EventLake

For identity and access programme leads

IDENTITY · SESSIONS · WORKLOADS

You finished the hard part. The adversary moved to the easy one.

Phishing-resistant authentication is a real improvement and it changed the plan rather than ending it. What follows a sign-in is a bearer artefact, and to almost every system that receives it, possession is indistinguishable from authentication.

WHERE EFFORT GOES

Two seconds at the door

Hardware-backed, attested, correct. Then eight hours — or thirty days — during which nothing looks again.

WHERE RISK SITS

Inside the session

A token lifted from a browser profile, an agent's memory, a log file or a build environment. The credential was never contested; it was reused.

THE FIX

Treat it as a standing claim

A session holds while its supporting conditions hold — device, posture, network, behaviour. Re-evaluate on change, not on a timer.

A stolen token, continuously evaluated

the decisive signal is not an identity signal

- 08:31 — **sign-in, hardware-backed** · device attested — the claim is issued
- 14:07 — **a non-browser process reads the browser profile** · an endpoint signal, meaningless there alone
- **14:09** — **binding fails from an unattested device — revoked everywhere** · the legitimate user notices nothing

THE LARGER POPULATION

Service accounts, workload identities, API keys, agents and integration credentials outnumber your staff by an order of magnitude, hold broader entitlements, rarely rotate, and cannot be asked for a second factor. Your identity programme is named after the smaller group.

They compensate by being predictable. A batch job runs at the same time, from the same place, against the same resources, forever — so **a service account doing something new is a stronger signal than a person doing something new**, and almost nobody alerts on it.

WHERE THIS GETS UNCOMFORTABLE

Continuous evaluation is a surveillance capability pointed at your own staff. Evaluate against the session's baseline rather than a personal profile, keep the signals in their own retention class, make the criteria legible to the people subject to them, and never let session telemetry feed performance management.

Aggressive revocation also makes availability a security decision. The recovery path must be as well designed as the enforcement, or the first bad revocation ends the programme.

START WITH THE COUNT

How many non-human identities do you have?

If the answer takes a project, that is the finding. We will produce the inventory — usually the most actionable list in the programme.

Book a session

contact@eventlake.com

We ask for a work email and a phone number, and we tell you what we will do with them before you submit. We do not sell contact data, and one unsubscribe stops everything.