SALT

Travel/
Hospitality

Securing Travel APIs: Protecting Customer Data and Transactions

Overview: The hospitality and travel industry uses APIs for booking, payments, and customer service. Protecting sensitive customer data is crucial. This document highlights the key security and compliance considerations, emphasizing the importance of robust API posture governance for data security and compliance.

Compliance Landscape:

- PCI DSS v4.0: Protects cardholder data, requiring secure handling of payment card information transmitted through APIs. [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 data of EU citizens, requiring hospitality and travel companies to implement appropriate security measures to protect this data. [Article 25]
- ISO/IEC 27001 & 27017: Data security in cloud environments, which is relevant for protecting sensitive customer data stored or transmitted in the cloud.
- MITRE ATT&CK Framework: Helps understand API threats, enabling hospitality and travel companies to defend against attacks proactively. API posture governance allows organizations to proactively implement defenses against these attacks by enforcing security best practices and continuously monitoring API behavior.

Key API Security Considerations:

- Secure Payment Processing.
- Data Encryption.
- Strong Authentication.
- Input Validation.
- Continuous Monitoring.
- Vulnerability Assessments.

How Salt Security Helps:

Salt Security provides a comprehensive API security platform tailored for the hospitality and travel industry:

- API Discovery for Complete Visibility: Discovers all APIs, including shadow and zombie APIs, ensuring comprehensive protection.
  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, including those targeting booking data and customer information.
- Data Security and Privacy Compliance: Offers visibility into sensitive customer data in motion through APIs, supporting data protection and privacy compliance, including GDPR.

Conclusion:

Protecting customer data and ensuring secure travel transactions is paramount in the hospitality and travel industry. 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.**