Salt Security Expands 'Universal Visibility' with API Security for Databricks and Edge Support for Netlify

LONDON, UNITED KINGDOM, January 22, 2026 /EINPresswire.com/ -- New capabilities extend Salt's discovery engine into the Agentic AI Action Layer and modern composable web architectures, providing the only dedicated API security visibility for Databricks agentic workloads.

Salt Security, the leader in API security and AI governance, today announced a major expansion of its platform's connectivity fabric with two new strategic integrations: the Salt Databricks Connector and the Salt Netlify Collector. These additions reinforce Salt's "Universal Visibility" strategy, ensuring that security teams can capture deep API context from every corner of the enterprise, whether it's a legacy on-premise server, a modern edge deployment, or the rapidly evolving Agentic AI Action Layer.

Securing the Agentic AI Action Layer at the Source. As enterprises rush to build Agentic AI, platforms like Databricks have become the operating system for AI workloads. While generalist security tools (CNAPPs) can scan Databricks infrastructure for misconfigurations, they remain blind to the actual behaviour of the AI agents running inside.

The new Salt Databricks Connector bridges this gap, providing a dedicated API security discovery engine for Databricks environments. It specifically targets the "Agentic Action Layer," identifying the Model Context Protocol (MCP) servers and AI agents that connect proprietary data models to the outside world.

• Ease of Use: Connects in minutes without complex instrumentation or manual configuration.
• Action-Layer Visibility: Instantly maps which APIs and data sources internal AI agents are accessing—visibility that infrastructure scanners miss.
• Unified Governance: Allows teams to apply the same rigorous security policies to their AI workloads as they do to their traditional APIs.

"Databricks is where the enterprise brain lives, but until now, we have not been able to see what the hands, the AI agents, are actually touching," said Eric Schwake, Cybersecurity Director at Salt Security. "Generalist tools can tell you if your S3 bucket is open, but only Salt can tell you if an AI agent inside Databricks is actively leaking PII through an unmonitored API. We are turning the lights on in the agentic action layer."

Rapid Support for the Modern Edge. Alongside AI visibility, Salt is addressing the fragmentation of modern web architectures. The new Salt Netlify Collector brings feature-parity traffic collection to decoupled frontend applications and Jamstack architectures.

Built to support major enterprise deployments, this collector demonstrates Salt's agility and ability to rapidly build and deploy collectors as the market evolves. As organisations decouple their frontends and push logic to the edge, standard gateways are often bypassed. Salt ensures security travels with the code.

• Universal Reach: Extends Salt's best-in-class traffic analysis to Netlify's edge network.
• Rapid Adaptation: Showcases Salt's flexible architecture, allowing the platform to support modern Content Delivery Networks (CDNs) and edge runtimes as fast as developers adopt them.

Availability: The Salt Databricks Connector and Netlify Collector are available immediately as part of the Salt Illuminate™ 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 organisations trust Salt to find API gaps fast, shut down risks, and keep their businesses moving. Learn more at https://salt.security

Contact
Charley Nash
Account Manager, Eskenzi PR
charley@eskenzipr.com

Charley Nash
Eskenzi PR
charley@eskenzipr.com
