Defending Against ARTEX & Agentic Offensive Frameworks

The CSA Third Wave controls, and how Netzilo delivers them

A guide for security leaders responding to the FBI ARTEX alert — CISOs, SOC managers, and the architects who will put the CSA controls in place.

Attackers now send agents to do the work.

ARTEX is an open-source framework in which AI agents run an intrusion on their own: they find what an organization exposes, try it, and keep going. The FBI warns that multiple threat actors have used it since August 2026 against financial, government, technology, defense and healthcare organizations. Four days after the FBI alert, more than 800 CISOs met in an emergency Cloud Security Alliance briefing.

⚠ UNDER 3 HOURS TO PRIVILEGED ACCESS

What an Agentic Offensive Framework (AOF) does once it picks your organization, as reported by the FBI and the CSA's CISO community:

1. Maps everything you expose: partner portals, legacy apps, MCP servers and AI gateways
2. Finds a credential left in the open and uses it at once
3. Turns your own agents against you with injected instructions and poisoned tool results
4. Moves laterally to privileged access, and returns within hours if cleanup is partial

HUMAN APPROVAL	PARTIAL CLEANUP	NETZILO
Arrives after the attacker is already in.	Re-compromised within hours.	**Decoys, guardrails and containment at machine speed.**

1 WHAT CSA SAYS TO START THIS WEEK

Three controls, one platform.

SHRINK

Lock down the entry points of your most critical apps.

Netzilo makes them private behind zero trust access, or publishes them behind sign-in, group admission and posture checks.

SECURE

Put agents into your security work, and secure them.

Netzilo governs every agent where it runs (device, SDK, browser, AI Gateway) with tool grants, guardrails and a full record.

DECEIVE

Plant decoys where an AOF will look.

Deploy a decoy adds lookalikes with synthetic keys beside every published app, MCP server and AI gateway. One touch blocks the attacker tenant-wide.

Speed is the gap. Netzilo closes it.

2 THE CONTROLS NETZILO DELIVERS

10 of the 20 CSA controls, delivered directly.

#	CSA CONTROL	START	HOW NETZILO DELIVERS IT
2	**Plant decoys; route activations first**	THIS WEEK	Lookalike apps, MCP servers and AI gateways with synthetic cloud and AI keys. One touch blocks the address tenant-wide and is reported.
3	**Lock down entry points of critical apps**	THIS WEEK	Private apps over zero trust access, or published behind sign-in, group admission and posture checks.
5	**Secure your own agents**	THIS WEEK	One engine on devices, in the SDK, the browser and the AI Gateway: model and tool grants, guardrails, behavior graph and kill chains.
7	**Monitor AI spend and token use**	THIS MONTH	AI Usage per user, agent and model. Limits cap spend, tokens and requests per hour, day, week, month or year.
8	**Pre-authorize containment**	THIS MONTH	Response Actions isolate AI activity by session, agent, user, group, device or account: under 1 s on devices, about 2 s at gateways.
11	**Contain transitive trust**	THIS MONTH	Vendors, MSPs and CI pipelines get scoped, posture-checked access. Removing one group cuts it.
12	**Close endpoint gaps**	THIS MONTH	Covers what EDR cannot see: agents' prompts, tool calls, MCP use and the processes, files and connections they start. Hosts without running EDR are blocked.
14	**Cyber-capable models with a fallback**	THIS QUARTER	One gateway for frontier and self-hosted open-weight models (Ollama, vLLM, SGLang), with failover on errors and timeouts.
15	**Boundaries and deny-by-default egress**	THIS QUARTER	Least-privilege policies down to subnet and port; micro-segmentation between peers.
20	**Detect and block attacks at runtime**	THIS QUARTER	Inline guardrails and multi-step kill chains over agent tool calls, processes, files and connections.

Netzilo also contributes to the other 10 controls, such as AI-first alert triage and complete remediation. A full mapping is available on request.

3 YOUR FIRST WEEK

A practical start, one day at a time.

DAY 1 01

Publish your three most critical apps and turn on **Deploy a decoy**.

Controls 2, 3

DAY 2 02

Move AI provider keys into the AI Gateway and set spend, token and request limits.

Controls 7, 14

DAY 3 03

Bring coding, desktop and custom agents under Netzilo and turn on guardrails.

Controls 5, 12, 20

DAY 4 04

Agree which Response Actions the team may take without sign-off, and at what scope.

Control 8

DAY 5 05

Give every vendor, MSP and CI pipeline its own group and least-privilege policies.

Controls 11, 15

ARTEX is already scanning perimeters.

Human-approved response cannot keep up. Put pre-approved, machine-speed defense in place this week.

Get Started → www.netzilo.com

Sources: Cloud Security Alliance, The Third Wave: ARTEX and Agentic Offensive Frameworks, Nov 25, 2026 · BleepingComputer, FBI warns ARTEX AI hacking tool is powering global cyberattacks, Nov 15, 2026