

## Q:MDR Data Sheet

Protect yourself from cyber attacks with QOMPLX's Managed Detection and Response (Q:MDR) service

---

Small and medium-sized enterprises (SMEs) face difficult and diverse challenges. Business owners must grow their businesses without the luxury of an experienced cyber security staff. Q:MDR, CYBER's managed security solution, helps you run your while protecting your networks from cyber attacks.

Sophisticated cyber adversaries want to gain domain dominance or establish persistence within your trusted networks: siphoning off sensitive data or laying the groundwork for crippling cyber attacks. But two-thirds of SMEs do not have the expertise to secure their networks.<sup>1</sup>

### Challenge

Q:MDR (QOMPLX'S Managed Detection & Response service) can help. Built on the flexible, high-speed Q:CYBER platform, Q:MDR helps you identify cyber threats fast. Our managed platform ingests, parses, normalizes, monitors, and correlates nearly any log source or security tool output. During deployment, our experts work with you to identify and onboard your critical sources. Q:MDR includes built-in integrations with QOMPLX [Identity Assurance](#), which protects your authentication controls from being attacked or subverted, and [Privilege Assurance](#), which helps you detect high-risk Active Directory configurations and privilege exposures.

**Our managed platform ingests, parses, normalizes, monitors, and correlates nearly any log source or security tool output.**



Ingests



Parses



Normalizes



Monitors



Correlates

---

<sup>1</sup> Source: Comptia, 2019. "Tech-Buying Trends Among Small and Medium-Sized Businesses"

# QOMPLX:CYBER

## Solution

Q:MDR experts work alongside your existing vulnerability management teams, technology operations teams and MSSPs. We monitor your network, hunt for threats, and alert you to imminent threats.

### **Q:MDR ingests and analyzes data from the following data sources:**

- Endpoint antivirus such as Symantec and McAfee
- Endpoint detection and response platforms, such as Carbon Black
- Email protection services, such as Trend Micro, MimeCast, Proofpoint and FireEye
- Vulnerability management systems, such as Tenable, Nessus, and Qualys
- Application log sources, such Apache HTTPD, Nginx, Microsoft SQL Server
- Operating system log sources, such as Windows Event Logs and Sysmon
- Monitoring systems, such as BMC and SolarWinds
- Security incident and event managers, such as Splunk, QRadar and LogRhythm
- Network security systems, such as NetWitness, Snort and Bro

Q:MDR offers both cybersecurity and peace of mind. We extend the capabilities of your team. With built-in integrations with QOMPLX's Identity Assurance and Privilege Assurance solutions, Q:MDR helps SMEs close the most critical pathways for ransomware attacks. Q:MDR benefits customers in the following ways:

- Comprehensive monitoring of cloud and on-site resources, either for primary coverage or to extend your team's ability to respond to after-hours events
- Timely and relevant alerts for security events and items of interest
- Customized service, with cyber intelligence and analytics, personalized escalation playbooks, and access to our deep bench of experts
- Cost efficiency. Q:MDR builds on your current resources and investments, and requires no up-front capital expenditures to realize benefits immediately

# QOMPLX:CYBER

## Key Features

During deployment, our experts work with you to identify and onboard your critical sources. Q:MDR includes built-in integrations with QOMPLX Identity Assurance, which protects your authentication controls from being attacked or subverted, and Privilege Assurance, which helps you detect high-risk Active Directory configurations and privilege exposures. Other features include:

- Data collection, consolidation, forwarding and normalization of log and event data
- 24x7 security event monitoring, notification, and alerting
- Complete visibility into ongoing analysis and incidents
- Security reporting, including insights and recommendations
- Web portal with log search, dashboards, and reports
- Monitoring of alerts from key security controls and log data sources

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

+1 (703) 995-4199

[info@QOMPLX.com](mailto:info@QOMPLX.com)

[www.QOMPLX.com](http://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 Reston, VA, QOMPLX, Inc. also has offices in New York and London. More information about QOMPLX can be found at <https://www.qomplx.com/>.