

Financial Services & Retail Banking

Post-breach crisis management & validation.

"The greatest post-breach risk is not exposure — it is uncertainty."

FORMAT

Case Study

ROLE

Chief Information Security Officer

PRODUCT

Intelligence Layer

CYBERSAGACITY.COM

© CyberSagacity 2026

ABOUT THE CUSTOMER · THE CHALLENGE

The hardest question: “are we still exposed?”

INDUSTRY	Financial Services & Retail Banking
REGULATORY	Governed by strict financial regulatory and compliance bodies
RESOURCE PROFILE	Mid-to-large internal task forces with multiple dedicated FTEs
CORE PAIN POINTS	Board pressure · regulatory scrutiny · long validation timelines · tool false-negatives

After a major breach, a regional bank was paralyzed by one question from regulators and the board. **An internal task force spent six months and multiple FTEs without a conclusion; the incumbent AST vendor spent three more months and still could not deliver a defensible view of residual risk.**



PRODUCT IN ACTION · HOW RESULTS WERE ACCOMPLISHED

From fragmented telemetry to re-exposure pathways in seconds.

01



Targeted telemetry ingestion

Introduced the Application Security Intelligence Layer to ingest fragmented tool telemetry and eliminate uncertainty from incomplete data.

02



Bypassing false negatives

Bypassed traditional AST false negatives that had left internal teams blind to existing vulnerabilities.

03



Instant pathway mapping

Pinpointed exactly where the breach could reoccur, identifying active re-exposure pathways in seconds.

04



Likelihood-based remediation

Generated a prioritized, likelihood-based remediation plan — compressing time-to-clarity from months to minutes.

The greatest post-breach risk was never exposure. It was uncertainty.

BUSINESS VALUE & IMPACT METRICS

9 months of uncertainty, resolved in seconds.

CyberSagacity gave leadership defensible, regulator-ready answers where nine months of manual effort and a vendor engagement had failed.

Seconds

To locate post-breach exposure pathways

Down from 9 months of manual failure.

8×

Productivity gain

Task-force effort redirected to resolution.

75%

Reduction in effective risk exposure

Residual risk made visible and closed.

500%

Improvement in AppSec ROI

Regulator-ready decisions,
defensibly delivered.

[Learn more at www.cybersagacity.com](https://www.cybersagacity.com) →