Unauthorized Changes are Hurting You.

Unauthorized changes present serious regulatory, operational, and security risks to any enterprise. Various regulations, including **OCC**, **SOX**, **PCI**, **NERC**, **GDPR**, and **HIPAA**, as well as internal and external auditors, require organizations to establish tight internal change control procedures for eliminating unauthorized changes.

Most IT organizations today suffer from **limited visibility** into the **actual changes** carried out in their IT environments, which is a critical requirement for meeting change control requirements. Even the intensive manual effort being performed today results in meeting only partial requirements, thereby exposing the organizations to serious risk.

To meet today's strict change control and audit requirements, IT Audit/Risk, Service Management, IT Operations, and Cyber-Security professionals must track all actual changes, reconcile actual changes with any approved change request, post alerts regarding any unauthorized changes, and maintain an audit-trail of all actual changes.

For more info: 1-888-841-5578 (US) | info@evolven.com | www.evolven.com

We Track Them Down.

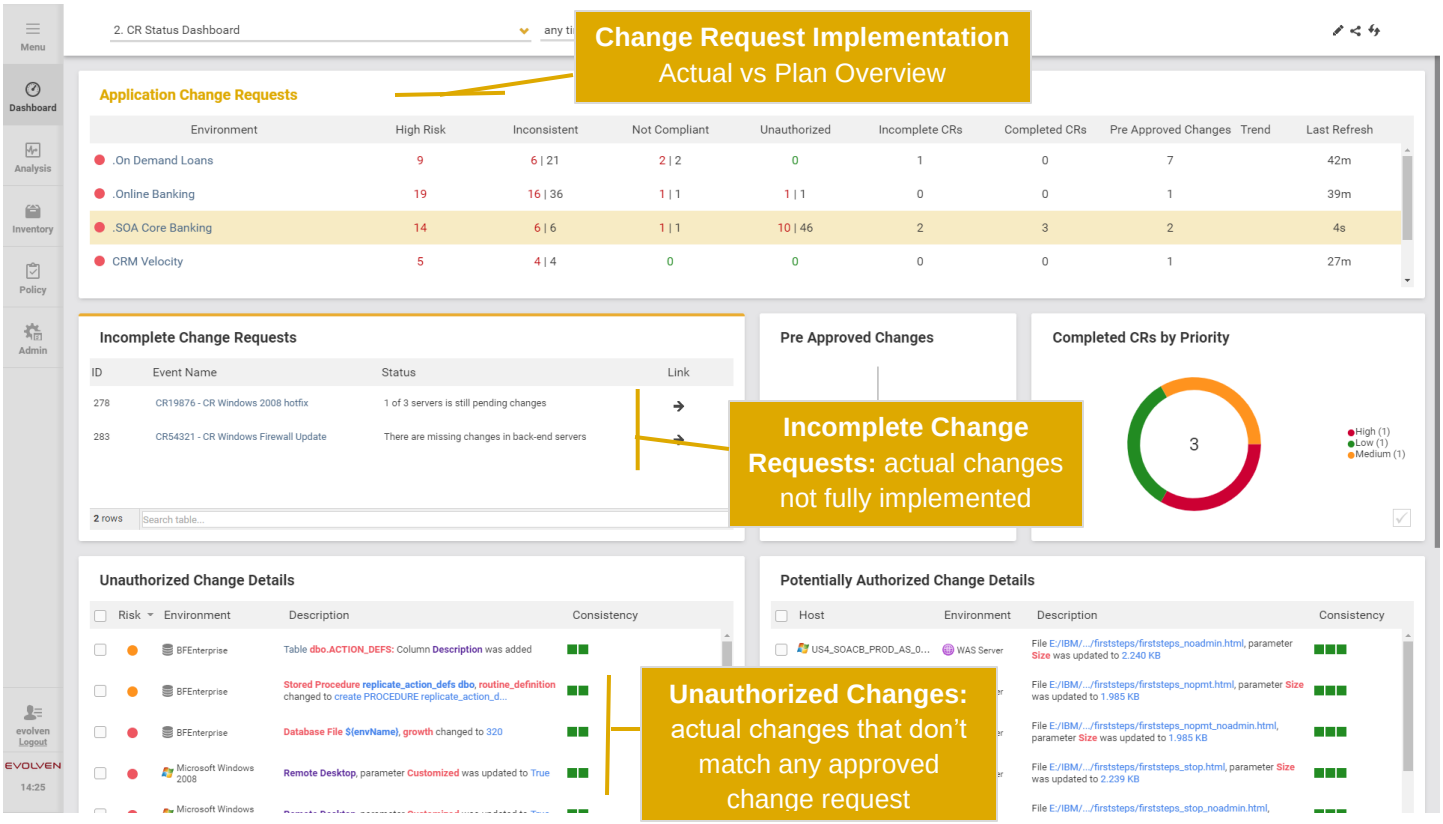
Evolven tracks all actual changes carried out in your end-to-end IT and Cloud environment. Using patented machine learning analytics to analyze the changes it collects for risk, it reconciles all changes, detects unauthorized changes, and provides a detailed audit trail

1. **Tracks all actual changes** across your end-to-end IT and cloud environment at the most granular level.

2. **Reconciles actual changes** with any approved change requests. Evolven is therefore able to detect any and all unauthorized changes – changes there were not approved, as well as incomplete changes.

3. **Alerts with respect to any unauthorized changes.** As soon as it detects unauthorized changes, Evolven sends actionable alerts.

4. **Reports and maintains a detailed audit-trail** of all actual changes, unauthorized changes, incomplete changes, and mis-configurations.



For more info: 1-888-841-5578 (US) | info@evolven.com | www.evolven.com

How Evolven Helps.

OCC	OCC requires the establishment of controls to prevent unauthorized changes to systems and programs and documentation of authorized changes. Evolven: • Detects, prioritizes, and reconciles all changes • Sends alerts to inform you if changes take you out of policy compliance • Provides a detailed audit trail of configuration changes, at the most granular level possible
SOX/COBIT	SOX/COBIT requires the establishment of internal controls and procedures to reduce the possibility of corporate fraud. Evolven tracks all actual changes and provides an automated audit trail. Unauthorized changes are detected and alerts are sent automatically.
PCI DSS	To meet PCI change detection requirements, Evolven alerts you on mis-configurations as soon as they occur.
NERC	To meet NERC CIP-010, Evolven detects unauthorized changes, detects any deviation from configuration baselines, or detects changes that violate defined security policies.
GDPR	GDPR requires assessing risk and matching controls to address those risks. Evolven detects, prioritizes, and reconciles changes that could compromise data or systems. Alerts will inform you if changes take you out of policy compliance.
HIPAA	To meet HIPAA Security Rule (Part 164), Evolven detects and prioritizes any unauthorized changes to ensure health data are not compromised.