AI EXECUTION CONTROL

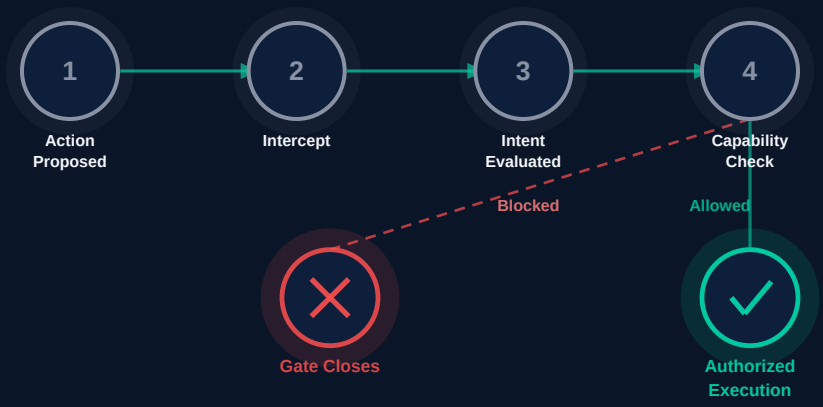
Control Agentic AI Execution at Machine Speed

Stop Reacting. Start Preventing.

Breakthru Technologies™ delivers execution-level enforcement that stops unauthorized AI actions before they occur, not after damage is done.

Pre-Execution Gate

Every AI and system action is intercepted before execution. Intent is evaluated against cryptographically enforced invariants. If the action is not authorized, the capability never materializes.



Data Protection Layer

Data, invariants, and capabilities are deconstructed and reconstructed in real time. Exfiltrated fragments are cryptographically unusable without authorized reconstruction blueprints.

HOW IT WORKS

Four steps from action to outcome.

1 — Action Proposed
An AI agent, automation, or system proposes an action — API call, file operation, model output, kernel transition, or autonomous behavior.

2 — Intercept
The solution intercepts the proposed action before it reaches the execution layer — before any syscall, tool invocation, or state change occurs.

3 — Intent Evaluated
The purpose of the action is evaluated against cryptographically defined invariants — the set of allowed behaviors for the system or agent.

4 — Capability Check
A capability object must be reconstructible for the action to proceed. If invariants are not satisfied, the capability cannot be reconstructed.

× — Gate Closes
If the required conditions are not satisfied, the execution gate remains closed. The capability never materializes. The action does not occur.

✓ — Authorized Execution
If conditions are satisfied, the capability materializes and execution proceeds — with a full, immutable audit trail.

A PARADIGM SHIFT

TRADITIONAL SECURITY	→	AI EXECUTION CONTROL
Detect after execution	→	Control before execution
Alert humans to respond	→	Enforce allowed outcomes automatically
Respond to damage after it occurs	→	Prevent damage from occurring
Guard prompts or data inputs	→	Govern what execution is allowed
Flag unauthorized behavior	→	Unauthorized actions are impossible
Encryption key at risk	→	Stateless, ephemeral key generation — nothing to intercept

USE CASES

Two scenarios. Both prevent damage.

Use Case 1 — AI & System Execution Control

AI agents and automation can act faster than humans can intervene. Breakthru controls what they are allowed to do — before they do it.

- → Agentic AI overreach and unauthorized API or tool invocation
- → Guardrail bypass, prompt injection, and hallucinated execution paths
- → Unauthorized system-state modification beyond defined scope
- → Autonomous model output exceeding allowed operational constraints

Use Case 2 — Data Protection & Ransomware / Quantum Resilience

Ransomware, breaches, and HNDL attacks depend on executing unauthorized operations or making stolen data usable. Breakthru eliminates both vectors.

- → Ransomware file enumeration and mass encryption blocked at execution
- → Exfiltrated data rendered cryptographically unusable — no usable keys
- → Harvest-now-decrypt-later quantum attacks defeated by stateless keys
- → Unauthorized cryptographic operations blocked before they execute

THE CHALLENGE

Classic 'Detect & Respond' solutions assume damage is inevitable. It isn't.

THE DETECT & RESPOND GAP

- Tools alert after execution — breach or ransomware event has already occurred
- AI agents act faster than human security teams can intervene
- Mean time to detect: 194 days avg; breach cost: $4.9M avg
- Prompt injection and hallucinated actions create uncontrolled execution paths
- Rogue AI behavior and unauthorized API calls are not detectable before execution
- Quantum-era adversaries harvest encrypted data today and decrypt it later

THE EXECUTION-CONTROL SHIFT

- Unauthorized actions blocked before execution — no damage, no remediation cost
- Cryptographic gating ensures unauthorized AI actions cannot execute
- Mean time to prevent replaces detect — risk eliminated at execution boundary
- Unauthorized actions are impossible — intent enforcement at execution layer
- Physics based data protection renders exfiltrated fragments cryptographically unusable
- Post-quantum architecture protects against both current and future adversaries

CORE DIFFERENTIATORS

Six capabilities that define a new security architecture.

Pre-Execution Control

Intercepts AI and system actions before syscalls, API calls, tool invocations, kernel transitions, model outputs, or autonomous actions. Unauthorized actions do not execute.

Cryptographic Execution Gating

Rules, policies, and constraints are collapsed into cryptographic invariants. Each action requires a reconstructible capability object. If it cannot be reconstructed, the action cannot be expressed.

Intent-Layer Enforcement

Evaluates the purpose of each action against defined invariants before execution — making unauthorized actions structurally unrepresentable rather than merely detected after the fact.

Physics-Based Data Protection

Data, invariants, and capabilities are locked with a physics-based protection model: scrambling, encryption, blueprints, replication, distribution, integrity checks, and zeroization after use.

Ransomware & Breach Resilience

Ransomware processes attempting file enumeration or encryption are intercepted at the execution boundary. Exfiltrated fragments cannot be reconstructed without authorized conditions.

Lightweight Inline Deployment

A lightweight inline control layer. No changes to AI models or applications. No rip-and-replace. Works alongside your current security stack — on-premises, cloud, or hybrid — from day one.

STANDARDS & FRAMEWORKS

Built for regulated industries and government-grade compliance.

FedRAMP High and NIST AI RMF compliance on active roadmap.

INDUSTRIES SERVED

Pre-execution control for every environment where AI can act faster than humans.

Financial Services

Prevent unauthorized AI-driven trading actions, API abuse, and data exfiltration. Enforce execution boundaries across automated systems and model pipelines with full audit trails.

Healthcare & Life Sciences

Protect patient data, AI-assisted diagnostics, and clinical automation from unauthorized access and rogue execution. Enforce HIPAA-aligned access controls at the execution layer.

Defense & Government

Enforce execution-level controls on AI systems, autonomous platforms, and classified data operations. FedRAMP High authorization in process. Built for environments where unauthorized execution is not acceptable.

Critical Infrastructure

Control what operational technology, AI monitoring systems, and automation can execute across energy, water, and transportation networks. Prevent ransomware and adversarial AI from reaching physical systems.

Ready to control AI at machine speed?

Schedule a briefing with a Breakthru specialist to see AI execution control in action.

info@breakthrutech.ai
www.breakthrutech.ai