Getting Security Compliance Under Control, Once and for All

MARKET TRENDS REPORT

govloop qmulos splunk> carahsoft

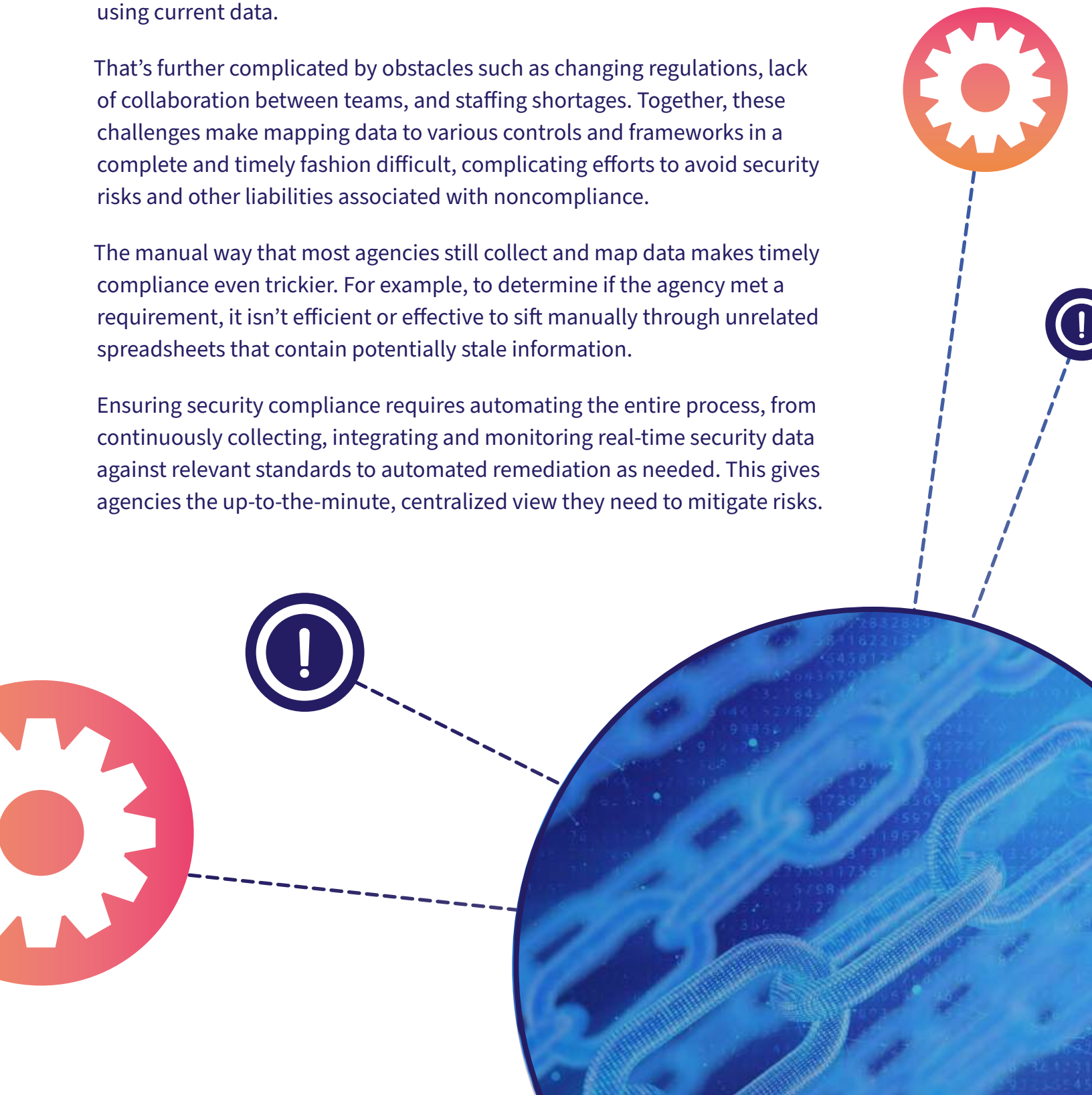
Executive Summary

Federal agencies must comply with an increasing number of stringent cybersecurity regulations to mitigate risk and improve cyber posture. But compliance isn't easy: Organizations must prove that they have implemented, and are continuously monitoring, specific security controls using current data.

That's further complicated by obstacles such as changing regulations, lack of collaboration between teams, and staffing shortages. Together, these challenges make mapping data to various controls and frameworks in a complete and timely fashion difficult, complicating efforts to avoid security risks and other liabilities associated with noncompliance.

The manual way that most agencies still collect and map data makes timely compliance even trickier. For example, to determine if the agency met a requirement, it isn't efficient or effective to sift manually through unrelated spreadsheets that contain potentially stale information.

Ensuring security compliance requires automating the entire process, from continuously collecting, integrating and monitoring real-time security data against relevant standards to automated remediation as needed. This gives agencies the up-to-the-minute, centralized view they need to mitigate risks.



By The Numbers

20

Number of federal agencies that failed to meet their event logging requirements as of August 2023

4,300

Average number of hours an organization annually spends achieving or maintaining compliance

"Where in years past a compliance team might have mitigated national security risks through sanctions-screening software and attention to a few sanctioned countries, today a new level of diligence and attention is required."

- Marshall Miller, Principal Associate Deputy Attorney General

61%

Amount of organizations whose compliance team's top strategic priority is keeping abreast of upcoming regulatory/ legislative changes

$12.72 billion

How much the federal government is predicted to spend on cybersecurity in 2024

700

The number of cybersecurity-related recommendations the Government Accountability Office has issued for federal agencies in the last 12 years

Security Compliance Faces Many Obstacles

Challenge: Multiple Roadblocks

Fully complying with evolving security standards can be difficult, especially with older, more manual and disconnected processes and data collection methods. Here are some of the biggest challenges:

Outdated Data. It's nearly impossible to ensure system compliance when analyzing outdated information. Take the example of Authorities to Operate, which typically certify systems for three years. Because of the effort required to update relevant data, an agency might update only one-third of it each year, on a three-year cycle. That means that two-thirds of the data is outdated at any given time. This can result in both noncompliance and unnecessary risks to the environment.

Disparate Data Storage. Collecting data is one thing, but storing it is another. Evidence for some controls could be on a user's laptop, in a personal folder, on a hard drive or in the cloud, for example. This makes ensuring that data is current and complete, along with verifying the origin of the data, difficult to prove. It also doesn't help that compliance and cybersecurity teams often operate in silos.

Frequent Data Collection and Analysis Deadlines. Many frameworks, mandates and controls require the same data several times per year, but in slightly different ways or formats, and per different timelines. This means agency staff must manually cross-map data to evidence requirements and controls, and then the controls to the various frameworks. It also typically requires an internal compliance team member to communicate with the person who runs that control to interpret the requirements and produce the right data in the correct form. This can result in a conflict of interest: An administrator running the control might want to paint the best picture, resulting in a misrepresentation of the true control posture.

Solution: Compliance Automation

To deliver current data that satisfies auditors in a timely fashion and improves its strength and security, an organization needs an automated approach to data gathering, analysis and monitoring. An effective automated compliance solution should be able to gather real-time data from all cybersecurity tools, applications, devices and platforms, regardless of where they are located or the type of data they house.

The system should interpret the data as it comes in from those systems to determine whether or not they're performing as effective controls for specific frameworks. A single dashboard should show everything being collected and mapped to each control, which makes it easier to identify anomalies and patterns.

Continuous, up-to-the-minute monitoring is important because it takes only seconds to exfiltrate a piece of data, including critical data. When the system identifies an anomaly or failed control, it should automatically remediate the issue.

Finally, it's critical to integrate threat intelligence into the automated compliance platform because that goes a long way toward mitigating risks from social engineering and other cybersecurity threats.

"Essentially, you are enabling real-time monitoring and visibility, which provides risk observability" and aligns with the zero-trust concept of conditional access, said Igor Volovich, Vice President of Compliance Strategy at Qmulos. "Instead of instructing the firewall administrator to close specific ports to address an issue, you can leverage the automated compliance model to assess control resilience, strategically reposition and prioritize assets, and appropriately close off vulnerabilities as necessary."

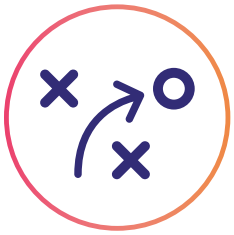
Best Practices

1. Respect the value of real-time data.

Data is the centerpiece of automated security compliance. Without it, compliance simply isn't possible. "It's easy to become confused about what's evidence, what's anecdotal and what's real because data has been through many hands, but ultimately data tells the truth," said LaLisha Hurt, an Industry Advisor at Splunk. "And without real-time data, it's difficult to communicate the story and make informed decisions that drive mission outcomes for government agencies."

2. Use automation to manage both risk and security.

Risk, security and compliance use much of the same data, but those functions traditionally are siloed. Newer automation technology allows agencies to use the same tech to monitor all of them. "For [security operations], you're looking at specific technologies, products and vendors, and with compliance, you have the same visibility, but through the lens of controls," Volovich explained. "You're abstracting one layer above, so instead of focusing on what your Palo Alto Defender or CrowdStrike solution is doing, a risk or compliance manager would focus on how insider threat management or [a] perimeter security control category is performing."



3. Leverage a single platform.

Start by identifying which frameworks and standards your agency must follow. Then take a full inventory of critical data, wherever it exists. Adopt a platform that can collect vast data from diverse sources, such as public and private clouds, on-premises data centers, third-party tools, custom and third-party apps, services, and devices. Then, find an automated compliance platform that can ingest, correlate, monitor and analyze that data in real time to generate audit trails. Leveraging a single platform to monitor and manage all of your cyber and compliance mandates provides a window into the same data but for different purposes — and that improves your security posture.

4. Measure progress against the gold standard.

If your compliance platform can stand up to Intelligence Community Standard (ICS) 500-27, the gold standard for enterprise insider threat management compliance within intelligence community organizations, you know you're on the right track. The standard requires granular auditing of insider threat activities to identify poor security practices and anomalous or risky behaviors.

5. Ensure that you are not a weak link.

DoD contractors in the Defense Industrial Base must comply with the CMMC, which aims to strengthen the security posture of prime contract holders interfacing with customer networks. It is critical that these DoD contractors use data-driven compliance automation tools to ensure that they aren't the weak link in the cybersecurity echo system.

Case Study: Ensuring Compliance, Now and in the Future

Leaders of a federal civilian financial agency, working to meet a looming deadline for the Office of Management and Budget (OMB) M-21-31 cybersecurity rule, realized their largely manual approach of logging data across hundreds of IT systems wouldn't work. It was too resource- and time-intensive and left the agency vulnerable to threats and missed deadlines. They needed a more automated approach — one that would ensure real-time, continuous compliance.

The agency turned to Qmulos' Q-Compliance platform, combined with Splunk's data analytics technology, to create an all-in-one solution that optimizes risk management efforts with real-time continuous monitoring. With this solution, the agency no longer needs to identify, analyze and manually report each log within the multisystem infrastructure. Instead, Qmulos searches the data in Splunk, and Q-Compliance provides real-time evidence.

Throughout the process, Qmulos collaborated closely with the agency's development and internal security teams to decode requirements related to the OMB mandate. This involved a comprehensive analysis of the agency's logging architecture and log data and working with Qmulos subject-matter experts to navigate the mandate's complexities and help with data onboarding.

The solution not only enabled the agency to meet the logging deadline, but proved that the agency was operationally secure. Agency leaders also know they have a repeatable and scalable way to continuously monitor controls in real time.

HOW QMULOS AND SPLUNK HELP

Together, Qmulos and Splunk have created an ecosystem that enables agencies to automate security compliance.

Q-Audit, built using ICS 500-27, uses machine data and proprietary insider threat analytics and alerts to detect anomalies in real time. Splunk provides the data layer through its data access model, which can collect information from any source across cybersecurity tools, applications, infrastructure and platforms.

For compliance requirements, Qmulos provides the expert translation layer on top of the data layer, interpreting the data as it enters the system. Q-Compliance delivers real-time insights and automated alerts about the organization's posture against frameworks and standards, such as National Institute of Standards and Technology (NIST) 800-53 and 800-171 (included in the Cybersecurity Maturity Model Certification), the Health Insurance Portability and Accountability Act, NIST's Cybersecurity Framework, the OMB M-21-31 rule, and the Federal Risk and Authorization Management Program/ StateRAMP, plus custom controls based on organizational requirements. Q-Compliance also helps organizations comply with zero-trust principles and aligns with the MITRE ATT&CK framework's threat-informed defense effort.

Q-Audit drives the analytics and alerts specifically built for ICS 500-27-defined event families and is designed for insider threat management. Real-time, customizable dashboards offer full visibility and enable agencies to drill down, on a granular level, to monitor and alert on auditable events and audit sources. Q-Audit also can map vendor-specific event codes to the audit policy and auditable event categories, showing what to log and how to monitor those logs in real time.

Conclusion

Agencies must comply with a host of security-related mandates and frameworks. Although they work hard to meet deadlines and provide necessary data, many agencies risk falling behind, thanks to manual processes and outdated data. It also can be difficult to find data stored in many places and to repeat data-finding activities and reporting in different formats for different audits. These challenges can lead to noncompliance, fines and other penalties, and can jeopardize security.

Manual processes are largely to blame. Replacing them with an automated approach to compliance not only helps agencies meet compliance deadlines, but improves overall cybersecurity. It also can save thousands of worker hours that organizations currently waste performing manual compliance processes. Without automation, agencies miss their mark in meeting their mission and IT job efficiency, costing hundreds of thousands of dollars.

An automated compliance solution should automate every step of the process, from data gathering, analysis and monitoring to mapping, identifying anomalies and patterns, and remediation. The most advanced system can even monitor users and device activity to ensure that agencies fulfill audit controls' actual purpose and mitigate organizational risk.

ABOUT

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government. For more information about this report, please reach out to info@govloop.com.

Qmulos is a next-gen compliance, security and risk management automation provider, delivering continuous compliance through its flagship Q-Compliance, Q-Core, and Q-Audit technology platforms. Qmulos enables organizations to achieve high compliance confidence while delivering a powerful and engaging compliance experience across all functions and phases of the enterprise compliance lifecycle. Leading government, commercial, and academic organizations use Qmulos' solutions to ensure the highest levels of cybersecurity.

Splunk helps make organizations more digitally resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent infrastructure, application and security incidents from becoming major issues, recover faster from shocks to digital systems and adapt quickly to new opportunities.

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the master government aggregator for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop