The Invisible Fortress

Embedding Zero-Trust Governance in the Supergraph

Capital One

Gaurav Singh

Distinguished Engineer - Cyber Security

Sulbigar Shanawaz

Distinguished Engineer - Enterprise Data Platform

THE PERSONA GAP

Why builders and risk teams talk past each other

Technical Persona

- Velocity & schema evolution
- Autonomy to ship fast
- Security feels like opaque runtime checks — an invisible gatekeeper that blocks deployments

VS

Risk Persona

- Liability management & NPI/PII protection
- Compliance with GDPR, GLBA, SOX
- Fast schema changes are unquantified liabilities

COMMON AREAS OF RISK

Data Exposure

Unintentional leaks of PII on public types

Persona Controls

Holistic impact assessments per persona

External Access

Internal vs. external API differentiation

Business Disruption

Breaking changes causing app failures

Compliance & Legal

GDPR/HIPAA violations from untracked data

OAuth Scope Drift

Excessive disclosure via misconfigured scopes

FINANCE & CYBERSECURITY RISK

NPI Exposure

Account numbers, transaction histories leaked via schema

GLBA / PCI DSS / SOX

Regulatory violations with SEC/FINRA enforcement

Attack Surface

Broken access control & query-complexity DoS attacks

Audit Trail

Who approved, why, and when — evidence for federal auditors

GRAPHQL RISK MAPPING

Translating technical elements into control objectives

GraphQL Element	Risk Context	Control Objective
Types & Fields	Asset Inventory	Data Classification (NPI/PII)
Directives (@auth)	Security Engine	Logical Access Control (SOX/GLBA)
Introspection	Reconnaissance	Attack Surface Reduction
Query Complexity	Resource Control	DoS Prevention & Stability

THE BLIND SPOT

Why legacy security fails the Supergraph

Silent Exposure

Firewalls miss field-level leakage — they don't speak GraphQL

Opaque Runtime Checks

Security logic buried in code, invisible to auditors and developers

"Culture of No"

Slow manual reviews become the only defense against unquantified risk

THE SUPERGRAPH

A strategic pivot: your single point of governance

Technical Contract

Unified interface between business and data

Strategic Entry Point

Single point for all federated traffic & governance

Live Risk Map

Real-time governance dashboard from metadata

THE PARADIGM SHIFT

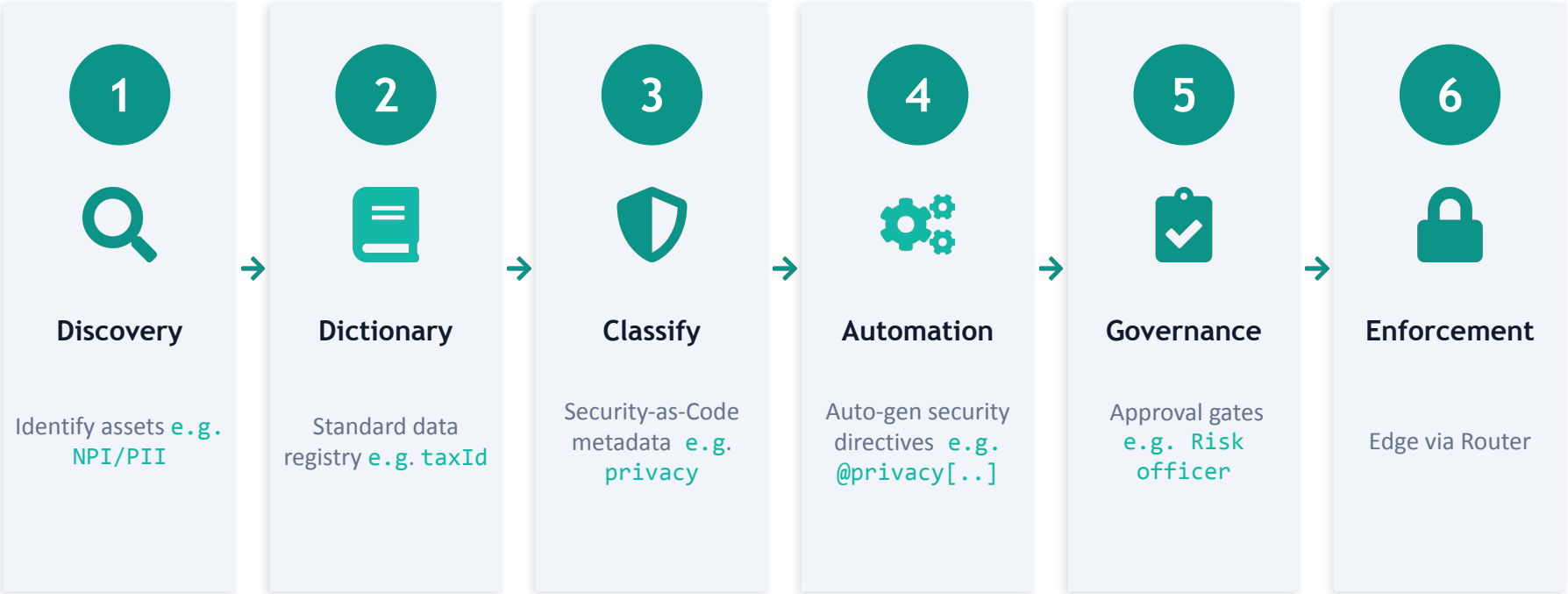
BEFORE

- Auth logic scattered in resolvers
- Security is a black box at runtime
- "Security surprises" in production
- Manual audit of backend code

AFTER

- Auth in the schema (design-time)
- Router = sub-ms Policy Enforcement
- Deterministic: schema blocks it before backend
- Machine-readable compliance evidence

THE 6-STEP GOVERNANCE LIFECYCLE



THE COLLABORATIVE ROADMAP

Risk Professionals

Define the risk rules
& security requirements

Schema Designers

Tag risk rules
to the schema

Engineers

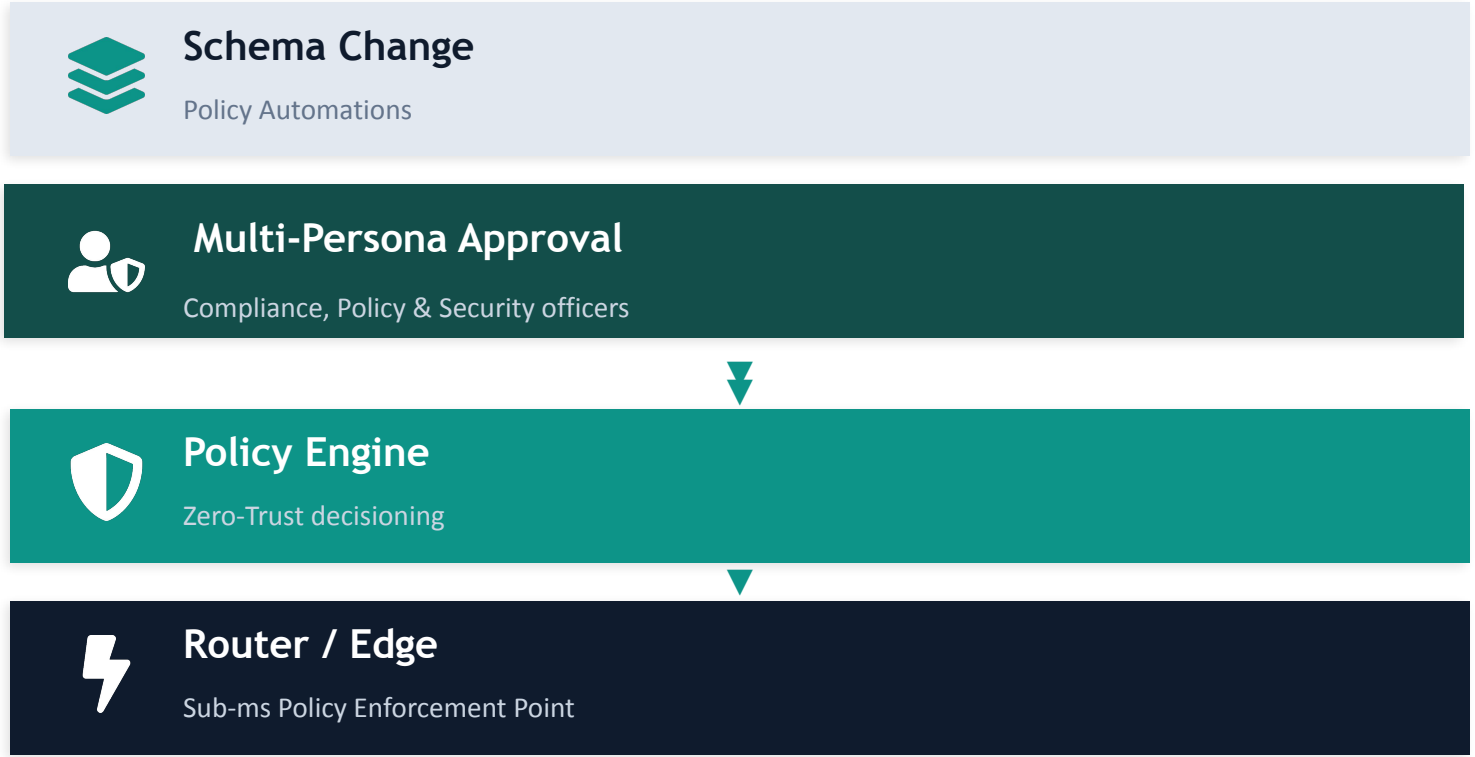
Codify as
design-time security

KEY OUTCOMES

Observability — live "who can see what" map

Automated Assurance — security as a built-in feature

VALIDATION & POLICY SYNERGY



SCHEMA AS ENFORCEMENT CONTRACT

Machine-readable evidence for regulators

```
type Author
  @privacy(policies: [PII_BASIC, PII_CONTACT])
  @compliance(frameworks: [GDPR, CCPA, UK_GDPR])
{
  id: ID!
  legalName: String!
    @privacy(policies: [PII_BASIC])
    @compliance(frameworks: [GDPR, CCPA])
  taxId: String
    @privacy(policies: [CONSENT_REQUIRED])
    @compliance(frameworks: [GDPR, SOC2])
    @proprietary(classification: RESTRICTED)
}
```

@privacy directives classify PII at the field level

@compliance maps directly to regulatory frameworks

@proprietary enforces internal access tiers

THE EFFICIENCY DIVIDEND

Faster

Security review
time per release

Instant

Enforcement

Auditable

Reporting & Audit Metrics

Risk is not the enemy of speed — opaque risk is.

THANK YOU

Gaurav Singh linkedin.com/in/-gauravsingh-

Sulbigar Shanawaz linkedin.com/in/sulbigar-shanawaz