# Salt Security Delivers First AI-Infused API Security Platform to Address Proliferation of GenAI Application Development

Salt's LLM, Pepper, has now been extended to the continuous API discovery and posture assurance steps in the API Security lifecycle

LONDON, UNITED KINGDOM, May 7, 2024 /EINPresswire.com/ -- Salt Security, the leading API security company, today announced the debut of its AI-infused API Security Protection Platform powered by Pepper, the company's Large Language Model (LLM) artificial intelligence. The launch of the platform marks the next generation of API security, leveraging AI throughout every aspect of the API lifecycle, to streamline and bolster API discovery, posture assurance, and threat detection, to mitigate risks faster.
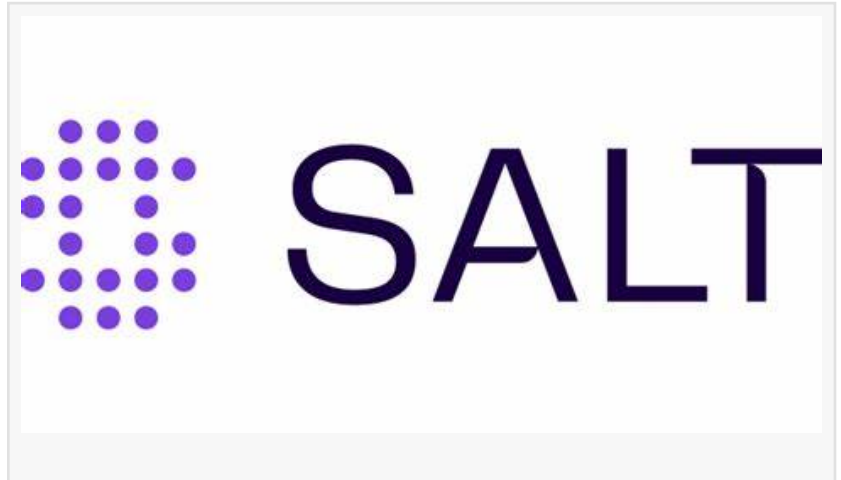
> "
> Leveraging generative AI for good, we have instilled our own LLM, Pepper, into our platform to help organizations solve the complex problems which generative AI creates."
> *Michael Nicosia, COO and co-founder, Salt Security*

Generative AI has enabled developers to create applications and APIs faster than ever before and at a vast scale. With the speed of API creation dramatically increasing, new risks are created that current technology is not equipped to keep pace with.

According to Gartner®, "The soaring prevalence of APIs, along with the lack of organizational awareness as to their extent, has created an expansive attack surface just waiting to be exploited by malicious actors*."

"Our business depends on securely and quickly delivering finance-related APIs for our partners and customers as we provide banking as a service," said Nuno Teodoro, Vice President, Group Cybersecurity. "With the GenAI landscape evolving at a fast pace, especially targeting, directly or indirectly, software development of critical products, we must lean on core capabilities from our technological partners, especially where API security is

considered. Salt's AI-infused API security platform is a perfect example of supporting the delivery of secure APIs that adhere to our policies and best practices, thus giving us the confidence that cyber resilience is incorporated into the APIs security life-cycle."

Leveraging generative AI, Salt's platform protects organizations from the risks associated with the speed and scale of new application development. As APIs are the nucleus of current and future applications, with the launch of Salt's new platform, the company is uniquely positioned to deliver the next phase of application security.

With the latest expansion to its offering, the Salt platform now delivers:
Enhanced API Continuous Discovery: At the outset, Salt Security's AI engine excels in the discovery phase by acting as an exhaustive investigator across the application landscape. It leverages machine learning to automatically detect all APIs, including those that are undocumented or embedded within microservices, ensuring comprehensive visibility over the network, leaving no API hidden and vulnerable. This level of comprehensive discovery is unparalleled in the industry, ensuring that no API remains unnoticed or vulnerable. While APIs are continuously created at speed by GenAI, the Salt Platform continually analyzes the API ecosystem to ensure the inventory is up to date.

API Posture Assurance: Moving to the next phase, Salt Security employs its AI-driven Posture Governance to monitor and analyze API configurations proactively. This AI system is adept at identifying deviations from security best practices and highlighting insecure configurations. By maintaining continuous surveillance, Salt Security aids organizations in upholding a robust API security posture, thus preventing potential breaches.

Robust API Behavioral Threat Protection: In the crucial phase of threat detection, Salt Security's patented Behavioral Threat Protection comes into play. The AI system analyzes API traffic in real-time, drawing from extensive datasets of known attack patterns. It is capable of detecting anomalies, suspicious activities, and potential zero-day exploits. Moreover, its adaptive learning algorithm, which evolves based on new data and past incidents, provides a dynamic and robust defense mechanism that is critical in today's fast-paced threat environment.

And to bolster the risk reduction, the Salt Labs team continues to discover API security flaws that translate to functionality added to the product. A recent example is with the critical security flaws within ChatGPT plugins, which could have allowed unauthorized access to third-party accounts and sensitive user data. Salt now has advanced OAuth protection built into the platform.

According to the Salt Labs State of API Security Report, Q1 2023, 59% of respondents manage more than 100 APIs, and 25% manage more than 500. 27% also stated that they've more than doubled their API count over the past year. This number is only set to increase as organizations leverage generative AI within business operations, which can lower the timeline of code and API creation from days to minutes or even seconds. Traditional API security solutions, such as API gateways, web application firewalls (WAFs) and content delivery network (CDN) solutions, already

struggle to keep pace with the expanding API attack surface and the introduction of generative AI further impedes their ability to deliver robust API protection.

With these enhancements, customers can now deliver an API-first model for modern applications to quickly and securely scale business operations, while simultaneously ensuring that they remain compliant with company as well as industry API policies and standards. Salt is the first security vendor to utilize AI throughout an API security platform. The new offering is available to organizations as a SaaS solution or managed security service delivered by Salt.

"Since founding the API security market, AI and ML have always been core components of our platform in order to provide organizations with the deep context and behavioral insights needed to mitigate the most sophisticated API security threats," said Michael Nicosia, COO and co-founder, Salt Security. "The recent growth of utilizing generative AI within business operations has not only expedited the volume of APIs, but also given attackers the means to launch more tactical attack campaigns. Leveraging generative AI for good, we have instilled our own LLM, Pepper, into our platform to help organizations solve the complex problems which generative AI creates in an easy to use and understand interface. With Pepper, organizations will experience enhanced API inventory management and documentation, streamlined threat and incident response, as well as robust API posture governance."

To learn more about Salt Security or to request a demo, please visit https://content.salt.security/demo.html.

*Gartner, API Security Maturity Model, By William Dupre, Gary Olliffe 2 April 2024
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

About Salt Security
As the pioneer of the API security market, Salt Security protects the APIs that form the core of every modern application. Protecting some of the largest enterprises in the world, Salt's API Protection Platform is the only API security solution that combines the power of cloud-scale big data and time-tested ML/AI to detect and prevent API attacks. With its patented approach to blocking today's low-and-slow API attacks, only Salt provides the adaptive intelligence needed to protect APIs. Salt's posture governance engine also delivers operationalized API governance and threat detection across organizations at scale. Unlike other API governance solutions, Salt Security's AI-based runtime engine pulls from the largest data lake in order to continuously train the engine. Salt supports organizations through the entire API journey from discovery, to posture governance and threat protection. Deployed quickly and seamlessly integrated within existing systems, the Salt platform gives customers immediate value and protection, so they can innovate with confidence and accelerate their digital transformation initiatives. For more information, visit: https://salt.security/

Charley Nash

Eskenzi PR
charley@eskenzipr.com

This press release can be viewed online at: https://www.einpresswire.com/article/709557606