Sponsored Content

Washington Technology

Keep Cyberdefense on Target

DFARS and other mandates require a closer alignment of cybersecurity and compliance efforts.

carahsoft | splunk>

Drive the Convergence of Cybersecurity and Compliance

Simplified self-reporting and managing risk through enterprise-wide visibility are critical factors.

FOR YEARS, compliance-based approaches have helped government systems integrators, aerospace and defense contractors, universities, and Federally Funded Research and Development Centers (FFRDCs) maintain a minimal level of security. These reporting systems are largely used in support of Governance, Risk and Compliance (GRC) mandates. This approach, however, has largely fallen short of ensuring a truly effective security posture, especially in the face of today's dynamic threat landscape with sophisticated external actors and potential internal adversaries contributing to a rising wave of data breaches.

The growing supply chain, with its complexities and uncertainties, has added to the challenge of regulatory compliance and information security. Organizations are increasingly caught between investments in these two initiatives, as the two disciplines have diverged over time. In many cases, they're owned by different units or sectors. At the same time, the increasing dependence on external service providers is prompting government to ratchet up its security requirements to ensure all information transacted about their missions is secure and breaches are minimized.

Chief among them is DoD DFARS and the associated controls specified in the NIST 800-171 guidance that focus on data security. Specifically two new clauses, DFAR 242.204-7012 and FAR 52.204-21, speak to the disclosure of information and safeguarding contractor information systems respectively.

While these may be regarded as compliance requirements, they provide a layer of data protection and enhance security organization-wide and across the supply chain. Mapped to NIST Special Publication 800-171, they define the controls a contractor should implement while processing government information, and enable self-reporting to ensure smoother audits.

Given the government's active role in ensuring compliance with DFARS, contractors are highly recommended to prioritize meeting these regulations and lay the groundwork for future similar self-reporting mandates. In fact, this new requirement is just the beginning. Contractors should expect, and be ready to adopt and adapt to changes related to additional DoD mandates, as well as broader federal guidance and NIST controls as they find their way into common practice.

The controls were intentionally written so as to be open to interpretation. They're meant really as guidelines. In many

SOLUTION REQUIREMENTS

The most effective way to comply with DFARS requirements is a solution that can meet not only compliance needs, but also provide self-reporting capabilities and incorporate organizational processes for secure operations. At its core this solution should be:

Flexible: Must offer a framework that includes all organization's business process entities

Scalable: Must account for business growth, whether organically, through acquisitions, partnerships or a combination

Central Management and Federated Access: Must provide centralized management through a single pane-of-glass to ensure consistent, easy management and self-reporting and organization-wide access to stakeholders through role-based access control

Data Source Agnostic: Must quickly interface with any and all data sources required to meet compliance requirements

Extensible: Must go beyond compliance and enable proactive security measures to enhance information protection against any and all threats—internal and external—and extend ROI.

Real-Time Architecture: Must aggregate log data and other relevant information from across the enterprise in real time to achieve accurate situational awareness.

Customization: Must be able to query and build inquisition mechanisms and visualizations based on stakeholders needs to effect quick decisions.

shutterstock.com

cases, these controls don't map on a one-to-one basis to NIST's SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations). However, there are many similarities.

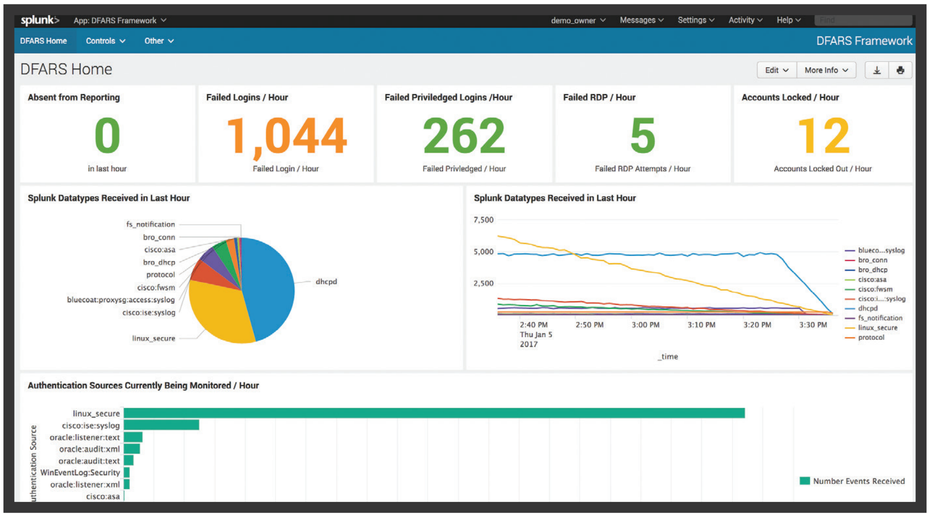
"Depending on the organization and its systems, these controls can be interpreted as either policy-based or technical," says Chris Hill, Director of Aerospace and Defense at Splunk. "Take Access Control 3.1.18, as an example, which directs contractors to control connection of mobile devices. You might think of a mobile device as a smart phone. But when you look a little deeper it could mean USB drives, laptops or any device that is not tethered. So it's open to interpretation. Every company doing business with the government has to interpret it based on their dealings and interactions to ensure complete protection of information being stored, transacted, shared or processed."

Previously, there was no one solution that could help organizations meet these broad compliance requirements and enhance security posture. Instead, they had to resort to interpreting DFARS or other compliance mandates and look for tools and products that could deliver on individual requirements and integrate them later. In most cases, if not all, they fell short of the goal for several reasons:

- The solution delivery process was inherently dispersed and in multiple silos in the form of heterogeneous processes and systems, making collecting and organizing information for reporting difficult, if not impossible.
- Since systems were set up to share information on a need-to-know-and-share basis, it was difficult to share information for compliance purposes.
- The various tools and products themselves don't easily integrate, requiring significant implementation and IT involvement.
- They don't meet the information currency requirement or provide self-reporting capabilities, making the audit process arduous and time-consuming.
- They require a trained and available administrator.

ENTER SPLUNK

Splunk is a leader in compliance and security solutions, and provides a framework expressly built on a flexible and extensible analytics platform. The Splunk platform automates compliance requirements, enables self-reporting and eases audits while enhancing an organization's overall security posture. The platform cuts across silos of operations and gathers, aggregates and correlates machine data, the authoritative trace generated by all digital activities. It's the one single source for simplified review and analysis in real time.



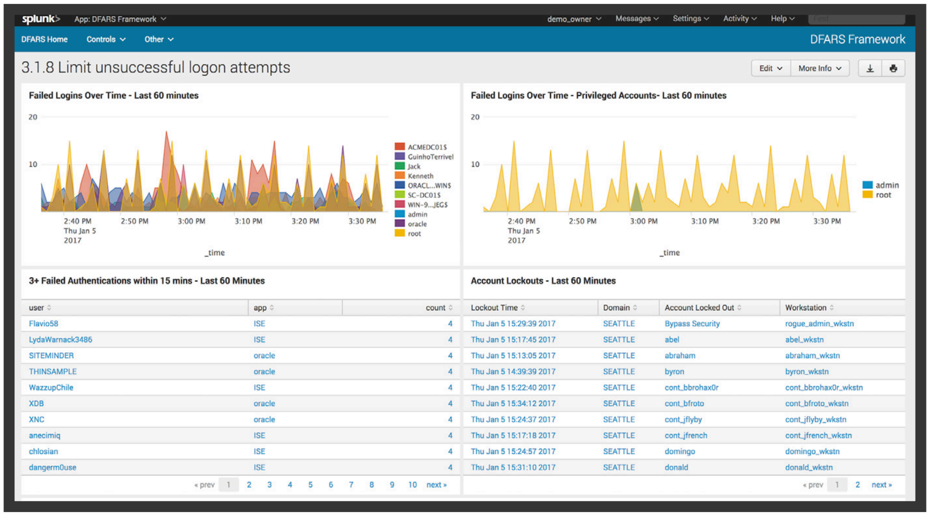
Splunk overcomes the traditional challenges of ingesting and normalizing data from heterogeneous systems by using schema-on-the-fly technology, eliminating the need to fit incoming data into predefined schemas but connect the dots as analysis and inquisition are carried out. It also removes the tedium of manual and ad-hoc data collection processes, which is a huge challenge with auditing compliance.

With this type of enterprise platform and a DFARS-specific framework, it's much easier to automate the reporting process instead of relying on manual processes, such as filling out spreadsheets and entering data for each application. Besides greater speed and accuracy, the system simplifies the audit process and speeds the resolution of issues before they result in major impact.

FLEXIBILITY IS KEY

To facilitate DFARS compliance, data from across an organization needs to be collected and aggregated in one place. Government contractors are often dispersed—not just into logical business units, but also geographically. The nature of their business has prompted organic growth and the need to team with other external providers to deliver on their business priorities. This not only means a complex collaboration and information-sharing environment, but also the need to account for resource churn (personnel who gain and lose access) which has to be monitored in real time.

Splunk's DFARS framework is built to provide the flexibility contractors need. It can gather data from any source and store it without requiring customization and database schema definitions every time a new source is added. Splunk uses a Common Information Model (CIM), to which thousands of data sources are already mapped. This simplifies and accelerates data ingestion. This inherent normalization, combined with the ability to define schema on demand (referred to as 'schema-on-the-fly' technology), makes for fast retrieval and the ability to quickly search and retrieve answers. The Splunk framework also offers predefined dashboards and reports for DFARS compliance. And with role-based access, auditors have access to the information in real time whenever it's required.



3.1.8 Limit unsuccessful logon attempts

Failed Logins Over Time - Last 60 minutes

Failed Logins Over Time - Privileged Accounts- Last 60 minutes

3+ Failed Authentications within 15 mins - Last 60 Minutes

user	app	count
Flavio58	ISE	4
LydaWarnack3486	ISE	4
SITEMINDER	oracle	4
THINSAMPLE	oracle	4
WazzupChile	ISE	4
XDB	oracle	4
XNC	oracle	4
anecimiq	ISE	4
chlosian	ISE	4
dangerm0use	ISE	4

Account Lockouts - Last 60 Minutes

Lockout Time	Domain	Account Locked Out	Workstation
Thu Jan 5 15:29:39 2017	SEATTLE	Bypass Security	rogue_admin_wkstn
Thu Jan 5 15:17:45 2017	SEATTLE	abel	abel_wkstn
Thu Jan 5 15:13:05 2017	SEATTLE	abraham	abraham_wkstn
Thu Jan 5 14:39:39 2017	SEATTLE	byron	byron_wkstn
Thu Jan 5 15:22:40 2017	SEATTLE	cont_bbrohax0r	cont_bbrohax0r_wkstn
Thu Jan 5 15:34:12 2017	SEATTLE	cont_bfroto	cont_bfroto_wkstn
Thu Jan 5 15:24:37 2017	SEATTLE	cont_jflyby	cont_jflyby_wkstn
Thu Jan 5 15:17:18 2017	SEATTLE	cont_jfrench	cont_jfrench_wkstn
Thu Jan 5 15:24:57 2017	SEATTLE	domingo	domingo_wkstn
Thu Jan 5 15:31:10 2017	SEATTLE	donald	donald_wkstn

SCALABILITY IS CRITICAL

Organizations that provide services to the government base their teams on the type, size and complexity of projects. While one project may not require significant resources, another might involve multiple teammates, technology providers and internal resources across business units. While an initial proposal may involve just a few people, delivery after winning work could require the organization to scale quickly.

Splunk's platform can ingest data that is a few megabytes per day and scale rapidly to petabytes per day without any modifications. This is particularly important since an organization's network is considered unclassified; and even with logical partitions, any data spill or unauthorized access needs to be reported in real time to ensure such breaches are contained and impact minimized.

CENTRAL MANAGEMENT WITH FEDERATED ACCESS

Given the distributed nature of systems and resources, it is critical to manage information from one central location. A single interface offers organizations a simplified consistent end-to-end view across silos without having to individually access them and correlate with other systems. This also affords the user the ability to ask any question and drill down into details to understand any specific activity and report on them.

Splunk enables federation with role-based access so stakeholders across the organization and supply chain can have their own customized views based on their interests and requirements. An auditor can be given the necessary views which can be accessed anytime and in real time.

DATA SOURCE AGNOSTIC

Compliance-related data comes from a variety of systems, devices, applications and networks. That makes it essential for a platform to be able to absorb and analyze data regardless of the source. Without that capability, organizations will have to manually ensure systems and data sources are compliant. They would have to request or write custom software or use a variety of tools to collect and analyze data.

With a platform like Splunk, which can ingest data from more than 1,000 different systems, contractors and organizations can be sure the process will remain automated and efficient. And for any sources that don't have a tie-in, it's easy to develop and deploy Splunk apps.

EXTENSIBILE TO MAXIMIZE ROI

Organizations are looking to invest in strategic technologies and partner with vendors who can improve business processes and ensure efficacies. In other words, they need a solution that can solve multiple challenges can extend an organization's investment in technologies.

Splunk's platform ingests machine data. For example, web server logs not only help with troubleshooting IT performance issues, but also lend themselves to hunting malware and performing business analytics. This capability, combined with access control and analytics, lets people ask different questions of the same data with which Splunk has already resolved multiple challenges.

MAXIMIZE EFFICIENCY

Instead of manually entering, compiling and reporting on data, it's far more efficient to automate the entire data collection process, analysis and report production process. It's more efficient when auditors have a tool that ingests, analyzes and visualizes data in real time.

Such a solution should be able to ingest data— including logs and other authoritative information—from any source regardless of type or format in real time. Analysts and operators get end-to-end, holistic visibility into all processes, user activity and systems. They can query data, look for insights and dynamically build visualizations and dashboards, while digging in at a granular level to understand the interactions, transactions and activities.

ABILITY TO CUSTOMIZE

Many reporting tools provide standard report formats, often addressing the lowest common denominator. The ability to quickly and easily create custom reports not only provides organizations with deeper insight into their operations, but helps satisfy DFARS compliance requirements. Customization is particularly important in the case of DFARS reporting controls, which most organizations interpret and measure differently. The ability to customize dashboards, visualization, searches and data collection makes compliance simpler and faster.

Even the Splunk framework itself is customizable. For example, an organization can customize dashboards to create real-time alerts for non-compliance, which lets teams quickly drill down and find out what is causing the non-compliance issue.

Meeting DFARS reporting requirements will take time and effort. Starting now and using the right type of platform and framework, organizations can get it done correctly and on time. Missing the deadline has consequences, like fines or lost bids. It will not reflect well on past performance and could result in a loss of confidence and reputation with potential partners.

BEYOND DFARS

DFARS is just one example of a growing set of requirements with which government contractors must comply. Compliance and cybersecurity are converging for broader visibility and to simplify self-reporting and auditing. A critical component to addressing these objectives is an understanding of how organizations will address the emerging security measures being put in place to protect any Unclassified Controlled Technical Information (UCTI) under the new DFARS compliance rules.

While DFARS may seem specific from a compliance perspective, it has broader reach and ramifications, such as prompting additional scrutiny to ensure security. From a compliance perspective, ad hoc and manual reporting or auditing processes will not scale, can cause delays and have further consequences downstream. Continuous monitoring will become a reality since any non-compliance will need to be spotted in real time, not when an audit is scheduled. Organizations will require near real-time, automated self-reporting capabilities so continuous audits can be regular and non-intrusive.

Compliance management may have diverged from cybersecurity, but with risk management approaches gaining favor as a preferred method of managing cybersecurity posture, it only makes sense for compliance and security to converge from a management perspective. The Splunk platform not only satisfies these growing requirements, but can also bring data together from across an organization in real time, accommodating today's dynamic supply chain.

DFARS REPORTING REQUIREMENTS

Before getting started with a platform or framework, ensure stakeholders understand what each control represents. Then inventory assets to understand what is present and establish a measurement baseline. DFARS reporting requirements include:

Access Controls:

3.17: Prevent non-privileged users from executing privileged functions and audit the execution of those functions

3.18: Limit unsuccessful logon attempts

3.1.18: Control connection of mobile devices

Audit and Accountability: 3.3.2
Ensure actions of individual users can be uniquely traced to those users so they can be held accountable for their actions.

Physical Security: 3.10.2
Escort visitors and monitor visitor activity to ensure visitors are validated and activities are traceable and accountable.

carahsoft. splunk>

For more information, please visit:
www.splunk.com/en_us/solutions/industries/aerospace-defense.html