SOLUTION DESCRIPTION

MSSP and multi-tenant operations

Where your analysts cross customer boundaries all day, and every crossing is something a customer is entitled to see.

What is different about this estate

A service provider inverts the usual model in three ways. **Cross-tenant access is the job**, not an exception — so "no standing access" has to be compatible with an analyst opening forty customers' queues in a shift. **Margin is a function of analyst minutes**, which makes the composition of the queue a commercial variable rather than an operational preference. And **you inherit your customers' obligations**: each one's retention, residency and erasure rules apply to data sitting in your platform, and they do not agree with each other.

Tooling built for a single enterprise handles all three badly. Tenant separation implemented as a filter in every query fails the first time someone writes a query without one — and in this business, that failure is a notification to every customer you have.

Four things the platform does about it

Isolation by keys and storage boundaries, not by query hygiene

A query missing its tenant scope returns nothing rather than the wrong customer's data. Both designs pass a penetration test on a good day; only one fails safely on a bad one.

Every crossing is an event in the customer's own store

Time-boxed, reason-bound grants, each opened with step-up, — and the access record lands where the customer can query it beside their telemetry. An access log you hold is a promise; an event in their store is a control, and it is also your best answer in a procurement review.

Findings cross the boundary; events do not

A technique seen at one customer improves detection for the rest as a compiled, reviewed rule carrying no customer-identifying content. It is a narrower benefit than the marketing version of cross-tenant learning, and it is the version that survives a customer's security questionnaire.

Retention and erasure are per tenant, per class

One customer's thirteen months and another's seven years coexist without a policy document that describes something the platform is not doing. An erasure request destroys that subject's key, which makes their personal data unreadable in every copy of the event store, and the erasure itself is recorded.

Where the margin actually moves. Not in triage speed — in queue composition. Adjudicating legitimacy against each customer's own change records removes the authorised-but-unusual cases that consume the majority of analyst minutes and never become incidents. What remains is harder per case and far smaller, and the analyst decision is retained as a reusable citation rather than a closed ticket.

White-label and the reporting surface

Customer-facing reports carry your identity, and every figure in them carries the query, window and computation time that produced it. That provenance is what lets a customer challenge a number and get an answer rather than a defence — and it is the difference between a monthly report that builds trust and one that erodes it slowly.

Coverage is reported the same way: per tenant, dated, conditional on the telemetry that tenant actually sends. A customer who is not collecting command lines has a smaller real coverage figure than one who is, and saying so is more defensible than a single number applied to everyone.

What we will not claim

Consolidating your customers onto one platform concentrates risk that was previously distributed. A compromise of us is a compromise affecting all of them at once, and no amount of tenant isolation makes that untrue — it only bounds it. That trade should be made deliberately and disclosed to your customers, not sold as pure upside.

We also will not tell you this reduces headcount. It changes what your analysts spend the shift on. Whether that becomes margin, growth, or better service is your decision, and we have no basis for a number.

EventLake

NEXT STEP

Bring one week of one customer's queue. We will classify what was genuinely ambiguous against what was authorised-but-unusual — the ratio is the business case, and it is specific to your book rather than to our benchmark.

Further reading: Paper 03 *The question is not "is this malicious"* · Paper 08 *A vendor who publishes no gaps* · Paper 11 *We are the most privileged software you will install.* All published, none behind a form. **eventlake.com**