Why Traditional Security Tools Leave Gaps in your API Security

Go Beyond Point Solutions to Secure Your APIs and Your Business

Introduction

APIs are crucial to modern business, facilitating seamless connectivity, driving innovation, and supporting digital transformation. However, in this interconnected environment, security challenges arise. APIs can expose sensitive data and critical business functions, making them attractive targets for attackers looking to exploit vulnerabilities and compromise organizations.

The Problem: Traditional Security Tools Leave Gaps in Your API Security

Current security solutions fail to protect API security's dynamic and complex nature adequately.

- **API Gateways:** Although API gateways are essential for basic traffic management and access control, they fall short in providing comprehensive API security. They offer limited visibility into east-west traffic within microservices, need help enforcing security policies against evolving attack techniques, and often need more context for effective threat detection.
- **AST Vendors:** AST tools are essential for identifying vulnerabilities in source code; however, they have limitations when securing APIs during runtime. They do not provide continuous monitoring, leaving APIs vulnerable between scanning sessions. Additionally, these tools often overlook vulnerabilities in third-party code and external APIs. Moreover, they do not actively detect or respond to attacks in real time.
- **WAFs/CDNs:** Web Application Firewalls (WAFs) and Content Delivery Networks (CDNs) effectively defend against known external threats; however, they struggle with the complexities of API security. Their lack of a deep understanding of API structures and data formats limits their effectiveness against API-specific attacks and business logic abuse. Additionally, they primarily concentrate on north-south traffic, which leaves internal APIs exposed and vulnerable.
- **API Ecosystem Tools:** These tools provide specialized functionality for API management and development but do not prioritize security. They frequently lack unified visibility across

all APIs, possess insufficient governance capabilities, and offer limited security oversight.

- **Other Security Tools:** Traditional security tools, such as SIEMs and endpoint security solutions, may include some features related to API security; however, they do not offer the focused and API-specific capabilities necessary for comprehensive protection.

These specialized solutions result in a disjointed security strategy, leaving your APIs open to advanced attacks that take advantage of vulnerabilities in your defenses.

The Salt Security Solution: Complete API Protection

Salt Security offers a comprehensive API security platform that surpasses traditional tools, providing:

- **Unmatched Visibility:** Discovers all APIs, including shadow, zombie, and rogue APIs, providing a complete inventory of your attack surface.
- **Deep Contextual Analysis:** Understands how APIs function, data flow, and user interactions to identify anomalies and prioritize potential risks.
- **Automated Posture Governance:** Salt's centralized policy hub simplifies API security posture management. Easily define and deploy policies across your API landscape, ensuring consistent enforcement of standards and proactive vulnerability remediation.
- **Robust Data Protection:** Identifies and safeguards sensitive data exposed through APIs, preventing data breaches.
- **AI-Powered Threat Prevention:** Patented intent enigne detects and mitigates advanced API attacks in real-time, including business logic exploitation and account hijacking.

Key Benefits:

- **Reduce API Risk:** Takes proactive steps to identify and address API vulnerabilities before they can be exploited.
- **Strengthen Security Posture:** Develops a thorough understanding of your API security environment.
- **Enhance Compliance:** Ensure compliance with regulatory requirements for API security and data privacy.
- **Accelerate Business Growth:** Innovate and launch new APIs with confidence, ensuring that security remains a top priority.

Salt Security: The Essential Foundation for API Security

Don't leave your APIs exposed to attacks. Contact Salt Security today to learn how our platform can secure your API ecosystem and protect your business.