zenphi | Google Cloud Partner

The Real Cost of Fragmented Security Automation

Security enforcement today relies on a mix of SOAR playbooks, RPA bots, scripts, and low-code workflows. Individually, these tools can work. But at scale, they introduce rigidity and operational overhead—especially for policy enforcement, identity workflows, and audit readiness.

When security automation becomes rigid, every exception becomes a cost.

AREA	RIGID / FRAGMENTED AUTOMATION	DETERMINISTIC ENFORCEMENT
Workflow changes	Require redesign	Adjust logic only
Execution model	Bots / scripts	API-driven
Policy enforcement	Inconsistent	Predictable
Auditability	Reconstructed	Built-in
Error handling	Reactive	Preventive
Scalability	Costly	Linear

The Real Daily Cost* of Fragmented Automation

Even when automation exists, IT and security teams often spend time **maintaining enforcement workflows** rather than enforcing policy.

Fixing broken automations (bots, recipes, scripts) *≈ 25-30 min/day (triage + rework + reruns)*	**$50**
Reconciling access mismatches and stale permissions *≈ 20 min/day (cleanup + checks + escalation)*	**$40**
Re-running failed enforcement workflows after partial execution *≈ 10-15 min/day (retries + exception handling)*	**$30**
Rebuilding audit evidence across siloed tools *≈ 20–30 min/day (log gathering + screenshots + reports + validation)*	**$50**
Coordinating exceptions across teams and systems *≈ 15–25 min/day (tickets + hand-offs + ownership clarification)*	**$40**
Annual impact:	**$210/day × 260 working days ≈ $54,600/year**

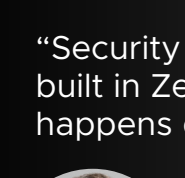
*Assuming that an average blended IT/security cost rate in the US of roughly $120/hour. The cost reflects not only labor but also the time lost in back-and-forth and rework

Why Fragmentation Creates Operational Debt

- Bot dependency
- Tool sprawl
- Hard-coded logic
- Per-action pricing
- Lack of ownership
- Limited granularity

The alternative isn't "more tools." It's a different execution model—one built for consistent enforcement

"Security policies aren't the hard part. Consistent execution is. Automations built in Zenphi helped us close the gap between intent and what actually happens day to day"



Francis Frain

VP, Information Security & IT
Infrastructure at Emerson College

Zenphi **supports enforcement-first workflows** for IT operations and Google Workspace environments—enabling consistent execution without automation sprawl

Common Zenphi-Driven Wins

Enforce by Event

Replace tickets and manual follow-ups with event-driven workflows that trigger automatically when the right signal occurs—new hire, role change, approval granted, policy violation detected, or scheduled audit run.

Enforcement happens on time, every time

Execute Deterministically

Run workflows with predictable logic and controlled actions—no bots, no brittle scripts, no "works until it doesn't." The same process executes the same way across systems, even when environments change.

Fewer exceptions, fewer reruns, fewer failures

Govern with Approvals

Build governance directly into execution. Route exceptions and high-risk actions through approvals and segregation of duties, with granular permissions defining who can authorize what—and under which conditions.

Control improves without slowing teams down

Stay Audit-Ready

Capture a complete execution record by default—what triggered the workflow, what decisions were made, and what actions were taken across systems. Evidence is generated continuously, not reconstructed later.

Audits shift from fire drills to repeatable reporting

Book A 20-Minute Workflow Assessment

Book A Call

Get a quick map of your highest-impact IT Ops automations.

zenphi