SOLUTION BRIEF • COMPETITIVE ANALYSIS

# Salt Security vs. Onyx Security

Onyx Security governs AI agents before they act. Salt Security secures the APIs, MCP servers, and downstream infrastructure where those actions execute. Governing the agent does not protect the environment it operates in.

| CATEGORY | PLATFORMS COMPARED | YEAR |
| --- | --- | --- |
| Agentic Security | Salt Security & Onyx Security | 2026 |

## OVERVIEW

### The risk lives downstream from where Onyx Security governs

Launched in March 2026, Onyx Security positions its Guardian Agent as a supervisory control plane that intercepts agent actions before they reach downstream systems. That is valuable governance — but by their own description, Onyx's coverage stops before anything reaches a downstream system. Salt Security was built to protect exactly those downstream systems: the APIs, MCP servers, and data infrastructure where agents execute real-world actions.

Salt Security brings eight years of production API security research to the agentic layer. The Agentic Security Graph maps and correlates every LLM connection, MCP server, API endpoint, identity, and data flow across code, cloud, and runtime — covering the full attack surface that Onyx's control plane stops before reaching.

**8**

Years of production API security research vs. Onyx Security's March 2026 launch.

**0**

Inline MCP gateways required. Salt protects the action layer without adding proxy dependencies.

**0**

Downstream API blind spots. Salt covers what agents do after every Onyx-permitted action.

PLATFORM APPROACHES

# AI control plane governance vs. action-layer security — different problems.

SALT SECURITY

## Action-layer security built on eight years of API expertise

Salt Security was built from the ground up as a security platform for the layer where agents execute: the APIs, MCP servers, and downstream services that agents interact with when they take real-world actions. The Agentic Security Graph maps and correlates the full environment out-of-band — no inline gateway, no proxy dependency.

Salt Surface discovers external exposure. Salt Collect monitors runtime traffic across 70+ infrastructure technologies. Salt Code governs pre-production. Eight years of production API security research means Salt's behavioral models understand how agentic attacks actually unfold — not just how they look to a supervisory agent deciding whether to permit a single request.

ONYX SECURITY

## AI agent governance and control plane

Onyx Security's Guardian Agent supervises agent behavior at the orchestration layer, intercepting actions before they reach downstream systems. It discovers agents, enforces governance policies, and can block or redirect unsafe actions in real time. Natural language policy controls aim to make governance accessible to non-technical stakeholders.

The constraint Onyx acknowledges in their own description: coverage intercepts "before anything reaches a downstream system." The downstream system — the API fabric, the east-west traffic, the data infrastructure — is where Salt operates. Onyx's control plane stops at the boundary that Salt's coverage starts from.

THE COVERAGE GAP

Onyx Security governs what agents are permitted to do. Salt Security detects what agents actually do to your enterprise API fabric — including everything that happens in downstream systems after an Onyx-permitted action executes. An agent that passes every Onyx governance check can still exfiltrate data through an API, escalate privileges through an MCP server, or execute unauthorized multi-step workflows across your infrastructure.

CAPABILITY COMPARISON

# Salt Security vs. Onyx Security: side by side

| CAPABILITY | SALT SECURITY | COMPETITOR |
|---|---|---|
| **Unified Agentic Discovery** | **STRONG**<br>Discovers APIs, MCP servers, and AI-driven assets across external exposure, cloud, code repositories, and runtime as a unified environment. | **PARTIAL**<br>Onyx discovers AI agents across SaaS, cloud, and endpoint environments. API fabric discovery across all infrastructure is not a primary capability. |
| **Agentic Security Graph** | **STRONG**<br>Correlates LLMs, MCP servers, APIs, identities, and sensitive data in one action-layer context — the only platform with this cross-fabric view. | **NOT AVAILABLE**<br>Onyx has no Agentic Security Graph. Cross-fabric correlation of LLM, MCP, API, and identity in a unified model is not available. |
| **Salt Code Governance** | **STRONG**<br>Governs API and MCP creation in repositories and developer workflows before risky logic ships to production. | **NOT AVAILABLE**<br>Onyx does not govern API and MCP creation in developer repositories pre-production. |
| **Runtime-to-Code Remediation** | **STRONG**<br>Feeds runtime findings back into DevOps workflows and AI coding assistants to fix root causes — closing the loop between detection and fix. | **NOT AVAILABLE**<br>Onyx does not feed runtime findings back into developer workflows or coding assistants. |
| **Identity-Aware Sequence Correlation** | **STRONG**<br>Tracks unique agentic identities and multi-step intent across sessions, tools, and services to detect campaigns, not just individual events. | **NOT AVAILABLE**<br>Onyx monitors agent behavior at the orchestration layer. Identity-aware sequence correlation across downstream API calls is not available. |
| **Behavioral Action-Layer Protection** | **STRONG**<br>Detects machine-speed business logic abuse beyond signatures, schemas, or known patterns. | **PARTIAL**<br>Onyx intercepts agent actions at the governance layer. Behavioral detection in downstream enterprise APIs after permitted actions execute is outside scope. |
| **Internal & East-West Coverage** | **STRONG**<br>Protects internal APIs and downstream service interactions that edge-only and model-only tools miss entirely. | **NOT AVAILABLE**<br>Onyx governs agents at the orchestration layer. East-west internal API traffic triggered by agent actions in downstream systems is not monitored. |
| **Action-Layer Data Security** | **STRONG**<br>Maps sensitive data in motion across APIs, MCP servers, and agent actions across the full fabric. | **PARTIAL**<br>Onyx monitors data access at the agent interaction layer. Sensitive data in motion across the downstream API fabric is not mapped. |

| CAPABILITY | SALT SECURITY | COMPETITOR |
| --- | --- | --- |
| **No Inline MCP Gateway Required** | **STRONG**<br>Salt delivers full agentic protection without proxying MCP traffic through an inline gateway — no latency, no proxy dependency, no developer workflow friction. | **REQUIRES INLINE GATEWAY**<br>Onyx's MCP coverage requires routing MCP traffic through an inline gateway, adding latency and creating a proxy dependency for agent-to-MCP connections. |
| **More Than an AI Control Plane** | **STRONG**<br>Salt secures the APIs where agents take action — not only AI observability, governance, orchestration, and ROI measurement at the control plane layer. | **CONTROL PLANE ONLY**<br>Onyx's platform operates at the AI governance and orchestration layer. Security of the downstream APIs and infrastructure where agents execute is outside current scope. |
| **Downstream API Business Logic Protection** | **STRONG**<br>Salt detects abuse in the enterprise APIs behind the agent — including attacks that pass every governance check because each individual action is authorized. | **NOT AVAILABLE**<br>Onyx governs agents before they act. Detecting business logic abuse in downstream APIs after permitted actions execute is outside the control plane scope. |

## 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 to protect the APIs agents act on

Ask Onyx to demonstrate visibility into the downstream API calls an agent makes after a permitted action executes. Show a specific API endpoint your agents call and ask what Onyx shows you about runtime traffic to that endpoint. If they cannot show runtime API traffic, you are looking at a governance tool, not a security platform. Salt covers that layer.

### If you are evaluating a newly launched platform

Onyx Security launched in March 2026. Enterprise security buyers rightfully apply scrutiny to first-generation products on critical infrastructure. Salt's eight years of production deployments at scale represent a level of enterprise credibility that a platform months old cannot match. In agentic security — a novel attack surface — that research foundation matters.

### If business logic abuse is a concern

Business logic attacks using AI agents look like authorized behavior at every governance checkpoint. An agent that is fully compliant with every Onyx policy can still orchestrate data exfiltration, privilege escalation, or unauthorized workflow execution through individually permitted API calls. Salt's behavioral correlation at the API layer detects these attack patterns. Onyx's control plane cannot.

### If you are considering Onyx alongside Salt

Onyx and Salt are not substitutes — they operate at different layers. Onyx governs agent behavior at the orchestration layer. Salt secures the infrastructure those agents act on. Organizations that deploy both get governance at the model layer and security at the action layer. The question for your evaluation is which gap is more urgent — and for most organizations with deployed agents, the action-layer gap is where immediate risk lives.

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 API and action-layer security is a requirement
- No inline MCP gateway or proxy dependencies are acceptable
- Multi-step behavioral attack detection in downstream infrastructure is needed
- East-west and internal API coverage is required
- Eight years of enterprise production API security credibility matters
- Agentic Security Graph correlation across the full fabric is needed
- Runtime-to-code remediation to fix vulnerabilities at the source is required

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

*Onyx Security addresses a specific and narrow governance use case:*

- Pre-execution agent governance and policy enforcement at the AI orchestration layer is the primary requirement with no downstream API security needs
- Natural language policy controls for non-technical governance stakeholders are specifically required and no action-layer security is in scope

*For any organization concerned about what agents do to their API infrastructure after governance checks pass, Onyx's coverage ends at the boundary where the risk begins.*

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

AI agent governance and agentic security protect different surfaces. Onyx governs what agents are permitted to do. Salt secures what they actually do to your infrastructure. A mature agentic security program needs both layers — but the action-layer coverage that Salt provides is the one with the most immediate risk exposure, because authorized agents can still cause significant damage through the APIs they legitimately call.

### 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 infrastructure today, and Salt Collect can show you what your agents are doing at the API layer — including the downstream actions that occur after every Onyx-governed permission check. **Request a demo at salt.security**

SALT