qmulos®

CORPORATE BROCHURE

Security. Compliance. Convergence.

ACHIEVING TRUE COMPLIANCE AUTOMATION

The State of Enterprise Compliance

Compliance has become an ongoing and costly challenge – with no end in sight. Regardless of all the effort, time, and resources dedicated to managing compliance, most large enterprises still consider compliance nothing more than a cost of doing business that does little to deliver any tangible security improvement or risk reduction.

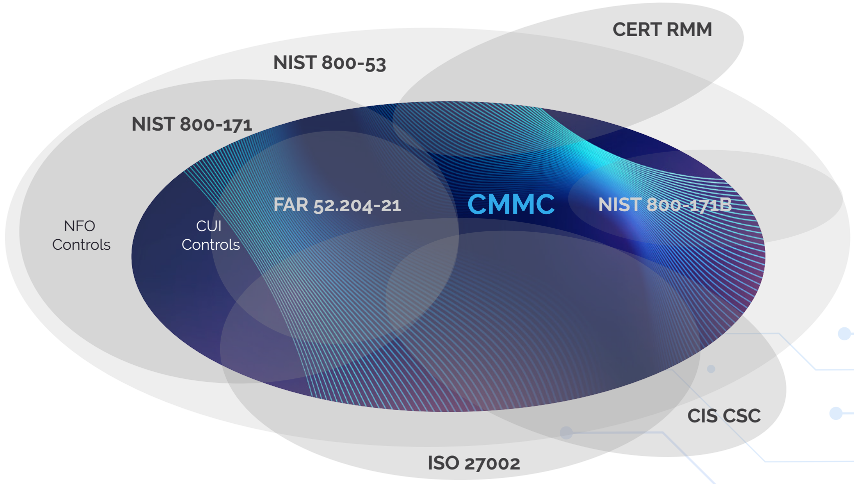
Cybersecurity threats are increasingly sophisticated and frequent, and damages from these attacks keep escalating. In response, enterprises often embrace point solutions, seeking the next shiny silver bullet to address the latest emerging threat category. Yet, despite all the technology investments, breach statistics keep climbing. Most organizations fail to recognize that technology has shifted the focus from risk management towards management of their complex security technology portfolios. Simply put, there is no buying your way to better security, not without addressing the real strategic deficit: the ongoing, legacy misalignment of risk, security, and compliance operations.

When treated as siloed functions in today's interconnected and interdependent digital economy, conventional approaches create complex matrices of cascading and overlapping risk exposures. In the absence of risk-first, business-aligned strategies to drive cross-functional synergy, most security and compliance technologies fail to achieve the true goals of cybersecurity, risk, and compliance: a resilient, agile, and trusted enterprise. As a result, cyber technology portfolios keep growing in cost and complexity, while legacy compliance models fail to deliver the risk visibility and real-time detection of control failures necessary to proactively manage cybersecurity risk.

Achieving, maintaining, and proving adherence to continuously changing standards, frameworks, and mandates requires real-time control visibility. For CISOs and their teams, demonstrating compliance for regulations like CMMC and FedRAMP is difficult within their sophisticated enterprise technology environments. (See figure below).

WITH QMULOS, COLLECT TECHNICAL EVIDENCE ONCE AND LEVERAGE IT ACROSS MULTIPLE FRAMEWORKS

CMMC EXAMPLE



CISO CHALLENGES

CISOs are often challenged by the tedious and time-consuming need to collect and analyze the same technical evidence 15-20, up to 30 times a year to meet different framework requirements. This is further exacerbated by their team's compliance fatigue and talent shortage.

Most modern compliance frameworks share common control requirements, which means becoming compliant with one standard carries benefits across other compliance obligations. However, the task of mapping data to evidence requirements, evidence to controls, and controls to various frameworks can be quite complex, especially when all you have to rely on is manual analysis. Investing in end-to-end compliance automation enables enterprises to streamline these tedious compliance tasks, freeing up analysts to focus on the actual objective: managing enterprise risk.

How Can Qmulos Help?

Qmulos makes evidence-based risk management decisions possible by providing real-time insights on overall enterprise risk posture. With more than a decade serving some of the top U.S. government agencies, defense, national security, and intelligence community clients, Qmulos helps to ensure agencies and their partners adhere to critical security compliance regulations, including FedRAMP, NIST and CMMC, among others.

Qmulos also supports IT risk management, making compliance an integral part of an enterprise's security readiness.

In the private sector, enterprises rely on Qmulos to drive timely and accurate risk visibility while reducing time-to-compliance lag and increasing their competitive advantage through accelerated third-party risk accreditation for regulations and strategies, such as SOX, HIPAA, NIST RMF, and Zero Trust.

Traditional compliance is reactive and only deals with historical data to show what happened days, weeks, or months ago. In today's new era of real-time compliance automation, Qmulos delivers the innovative power of Converged Continuous Compliance™ through its flagship Q-Compliance platform. This technology enables organizations to connect their data once and leverage it across all major frameworks and standards–dramatically accelerating the time it takes to achieve evidence-based compliance with confidence. Q-Audit, our insider threat management platform, provides real-time analytics based on the Intelligence Community Standards ICS 500-27.

Qmulos helps ensure demonstrable compliance with these critical regulations and more:

- 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

The Power of Automation

Organizations trying to meet a NIST moderate baseline have to account for 239 controls, 143 of which are technical controls. Manual compliance puts a burden on the IT and compliance teams tasked with meeting these standards. Q-Compliance dramatically streamlines and simplifies resource-intensive processes to save time, save money, and enable real-time awareness of security vulnerabilities.

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

Q-Compliance

WHAT IT IS

Q-Compliance is a wholly new paradigm for risk visibility that accelerates and simplifies ongoing compliance management. Built on a high-performance, big data platform, Q-Compliance continuously monitors and collects data in real time from networks, systems, tools, and devices both on premise and in the cloud. Result: Security operations teams gain a comprehensive and dynamic view of their cybersecurity posture at all times – and in hybrid environments.

HOW IT WORKS

Q-Compliance analyzes data from any source to identify compliance gaps, flagging potential security weaknesses to keep organizations fully protected. Real-time data ingestion and assessment helps organizations achieve accurate, traceable, and up-to-the-minute compliance, protecting against revenue loss or non-compliance delays.

KEY FEATURES

Whether they are running hybrid cloud environments or maintaining critical business applications on premises, enterprises can achieve compliance requirements and still innovate – no matter what framework or compliance standard needs to be adhered to.

Customers can take advantage of:

- Complete control sets and multiple frameworks
- Multi-level organizational hierarchies
- Multi-tenant organization based access control
- System boundaries and control inheritance
- Built-in control baselines
- Custom controls and control overlays
- Hundreds of pre-built control analytics
- Support for all types of evidence
- Enterprise compliance scanning for Windows and MacOS
- Automated control assessments
- Dashboards and workflows to manage operational compliance activities
- File-based evidence upload and POAM management and maintenance

> *"We made more progress than other agencies on the OMB mandate. We were able to raise the compliance scores and get the major platforms to 100% compliance. It was a huge effort."*
>
> **– IT Specialist, OMB M-21-31 Lead**

IMPACT ON RISK MANAGEMENT

Q-Compliance provides real-time decision-making based on machine learning and big data analytics from across the enterprise. Continuous monitoring of security controls highlights gaps and enables rapid remediation.

KEY BENEFITS

Q-Compliance is reinventing how the largest enterprises handle compliance. Dynamic and evolving organizations with security and risk postures changing on an hourly basis can be confident that they have full visibility into their compliance status across their control ecosystem, empowering proactive, evidence-based risk management decisions.

Q-Compliance also provides multi-compliance framework support for common enterprise compliance frameworks using over 700 out-of-the-box visualizations and analytics. Automated technical evidence collection makes it easy to support existing and new compliance requirements and custom frameworks.

Forward-looking organizations work with Qmulos to:

- Demonstrate their proactive stance on security and risk maturity
- Alleviate internal teams from a massive amount of manual tasks, enabling resources to focus their energy on high-value work and actual risk management
- Reduce risk exposure timelines by continuously identifying control failures and streamlining prioritized control remediation at scale
- Empower compliance confidence in meeting industry, state and federal requirements and frameworks
- Automate data collection, eliminating all manual tasks wherever possible
- Future-proof against all major framework updates
- Deliver short-term and long-term ROI with Converged Continuous Compliance™
- Streamline enterprise audits for mission-critical and insider threat initiatives
- Drive confidence in compliance reporting in light of increasing regulatory scrutiny over reporting accuracy and personal accountability for agency lenders and authorizing officials

TRUE COMPLIANCE AUTOMATION

Q-Compliance is the ONLY automated compliance tool for technical evidence data collection from any data source. Q-Compliance automates control assessments, system authorizations, and system security plan reports, eliminating the need for continuous data calls for technical evidence collection across frameworks.

QMULOS DELIVERS CONVERGED CONTINUOUS COMPLIANCE™

Converged Continuous Compliance™ automates and simplifies continuous controls monitoring and real-time risk visibility across enterprise systems, encompassing current and emerging cybersecurity compliance requirements.

Customers save time, effort, and money by ensuring that today's cyber threats are met with highly effective, and continuously validated security controls. In addition, Qmulos-driven efficiencies enable critical talent resources to realign from manual data management activities to true risk management decisions.

DEMONSTRATING COMPLIANCE IS A CHALLENGE

Demonstrating compliance has long been a problem. Continually getting more complex, many customers tell us they are collecting the same evidence dozens of times a year based on different frameworks. The permanent drain of time, money, and resources needed to maintain compliance has become untenable.

- Cybersecurity practices among vendors are becoming an expectation, as 44% of firms say they are being asked for proof of cybersecurity as part of a request for proposal (RFP). (**ACA Key Trends and Forces Shaping Risk and Compliance Management in 2021**)
- Stagnant budgets and a shifting workforce have left many compliance teams feeling stretched, with 87% of organizations reporting they have no additional capacity due to being understaffed or only adequately staffed. (**Deloitte State of Compliance 2020 Report**)

Q-Compliance Solves the Hard Part of Compliance

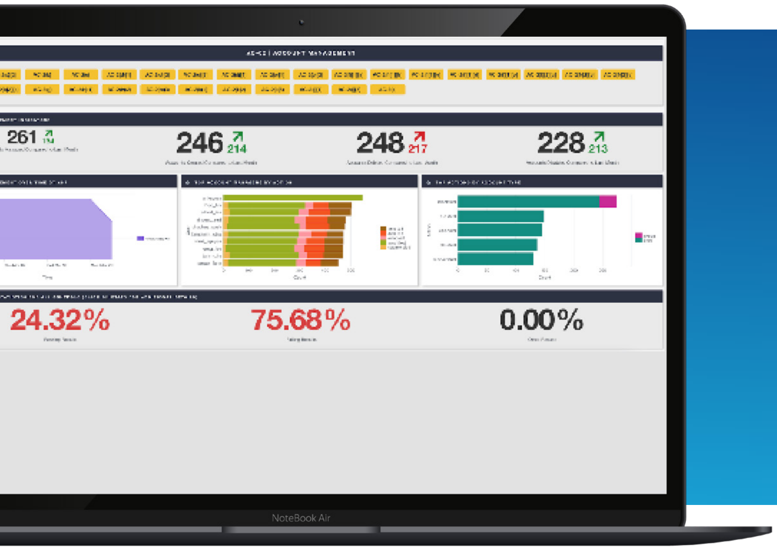
By continuously monitoring the effectiveness of all technical controls from any framework, in any environment, in one location, and in real time, organizations benefit from significant time savings and a drastically improved security posture.

If You Want To...	Use Legacy GRC Vendor	Use a Niche Cloud Vendor	Use a Big Data Platform	qmulos	Qmulos Benefits
Manually collect and upload control evidence to include documents and snapshots of technical evidence.	Yes	Yes	No	Yes	**Avoid:** high labor costs, minimally-passed audits, team burnout, lack of real-time data access, and immediately out-of-date compliance with no real security value.
Automatically collect technical evidence accross controls to ensure they remain in place over time and at any point in time. *[Leverage data from any technology that implements a compliance or security control.]*	No	**Limited** Technical evidence collection is typically restricted to a specific cloud provider.	**Partial** Able to collect from various data sources, but with no built-in way to map that data to various controls and frameworks.	**Yes** Collect technical evidence from virtually any data source (any device, operating systems, scanners, directories, DNS, routers, etc.).	Significant time savings for compliance and security ops personnel, freeing up time to focus on valuable security and risk management activities.
Continously monitor the effectiveness of controls from any environment in one location in near real-time.	No	**Limited** Typically specific to a particular cloud provider. Does not typically include on-prem systems and devices.	**No** No out-of-the-box solution to map evidence to controls and manage compliance requirements like passing/failing.	**Yes** Monitor technical evidence for controls associated with assets in any environment (cloud and on-prem).	Drastically improved security posture and protection of critical data, systems, and networks.
Manage and report on the establishment and effectiveness of management, operational, and all technical controls from virtually any compliance framework and/or custom "customer defined" control library.	**Limited** Yes for non-technical controls No for technical and custom controls that are technical	**Limited** Typically focused on specific frameworks and does not include ability to dynamically create and monitor evidence for custom controls.	**No** Would require custom built applications to capture the concept of control.	**Yes** Includes numerous control frameworks and allows for custom controls to be defined and data/evidence mapped to those controls in the UI.	Significant time savings for reporting, minimizing or eliminating manual reporting and ability to provide auditors with near real-time reporting.

Q-Compliance Transforms Risk Management into a Real-Time, Proactive Function with Up-to-the-Minute Dashboard Views

ACCOUNT MANAGEMENT

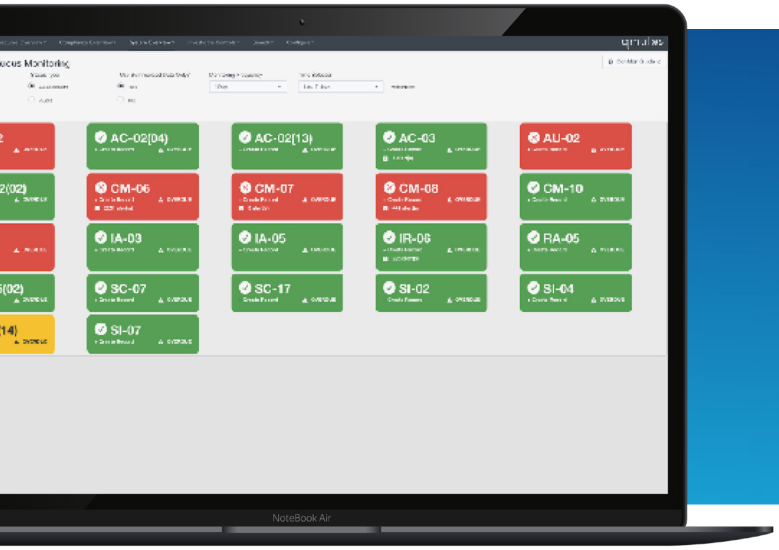
Users can click on a specific control to see the technical evidence for it, down to a single data point.



Context and timeliness matter, and data tells the truth. Q-Compliance visualizations offer full-scope interactive access to accurate real-time control posture data, informed by continuously collected technical evidence across your entire enterprise, takes the guesswork out of compliance, security, and risk management. Easily navigate your compliance landscape and drill down into each control family, its technical evidence, or each individual datapoint informing the currently reported compliance state.

CONTINUOUS MONITORING DASHBOARD

These easy-to-read visualizations show which controls are currently passing or failing, what alerts have been triggered, and when they were last reviewed.

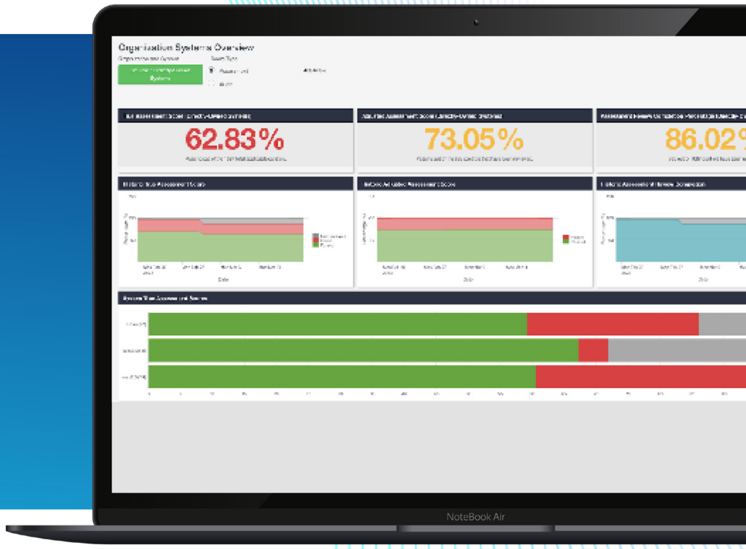


Q-Compliance data-centric automation turns tedious compliance management tasks into easy-to-use interactive visualizations, powering real-time insights into control pass/fail status, automated alerts, and control review records. Instead of chasing control data, analysts can enjoy a simple graphical interface that answers their compliance questions at once.

ORGANIZATION OVERVIEW

Executive level overview of the directly owned systems gives real time assessment scoring to top level management.

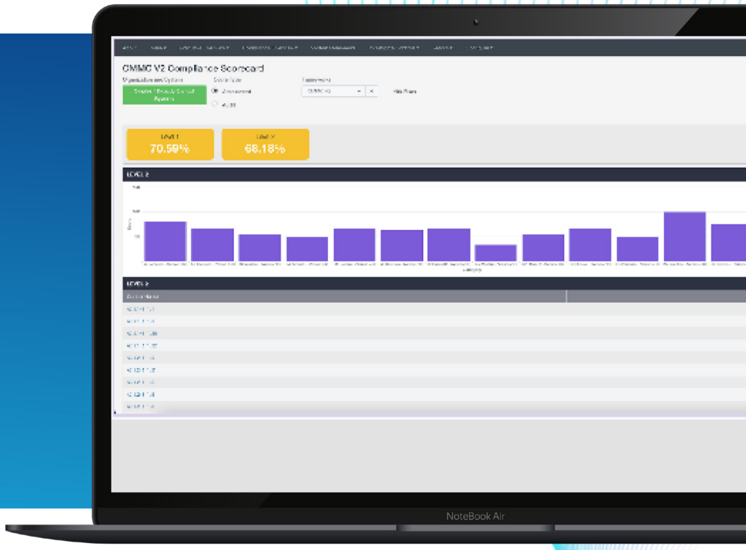
Say goodbye to slide decks and manual reports! Qmulos delivers robust built-in capabilities that transform your executive reporting from a static historical function into an interactive strategic risk management exercise. Instead of reporting on past compliance issues, Qmulos empowers you to assess your compliance posture across the enterprise in real-time, enabling leadership to prioritize most critical remediation activities as dictated by business needs.



COMPLIANCE FRAMEWORK SCORECARD

Enterprises can see their compliance score at a moment's notice: this is an example framework scorecard for CMMC v2.0.

The question you dread to hear but would love to be able to answer: How compliant are we? Leveraging the power of continuously collected technical evidence, you'll be able to answer this question with complete confidence, and best of all, in real-time! As compliance requirements evolve, so must your compliance posture. You and your leadership need to know where the enterprise stands on a continuous basis, not where it stood three months ago - or three years. Qmulos Compliance Framework Scoring makes it possible.



Q-Audit

WHAT IT IS

Built on Splunk's scalable-to-everything platform, Q-Audit provides customers with comprehensive visibility into their network and improves enterprise security – while keeping auditors satisfied. Q-Audit uses the intelligence community's current gold standard for mitigating enterprise insider threats (ICS) 500-27, as well as NIST, DoD, NISPOM, and commercial audit best practices to ensure that an organization is fulfilling the actual purpose of audit control.

HOW IT WORKS

Q-Audit integrates with and pulls data from any cybersecurity tool, app, device, or platform and can be deployed on premise or in the cloud to monitor the events required for auditing. Using real-time data, Q-Audit drives the analytics and alerts built specifically for event families and events defined in ICS 500-27. Additionally, the data populates easy to understand visuals with at-a-glance trends and granular drill-downs to monitor and alert on auditable events and audit sources. Q-Audit 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.

> *"It's great that you can take all our feedback for the Insider Threat Hub and produce something digestible for the team. I can take this to my leadership team, to my Insider Threat Hub team, and start digging into what the anomalies are, and immediately take it from monitoring to investigating."*
>
> **- Director of SRM**

KEY FEATURES

Q-Audit leverages machine data, insider threat analytics, and dynamic alerting to provide immediate feedback on anomalies. Security, risk, and compliance managers can use the visualization to drive risk decisions and risk reduction actions on a near real-time basis.

Many organizations use Splunk to just store audit logs. Q-Audit takes things to a whole different level by showing what you should log, monitoring logs and sending alerts in real time. Q-Audit also enables actual monitoring of users and both Windows and MacOS device activity, ensuring that your organization is fulfilling the actual purpose of audit controls.

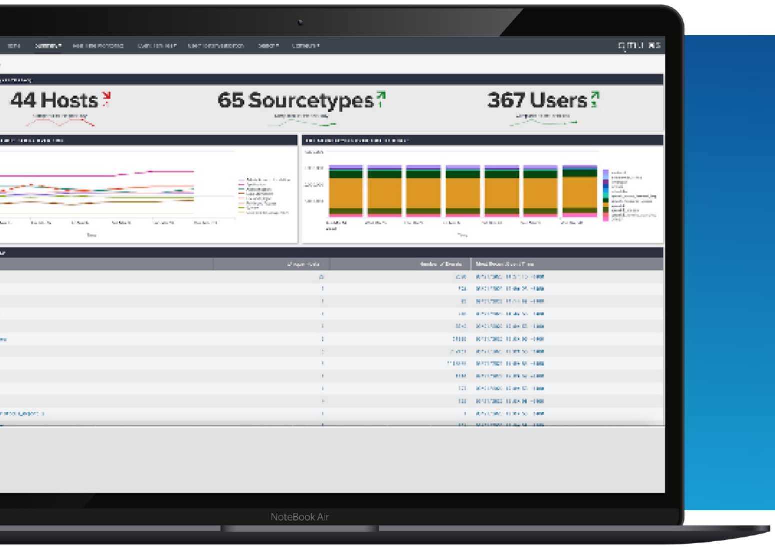
KEY BENEFITS

- Provides out-of-the-box compliance for ICS 500-27, NIST, and FedRAMP audit controls
- Reduces manual efforts and costs
- Identifies potential insider threats
- Alerts on suspicious events
- Monitors analytics in real-time
- Investigates malicious activity
- Delivers quick time-to-value
- Satisfies the auditors

Q-Audit Data Populates Easy to Understand Visuals

DATA SUMMARY

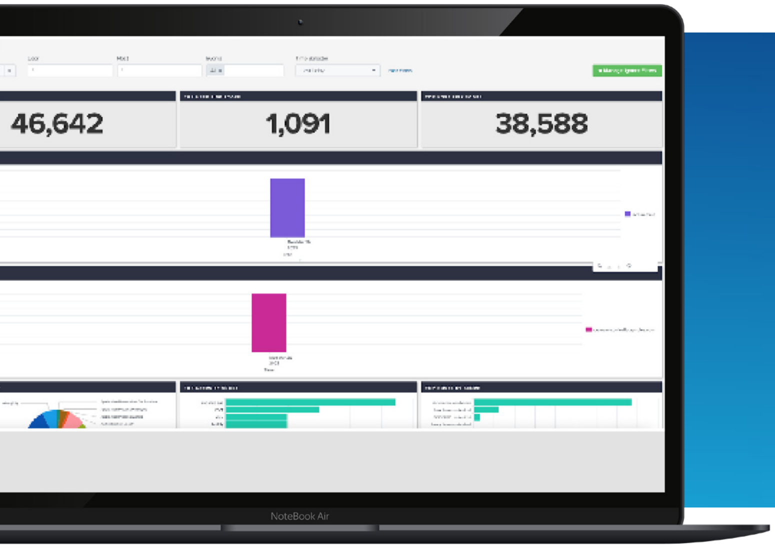
View your whole network to make sure it's auditing what it should be auditing.



Insider threat management depends on adequate coverage and real-time data. Never wonder if your monitoring data is accurate or timely - simply check the Data Summary visualizations to verify your automated data collection processes and identify any issues requiring attention. No more debugging logs to find a missing data link!

RISK SCORING

Quickly identify your riskiest user, the riskiest host, and the events causing these scores.

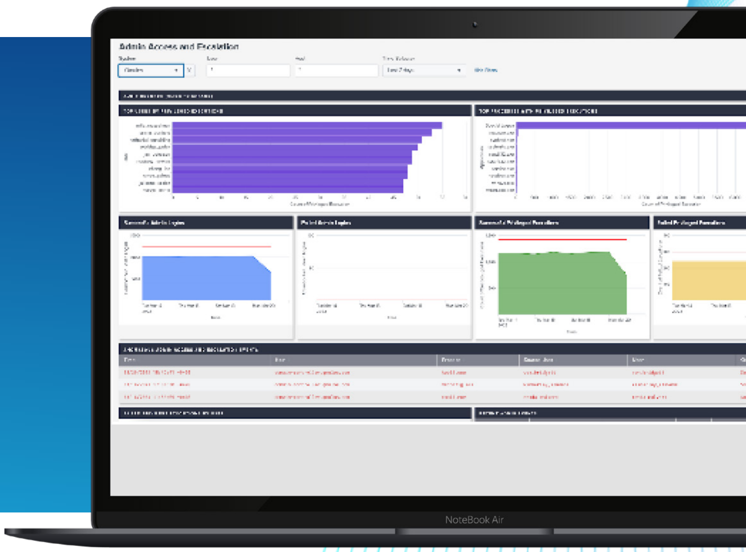


Data is important, but what you're after is intelligence, actionable insights, indications of potential activity of interest that warrants additional investigation. Qmulos turns raw data from across your enterprise into insider threat management alerts and reports, delivered via easy-to-read interactive visualizations with full contextual drill-down capabilities and built-in investigative workflows.

EVENT FAMILY

View an event family (in this case Admin Access and Escalation) including historic trends, anomalous events, and context-sensitive menus for additional investigation.

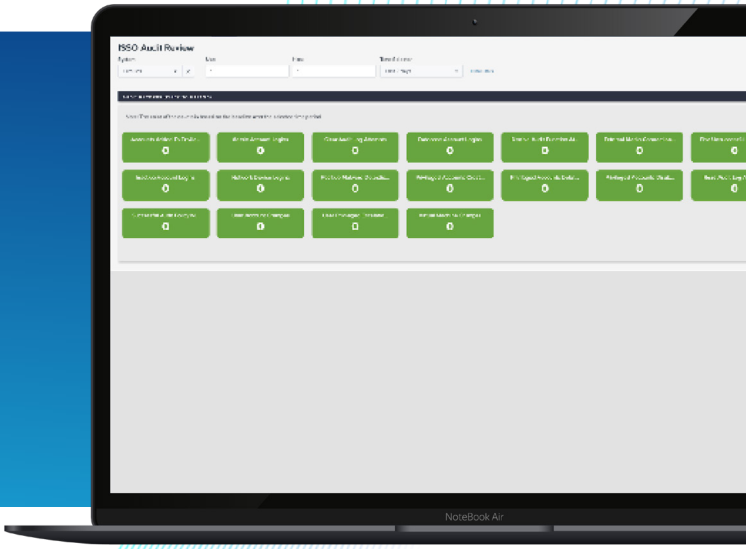
Once an alert has been validated, you need to investigate the incident quickly to determine the extent of the issue and any necessary response actions. Qmulos designed our Q-Audit platform with the analyst in mind, providing interactive access to all source events, historic trends, anomalies, and context-sensitive drilldowns to help drive the incident to rapid resolution.



ISSO REVIEW

Provides a collection of visuals for ISSOs to quickly review their auditing situations.

ISSOs can easily identify audit events of interest without having to parse through logs, executive complex queries, or run reports on exported data dumps using third-party tools. Qmulos delivers all audit alerts based on a set of defined criteria directly to ISSOs, in real-time, through a simple ISOO Audit Review visualization.



Services and Support

Qmulos supports risk management teams from kick-off to deployment, through to full adoption. We tailor our services to meet your organization's specific needs:

WHAT WE OFFER

- Requirements interviews/workshop: understand pain points and gather requirements across key stakeholder teams
- Customer success plan: develop organization wide definition of success for the project in relation to your strategic goals
- Implementation roadmap: collaborate with your team to develop roadmap to deploy and roll out product based on team needs
- Product adoption processes: develop and implement business and IA processes to encourage feedback and improvement

WHAT IT MEANS FOR YOU

- Stakeholder buy-in: key teams are invested in your project success
- Stakeholder engagement: key stakeholders are aligned on project goals and requirements
- Customization: product (e.g., dashboards, controls) and services (e.g., deployment and training) are tailored to your needs
- Successful adoption: relevant stakeholders regularly and effectively use Qmulos to streamline daily activities

Q-Compliance End User Training

Make effective use of Q-Compliance and all of its features and functionality. The hands-on workshop consists of presentations and labs to be completed in an AWS environment. The class goes in-depth on:

- Building out baselines and assets
- Defining organizations and systems
- Configuring controls
- Creating executive dashboards
- Collecting and alerting on evidence and daily system priorities

Q-Compliance Deployment Training

This workshop is a walkthrough of how to deploy, install, and configure the application. Attendees will master the creation of custom controls and visualizations, configuring, ingestion, and mapping data to any framework needed.

Q-Audit End User Training

This training introduces the ICS 500-27 standard, the foundation for the Q-Audit software solution. The course walks through all the features and functionality of the visualizations in Q-Audit, and explains how they support the auditing requirements of the standard. The course ends with multiple hands-on lab exercises that demonstrate how users can use the audit and investigative capabilities of Q-Audit to respond to different security scenarios in an organization.

Q-Audit Deployment Training

Deployment training prepares students for installing and configuring the Q-Audit application in their organization. It explains the required data sources and corresponding data models to populate Q-Audit; how to configure and onboard the two primary data sources - Linux and Windows audit logs; how to install Q-Audit and supporting technical add- ons in Splunk; how to configure Q-Audit and verify that the installation is correct. Students are provisioned with their own virtual machines, work through all the exercises, and finish the course with a fully functional instance of Q-Audit.

Get Started Today

Contact Qmulos at sales@Qmulos.com to get started on your path to next-gen cybersecurity compliance.

INTERESTED IN A Q-COMPLIANCE DEMO?

Email sales@qmulos.com and a Qmulos cyber compliance and risk management automation expert will be in touch.

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