splunk>

TECH BRIEF

ENABLING REAL-TIME VISIBILITY AND REPORTING ON COMPLIANCE CONTROLS WITH SPLUNK

A Historical Challenge

Maintaining visibility into security posture with respect to federally-mandated information security controls has historically been a challenging and often time-consuming line of activity across Federal agencies, DoD components, systems integrators, contractors, and research institutions. These challenges in many ways have been driven by the underlying technical complexities of implementing meaningful solutions for automated analysis and reporting on the status of information security controls specified in NIST Security Engineering and Risk Management Group guidance and doing so in a timely manner.

Evaluating the Underlying Historical Technical Complexities

Distilling down these underlying technical complexities reveals four key challenges: scope and scale of information and systems; diversity of the environments; constant changes across the environment; and aggregation, analysis and status reporting on security posture.

Scope and Scale

In many cases, the scope and scale of most executive agencies, DoD components, large systems integrators, and research institutions are so complex and distributed that agency heads, chief information officers senior information security officers (ISSMs/ISSOs) have historically been challenged to effectively maintain a comprehensive view of their security posture across the whole of their organization and down into each of their suborganizations.

Diverse Environments

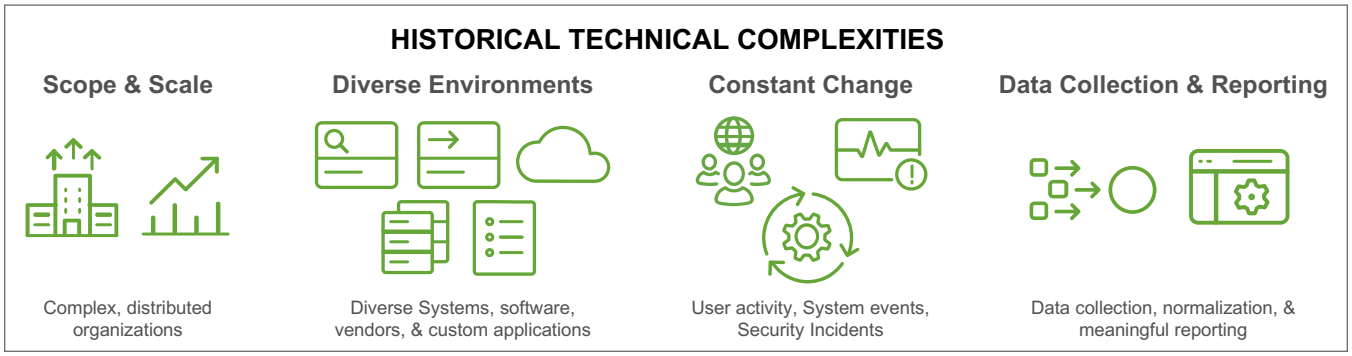
Further complicating this scope and scale challenge is the diversity of the environments across these organizations. In many cases sub-organizations, with their varying responsibilities, priorities, and mission sets, contain a diverse array of systems, software and vendors. When viewed individually, the components of these diverse environments are not necessarily problematic from a security perspective. The key challenge arises when attempting to gain a comprehensive understanding of security posture across the diverse components of a sub-organization's infrastructure. This sub-org challenge exists to some degree across each component and when aggregated up to the full Executive agency, DoD component, or organizational level, it makes holistic understanding of security posture a considerable challenge. Leaders need a solution that can provide visibility into down into and across their environments, regardless of its architecture or the components it is comprised of.

Constant Change

Adding to the challenges posted by the scale and diversity of these environments is the near constant change introduced by system usage and configuration. The dynamic nature of information systems and users creates a real-world scenario that requires continuous monitoring to truly understand the security posture of an environment, sub-agency or agency.

Data Collection and Reporting

Beyond the importance of complying with federal law and DoD instructions, understanding and reporting on the security posture of information systems that agencies use to drive critical missions is a matter of national stability and security. Unfortunately, the data collection, analysis and compilation required for reporting can be a time-consuming exercise that takes time away from other important tasks and in some cases produces an outdated view of system security posture. This challenge ties in closely with the importance of continuous monitoring mentioned previously in the context of constant change. if that reporting is simply an outdated snapshot in time versus a near real-time assessment driven by continuous monitoring, then agency leaders are ill-equipped to make data-driven decisions related to the status and security of the critical infrastructure under their purview.



Splunk's Approach

Splunk has crafted a quick-start solution that is specifically tailored to address each of these historical technical complexities and drive rapid operationalization of continuous monitoring of technical security controls relevant to U.S. civilian agencies, DoD components, systems integrators, and research institutions. This solution was specifically aligned to address the key historical technical challenges cited above:

Scope and Scale

Splunk's compliance posture analytics solution, based on Splunk Enterprise software, natively provides a highly-scalable platform that can ingest and analyze virtually any type of machine data. This naturally aligns with the scope and scale challenge in that it provides an easy path to consolidate and automate collection of "compliance-relevant" status information - on-prem, in the cloud, or across hybrid environments.

Diverse Environments

Splunk software provides data normalization through a set of common information models. This means that the compliance posture solution provides a vendor agnostic view of even the most diverse environments - regardless of the the separate types of systems, information, and vendors that comprise any given agency or sub-organization. This cross-cutting, vendor agnostic view enables teams to look across the diverse components of their organizations and assess their posture with respect to the relevant technical security controls.

Constant Change

The pre-packaged analytics and visualizations included in Splunk's compliance posture solution, built on top of Splunk's near real-time architecture, ensures that agency heads and operations teams are able to identify security events that are trending toward non-compliance *as they emerge*. This continuous visibility into constantly changing environments is one of the drivers that has made Splunk Enterprise a central component of the continuous diagnostics and mitigation (CDM) program at the U.S. Department of Homeland Security. Unlike legacy solutions based on schema-on-write databases, Splunk's schema on the fly approach enables agency security and compliance analysts to ask additional questions of their data and drive new insights dynamically without having to wait to redesign a database schema first.

Data Collection and Reporting

Some of Splunk's largest customers ingest over two petabytes of data per day across distributed infrastructure and multiple geographic locations. Splunk's compliance posture analytics solution has created a total paradigm shift in continuous monitoring for compliance and information security by combining the ability to rapidly collect, analyze, and report on data from across complex environments and providing meaningful insights and reporting in near real time – all within the context of the relevant technical compliance and risk management frameworks applicable across Executive Agencies, DoD components, Federal Systems Integrators, and major research institutions.

Anticipated Impact

Accelerated path to compliance

- Wide visibility Agency-level or org-level compliance/security posture
- Newly gained visibility into compliance posture will aid prioritization of corrective actions for non-compliant resources

Consistent implementations

- Universal platform for machine data that consolidates and normalizes compliance/security-relevant data regardless of the vendor
- Data normalization supports consistent reporting across the agency/sub-agency while providing flexibility as systems and mission requirements continue to evolve

Maintaining compliance

- Visibility drives quick identification and correction of short-term variances/non-compliance

Better decisions based on current data

- Understanding the current status of the environment at any given time enables agency heads, chief information officers and senior agency information security officers to dynamically prioritize resources as the situation dictates

Splunk can help executive agencies, DoD components, systems integrators, and research institutions quickly gain visibility into the security posture of their systems in the context of FISMA, DoD RMF, or DFARS controls. Thousands of public and private sector enterprises already rely on Splunk software to gain visibility into their security posture, increase efficiencies, and enable data-driven decision-making. Contact us to learn more.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com