COVER FEATURE / NOVEMBER 23, 2026

WHEN THE NETWORK BLINKS

Can Modern Travel Survive Its Own Complexity?

Three disruptions in five days exposed the travel industry's dependence on technology nobody notices until it breaks. Now an ambitious new generation of AI promises to keep the machine running. The question is whether it can also teach the machine how to fail.

BY THE INVESTIGATIVE DESK OF THE HOSPITALITY GAZETTE



EDITORIAL ILLUSTRATION

A hotel guest ought to be able to do three things without needing a seminar in distributed computing: make a reservation, get into the room, and go to sleep.

INVESTIGATIONS / COVER FEATURE

That is the entire proposition. All the rest—the loyalty tiers, the apps, the predictive pricing, the promises of seamless arrival—is supposed to make those three things easier. Yet the industry has been quietly reconstructing that simple transaction into a relay race involving identity servers, cloud platforms, telecommunications networks, payment gateways and software providers whose names most guests have never heard.

Usually, it works magnificently. And because it usually works, everyone is tempted to forget how much has to go right.

Then came the middle of November.

On Friday the 13th, a network failure led the Federal Aviation Administration to order a nationwide ground stop. On Monday, November 16, United Airlines delayed departing flights after a technology problem interfered with information flight crews needed before takeoff. On Tuesday, Marriott Bonvoy members found themselves unable to sign in to the company's website and app for hours, while hotel professionals were comparing notes about other technology behaving badly behind the front desk.

Three failures in different organizations and different technical systems. Not a single attack. Not a single broken master switch. Nothing so tidy.

And that, in some ways, is the more uncomfortable story.

The travel economy has become an extraordinary machine for turning intent into movement. It can recognize a passenger, price a seat, assign a room and deliver a digital key before a human employee has introduced themselves. It is also a machine with a great many ways to refuse to cooperate.

For an industry that prides itself on predicting demand down to the last room night, we are remarkably casual about the possibility that the systems managing that demand might disappear precisely when we need them.

The travel industry has built an extraordinary technological machine. But has it built one that can survive its own complexity?

That question is no longer reserved for engineers. The answer is shaping a new race among travel platforms, cloud providers and artificial intelligence companies. Their pitch is dazzling: software that sees trouble coming, finds affected travelers, rearranges itineraries, diagnoses infrastructure problems and perhaps repairs them without waiting for human intervention.

It sounds like the future. It may be part of it. But the real measure of progress won't be how intelligently the system behaves when everything is connected. It will be what remains possible when it isn't.

NOVEMBER 2026

Three disruptions in five days

FRI / NOV 13 **FAA network**	Telecommunications instability led to a nationwide ground stop. The FAA counted 12,462 cancellations that day for all causes.
MON / NOV 16 **United Airlines**	A systems outage delayed departures for more than 90 minutes. Crews reported trouble receiving final aircraft weight information.
TUE / NOV 17 **Marriott Bonvoy**	Website and app sign-ins failed for hours. Marriott confirmed a sign-in issue. The full scope of reported property-level problems remained undetermined.

The incidents were technically independent. See reporting sources [1]–[3].

NOVEMBER 13 / AIR TRAFFIC CONTROL

Friday: The Sky Hits Pause

Air traffic control is not a hotel front desk, and there are excellent reasons its operators cannot improvise through a systems problem the way a resourceful night auditor might. On November 13, the FAA's telecommunications network became unstable as excessive connection attempts flooded infrastructure that supports communications and radar feeds. The agency identified potential sources in Amarillo, Texas, and El Dorado, Arkansas, where contractor L3Harris had been working on a router installation.

According to the FAA's account, the network was receiving roughly 1,000 connection attempts every four to five seconds. Instability affected 17 of the country's 22 en route air traffic control centers. The agency ordered the ground stop at approximately 3:30 p.m. Eastern and reported that air traffic resumed at 8:15 p.m. [1]

The distinction between an unstable system and a completely dead one matters. The FAA said some frequencies and radar feeds remained reliable. Controllers and pilots continued using established safety procedures, and about 3,500 aircraft already airborne landed safely. The decision to restrict departures was a safety measure, not evidence that aircraft had suddenly become impossible to control.

But safety and commercial continuity are two different things. The FAA could protect the aircraft already in the sky while the system of getting the next aircraft into the sky ground to a halt.

By its own count, 12,462 flights were canceled on November 13, although the agency expressly noted that not all cancellations were caused by the ground stop.

The fallout continued as carriers tried to put aircraft, crews and passengers back where their schedules said they belonged. [1]

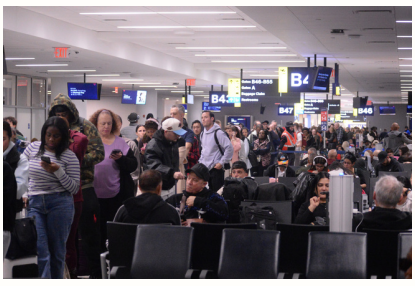
An airline schedule is a particularly unforgiving form of choreography. A plane expected in Chicago must arrive before it can depart for Denver. The crew needs sufficient legal duty time. The next passengers need to be present. The assigned gate needs to be available. One missed movement can ruin several acts of the performance.

Hotel operators know this choreography from the receiving end. An arrival that doesn't arrive is not merely a cell in a reservation report. It may be a guaranteed room that cannot be confidently released, a tour group with an uncertain arrival time, a banquet that doesn't serve the number of guests it expected or a frightened traveler looking for a bed because the flight home never left.

For a hotel near an airport, disruption can bring a sudden rush of distressed demand. At the intended destination, it can produce empty rooms and missed spending. An occupied room at one property may represent a ruined itinerary at another. The RevPAR report does not explain that distinction. It wasn't designed to.

The FAA's preliminary technical findings also dismantled one of the week's more sensational theories. The agency said it had no indication of a cyberattack. The network had stumbled during work on a system already in need of modernization. [1]

It would be comforting to identify a cinematic villain. A malicious mastermind can be caught. Aging infrastructure, imperfect testing and complicated dependencies demand something less gratifying: sustained management.



DOCUMENTARY Travelers fill a gate area at New York’s John F. Kennedy International Airport during the FAA’s nationwide ground stop on November 13, 2026. [01]



DOCUMENTARY Travelers wait near flight-information displays at New York’s John F. Kennedy International Airport during the November 13, 2026, nationwide ground stop. [02]



ARCHIVAL Air traffic controllers work at the FAA’s Washington Air Route Traffic Control Center in this undated archival photograph. [03]

NOVEMBER 16–17 / UNITED AIRLINES AND MARRIOTT BONVOY



ARCHIVAL A United Airlines Boeing 737-800 is parked at a Denver International Airport gate in this June 2014 file photograph. [04]



ARCHIVAL A Marriott Bonvoy sign is shown in this February 2024 file photograph. [05]

Monday: Ready for Takeoff. Waiting on Software.

Three days later, United Airlines provided a different demonstration of the same fundamental truth. Departing flights were delayed while the airline worked through a systems outage. Pilots reported trouble receiving final aircraft weight information used for required takeoff performance calculations. United said the disruption lasted more than 90 minutes; aircraft already in the air and United Express flights were unaffected. The airline found no indication of a cybersecurity incident. [2]

Consider what that means. You can have an aircraft at the gate, fuel in its tanks, a trained crew in the cockpit and passengers who have already endured the boarding process. None of it is enough if the information required to establish safe takeoff performance is unavailable.

The correct decision is not to depart and hope for the best. The correct decision is to wait. That's what happened.

The absurdity is not that United followed safety rules. The absurdity, if there is one, is how thoroughly a modern machine can depend on an apparently mundane piece of information. The weight of an airplane is hardly a new aviation concept. Computing and delivering the number now sits inside a complex digital operation.

The Associated Press reported roughly 600 United delays that evening, while noting it was not clear how many were directly attributable to the outage.

United did not publicly establish the precise technical cause in the reporting reviewed for this feature. [2]

That is enough to understand the lesson without pretending to know which line of code misbehaved. The aircraft did not need to break for the operation to stop.

Tuesday: Trouble Behind the Login

Then Marriott had its turn.

On November 17, users trying to sign in to Marriott.com and the Bonvoy app encountered failures. Reports began climbing around 9:15 a.m. Eastern. By roughly 2 p.m., tests by *Skift* found sign-in working again. Marriott confirmed a problem affecting website and app sign-ins, said it worked with technology partners to restore service, and reported no indication of a cybersecurity cause. [3]

That was the public-facing story. Behind the front desk, the conversation was less tidy.

In accounts shared with *The Hospitality Gazette*, hotel professionals were also describing trouble with operational systems: difficulty viewing night-audit reports, submitting income journals and responding to guest needs. Colleagues raised concerns about PMS, customer-management and accounting functions that appeared unavailable or unreliable. Some of the discussion was plainly alarmed. Anyone who has spent time in hotel operations knows how quickly a bad system day turns into a group conversation nobody particularly wanted to join.

TUESDAY / CONTINUED

These were firsthand industry accounts, not a completed technical postmortem. They don't establish a chain-wide PMS outage, a single common cause or the precise scope of each problem. But they belong in this story for a reason: **the corporate announcement tells you what the company confirmed; the operators tell you what their workday felt like.**

And those are not always the same account.

A guest sees a stalled login, an unavailable mobile check-in or a key feature that won't cooperate. An operator may be trying to finish the night audit, retrieve information, send the income journal and answer a guest's question while one or more systems refuse to behave. The guest-facing inconvenience and the back-office friction are different problems. Both can make the operation feel considerably less seamless than the brochure promised.

We should not pretend that every reported problem came from Marriott's authentication failure. Equally, we should not mistake the limits of a public corporate statement for proof that nothing else was happening at individual properties. A hotel is not operated exclusively through the Bonvoy app, and the people trying to run one rarely experience technology as neatly separated product categories.

This is where the industry's obsession with frictionless service meets a rather stubborn reality. The polished digital entrance matters. So do the unglamorous systems that reconcile the day's business and tell employees what's happening inside their own building. Guests notice the first failure immediately. Managers may spend hours untangling the second.

And when either one misbehaves, the humble front desk—so often portrayed as the antique technology awaiting disruption—still has to solve the problem standing in front of it.

Seamless, Until It Isn’t

These three incidents were not one cascading technical failure. An FAA communications problem did not cause United's application outage, and United did not knock out Marriott's logins. Their connection is structural rather than causal.

Each exposed how much of a supposedly physical service now depends on information arriving from somewhere else, in the right form, at the right time.

A passenger does not buy a successful weight-and-balance calculation. The passenger buys transportation. A traveler doesn't reserve a collection of database records. The traveler buys a room. Nobody packs for a vacation imagining that the highlight will be a troubleshooting conversation about single sign-on.

Yet the industry delivers its physical promises through an ever more intricate procession of digital permissions.

That architecture offers enormous advantages. Central systems can manage global inventory, keep prices aligned, reduce repetitive work, identify fraud and support travelers in ways the old handwritten ledger never could. The nostalgic argument that hotels should abandon their clouds and return to filing cabinets is nonsense.

The argument worth having is about what we have traded away for that efficiency—and whether we have bothered to buy enough resilience in return.

There is a difference between a system designed to be available and a business designed to remain useful when the system is unavailable. Availability is an engineering ambition. Continuity is an operating discipline. The first asks whether a platform is working. The second asks whether a guest can still be served.

That distinction points directly toward what the technology industry is building next.

The Machines That See Trouble Coming

On November 16, Sabre announced a new generation of proactive, event-driven travel APIs and previewed a travel integration for xAI's Grok Bot. The company described tools that could recognize flight disruptions, identify affected travelers and push information into agency systems or connected AI agents without waiting for someone to start another search. [4]

This is a meaningful shift. Much travel software is transactional: ask a question, receive an answer, make a booking. Event-driven systems can respond to changed conditions. If a flight is canceled, the software can surface alternatives while a traveler is still trying to understand what happened.

Sabre outlined different levels of response, from alerting a human advisor to presenting a policy-compliant option for traveler approval, and potentially allowing an authorized agent to act. The technology is entering a landscape of beta releases, previews and staged deployments. That is not the same thing as a demonstrated system that automatically books a particular passenger into a particular hotel room whenever an aircraft diverts.

Still, the commercial implications are hard to miss. Who controls the customer relationship when the traveler no longer searches hotel websites but delegates a problem to an AI agent? Who receives the booking? Who decides which property is offered first? Who pays the intermediary that made the choice?

Hotel brands spent years persuading guests to book directly, download the app and enter the loyalty ecosystem. An intelligent travel agent with access to competing inventory may not have much sentimental attachment to those campaigns. It may care about price, policy, proximity, availability and whether the supplier can actually complete the transaction.

The next fight over hotel distribution may be less about whose website gets the click and more about whose inventory gets selected by software making the click unnecessary.

That isn't proof that hotel brands will lose control of distribution. It is a reason they should be paying close attention.



ILLUSTRATIVE Self-service check-in and baggage-drop kiosks at Wuhan Tianhe International Airport, photographed in October 2020. [06]

Amadeus is moving into the same territory from another angle. Its Max for Travelers initiative combines a conversational travel assistant with orchestration and access to airline systems. The first available use case centers on voluntary rebooking, with additional booking and disruption-recovery capabilities planned. Its research on the intelligent journey argues that the next competitive prize may be coordinating the traveler across airlines, hotels, payments, identity and servicing. [5]

Imagine the useful version. A delayed flight is recognized before a traveler gets to the counter. The traveler receives options that actually reflect company policy or personal preferences. An airline, hotel and ground-transport provider exchange enough information to prevent three separate customer-service arguments.

Now imagine the less useful version: five supposedly intelligent agents disagreeing about whether the traveler has a confirmed reservation while all five confidently claim the situation is under control.

Interoperability is the unglamorous word at the center of this revolution. An AI agent can be brilliant at language and still be helpless without accurate data, authorized access and systems that accept the transaction it wants to perform.

A fluent explanation of a canceled flight is not a replacement flight.

AI Enters the Engine Room

The travel platforms aren't alone. The cloud companies that host much of the digital economy are teaching software to investigate and respond to infrastructure trouble.

Microsoft's Azure SRE Agent can examine logs and metrics, investigate incidents, suggest remedies and, when configured with suitable permissions, perform remediation actions. Amazon Web Services has connected its Resilience Hub with AWS DevOps Agent so infrastructure teams can assess failure scenarios, review tests and investigate recovery behavior. [6][7]

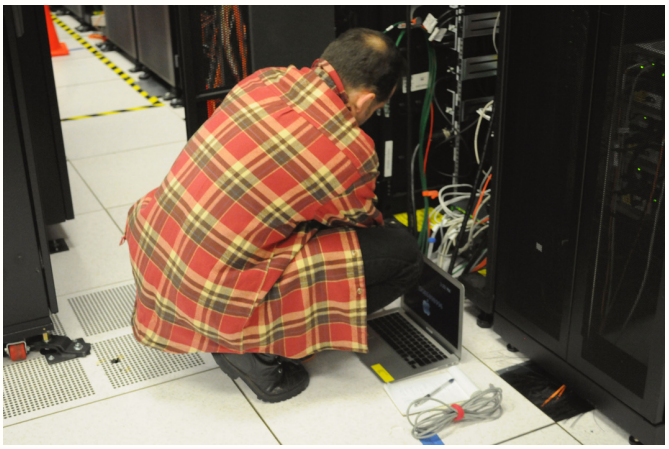
This is not just another customer-service chatbot with a different logo. Site reliability engineering is concerned with what keeps the service running: failed dependencies, overloaded resources, unsuccessful deployments, slow recovery and the messy interactions that arise in real computing environments.

A capable agent that can correlate signals and investigate possible causes could give technical teams something precious during an outage: a head start. An even more capable system might execute a tested response quickly enough that many customers never notice the failure.

That is a serious achievement worth pursuing.

But the promise comes with its own engineering trap. An automatic fix can also be an automatic mistake—delivered at machine speed.

During the November 12 Microsoft 365 disruption, a latent software defect combined with reduced capacity, traffic changes and peak demand. Microsoft's post-incident report describes how automated redistribution of traffic to remaining servers expanded and accelerated the impact after affected gateways became unavailable.



ILLUSTRATIVE A technician works with a laptop at a server rack at the National Energy Research Scientific Computing Center in this October 2011 photograph. [07]

Microsoft said the incident was not caused by AI tooling. [8]

That last point is important. The event does not prove AI recovery systems are dangerous. It demonstrates that automation itself can amplify the wrong assumption. If the supposedly healthy backup environment cannot handle the traffic sent to it, failover can turn one problem into several.

Now add autonomous AI to that picture. It must not merely know how to act. It must know when *not* to act, which changes require human permission, how to reverse an unsuccessful intervention and how to keep one bad decision from spreading.

An industry that has already learned to turn a minor configuration mistake into a national headline should perhaps be selective about giving software the keys to every control room.

The Art of Failing Gracefully

The most encouraging resilience development may be less glamorous than a fully autonomous AI agent.

Oracle Hospitality documents a Reservation Degraded Mode in OPERA Cloud Distribution. For supported reservation flows through the Oracle Hospitality Integration Platform, the distribution layer can continue accepting certain bookings when an OPERA Cloud Property or Central system is temporarily unavailable. Transactions are queued and reprocessed after connectivity is restored. The feature has defined limitations, including exclusions for some channels. [9]

This is not an offline front desk. It doesn't mean a desk clerk can complete every check-in without the cloud, and it doesn't solve every question of guest identity, payment, inventory or room access.

It is, however, a practical expression of an excellent principle: **when one part of the system fails, preserve whatever useful work can safely continue.**

Engineers call that graceful degradation. Hoteliers might call it common sense with better documentation.

The principle deserves far more attention than it receives. A property that cannot reach its central server may still need a trustworthy list of expected arrivals, current occupancy, clean-room status and authorized ways to issue keys. But those capabilities must be designed, secured and reconciled—not conjured from a manager's memory in the middle of a sold-out night.

A separate firsthand account provided to *The Hospitality Gazette* illustrates the stakes. During a Hilton PEP outage at an Ohio hotel, the general manager described staff relying on an earlier guest ledger and housekeeping boards to identify available rooms, then escorting guests using a master key. That event was not the Marriott sign-in incident. It was an example of a more extensive property-system interruption—and of how rapidly the burden shifts to employees when the normal information flow disappears. [10]



ILLUSTRATIVE An electronic lock and privacy notice on a hotel room door, photographed in April 2012. [08]

The important story isn't one Ohio hotel. It's an international industry that has grown comfortable discussing cloud uptime while too often treating local continuity as an afterthought.

A resilient platform can queue transactions and restore data later. A resilient hotel must also know what to do during the interval. These are not competing ambitions; they are different pieces of the same operating promise.

There are complications. Local copies of guest records create security and privacy obligations. Offline payments involve real authorization risk. Room assignments can conflict with bookings arriving through other channels. Digital credentials have to be validated without creating a security shortcut. Reconciliation after an outage is not an administrative footnote—it is how the property prevents tomorrow's surprise double-booking from becoming the next crisis.

None of this is an argument against continuity. It is an argument for building continuity properly.

When the Brand Owns the System, Who Owns the Mess?

Now we reach the part of the conversation where technology turns into money, and the room becomes considerably quieter.

In franchised lodging, the brand often establishes required technology standards while an independently owned property carries much of the immediate responsibility for delivering the stay. The specific rights, fees, obligations and remedies differ by brand and contract, but the commercial tension is plain enough.

A corporate platform can determine what systems a hotel must use. The hotel still has to explain to the guest why those systems aren't working.

When software functions as advertised, property owners and management companies may enjoy faster transactions, better revenue intelligence and less repetitive work. When it fails, the expenses can arrive in much less glamorous forms: overtime, manual processing, extra service recovery, delayed transactions and staff diverted from other duties.

The crucial question is not whether every franchisor must automatically compensate every owner for every error. That would turn a complicated contractual problem into a slogan. The question is whether the economics of mandated technology reward not only efficiency and adoption but also reliability, transparency, meaningful contingency capability and recovery speed.



ILLUSTRATIVE A hotel reception counter and seating area in a January 2019 file photograph. [09]

Consider the operating reality. A hotel is evaluated relentlessly on guest satisfaction, staffing productivity and financial performance. It may be required to use a prescribed platform without being able to choose the architecture behind it. If that platform fails, the property cannot defer the guest experience until a technical incident has been closed.

Owners are entitled to ask what resilience they are purchasing along with the software. Managers are entitled to ask what they are supposed to do when it disappears. Employees are entitled to procedures that amount to more than finding the most experienced person on shift and hoping they remember how the old system worked.

And guests are entitled to receive the hospitality that was sold to them, whether or not the server has decided to participate.

Hospitality risk & vulnerability matrix

Qualitative summary based on the reporting and continuity measures discussed in this feature.

DEPENDENCY	OPERATIONAL EXPOSURE	CONTINUITY MEASURE
Airspace and dispatch	Departures can stop when controllers lose reliable feeds or crews lack required flight data.	Use established safety procedures and coordinate traveler recovery.
Cloud and sign-in	Account access or property workflows can become unavailable when a central service fails.	Plan local continuity for essential work and reconcile transactions after service returns.
AI-mediated booking	Agents depend on accurate data, authorized access and systems that can complete the transaction.	Define approval limits, fallback options and what an agent can safely do.
Front desk and room access	Employees may need to verify arrivals, room status and access when a property system is down.	Maintain secure access to current information and authorized ways to issue keys.

The Next Luxury Is Reliability

The industry's future technology will be evaluated partly by how much it can automate. It should also be evaluated by how elegantly it handles the moment automation becomes unavailable.

A sophisticated resilience architecture needs several layers working together. It needs awareness of operating conditions and the ability to recognize trouble early. It needs intelligent coordination when disruptions affect travel plans. It needs engineering safeguards that prevent automated recovery from magnifying the damage. It needs independent continuity for essential tasks where that is technically and legally appropriate. And it needs a disciplined way to reconcile everything when the primary systems return.

Not every hotel needs its own miniature data center. Not every reservation belongs in an offline cache. Not every AI recommendation should become an automatic action. The point is to match contingency capability to the actual business consequences of losing a dependency.

Consider how different the industry could become if resilience were part of product design rather than an appendix in the disaster-recovery binder.

A travel agent could know about a canceled flight early enough to offer workable alternatives. A hotel could receive credible arrival intelligence without guessing who might appear at midnight. A technical operations team could identify a failing dependency before it knocks out the entire service. A front desk could retain secure access to essential, up-to-date local information even during a central outage, where its systems support that capability. And when the network returned, the machines could help reconcile what happened rather than forcing somebody to untangle it manually over the next three shifts.

That is a much more consequential vision of AI than a chatbot answering what time breakfast ends.

It's also considerably harder to build. It requires cooperation among competitors, contractual clarity, reliable interfaces, security discipline and a willingness to spend money on capabilities that may sit quietly for years before proving indispensable.

Resilience is not as photogenic as a new guest-facing feature. It does not look particularly impressive in a product demo when the internet is working and everyone has remembered their password. The payoff is the day when something breaks and the hotel simply continues serving people.

In hospitality, that should count as a competitive advantage.

Teach the Machine to Take a Hit

The November disruptions offer no reason to retreat from technology. The FAA used safety procedures to bring aircraft down safely. United delayed departures rather than operate without necessary information. Marriott restored its sign-in service. These are not arguments that modern travel is collapsing; they are reminders that reliability demands continuous work.

Nor should the rush toward intelligent recovery be dismissed as marketing theater. Sabre and Amadeus are developing ways to respond to travel disruptions. Microsoft and AWS are building tools for diagnosing infrastructure faults. Oracle has documented a mechanism for continuing selected reservation transactions through certain downstream outages. The field contains genuine work, genuine ambition and plenty of unfinished business.

But there is a distinction between making a machine cleverer and making the business it serves more dependable.

A clever machine can tell you why the guest cannot check in. A dependable operation can still find an authorized, safe way to put that guest in a room.

A clever machine can notice that a flight has been canceled. A dependable travel system can help the traveler work out what happens next.

A clever machine can identify the failed component. A resilient design can prevent that component from taking everything else down with it.

The next era of hospitality technology should make room for all three—and resist the temptation to declare victory because the first has become very impressive.

We have spent decades teaching the travel machine to remove friction. Now we need to teach it to absorb shock.

Because when the network blinks, the obligation doesn't.

The room still has to be ready. The flight still has to be safe. And somebody still has to open the door.



ARCHIVAL A hotel concierge holds up a room key while speaking on the telephone in Rome in this August 2006 file photograph. [10]

Source register

1. Federal Aviation Administration, **“Nationwide Ground Stop: Questions and Answers,”** November 15, 2026. https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers

2. Associated Press, **United Airlines system outage reporting**, November 16–17, 2026. https://apnews.com/article/5a5e5f75bb07f11ffb8750901f0076ff

3. Sean O'Neill, *Skift*, **“Marriott Bonvoy Sign-Ins Were Down for Hours,”** November 17, 2026; *Hotel Dive*, November 18–19. https://skift.com/2026/11/17/marriott-bonvoy-sign-ins-were-down-for-hours-disrupting-mobile-keys/ ; https://www.hoteldive.com/news/marriott-technology-disruption/875122/ . Supplementary property-level accounts: contemporaneous colleague discussions shared with *The Hospitality Gazette* describing trouble accessing night-audit reporting, submitting income journals and managing guest-service needs; independently established technical scope remains undetermined.

4. Sabre Corporation, **“Sabre Accelerates Agentic Travel Leadership…”**, November 16, 2026. https://sabre.gcs-web.com/node/20256

5. Amadeus, **“Amadeus Max for Travelers: Agentic AI for Airline Customer Service,”** 2026; **“Would you let AI manage your next trip?”**, November 16, 2026. https://amadeus.com/en/blog/articles/amadeus-max-travelers-agentic-ai-airline-support ; https://amadeus.com/en/newsroom/press-releases/intelligent-journey-2032-ai-travel

6. Microsoft Learn, **“Azure SRE Agent general FAQ.”** https://learn.microsoft.com/en-us/azure/sre-agent/faq

7. Amazon Web Services, **“Launch AWS DevOps Agent to review findings and test results from AWS Resilience Hub,”** October 15, 2026. https://aws.amazon.com/about-aws/whats-new/2026/10/aws-devops-agent-test-results-aws-resilience-hub/

8. Microsoft 365, **Post-incident report EX1550543/MO1550821**, November 2026 (public copy). https://www.365fanatic.com/wp-content/uploads/2026/11/postincidentreport-mo1550821.pdf

9. Oracle Hospitality, **“Updated Reservation Services to Support Reservation Degraded Mode,”** OPERA Cloud Distribution documentation. https://docs.oracle.com/en/industries/hospitality/opera-cloud-distribution/25.5/ohdrn/updated_reservation_services_to_support_reservation_degraded_mode.htm

10. *The Hospitality Gazette*, **Primary source interview record: Hilton PEP outage, Xenia, Ohio**, November 22, 2026; provided in the research dossier accompanying the submitted manuscript.

Editorial record: Publicly confirmed Marriott sign-in disruption and contemporaneous operator accounts are distinguished in the reporting. The Xenia Hilton PEP account concerns a separate incident and appears only as a brief supporting example.

Photography Credits & Sources

Photographs are reproduced under their listed licenses or public-domain status. Third-party rights remain with their respective holders.

01 / DOCUMENTARY

A terminal on hold

“JFK during 2026 FAA ground stop - 7” — Sashimi-b / Wikimedia Commons. Full frame.

CC BY-SA 4.0
commons.wikimedia.org/wiki/Special:PermanentLink/1301589176
creativecommons.org/licenses/by-sa/4.0/

02 / DOCUMENTARY

Waiting by the flight displays

“JFK during 2026 FAA ground stop - 1” — Sashimi-b / Wikimedia Commons. Full frame.

CC BY-SA 4.0
commons.wikimedia.org/wiki/Special:PermanentLink/1301101410
creativecommons.org/licenses/by-sa/4.0/

03 / ARCHIVAL

Inside air traffic control

“AirTraffic-8” — Federal Aviation Administration / Wikimedia Commons. Full frame.

U.S. public domain
commons.wikimedia.org/wiki/Special:PermanentLink/1169135461
uscode.house.gov/us/usc/t17/s105/

04 / ARCHIVAL

United aircraft at the gate

“United Airlines Boeing 737 at Gate B31” — DReifGalaxyM31 / Wikimedia Commons. Full frame.

CC BY 3.0
commons.wikimedia.org/wiki/Special:PermanentLink/1284831320
creativecommons.org/licenses/by/3.0/

05 / ARCHIVAL

The loyalty sign-in

“Marriott Bonvoy” — Schumi4ever / Wikimedia Commons. Full frame.

CC BY-SA 4.0
commons.wikimedia.org/wiki/Special:PermanentLink/1206879381
creativecommons.org/licenses/by-sa/4.0/

06 / ILLUSTRATIVE

Self-service departures

“Self Check-in and Baggage Drop Kiosks at Wuhan Tianhe Airport” — Zheng Zhou / Wikimedia Commons. Full frame.

CC BY-SA 4.0
commons.wikimedia.org/wiki/Special:PermanentLink/1189681536
creativecommons.org/licenses/by-sa/4.0/

07 / ILLUSTRATIVE

The work behind the network

“Technician with laptop working on server rack at NERSC” — Derrick Coetzee / Wikimedia Commons. Full frame.

CC0 1.0
commons.wikimedia.org/wiki/Special:PermanentLink/1173181278
creativecommons.org/publicdomain/zero/1.0/

08 / ILLUSTRATIVE

Access at the room door

“HotelPrivacyAMS 20120402 080145” — Elgaard / Wikimedia Commons. Full frame.

CC BY-SA 3.0
commons.wikimedia.org/wiki/Special:PermanentLink/1181592956
creativecommons.org/licenses/by-sa/3.0/

09 / ILLUSTRATIVE

Where the guest turns

“Hotel Reception” — The Down Town Hotel / Wikimedia Commons. Full frame.

CC BY-SA 4.0
commons.wikimedia.org/wiki/Special:PermanentLink/1270140308
creativecommons.org/licenses/by-sa/4.0/

10 / ARCHIVAL

Somebody still has to open the door

“A hotel concierge handing room keys, Rome - 3566” — Jorge Royan / Wikimedia Commons. Full frame.

CC BY-SA 3.0
commons.wikimedia.org/wiki/Special:PermanentLink/1250928725
creativecommons.org/licenses/by-sa/3.0/

Cover artwork • Editorial illustration supplied for this feature.