# Premiums protected

## QOMPLX finds and fixes gaps in insurer's cybersecurity

### Challenge

Anthem Blue Cross Blue Shield, the City of San Francisco, Google, and Target all 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 the victim of a third-party data breach that affected more than 40 million customers.

When a major annuities and life insurance issuer surveyed the landscape and saw the perils, they knew they couldn't risk the same fate.

**1.**
The QOMPLX 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 eliminated all material external exposures within 60 days of starting the engagement

| | |
|---|---|
| INDUSTRY: | Finance and insurance |
| HEADQUARTERS: | North America |
| EMPLOYEES: | 500+ |
| OFFICES: | Global |
| SELECT SERVICES: | ■ Insurance<br>■ Annuities |
| ANNUAL REVENUE: | USD billions |

## Solution

The QOMPLX Special Situations Advisory Team built a multipart solution to secure the client's technology stack that included:

- A 60-day drive-to-zero surge to contain and eliminate all critical/ high/ and medium-rated external vulnerabilities
- A six-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 improved due to the QOMPLX Special Situations Advisory team and proprietary technology that:

- Professional Services team utilized Q:SCAN and OSINT tools to map and eliminated all material external exposures inside of 60 days
- The QOMPLX ITDR suite of solutions including Identity Assurance and Privilege Assurance protected all active directory domain controllers via continuous monitoring and detection for common tactics, including Kerberoasting and Golden Ticket attacks
- Advised the client on 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.