

# Hospitality and Data Security: Distributed environments, short staffed and managing highly sensitive data

## Today's Challenges: Sensitive Data Visibility

CISOs, Information Risk professionals, and security analysts are fighting in the dark; They may know roughly from where the threat actors are coming, and can throw more resources toward the potentially vulnerable areas, but are they focusing the right controls on the right data assets?

The Hospitality industry is on the rebound: the COVID-19 pandemic halted operations around the globe as consumers were quarantining at home so franchisees and corporate offices were stuck trying to maintain operations in the face of an unpredictable future. For many organizations, this meant an acceleration of cloud adoption for centralized operations – which drives greater efficiencies and scale.

## Highlights



Skills gap can lead to insufficient data protection programs, policy violations and data breaches



Up to **8 IT FTEs** can be replaced by automating data discovery and classification activities



Increased data collection for loyalty programs can increase risk but with the right controls you can rest easy



Classification accuracy at, or above **96%** leads to greater usage of sensitive data intelligence to create customized experiences

However, the actual properties – hotels, resorts, motels – sometimes run by franchisees moved even further from corporate cyber controls; these franchisees are still using legacy infrastructure to manage very sensitive data. As the world returns to a pre-pandemic life and traveling is back, the stakes couldn't be higher for hospitality organizations to ensure proper data security controls.

The hospitality industry faces unique challenges as it relates to its cybersecurity and more specifically protecting its most sensitive data inclusive to the data domains of Guests, Loyalty, Booking, and Stay for the millions of customers that are served.

First, Hospitality organizations are highly distributed environments where in the case of many, they have thousands of sites serving customers and a central headquarters who is managing from a distance. This decentralized approach is increasingly challenging since IT operations are often managed on-site by non-IT professionals yet they're taking stewardship of highly sensitive data.



In many cases, the hotels, resorts, or motels have low network bandwidth and small IT footprints so they cannot utilize modern security tools that require more powerful server hardware to operate properly. Similarly, without skilled individuals on-site, the day-to-day managers of properties cannot be expected to do their day jobs and also run sophisticated cyber security tools.

The next challenge comes from a history of breaches. MGM, Marriott, Choice Hotels, Drury and others have experienced significant breaches in the past few years. This is no coincidence. Hospitality organizations are often mature businesses with compressed margins so they are cost conscious and do not always have adequate budgets for IT and Security. Bad actors realize that these organization's sit on very sensitive data without always having the controls and security as other industries like Financial Services or Healthcare, which makes them an easier target. No business should present itself as an easy target.

Additionally, being a relatively low margin business forces organizations look for more nuanced ways to appeal to customers. One way this manifests itself is through loyalty programs where customers earn points by staying at properties to be redeemed for discounted or free future stays. In addition, this behavior data provides Hospitality organizations with valuable insight on their customers which can be used for individualized offerings or new revenue streams such as customized vacation packages. The risk it introduces is another threat vector since a loyalty number is tied back to an individual profile.

As highlighted previously – breaches are an issue for Hospitality organizations, so the addition of loyalty programs, while potentially revenue generators, can also complicate things and turn into new areas of risk.

Finally, Hospitality has been impacted by the dreaded security skill shortage. Organizations across the globe are struggling to find enough cybersecurity professionals to manage their security operations and the Hospitality industry is no different. With thousands of jobs open but a lack of available, skilled workforce, there are gaps in security coverage that can have profound impacts on business operations.

## **Solution– Proven technology focused on the Hospitality industry**

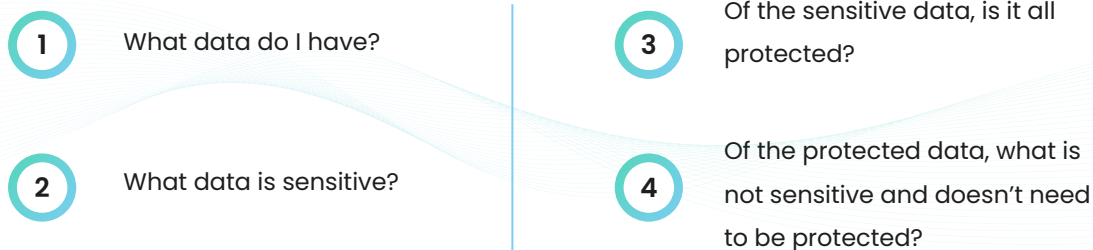
While there is a level of fear and uncertainty as it relates to the Hospitality industry and cyber security, there are new partners – with proven track records – that are entering the scene to solve these problems with a focus on protecting sensitive data. Itouch.io has developed key solutions to specifically address these challenges of holistic Data Protection facing the Hospitality industry.

At a high-level, Itouch.io Inventa is a sensitive data intelligence solution utilizing advanced ML techniques to discover, classify and inventory sensitive data, then layer on-top business context plus insights to drive efficient, risk based decision making. By creating a sensitive data inventory, Hospitality organizations can leverage full data visibility into prioritized data protection so that the highest value assets are protected from internal or external threats – including loyalty program data which should be treated as a crown jewel.

Similarly, as a means of overcoming the skills shortage, Itouch.io Inventa's automation capabilities means that the system is always running and inventorying sensitive data then passing it to the relevant downstream controls. For example, SIEMs can ingest Itouch.io's sensitive data intelligence to cut through noise and only prioritize investigations on incidents related to sensitive data. Customers have reported saving up to 8 FTE from Itouch.io's automation and an 85% reduction in alerts from their SIEM. Not only does this lead to greater operational efficiencies but also optimized resource allocation so individuals can focus on the right tasks.

Distributed environments with minimal IT infrastructure has been a long-running concern for Hospitality organizations. How can you protect properties from a distance with limited resources? Itouch.io has taken its core scanning technology and developed a light-weight option for distributed environments with limited internet bandwidth and minimal server resources. This approach provides corporate offices with visibility into sensitive data at the properties while not relying on property managers to also be security professionals. Combining the light-weight option with the existing Inventa Analytical Engine means that CISOs and Risk Professionals will still be able to use the Itouch.io Inventa Console Manager to view their sensitive assets across their full estate in an efficient manner. This new-found capability will be a game changer for distributed organizations like hospitality chains with global operations.

**1touch.io Inventa™** helps security professionals answer four core questions:

- 
- 1 What data do I have?
  - 2 What data is sensitive?
  - 3 Of the sensitive data, is it all protected?
  - 4 Of the protected data, what is not sensitive and doesn't need to be protected?

## **Conclusion – Reduce risk, increase visibility and sleep well at night!**

As data continues to proliferate and move out to the cloud from the traditional data centric or mainframe environment, it's more and more important to have strong data visibility to ensure the right data is being protected, used, or deprecated. From the hospitality industry perspective, breaches, skills shortage and distributed environments are going to be key challenges but with the right partners they can be managed. Having strong sensitive data intelligence will make the entire organization smarter and more context-aware leading to better decision-making with a more secure IT posture.

[1touch.io](#) is here to be your partner in tackling data security challenges, especially for distributed properties with limited IT footprints. As the ONLY best-of-breed, dedicated discovery and classification solution in the market, **1touch.io's Inventa™** can provide the required level of sensitive data intelligence for any data in any repository while it's at rest and in motion across the network.

[Contact us to learn more](#) about how we can help with Subrogation or other challenges.