Arkose Labs
PROVEN ACCOUNT SECURITY

HOW AI IS SHAPING THE HOTEL INDUSTRY

Key Insights from New Research: The Intersection of AI, Digital Fraud and Cyber Defenses

Hotel Cybersecurity Strategies Are Shifting

For the hospitality industry, streamlining bookings with an intuitive online platform is key to providing a great user experience. But within this vast digital ecosystem, hotels must balance offering world-class service to good users while keeping bad actors out.

When fraudsters target hotels, they look to take control of customer accounts, steal personal data, abuse loyalty points and manipulate inventory. And using AI, cybercriminals can scale these attacks faster.

This infobrief provides key insights from our new report, The Intersection of AI, Digital Fraud and Cyber Defenses. It highlights how AI is impacting threats and defenses in hospitality, and explores how hotels can harness AI to fight back against cyber-enabled fraud.

Generative AI Checks In

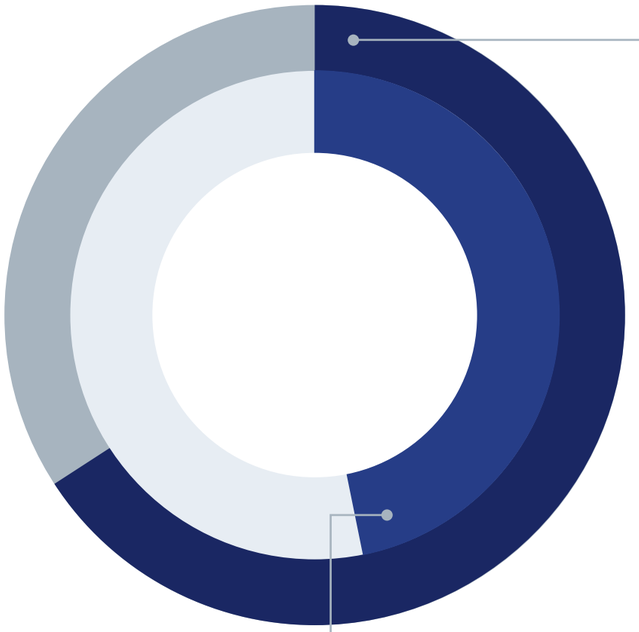
Generative AI has lowered barriers for bad actors, giving even inexperienced cybercriminals the ability to launch convincing attacks at scale. Large Language Models (LLMs) are helping fraudsters to orchestrate phishing schemes and evade detection by appearing more humanlike. And Large Action Models (LAMs) have further expanded the landscape for potential cyber threats.

The results of our recent survey showed that hotels are among the businesses that are particularly concerned about the growing threat of generative AI.

"A trend that we are hearing about at the Loyalty Security Alliance is fraudsters using AI-generated voice technology to contact call centers to attempt fraud. As call centers are less defended and super vulnerable, this is a worrying trend, and it really brought to light for me how fraudsters are now embracing AI to attack businesses." – Chris Staab, Co-founder LSA

64%

of hotels reported that generative AI has increased the frequency of cyber threats against their businesses



46%

said that it was increasing the sophistication of attacks.

Fake Account Creation Tops the Worry List for Hotels

1. For hotel cybersecurity teams, fake account creation is the leading concern, with 79% of surveyed hotels reporting that they are moderately to very concerned about this. Fraudsters are posing as genuine customers to exploit promotional offers. And for hotels that experience high volumes of digital traffic, it's easy for malicious actors to go unnoticed until the damage is done.

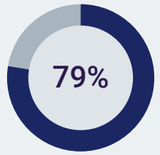
2. 61% of hotels are worried about inventory hoarding. After creating fake accounts, fraudsters create bogus reservations, blocking legitimate customers from booking rooms. This type of denial of inventory scheme disrupts revenue management systems and can lead to significant losses, especially during peak seasons.

3. Meanwhile, 71% are worried about account takeovers. AI can speed up the process for testing numerous login combinations, and hackers can create automated credential stuffing attacks using stolen login credentials from previous breaches.

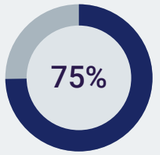
4. 68% of hotels are concerned about loyalty point theft and fraud. Often used along with account takeover attacks, seizing control of a customer’s unused loyalty points increases the value of attacks for fraudsters. This practice stands to frustrate good users and devalue the loyalty program for legitimate customers.

Most Concerning Attack Types

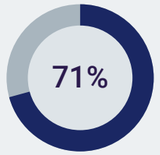
Hotel cybersecurity teams lose sleep over the depth, breadth and speed of these attack types, if they are not addressed. When loyalty accounts are drained, rooms are fraudulently booked or customer data is compromised, travelers lose trust fast. And it's more than reputation damage—it's a potential death blow to long-term business viability in the competitive hospitality space.



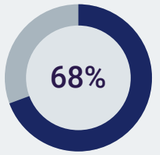
Fake account creation/fake new accounts



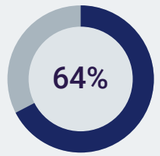
Generative AI-based threats



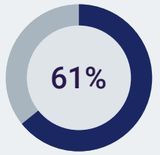
Account takeovers (ATO)/Credential stuffing



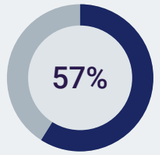
Loyalty point theft/fraud



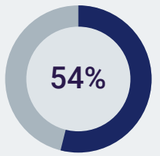
SMS toll fraud/IRSF



Inventory hoarding



MFA compromise (reverse-proxy phishing)



Bonus abuse

No Vacancy for Fraud

For enterprises in all industries facing increasingly sophisticated cyber attacks, there are operational, financial and reputational risks to contend with. The hotel industry is no exception. For more than half of the hotels we surveyed, the cost of these negative consequences is between US$1 million and $9.9 million. Decreased customer acquisition was the negative consequence causing most concern to hotels, with 71% reporting that they have suffered negative effects due to this. And increased operational overheads are also a major issue: 68% of hotels have noticed negative impacts in the last two years, due to threats to critical business applications.

Plus, half of hotels reported suffering a lack of interest from the partner ecosystem as a result of these threats. It's a sign that scams aren't just a one-off inconvenience. Rather, fraud left unchecked threatens to unravel business models and severely impact the long term viability of hospitality businesses.

Investment in AI is Here to Stay

Against this new generation of fraudsters targeting hospitality businesses, hotels need a robust defense. Half of hotels expect that AI powered cybersecurity will improve their threat intelligence gathering, and help their teams to better defend against human fraud farm attacks. But the leading benefit is expected to be better defense against AI-powered bot attacks, with 54% optimistic that an AI-powered security solution will help them square up to fraudsters deploying these attacks.

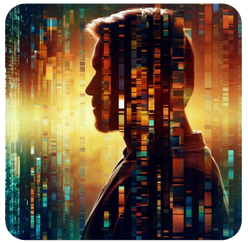
of hotels have seen a reduction in the overall cost of securing their operations business thanks to AI.

3/4 hotels are using AI to respond faster to security incidents

When considering a vendor to support their security needs, the top concern for hotels is use of AI. Many are already getting on board with new technology to fight fraud. 75% of hotels we surveyed told us that they're leveraging AI to enable faster response times to security incidents, and 71% are using it to analyze historical data and identify vulnerabilities.

71%

Report using AI to analyze historical data and identify vulnerabilities



75%

Report leveraging AI to enable faster response time to security incidents

68%

Report using AI to predict future security threats

54%

Report deploying AI tools to continuously monitor infrastructure

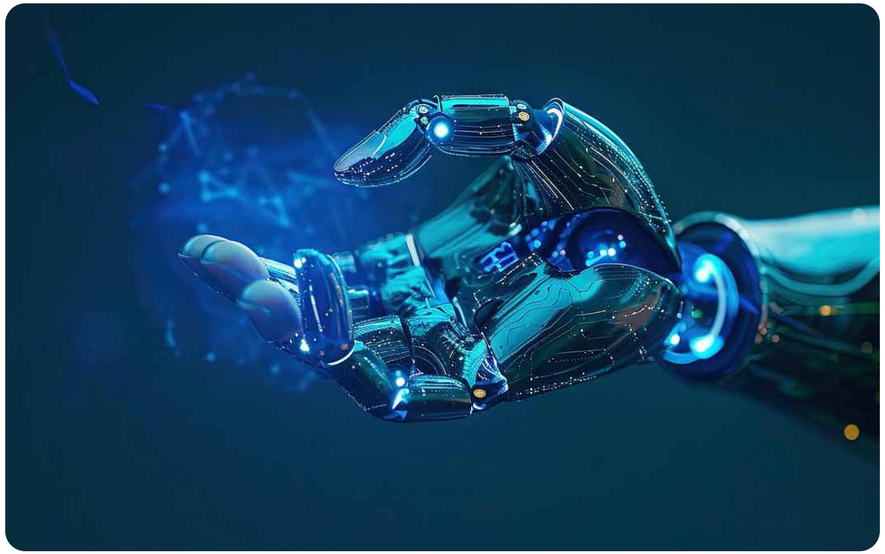
50%

Report automating processes with AI to reduce manual tasks

68%

Report analyzing cybersecurity data in real-time with AI tools

AI-powered solutions are delivering some tangible results for cybersecurity teams. Some of the benefits already realized across the industry are better threat detection and improved threat intelligence gathering, and defense against human fraud farms and bot attacks.

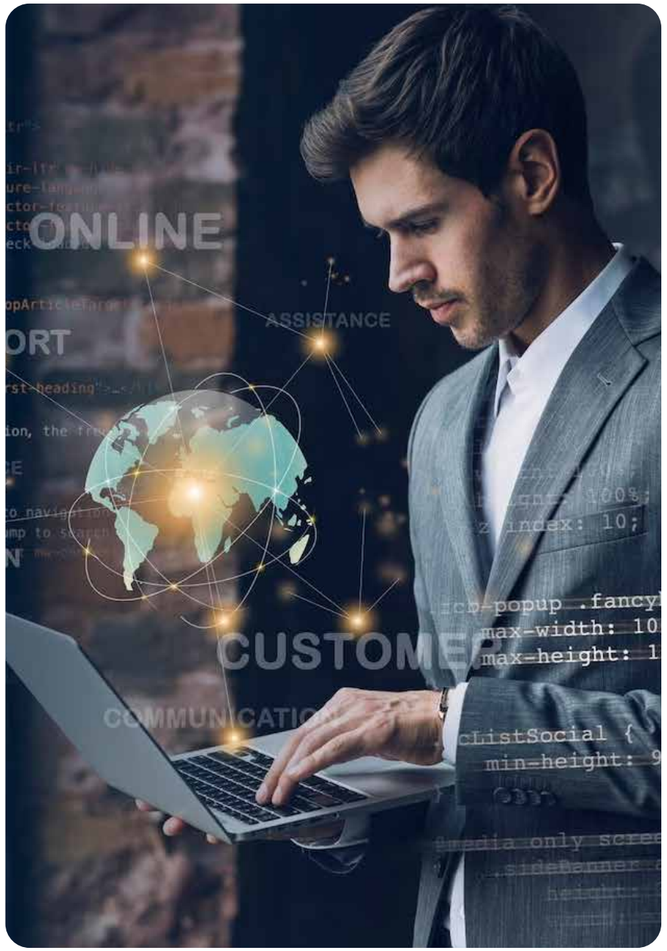


Already Realized Benefits

- Improved threat detection and response
- Improved threat intelligence gathering
- Reduced overall cost of securing the business
- Better defense against basic bot attacks
- Better defense against AI-powered bot attacks
- Better defense against Generative AI-powered attacks
- Better defense against human fraud farm attacks

As AI-powered fraud threats evolve, the cost of inaction rises. Hotels need strong defenses to keep pace with customer expectations and competitive pressures. To truly secure their future, hotels should adopt AI solutions that not only meet today's challenges but anticipate tomorrow's. This requires a bold approach—embracing innovation and partnering with experts who can help navigate the complexities of AI-powered security.

The time to act is now. Will your company rise to the challenge? We invite you to set up a personalized meeting to discuss these results and talk about your needs.



About Arkose Labs

Arkose Labs is the leading global account security company, offering device ID, phishing protection, email intelligence and bot management. The biggest enterprises in the world, including two of the top three banks, Microsoft, Expedia, Roblox and more rely on Arkose Labs to stop account takeovers, fake account creations and SMS toll fraud. No other vendor provides more proactive support for internal security teams, actively takes down threat actor groups or excels like Arkose Labs in sabotaging the profitability of attackers. Ready to see how the Arkose Account Security platform can protect your enterprise from scammers and enhance your fraud protection strategy? Schedule a call with an expert today.

Contact Us

USA

400 Concar Dr, Fl 4
San Mateo CA. 94403

Australia

T.C. Beirne Building, 315
Brunswick Street (level 4),
Fortitude Valley, Brisbane
QLD 4006

United Kingdom

167-169 Great Portland
Street, 5th Floor, London,
W1W 5PF

Costa Rica

Calle 118B San Rafael
San José, SJ 1020

India

Redbrick Offices,
Tower B 2nd Floor,
Panchshil Business Park
Balewadi High Street, Off,
Baner – Balewadi Rd,
Pune, Maharashtra 411045

Argentina

Avenida Corrientes 800,
Buenos Aires,
Buenos Aires C1008