Technical know-how and trustworthy transparency

QOMPLX experience and execution helps a hyperscale edge data center deliver on client promises

Challenge

In today's digital world, speed thrills, lag kills, and companies must deliver a flawless online experience or go extinct. And as North America's leading network-neutral interconnection and hyperscale edge data center company knows all too well, connectivity, low latency, and digital availability are everything.

With a carrier-dense ecosystem of 700+ networks, over 300 cloud service providers, dozens of onramps, and strict SLAs, the client must be available to meet unpredictable and dynamic needs.

So when their self-managed SIEM resulted in generic monitoring reports that lacked context, action items, and a plan to identify and respond to threats, they knew the race against crime was on.

INDUSTRY:	Technology	
HEADQUARTERS:	Denver, Colorado	
EMPLOYEES:	100+	
OFFICES:	Denver, Colorado	
SELECT SERVICES:	■ Content ■ Data center	■ Financial services
ANNUAL REVENUE:	USD millions	

1.
North America's leading network-neutral interconnection and hyper scale edge data center company needed technical expertise and transparent reporting to find Active Directory flaws

2.
The client overpaid for alert information which lacked the context needed to effectively take action

3.
QOMPLX provided the technology, experience, and execution needed for the client to deliver on its promise

Solution

Going with QOMPLX was an easy decision due to:

- **Proprietary technology and data ingestion** The QOMPLX analytics platform combines real-time identity verification with customizable attack detections and interactive visualizations to secure the active directory
- **Security Operations Center (SOC) expertise** Averaging 15+ years of experience beating cybercriminals, QOMPLX experts impressed with their ability to anticipate threats and defeating lateral-movement attacks
- **Managed Detection and Response (MDR)** QOMPLX's MDR solution is customizable to fit client needs. It ingests, parses, normalizes, monitors, and correlates nearly any log source or security tool output, providing a powerful layer of security

Impact

There is no substitute for top-tier technology, honesty, and execution.

The native flexibility QOMPLX offers around data source integration enabled the client to feed Sumo alerts easily, expediting time to value. And when Q:Cyber detection rules and analytics were configured to run in stream, the client enjoyed a 54,000% decrease in alert volume.

With the QOMPLX SOC's expertise and transparent reporting, the client went into the rules builder to see the logic employed, alert metadata, and then collaborated on a managed detection and response plan.

The result: Visibility. Security. Scalability.

> With improved cybersecurity in place, the client can reliably scale smarter and faster to get its clients closer to their customers.

Why QOMPLX®

QOMPLX harnesses data to provide unified visibility into cyber risks and trust in identity. QOMPLX solutions reduce cyber risk and attack surfaces by mapping exposures and performing real-time detection of attacks. This approach increases network observability by closing the largest remaining gaps in cybersecurity: identity verification, cross-tool data fusion, and data interoperability. QOMPLX defends some of the world's most renowned brands by re-establishing trust for client organizations, assuring authentication, and enabling confident security decisions.

For more information, visit qomplx.com and follow us @QOMPLX.