SALT

SOLUTION BRIEF • COMPETITIVE ANALYSIS

Salt Security vs. Akto

Akto pivoted from API testing to AI agent security in 2025, building a platform around endpoint hooks and per-server MCP guardrails. Salt Security secures the downstream enterprise APIs and full API fabric that Akto's endpoint model cannot reach.

CATEGORY	PLATFORMS COMPARED	YEAR
Agentic Security	Salt Security & Akto	2026

OVERVIEW

Endpoint-level security misses where enterprise API attacks land

Akto started as an open-source API testing platform and pivoted to AI agent security in 2025. Its architecture deploys endpoint hooks into MCP clients, proxies between MCP clients and servers, and runs automated red teaming. Guardrails are activated per MCP server via YAML configuration — giving teams control at the tool invocation level, but no visibility into the downstream enterprise APIs where those tools execute.

Salt Security covers the layer below and beyond Akto's endpoint model: the enterprise APIs, business logic, and downstream services where agents execute real-world actions. The Agentic Security Graph maps and correlates the full environment as a unified fabric — no per-server activation, no hooks to deploy, no endpoints to register.

0

Per-server guardrail activations required. Salt governs the full fabric without per-server YAML configuration.

8

Years of production API security research. Akto pivoted to AI agent security in 2025.

0

Endpoint hooks required. Salt covers the downstream API fabric without deploying hooks at MCP clients.

PLATFORM APPROACHES

Endpoint hooks and per-server guardrails vs. fabric-wide API security.

SALT SECURITY

Fabric-wide coverage without per-server configuration

Salt Security covers the action layer that Akto's endpoint model stops before: the enterprise APIs, business logic, and downstream services where agents execute real-world actions at scale. The Agentic Security Graph maps and correlates LLM connections, MCP servers, APIs, identities, and sensitive data as a unified fabric.

No per-server activation. No YAML configuration rules per server. No endpoint hooks to deploy. Salt's coverage applies uniformly across the full agentic environment — external exposure, cloud infrastructure, code repositories, and runtime — from day one.

AKTO

Endpoint hooks and per-server MCP guardrails

Akto deploys endpoint hooks into MCP clients and proxies between clients and servers. Guardrails are activated per MCP server through YAML rule configuration, and automated red teaming runs 1,000+ attack probes against configured targets. Coverage is scoped to the endpoints and servers that security teams have explicitly configured.

The constraint: Akto's protection is as broad as the YAML configuration covering it. MCP servers not yet added to the configuration are unprotected. And the downstream enterprise APIs that agents call through those MCP servers — where business logic abuse actually occurs at scale — are outside Akto's scope entirely.

THE COVERAGE GAP

Akto controls what happens at configured endpoint and tool invocation points. Salt monitors what happens to your enterprise APIs when those tools execute downstream. Business logic abuse at enterprise scale does not happen at the MCP endpoint — it happens in the APIs the endpoint calls, the data those APIs touch, and the behavioral sequences that accumulate across dozens of individually authorized tool invocations.

CAPABILITY COMPARISON

Salt Security vs. Akto: side by side

CAPABILITY	SALT SECURITY	COMPETITOR
Unified Agentic Discovery	**STRONG** Discovers APIs, MCP servers, and AI-driven assets across external exposure, cloud, code repositories, and runtime as a unified environment.	**PARTIAL** Akto discovers MCP servers and agents within configured hook and proxy paths. APIs and assets outside configured coverage are not discovered.
Agentic Security Graph	**STRONG** Correlates LLMs, MCP servers, APIs, identities, and sensitive data in one action-layer context — the only platform with this cross-fabric view.	**NOT AVAILABLE** Akto has no Agentic Security Graph equivalent. Cross-fabric correlation of LLM, MCP, API, and identity in a unified model is not available.
Salt Code Governance	**STRONG** Governs API and MCP creation in repositories and developer workflows before risky logic ships to production.	**PARTIAL** Akto provides pre-production API testing capabilities from its testing heritage. Repository-level API and MCP governance is not a primary current capability.
Runtime-to-Code Remediation	**STRONG** Feeds runtime findings back into DevOps workflows and AI coding assistants to fix root causes — closing the loop between detection and fix.	**NOT AVAILABLE** Akto does not feed runtime findings back into DevOps workflows or AI coding assistants.
Identity-Aware Sequence Correlation	**STRONG** Tracks unique agentic identities and multi-step intent across sessions, tools, and services to detect campaigns, not just individual events.	**NOT AVAILABLE** Akto monitors at the endpoint and tool invocation level. Identity-aware multi-step sequence correlation across downstream API sessions and services is not available.
Behavioral Action-Layer Protection	**STRONG** Detects machine-speed business logic abuse beyond signatures, schemas, or known patterns.	**PARTIAL** Akto runs automated red teaming against configured targets. Runtime behavioral detection in downstream enterprise APIs after tool invocation is outside scope.
Internal & East-West Coverage	**STRONG** Protects internal APIs and downstream service interactions that edge-only and model-only tools miss entirely.	**NOT AVAILABLE** Akto's hooks and proxies operate at MCP client and server boundaries. East-west internal API traffic triggered by agent actions in downstream systems is not covered.
Action-Layer Data Security	**STRONG** Maps sensitive data in motion across APIs, MCP servers, and agent actions across the full fabric.	**NOT AVAILABLE** Akto monitors at the hook and proxy level. Sensitive data in motion

CAPABILITY	SALT SECURITY	COMPETITOR
		across downstream enterprise APIs and the full fabric is not mapped.
Beyond Endpoint Hooks and MCP Proxies	**STRONG** Salt secures downstream enterprise APIs and business logic across the full fabric — not only the local hook, shield, or proxy activity at individual MCP configurations.	**ENDPOINT ONLY** Akto's coverage is scoped to configured endpoint hooks and MCP proxies. Downstream enterprise APIs and business logic are outside scope.
Business-Logic Protection for Downstream APIs	**STRONG** Salt detects abuse in the enterprise APIs behind the agent — not only prompt, tool, or endpoint policy violations at the guardrail layer.	**NOT AVAILABLE** Akto's guardrails operate at the tool invocation level. Business logic abuse in downstream enterprise APIs after permitted invocations is not detected.
No Per-Server Guardrail Activation Required	**STRONG** Salt applies governance as a unified platform capability across the full fabric — without requiring teams to select, configure, and activate each MCP server individually.	**REQUIRES PER-SERVER SETUP** Akto requires individual MCP server selection and YAML guardrail configuration. Servers not yet configured are unprotected, and the operational burden scales with your MCP footprint.

Questions to ask in your evaluation

The most productive evaluation question is not which platform has more features, but which platform covers the layer where your risk is highest. Use these scenarios to drive the conversation.

If you need coverage of downstream enterprise APIs

Ask Akto to demonstrate visibility into the enterprise API calls that your agents make through MCP tool invocations. Show them a specific business process your agents execute and ask what Akto shows you about the downstream APIs involved. If those APIs are outside the configured hook and proxy paths, Akto cannot see them. Salt covers that layer from day one.

If per-server configuration overhead is a concern

Akto requires each MCP server to be individually configured with YAML guardrail rules. In environments with dozens or hundreds of MCP servers — particularly where developers are creating new integrations rapidly — this per-server overhead becomes a significant operational burden. Ask Akto how many servers your security team would need to configure and maintain. Salt has no equivalent per-server activation requirement.

If business logic abuse through authorized tool calls is a threat

An agent can call every configured Akto-protected MCP endpoint with fully authorized requests, and those calls can still orchestrate data exfiltration, unauthorized data access, or privilege escalation through the downstream APIs. Salt's behavioral correlation across the full API sequence — not just the tool invocation — detects these patterns. Akto's endpoint model cannot.

If you are considering Akto for MCP endpoint governance and Salt for API security

These platforms are complementary, not substitutes. Akto's endpoint-level red teaming and tool invocation governance addresses one layer. Salt's action-layer security covers the broader API fabric that those tools operate within. The more urgent coverage gap for most organizations is the downstream API layer that Akto does not reach.

S U M M A R Y

Key differentiators

S A L T S E C U R I T Y I S T H E S T R O N G E R C H O I C E W H E N …

- Downstream enterprise API and business logic protection is a requirement
- No per-server MCP guardrail activation overhead is acceptable at scale
- Agentic Security Graph correlation across the full LLM, MCP, and API fabric is needed
- East-west and internal API coverage beyond endpoint hooks is required
- Behavioral attack detection across multi-step API sequences is a priority
- Fabric-wide governance without endpoint hook deployment is needed
- Eight years of production API security research behind behavioral models matters

A K T O M A Y B E C O N S I D E R E D W H E N …

Akto may be considered in a specific and narrow scope:

- Automated red teaming against specific, already-identified MCP server configurations is needed and downstream API coverage is out of scope
- Endpoint-level guardrails at a known, bounded set of MCP invocation points is the specific requirement

For any organization concerned about what agents do to their enterprise APIs after tool invocations, Akto's endpoint scope will not cover the primary risk surface.

T H E C O M B I N E D P I C T U R E

Endpoint-level agent security and enterprise API security address different attack surfaces. Akto's endpoint hooks and per-server guardrails provide control at tool invocation points. Salt secures the downstream enterprise API fabric where the business logic, data access, and real-world consequences of those invocations occur. In agentic environments, the downstream API layer is where attacks at enterprise scale are executed.

S E E T H E A C T I O N L A Y E R F O R Y O U R S E L F

Salt Surface can show you the full external exposure of your agentic environment — including every API your agents call through MCP tool invocations — with zero deployment and no per-server configuration required. **Request a demo at salt.security**