SOLUTION DESCRIPTION

Regulated financial services

Where the supervisory question is not "were you attacked" but "can you demonstrate what you knew, when, and what you did about it".

What is different about this estate

Three properties change the engineering, and they compound. The estate is **old in layers** — a mainframe boundary, a decade of middleware, a recent cloud programme, and an acquisition nobody has finished integrating. It is **supervised continuously** rather than audited annually, so evidence production is an operational load, not a project. And **availability is a regulated outcome**: an automated containment action that takes a payment rail offline is itself a reportable event.

The practical consequence is that the usual security-platform trade — accept some operational risk to reduce some security risk — has to be made explicitly, in writing, by someone with the authority to accept it. Tooling that cannot express the trade forces the institution to decline the automation entirely, which is the outcome most of these estates have reached.

Four things the platform does about it

Evidence is a query, not a reconstruction

Observations, judgements and actions share one store and one clock, so "what did we know at 11:02 and what did we do by 11:07" is answerable in one place. Alerts keep the events that justified them rather than a query that will return something different next year.

Retention is declared per record class, with a reason

Authentication, endpoint telemetry, adjudications and response actions carry different lifetimes because they answer different obligations. A single global window is simultaneously too short for the supervisor and too long for the data-protection regime.

Automated response is bounded before it is armed

Every action computes what it will touch against the current estate — hosts, sessions, tiers — and refuses to run unattended when the scope cannot be computed. Irreversible actions are held for a person's approval on a channel that does not depend on the estate under contest.

Third-party and vendor access is a first-class subject

Outsourced operations mean sessions held by people who do not work for you. Those sessions are scoped, expiring and continuously re-evaluated.

The reporting consequence. Every figure that reaches a board pack or a supervisory return carries the query, window and computation time that produced it. A number challenged in a review is re-derivable rather than defended from memory — which is the difference between a finding and a conversation.

Where a payments estate breaks the usual playbook

Isolating a compromised host is the standard first move and it is wrong on a settlement node mid-window. The platform reads a criticality class from the asset itself — not from a playbook setting an operator can relax under pressure — and in the classified tiers it proposes rather than acts, carrying the full computed scope so the person with authority over the rail decides with the security case in front of them.

That list is written down during deployment, before anything is armed: which asset classes carry the class, who may override, and what the platform is never permitted to do unattended.

What we will not claim

We do not map to a named regulation on this page, because a control mapping is only meaningful against your interpretation of your obligations in your jurisdiction — and a vendor asserting compliance on your behalf is doing you a disservice. What we bring is the evidence layer that makes your own mapping demonstrable.

We also do not detect authorised misuse. A person acting within their entitlements, at ordinary volume, for the wrong reason produces no anomaly and matches an approved pattern. That is a governance problem wearing a detection costume, and no platform resolves it.

EventLake

NEXT STEP

Bring the evidence request that took six weeks. We will walk which parts become a query, which stay manual, and which would still be unanswerable — that third category exists, and naming it early is worth more than a demonstration.

Further reading: Paper 05 *Delegation is a design problem* · Paper 06 *Evidence should be a query* · Paper 11 *We are the most privileged software you will install.* All published, none behind a form. eventlake.com