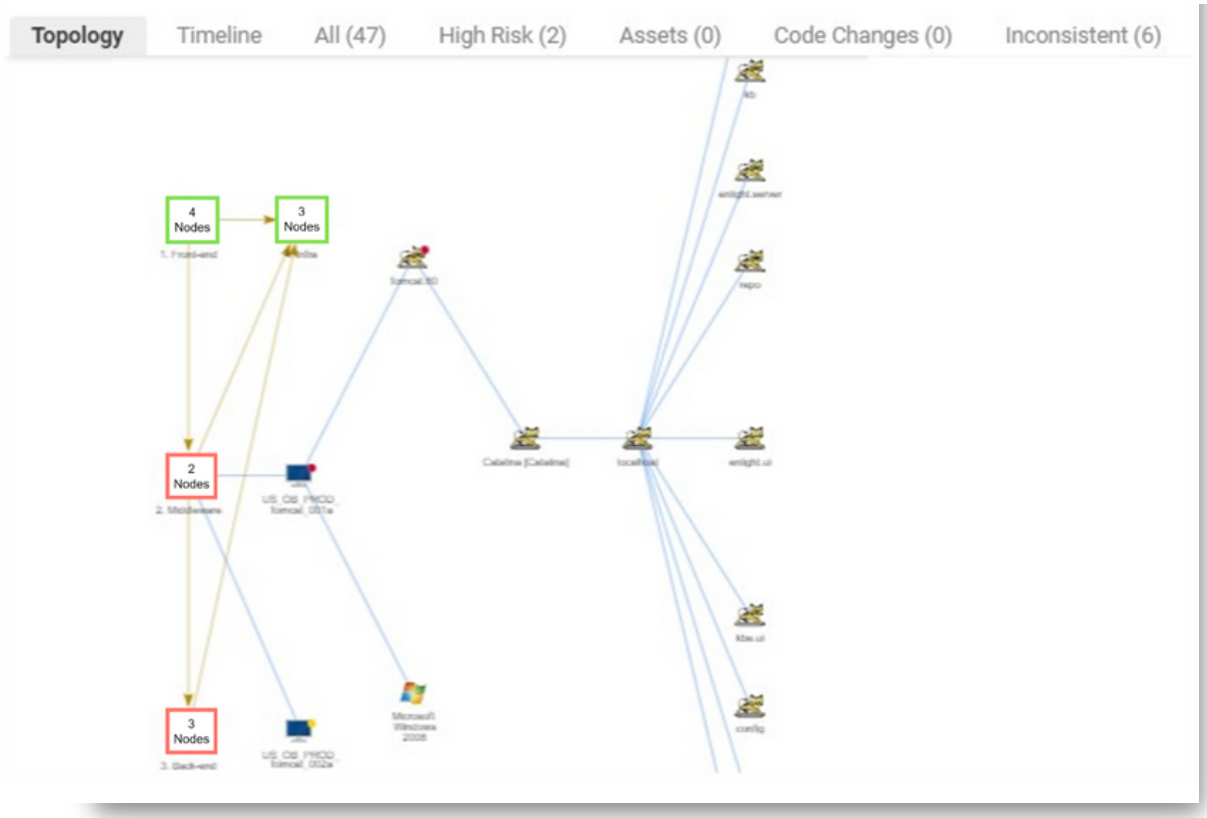

Figure 5: APM Topology Displayed in Evolven's Dashboard

The same process was set up to do the identical function with the CMDB portion of ServiceNow. The bank realized that they need a solution to arbitrate between the conflicting tools to reach a reconciliation. Evolven's function in this first phase was to use its operational data insights from its enhanced search technology to point out the differences between APM application mapping and the ServiceNow CMDB.

Next, in Phase Two Evolven was used to identify the root cause of problems that were missed during the ITIL incident management process. As the incident management process can be somewhat reactive, the goal was to reduce the meantime to repair (MTTR) for outages. Evolven was configured to analyze the end-to-end environment, including bespoke systems, and to optimize change correlation.

The Evolven implementation team developed a standard operating procedure (SOP) for issue investigation working with the incident managers and subject matter experts (SMEs) involved in the problem management process.

After that, in Phase Three following several months focused on incident management, integration between Evolven and APM was configured to import APM health rules violations with the status of severe or critical for use in correlation with the information about actual changes detected by Evolven. This was done to evolve to an ITIL Problem Management approach focused on preventing outages and problems from risky changes that impacted users. The goal was to uncover problems and resolve them before they impacted users.

The bank's Evolven SME was tasked with pulling the correlated change data from Evolven and sharing it with the rest of the team participating in the incident investigation. Evolven's SME was also requested to explain the data provided by Evolven in case of questions from the rest of the team. Initially, Evolven was applied to a subset of critical business systems. Once the process was proven to be working, it was extended to the rest of the IT environments.

Finally, in Phase Four a self-service approach to Evolven was adopted.

The tier 2 support team at the bank had sufficient expertise to operate it and interpret the data without their SME. This enabled the SME to move on to newer use cases.

Results

There were many occasions when Evolven identified rogue changes that bypassed the authorization process. Evolven's detection of these risky changes enabled the bank to prevent impact to customers. Without using Evolven the bank would have had no way to detect unauthorized changes (See Figure 6)

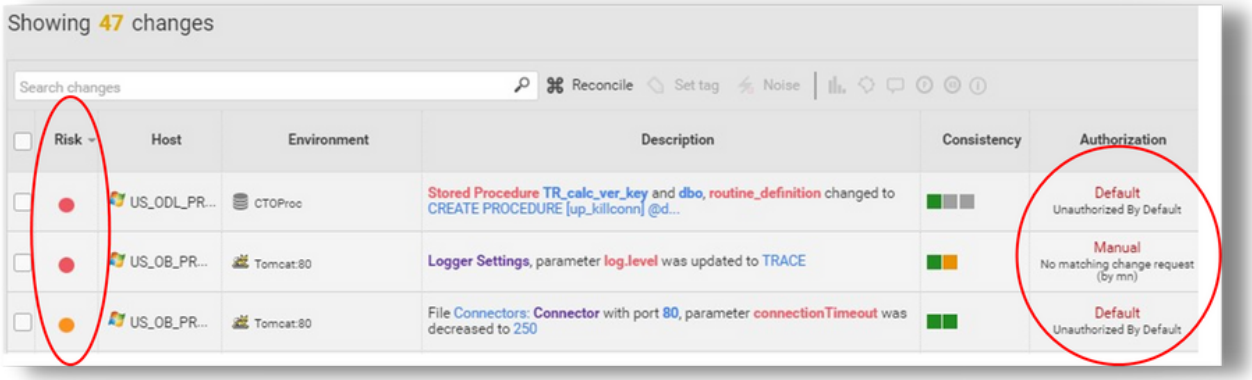

Figure 6: Evolven Displays Unauthorized Changes and the Risk they Present

The bank confirmed, based on the empirical observations, that investigation would have taken significantly longer if conducted without Evolven and would have impacted user experience. The following are examples where Evolven and APM integration provided great value:

- The private cloud deployment of the bank's applications experienced non-reproducible performance issues. These were successfully discovered by APM. Evolven and APM together, then took this information and uncovered several platform nodes that were misconfigured, and determined that they were the definitive root cause of the intermittent failures.

- APM detected a significant performance degradation in a critical business system. This information was passed via API to Evolven which identified that a recent OS patch reduced the size of the swap file. This patch was determined to be the root cause of the performance degradation.

- AAPM identified an increasing rate of transaction failures caused by delays due to slow Oracle SQL query response times. This determination was passed to Evolven which established that there was a change in the database configuration that caused certain queries to access a database in the secondary data center that was turned off for maintenance. Evolven concluded that the root cause of the transaction failures was the change in the database configuration.

- APM detected dropped transactions and sent an alert to Evolven. Evolven used this health rule exception alert and determined that this was caused by configuration changes in a JVM (See figure 7).

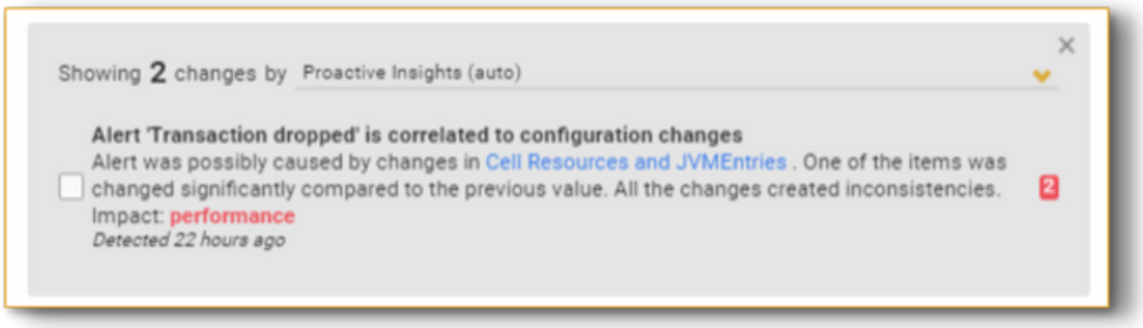

Figure 7: Evolven Explains Transaction Failure

Four-Dimensional Observability

Integrated Evolven and APM's Four-Dimensional Observability delivers the capability to foresee the risk of changes leading to potential problems, and the prescriptive advice to prevent impact before there is damage. It also provides businesses with the insight to determine the root cause of problems that were due to risky changes.

APM and Evolven's technology working in unison will help your business move from being reactive to making risk-informed decisions and prevent risky changes from impacting the customer experience. Use the combined solution to stay ahead of problems, and manage stability, compliance, and security risks.

By leveraging how APM and Evolven are smarter together, you can focus on the real mission - delivering business value to your customers.

About Evolven

Although we all recognize that changes are the root cause of most security, compliance and stability issues, IT still struggles to identify what has actually changed. Evolven allows enterprises to track all actual changes that have occurred in their environment, using machine learning to identify and prioritize the riskiest ones. With Evolven, IT Operations, DevOps, and ITSM teams experience fewer incidents, faster MTTR, and improved productivity.

Evolven is a recognized AIOps (Artificial Intelligence for IT Operations) leader and was named IDC Innovator of the year in 2017 and Gartner as a Cool Vendor in IT Operations. Evolven has also been included in Red Herring Top 100 North America. TiE 50 Top Startups, 20 Most Promising Data Center Solution Providers, Top 10 Banking Analytics Solution Provider, and was a recipient of ITOA50 awards.

To find out more visit www.evolven.com and follow updates on LinkedIn and Twitter.