Salt Security Brings MCP Threat Protection to AWS WAF, Blocking AI Agent Abuse in Real Time

LAS VEGAS, NV, UNITED STATES, December 3, 2025 /EINPresswire.com/ -- Salt Security, the leader in API security, today announced it is extending its patented, award-winning API behavioural threat protection to detect and block malicious intent targeting Model Context Protocol (MCP) servers deployed within the AWS ecosystem. Building on the recent launch of Salt's MCP Finder technology, Salt now enables organisations to identify external misuse and abuse of MCP servers by AI agents and attackers, and automatically block these threats using its integration with AWS WAF.

MCP servers have rapidly become a key component of enterprise AI architecture, enabling LLMs and autonomous agents to call APIs, execute tools, and complete workflows. But they also represent a new threat vector. Deployed without central oversight and often exposed to the internet, MCP servers are increasingly targeted by adversaries for unauthorised access to critical data and system access.
With this new capability, Salt enables customers to use their existing AWS WAF deployments to block attacks on MCP infrastructure. The protections are informed by real-time behavioural threat data from Salt's platform.

"Most organisations don't even know how many MCP servers they have, let alone which ones are exposed or being abused," said Nick Rago, VP of Product Strategy at Salt Security. "This capability lets them take action quickly, using existing controls to prevent real threats without needing to deploy new infrastructure."

The solution is based on Salt's MCP Finder technology, which provides full visibility into the MCP layer across external, internal, and shadow deployments. By combining that discovery with AWS WAF, customers can:

• Automatically block MCP misuse and abuse before it impacts applications
• Discover previously unknown or unmanaged MCP implementations and ensure traffic is routed through AWS WAF for inspection and protection
• Extend AWS WAF edge protection to the AI action layer
• Apply intent-based behavioural threat detection to stop attacks targeting key AI infrastructure that traditional tools miss
• Continuously update protections based on evolving attacker tactics

Salt Security is showcasing these capabilities at AWS re:Invent 2025. The integration is available now as part of the Salt Security API Protection Platform.

About Salt Security
Salt Security secures the APIs that power today's digital businesses. Salt delivers the fastest API discovery in the industry—surfacing shadow, zombie, and unknown APIs before attackers find them. The company's posture governance engine and centralised Policy Hub automate security checks and enforce safe API development at scale. With built-in rules and customisable policies, Salt makes it easy to stay ahead of compliance and reduce API risk. Salt also uses machine learning and AI to detect threats early, giving companies a critical advantage against today's sophisticated API attacks. The world's leading organizations trust Salt to find API gaps fast, shut down risks, and keep their businesses moving. Learn more at https://salt.security.

Media Contact -
Dr. Karl Bateson - karlb@salt.security

Charley Nash
Account Manager
charley@eskenzipr.com
Visit us on social media:
LinkedIn
