CEQUENCE

Vacation Mode ON, Scam Mode OFF

Stay Cyber-Safe on Your Travels

As travel and hospitality companies prepare for peak seasons like vacations and holiday periods, the increase in travelers also brings a rise in cyber threats. Cybercriminals use the high traffic volume as cover for their attacks. For travelers, this means staying vigilant to protect your personal information and trip details. For travel companies, it's crucial to enhance security measures to safeguard customer data and maintain trust. By staying informed and proactive, both sides can ensure that the excitement of the season doesn't give way to a cyber nightmare.

We analyzed the top 10 travel and hospitality companies with Cequence API Spyder to discover at-risk public APIs, hosting providers, security issues and more, and here's what we found:

Security

Cequence has observed across industries that when there's a peak season for the industry, such as vacation and holiday season for travel and hospitality, bad actors will use the increased traffic as a cover for their attacks. The **DNS** (increased queries are consistent with increased traffic) and **DDoS** (attacks increase during times of increased traffic) data lends credence to that observation.

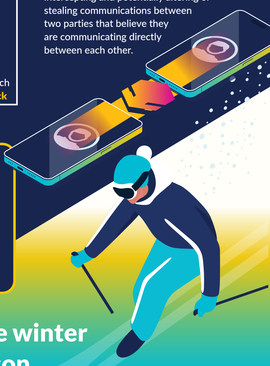
While all companies had serious, public-facing vulnerabilities, these are fixable issues and should be addressed.

All 10 companies had serious, public-facing vulnerabilities

4 companies had

91% of the total serious vulnerabilities, most of which would allow an **MitM attack**

Man-in-the-Middle (MitM) Attacks
are cyberattacks where an attacker is secretly intercepting and potentially altering or stealing communications between two parties that believe they are communicating directly between each other.



FEWEST VULNERABILITIES
These companies had the fewest public-facing vulnerabilities

GOLD	SILVER	BRONZE
Skyscanner	Kayak	Orbitz

October begins the winter travel holiday season,

and that's also when the most DNS queries and DDoS attacks occurred last year. November 2023 showed the highest number of DDoS attacks against the travel industry for the entire year, almost double the second-highest month (October 2023).

Largest DDoS Attack	Longest DDoS Attack	Average Duration
1.03 Gbps	7.43 Hours	15.18 Mins

Governance & Compliance

PCI DSS is a security standard that governs handling of credit card information. PCI DSS v4.0 has several new requirements that go into effect April 1, 2025, so now is the time for businesses handling credit card data to ensure their compliance.

4.1.25 **New Payment Card Industry Requirements**

These travel and hospitality companies all do significant business online, and in the process, receive credit card information from customers. It's critical that these companies ensure they are compliant with PCI DSS and are protecting their customers' sensitive information.

Cloud Sprawl

"Cloud sprawl" is uncontrolled expansion of an organization's cloud infrastructure, often caused by inorganic growth (acquisitions), siloed departments, or lack of a cohesive and defined cloud strategy. Since the provider's systems are publicly accessible, it's important for organizations to be aware of what's hosted and where it is.

5 to 21
Number of hosting providers used by each of the travel companies

MOST POPULAR CLOUD PROVIDER

GOLD	SILVER	BRONZE
Amazon Web Services	Google Cloud Platform	Microsoft Azure

Unintentionally Public Servers

Servers that are normally accessible only to internal company users, such as development servers or internal application servers, are sometimes made publicly accessible. It's possible these are known systems and the IT team is aware of them, but frequently dev or QA teams will temporarily deploy a test system and neglect to decommission it when its task is complete. These servers are typically unmonitored and unmanaged and can provide attackers a way in, so it's important to continuously discover your public-facing attack surface and be aware of the non-production and internal app servers that are publicly accessible.

8 of the 10 companies had publicly-accessible non-production or internal application servers

One site had over

300 publicly-accessible non-production or internal application servers

FEWEST ACCESSIBLE NON-PRODUCTION OR INTERNAL APPLICATION SERVERS

GOLD	SILVER	BRONZE
Orbitz & Travelocity	Kayak	Skyscanner

Ready for Takeoff?

Keep Your Travel Plans Smooth and Secure

As you pack your bags and prepare for exciting adventures, remember that a safe trip is the best trip. For travelers, staying vigilant and safeguarding your digital presence ensures your holiday is as enjoyable as it is stress-free. For travel companies, continuing to prioritize security helps protect your clients and fosters trust in your services. Let's work together to keep every journey secure and memorable. Travel smart, stay protected, and make the most of every moment. Bon voyage!

Travel, hospitality, and other enterprises - try a free API security assessment today:
www.cequence.ai/assessment/

DNS and DDoS data provided by Vercara.

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai