SOLUTION BRIEF

Armis Brief: Cyber Exposure Management in Hospitality

The hospitality industry is undergoing a period of rapid transformation, in the form of evolving consumer expectations, economic pressures and increased competition. Some of the trends shaping the industry include:

- **New Menu Offerings & Restaurant Expansion**

  Restaurants and hotels are continuously evolving their menus and service offerings to attract and retain customers. However, inflation and rising operational costs remain critical challenges. Addressing supply chain inefficiencies can help mitigate these cost pressures.

- **Digital Enablement & Third-Party Integrations**

  Businesses are increasingly investing in technology to help them stand out. This includes innovations such as mobile ordering, contactless payment, and third-party delivery services, to enhance customer convenience and drive revenue growth.

- **Consumer-Driven Menu Adaptations**

  Many businesses are adapting their menus based on market research, customer preferences, and promotional strategies to balance cost savings while maintaining customer satisfaction.

- **Workforce Management & Talent Retention**

  Attracting and retaining top talent remains a challenge, requiring businesses to focus on employee experience, automation, and training programs.

- **Technology Adoption & Cybersecurity Risks**

  Hospitality businesses are leveraging AI, automation, and IoT-driven solutions to streamline operations, improve guest experiences, and reduce costs. However, increased digital adoption introduces heightened cyber exposure management and security risks.

Key Challenges

The growing digitalization of hospitality operations means a growing asset and device infrastructure; and with this, comes with cybersecurity challenges including:

Lack of Comprehensive Asset Visibility

Hospitality businesses manage vast networks of connected devices, from POS systems and IoT-enabled smart devices to reservation platforms and guest Wi-Fi. Without a centralized platform to track these assets, businesses struggle to maintain security and compliance.

Threat Identification, Prioritization & Response

Security teams often lack the ability to quickly identify, contextualize, prioritize and remediate threats. The inability to prioritize vulnerabilities and other security issues leaves systems exposed to attacks.

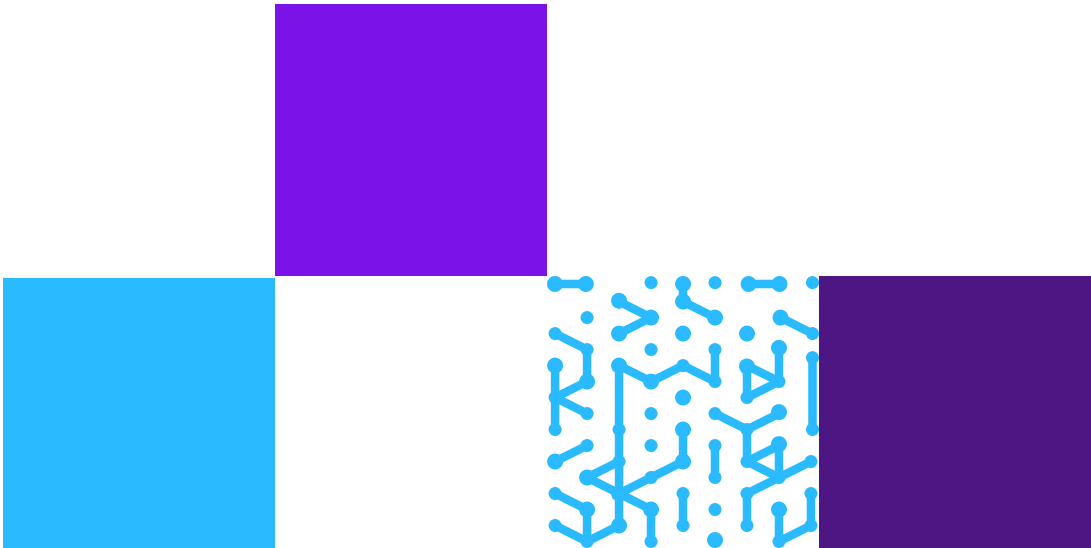
Regulatory Compliance & Security Frameworks

The industry must adhere to multiple regulations, including:

- PCI DSS (Payment Card Industry Data Security Standard)
- CIS (Center for Internet Security) Controls
- GDPR (General Data Protection Regulation)
- ISO 27001

Proactive Threat Mitigation

Attackers increasingly target hospitality businesses due to the high volume of financial transactions and personally identifiable information (PII). Preventing breaches before they occur is crucial to maintaining operational stability and customer trust.



Notable Cyber Threats in the Hospitality Industry

Over the past five years, numerous cyber incidents have impacted the hospitality industry, underscoring the urgent need for robust security measures. Examples include:

- **International Hotel Chain Data Breach (2018 & 2020)**

  A series of breaches exposed sensitive customer data, including passport numbers and credit card information, affecting over 500 million guests.

- **Hotel Resort Breach (2019)**

  Personal details of over 142 million guests were leaked due to a cloud misconfiguration.

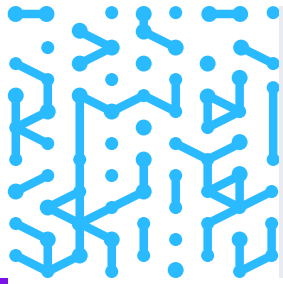
- **Major Food Chain POS Malware Attack (2016-2019)**

  A point-of-sale malware campaign affected hundreds of Wendy's locations, leading to the theft of customer payment data.

- **Ransomware Attacks on Hotel Chains**

  Several high-profile hotel chains have been hit by ransomware attacks, disrupting reservation systems and guest services.

With cyber threats growing in frequency and sophistication, hospitality businesses must adopt a proactive security approach through Cyber Exposure Management.



How Armis Supports the Hospitality Industry

Armis Centrix™ provides a comprehensive cybersecurity solution tailored to the unique needs of the hospitality industry. As a unified, cloud-based Cyber Exposure Management platform, Armis Centrix™ provides real-time visibility, risk assessment, and automated threat response. It seamlessly integrates with existing security tools such as SIEMs, endpoint protection solutions, and compliance frameworks. Its agentless architecture ensures frictionless deployment, allowing hospitality businesses to enhance their security posture without disrupting operations.

Armis Centrix™ for Asset Management & Security

Hospitality businesses operate in a highly connected environment, with a mix of IT, OT, IoT, and third-party devices. Armis Centrix™ delivers continuous visibility into all connected assets, helping businesses track, monitor, and secure their infrastructure. By automatically identifying rogue or unauthorized devices, the platform ensures that every asset is accounted for and protected from cyber threats.

Armis Centrix™ for VIPR - Prioritization & Remediation

Given the sheer volume of connected devices, hospitality organizations need a way to assess risks efficiently. Armis Centrix™ enables businesses to prioritize vulnerabilities based on their potential impact, ensuring that the most critical threats on the most critical devices are addressed first. Its integration with security workflows allows for streamlined patching and remediation, reducing exposure to known exploits. Additionally, its AI-powered threat intelligence capabilities helps identify when assets are behaving as expected or when they are out of the norm.

Armis Centrix™ for Early Warning

Empowers the hospitality industry with early warning intelligence to anticipate and mitigate cyber risk effectively. By leveraging AI-driven actionable intelligence, Armis provides insights into the vulnerabilities that threat actors are exploiting in the wild or are about to weaponize, allowing organizations to understand their impact and take preemptive action. With deep monitoring of the dark web, deception technology and human intelligence, Armis Centrix™ for Early Warning ensures unparalleled coverage and accuracy. Automated alerts and predefined security playbooks ensure rapid response, mitigating risks in real-time.

Key Business Outcomes

Armis secures some of the largest and most complex hospitality organizations at scale, globally. Key business outcomes that Armis customers cite include:

- **Customer Trust & Brand Reputation**
  Secured guest data and transactions to maintain customer confidence.
- **Enhanced Operational Resilience**
  Proactively mitigated security threats to prevent costly breaches and downtime.
- **Stronger Compliance Posture**
  Simplified regulatory compliance with automated security controls and reporting.
- **Cost Savings & Efficiency Gains**
  Reduced the risk of unchecked cyber exposure while optimizing security operations.

Armis At Scale for the Hospitality Industry

- **Complete Asset Visibility**
  Full-spectrum monitoring of IT, OT, IoT, and third-party systems, ensuring no device goes undetected.
- **AI-Driven Threat Intelligence**
  Predict and prevent cyberattacks with machine learning-powered insights.
- **Seamless & Agentless Deployment**
  Quick and frictionless implementation, full interaction and cooperation with your existing technology stack; with no impact on business operations.
- **Industry-Specific Threat Detection**
  Tailored security measures designed for the unique cybersecurity challenges of hospitality businesses.

By leveraging Armis Centrix™, the hospitality industry can stay ahead of evolving threats, protect its digital infrastructure, and provide a safe and seamless experience for guests and employees alike.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial