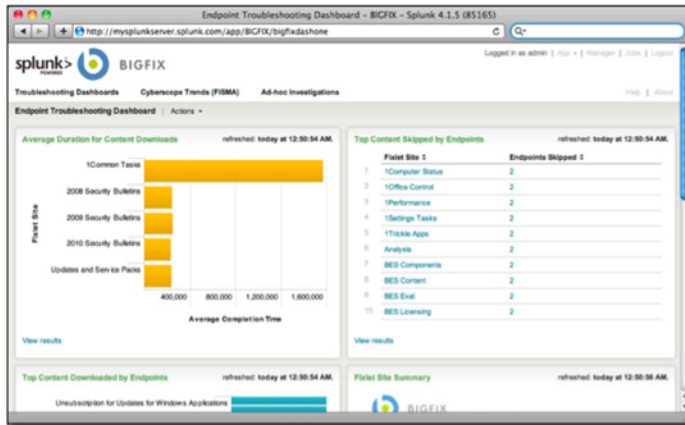


Splunk App for BigFix

Using Splunk for continuous monitoring supporting FISMA 2.0.

The Challenge

In recent interviews with various federal agencies including the Department of Homeland Security (DHS), it was revealed that the audit and accountability (AU) controls in NIST 800-53a pose a big challenge for FISMA compliance. The challenges are:



- Continuous Monitoring — Need for Real Time and Dynamic ability to monitor changes or threats (800-37)
- Immediate Scaling — Scale as mission or data rapidly increases and changes across multiple platforms or sites (800-39)
- On Going Authorization — Reporting real-time trending and historical views of large data sets from multiple sources (800-53)
- Real Time Risk Assessment — Tie enterprise architecture to security process for Risk Management Framework (RMF) (800-37)

Federal Agencies have hundreds or thousands of custom applications running on servers and workstations that make compliance with NIST 80-53 AU technical controls problematic. The AU controls cover the creation of incident response policies, assessment methods and objectives, and identify data to be collected and stored for system performance and configuration (see FISMA: Audit & Accountability Control table on page two).

Monitoring key components of the national infrastructure means needing to look beyond snapshot audits, preparing for continuous monitoring, and compliance transparency for governing agencies.

The Solution

Splunk Enterprise and BigFix together meet the 800-53 AU technical audit and accountability challenges.

BigFix provides the ability to manage hundreds to hundreds of thousands of systems in real time. The BigFix agent resides on the host and has comprehensive visibility into any host configuration data, including patch status, configuration

status, malware status, software installed and more. The status of this information is visible in real-time from the BigFix Unified Management Console and helps to satisfy AU control compliance. Agencies that find themselves addressing issues in a reactive mode can become proactive and gain situational awareness over their infrastructure, reduce security risks, and eliminate unnecessary costs.

BigFix helps IT operations and security teams become proactive by supporting sustainable and cost-effective compliance programs.

While BigFix provides pervasive visibility into the current state of the endpoints in real-time, the solution can be augmented with Splunk to provide comprehensive real-time and historical trending and reporting, as well as user specific dashboards for operational intelligence and situational awareness.

Splunk, with its ability to scale to collect, index and report on terabytes of time-stamped ASCII text data monitors the BigFix data stream and provides the critical continuous monitoring for AU controls 3 through 14 in real-time. Splunk also allows the user to configure real-time graphical elements based on saved searches that can be aligned with an agency's key performance indicators (KPIs). The user can also drop-and-drag these graphical KPI elements onto dashboards monitoring key agency metrics. Using Splunk's built-in role-based access controls, dashboards can be created for various parts of the agency or the Office of Management and Budget (OMB). This creates agency transparency and supports continuous monitoring audit views for FISMA compliance, and provides ongoing operational intelligence into the current and historical security state of the infrastructure.

Using Splunk to Troubleshoot and Audit BigFix

For many agencies with BigFix installed, BigFix has become mission critical. Using Splunk to troubleshoot BigFix issues can yield faster results.

- Splunk supports ad-hoc investigations, allowing the BigFix administrator to troubleshoot in real-time (the alternative is to escalate the issue and ship the logs to BigFix developers)
- Splunk can monitor the health of the BigFix environment, sending a proactive email alert if a relay (running on Windows machines) is down. The admin gets an alert from Splunk without having to log into BigFix.
- BigFix performance can be affected by external factors. An IDS, firewall or Host based IDS can interfere with commands or cause a client loop. Splunk can give visibility into the larger network environment in which BigFix is running.
- Splunk can use a 'transaction' command to monitor the amount of time it takes for BigFix components to communicate with each other. Splunk can alert if a Fixlet messages is taking longer than average to get to a client.

- Splunk can monitor BigFix master operator actions. Having multiple users with “Master Operator” level credentials means those users can change any BigFix component. Controls to keep master operators from changing component assets cannot be separately enforced. Splunk can act as a mitigation control by monitoring Master Operator actions in the audit table of the SQL database for inappropriate use or action.

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.

Splunk & BigFix – Working Together in Real-time

Understanding what’s happening in your enterprise architecture in real-time is the key benefit of having Splunk and BigFix in your environment. BigFix endpoints report back anytime there is a status change and can be configured to continuously or selectively enforce endpoint policies such as Federal Desktop Core Configuration (FDCC). Splunk provides the metrics and single pane of glass for time-stamped ASCII text and can communicate with third-party data sources that contain critical asset information.

FISMA: Audit & Accountability Control	BigFix	Splunk
AU-3 Content of Auditable Events	•	
AU-4 Audit Storage Capacity	•	•
AU-5 Response to Audit Processing Failures	•	•
AU-6 Audit Review, Analysis, and Reporting		•
AU-7 Audit Reduction & Report Generation		•
AU-8 Time Stamps	•	
AU-9 Protection of Audit Information	•	•
AU-10 Non-Repudiation	•	•
AU-11 Audit Record Retention	•	•
AU-12 Audit Generation	•	•
AU-13 Monitoring for Information Disclosure	•	•
AU-14 Session Audit	•	•