EVOLVEN

DRIFT DETECTION AND CONSISTENCY ANALYSIS

When expectations do not match reality.

Exceeding Expectations

Configuration drift is the result of changes over time, due to manual or automated updates, patches, or releases made by application or infrastructure teams where the system or environment becomes inconsistent with its intended configuration or the documented standard, potentially leading to performance issues, security vulnerabilities, non-compliance, or reliability concerns.

Configuration drift can occur in any type and layer of systems, from application to infrastructure, from data center to the cloud, from pre-production to production and DR environments. For example, configuration drift might occur as a result of undocumented and unauthorized change or when a deployment was not completed leaving some of its environment components out of sync.

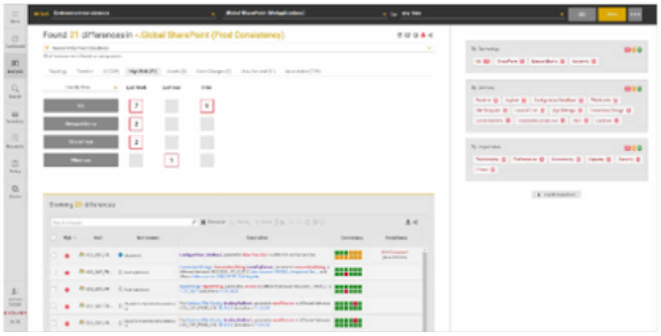
To mitigate configuration drift, Evolven's Configuration Risk Intelligence Platform collects granular configuration and tracks actual changes across the entire hybrid multi-cloud environment. It leverages a patented AI-based engine to analyze millions of configurations and changes across managed systems to identify misconfigurations, anomalies and inconsistencies and communicate them with meaningful risk scoring for remediation.

Evolven's Configuration Risk Intelligence Platform's deep and broad view of granular configuration and all changes in hybrid multi-cloud environments provides a capability to catch drift that others would easily miss and filter out noise that can impede action.

The same can be said about the patented AI-based analysis of drift where common practice and tools require manual intervention to simply capture baselines and compare them with scoped targets. Evolven's approach automatically captures configuration states, compares them in real time, and finds inconsistencies automatically.

Benefits

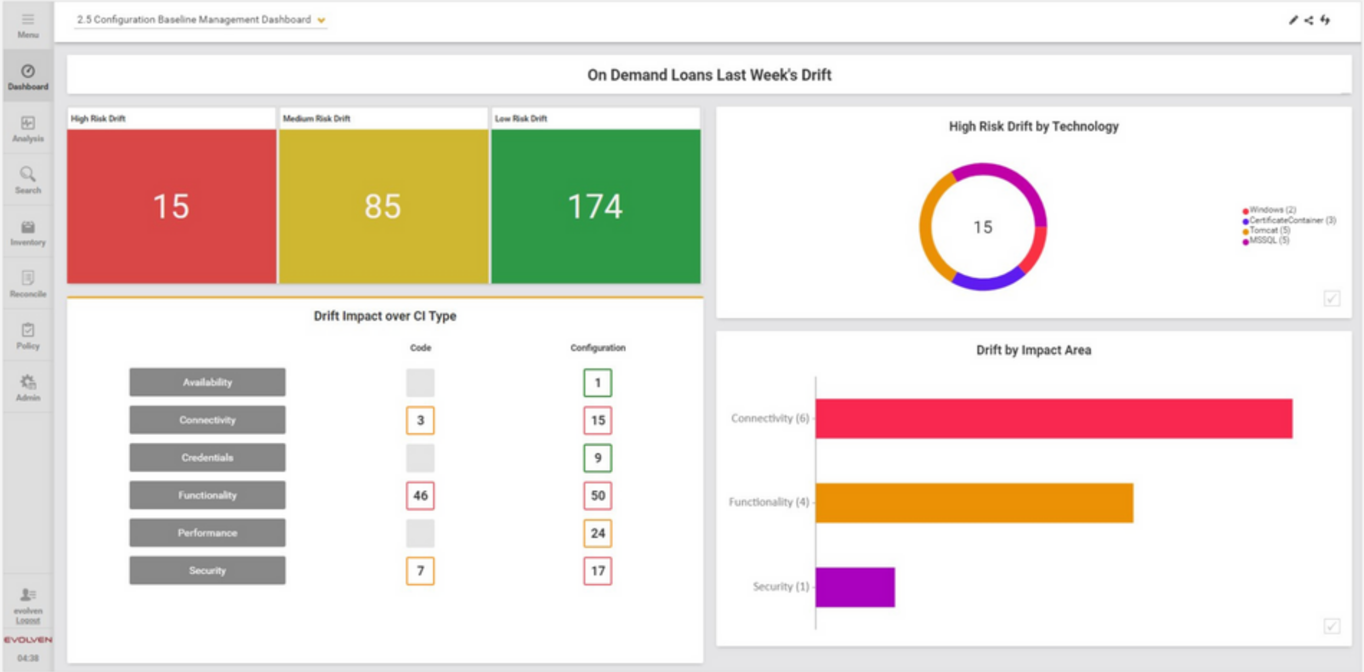
- **Improved performance:** Identifying and addressing inconsistencies from good configuration baselines and misalignments between environments reduces downtime, errors, and other performance issues.
- **Enhanced security:** Drift Detection and Consistency Analysis helps identify security weaknesses that can be exploited by attackers.
- **Better compliance:** Drift Detection and Consistency Analysis provides change and configuration control ensuring standards and regulations are met and maintained over time, reducing non-compliance.
- **Increased efficiency:** Automating consistency analysis reduces the time and effort required to monitor and maintain IT systems.
- **Improved decision-making:** Drift Detection and Consistency Analysis enables IT managers to communicate more effectively across silos and make informed decisions based on risk scoring and potential impacts.



Found 21 differences in -Global SharePoint (Prod Consistency)

Showing 21 differences

Figure 1: Environment Consistency Analysis



2.5 Configuration Baseline Management Dashboard

On Demand Loans Last Week's Drift

High Risk Drift	Medium Risk Drift	Low Risk Drift
15	85	174

Drift Impact over CI Type

	Code	Configuration
Availability		1
Connectivity	3	15
Credentials		9
Functionality	46	50
Performance		24
Security	7	17

Figure 2: Configuration Baselines and Drift Impact Types

Drift Can Be Anywhere

Drift can be anywhere and can affect availability, connectivity, performance, functionality, compliance and security.

Drift from an approved baseline refers to the deviation of a parameter from its initially established, authorized standard or reference point caused by a change.

Drift from a configuration standard such as CIS, PCI, or NIST refers to the deviation of system configurations, settings, or controls from the prescribed guidelines outlined by the respective standard. This may be drift introduced by the initial system state or made by a change and could be due to changes in the standard.

Drift within an environment refers to the gradual and unintended changes or variations that occur over time within a cluster of systems that are intended to be similar, such as web servers clusters or high availability environments. These discrepancies potentially lead to degraded performance, loss of service, or security vulnerabilities.

Drift between environments, such as pre-production to production, or production to disaster recovery, refers to the undesired configuration discrepancies or inconsistencies between the different environments, potentially leading to ineffective testing, failed deployments, stability losses, etc.

Near Real Time Analysis

Evolven's ability to acquire a vast amount of configuration data across enterprise and cloud contributes to automatic and near real time assessments of the actual parameter values.

Our patented algorithms go beyond finite checklists or rule-based knowledge bases dynamically analyzing configuration and change data. They are based on unsupervised machine learning, calculating entropy to estimate a level of surprise. These algorithms evaluate data across environments in near real time to identify potential misconfigurations and risky changes that could negatively impact stability, compliance and security of the analyzed systems and environments.

Learn more about Evolven's algorithms at https://patents.google.com/patent/US20180239682A1.

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