



## AI Control Suite

# Market Evidence for Run time Enforcement

**Document type:** Investor Briefing

**Date:** April 2026

**Confidentiality:** Company Confidential

## Table of Contents

|                                                                  |          |
|------------------------------------------------------------------|----------|
| <b>Executive Summary .....</b>                                   | <b>3</b> |
| <b>1. Operational Costs of Governance Issues .....</b>           | <b>3</b> |
| <b>2. Costs of Bespoke Solutions vs. Rapid Enforcement .....</b> | <b>3</b> |
| <b>3. Opportunity Cost of Delayed Deployment .....</b>           | <b>4</b> |
| <b>4. Data Source Verification.....</b>                          | <b>5</b> |

## Executive Summary

Quantifying the impact of runtime policy enforcement for AI agents involves analyzing direct financial losses from breaches, the overhead of building bespoke governance, and the often-overlooked opportunity cost of stalled innovation.

Research from 2025 and 2026 indicates that while AI automation can reduce breach costs, the **lack of runtime governance** (often referred to as "Shadow AI" or ungoverned agentic behavior) acts as a significant cost amplifier.

### 1. Operational Costs of Governance Issues

Governance failures in AI agents lead to specific operational "penalties." According to the **IBM Cost of a Data Breach Report 2025**, the absence of governance creates a measurable financial burden:

- **Shadow AI Surcharge:** Organizations with high levels of "Shadow AI" (ungoverned AI tools/agents) saw an additional **\$670,000** in average breach costs compared to those with proper oversight.
- **The Access Control Gap:** A staggering **97% of organizations** that suffered an AI-related security incident lacked proper AI access controls.
- **Detection Delay:** Ungoverned AI breaches have a longer lifecycle (averaging **247 days**), which is 6 days longer than the global average, increasing the window of exposure and data exfiltration.

### 2. Costs of Bespoke Solutions vs. Rapid Enforcement

The market is shifting from multi-year "bespoke" digital transformations to modular, real-time enforcement.

- **The \$1.3bn Benchmark:** Historical "bespoke" transformations, such as the **New Zealand Inland Revenue's \$1.3bn (NZD)** digital overhaul, serve as a cautionary tale of the scale required when "people, platform, process, and policy" are built from scratch.
- **Modern Bespoke AI Costs:** In 2024/2025, bespoke AI builds for specific global functions (legal/marketing) have been reported to cost tens of millions, though they can deliver massive ROI (e.g., **\$250m annual savings**).

- **Enforcement Savings:** Conversely, using standardized AI security and automation can save an organization **\$1.9 million to \$2.2 million** per breach by shortening the identification and containment time by up to **100 days**.

### 3. Opportunity Cost of Delayed Deployment

The primary "hidden" cost of missing runtime policy enforcement is the inability to move agents from pilot to production.

- **Release Delays:** 2026 research from **Salt Security** indicates that **47% of organizations** have delayed production releases of AI agents specifically due to security and policy concerns.
- **Market Stagnation:** While the **AI-driven Policy and Governance market** is expected to reach **\$3.75 billion by 2026** (CAGR of 39.6%), the delay in deployment means firms are missing out on the 20-30% productivity gains associated with agentic workflows.
- **Restrictive Prohibitions:** Approximately **27% of organizations** have chosen to completely ban Generative AI applications rather than risk deployment without controls, sacrificing all potential competitive advantages.

### 4. Costs of Policy Breaches

When policy is breached—whether through data exfiltration or unauthorized external communication—the costs are high:

- **Regulatory Penalties:** In the US, breach costs surged to **\$10.22 million** in 2025, driven largely by stricter regulatory fines for compliance failures.
- **The "Automation Paradox":** Automation without governance redistributes risk. While it handles volume, it introduces "blind spots." Organizations with no AI governance policies (**63% of breached firms**) face higher escalation costs because they lack the "deterministic functions" required to halt a violating path at runtime.

## 5. Data Source Verification

The following sources were used to compile this data (verified current as of 2025-2026):

1. **IBM Cost of a Data Breach Report 2025** (Accessed via Baker Donelson/DataFence): Provides specific figures on the **\$670k Shadow AI surcharge** and the **97% lack of access controls** in AI breaches.
  - <https://www.datafence.ai/data-breach-report-2025>
2. **The 2025 AI Index Report | Stanford HAI**: Details the sharp rise in AI-related incidents and the gap between recognizing risks and taking action.
  - <https://hai.stanford.edu/ai-index/2025-ai-index-report>
3. **Salt Security Research (2026)**: Documents that **47% of organizations** delay AI agent production due to security concerns.
  - <https://www.einpresswire.com/article/904519615/salt-security-research-as-ai-agents-outpace-security-most-organizations-face-an-unsecured-api-surge>