



What to Look for in a STIG Automation Solution Before You Buy

Not All Compliance Automation is Created Equal

Before you use critical funds on a STIG automation solution, make sure it actually delivers on coverage, speed, scale, and simplicity. This checklist will help.

The Core Evaluation Categories

- 1. Speed to Value
- 2. Ease of Use & Training Requirements
- 3. Comprehensive STIG Coverage
- 4. Drift Detection & Continuous Validation
- 5. Scalability Across Environments
- 6. Audit & Reporting Capabilities
- 7. Proven Track Record with Federal Agencies



Questions to Ask

1. Speed to Value

- How quickly can the solution be deployed?
- Can it show measurable results in less than 6 months?

Lightweight deployment and out-of-the-box policies accelerate time-to-impact.

2. Ease of Use & Training Requirements

- Does the solution require specialized scripting skills or ongoing training?
- Is it easy for operators and admins to use day-to-day?

Intuitive UI, low learning curve, and ongoing support that is built for the people who manage compliance...not just engineers.

3. Comprehensive STIG Coverage

- Does it cover all DISA STIGs, including OS, application, and infrastructure STIGs?
- Is it updated in lockstep with DISA's release cycles?

Comprehensive, ongoing STIG content support with automated updates.

4. Drift Detection & Continuous Validation

- Can the solution detect when systems fall out of compliance?
- Is continuous monitoring built in, or is it point-in-time only?

Built-in continuous compliance engine with auto-remediation capabilities.

5. Scalability Across Environments

- Does it support disconnected, classified, or cloud environments?
- Can it scale across teams and mission units?

Built for air-gapped, tactical, and hybrid deployments with lightweight architecture.

6. Audit & Reporting Capabilities

- Can it produce auditor-ready reports?
- Does it track control enforcement over time?

Granular reporting with historical logs, user actions, and rollback visibility.

7. Proven Track Record with Federal Agencies

- Has the solution been deployed in similar mission environments?
- Are there trusted references or ATO'd implementations?

Used across DoD with proven impact.

What to Avoid in STIG Solutions

- Shelfware that requires 6-month deployment windows
- Solutions that treat STIGs as a feature, not a focus
- Solutions that still require heavy scripting/customization



Make the Smart Buy

Use this checklist to cut through the noise and invest in automation that works for your mission.

Download our free guide ["100 Days to STIG Policy Implementation"](#) or contact our sales team to get started.

