Security steps up

QOMPLX protects global financial firm from ransomware

Challenge

In combat, the best way to defeat your enemy is to compromise their infrastructure. Unfortunately, criminal gangs and nation-state actors are employing that same strategy, as they zero-in on companies' critical infrastructures to steal data, launch ransomware attacks, and damage reputations.

Nearly all of these attacks target the active directory, including NTLM and Kerberos Protocols.

One of the world's top financial services firms retained QOMPLX to protect its critical infrastructure. The company also wanted to ensure that its aggressive acquisition strategy did not expose them to significant cybersecurity risks.

1.
In 2019, a top global financial services firm retained QOMPLX to help protect their active directory from attacks common to ransomware actors

2.
QOMPLX proposed a three-phased deployment of its Managed Assurance, Managed Detection & Response, and Special Situations Advisory services

3.
QOMPLX empowered the client to automatically identify skilled hackers attempting to breach their critical control infrastructure in real-time, with no false positives

INDUSTRY:	Financial services
HEADQUARTERS:	North America
EMPLOYEES:	>10,000
OFFICES:	North America
SELECT SERVICES:	■ Escrow services ■ Insurance
ANNUAL REVENUE:	USD billions

Solution

QOMPLX recommended a phased program including:

- **Critical infrastructure protection** QOMPLX Identity Assurance maps the on-prem and cloud-identity environment (including hundreds of domain controllers), validates authentication traffic, and protects against leading attack techniques
- **Managed detection and response** QOMPLX Managed Detections & Response ingests, parses, normalizes, monitors, and correlates logs source and security tools to detect cyber threats in real-time
- **Acquisition diligence** The QOMPLX Special Solutions Advisory Team did pre-acquisition assessments on three targets, producing "red flags" letters that identified key weaknesses while recommending strategic uplift initiatives

Impact

QOMPLX instituted an industry-leading, three-phase, comprehensive solution that enabled the client to gain a clearer picture of its critical control security and associated risks faced by acquisition targets.

Despite growing global network offices and servers, the client is now assured that their critical infrastructure is mapped, monitored, and protected.

The visibility provided by QOMPLX, coupled with its ability to quickly identify would-be hackers attempting to breach the critical control infrastructure in real-time, is a true difference maker – and reputation saver.

> With QOMPLX, the client now has increased visibility, vigilance, and security – and that creates peace of mind

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.