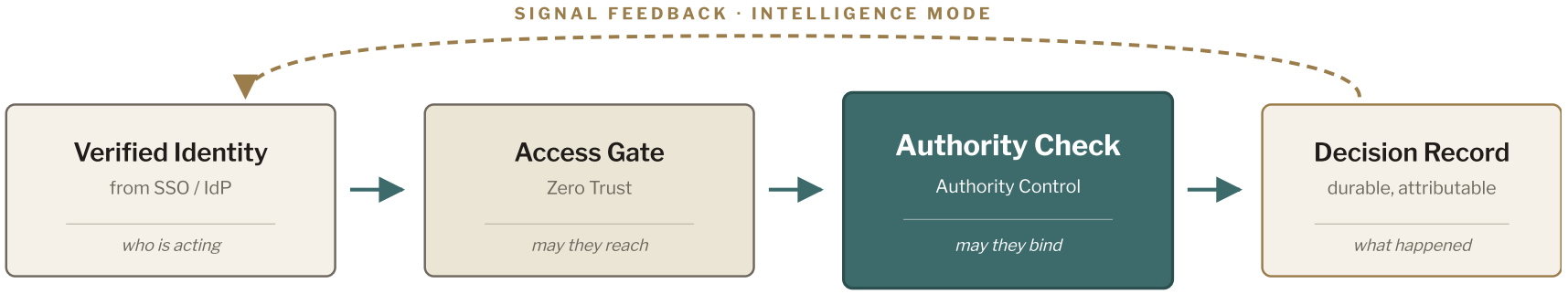
The Commitment Boundary

Access is verified. Commitment is not.

In many enterprise breaches, a legitimate identity creates consequences the organization never authorized, even when controls confirm identity, device, network, and access correctly. The gap is at the commitment boundary, where no structure confirms whether the identity holds authority to bind the organization.

Zero Trust verifies identity. Authority Control verifies the authority to bind the organization through that identity. **Together they form a single observable enforcement architecture.**



Zero Trust protects the token. Authority Control protects what the token is allowed to do.

INTELLIGENCE MODE · VALUE FROM DAY ONE

Authority Control deploys in intelligence mode, actively producing structured signals that flow into the existing Zero Trust layer from day one. No operational disruption. Enforcement activates when the organization is ready, on its own timeline.

CONSTRAIN

Define and enforce authority scope for each integration and identity, narrowing the surface that compromised credentials can act through.

INFORM

Signal authority anomalies and unusual commitment patterns into the access layer, sharpening Zero Trust posture in real time.

ENFORCE

Hold commitments that fall outside defined scope, with a durable record for every enforcement event.

Zero Trust secures access. Authority Control secures consequence.

Peer infrastructure for the moment authentication ends and obligation begins.

NEXT STEP

invariancearc.com

Operating concept available on request · Confidential briefings under NDA

What happens at the moment of commitment

On February 21, 2025, a compromised transaction entered Bybit's trusted, multisig-approved workflow and executed at machine speed. $1.4 billion in Ethereum became irreversible within minutes.

Without Authority Control

✓ Identity verified
✓ Approval valid
✓ Access granted

▼

COMMITMENT BOUNDARY

▼

Transaction executes
No authority check at the point of commitment

▼

$1.4B
committed · irreversible

With Authority Control

✓ Identity verified
✓ Approval valid
✓ Access granted

▼

COMMITMENT BOUNDARY

▼

Authority evaluated at boundary
Outside verified scope · Stopped

▼

$0
authorized

Same identity. Same approval. Different outcome.

COMMITMENT SURFACES

The organization defines scope. Authority Control governs the boundary wherever it appears.

Delegated Access	System Changes	Automated Operations
Credential exceeds scope	*Change binds organization*	*Action creates consequence*

Different surfaces. Same boundary.

CONSTRAIN
Define authority scope for each integration and identity.

INFORM
Signal authority anomalies into the access layer.

ENFORCE
Hold commitments that fall outside defined scope.

One architecture across every commitment surface.

Salesloft / Drift

Valid token, out-of-scope consequence. The exposure persists wherever delegated integrations carry implicit authority to act broadly within their access scope.

FINANCIAL SERVICES · ENTERPRISE SAAS

DISCLOSED AUGUST 2025 · 700+ ORGANIZATIONS AFFECTED

CURRENT EXPOSURE

OAuth tokens tied to a legitimate Drift-to-Salesforce integration were used to query and extract Salesforce data across hundreds of organizations. The token and session looked legitimate; the downstream data action did not match the intended delegation. Every enterprise consuming OAuth-mediated SaaS integrations carries the same structural exposure today.

WHY ZERO TRUST DOES NOT STOP IT

Zero Trust verifies the identity, the token, and the session. It does not evaluate whether the resulting export behavior fits the narrow purpose for which that integration was originally trusted. Access is verified. Consequence is not.

WHAT AUTHORITY CONTROL ADDS TODAY · THREE DEPLOYMENT POSTURES

CONSTRAIN

The customer defines authority scope for the integration: allowed actions (read conversation context, create or update contacts), prohibited actions (bulk export of accounts and opportunities, retrieval of stored secrets), magnitude limits, and aggregate exposure bounds.

INFORM

Authority Control evaluates each action against the authority scope through Salesforce Event Monitoring. Anomalies and out-of-scope attempts are signaled to the access layer in real time, even before any enforcement is turned on.

ENFORCE

Bulk export attempts that exceed the defined scope are held with a durable, attributable record, regardless of whether the underlying token is authenticated. Optional enforcement is activated when the customer is ready.

WHO DEPLOYS · CUSTOMER EDGE

Authority Control is deployed by the Salesforce customer, independently of the platform vendor. The customer defines authority, owns the data, and controls integrations. The exposure can be addressed today through customer-side deployment.

OUTCOME WITH AUTHORITY CONTROL

Compromised tokens cannot create consequence beyond the authority scope defined for the integration.

Exposure from credential compromise is bounded by what the integration was authorized to do, not by what its credentials technically allow.

The SolarWinds Pattern

Trusted channel, changed behavior. The structural pattern from 2020 is still unaddressed and reproduces in current attacks.

SOFTWARE SUPPLY CHAIN · THE UNADDRESSED PATTERN

DISCLOSED 2020 · PATTERN REPRODUCING IN 2025–2026

CURRENT EXPOSURE

Organizations trust software through legitimate delivery channels and grant it privileged operational access. When the software behavior changes, the original trust relationship persists and the downstream actions still appear legitimate. The pattern reproduces in MCP rug pull attacks, the Smithery platform compromise, and every authority delegation bound to identity rather than to a defined scope of action.

WHY ZERO TRUST DOES NOT STOP IT

Zero Trust verifies trusted software identity and approved distribution paths. It does not evaluate whether the new downstream behavior still matches the originally authorized purpose of that software. The original trust relationship persists after behavior changes.

WHAT AUTHORITY CONTROL ADDS TODAY · THREE DEPLOYMENT POSTURES

CONSTRAIN

Authority scope is defined for what the software is supposed to do: allowed network destinations, allowed operational actions, allowed configuration changes. Delegation is bound to authorized behavior, not to the software identity.

INFORM

Authority Control consumes operational telemetry and evaluates each action against the authority scope. Behavior outside the scope is detected, recorded, and signaled to access control systems for containment, even when the delivery path remains legitimate.

ENFORCE

Where interposition is feasible, out-of-scope actions are held at the boundary. Where interposition is harder, the signal path drives access policy adjustment in the existing Zero Trust layer to contain the consequence.

DEPLOYMENT NOTE · INTELLIGENCE MODE IS THE REALISTIC PATH

For software supply chain compromises, intelligence mode is the most defensible deployment posture. Authority Control detects commitments inconsistent with delegated authority and signals to access control systems for containment, rather than claiming direct execution-layer blocking. Full enforcement requires deeper infrastructure integration that customers should expect over time, not on day one.

OUTCOME WITH AUTHORITY CONTROL

Behavior outside the originally authorized purpose is surfaced immediately, written to a durable record, and returned as a commitment-aware signal even when the delivery path remains legitimate.

The original trust relationship no longer persists silently after behavior changes.