

## SOLUTION BRIEF | AUTONOMOUS DEFENSE

# Salt Autonomous Defense

Detection is not resolution. Turn Salt's agentic and API intelligence into blocked attacks, revoked access, and remediated risk.

## CATEGORY

Agentic security

## CAPABILITY

Salt Workflows

## PLATFORM

Salt Agentic Security Platform

## OVERVIEW

**Security cannot move at ticket speed when attackers move at machine speed**

Security teams have spent years improving detection. But when a risky agent, a vulnerable API, or an active attack is found, response still depends on manual handoffs and changes across disconnected systems. As AI accelerates the discovery and exploitation of weaknesses, that delay becomes a security risk of its own.

Autonomous Defense closes the gap. Built on an expansion of Salt Workflows, it lets Salt trigger defensive controls automatically to block malicious activity, revoke risky access, and start remediation across the systems customers already use. Tickets, SIEM enrichment, notifications, and audit logging remain available, but they are no longer the end state.

**49.8%**

of organizations confirmed or suspect an AI agent took an action they did not intend, expect, or authorize in the past year.

Salt Security, 2H 2026 State of Agentic AI and API Security

**12.5%**

can consistently trace an agent's full path from the initial prompt through the MCP servers and APIs it reached.

Salt Security, 2H 2026 State of Agentic AI and API Security

## CONTROL

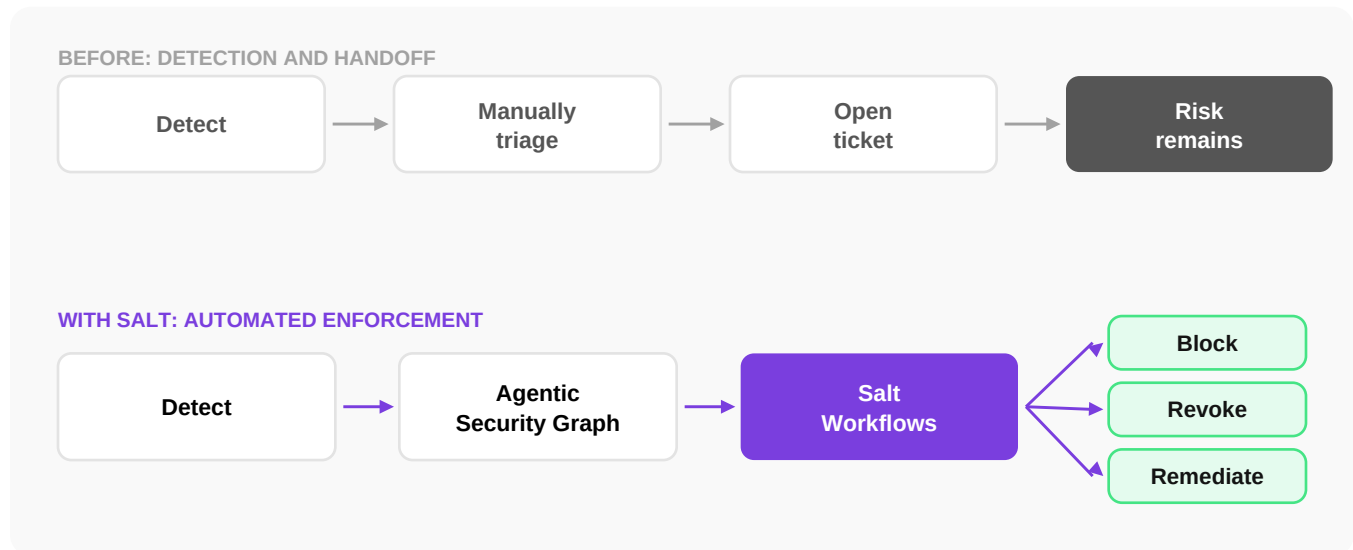
**Autonomous when appropriate. Controlled when required.**

Customers decide which findings trigger immediate action, which changes require approval, and which enforcement points are used. Security teams respond at machine speed while keeping control of sensitive operations and a full audit trail.

## THE APPROACH

# From detection to defense in one operational loop

The Agentic Security Graph connects AI agents, MCP servers, tools, and downstream APIs with context from exposure, source code, configuration, and runtime behavior. That intelligence identifies dangerous paths and informs the policy driven actions each customer chooses to enforce. Salt Workflows then carries the decision out through connected controls.



Illustrative workflow. Actions depend on customer policies and connected enforcement capabilities.

## WHAT IT DOES

# Four ways Salt acts on what it finds

1

### Revoke risky agent and MCP tool access

Disable unauthorized MCP connections, quarantine shadow tools, or remove excessive privileges through supported management controls.

2

### Block active exploitation

Push targeted blocking rules or virtual protections to existing WAFs, API gateways, and other enforcement points.

3

### Enforce AI and data protections

Update supported guardrail policies, block unsafe requests, or redact sensitive data through connected gateways.

4

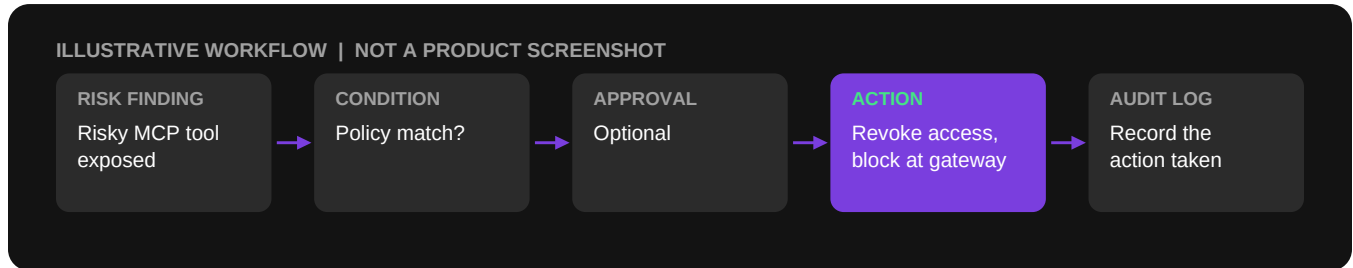
### Remediate posture gaps

Trigger configuration changes to close exposed APIs, reinstate rate limits, or restore approved security settings.

## BUILT IN

# Flexible automation inside the platform

Salt has embedded a visual, drag and drop workflow builder directly in the Agentic Security Platform. With 200+ out of the box connectors and a marketplace of Salt built integrations, customers design enforcement, governance, and remediation workflows across security, infrastructure, IT, and collaboration systems without complex custom development.



Integrations available today include Jira, ServiceNow, Slack, Microsoft Teams, CrowdStrike, Azure DevOps, Wiz, Apigee, and WAFs, with more added over time. Workflows runs on Salt's own cloud infrastructure, so customer data stays within Salt's environment.

## WHY SALT IS DIFFERENT

| DIMENSION                | TYPICAL APPROACH                      | SALT AUTONOMOUS DEFENSE                                          |
|--------------------------|---------------------------------------|------------------------------------------------------------------|
| Where response starts    | An alert, then a ticket and a handoff | A policy driven action tied to the finding                       |
| Context for the decision | One layer: model, gateway, or edge    | One graph from agent to MCP server, tool, API, and data          |
| Enforcement points       | Tied to one vendor's controls         | The WAFs, gateways, and IT tools already in place                |
| Human control            | All manual, or all automatic          | Customer defined: act now, or require approval, with audit trail |

## AVAILABLE NOW

### Salt Workflows is available to Salt customers today.

Salt is migrating existing workflows to the new experience, with support for customer specific requirements. See a risk finding trigger a block, a revoke, and a remediation in your own environment.

[Book a demo](#)
[salt.security/demo-request](https://salt.security/demo-request)

Capabilities depend on customer policies and the enforcement controls connected. Press release scheduled for October 27, 2026.