COMPLIANCE MODERNIZATION

The Key to Survival in an Always-On World

Compliance that is automated, real-time, and converges the functions of compliance, risk, and security is a crucial strategy in today's sophisticated threat landscape.

Global spending on cybersecurity products and services is expected to reach $1.75 trillion cumulatively from 2021 to 2025.

Hackers leaked more than 2 billion data records containing usernames and passwords in 2021, an increase of 35% from 2020.

Real-Time Cyber Threats Demand Real-Time Compliance

Despite the fact that the world spends more on cybersecurity every year, the number of data breaches continues to rise. Moreover, the impact of cyberattacks keeps expanding, even as security vendors and providers introduce additional solutions to the market. Hackers continue to target data assets across all industries to be sold on the dark web or leveraged for extortion, recently resulting in historic numbers of records stolen.

As expected, these almost daily breach headlines are raising regulatory scrutiny: demands for transparency and accountability are coming from regulators like the SEC, FTC, and the DOD. Business leaders at the highest levels, including CEOs, are increasingly being held to account for negligence leading to cybersecurity breaches and data exposure, as well as malfeasance in cases of falsified compliance records.

Companies are now being asked to validate the state of their enterprise security program on a continuous basis, paving the way to a new era of personal accountability and even criminal liability for those in charge. The need for complete confidence in an enterprise security program has never been more acute, and business leaders are increasingly asking their security, risk, and compliance teams one simple but loaded question: Can I trust this data?

Why Businesses Are Struggling with Cybersecurity More Than Ever

According to Cisco, 500 billion devices are expected to be connected to the Internet of Things (IoT) by 2030, a huge growth in devices that connect ever more of daily life to the Web.

The fundamental misalignment and disconnection between risk, security, and compliance lies at the root of the issue. Our modern digital economy produces intricate matrices of cascading and overlapping risk surfaces and exposures whose scope and impact range from local to national to global in scale and effect. This inherent complexity presents significant challenges to private industry and national security organizations seeking to manage cybersecurity threats as they emerge - in real-time.

True cybersecurity cannot be achieved when risk, security, and compliance are considered separate domains and functions. The lack of integration between security and compliance limits enterprise risk observability, making environments easy targets of compromise - and bad actors continue to exploit these bureaucratic inefficiencies.

To overcome the security threats facing the modern enterprise, stakeholders from compliance, risk and security must converge, and leverage the power of big data analytics for a transformative, effective, and more efficient approach to defending the enterprise against today's advanced cyber threat landscape.

> **"No threat facing America has grown as fast, or in a manner as difficult to understand, as the danger from cyberattacks."**
> (The Growing Threat of Cyber Attacks)

DATA IS DATA

It is time to stop treating risk data differently based on its source and recognize the simple truth that "data is data", and that there is no separate compliance data, or risk data, or security data. The answer lies with driving true enterprise-wide risk visibility and management maturity that includes all and serves all - equally.

REGULATORY SECURITY COMPLIANCE

The cost of achieving regulatory security compliance is on average $5.47 million each year. The average cost for organizations that experience non-compliance-related problems is far higher – $14.82 million. The average cost of non-compliance has risen more than 45% in 10 years.

Reducing Compliance Latency, Risk Mitigation Timelines & Duplication of Work Effort

Many large organizations are spending jaw-dropping amounts of money on compliance and getting zero security value out of it because they treat them as siloed functions designed for distinctly different objectives. As a result, they operate on different timescales and expectations. Why is this? Because compliance audits or reports, in most cases, are moment-in-time snapshots. Regardless of how secure or compliant an organization happened to be at that point in time, the audit does not reveal anything meaningful about whether an organization is secure or compliant right now.

Adding to the lack of precision and timeliness is the way audits and assessments are typically performed:

- periodic interview-based capture and validation of control data within a (hopefully) representative sample of key enterprise systems and security apparatus, with findings extrapolated for an "average temperature" reading across the enterprise, or
- exhaustive surveys of all systems and their security controls - a process whose inherent manual overhead permits only a limited assessment cadence, in many environments only performed once every 2-3 years.

In either case, these models are highly dependent on subjective analysis as opposed to objective technical evidence.

WITH QMULOS, THE COMPLIANCE VALUE PROPOSITION BECOMES EXPONENTIALLY GREATER. ORGANIZATIONS CAN CONNECT THE DATA ONCE AND USE IT ACROSS THESE SUPPORTED FRAMEWORKS AND STRATEGIES:

- cATO
- CDM
- CMMC
- CMS ARS
- FedRAMP
- HIPAA
- ICS 500-27
- ISO/IEC 27001
- NIST CSF
- NIST 800-137A
- NIST 800-53
- OMB M-21-31
- RMF/NIST 800-37
- Sarbanes-Oxley (SOX)
- SOC-2
- StateRAMP
- ZeroTrust

Over 50% of organizations are planning on incorporating the use of AI and automation technologies in 2023.

A survey of Global 500 companies found that leaders choosing to invest in AI and automation business tools and software solutions expect to see significant growth within the next few years.

Out with the Old, In with the New

Getting compliance to perform on the same timescale as security operations has been historically challenging to even imagine, let alone implement. Compliance latency is the inherent flaw of most traditional compliance programs, and it is often coupled with a focus on just passing compliance audits without the capacity to objectively validate their accuracy. This scenario serves as the major reason behind the cliché, "compliant but not secure," as is frequently mentioned in the wake of a publicized breach.

Yet, this long-accepted status quo does not need to persist. Mature, forward-thinking organizations that wish to evolve beyond the inherent limitations of traditional, legacy compliance models, can transform their programs through the power of convergence.

Today, organizations are expected to look towards automation, AI and machine learning-based solutions in an effort to augment human capabilities. This means investing not only in individual tools and capabilities but making strategic investments into risk management, starting with:

- Risk observability,
- Timely detection of security control failures,
- Transforming legacy security, risk, and compliance processes into modernized, automated, and machine-augmented functions.

As leaders move to embrace these concepts, it's important to understand the different types of "automation," especially compliance automation, their key differences, and their respective capacity to energize and sustain enterprise compliance modernization initiatives.

QMULOS PHILOSOPHY:

“Anything that can be automated, should be.”

TECHNICAL EVIDENCE COLLECTION & REVIEW

80%

Time Savings

Reduce time and effort to chase and follow up on evidence through automated collection

COMPLIANCE AUTOMATION

80%

Decrease in Control Review Time

Leverage technical automation of pass/fail thresholds, POAM creation, control alert logging, and more

OPERATIONAL SECURITY AWARENESS

50%+

Increase

Monitor a greater number of critical controls on a daily basis instead of yearly

ONGOING ASSESSMENT

$20K+

Potential Annual Cost Savings per Framework

Use Q-Compliance to provide the evidence necessary to demonstrate ongoing assessments

Not All Compliance Automation Solutions Are Created Equally

A simple search for “compliance automation” will yield a plethora of solutions claiming the title. However, compliance leaders need to be aware of the critical difference between “compliance workflow automation” and “end-to-end, full compliance lifecycle automation.” While the current marketplace offers many solutions that automate the human workflow elements of compliance, Qmulos has taken a different path by designing a fully automated compliance platform that is built around a simple philosophy: “anything that can be automated, should be.”

Starting with technical evidence collection, through data validation, control state analysis, creation of POA&Ms and SSPs, reporting, dashboard, audit and assessment support, Qmulos automates every phase of the compliance workflow and maps data to specific controls as outlined in the latest industry, state and federal standards.

It's Time for Security-Compliance Convergence

Enterprise cybersecurity teams need the ability, and visibility, to make consistent decisions about deploying their team's limited resources in defense of enterprise assets, infrastructure, and operations. A converged continuous compliance management approach empowers real-time control observability and up-to-the-minute risk visibility that enables well-informed risk management decisions.

With cybersecurity and privacy compliance frameworks, standards, and regulatory mandates providing consistent guidelines for the selection, implementation, and continuous validation of security controls, leading compliance management teams are choosing to rely on objective factual data about the state of their technical security controls – as opposed to mere opinions collected through periodic surveys.

FEDERAL CIVILIAN CUSTOMER

Use Case: Q-Compliance for Continuous Monitoring and FISMA Metrics

Problem

Customer assessment process and cybersecurity operation mostly performed manually. Process was laborious and time-consuming, with customer assessors gathering and uploading technical evidence to their GRC tool during assessments periods. There was no immediate visibility to their vulnerability and cybersecurity risks.

Solution

By leveraging Q-Compliance visualizations via cybersecurity data on the Splunk platform, customer gained broad visibility to their compliance posture – from access control, configuration management, to vulnerability. Customer Splunk administrators, along with our Qmulos deployment engineer and solutions architect, worked with ISSOs and ISSMs to refine control dashboards, as well as develop custom dashboards, for everyday continuous monitoring.

Results

Customer is leveraging their continuous monitoring program for real-time visibility into their cybersecurity posture. The team is also developing executive-level reporting in Q-Compliance for their FISMA metrics to reduce the amount of time spent on technical evidence gathering and reporting.

FEDERAL CIVILIAN CUSTOMER

Use Case: Q-Compliance for Assessments

Problem

Customer assessment team was spending too much time conducting data calls with system owners, gathering evidence, and uploading them to their GRC tool; instead of addressing vulnerability and reducing gaps in their environment.

Solution

Customer and Qmulos teams kicked off a technical and compliance discovery process to identify the biggest pain points and needs with their ISCM, ISSO, ISSM, and GRC teams. Starting with their critical volatile controls, the Qmulos deployment engineering and customer success teams captured technical data requirements for controls, as well as additional visuals needed to meet control language. Starting with the out-of-the box visuals for controls, the ISCM team reviewed and requested refinements to pass/fail controls.

Results

Q-Compliance now allows customer's assessors to decrease the amount of time spent on data calls by using real-time technical evidence to pass/fail controls for regular assessments.

SMART CISOS AND MATURE ORGANIZATIONS UNDERSTAND THAT THERE IS NO SPENDING THEIR WAY OUT OF SECURITY ISSUES OR INTO A BETTER RISK POSTURE. AN AVERAGE ENTERPRISE ALREADY FIELDS 70+ SECURITY SOLUTIONS AND THEY NEITHER NEED NOR CAN AFFORD ANY MORE.

DEFENSE CUSTOMER

Use Case: Q-Audit to Meet ICS 500-27 Requirements

Qmulos has been working with a USAF customer since 2016 to help them meet ICS 500-27 requirements.

Problem

Customer team did not have a streamlined, real-time, user-friendly method for audit needs and to meet the ICS 500-27 requirement.

Solution

Qmulos team installed and stood up Q-Audit for customer's three environments, which provided visibility into all audit event families for their environments, including applications, authentications, data movement and privileged access.

Results

Q-Audit allows the customer team to effectively and efficiently meet their ICS 500-27 requirements.

How CISOs Are Navigating the Always-On World

As more and more regulations are put in place requiring companies to meet certain cybersecurity and compliance standards, the demand for dynamic, evidence-based security management capabilities to help companies report on and meet these requirements will continue to grow.

The old approach of buying 'best-of-breed' technology is reactive and costly. Most organizations tend to take a bottom-up, technology-driven approach, matching attack categories with technology capabilities, then filling the gaps with more technology while overlooking their compliance programs as a valuable source of insight about either risk or control posture.

Today more CISOs are opting to proactively manage risk with better visibility into security performance metrics through platforms like Q-Compliance.

AN AVERAGE ANNUAL EXPENSE OF $3.5 MILLION IS INCURRED BY ORGANIZATIONS TO MEET REGULATORY SECURITY COMPLIANCE, ACCORDING TO A STUDY BY PONEMON INSTITUTE AND TRIPWIRE. **NON-COMPLIANT ORGANIZATIONS FACE COSTS NEARLY 3 TIMES AS HIGH, AVERAGING AT $9.4 MILLION**, DUE TO ISSUES LIKE BUSINESS DISRUPTION AND LEGAL SETTLEMENTS.

– I.S. PARTNERS LLC

COMMERCIAL CUSTOMER

Use Case: Q-Compliance and Q-Audit to Achieve Continous Control and Monitoring and Combat Insider Threats

Challenge

The Customer lacked a cohesive compliance solution. Its assessments were paper-based and manually-driven, requiring time-consuming data calls and evidence collection. Each ISSO manages 15 systems, creating backlogs around assessments and audits. The lack of automation and continuous monitoring was degrading its security posture and making it difficult to meet ConMon security controls and NIST 800-53 requirements.

Solution

With a vision and desire to be technologically innovative and progressive, the Customer and Qmulos kicked off a collaborative partnership to identify the strategic needs across sales, delivery, and development, and better understand the Customer's biggest pain points. The Qmulos deployment, engineering and customer success teams moved quickly to roll out Q-Compliance and Q-Audit to implement continuous control monitoring and insider threat hub.

Results

Q-Audit replaced a homegrown application with a more robust threat alert system. Q-Compliance helped decrease the amount of time spent on data calls by using real-time technical evidence and accelerated assessment and audit readiness.

CISOs should be able to:

- Consider technology choices through the lens of risk controls, enabling credible and transparent technology portfolio management decisions that are immune to vendor preferences or the latest market(ing) fads.
- Understand the original intent of security and regulatory compliance as a model for proactive and consistent risk management (leading indicator), not just a historical reporting and audit function (lagging indicator).
- Recognize that managing risk, compliance, and security as distinct and separate functions is not only wasteful and inefficient, but denies the enterprise the ability to cross-leverage significant people, process, and technology investments for the ultimate purpose of managing risk.
- Streamline the detect-understand-mitigate sequence (i.e. the OODA loop) and inform decision-makers with the most accurate and timely facts about their environment.
- Know the difference between objective data and subjective opinion when it comes to how risk information is sourced, analyzed, and delivered to the decision-makers, and then know how to categorize both technical and organizational capabilities accordingly.

Next-Generation Compliance to the Rescue

An integrated approach to cybersecurity and risk transformation – what Qmulos refers to as converged continuous compliance –businesses can discover untapped potential in their investments in compliance and security. This always-on approach guarantees that well-designed, efficient, and continuously validated security controls are in place to counteract today's always present cyber threats. Additionally, the efficiencies brought forth by automation allow for the reallocation of crucial talent resources from manual data management tasks to effective risk management choices.

Each enterprise must find its own path to convergence, and hopefully that happens before their next breach.

For more information on transforming a cybersecurity strategy to one that is truly business aligned and security-optimized to respond to the rapidly changing compliance and global threat landscape, please reach out to Qmulos.

BUSINESSES CANNOT OUTSPEND, THEY HAVE TO OUTMANEUVER.

More than two-thirds of global enterprises indicated their plan to increase their security spend in 2022, keeping with the historic annual growth rate of 10 percent. However, global cybersecurity losses have gone up by more than 160 percent, highlighting the sobering reality of the serious economic incentives behind cybercrime.

About Qmulos

Qmulos is a pioneering next-gen compliance, security and risk management automation provider, delivering the innovative power of converged, continuous compliance through its flagship Q-Compliance 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. Government and industry leaders in the public and private sectors use Qmulos' solutions to ensure the highest levels of cybersecurity.

qmulos.com

qmulos