Technical Value Brief

How Evolven Supports NIST 800-53 SI-7 Control Compliance

Overview

Federal agencies must comply with NIST 800-53 SI-7, which mandates integrity monitoring and protection of software, firmware, and information systems to detect and prevent unauthorized modifications. Evolven Configuration Risk Intelligence provides AI-powered visibility into configuration changes across both **data centers and cloud environments**, ensuring compliance with SI-7 requirements by detecting unauthorized modifications, validating integrity, and preventing security risks across hybrid IT environments.

EVOLVEN

Mapping Evolven Capabilities to SI-7 Control Requirements

SI-7 (1) Integrity Checks

✓ **Requirement:** Perform integrity verification of software, firmware, and information integrity.

🔹 **Evolven Solution:** Evolven continuously monitors critical files and configuration elements across applications, operating systems, databases, and network devices in both **on-premises data centers and cloud environments**. Evolven extends its monitoring capabilities to **native cloud resources**, including cloud security groups, security roles, virtual machines, container configurations, API gateways, and more. It detects unauthorized, risky, or unexpected changes, allowing SecOps teams to maintain the integrity of system configurations across both traditional and cloud-native infrastructures.

SI-7 (2) Automated Notifications of Integrity Violations

✓ **Requirement:** Alert personnel of integrity verification failures or unauthorized changes.

🔹 **Evolven Solution:** Evolven's AI-driven analytics detect unauthorized modifications in **both cloud and on-premises environments** and provide **timely** alerts to security teams. It integrates with ITSM and SIEM solutions, such as ServiceNow and Splunk, to automatically escalate security violations, ensuring swift remediation of unauthorized or high-risk changes.

SI-7 (5) Automated Response to Integrity Violations

✓ **Requirement:** Implement automated mechanisms to address integrity violations.

🔹 **Evolven Solution:** Evolven enhances security automation by correlating detected changes with predefined risk policies. It can trigger automated remediation actions via integrations with security orchestration tools and IT automation platforms, ensuring rapid response to integrity threats across **both data centers and cloud environments**.

SI-7 (6) Cryptographic Protection

✓ **Requirement:** Use cryptographic methods to verify software, firmware, and information integrity.

🔹 **Evolven Solution:** Evolven applies cryptographic hashing techniques to detect unauthorized file modifications and maintain integrity across **hybrid environments**, ensuring that security standards are met in both **cloud and on-premises infrastructure**.

SI-7 (7) Integration with Other Security Capabilities

✓ **Requirement:** Integrate integrity verification with other security mechanisms, such as intrusion detection and access control.

🔹 **Evolven Solution:** Evolven complements existing security tools by correlating configuration changes with performance and security incidents. It integrates with SIEM, EDR, and ITSM platforms, ensuring security teams have contextual intelligence to investigate and mitigate potential threats efficiently across

both cloud and on-premises environments.

SI-7 (8) Unauthorized Change Detection and Reporting

✓ **Requirement:** Identify and report unauthorized changes.

🔹 **Evolven Solution:** Evolven provides deep visibility into actual changes occurring across **data centers and cloud platforms**, distinguishing between authorized, unauthorized, and risky modifications. Its detailed audit trails facilitate compliance reporting, helping agencies demonstrate adherence to NIST SI-7 requirements.

🔹 **Automated Reconciliation:** Evolven also enables **automated reconciliation of actual changes against approved change requests and authorized automated deployments**. By integrating with ITSM platforms like ServiceNow and BMC Helix, Evolven correlates detected changes with documented approvals, flagging deviations that could indicate unauthorized modifications. This ensures full alignment with governance policies, reduces audit burden, and enhances security posture by immediately identifying and addressing unapproved changes.

SI-7 (12) Supply Chain Integrity Monitoring

✓ **Requirement:** Verify the integrity of software and firmware throughout the supply chain.

🔹 **Evolven Solution:** Evolven monitors the entire software and configuration lifecycle, detecting unauthorized updates, vulnerable libraries, and deviations from approved baselines in **both cloud and on-premises environments**. It helps agencies enforce security policies across the supply chain, mitigating risks from compromised third-party components.

Business Impact for Federal SecOps Teams

✓ **Reduced Risk Exposure:** Proactively detect misconfigurations and unauthorized changes before they lead to security incidents.

✓ **Enhanced Compliance Readiness:** Maintain continuous adherence to SI-7 requirements with audit-ready reporting and policy enforcement.

✓ **Accelerated Incident Response:** Automate identification and remediation of integrity violations, reducing Mean Time to Resolution (MTTR).

✓ **Seamless Integration:** Works alongside existing security and IT management tools, providing a unified security posture across **hybrid environments**.

Why Federal Agencies Trust Evolven

Leading government organizations rely on Evolven to ensure compliance with stringent security mandates such as NIST 800-53. By delivering **timely**, AI-powered insights into IT environment integrity across **data centers and cloud platforms**, Evolven empowers federal SecOps teams to enforce proactive security, mitigate compliance risks, and maintain operational resilience.

📧 **For more information, contact us at info@evolven.com or 1 (866) 866-2320