CINQUE
BY LOOM SECURITY

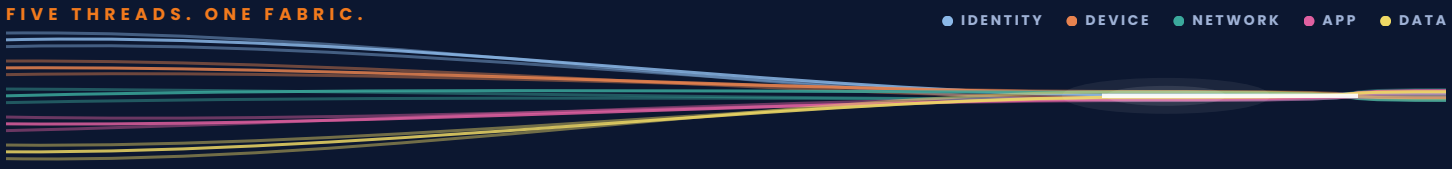
FOR FINANCIAL SERVICES SECURITY LEADERS

MORE TOOLS HAVE NOT GIVEN YOU MORE VISIBILITY

Which identities moved money last night?

Your IGA knows who was entitled. Your DLP knows a file moved. Your fraud platform knows a payment cleared. **None of them can tell you whether that behavior was normal for that identity.** The gap between *entitled* and *actual* is where the risk lives: payment rails, fintech partner connections, contractor access, and the agents now touching KYC, AML and fraud workflows. **CINQUE is the correlation layer above the stack you already own** — AI-native Unified Security Posture Observability.

FIVE THREADS. ONE FABRIC.



THE RECONCILIATION NOBODY RUNS

Every other balance in your institution gets reconciled. **Access does not.** Entitlement is asserted in your role model; behavior is the only proof.

PERSONA	ENTITLED — PER RBAC	OBSERVED — PER CINQUE	VARIANCE	READ TOGETHER
Treasury analyst	Initiate payments	→ Initiate **and** approve	FOUR-EYES BREAK	
Payment service account	3 systems, batch window	→ 7 systems, **off-window**	SCOPE DRIFT	
AML review agent	Read case files	→ Read **and** bulk export	NEW EXPORT PATH	
Fintech partner integration	Sandbox API only	→ **Production** ledger read	BOUNDARY CROSSED	
Branch operations	Teller applications	→ Teller applications	RECONCILED	

Illustrative. Each variance above sits below the triage threshold of the console that owns it — it exists only once all five control points are read together.

Detection tells you what happened. Context tells you whether it was supposed to happen.

WHERE FINANCIAL INSTITUTIONS POINT IT FIRST

Segregation of duties, verified
Asserted in your entitlement model, proven only in behavior. CINQUE shows where one persona sits on both sides of a control.

Payment-path exposure
Not just who *can* reach money movement, but which identities are behaving like they are moving toward it.

Third-party & fintech access
Your vendor register records who you contracted with, not what those identities actually touched.

Agents in regulated workflows
KYC, AML and fraud agents run on borrowed human authority. CINQUE baselines them as personas of their own.

MAPPED TO WHAT YOUR EXAMINERS AND AUDITORS NOW EXPECT

THE EXPECTATION	WHO IS ASKING	WHAT CINQUE'S CONTEXTUAL VISIBILITY GIVES YOU
A current, defensible inventory of systems, identities and access	**NYDFS Part 500 · CRI Profile · NIST CSF 2.0**	→ Personas discovered from **observed behavior** — human, non-human and agentic — current by construction, not by refresh date.
Evidence of how sensitive data and money actually move, not how the diagram says they do	**DORA · CRI Profile · PCI DSS v4.x**	→ One correlated journey **per persona** across all five control points, showing where access to money and NPI concentrates.
An accounting of the AI you run, including agents acting with borrowed human authority	**NYDFS AI letters · CRI Profile v2.2 & AI resources**	→ **Shadow AI, rogue service accounts and agents** as first-class personas with observed behavior.
Evidence you can stand behind at exam, in your third-party register, and to the board	**Your examiner · DORA register · NYDFS TPSP letter**	→ A short list of correlated, business-contextualized risks with **the full journey attached**.

Sourcing. *Framework references reflect published requirements as of July 2026; the FFIEC retired its Cybersecurity Assessment Tool in August 2025 without endorsing a successor. Requirements vary by charter and jurisdiction — the direction toward continuous inventory, data-flow evidence and accounting for the AI you run does not.*

Your data, handled like we mean it. Anything you share for an evaluation is limited and point-in-time, analyzed in an isolated environment, and deleted when we are done. Ask us for the data-handling summary — we are a security company; we expect the question.

SEE CINQUE ON YOUR ENVIRONMENT

Book a demo.
See your correlated risk picture.

Book a demo →

loomsecurity.io/requestdemo.html
info@loomsecurity.io

LOOM SECURITY

CORRELATE YOUR VISIBILITY. KNOW YOUR SECURITY POSTURE.