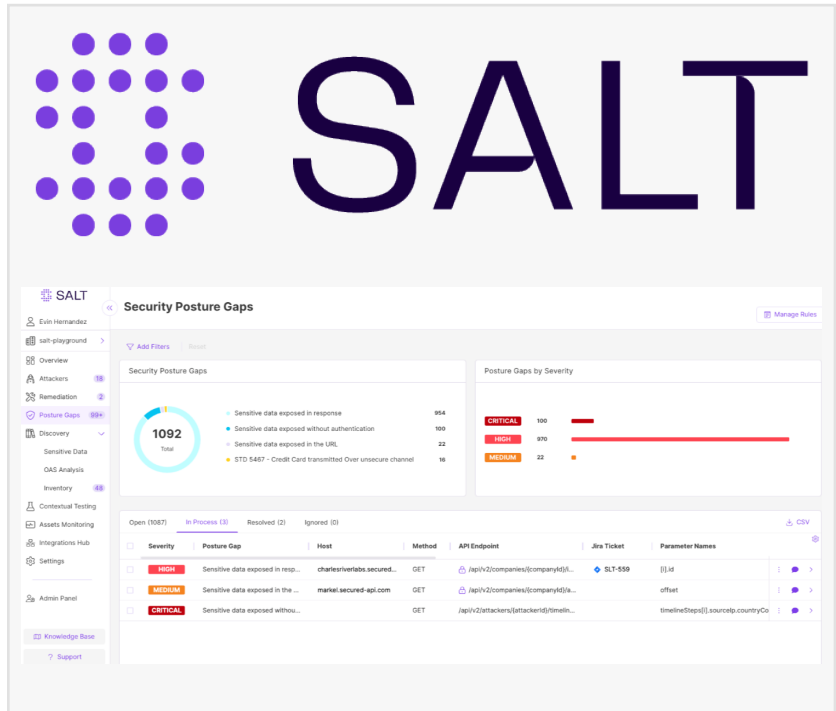


Salt Security Delivers Another Technology Breakthrough with Industry's Only API Posture Governance Engine

Company enriches signature platform to ensure accurate API discovery, policy adherence and protection against API-targeted attacks

LONDON, UNITED KINGDOM, January 17, 2024 /EINPresswire.com/ -- [Salt Security](#), the leading API security company, today announced multiple advancements in discovery, posture management and AI-based threat protection to the industry leading [Salt Security API Protection Platform](#). Salt leapfrogs traditional posture management by providing the industry's first API posture governance engine delivering operationalised API governance and threat detection across organisations at scale.



According to Gartner®*, "API usage is increasing, but most organisations still lack knowledge about how to secure it. As API exploits become widely available, and the impact of API attacks

grows, CISOs and software engineering leaders need to understand how to tackle API security". Proper governance helps bring more context and more value to behavioural threat protection.

“

APIs sit at the core of today's modern applications, connecting enterprises to vital data and services.”

Roey Eliyahu, CEO at Salt Security

With the latest expansion to its AI-based platform, Salt now delivers:

Industry's first API posture governance engine - Which

helps organisations minimize risk on their API first journey, by having the ability to author corporate standards for API posture, and assess compliance with those standards, along with

industry best practices, and regulatory requirements. Unlike typical API security solutions that focus primarily on detection and mitigation of threats, Salt's platform introduces the first-ever engine dedicated to API posture governance. The new functionality helps ensure that all API lifecycle stakeholders (architects, developers, API product managers, AppSec, SecOps) are in sync and security standards are followed as an API makes its way through its lifecycle.

New API filtering and querying capabilities - Which provides context rich API asset discovery and management, helping organisations mine more intelligence from their discovered API assets. This feature allows organisations to extract detailed insights about their APIs, such as their purpose, usage patterns, and associated risks. The ability to create posture governance policies directly from these insights is a significant leap forward, offering a new level of depth and customisation.

Enhanced behavioural threat response capabilities - Which will provide SecOps personnel with the capability to more effectively prioritise, triage, and analyse API related security events, and drastically reduce mean time to respond and resolve. More API sprawl means more opportunity for threat actors targeting APIs. This trend will continue in 2024, as evidenced by Salt Security's latest State of API Security Report, Q1 2023, which found a 400% increase in unique API attackers this last year and its State of API Security for Financial Services and Insurance Report where 92% of respondents say they have experienced a significant security issue in production APIs over the past year, with nearly one out of five have suffered an API security breach. Salt's new attacker activity filtering, querying, and threat hunting capabilities leverages findings derived from industry's most mature and advanced behavioural threat detection platform, coupled with its context rich API asset intelligence. The integration of this advanced threat detection with API asset intelligence equips security teams with the tools to rapidly and effectively address API-related security events.

New ecosystem enrichment capabilities - Which will share API intelligence with the broader lifecycle ecosystem. The platform's enhanced integrations with application security testing platforms, data enrichment through its public API, and advanced outbound integrations (like syslog and Splunk) are designed to ensure that API security is not a standalone effort but an integrated part of the broader security infrastructure. This holistic approach to API security, focuses on both internal asset management and external ecosystem integration. All of these improvements help organisations more easily share and operationalise Salt's API asset and threat intelligence with existing security technology investments.

Enterprise onboarding and operationalisation improvements - Which reduce API risk quickly with minimal operational friction. These latest updates aim to help ease this burden with new improvements in role based access control, improved integrations to corporate identity systems, enhanced system health management and audit controls, and improved data collection and data protection mechanisms.

"APIs sit at the core of today's modern applications, connecting enterprises to vital data and

services,” said Roey Eliyahu, CEO at Salt Security. “However, with the ever-growing abundance of APIs, businesses are struggling to keep track of the APIs they have within their environment and even more so, are unsure of their current API posture against best practice policy and their own custom policies. By providing the industry's first API posture governance engine, Salt is helping organisations govern their API-first journeys using API intelligence to discover and effectively manage API assets, ensuring that corporate standards and industry best practices are followed throughout an API's lifecycle.”

More API sprawl means more opportunity for threat actors targeting APIs and this trend will only continue in 2024. According to the Salt Labs State of API Security Report, Q1 2023, 94% of organisations experienced security problems in production APIs in the past year, and an unfortunate 59% have experienced application rollout delays resulting from security issues identified in APIs. The Salt posture governance engine captures API data with ease, simplifying how organisations share and respond to API threat intelligence. The platform provides pre-packaged templates for accelerated ramp up time, allowing organisations the ability to create their own posture rules, organise and categorise their rules, and extensively filter their APIs. Unlike other API governance solutions, the Salt AI-based runtime engine pulls from the largest data lake in order to continuously train the engine. Salt is the only API security company to deliver AI-based API security, advanced discovery and innovative posture gap analysis, which is needed to unlock the intelligence discovered within APIs.

To learn more about Salt's API posture governance engine, join our webinar, “A New Strategy for Reducing API Risk,” on Tuesday, January 30 at 9am PT/12pm ET. [Register here](#). Platform demos can also be scheduled by visiting: <https://content.salt.security/demo.html>.

*Gartner, Research Index: Everything You Should Do to Address API Security, 31 March 2023. 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

Salt Security protects the APIs that form the core of every modern application. Its patented 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. By correlating activities across millions of APIs and users over time, Salt delivers deep context with real-time analysis and continuous insights for API discovery, attack prevention, and hardening APIs. 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/681672906>

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.

© 1995-2024 Newsmatics Inc. All Right Reserved.