Security steps up

QOMPLX protects global financial firm from ransomware

1.
In 2019, a top global financial services firm retained QOMPLX's services to help protect their Active Directory from attacks common to ransomware actors.

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

2.
With QOMPLX, the client can now automatically identify skilled hackers attempting to breach their critical control infrastructure (CCI) in real-time, with no false positives.

Challenge

Criminal gangs and nation-state actors have used attacks on companies' critical infrastructures to steal data, launch ransomware attacks and damage reputations. Nearly all of these attacks target Active Directory including NTLM and Kerberos Protocols.

One of the world's top financial services firms retained QOMPLX to ensure that their critical infrastructure was protected. In addition, the company wanted to ensure that its aggressive acquisition strategy did not expose them to significant cybersecurity risks.

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

Solution

To keep their cyber risks well-controlled, QOMPLX engaged with the client in a multi-year program in three phases:

- **Critical infrastructure protection.** The client deployed QOMPLX's Identity Assurance software to map their entire on-prem and cloud-identity environment (including hundreds of Domain Controllers), validate all authentication traffic, and protect against leading attack techniques.
- **Managed detection and response services.** The client used QOMPLX's Managed Detections & Response (MDR) software-as-a-service to ingest, parse, normalize, monitor, and correlate logs source and security tools to detect cyber threats in real-time.
- **Acquisition diligence.** The client retained QOMPLX's Special Solutions Advisory team to perform pre-acquisition assessments on three targets, producing three "red flags" letters that identified key weaknesses and recommended strategic uplift initiatives.

Impact

With QOMPLX's industry-leading, three-phase, comprehensive solution, the client has a much clearer picture of not only their own critical control security but also of the associated risks they face from acquisition targets.

Despite their growing global network offices and servers, the client can now sleep easy: with QOMPLX, rapid identification of skilled hackers attempting to breach their critical control infrastructure (CCI) in real-time.

> With QOMPLX, the client can now automatically identify skilled hackers attempting to breach their critical control infrastructure (CCI) in real-time

Why QOMPLX®

QOMPLX is the cloud-native leader in risk analytics. We help organizations around the world make intelligent business decisions and better manage risk through our advanced, proprietary risk cloud. We are the leaders at rapidly ingesting, transforming, and contextualizing large, complex, and disparate data sources through our data factory in order to help organizations better quantify, model, and predict risk in areas including cybersecurity, insurance, and finance. For more information, visit **qomplx.com** and follow us **@QOMPLX**.