Sprita iT

Hospitality Industry

Secure Digital Transformation and Risk Management

A Sector in Digital Transformation

The hospitality industry is undergoing rapid digitalization. Hotels, airlines, restaurants, and travel platforms depend increasingly on online booking systems, mobile apps, loyalty programs, and digital payments. While this enhances customer experience, it also increases exposure to cyber threats and regulatory pressure. Hospitality systems handle highly sensitive data, including credit card information, passports, travel histories, and customer preferences. A single breach can result in significant financial losses, regulatory penalties, and severe damage to the trust of guests.

Key Cybersecurity Challenges in Hospitality

- Protecting guest and payment data in compliance with PCI DSS, GDPR, and other frameworks.
- Managing complex, interconnected systems with multiple vendors and integrations.
- Addressing vulnerabilities in web and mobile applications exposed to attackers.
- Securing the digital supply chain, including third-party providers and integrations.
- Preserving brand reputation, as customer trust directly impacts loyalty and occupancy.

Our Solutions: Comprehensive Security for Hospitality

1. Our solutions ensure application and supply chain security across the sector:
    a. Application Security
    b. Automated identification of vulnerabilities in booking platforms, mobile apps, and billing systems.
    c. Alignment with OWASP Top 10 and CWE standards.
    d. Clear, auditable reports for compliance and regulatory inspections.
2. Dependency and Third-Party Risk Management:
    a. Continuous monitoring of open-source libraries, APIs, and third-party systems.
    b. Real-time alerts for vulnerabilities and licensing risks.
    c. Risk assessments before integrating new providers.
    d.
3. Digital Supply Chain Protection:
    a. CI/CD pipeline monitoring to detect tampering or unauthorized modifications.
    b. Validation of integrity for every application release.
    c. Evidence-based reporting to strengthen regulator and partner confidence.
4. SLA Definition and Risk Evaluation:
    a. Support in defining Service Level Agreements (SLAs) with security and quality metrics.
    b. Risk evaluation for adopting or maintaining systems like PMS, CRM, and booking engines.
    c. Prioritization of cybersecurity investments based on business impact.

Strategic Benefits for Hospitality Leaders

Simplified Compliance: Automated evidence for PCI DSS, GDPR, and local regulations.

- Cost Savings: Early detection reduces remediation and downtime costs.
- Enhanced Guest Experience: Secure and reliable systems build trust.
- Stronger Brand Reputation: Proactive security becomes a differentiator.
- Accelerated Innovation: Digital transformation initiatives proceed securely.

Use Cases in Hospitality

Hotels: Protecting property management systems (PMS), booking platforms, and loyalty programs.

- Airlines: Securing ticketing, check-in systems, and mobile applications.
- Online Travel Agencies (OTAs): Safeguarding APIs and travel search engines.
- Restaurants and Entertainment: Protecting digital payments and reservation platforms.

Benefits Overview

Benefit	Description
Regulatory Compliance	Evidence aligned with PCI DSS, GDPR, and hospitality data regulations.
Operational Savings	Reduced remediation and downtime through proactive security.
Customer Trust	Stronger guest loyalty by protecting personal and payment data.
Risk Evaluation	Assessing risks in adopting or maintaining hospitality systems.
Innovation Enablement	Secure foundation for digital transformation initiatives.

Secure Hospitality, Trusted Experiences.

Sprita iT empowers the hospitality sector to secure booking platforms, mobile apps, loyalty programs, and digital payments. Our solutions simplify compliance, protect guest data, mitigate operational risks, and enhance brand reputation—transforming cybersecurity into a driver of customer trust and digital transformation.