

Change is Inevitable and Should be Visible.

### **Unauthorized Change Impacts**

Unauthorized change is a problem in any environment for three key reasons:

- 1. Security Risk: Unauthorized changes can introduce security vulnerabilities and put an organization's data and systems at risk. And unauthorized changes can also indicate that an intruder has penetrated the defense perimeter.
- 2. Compliance Risk: Almost all compliance standards mandate good change control processes and unauthorized changes will indicate when those processes are not being followed.
- 3. Operational Risks: Unauthorized changes can lead to systems being unavailable, slowed, or unreliable which can cost you time and money for correcting root cause issues but also cost your business revenue and customers.

## WE USE EVOLVEN TO KNOW WHAT CHANGED.

Mark Psenicka, Enter prise Systems Monitoring Manager, NYCB Detecting all changes in your IT environment is a first step to ensure security, compliance and operational stability. With Evolven's Configuration Risk Intelligence Platform, you gain visibility into all changes in your hybrid multi-cloud environment. Evolven's AI-based analytics automatically reconciles actual and approved changes assessing their risk so you can make better decisions to save time and minimize risk.

### **Benefits**

- Detect and capture all changes at the most granular level in hybrid multi-cloud from application to infrastructure and from onpremises to the public cloud in near realtime
- Complete visibility into all types of changes such as code, configuration, and data changes across files, databases, network and storage devices, APIs, containers, cloud environments, and more
- Automatic reconciliation of almost all detected changes to distinguish authorized, potentially authorized, and unauthorized changes
- Detailed change audit trail addressing compliance requirements
- Automatic insights based on patented algorithms that can identify risky changes before they become costly incidents, reducing outages by 35% or more
- See what changed, how it changed, when it changed, and who changed it with 50% or more faster security incident response and forensic investigations with root cause analysis in minutes, rather than days
- Automatic noise reduction with patented technology

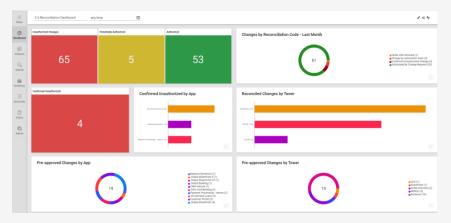


Figure 2: Screenshot of a Reconciliation Dashboard in Evolven

### **Single Source of Truth**

For modern IT visibility you need a single source of truth.

From AIX to Windows and AWS to VMWare, Evolven's Configuration Risk Intelligence Platform provides crucial insights into all actual granular changes - unauthorized and authorized - in one place.

## **Drift Can Be Anywhere**

Authorization of changes comes from a symmetry between planned and actual executed changes. The Evolven Configuration Risk Intelligence Platform has an AI-based Analytics Engine that makes decisions about this symmetry using patented trained and untrained machine learning, not just simple rules.

Unauthorized changes derive from detected changes that lack approval. Examples of these could be:

- Application parameters or systems that should never change without prior approval
- Configuration changes blocklisted by security and operations stakeholders
- Changes made at the wrong time
- Changes made in the wrong place
- Changes made in the wrong way

Essentially, rather than trying to brute force change reconciliation through legacy means, the Evolven Analytics Engine is sorting through the noise and the mess to help you make decisions you can live with - quickly and efficiently.

## Less Noise = More Time

# Unauthorized Change Details Risk Host Description Consistency US\_ODL\_PR... File running config.txt: access-mucfwt63-traverse-in in interface mucfwt63-traverse was removed US\_ODL\_DAPAdminLimits, parameter MaxPoolThreads was decreased to 3 (time anomaly) US\_ODL\_UDAPAdminLimits, parameter MaxActiveQueries was decreased to 10 (time anomaly) US\_ODL\_UDAPAdminLimits, parameter MaxConnections was decreased to 3000 (time anomaly) US\_ODL\_UDAPAdminLimits, parameter MaxConnections was decreased to 3000 (time anomaly) US\_ODL\_UDAPAdminLimits, parameter MaxConnections was decreased to 3000 (time anomaly) File C-/Program Files/\_/META-INF/MANIFESTMF, parameter DB-Connection-Max-Age was updated to 500 File C-/Program Files/\_/META-INF/MANIFESTMF, parameter DB-Connection-Max-Age was updated to 500 File C-/Program Files/\_/META-INF/MANIFESTMF, parameter DB-Connection-Max-Age was updated to 500

Figure 2: Unauthorized Change Details show prioritization by risk score - without rules.

Show: All Auto 25 50 100

Some tools can generate a lot of unnecessary information stressing already burdened staff. And up to 95% of the system traces these tools generate may be false positives and noise.

Evolven's patented AI will reduce noise to a whisper by automatically reconciling benign changes, freeing your staff to focus on higher value work in security, compliance, and stability. This filtering on true positives without rules that have to be defined by end users is a unique capability of the Evolven Configuration Risk Intelligence Platform.

To find out more visit <u>www.evolven.com</u> and follow updates on <u>LinkedIn</u> and <u>Twitter</u>.