Premiums protected

QOMPLX finds and fixes gaps in insurer's cybersecurity

1.
QOMPLX's Special Situations Advisory team built a multipart solution to secure the client's technology stack, including a 60-day drive-to-zero surge to contain and eliminate all critical-, high- and medium-rated external vulnerabilities.

2.
QOMPLX's eliminated all material external exposures for the client within 60 days of starting the engagement.

Challenge

Anthem Blue Cross Blue Shield, the City of San Francisco, Google, and Target have suffered breaches via over-privileged insiders. In Anthem's case, an employee stole 18,000 members' health information. In San Francisco, a fired admin locked city records containing email, payroll, and police records. At Google, a former employee left the company with 14,000 documents including trade secrets on autonomous driving. Target was victim to a third-party data breach that affected more than 40 million customers.

When a QOMPLX client and major annuities and life insurance issuer saw the trouble with Target, they knew they couldn't risk the same fate. QOMPLX has the proven solution.

INDUSTRY:	Finance and Insurance
HEADQUARTERS:	North America
EMPLOYEES:	500+
OFFICES:	Global
SELECT SERVICES:	■ Insurance ■ Annuities
ANNUAL REVENUE:	USD Billions

Solution

QOMPLX's Special Situations Advisory team built a multipart solution to secure the client's technology stack:

- A 60-day drive-to-zero surge to contain and eliminate all critical-, high- and medium-rated external vulnerabilities;
- A 6-month strategic security transformation program to build maturity models, NIST-aligned risk programs, and cyber team capacity
- Ongoing instrumentation and monitoring of critical control infrastructure, to strengthen the client's Active Directory
- An economic model quantifying reductions in tail value at risk (TVAR), cyber insurance premiums, and retained cyber risks

Impact

The client's security program strength has improved with QOMPLX's Special Situations Advisory team:

- QOMPLX mapped and eliminated all material external exposures inside of 60 days
- All Active Directory domain controllers are protected by continuous monitoring for common tactics, including Kerberoasting and Golden Ticket attacks
- The client has a 3-year cybersecurity strategy, uplift, and staffing plan to reduce their financial tail risk in dollar terms by 90%, and their cyber insurance premiums by 60%

> QOMPLX mapped and eliminated all material external exposures for the client within 60 days of starting the engagement

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**.