AI Enablement

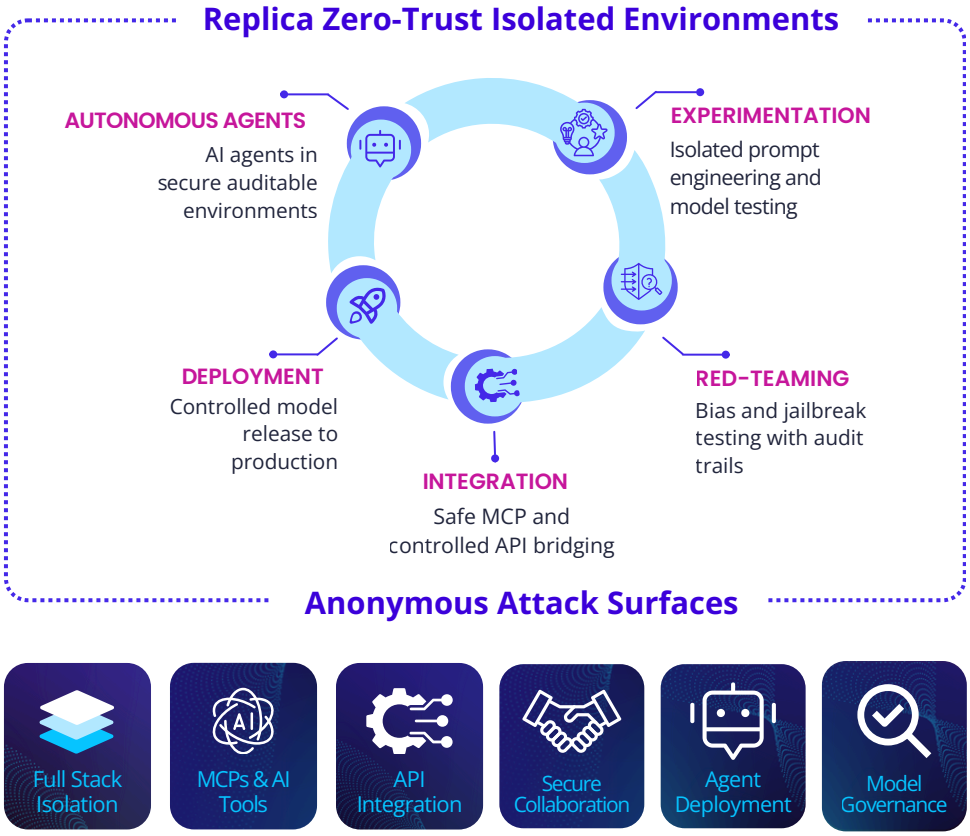
Replica Isolated Environments

Instant. Secure. Frictionless

Secure AI Innovation & Experimentation

Organizations are racing to explore the potential of LLMs, AI agents, and new frameworks like the Model Context Protocol (MCP) for tool integration. From prompt engineering and fine-tuning to RAG pipeline development and production deployments, success comes when teams have the freedom to experiment, the ability to tap any tool or dataset, and the confidence that every step is protected and compliant.

Replica makes that possible by delivering secure, fully isolated AI workspaces where even risky integrations like MCP can be explored safely, without compromising trust. Every phase of the AI lifecycle, from idea to deployment, takes place in an environment built for safe experimentation, seamless integration, and confident release—helping teams deliver breakthrough AI capabilities with complete oversight and enterprise-grade protection.



Business Challenge

Accelerating AI Innovation with Confidence

AI teams face intense pressure to refine prompts, test capabilities, and adopt standards like MCP at speed. Success depends on connecting to any dataset or API, refining ideas, and executing on demand. Conventional security and IT wasn't built for this pace. Forward-looking teams need an approach that sustains AI velocity while keeping every action secure, governed, and compliant.

Current State Limitations:

- Risky experimentation with proprietary data in uncontrolled environments
- Unvetted AI agents operating inside core infrastructure without oversight
- Data exposure when connecting internal systems to external AI APIs
- Unmonitored MCP tool execution creating new data exfiltration paths
- Compliance gaps from ungoverned model training and prompt engineering

Replica Isolated Environments

The Solution

Replica gives AI teams secure, fully isolated environments built to accelerate innovation while protecting data, models, and infrastructure. Key AI workflows—from early experimentation through secure integration, safe MCP execution, and agent oversight—take place inside controlled workspaces that preserve security, ensure compliance, and maintain auditable oversight.

Key Benefits

Secure AI Experimentation
Isolated MCP execution with no data leakage

Governed Red-Teaming
Safe testing with audit trails.

Safe Data Bridging
Secure internal to API connections.

Controlled AI Agents
Autonomous agents with complete logging.

With controlled network access and built-in governance, teams can use their preferred tools, connect to any dataset or API, and safely explore new capabilities with full oversight.

Accelerating AI Innovation

With Replica, teams driving AI initiatives can explore, test, and refine LLMs and agents under tight governance with safe data bridging and audit trails—confidently moving ideas forward without risking core systems. We help you say "yes" to your most ambitious AI experiments while keeping your business protected.

The Replica Advantage

Isolated AI Workspaces

Instantly create secure, independent environments for AI experimentation, integration, and deployment—protecting data, models, and infrastructure from exposure.

Seamless Tool & Data Access

Connect to approved datasets, APIs, and AI services while using preferred tools, enabling rapid experimentation without delays or constraints.

Secure Collaboration

Share environments across teams for joint model development, testing, and evaluation while maintaining control, visibility, and governance throughout the process.

AI Audit & Compliance

Capture a complete record of training runs, prompt interactions, and deployments to ensure integrity, meet compliance requirements, and streamline reporting.

Built by Former Intelligence Professionals
Replica was born from decades of cyber counterintelligence experience. Every capability is rooted in operational tradecraft proven in the most sensitive missions.