

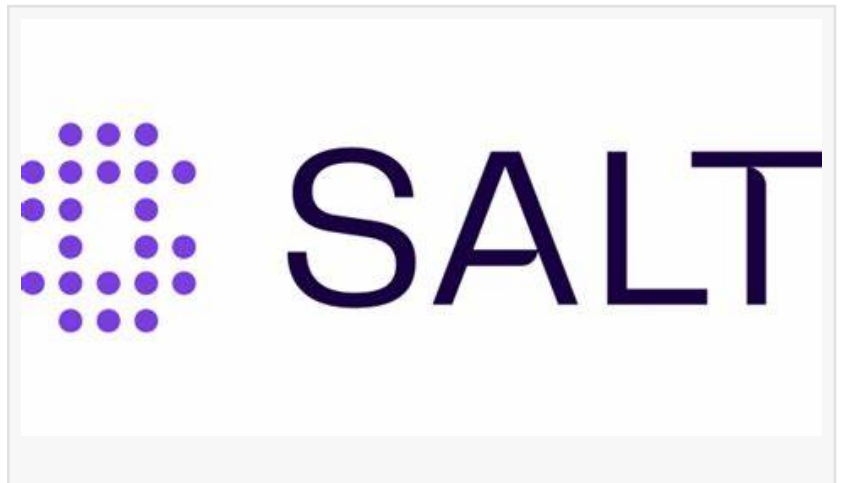
Salt Security Debuts First AWS WAF Managed Ruleset for AI Agent and API Protection

Announced at Black Hat USA 2026, Salt's new managed ruleset extends AWS WAF with purpose-built protection against API abuse and AI agent-driven threats.

LONDON, UNITED KINGDOM, August 4, 2026 /EINPresswire.com/ -- [Salt Security](#), the leader in Agentic and API Security, today announced the availability of Salt Managed Rules for AWS WAF in AWS Marketplace.

Delivered through the AWS WAF

Partner Managed Rules program, it is the first managed ruleset purpose-built to secure both APIs and the AI agents that drive them. AWS WAF customers can attach it to existing web ACLs directly from the AWS console and be protected in minutes, with no proxies, no traffic redirection, and no new infrastructure to operate.



“

By bringing Salt's API and agentic security intelligence directly into an AWS WAF as managed rules, we're giving every AWS customer an easy way to deploy these new rules in minutes.”

Roey Eliyahu, CEO and Co-founder of Salt Security

At Black Hat USA 2026, visitors to Salt Security's booth #5938 can request an Agentic Attack Assessment with Salt Labs researchers, see the Agentic Security Graph in action, and get a first look at the new AWS WAF managed ruleset.

APIs now power nearly every digital experience, and AI agents are rapidly becoming the fastest-growing source of API traffic. Traditional WAF rules were never designed to understand the behavioural nuances of APIs or the dynamic nature of AI-powered agents, leaving security

teams with blind spots that existing tools do not cover. The recent [Hugging Face](#) incident illustrates exactly how that gap is being exploited. Salt's managed ruleset closes those gaps inside the AWS WAF deployments customers already run.

The Salt Managed Rules deliver:

- Advanced API threat detection, blocking common and complex attack vectors including

credential brute force, excessive GraphQL queries, SSRF, prototype pollution, and JWT-based anomalies.

- Industry-first [Model Context Protocol](#) (MCP) awareness, identifying and labelling traffic from MCP endpoints, blocking unauthenticated MCP access, and providing deeper observability into MCP interactions in AWS WAF environments.
- Context-aware rate limiting, with smart limits on sensitive parameters such as user IDs and email addresses to stop enumeration and abuse patterns.
- Security signal enrichment, labelling critical request attributes (auth headers, user identifiers, GraphQL queries) to boost detection fidelity and downstream analytics.

"AI agents are transforming how applications are built, and APIs are the layer where those agents act," said Roey Eliyahu, CEO and Co-founder of Salt Security. "By bringing Salt's API and agentic security intelligence directly into an AWS WAF as managed rules, we're giving every AWS customer an easy way to deploy these new rules in minutes, so organizations can immediately see and stop the API and AI agent threats that legacy rules were never built to catch."

Availability

Salt Managed Rules for AWS WAF — AI Agent & API Security is available now in the AWS Marketplace across all commercial AWS Regions and globally via Amazon CloudFront. Existing AWS WAF customers can subscribe and attach the ruleset to their web ACLs directly from the AWS console. Learn more at the AWS Marketplace listing. A step-by-step deployment walkthrough is available [here](#).

About Salt Security

Salt Security is the leading Agentic and API Security company, protecting the world's most innovative enterprises from AI agent and API attacks. The Salt Security Agentic Security Platform secures the full agentic ecosystem, discovering all agents, MCP connections, and APIs, stopping attacks in real time, and eliminating vulnerabilities before they reach production. Salt Security was founded in 2016 and is backed by Sequoia Capital, S Capital, Tenaya Capital, Salesforce Ventures, Advent International, and other leading investors. For more information, visit salt.security.

Charley Nash
Eskenzi PR
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/931634041>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.