

Authority Persistence Boundary

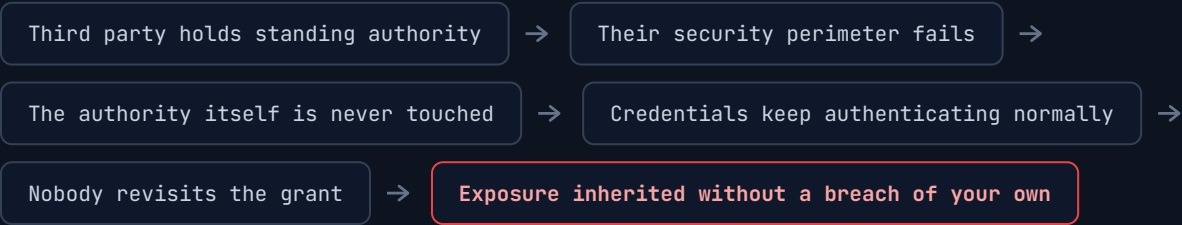
DEFINITION

The boundary between a trust relationship failing and the authority it granted actually becoming invalid.

FRAMEWORK FLOW

01 The Condition A third party retains valid authentication and delegated authority into your infrastructure.	02 The Boundary Trust sits outside your security perimeter. The authority it produced sits inside your infrastructure boundary.	03 Failure State The third party is compromised — its credentials and delegated authority remain technically valid regardless.	04 Consequence You inherit transitive control-plane exposure without your own security perimeter ever being breached.
--	--	---	--

Failure State: Transitive Authority Exposure



THE DIAGNOSTIC SIGNAL

AUTHORITY OWNERSHIP

Ask the third party whether their standing access is still needed and still correctly scoped. The answer is almost always yes — confidently, and often wrong.

REVOCATION OWNERSHIP

Ask who is responsible for revoking a vendor's authority the moment trust in that vendor changes. The honest answer is usually nobody — no owner, no trigger, no process.

TRIGGER CONDITION

Activates the moment a third party's own security posture is compromised, disputed, or simply unverifiable — not on a fixed recertification schedule.

REMEDIATION SHAPE

An independent revocation trigger, a standing-access inventory, time-boxed grants, and an assigned owner accountable for closing the gap — architectural, not procedural.

WHERE THIS SHOWS UP

CONSULTING & SYSTEMS INTEGRATORS

Standing administrative credentials issued for the length of an engagement, rarely time-boxed to it, and rarely revisited once the engagement quiets down.

MANAGED SERVICE PROVIDERS

Broad, often persistent access across every client tenant an MSP serves — a single MSP compromise is a multi-tenant exposure by construction.

SAAS ADMINISTRATIVE INTEGRATIONS

OAuth grants and admin-console integrations that outlive the project that justified them, discovered only during an unrelated access review.

CI/CD & AUTOMATION SERVICE IDENTITIES

Long-lived service principals and pipeline credentials held by third-party automation platforms, authenticating on a schedule nobody watches.

ARCHITECTURAL RELATIONSHIPS

#156

Authority Survivability Boundary

RELATED MODERATE

Inverse condition, same doctrinal family — #156 asks what happens when authority becomes unavailable; #169 asks what happens when it remains fully available after the trust that justified it has already failed.

#160

Identity Boundary Inversion

RELATED WEAK – CROSS-PILLAR

Doctrinal parallel — #160 establishes identity as the effective control boundary; #169 examines the case where that boundary is held by a third party, and stays held even after the third party is compromised.

#165

Authority Arbitration Gap

RELATED WEAK – CROSS-PILLAR

Distinguishes two failure modes — #165 is unresolved conflict between correctly-scoped, coexisting authorities; #169 is a single authority whose triggering trust condition silently failed while the authority itself stayed unchanged.

ANCHOR /third-party-cloud-access/

FRAMEWORK HOME

The condition is vendor-agnostic — consultants, MSPs, migration partners, SaaS integrations, and automation identities all produce the same authority-persistence gap regardless of which third party holds the access.

"Every third-party integration can correctly explain why its access was granted. Almost none can explain why it's still valid — not because anyone forgot to ask, but because nothing ever asked automatically."