Cloud-Hosted Hotel PMS Data: Who Holds the Keys and Why It Matters

Maestro PMS answers questions about data stored in the cloud and how hotel & resort operators can curtail uncertainty

MARKHAM, ONTARIO, CANADA, July 11, 2023 /EINPresswire.com/ -- What's in the cloud — and who owns it — anyway? Despite the hospitality industry's reliance on cloud computing, security myths and other concerns swirl among discussions about the technology, sometimes leading hotel operators to mistrust potential technology partners. These rumblings can lead to a storm of operational disruptions, leaving hoteliers feeling rudderless in a marketplace that requires constant adjustment and reaction.

> Hoteliers must ensure they have an adequate plan in place to protect their cloud-based infrastructure and then ensure its cloud security settings are properly configured as early as possible."
>
> *Warren Dehan*

Maestro, the preferred Web Browser based cloud and on-premises all-in-one PMS solution for independent hotels, luxury resorts, conference centers, vacation rentals, and multi-property groups, says it is critical that hoteliers trust their technology partners, particularly those hosting and protecting their data. The hotel PMS company examines three of the most significant questions operators have about their data in the cloud and how they can take steps to curtail uncertainty.

Is Cloud-Hosted Data Secure?

"Every security system has its strengths and weaknesses, but there are many ways to assess your hotel's vulnerability to intrusions," said Warren Dehan, Maestro president. "Cloud computing's flexibility and accessibility across multiple devices, though useful for hotel operations, can create a menagerie of potential exploits. Hoteliers must ensure they have an adequate plan in place to protect their cloud-based infrastructure and then ensure its cloud security settings are properly configured as early as possible. This is an extremely important

point for independent hoteliers with a self-host or private cloud strategy, or those who often lack the available staff to monitor these settings frequently."

Next, Dehan said operators must take steps to actively prevent internal data from being shared outside of the hotel. This includes adjusting daily activities, such as refusing to share internal links with outside collaborators and efficiently revoking account access for former employees. Management is also encouraged to limit security privileges to specific hotel workers, controlling the number of active accounts capable of being compromised.

"Cloud-based systems are also open to cyber-attacks and malware incursions, and there are a wealth of cybersecurity tips operators can follow to avoid or mitigate the likelihood of such an attack," Dehan said. "Operators should consult their technology partners to identify the clearest strategy for keeping your property's digital identity secure. The most significant red flag a hotelier can watch out for in technology is the lack of an adequate security plan or the inability to articulate such a plan. Providers should be able to tell hoteliers where their servers are located geographically, the details of their redundancy and disaster recovery plans, and outline the level of daily maintenance and support hoteliers should anticipate getting."

Whose Data Is It Anyway?

Hoteliers are actively collecting consumer data from equipped property management, global distributions, revenue management, and other systems — but with so many sources all collecting data for the same goal, who does this data actually belong to?

The more pressing question for operators remains, "What rights do I have to my data?" The answer to this question largely depends on a hotel's contractual agreement with its technology partners. Vendor agreements rarely stipulate ownership of customer or partner data, but this must be clarified contractually so that if the need to extract it in the future is needed, it is an easy task with the vendor's assistance.. Additionally, vendors typically request access to client or customer data to a certain degree to provide functioning cloud service. This can also extend to data usage agreements, whereby technology partners request the right to access client or customer data to gain insights used to improve their services in both quality and consistency.

"Other aspects independent hoteliers must consider as part of a data ownership agreement include an agreement from technology partners to implement security measures in the first place and to commit to protecting data belonging to the property and its guests from access, breach, or loss," Dehan said. "As a final component, independent operators are recommended they specify clear language in the agreement regarding how long technology partners must retain customer and guest data and how it is deleted. This enables operators to walk away from a technology partnership without the fear that their data may be compromised later when the relationship no longer exists."

Are there best practices to follow?

Hotels need technology to remain competitive today, and therefore it is imperative to find a technology partner they trust, particularly independent operators. Operators must also try to understand the shared responsibility model, which impacts every aspect of data usage and security today. As a result, hoteliers have responsibility for data security regarding on-property activities, while technology and cloud service partners are responsible for protecting their networks from outside attacks and ensuring everything is working properly. Operators must clearly outline their responsibilities at the outset of an agreement and properly train workers to comply with these requirements.

“Training is one of the most important best practices hotels can embrace for improving cloud security protocols,” Dehan said. “Considering that most incursions are a result of improperly configured or used equipment, operators should train staff to notice anything out of place and what to do to elevate these concerns. Hotels can also adopt automated solutions designed to prompt workers to follow specific policies or refresh their knowledge.”

Maestro advises hoteliers to conduct a full audit of their potential cloud-based security vulnerabilities, ideally cooperating with their technology partners and an outside firm. This can help locate misconfigured equipment, users with outside access to their data, and other concerns before they become threats. By taking these challenges seriously, hoteliers can protect themselves against data breaches and increase the efficiency of their security systems while gaining access to vital cloud-based operations and management platforms. Protecting a hotel’s data security ultimately improves the staff and guest experience and a hotel’s overall value.

# # #

About Maestro
Maestro is the preferred Web Browser based cloud and on-premises PMS solution for independent hotels, luxury resorts, conference centers, vacation rentals, and multi-property groups. Maestro’s PCI certified and EMV ready enterprise system offers a Web browser version (or Windows) complete with 20+ integrated modules on a single database, including mobile and contactless apps to support a digitalized guest journey as well as staff operations. Maestro’s sophisticated solutions empower operators to increase profitability, drive direct bookings, centralize operations, and engage guests with a personalized experience from booking to check out and everything in between. For over 40 years Maestro’s Diamond Plus Service has provided unparalleled 24/7 North American based support and education services to keep hospitality groups productive and competitive. Click here for more information on Maestro. Click here to get your free PMS Buying guide.

Warren Dehan
Maestro PMS
+1 905-940-1923
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/643939813

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2023 Newsmatics Inc. All Right Reserved.