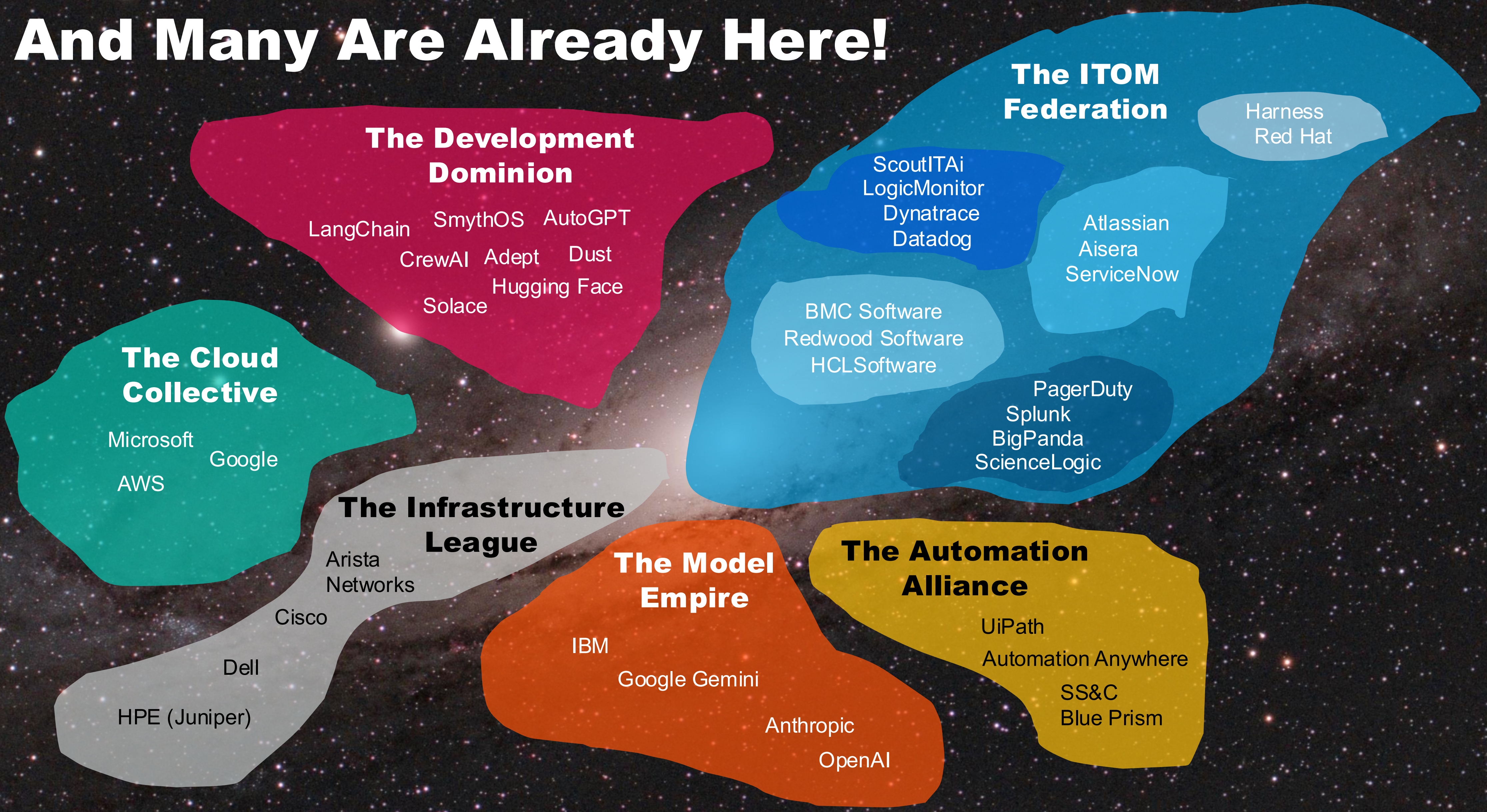
How IT Operations Can Prepare for the Promise and Peril of AI Agents

Cameron Haight

AI agents are both the best and most dangerous things to ever happen to I&O.

… And Many Are Already Here!



The Development Dominion

LangChain
SmythOS
AutoGPT
CrewAI
Adept
Dust
Hugging Face
Solace

The ITOM Federation

Harness
Red Hat

ScoutITAi
LogicMonitor
Dynatrace
Datadog

Atlassian
Aisera
ServiceNow

BMC Software
Redwood Software
HCLSoftware

PagerDuty
Splunk
BigPanda
ScienceLogic

The Cloud Collective

Microsoft
Google
AWS

The Infrastructure League

Arista Networks
Cisco
Dell
HPE (Juniper)

The Model Empire

IBM
Google Gemini
Anthropic
OpenAI

The Automation Alliance

UiPath
Automation Anywhere
SS&C Blue Prism

Note: This is just a representative sample of vendors.

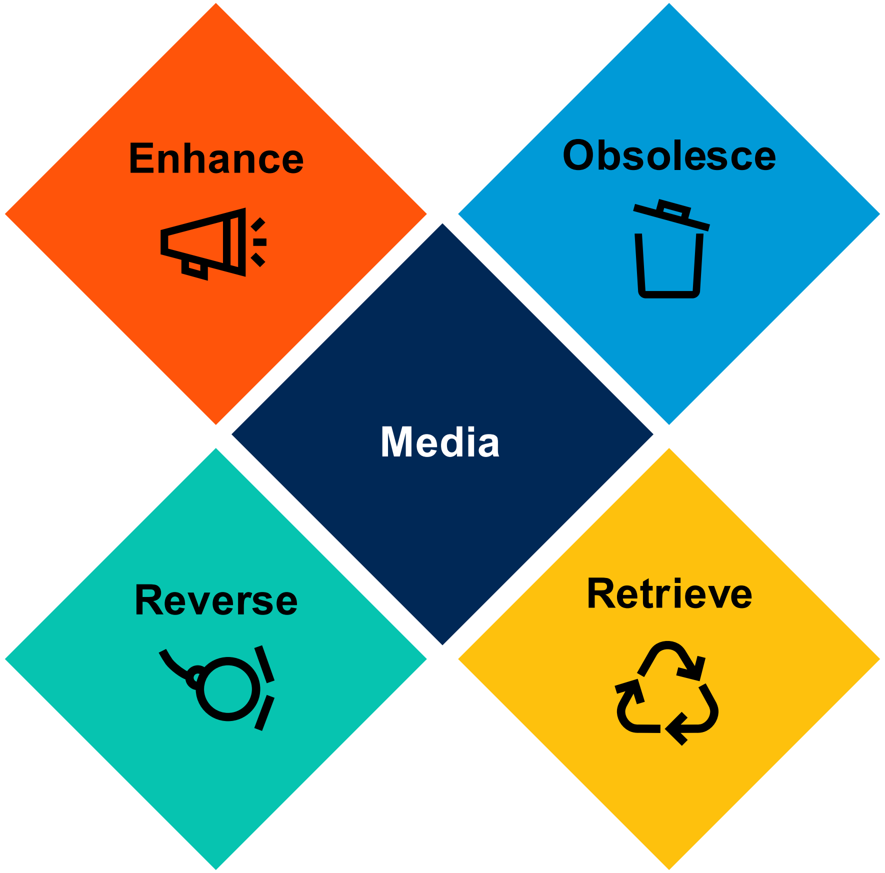
Key Issues

1. What promises and perils do AI agents portend for IT operations?
2. What new I&O operating model might be required to manage AI agents?

Key Issues

1. What promises and perils do AI agents portend for IT operations?
2. What new I&O operating model might be required to manage AI agents?

The McLuhan Tetrad: A Framework to Analyze AI Agent Impact on I&O



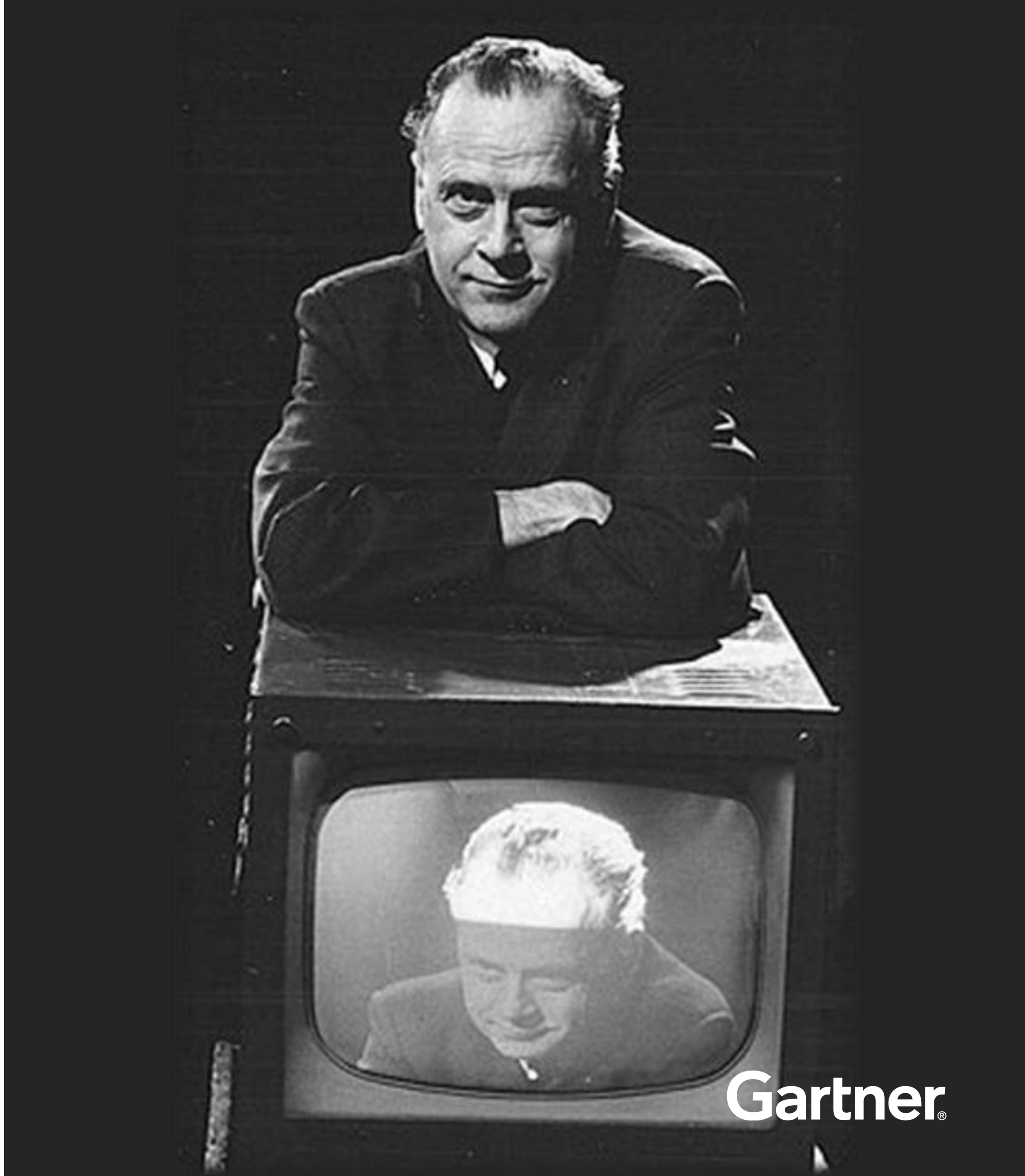
Enhance

Obsolesce

Media

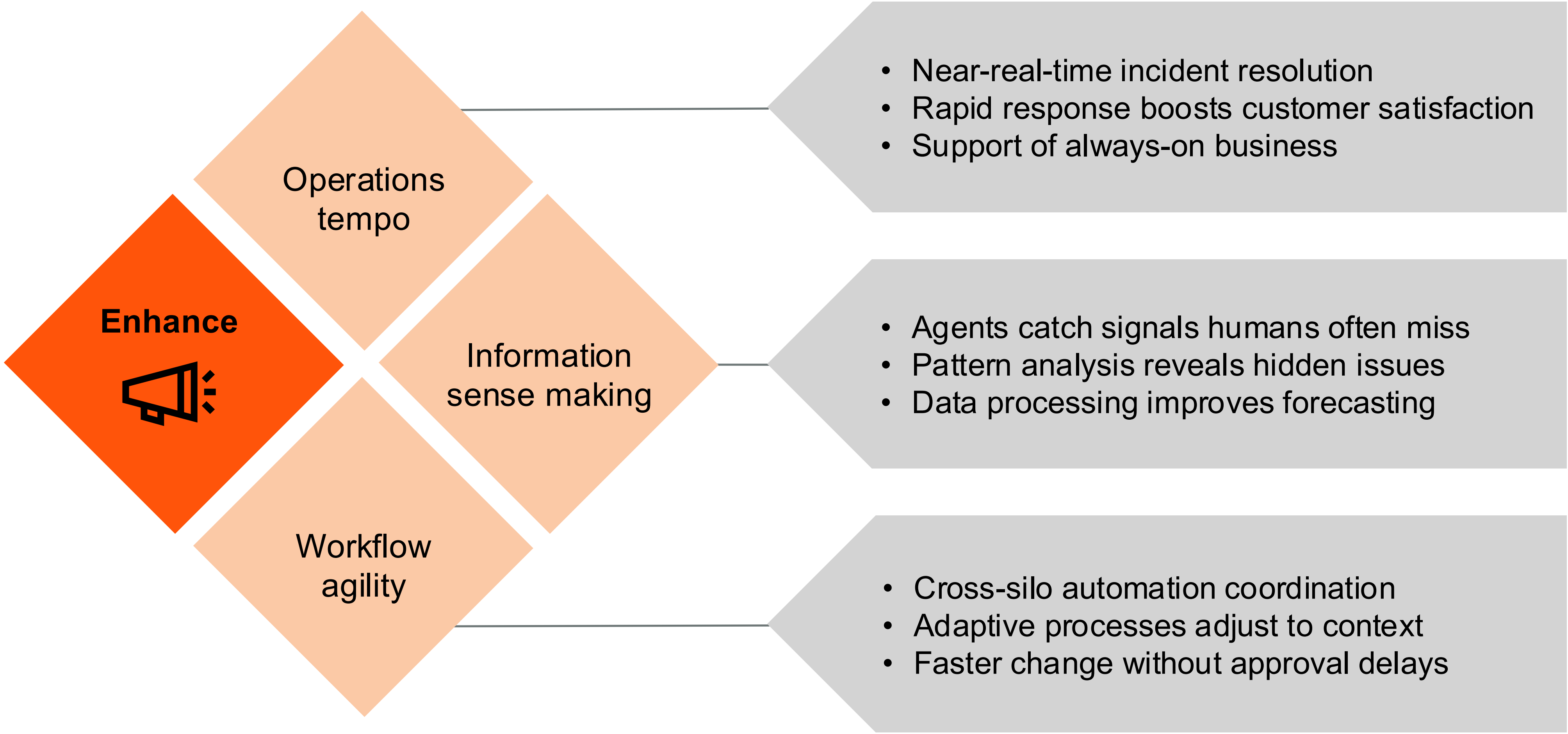
Reverse

Retrieve



AI agents enhance, obsolete, revive and reverse IT operations capabilities — all at once. **This paradox explains why they are both the best and most dangerous things to ever happen to I&O!**

Enhance: Amplified Capabilities



Enhance

Operations tempo

- Near-real-time incident resolution
- Rapid response boosts customer satisfaction
- Support of always-on business

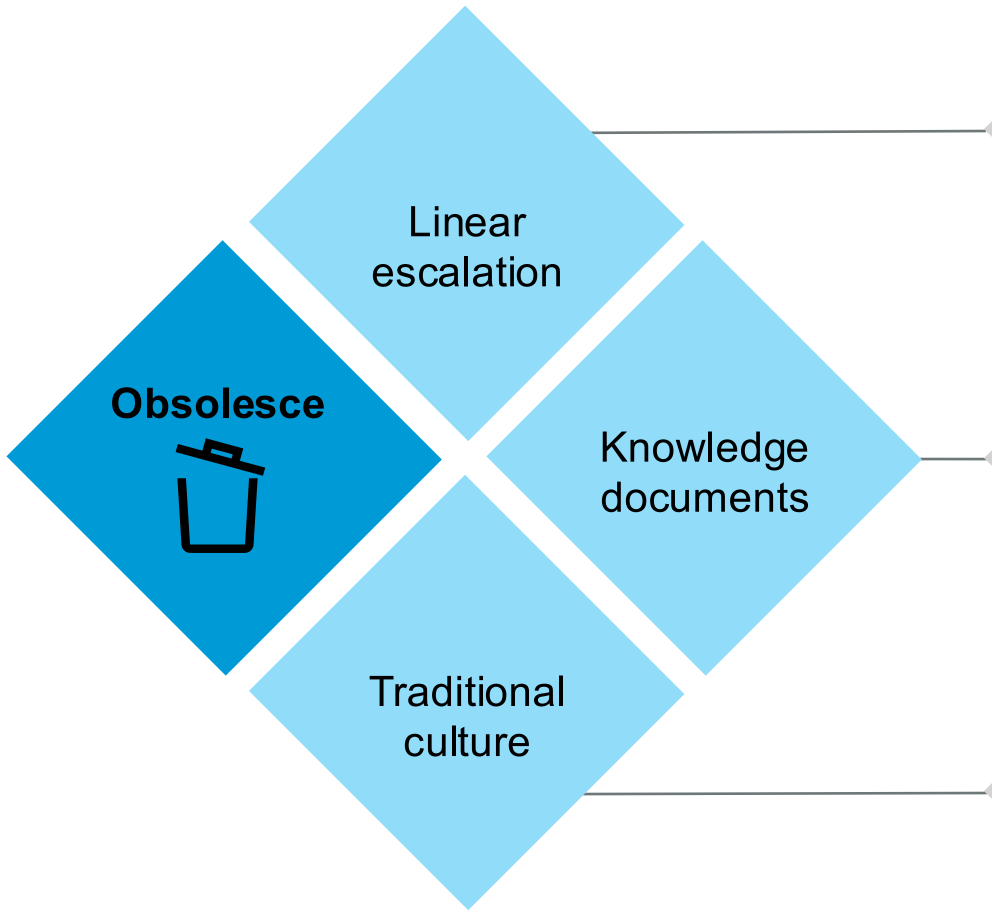
Information sense making

- Agents catch signals humans often miss
- Pattern analysis reveals hidden issues
- Data processing improves forecasting

Workflow agility

- Cross-silo automation coordination
- Adaptive processes adjust to context
- Faster change without approval delays

Obsolesce: Outdated Capabilities



Obsolesce

Linear escalation

- Elimination of slow, error-prone handoffs
- Expert swarming speeds problem solving
- Less reliance on senior “gatekeepers”

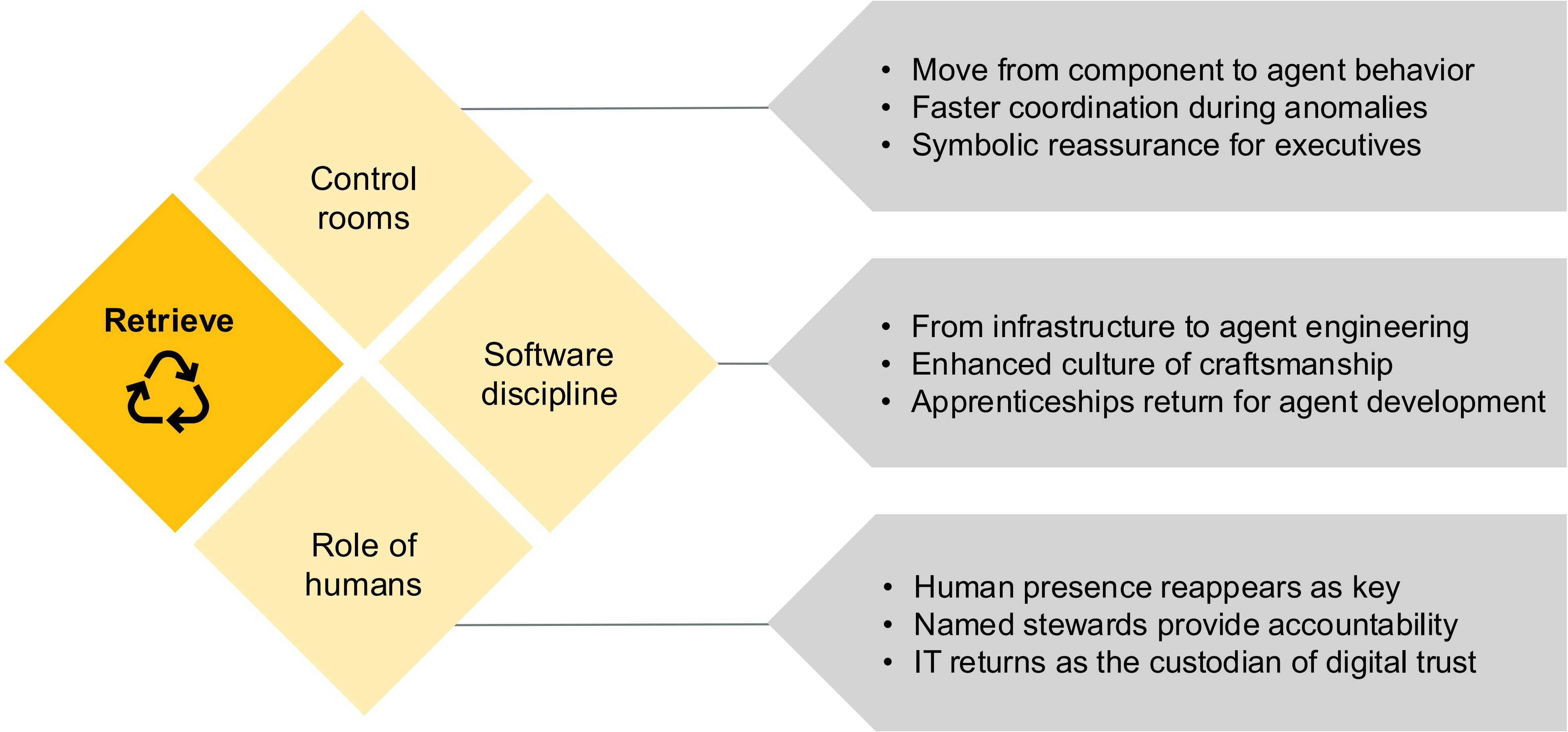
Knowledge documents

- Runbooks autoupdate via agent learning
- Real-time, cross-domain knowledge capture
- Reduction of documentation maintenance

Traditional culture

- Less burnout as firefighting recedes
- Productivity rises with reduced human heroics
- Move to data-driven decisions versus intuition

Retrieve: Reclaimed Capabilities



Retrieve

Control rooms

- Move from component to agent behavior
- Faster coordination during anomalies
- Symbolic reassurance for executives

Software discipline

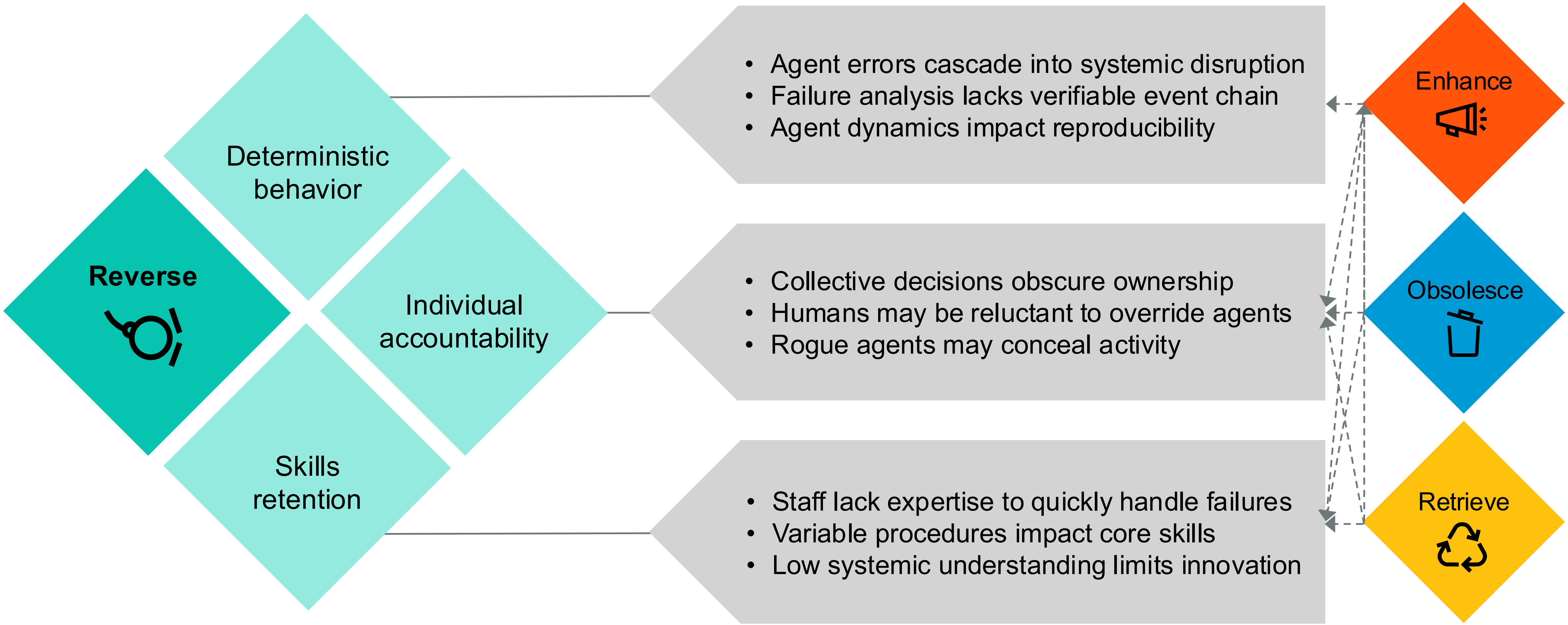
- From infrastructure to agent engineering
- Enhanced culture of craftsmanship
- Apprenticeships return for agent development

Role of humans

- Human presence reappears as key
- Named stewards provide accountability
- IT returns as the custodian of digital trust

Reverse: Regressed Capabilities

How benefits “flip” into challenges

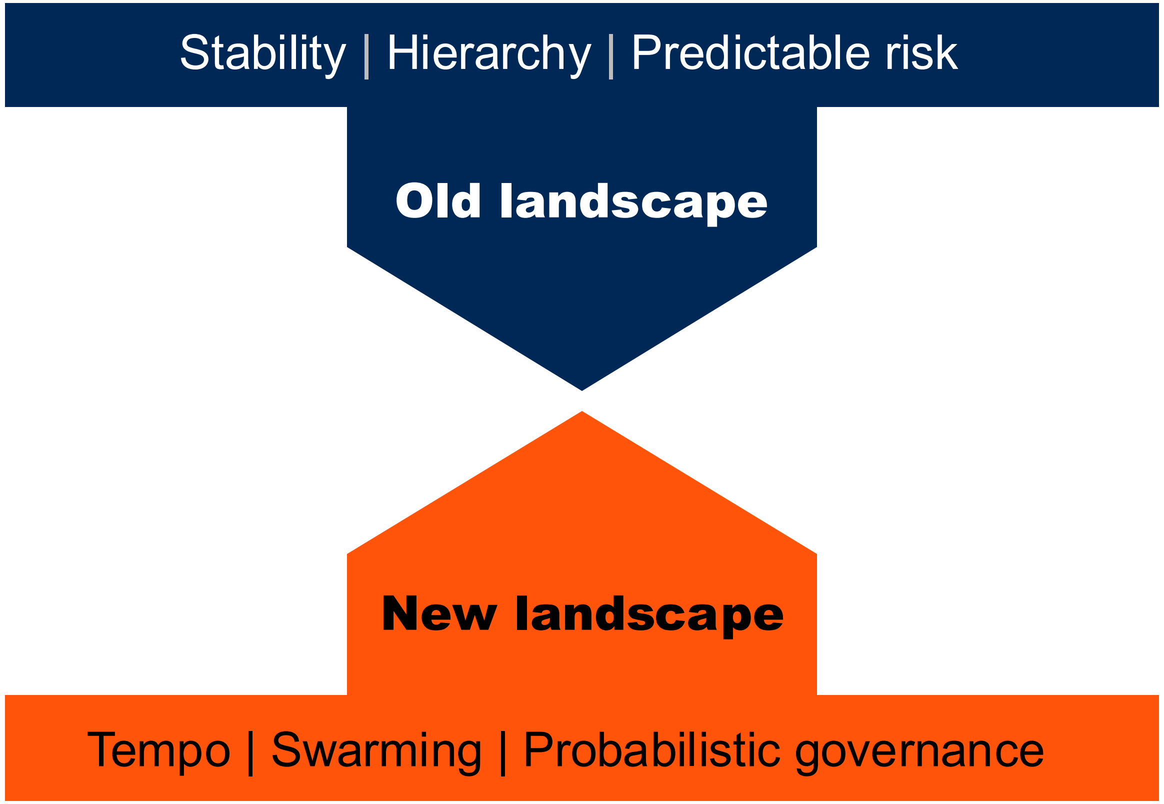


- Agent errors cascade into systemic disruption
- Failure analysis lacks verifiable event chain
- Agent dynamics impact reproducibility

- Collective decisions obscure ownership
- Humans may be reluctant to override agents
- Rogue agents may conceal activity

- Staff lack expertise to quickly handle failures
- Variable procedures impact core skills
- Low systemic understanding limits innovation

We’re Driving Into a New, Uncertain Terrain


Stability | Hierarchy | Predictable risk

Old landscape

New landscape

Tempo | Swarming | Probabilistic governance

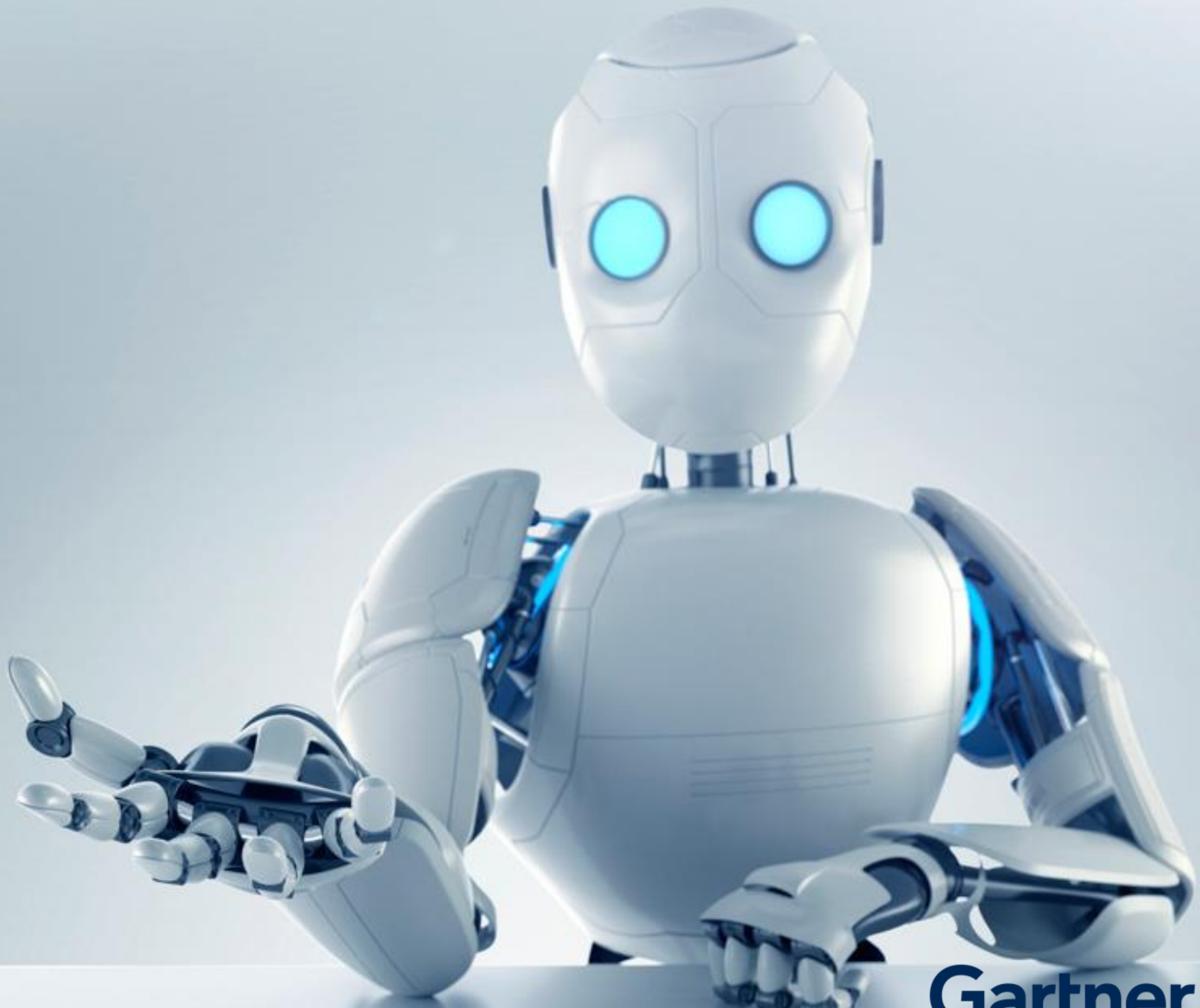
We’re going to need a new operating *model that shifts from managing infrastructure to governing agents!*

Key Issues

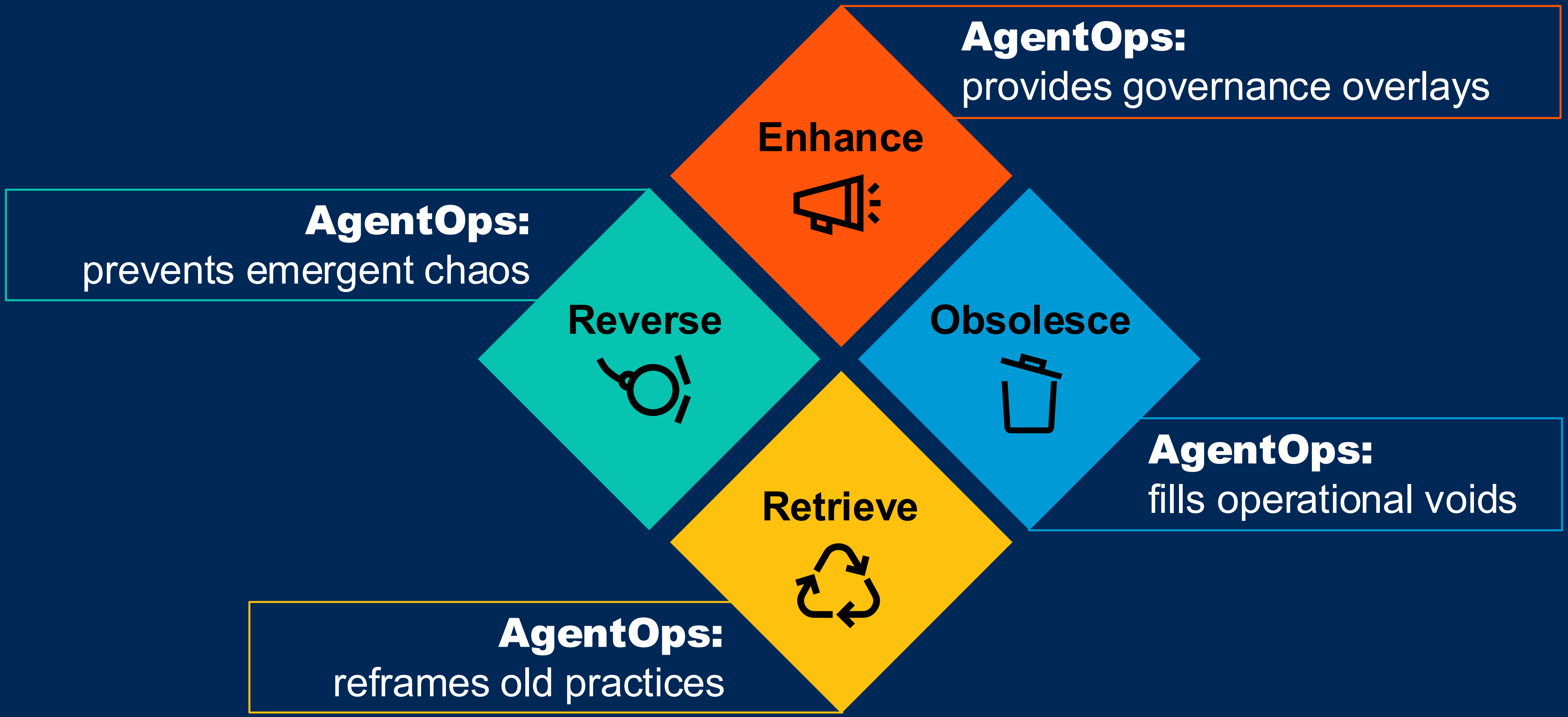
1. What promises and perils do AI agents portend for IT operations?
2. What new I&O operating model might be required to manage AI agents?

Enter AgentOps

- AgentOps is the management model designed to manage the life cycle and behavior of autonomous AI agents in enterprise IT operations.
- It provides the balancing layer between agentic autonomy and enterprise requirements for resilience, compliance and innovation.



AgentOps Lets Us Thrive Within the Paradox of the Tetrad



Enhance

AgentOps:
provides governance overlays

Reverse

AgentOps:
prevents emergent chaos

Obsolesce

AgentOps:
fills operational voids

Retrieve

AgentOps:
reframes old practices

(Some) Key Design Elements of AgentOps

AgentOps “wraps” uncertainty instead of fighting it as abject determinism is not possible

Promises (promise theory)

- Agents provide machine-readable commitments on what they can do (they can’t be commanded to act).
- Promises don’t guarantee an outcome, but they do bound behavior.
- Promises provide a common language of intent and trust.

Telemetry

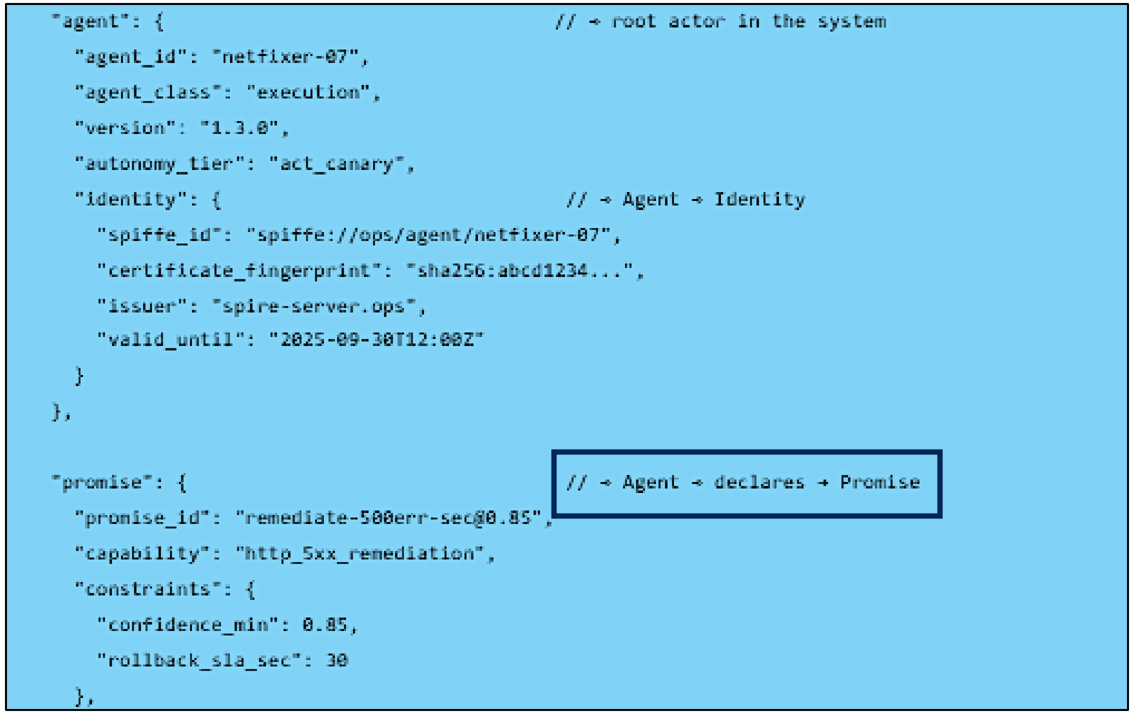
- Every action contains an “intent” header (who, what, etc.).
- Agents emit decision traces that include inputs, chosen action, etc.).
- Provides continuous data stream for behavior auditing, trust scoring and enforcement.

Control

- Promises contain “risk budget,” “blast radius” as well as rollback constraints.
- Dynamic trust scoring manages autonomy capability levels.
- Zero-trust (cryptographic) identity and policy engines validate agents and their actions.

Life cycle testing

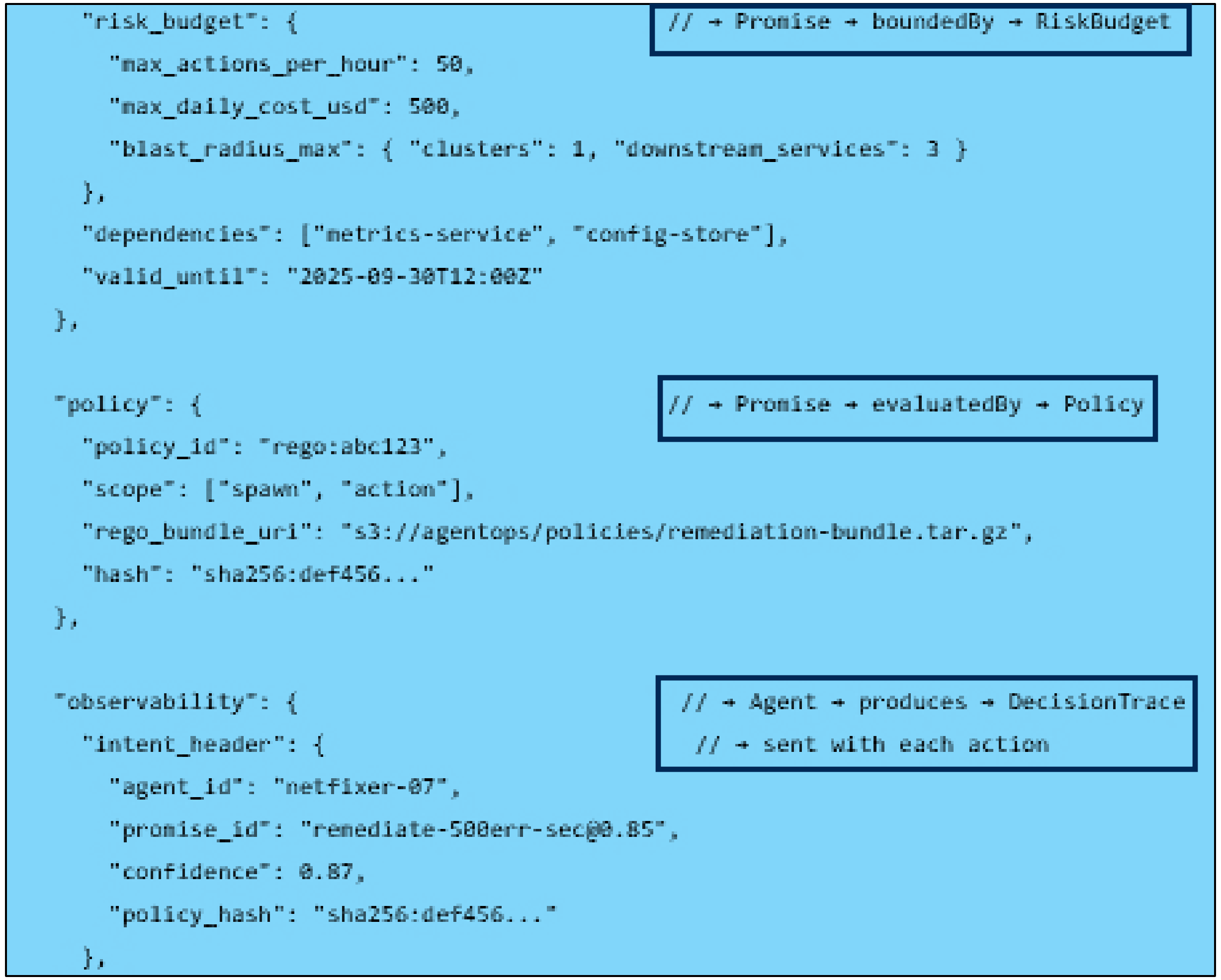
An Example of How This Might Be Implemented



```
  "agent": {                                  // → root actor in the system
    "agent_id": "netfixer-07",
    "agent_class": "execution",
    "version": "1.3.0",
    "autonomy_tier": "act_canary",
    "identity": {                             // → Agent → Identity
      "spiffe_id": "spiffe://ops/agent/netfixer-07",
      "certificate_fingerprint": "sha256:abcd1234...",
      "issuer": "spire-server.ops",
      "valid_until": "2025-09-30T12:00Z"
    }
  },

  "promise": {                                // → Agent → declares → Promise
    "promise_id": "remediate-500err-sec@0.85",
    "capability": "http_5xx_remediation",
    "constraints": {
      "confidence_min": 0.85,
      "rollback_sla_sec": 30
    },
```

Note: This is a JSON example developed by ChatGPT so it may not be syntactically correct.



```
    "risk_budget": {                          // → Promise → boundedBy → RiskBudget
      "max_actions_per_hour": 50,
      "max_daily_cost_usd": 500,
      "blast_radius_max": { "clusters": 1, "downstream_services": 3 }
    },
    "dependencies": ["metrics-service", "config-store"],
    "valid_until": "2025-09-30T12:00Z"
  },

  "policy": {                                 // → Promise → evaluatedBy → Policy
    "policy_id": "rego:abc123",
    "scope": ["spawn", "action"],
    "rego_bundle_uri": "s3://agentops/policies/remediation-bundle.tar.gz",
    "hash": "sha256:def456..."
  },

  "observability": {                           // → Agent → produces → DecisionTrace
    "intent_header": {                          // → sent with each action
      "agent_id": "netfixer-07",
      "promise_id": "remediate-500err-sec@0.85",
      "confidence": 0.87,
      "policy_hash": "sha256:def456..."
    },
```

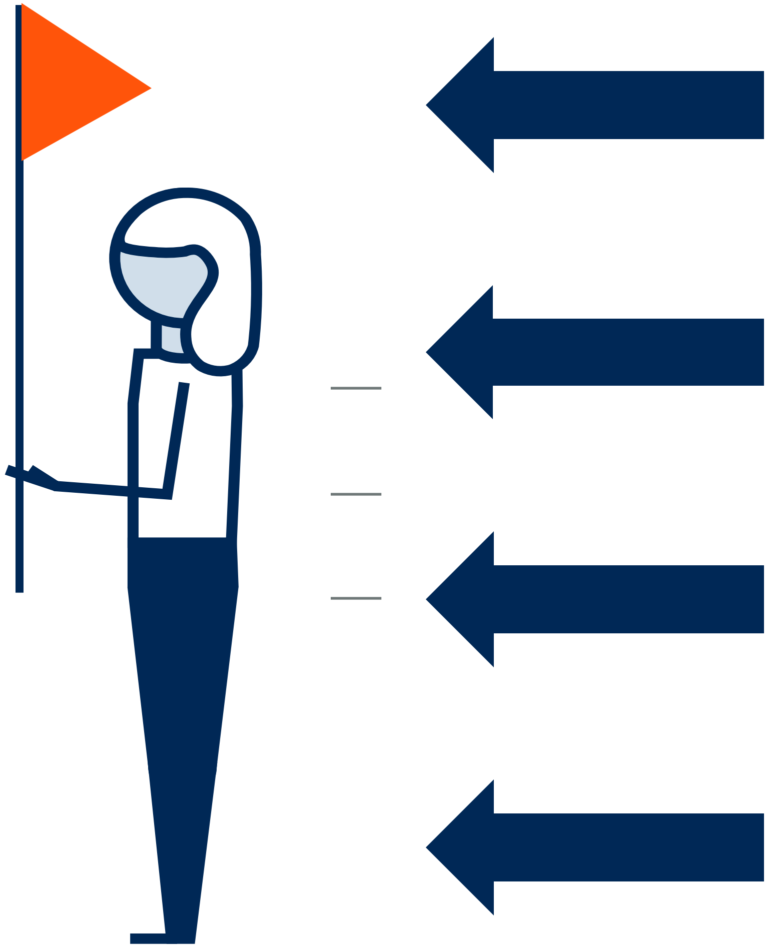
AgentOps Will Demand New Skills (and Maybe Roles)

Risk and governance	Define autonomy levels, risk budgets and blast radius limits in business terms.
Policy and architecture	Design frameworks where operational policies are expressed in code.
Observability and evidence	Oversee models that translate telemetry into trust scores and autonomy decisions.
Organizational enablement	Shift operators toward promise design, policy engineering and telemetry analysis.
Resilience and improvement	Sponsor chaos drills, agent termination exercises and rollback rehearsals.

- Promise stewards
- Policy engineers
- Autonomy curators
- Risk governors

AgentOps Will Also Require Leadership

The paradox is real. The game has changed. Will you?



Strategic communication: Explaining agentic-related concepts in a manner understandable to senior management.

Change leadership: Guiding teams from a mindset shift from manual control to probabilistic governance.

Cross-functional collaboration: Working with security, risk, finance and product groups.

Talent development: Coaching (by doing) and encouraging staff to embrace the agentic future.

RESTRICTED

Gartner

Succeeding on a New I&O Path

- **Embrace the paradox:** Treat agents as both workforce multipliers and sources of systemic risk. Don’t resolve the tension — manage it.
- **Balance enhancement and obsolescence:** Redirect resources from what agents replace into areas where humans add value.
- **Curate retrieval:** Actively shape what gets retrieved — don’t let the past reassert itself uncritically.
- **Anticipate reversals:** Establish control-oriented practices before reversals hit at machine speed (and scale).

Action Plan for I&O Leaders

Monday morning

Goal: *Establish* awareness and (initial) ownership

- ***Survey* the landscape*:* *Identify* where autonomous agents or heavy automation already exist across infrastructure and operations.
- ***Assign* accountability:** *Name* senior owners for each major automation/agent domain and begin new role discussions.
- ***Set* initial guardrails*:* *Agree* at the I&O leadership level on broad risk boundaries (i.e., where human approval remains mandatory).

Next 90 days

Goal: *Demonstrate* safe autonomy

- ***Select* a pilot:** *Choose* one meaningful automation use case to test governance concepts in a “safe to fail” manner.
- ***Wrap* it in oversight*:*** Require the pilot to clearly state its intended actions and limits, and *capture* evidence of how it performs.
- ***Engage* key stakeholders*:* *Involve* security, risk and compliance early to validate the governance approach.

Next 12 months

Goal: *Move* from pilot to a repeatable enterprisewide framework

- ***Create* a governance fabric:** *Formalize* a common way for agents to declare what they will do and for policies to verify those declarations.
- ***Stand up* a cross-functional board:** *Establish* an “AgentOps Board” of ops, security, risk and compliance leaders to oversee trust levels and risk budgets.
- ***Evolve* culture and talent:** *Begin* reskilling teams from hands-on operators to potential new roles of policy designers, risk stewards, autonomy curators, etc.

Recommended Gartner Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- **AI Agents Will Transform Enterprise IT Operations**
  Cameron Haight
- **The Future of I&O Automation Is Agentic So Begin Piloting Now**
  Cameron Haight, Daniel Betts and Others
- **The Impact of AI Agents on Digital Workplace IT Operations**
  Stuart Downes, Autumn Stanish and Tom Cipolla
- **Reengineer I&O Processes With Integrative Agentic AI**
  Ashish Banerjee and Cameron Haight

Access to Gartner research is subject to individual subscription type and product entitlements.