

Secure Retail APIs: Protecting Customer Data and Transactions

Overview: Retailers rely on APIs for e-commerce, payment processing, and customer engagement. Protecting sensitive customer data and ensuring secure transactions are crucial. This document highlights the key security and compliance considerations for retail APIs, emphasizing the role of API posture governance in maintaining a secure and compliant API ecosystem.

Compliance Landscape:

- **PCI DSS v4.0:** Mandates security standards for all entities that store, process, or transmit cardholder data, with specific requirements for securing APIs involved in payment processing. [Req. 2.2.7, 6.2.3, 6.2.4, 6.3.2] API posture governance helps ensure continuous compliance with PCI DSS requirements by automating the enforcement of security controls and providing ongoing monitoring of API configurations to prevent deviations from a secure state.
- **GDPR:** Applicable if handling personal data of EU customers, requiring retailers to implement appropriate technical and organizational measures to protect this data. [Article 25] API posture governance provides a framework for implementing and enforcing these data protection measures, ensuring adherence to GDPR's principles of data protection by design and default.
- **ISO/IEC 27001 & 27017:** Provides a framework for securing data, particularly in cloud environments, which is relevant for protecting customer data and ensuring secure transactions.
- **MITRE ATT&CK Framework:** Helps understand and mitigate API-specific threats, enabling retailers to proactively defend against attacks.

Key API Security Considerations:

- Secure Payment Processing (PCI DSS).
- Data Encryption and Privacy (GDPR).
- Strong Authentication and Authorization.
- Input Validation and Rate Limiting.
- Continuous Monitoring and Logging.
- Regular Vulnerability Assessments.



How Salt Security Helps:

Salt Security provides a comprehensive API security platform tailored for the retail industry:

- **API Discovery for Comprehensive Protection:** Discovers all APIs, including shadow and zombie APIs, ensuring that all potential attack surfaces are identified.
- **Posture Governance for Ongoing Security:** Following API discovery, Salt automates security (e.g., PCI DSS, GDPR) with pre-built/custom rules. This proactive approach to API posture governance minimizes the risk of costly compliance failures and data breaches.
- **Vulnerability Assessment and PCI DSS Compliance:** Detects API vulnerabilities that could expose cardholder data, supporting PCI DSS compliance.
- **Threat Detection and Fraud Prevention:** Uses AI-driven behavioral analysis to detect and prevent sophisticated attacks like credential stuffing, API abuse, and other fraudulent activities.
- **Data Security and GDPR Compliance:** Offers visibility into sensitive customer data in motion through APIs, supporting data protection and GDPR compliance.

Conclusion:

Retailers must prioritize API security and a strong API posture governance strategy to protect customer data, ensure secure transactions, and maintain trust. Salt Security provides a robust 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**.