



Securing Software APIs: Building Trust and Reliability

Overview: Technology and software companies build and deploy APIs that power modern applications. Security is paramount to maintaining trust and reliability. This document outlines key considerations for securing software APIs, emphasizing the role of robust API posture governance in ensuring security and compliance.

Compliance Landscape:

- **ISO/IEC 27001 & 27017:** Offers a framework for protecting data, especially within cloud environments, crucial for securing sensitive data processed by software APIs. API posture governance provides a structured approach to implementing and maintaining these security controls, ensuring continuous data protection and simplifying security management.
- **GDPR:** Becomes applicable when handling personal data of EU users, requiring software companies to implement appropriate security measures for data protection. [Article 25] API posture governance helps software companies meet these requirements through automated enforcement of security policies and data protection by design principles, reducing the risk of non-compliance and reputational damage.
- **MITRE ATT&CK Framework:** Provides a knowledge base of adversary tactics and techniques specifically relevant to API threats, enabling software companies to proactively defend against attacks. API posture governance helps organizations proactively mitigate these threats by enforcing security best practices and continuously monitoring API behavior for malicious activity, enhancing threat detection and response capabilities.

Key API Security Considerations:

- Secure API Design and Development.
- Strong Authentication and Authorization.
- Data Encryption and Privacy.
- Input Validation and Rate Limiting.
- Continuous Monitoring and Logging.
- Regular Vulnerability Assessments and Penetration Testing.



How Salt Security Helps:

Salt Security provides a comprehensive API security platform tailored for technology and software companies:

- **API Discovery and Inventory Management:** Discovers all APIs, including shadow and zombie APIs, to ensure a complete understanding of the API landscape.
- **Posture Governance and Security:** Following API discovery, Salt automates security policy enforcement (e.g., GDPR) with pre-built/custom rules. This proactive approach to API posture governance minimizes the risk of costly compliance failures and data breaches.
- **Secure API Design and Development Support:** Provides insights and guidance for secure API design and development practices.
- **Vulnerability Assessment and Secure Coding Practices:** Detects API vulnerabilities, including those arising from insecure coding practices.
- **Threat Detection and Attack Prevention:** Uses AI-driven behavioral analysis to detect and prevent sophisticated API attacks.
- **Data Security and Privacy Compliance:** Offers visibility into sensitive data in motion through APIs, supporting data protection and privacy compliance, including GDPR.

Conclusion:

Technology and software companies must prioritize robust API security and a strong API posture governance strategy to build secure and reliable software, protect user data, and maintain trust. Salt Security provides a comprehensive solution to meet these critical needs and help you achieve and demonstrate compliance. For a more in-depth understanding of API security compliance, please refer to our comprehensive **API Compliance Whitepaper**.