Feature Brief: Enhance Your API Security with Salt Surface

Introduction:

In today's digital landscape, APIs are crucial for modern applications, enabling seamless data exchange and driving innovation. However, this connectivity also exposes organizations to significant security risks, as APIs are prime targets for cyberattacks. Therefore, robust API security is essential.

Salt Security offers a comprehensive, AI-infused API security platform that provides panoramic discovery, posture governance, and behavioral threat protection for all your APIs. Salt Surface was designed to enhance the capabilities of panoramic discovery.

Salt Surface is an active reconnaissance tool designed to mimic the tactics used by API attackers. It helps organizations proactively identify and validate exposed API endpoints. Unlike traditional passive discovery methods that rely solely on observing API traffic, Salt Surface employs active discovery techniques to uncover hidden vulnerabilities and enhance security posture.

How Salt Surface is Different:

Salt Surface stands out with its active discovery capabilities, going beyond traditional passive methods to actively identify and validate exposed API endpoints. Its panoramic discovery approach offers a comprehensive view of API assets by monitoring traffic across various lifecycle stages. Serving as a reconnaissance tool, Salt Surface provides a deeper understanding of an organization's API attack surface and exposes current risks. The technology is powered by the expertise and research from Salt Labs, a leader in API security research. Unlike competitors that often provide unrelated data, Salt Surface focuses on delivering relevant and actionable insights by specifically finding and reporting exposed API endpoints. Ultimately, it helps organizations enhance their security posture by identifying potential security gaps before threat actors can exploit them.

Summary of Salt Surface Features:

Salt Surface actively researches internet facing API assets, examining domains and subdomains to pinpoint API endpoints. It then validates the existence and exposure of these endpoints, reporting its findings directly in the Salt dashboard. Trained by Salt Labs, it employs tactics and techniques used by leading API security researchers. This approach not only improves overall security by identifying unmonitored API traffic but also proactively detects security gaps before they can be exploited. Salt Surface is adept at uncovering shadow and zombie endpoints that might otherwise be overlooked. By ensuring security measures are correctly deployed across different environments, it helps organizations maintain a strong defense. Additionally, it highlights potentially sensitive information exposed online and performs comprehensive reconnaissance by mining data from repositories, forums, and other online sources. Finally, it alerts users if internal API specifications or contracts become publicly accessible.

Conclusion:

Salt Surface is an essential capability for organizations that prioritize API security. By providing proactive threat detection and exposing potential security gaps, Salt Surface empowers organizations to strengthen their security posture and protect their valuable API assets.