Shield Your Code, Secure Your APIs

The Critical Role of APIs in the Software/Technology Industry

APIs are essential for modern software development as they allow seamless communication and data exchange between different software platforms. They enable innovation, faster development, and the creation of interconnected digital ecosystems.

However, exposing APIs to the public internet poses security risks, as malicious actors could exploit them. Breaches or disruptions can lead to data breaches, unauthorized access to code, and supply chain attacks, affecting business continuity, customer trust, and competitive advantage. The dynamic nature of software development and the increasing complexity of software architectures make API security even more challenging.

Key API Challenges in the Software/Technology Industry

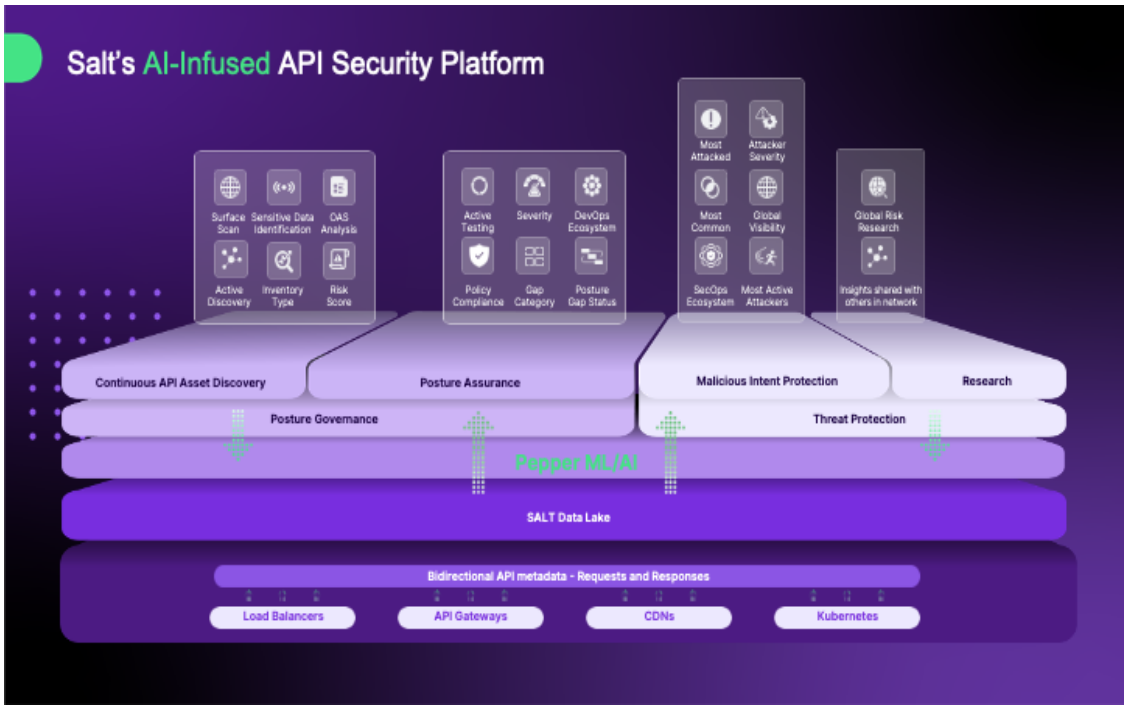
- **API Exposure and Exploitation:** Publicly exposed APIs are vulnerable to attacks by malicious actors who seek to steal data, disrupt services, or gain unauthorized access to sensitive systems.
- **Data Breaches and Intellectual Property Theft:** APIs often handle sensitive customer data and proprietary code, making them attractive targets for cybercriminals. A breach can result in significant financial losses, reputational damage, and loss of competitive advantage.
- **Supply Chain Attacks:** The integration of third-party APIs and software components introduces potential vulnerabilities that can be exploited by attackers to compromise the entire software supply chain.
- **Evolving Threat Landscape:** Cybercriminals are constantly developing new techniques to exploit API vulnerabilities. Proactive and adaptive security measures are crucial to stay

ahead of these threats.

- **Rapid Development Cycles:** Agile development methodologies and the pressure to release software quickly can sometimes lead to security being overlooked or deprioritized.

Why Salt Security is the Best Solution for Software/Technology

Salt Security provides a comprehensive AI-infused API security platform aimed at safeguarding sensitive data, intellectual property, and ensuring the integrity of software and technology services. The capabilities offered by Salt Security address the fundamental API security needs of the software and technology sector.



- **API Discovery:** Salt Security's continuous API discovery capabilities ensure that all APIs, including shadow APIs, zombie APIs, and those used in integrations with third-party services, are identified and protected. This eliminates blind spots and reduces the risk of unauthorized access to sensitive data and systems.
- **API Posture Governance:** Salt Security helps software and technology companies proactively identify and remediate misconfigurations, vulnerabilities, and compliance gaps in their APIs. By enforcing security policies and best practices, Salt Security helps maintain a strong security posture and protect against common API vulnerabilities like broken object level authorization (BOLA) and injection attacks.
- **API Behavioral Threat Protection:** Salt Security leverages AI and machine learning to analyze API traffic in real-time, detecting and blocking sophisticated threats like account

takeover attempts, data exfiltration, and denial-of-service attacks. This proactive approach safeguards intellectual property, customer data, and ensures business continuity.

In addition to these core capabilities, Salt Security also offers:

- **Security Ecosystem Enrichment:** Salt Security integrates smoothly with your current DevSecOps tools and processes, including DAST platforms. It enhances your security setup by providing continuous API discovery, posture governance, and threat protection. This allows you to prioritize security at an earlier stage, detect and resolve API vulnerabilities during the development phase, and protect your intellectual property and customer data.
- **Scalability and Performance:** Salt Security's cloud-native architecture is designed to effortlessly scale and meet the demands of high-growth software and technology companies. Whether you're experiencing rapid user adoption, expanding into new markets, or handling massive volumes of API traffic, Salt Security can adapt to your needs without compromising performance or security. This ensures that your APIs remain protected and your services operate smoothly, even as your business scales.
- **Regulatory Compliance:** Salt Security assists software and technology companies in fulfilling various regulatory compliance requirements, such as GDPR, CCPA, and industry-specific regulations. The platform offers strong data protection, access controls, and audit trails, allowing you to showcase compliance and establish trust with your customers.

Conclusion:

In an industry driven by innovation and digital trust, Salt Security enables software and technology-focused organizations to confidently adopt new technologies and business models while protecting their APIs, customers, and competitive advantage.