RedSeal Workflow

Automate exposure management with a simple, low/no-code builder that connects RedSeal to your existing tools, eliminates repetitive tasks, and confirms fixes.

Challenge & Solution

Security and networking teams waste valuable time on repetitive tasks like ticketing, routing issues, and validating fixes. Integrations often rely on fragile custom code or expensive consultants, which slows response and creates accountability gaps.

RedSeal Workflow changes this. With a low/no-code builder, it embeds RedSeal's exposure intelligence into the security systems and tools you already use, **eliminating the need for one-off integration projects** that can run $50K-$100K each.[1]

Benefits & Outcomes

RedSeal Workflow speeds remediation, clarifies ownership, and improves efficiency across SecOps and NetOps. By automating routine steps and validating fixes, teams save time and focus on higher-value work — while exposures are resolved consistently, saving hundreds of analyst hours annually.[2]

Key Benefits

- ✓ **Save time by automating repetitive tasks**
- ✓ **Act faster by routing issues directly to the right teams**
- ✓ **Increase confidence with built-in validation of fixes**
- ✓ **Lower costs by replacing fragile custom scripts and expensive consulting**
- ✓ **Adapt easily to changing policies and priorities**

© 2025 RedSeal. All rights reserved.

How It Works

RedSeal Workflow is an add-on automation capability within the RedSeal platform that streamlines exposure management processes. Customers can design workflows using a low/no-code builder, triggered by scheduled events, change requests, or user actions. These workflows connect RedSeal's hybrid environment model with external systems, execute predefined actions such as creating scopes or opening tickets, and include optional validation steps to confirm that exposures are resolved after remediation. RedSeal Workflow bridges the gap between insight and action—automating exposure validation and response steps to help teams close the loop faster.

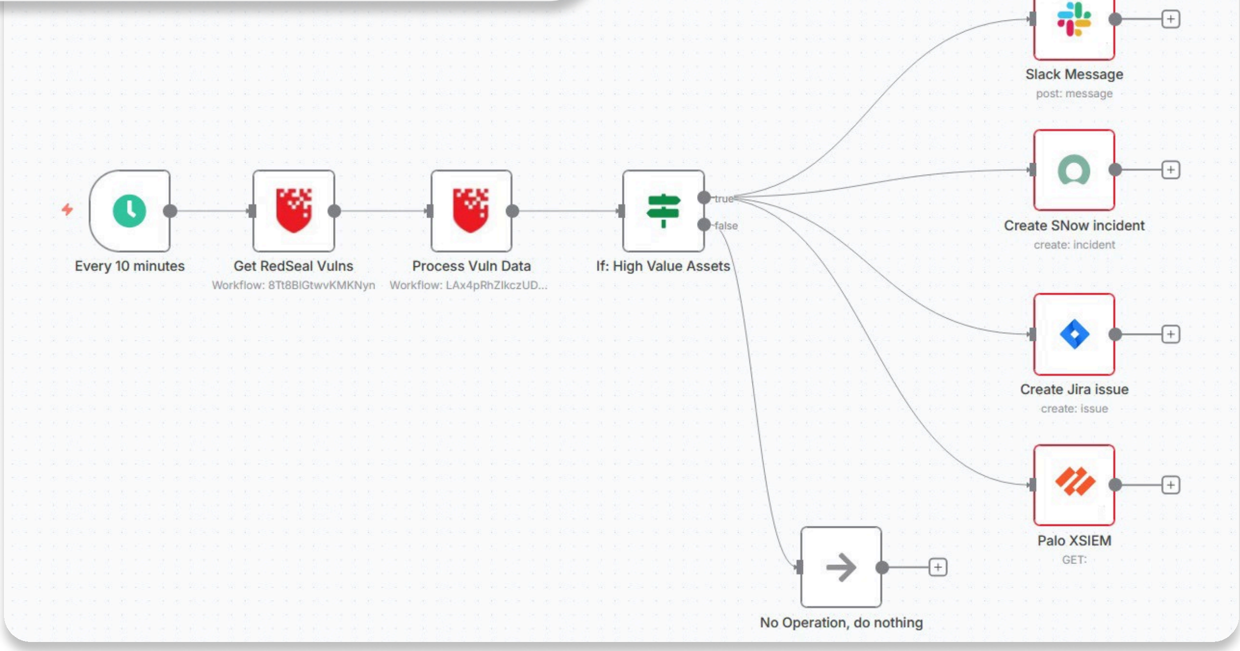
ROI Snapshot

With RedSeal Workflow, customers typically realize 3–6x ROI in the first year[3], combining analyst time savings, integration cost avoidance, fewer failed changes, and faster remediation.

Why RedSeal Workflow is Different

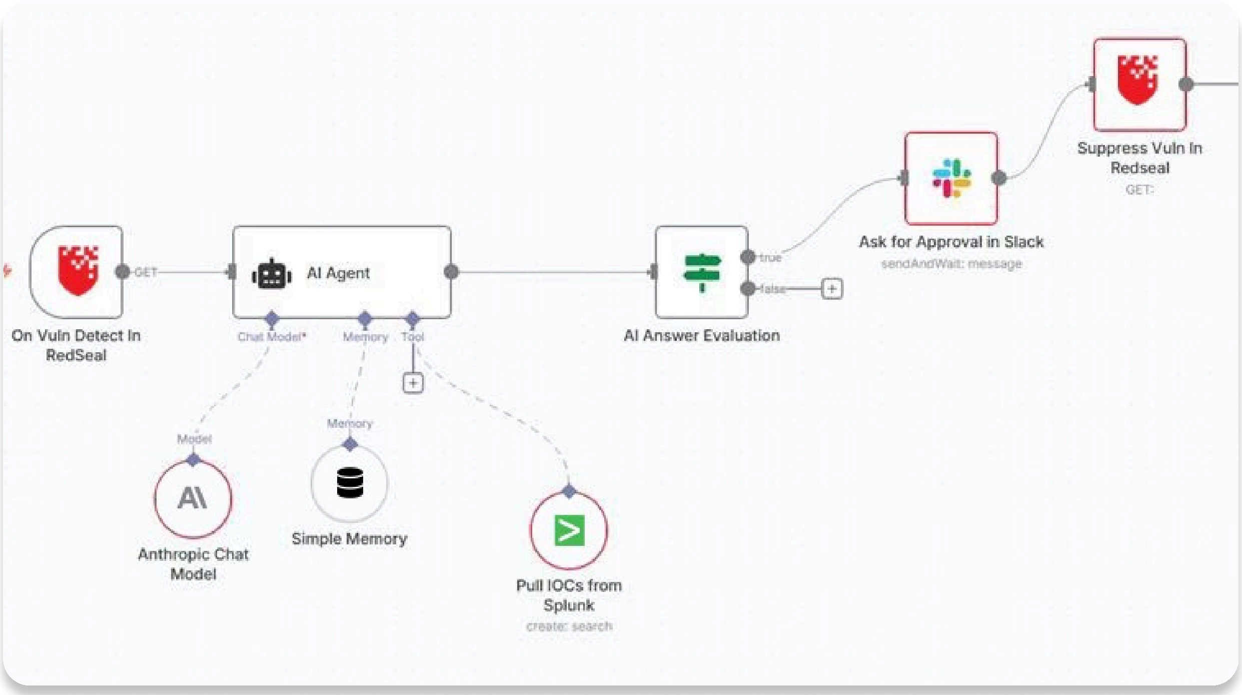
Unlike SOAR platforms or fragile custom scripts, RedSeal Workflow is designed specifically for exposure management — with automation built directly into the RedSeal platform.

- **Grounded in hybrid environment visibility** – RedSeal brings together IT, OT, and cloud into one model, so workflows run on a complete and accurate view of your environment.
- **Native, out-of-the-box orchestration** – No third-party workflow tools required; automate common processes immediately.
- **Focused on exposure management and validation** – Goes beyond incident response to proactively reduce risk.
- **Flexible and adaptable** – Tailors to each organization's policies, processes, and data sources.



***Ticketing workflow:** RedSeal vulnerabilities are processed and, if high-value assets are impacted, tickets are created in Slack, ServiceNow, Jira, or Palo Alto XSIEM.*

© 2025 RedSeal. All rights reserved.



Suppression workflow: *RedSeal detects a vulnerability, requests approval in Slack, and suppresses the finding in RedSeal if it's confirmed to be non-actionable.*

Example Use Cases

Teams use RedSeal Workflow to streamline critical processes — from aligning with policies to enforcing compliance and validating changes. By accelerating remediation cycles, organizations can cut average time-to-fix from five days to two, shrinking their window of exposure by 60% and reducing overall business risk[4].

All ROI figures are illustrative and based on modeled assumptions, industry benchmarks, and anecdotal customer data. Actual results will vary by organization. RedSeal does not guarantee specific cost savings or risk reduction outcomes.

1. Integration project cost ranges are based on consulting SOW benchmarks (Accenture, Wipro, boutique firms). Actual customer costs may differ depending on scope, systems, and vendor rates.
2. Estimated based on industry task-time studies (SANS, EMA) and modeled analyst workloads. Actual time savings will vary by organization size, analyst cost, and process maturity.
3. ROI estimate combines modeled analyst time savings, avoided integration costs, reduced failed changes, and faster remediation. Figures are illustrative and not a guarantee of individual results
4. Based on modeled remediation cycle improvements compared with industry averages (Verizon DBIR, IBM). Actual remediation times may vary by environment, team capacity, and incident severity

Policy Alignment: Continuously compare exposures against CISA KEV or other lists; auto-create targeted scopes.

Compliance Enforcement: Validate against PCI, NIST, or internal policies and route findings to compliance teams.

Cross-Team Orchestration: Push vulnerabilities into ServiceNow/Jira and notify owners in Slack/Teams.

Change Control Validation: Model proposed changes before deployment and confirm fixes afterward.

Contact RedSeal for more information or request a demo today.

RedSeal, a leader in exposure management, helps organizations know their environments better than any adversary. By creating a dynamic digital twin, RedSeal delivers comprehensive visibility, strengthens digital resilience, and reduces business risk. Trusted by Fortune 1000 companies and U.S. military branches, RedSeal enhances operational efficiency and improves security outcomes.

www.redseal.net | info@redseal.net | +1 408-641-2200 | 888-845-8169
© 2025 RedSeal. All rights reserved.