Q:CYBER Tech Spec

Security Options, Reimagined

Introduction

Q:CYBER, QOMPLX's cloud-based cybersecurity software solutions, offers today's leading firms the most comprehensive enterprise security monitoring, protection, and data management possible. It's the only suite of integrated applications that offers an open, data streaming, and cloud-agnostic analytics platform for security.

Q:CYBER delivers all the capabilities of a truly modern cloud-native SIEM, from complete enterprise visibility and context to the range of analytics required to quickly protect networks and systems from attacks and other exposures.

Designed to be easy to use, and make onboarding data faster than ever before, Q:CYBER also eliminates most of the inefficiencies that impact cybersecurity teams today. Q:CYBER's advantages include:

- Minimalistic style, designed by security experts, to increase efficiency by providing security analysts with exactly what they need when they need it
- Unique, unified data model allows security analysts to add new data sources in minutes, instead of waiting days or weeks for data engineering resources to write parsers and orchestrate data
- Automated processes and features enable security operations center (SOC) analysts to complete tasks typically performed by more senior resources
- Deterministic and heuristic analytics proactively detect more threats and exposures faster while significantly reducing false positives, false negatives and alert fatigue
- Streamlined incident response workflows let analysts manage incidents from start-to-finish from a single screen, instead of constantly clicking between different windows and applications
- Flexible and advanced query and analytics options significantly reduce investigation times and yield better results

Our Approach

When effectiveness, efficiency, eliminating risk matter, top companies choose Q:CYBER.

On their own, each application in the Q:CYBER suite significantly enhances specific areas of your security operations. As an integrated solution, Q:CYBER provides the most comprehensive enterprise security information and attack detection capabilities available. With Q:CYBER, your security teams can much more effectively respond to current and future security challenges.

The Q:CYBER suite of cloud-based cybersecurity software solutions includes the following applications:

Privilege Assurance

QOMPLX's Privilege Assurance helps your organization:

- Identify weaknesses in your Active Directory environment
- Spotlight accounts that pose a risk to your organization
- Find machines running outdated operating systems
- Identify concentrated pockets of privileges that malicious actors will try to exploit

Identity Assurance

Using QOMPLX Identity Assurance, IT administrators and security teams can:

- Identify and map all Active Directory domain controllers
- Identify one-way and two-way Active Directory trust relationships in their organization and with outside parties
- Instrument all Active Directory domain controllers to verify that every authentication transaction is correctly implementing the Kerberos protocol
- Identify the most critical Active Directory attack techniques, including our deterministic Silver Ticket attack detection, Golden Ticket attack detection

Q:SCAN

QOMPLX's QSCAN helps your organization:

- Understand the “ground truth” of your enterprise risk posture
- Identify risk exposures such as data breaches, malware outbreaks or misconfigured/vulnerable IT assets
- Enumerate external assets using open source intelligence and device footprinting techniques
- Correlate open source and proprietary data with internal scan data to measure operational risk exposure

Security Monitoring

QOMPLX's Security Monitoring helps your organization:

- Rapidly identify and contain attacks as they happen, by ingesting, parsing, normalizing, and monitoring logs from security tools and other sources
- Allowing the creation of custom own rules, detections and analytics
- Supporting ad hoc analysis and threat hunting via scratchpad analytics
- Integrating logs from cloud services and tools

D&B Cyber Risk Rating powered by QOMPLX

With the D&B Cyber Risk Rating powered by QOMPLX, security professionals can:

- Assess operational risk, not operational intelligence,
- Focus on actionable operational risks instead of being buried in a sea of data.

Q:ASSESS

QOMPLX's Q:ASSESS family of next-generation products allows security teams to:

- Determine both the maturity and posture of their cybersecurity program,
- Estimate the effort, time and money needed to move their cybersecurity program up to the next level of maturity,
- Identify the tradeoffs between program investments and risk reduction, and
- Calculate their organization's return on security investment.

Our Methodology

Q:CYBER delivers richer visibility into your data and enables more intuitive and efficient querying and analysis. In near real time, you can add, parse, enrich, cleanse and transform data from large volumes, wide varieties and increasing velocities of data.

Adding new data sources has traditionally been a lengthy process that took days or weeks and required the use of data engineering resources. Q:CYBER helps customers' overcome these obstacles by creating a unified data model and enabling security teams to add data sources in minutes and make them available for immediate analysis.

Q:CYBER uses a unique data acquisition pipeline to automate tedious manual processes and ensure you can add data from on-premise and cloud-based applications and devices. It also makes data management cost effective and flexible. You can retain data within Q:CYBER databases for a specified period, and then, over time, archive in hot or cold storage either on-premise or in the cloud.

Q:CYBER's Features Include:

- **Advanced Monitoring for Unprecedented Visibility and Context**
  Q:CYBER allows you to view graphs and visualizations about most aspects of your network, devices, applications, users and sensitive data.
- **Advanced Protection for Immediate Detection and Response**
  Q:CYBER provides a range of easy-to-use threat detection, advanced analytics and incident response capabilities to make your security team more efficient and deliver better outcomes.
- **Powerful Data Orchestration and Management**
  A cornerstone of Q:CYBER's design is the ability for security teams to quickly and easily add, query and analyze data streams from many sources.

Ready to learn more about *Q:CYBER*? Contact us today.

+1 (703) 995-4199 | info@QOMPLX.com | www.QOMPLX.com

Why QOMPLX®

QOMPLX makes it faster and easier for organizations to integrate all of the disparate data sources across the enterprise into a unified analytics infrastructure to make better decisions. This broader analytics infrastructure is provided through QOMPLX:OS, an enterprise operating system that powers QOMPLX's decision platforms in cybersecurity, insurance underwriting, and quantitative finance. Headquartered in Tysons, VA, QOMPLX, Inc. also has offices in New York and London. More information about QOMPLX can be found at https://www.qomplx.com/.