



Safeguard Patient Data, Secure Healthcare APIs

The Critical Role of APIs in Modern Healthcare

APIs are transforming the healthcare industry by facilitating seamless data exchange between electronic health records (EHRs), telemedicine platforms, patient portals, medical devices, and other vital systems. They support efficient care coordination, remote patient monitoring, and personalized treatment plans. APIs also play a key role in advancing medical research and enabling the development of innovative healthcare solutions.

However, due to the sensitive nature of patient health information (PHI) handled by APIs, they are often a target for threat actors. A breach or disruption can have serious consequences, including compromised patient safety, privacy violations, and a loss of trust in healthcare providers. Given the interconnected nature of healthcare systems and the growing reliance on APIs, robust security measures are essential.

Key API Challenges in the Healthcare Industry

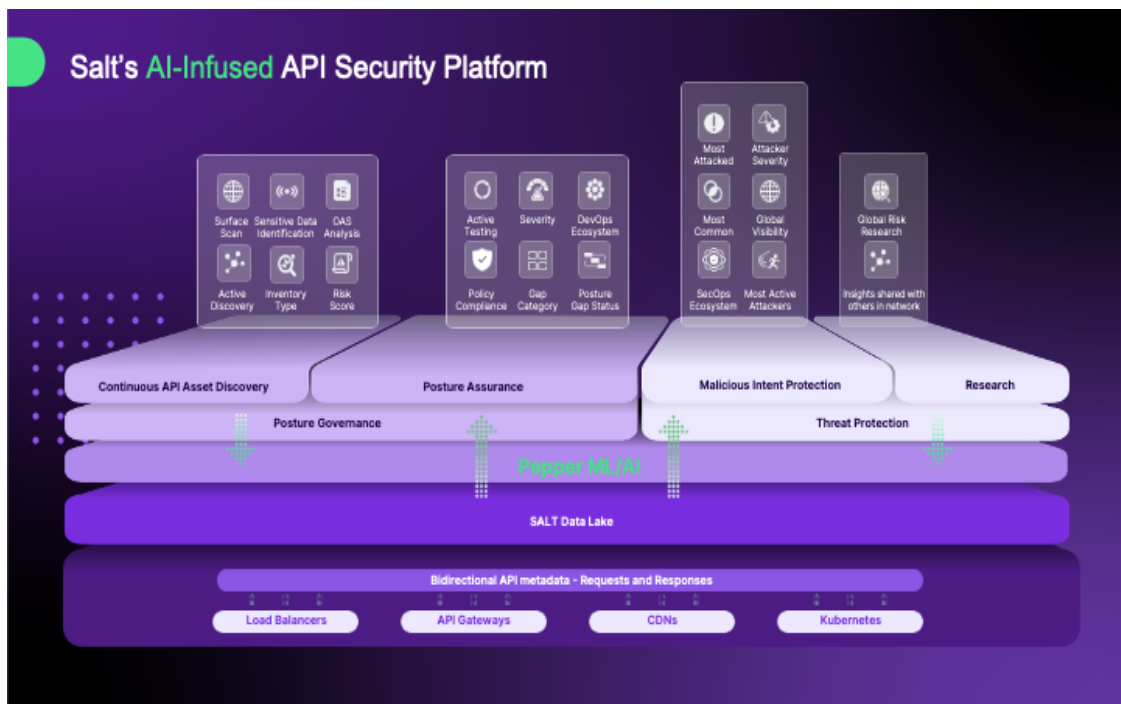
- **Data Sensitivity and Privacy:** APIs handle large amounts of Protected Health Information (PHI), such as medical histories, diagnoses, and treatment plans. Protecting this data is not only a legal requirement (HIPAA) but also a moral imperative.
- **Ransomware and Data Breaches:** Healthcare organizations are increasingly targeted by ransomware attacks and data breaches, which can disrupt operations, compromise patient care, and result in significant financial losses.
- **Connected Medical Devices and Telemedicine:** The growing adoption of connected medical devices and telemedicine platforms expands the attack surface and introduces new API security challenges.

- **Evolving Threat Landscape:** Cybercriminals are constantly adapting their tactics to exploit vulnerabilities in healthcare APIs. Proactive and adaptive security measures are crucial to stay ahead of these threats.

Why Salt Security is the Best Solution for Healthcare

Salt Security provides a comprehensive AI-infused API security platform to safeguard sensitive patient data and ensure uninterrupted healthcare services.

- **API Discovery:** Salt Security's continuous API discovery capabilities ensure that all APIs, including those from legacy systems, shadow APIs, and those connected to medical devices, are identified and protected. This



eliminates blind spots and reduces the risk of unauthorized access to PHI.

- **API Posture Governance:** Salt Security helps healthcare organizations 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 meet HIPAA compliance requirements.
- **API Behavioral Threat Protection:** Salt Security uses AI and machine learning to analyze API traffic in real-time, detecting and blocking sophisticated threats like ransomware, data exfiltration attempts, and unauthorized access to PHI. This proactive approach safeguards patient data and ensures the continuity of critical healthcare services.



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

- **Security Ecosystem Enrichment:** Salt Security integrates with your current healthcare security infrastructure, including electronic health record (EHR) systems, identity and access management (IAM) solutions, and security information and event management (SIEM) platforms. This enhances your security setup with advanced API threat protection, helping you defend against attacks targeting patient data and critical healthcare services.
- **Scalability and Performance:** Salt Security's cloud-native architecture is designed to seamlessly scale with the demands of the healthcare industry. Whether you're experiencing peak usage during a public health emergency or managing the growing volume of data from connected medical devices, Salt Security can handle the load without compromising performance or security. This ensures that your APIs remain protected and your healthcare services operate smoothly even under pressure.
- **Regulatory Compliance:** Salt Security assists healthcare organizations in meeting strict regulatory compliance requirements, such as HIPAA, HITECH, and GDPR. The platform provides robust data protection, access controls, and audit trails, enabling you to demonstrate compliance with industry regulations and safeguard patient health information

Conclusion:

In an industry where patient safety and data privacy are paramount, Salt Security empowers healthcare organizations to embrace digital innovation while safeguarding their APIs, patients data, and reputation.

