SPONSORED BY

qmulos

Achieving real-time compliance and cybersecurity

How Qmulos and Splunk made it happen

SC Media

CRA Business Intelligence

ebook
An SC Media publication

Compliance Automation + data analytics = a powerful process

Cybersecurity and regulations have grown far too complicated to rely on manual compliance processes. ***Paul Wagenseil*** *explores the value of modern, automated compliance-management platforms.*

OUR EXPERTS

LaLisha Hurt
Federal Government Industry Strategist, Splunk

Tieu Luu
Chief Product Officer, Qmulos

Lee Waskevich
Vice President Security, ePlus

Ross Young
CISO-in-Residence, Team8

As cyberattacks become more sophisticated and damaging and government agencies and industry bodies react to new threats by imposing additional rules and regulations, organizations need help adapting to the changing landscape and modernizing outdated compliance processes.

To keep up with ever-shifting regulations, and to boost their cybersecurity defenses against increasing threats, enterprises and large companies are moving toward modern, automated governance, compliance and risk-management (GRC) platforms.

One of the most effective ways to implement a modern GRC platform is to pair it up with a robust and well-known data-analytics tool like Splunk. Qmulos offers compliance automation applications that run in Splunk and continuously monitor the effectiveness of security controls across multiple compliance frameworks, identify weaknesses and deficiencies and ultimately reduce risk.

Combining the sweeping data-ingestion capabilities of Splunk and the continuous control monitoring capabilities of Qmulos can not only bring an organization up to date with modern compliance processes but prepare it for the unforeseen threats and regulatory changes of the future.

The following pages outline the challenges that led to the Splunk/Qmulos partnership and how that partnership works.

> ***"You're just drowning in new compliance mandates that are in many cases overlapping and redundant. The underlying controls to secure accounts, detect attacks, prevent supply-chain threats, and so forth are all the same."***
>
> **Tieu Luu** | Chief Product Officer, Qmulos

Why legacy compliance programs don't measure up

Compliance-management programs have gone through several stages as regulators and industry bodies have imposed new requirements, from HIPAA to PCI DSS to FINRA to GDPR. Each stage adds another layer of complexity and more process consolidation.

Ross Young, CISO-in-Residence at Team8, says there are four generational differences in GRC tools:

1. **Focus on filling out one questionnaire per standard.**
2. **Have one umbrella framework mapping to all the standards so organizations only have to fill it out once per team.**
3. **Focus on collecting evidence automatically from organization tools to fill out the questionnaire for everybody else.**
4. **Map to things that are more influential and effective, like the MITRE ATT&CK framework and other things that may not just be a particular standard.**

Most organizations are somewhere between the second and fourth stages. Few may be able to fully automate their processes, leaving them at a disadvantage as the pace of regulatory change accelerates.

Security issues growing more dire

Those changes are driven by the increasing complexity of threats, and the increasing rate at which new threats emerge.

"What we're seeing across the board is a rising volume and sophistication of cyberattacks," says LaLisha Hurt, Federal Government Industry Strategist at Splunk. "This includes anything from ransomware, phishing, advanced persistent threats, as well as increasing regulatory compliance demands. We see this with agencies having to navigate a growing list of global, regional and industry-specific regulatory frameworks."

Cybersecurity tools and service providers are the first to react to new threats, but some types of threats become so pervasive that new regulations are created as a result. Credit card theft led to PCI DSS; identity theft and privacy issues led to GDPR; and as we'll explore in a bit, the SolarWinds supply-chain attack led to a new government regulation known as OMB M-21-31.

"[Regulators] come out with new requirements, recommendations, best practices for how organizations need to respond to protect against those things," says Tieu Luu, Chief Product Officer at Qmulos. "And then to really force people to do those things, they become compliance requirements."

That's all well and good, at least in theory. You can also make a good argument that strict regulations help raise the bar for cybersecurity across industries. However, the sheer number of rules and regulations, and the substantial overlap between competing standards, can result in cybersecurity personnel and compliance officers becoming overwhelmed.

"You're just drowning in new compliance mandates," says Luu. "And a lot of them really cover the same thing. The underlying controls to secure accounts, detect attacks, prevent supply chain threats, and so forth are all the same."

Lee Waskevich, Vice President of Security at managed service provider ePlus, says that even efforts to modernize business practices or methods — such as by incorporating AI, migrating assets to the cloud or streamlining network architecture — can also lead to more risk, threats and regulations.

"Outside of the threats, attacks and lack of resources, there's also cyber challenges that are coming by way of business initiatives, in terms of how they're disrupting their own businesses, serving their customers and constituents, or otherwise," Waskevich says. "This then spurs on new types of attacks, and those attacks are, then, many times what's used as part of governance and compliance frameworks and standards that people have to make sure they shore up against."

Questionnaires and snapshots don't convey the full picture

Given this unstoppable cycle of threats, reactions, regulations and more threats, it's getting harder and harder for organizations to keep pace.

That's especially true when the organizations are hampered by compliance-reporting methods and audits that involve manually filling out questionnaires, interviewing a few key people in sensitive roles, reviewing security policies and controls, and capturing point-in-time samples or "snapshots" of an organization's compliance and security posture.

Occasionally, auditors will demand evidence, Luu says. But because it's done via sampling and point-in-time, organizations don't get a complete set. It's also out of date by the time it's done. With the speed at which threat actors operate, the speed at which threats and attack vectors evolve, those point-in-time mechanisms just aren't effective.

> ***"You're just drowning in new compliance mandates, and a lot of them really cover the same thing."***
>
> **Tieu Luu** | Chief Product Officer, Qmulos

Auditors sometimes settle for 'good enough'

It's through compliance and regulation that organizations can be certain they're maximizing their efforts against threats and shortfalls — if that compliance is done well. By implementing regulatory frameworks, companies can try to fill in security gaps, and all organizations have them in their security postures.

That's why it can be dismaying to encounter shortcuts and workarounds that may arise due to the complexity, or impossibility, of manual compliance, as well as the often-unclear nature of the required controls. Sometimes just showing that you have the policies in place is enough to satisfy auditors and assessors — but is that really boosting your cybersecurity?

Young worries about the still largely reactive attitude of the greater business and legal establishment towards compliance and cybersecurity, which again contributes to the cycle of incident-reaction-regulation-repeat.

"Nobody cares [about your compliance status] until after a breach," he says. "And then after a breach, they're going to cite you on standards that are vague and can be openly interpreted in any possible way — what the regulator thinks you should have done, versus what's required by the standards, versus what your outside counsel actually believes you need to do, are all completely different things."

> ***"When you start to see some of these large entities impacted by data breaches, you start to lose trust."***
>
> **LaLisha Hurt**
> Federal Government Industry Strategist, Splunk

How modern, automated compliance programs fill the gaps

Modern compliance platforms solve many problems by taking as much as possible out of the hands of humans and automating it:

- **Instead of in-person interviews, you have scanning of logs and actions.**
- **Instead of painstaking updates in the wake of a framework change, you have automatic implementation of new controls and requirements.**
- **Instead of point-in-time snapshots, you continuously monitor an organization's security controls and compliance stance.**
- **You're getting a movie instead of a few postcards, and you'll have a better idea of what must be fixed.**

"Once you're continually collecting all of that data, and you've got the full set, that's where automation comes into play," says Luu. "Now you can automatically flag when something has happened or when a device has been misconfigured that fails the control requirement."

Automation allows practitioners at both the executive leadership level, all the way down to junior analysts, to have almost real-time visibility into issues and risks, things that they should be working on and focusing on. It also allows teams to be more efficient overall.

That visibility into risk helps the top brass better understand the challenges that the security and compliance teams face. The CEO or the board may not understand the technical details of a network intrusion or a control shortfall, but they'll understand when something becomes a threat to the business's core mission.

Stronger, better, faster

Full-fledged, modern compliance programs certainly boost cybersecurity, but they may also confer a competitive advantage upon those organizations that use them over those that don't.

"Compliance frameworks help to provide that measuring stick by which you can hold an accounting to that company and making sure that they're taking the proper precautions, they're putting the right processes in place, they're leveraging technology when and where appropriate, and overall, they have a seriousness around maintaining that compliance," says Waskevich.

A strong security and compliance posture will certainly be a factor in business-to-business due-diligence and third-party-risk assessments. Nobody wants to take on a partner who's got a high level of cybersecurity risk, and no one wants to acquire a company that may have hidden cybersecurity flaws.

In finance, banking, healthcare or other highly regulated industries, being able to demonstrate security compliance beyond what your competitors can achieve is naturally an advantage. But will stronger compliance affect retail consumer behavior?

LinkedIn and Equifax suffered huge data breaches that compromised the personal information of tens of millions of customers, but they're still doing fine. Target's big credit-card breach impacted business in the short term, and the CEO resigned, but more than a decade later, it's still in business.

"Compliance alone is probably not going to be the differentiator for companies," says Hurt. "But if you do have an unfortunate security breach that's costly, you have downtime to your customers, you have damage to your reputation, there will be impacts."

When you start to see some of these large entities impacted by data breaches, she says, they start to lose the trust of customers and partners. Those entities start to wonder if your data and PII is secure.

Luu thinks the public's tolerance of security incidents that affect ordinary consumers may be changing, and that change may affect the nature of organizational compliance.

"There's increasing demand for more transparency in people reporting their security posture," he says, "There's a change in the climate, there's a change in regulations that's pushing for more transparency. And if you're doing things the old way, you're not going to be able to meet those increased demands for transparency and real-time reporting. For years, the mantra 'compliance does not equal security' has been widely accepted. However, with advancements in real-time compliance implementation and monitoring of critical controls, the narrative is shifting—modernized compliance is now essential for true security."

We'll have to see how long it takes the greater awareness of cybersecurity posture in American executive suites to trickle down to the shopping malls or to online retail customers. But Waskevich argues that another factor, one that has seen government regulators take cybersecurity executives to court, may accelerate the awareness process:

"The average tenure for CISOs and those in charge of security is lower and lower, and now CISOs are becoming increasingly liable if they're not performing the diligence required to help protect that company. It's incredibly important that the compliance tools are there to help provide a spotlight and really a guiding artifact, if you will, to help in the company to shore things up."

Combining compliance and security with data analytics

What's the ideal format for a modern, automated compliance and risk-management platform? For compliance automation provider Qmulos, it made sense to marry its software with one of the biggest data-analytics platforms out there: Splunk.

For Qmulos, Splunk offers a massive ingestion of data from across an organization that can be sifted, sorted, categorized and acted upon. Qmulos' tools can also work with the security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools built into Splunk to analyze and mitigate security incidents and shortfalls.

It was Splunk's "powerful underlying data infrastructure," as Luu put it, as well as its constant development, that made Qmulos decide to build its products atop the data-analytics giant.

Hurt points out that Splunk can gather information from anywhere in an organization – endpoints, cloud, remote, network infrastructure or otherwise – and provide Qmulos maximum visibility into processes, devices and other assets.

"Automation of compliance and security workflows is huge, because a lot of folks are managing all of these controls and frameworks manually," says Hurt. "The combination of our capabilities actually enables the automation of repetitive security and compliance tasks."

Luu says that while Qmulos does need Splunk to operate, it also accommodates compliance programs that may still have, as many do, some manual elements.

"We have the ability to automate that more human, manual workflow aspect of it," he says. "We detect a compliance finding, we can automatically create a POAM [plan of action and milestones], which then gets assigned to someone to go perform whatever steps are needed to go remediate the finding."

> *"You need that top-down executive-level buy-in to embrace this shift in how compliance is done today."*
>
> **Tieu Luu**
> Chief Product Officer, Qmulos

The data repositories created by Splunk and similar tools are also a prime target for attackers, as Hillestad points out, and must be carefully guarded. But if your organization can afford or already uses such a platform, and you can protect it, then running something like Qmulos alongside it becomes a no-brainer.

We're from the government, and we need your help

Luu related how in the past year, Qmulos and Splunk together helped a U.S. federal government agency drastically improve its compliance and security posture.

In the wake of the devastating SolarWinds supply-chain breach, which affected numerous government departments (and which also involved breaches at Microsoft and VMware) the U.S. Office of Management and Budget issued a new compliance standard in the form of Memorandum 21-31, otherwise known as OMB M-21-31.

It dictates what kind of logs and cybersecurity event monitoring U.S. federal government must maintain, partly to create evidence and forensic trails in case of further attacks, but also to make sure that government agencies share standards and data. The memo also creates four event-logging, or "EL," maturity-model tiers ranging from zero (the bare minimum) to three (the most comprehensive).

In the case of this agency, Luu says, Qmulos' flagship Q Compliance tool was able to quickly assess the department's compliance with M-21-31.

"We have a specific solution built into Q Compliance for M-21-31," he says. "Immediately we identified where their gaps are, where they're collecting the required data, where they're not. We have a scorecard that shows their scores against each of the enterprise logging levels defined in M-21-31, levels zero through three."

The team then worked with on-site staffers to feed the required controls data and other information into Splunk and raise the agency's compliance level.

"As they were doing that, the scorecards updated to show the new compliance levels across each of the enterprise logging levels defined in M-21-31," says Luu. "Over time, once all of that data was onboarded and all of the dashboards and scoring levels updated, they were able to reach their EL3, which is the highest level of maturity."

Hurt and Luu also agreed that company leadership should move compliance from what Luu called a paper-pushing exercise to an automated, data-driven, modern platform. Otherwise, such an institutional change isn't likely to succeed.

A culture of compliance must come from the top

Automated tools and big data can't solve the biggest obstacle to better security and compliance: organizational culture. Every expert we spoke to said that the human factor is the most important one when trying to achieve maximum compliance, even after maximum automation has been reached:

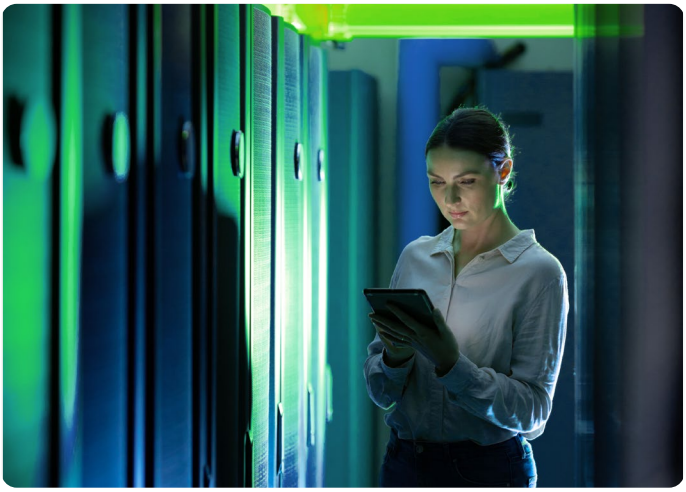
- **Changing the culture to a point where security is top of mind for every person in the organization is the goal.**
- **Compliance and cyber security must be championed at the highest levels of the organization to cultivate a cyber-first culture.**
- **People need an environment where it's okay to bring issues forward and be transparent.**

"It takes a lot of executive top-down buy-in," says Luu. "We've seen this with our customers, those that have been successful and those that haven't. It's because there are a lot of stakeholders involved, and you need that top-down executive-level buy-in to embrace this shift in how compliance is done today."

"Make sure you're engaging in regular audits and self-assessments," Hurt added. "Even getting an independent third party to review, that's key."

Top brass needs to see security as a business enabler rather than an inhibitor.

A clear way to do that, Hurt says, is to make sure the organization can maintain compliance and use a compliance platform that can help showcase where and how it's adhering, excelling, or in some cases, falling short and making room for improvement."



> ***"Look at the data and trust what the data tells you, rather than what the interview or the person interviewing has told you."***
> **Tieu Luu** | Chief Product Officer, Qmulos

The future of compliance and regulation

It seems almost inevitable that as the volume and sophistication of cyberattacks continues to increase, so will the number of regulations with which organizations must comply. That only strengthens the case for implementing a modern compliance platform as soon as possible.

"I think we will continue to see more compliance regulations come out from the government and other regulatory bodies," says Luu.

"To stay on top of that," he adds, "[you'll need] a robust platform that allows you to continuously and automatically collect that data that serves as technical evidence from which you can then apply different analytics and detections to help you identify your compliance issues and findings in real time."

Leaving aside specialized regulations governing specific industries, federal agencies or federal contractors, the U.S. has no all-encompassing laws governing data protection. That leaves it up to the states, and their patchwork of laws may lead to further confusion.

Despite potential regulatory chaos and near-certain regulatory overload, Luu says that organizations can stay ahead of rapid compliance changes if they learn to analyze the evidence accurately.

"Look at the data and trust what the data tells you, rather than what the interviewee or the person interviewing has told you," he says. "Become a strong data analyst with a platform like Splunk/Qmulos where you can look at that data and come to your own conclusions as to whether that control is operating effectively or not."

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, the Official Cyber Security Summit, TECHEXPO Top Secret, and now LaunchTech Communications.
To learn more, visit CyberRiskAlliance.com.

SPONSORED BY

Qmulos is a next-gen compliance, security and risk management automation provider, delivering the innovative power of converged, 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.
To learn more about Qmulos, visit: www.qmulos.com.

ePlus is a customer-first, services-led, and results-driven industry leader offering transformative technology solutions and services to provide the best customer outcomes. Offering a full portfolio of solutions, including artificial intelligence, security, cloud and data center, networking and collaboration, as well as managed, consultative and professional services, ePlus works closely with organizations across many industries to successfully navigate business challenges. To learn more, visit: www.eplus.com.

Splunk, a Cisco company, helps build a safer and more resilient digital world. Organizations trust Splunk to prevent security, infrastructure and application issues from becoming major incidents, absorb shocks from digital disruptions, and accelerate digital transformation. To learn more, visit: www.splunk.com.

MASTHEAD

EDITORIAL

SVP OF AUDIENCE CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com

Compliance Simplified. Risk Minimized. Security Amplified.

In today's evolving regulatory landscape, compliance is essential for resilience and security. Qmulos empowers organizations to achieve continuous compliance with ease, turning complex regulations into manageable processes. As premium Splunk applications, Q-Compliance and Q-Audit solutions help you meet standards, enhance security, and minimize risk through real-time control monitoring, and actionable insights.

Whether you're tackling NIST, CMMC, SOC2, or industry-specific frameworks, Qmulos has you covered. Our solutions provide:

- Real-Time Compliance Automation
- Audit-readiness with continuous monitoring and reporting.
- Automated Workflows
- Time savings and risk reduction by automating the entire compliance lifecycle—from assessments to documentation.
- Data-Driven Insights
- Advanced analytics to make informed decisions that strengthen your compliance and security.
- Flexibility and Scalability
- Scalability for your organization's needs, ensuring you're prepared for tomorrow's challenges.

Learn More

Read Now

Traditional, Siloed Compliance Isn't Working

Compliance that is converged with security and risk and supports an optimized cybersecurity posture is the future. Learn how your team can:

- Leverage compliance for greater cybersecurity
- Institute a compliance approach that eases the stress of new regulations
- Eliminate tedious manual data collection
- Leverage technology to provide real-time security and risk insights
- Automate reporting