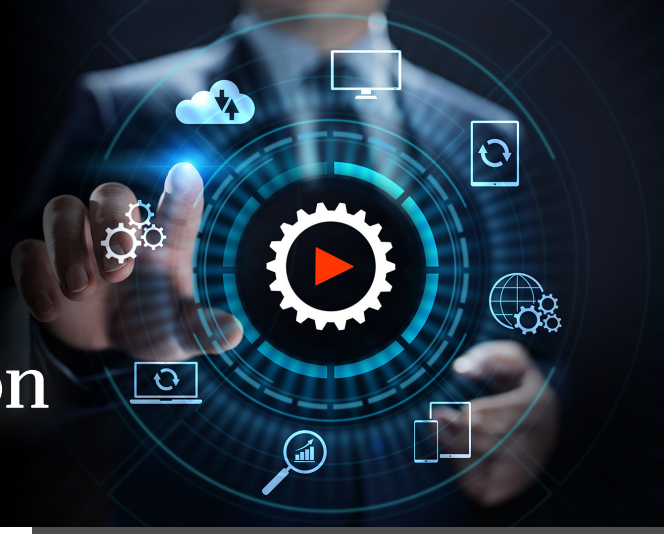
readyworks

CISA BOD 23-01 Compliance Orchestration



THE PROBLEM: Outdated, manual processes for IT asset lifecycle management (ITALM) exposes organization to CISA BOD 23-01 compliance violations and increases security risks and operational inefficiencies that drive up costs.

The Cybersecurity and Infrastructure Security Agency (CISA) has instructed federal, executive branch departments, and agencies to improve asset visibility and vulnerability detection on federal networks to safeguard federal information and information systems. Known as CISA binding operational directive (BOD) 23-01, it focuses on two areas: asset discovery and vulnerability enumeration. The directive provides stringent, recurring deadlines for both areas.

Interoperability among systems and manual processes for managing data (i.e., spreadsheets) makes meeting these deadlines extremely challenging and labor intensive.

THE SOLUTION: READYWORKS

ReadyWorks is a digital platform conductor. It collects, normalizes, and analyzes information from IT asset discovery and management tools, identifies security vulnerabilities, and orchestrates and automates workflows to quickly mitigate risks and ensure CISA BOD 23-01 compliance.

BUSINESS IMPACT:

- **Conformance with CISA Policies:** Ensure compliance with BOD-23-01 and internal security policies.
- **Improved security:** Identify security vulnerabilities and ensure all hardware is accounted for and all systems are up to date.
- **Operational Integration:** Improve operational efficiencies and reduce labor costs by eliminating manual processes that drive up labor costs associated with continuous BOD-23-01 compliance.
- **Lower costs:** Automated data integration reduces labor costs for ITALM including reporting as required by BOD-23-01.

readyworks

WITH READYWORKS:

- Comply with the weekly automated asset discovery and on-demand asset-discovery requirements of CISA BOD 23-01 with a comprehensive, real-time view of yourentire IT estate.
- Easily identify any vulnerabilities, such as outdated operating systems, unpatched software, or non-compliance to regulations by querying data to comply with the 14-day timeframe and take a prescribed action. For example, systems that have been identified as requiring a patch will be automatically added to a workflow to install the patch.
- Leverage connectors to automatically update the Continuous Diagnostics and Mitigation (CDM) agency Dashboard with curated, real-time data.
- Create daily automated scans to identify any outdated vulnerability detection signatures (VDS) to update and comply with BOD 23-01 requirements.

WHAT'S INCLUDED:

- Bi-directional connectors to collect asset information from data-sources including asset discovery and management tools, vulnerability scanning tools, CMDBs, global policy systems, configuration platforms, identity management systems, ITSM tools, and security alert systems. (10 connectors included in standard subscription.)
- Outbound orchestration to update source systems of record.
- Automated workflows for patch management and migration of EOL systems.
- Automated workflows to notify stakeholders of cybersecurity threat scenario.
- Automated workflows for escalations on security violations.
- Customizable communication templates.
- Full suite of asset inventory and audit response reports.
- Configurable dashboards and reports that check compliance with CISA BOD 23-01 protocols (e.g., vulnerability scanning and remediation).
- Guided implementation followed by ongoing support and training.

Request a demo today.

GO TO READYWORKS.COM/DEMO