

Splunk App for FISMA Continuous Monitoring

Automated Monitoring for NIST 800-53 Controls
Supporting the Risk Management Framework

Challenges

Any government agency, whether it is a civilian, defense or intelligence agency, depends on information technology to help support data integrity, reduce mission risk and ensure the confidentiality and availability of information.

In response to these needs, NIST published its Risk Management Framework (RMF) as part of the NIST publication 800-37 (updated February 2010). This framework outlines a six-step continuous monitoring process to establish security best practices for governmental agencies. NIST 800-37 complements the guidance in NIST 800-137 (draft) and provides a more in-depth view of the continuous monitoring methodology and strategy. The continuous monitoring process steps in NIST 800-137 (draft) are listed as: Define, Establish, Implement, Analyze/Report, Respond and Review/Update.



Organizations implementing a continuous monitoring process should do so in an automated fashion—to reduce the time and labor spent poring over terabytes of data from workstations, servers, applications and other elements across the IT infrastructure.

Why Splunk?

Splunk Enterprise is a highly scalable engine for machine-generated IT data. It collects, indexes and harnesses machine data from across your physical, virtual or cloud infrastructures in real time. Unstructured machine data is given structure through time-based indexing so that analytics can be applied to data to gain insight and understanding. Splunk captures and monitors real-time data streams from applications, network devices, hosts, security devices and software. In addition to real-time streams, Splunk analyzes historical data looking for trends, patterns and anomalies. Splunk supports continuous monitoring and also delivers a security-related context you can apply to any event from any layer of an IT infrastructure.



“If you want to do continuous monitoring you have to use Splunk. Before Splunk, our dashboard was unreliable and had no timely connection to reality.”

US Department of Justice

The IT infrastructure is dynamic. Vendor technology updates and new versions that contain security patches can't wait for new connectors or parsers. Splunk reads native log data from operating systems and monitors for specific conditions that may indicate hosts that are out of compliance. Using Splunk, this data can then be cross-referenced directly to specific and appropriate NIST 800-53 controls.

Splunk scalability

Continuous monitoring requires highly scalable data management. Splunk scales linearly across commodity servers and supports the largest of data volumes. And when you add servers to collect additional data it doesn't impact search performance. You can collect terabytes of data per day and also search for exactly what you want in seconds.



“The dashboards load instantaneously, which is a big deal for an environment as large as ours.”

Federal Reserve

Reporting without a schema

Continuous monitoring is in its early stages and the FISMA reporting requirements are still in flux. With a traditional relational database a new report might require you to go back and modify the schema—potentially taking days or weeks. With Splunk, there is no fixed schema and a common information (CIM) model supporting FISMA is applied. Splunk collects and stores IT data in a flat file and fully-indexed structure that can be scaled across multiple Splunk servers. You can generate reports on the fly without the cost or complexity of having to reload the data into a highly structured relational database model.

Ad-hoc search and forensic navigation across all IT data

The Splunk freeform search language and highly interactive user interface give immediate results and make it faster to interact with IT data than homegrown scripting or report/SQL-oriented tools. Splunk makes it easy to implement incident response procedures including in-depth incident investigations of suspected compromises.



“We are using Splunk to pass our FISMA assessments.”

NASA

The Splunk App for FISMA

The Splunk for FISMA App provides a plug-and-play framework for continuous monitoring of specific NIST 800-53 controls for Windows and Unix/Linux systems that eases the burden of desktop compliance. Security-specific product add-ons are also supported through additional services. The following controls are continuously monitored with searches and dashboards within the Splunk for FISMA App:

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-4 Information Flow
- AC-6 Least Privilege
- AC-7 Unsuccessful Login Attempts
- AC-12 Session Termination
- AC-14 Permitted Action w/o Authentication
- AC-17 Remote Access
- AC-18 Wireless Access Restrictions
- AU-2 Auditable Events
- AU-3 Content of Audit Records
- AU-5 Response to Audit Processing Failures
- AU-8 Time Stamps
- AU-9 Protection of Audit Information
- CM-4 Configuration Changes
- PE-11 Emergency Power
- PE-14 Temperature Controls
- SC-10 Network Disconnect
- SI-3 Malicious Code Protection
- SI-11 Error Handling
- IA-5 Authenticator Management
- PS-4 Personnel Termination

Splunk provides an easy-to-digest graphical view of these controls in the “Continuous Monitoring” dashboard, which supports continuous monitoring for three risk based components:

- ACM – Account Management
- ACP – Privileged Access
- ACL – Login Access

This simple and clean view with high-level gauges, historical trending and heat map allows you to quickly determine if any controls need further investigation.

For each supported control Splunk supplies a detailed view with interactive charts and tables that enable you to immediately drill down into the original event data and further understand what is causing the increased risk.

Splunk also supports additional controls depending on what other tools you may have in your environment. Other controls can be built and supported based on data collected from SCAP tools. For example, the Splunk for Tivoli Endpoint Manager (formerly BigFix) application (available at no cost on www.splunk.com) will ingest information about vulnerabilities and patches from your Tivoli Endpoint Manager server. Splunk’s ability to ingest data in any format and then perform on-the-fly normalization makes it possible to generate continuous monitoring reports and gain wider visibility—and consolidate multiple tools in the process.

The Splunk App for FISMA is based on a common information model (CIM) that allows for easy mapping of new data types and sources into the application. Also, since the App was built with automated reporting in mind it is fully compatible with the Office of Management and Budget’s (OMB) interactive collection tool, CyberScope.

Free Download

[Download Splunk](#) for free. You’ll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.