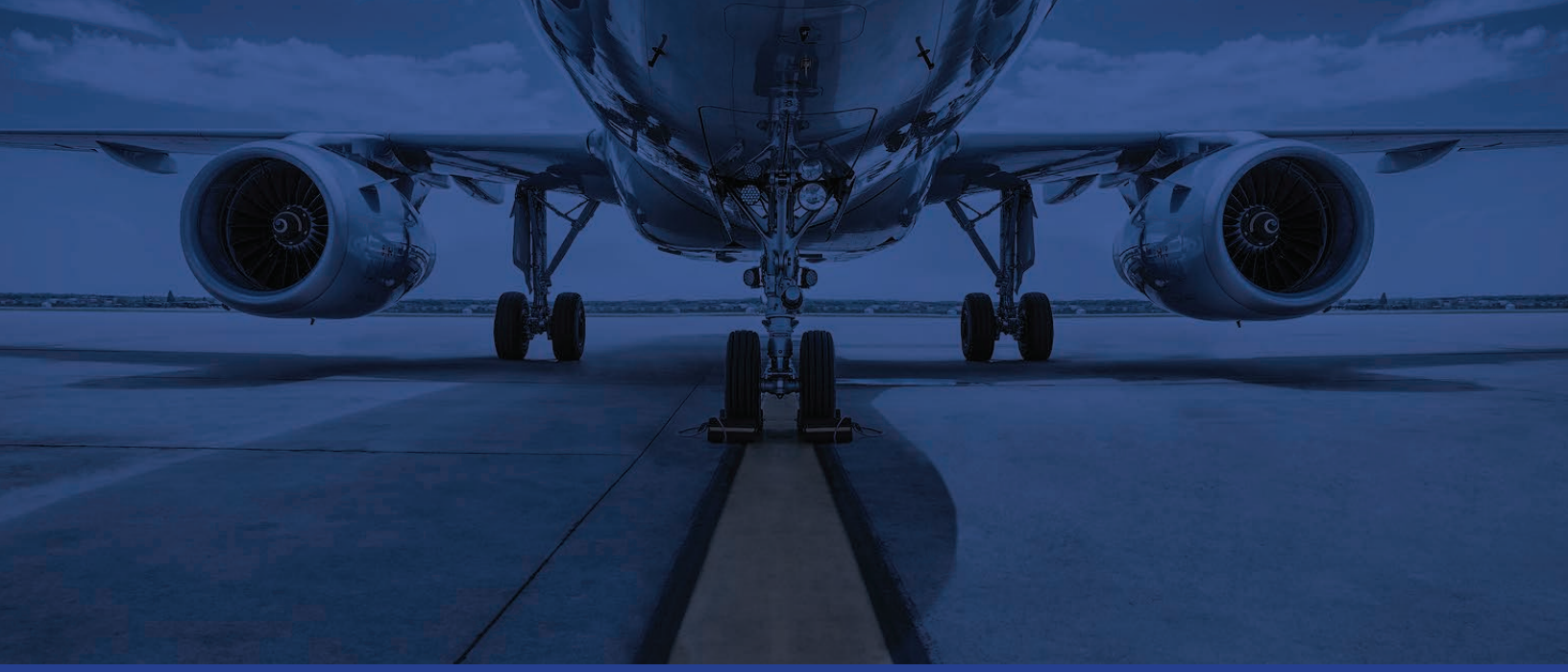
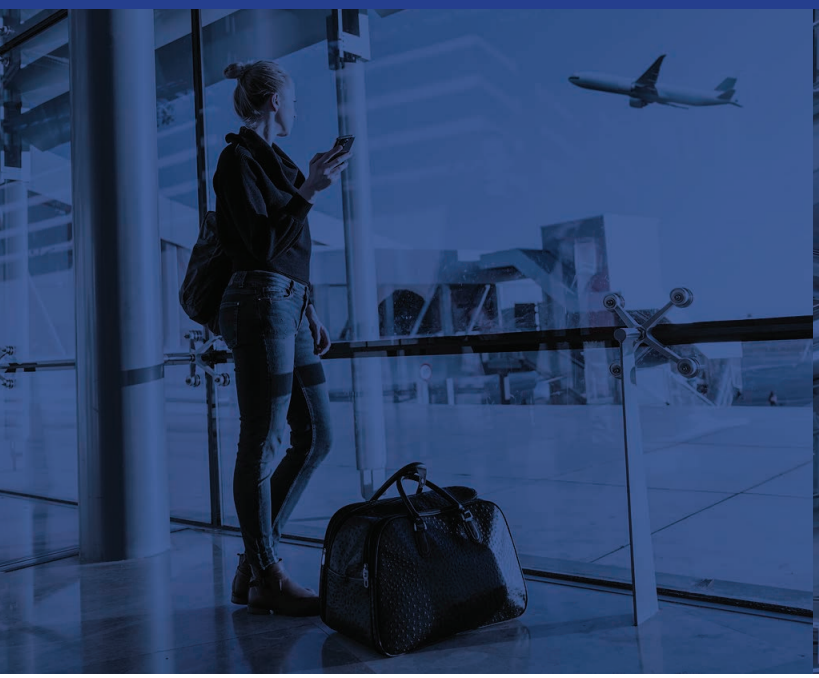


ATTENTION
ALL PASSENGERS:

Airport Networks Are Putting Your Devices & Cloud Apps at Severe Risk



CORONET

TABLE OF CONTENTS

EXECUTIVE SUMMARY

According to the Bureau of Transportation Statistics, U.S.-based airlines transported more than 746 million passengers to and from airports across the country in 2017. When combined with international-based carriers, close to one billion people made their way through one or more of America's 5,000 airports designated for commercial flights during a single calendar year.

In an attempt to maximize the traveler experience, the vast majority of airports now provide free or low-cost Wi-Fi for passengers to connect to for work, entertainment or a combination thereof.

Unfortunately, Wi-Fi security is often sacrificed by airport operators in exchange for consumer convenience, leaving networks unencrypted, unsecured or improperly configured. After all, it wasn't until February 2018 that Americans finally started to rank cybersecurity as more important than expediency (according to an IBM study).

Even for those airports that do prioritize security, attack techniques such as the Key Reinstallation Attack (KRACK), which can break the WPA2 protocol to capture and/or expose information shared over public and private Wi-Fi, presents significant risk to passengers in transit.

This report identifies the current cyber risk landscape at the top *45 busiest U.S. airports. Its purpose is to help educate all travelers on:

- Specific airport risk level based on network threats and device vulnerabilities.
- How insecure or deceptive airport networks can drive the exploitation of vulnerable endpoint devices, subsequently compromising the systems, files and cloud apps that devices connect to.
- How Coronet's FREE SecureCloud platform can help business travelers automatically identify network threats at airports, thereby protecting their cloud apps and data from compromise, unauthorized access and malware and ransomware spread.

**Data for Honolulu's Inouye International Airport and Oakland International Airport was not available.*

THE CYBER RISK TO BUSINESS TRAVELERS

For attackers, it is infinitely easier to access and exploit data from devices connected to Wi-Fi in an airport than it is to do so within the confines of a well-protected office. In fact, the lax cybersecurity posture at most airports has created an environment in which adversaries can utilize insecure public Wi-Fi as the attack vector to introduce a plethora of advanced network vulnerabilities, such as captive portals (AKA Wireless phishing), Evil Twins, ARP poisoning, VPN Gaps, Honeypots and compromised routers. Any one of these network vulnerabilities can empower an attacker to obtain access credentials to Microsoft Office 365, G-Suite, Dropbox and other popular cloud apps; deliver malware to the device and the cloud, and snoop and sniff device communications.

In many instances, business travelers connected to risky airport networks unintentionally share important information about their cloud-based-apps with adversaries. Such compromise can trickle down through entire organizations, leading to operational disruption, financial losses and even reputational harm, among other damages. While large enterprises are equipped to recover from such events, many mid-market and small businesses are ill prepared to remediate and regain business continuity with any haste. In fact, six out of ten small businesses hit with a cyberattack go out of business within six months of the breach.

METHODOLOGY

To identify the airports with the greatest cyber risk, Coronet collected data from more than 250,000 consumer and corporate endpoints that traveled through America's 45 busiest airports over the course of five months. Coronet then analyzed the data, which consisted of both device vulnerabilities and Wi-Fi network risks captured from our threat protection platform. Following the completed analysis, the data was combined and standardized to compile the Coronet Threat Index for each airport.

Device Vulnerabilities – Coronet assigned each endpoint device a vulnerability score based on weighting its security posture factors, including:

- Active and updated anti-malware
- Active and updated firewalls
- Password protection for device/OS access
- Trusted OS (i.e. from legit source and not rooted/jailbroken)
- Trusted apps
- Disk/storage encryption
- Privileged user account and permissions

The greater the vulnerabilities that a device had, the higher the vulnerability score it was assigned. For each airport, we averaged the device vulnerability score for all devices within one kilometer. The Airport Device Vulnerability Score has a risk range of 1 to 5 (the higher the score the higher the risk) that reflects the average vulnerability level of endpoint devices in the airport.

Network Risk Score - Coronet SecureCloud scanned connected and neighboring Wi-Fi networks, using proprietary algorithms to assess network risk score, denoting the probability of an attacker on these networks. This risk score was used for conditional access to corporate services. The Airport Network Risk Score has a risk range of 1 to 5 (the higher the score the higher the risk) and takes into account the chance of connecting to a risky Wi-Fi networks in the immediate vicinity of and the individual risk within each specific network.

Based on our analysis, it is our opinion that an acceptable risk level is below 6.5, and any score higher represents unacceptable exposure.

TOP 10 MOST VULNERABLE AIRPORTS

DMA	CODE	CITY	THREAT INDEX SCORE
San Diego International Airport	SAN	San Diego	10
John Wayne Airport-Orange County Airport	SNA	Santa Ana	8.7
William P Hobby Airport	HOU	Houston	7.5
Southwest Florida International Airport	RSW	Fort Myers	7.1
Newark Liberty International Airport	EWR	Newark	7.1
Dallas Love Field	DAL	Dallas	6.8
Phoenix Sky Harbor International Airport	PHX	Phoenix	6.5
Charlotte Douglas International Airport	CLT	Charlotte	6.4
Detroit Metropolitan Wayne County Airport	DTW	Detroit	6.4
General Edward Lawrence Logan International Airport	BOS	Boston	6.4

NATIONAL AIRPORT WI-FI NETWORK OVERVIEW

- Probability of connecting to medium risk network: **1%**
- Probability of connecting to high risk network: **0.6%**

5

NEWARK LIBERTY INTERNATIONAL AIRPORT

- Probability of connecting to medium risk network: 1%
- Probability of connecting to high risk network: 0.6%

4

SOUTHWEST FLORIDA INTERNATIONAL AIRPORT (FT. MYERS)

- Probability of connecting to a medium risk network: 19%
- Probability of connecting to high risk network: 6%

3

HOUSTON WILLIAM HOBBY INTERNATIONAL AIRPORT

- An attacker on a Wi-Fi network named "SouthwestWiFi" performed an attack on SSL/HTTPS traffic.
- Probability of connecting to medium risk network: 21%
- Probability of connecting to high risk network: 6%

2

JOHN WAYNE AIRPORT-ORANGE COUNTY AIRPORT

- Probability of connecting to a medium risk network: 26%
- Probability of connecting to high risk network: 7%

1

SAN DIEGO INTERNATIONAL AIRPORT

- An Evil Twin Wi-Fi access point with the name "#SANfreewifi" was used at the San Diego international airport, running an ARP Poisoning attack.
- Probability of connecting to a medium risk network – 30%
- Probability of connecting to a high-risk network – 11%

TOP 10 LEAST VULNERABLE AIRPORTS

DMA	CODE	CITY	THREAT INDEX SCORE
Tampa International Airport	TPA	Tampa	5.3
Miami International Airport	MIA	Miami	5.3
Lambert St Louis International Airport	STL	St. Louis	5.3
Kansas City International Airport	MCI	Kansas City	5.2
Louis Armstrong New Orleans International Airport	MSY	New Orleans	5.2
San Antonio International Airport	SAT	San Antonio	5.2
Washington Dulles International Airport	IAD	Washington	5.1
Nashville International Airport	BNA	Nashville	5.1
Raleigh Durham International Airport	RDU	Raleigh-Durham	4.9
Chicago Midway International Airport	MDW	Chicago	4.5

COMPLETE RANKINGS (WORST TO BEST)

TAKING ACTION

RED: Above 5.9 – Never connect without proper protection for your devices. Use a security solution that can identify both malicious networks and attackers and can offer full protection, for your cloud services, devices and cloud apps are at severe risk.

ORANGE: Between 5.4 and 5.9 – Download device protection that can identify malicious networks and attackers for personal use, and connect only to networks that you identify and know.

YELLOW: Below 5.4 – Connect carefully only to a networks that you can identify and know.

DMA	CODE	CITY	THREAT INDEX SCORE
San Diego International Airport	SAN	San Diego	10
John Wayne Airport-Orange County Airport	SNA	Santa Ana	8.7
William P Hobby Airport	HOU	Houston	7.5
Southwest Florida International Airport	RSW	Fort Myers	7.1
Newark Liberty International Airport	EWR	Newark	7.1
Dallas Love Field	DAL	Dallas	6.8
Phoenix Sky Harbor International Airport	PHX	Phoenix	6.5
Charlotte Douglas International Airport	CLT	Charlotte	6.4
Detroit Metropolitan Wayne County Airport	DTW	Detroit	6.4
General Edward Lawrence Logan International Airport	BOS	Boston	6.4
Orlando International Airport	MCO	Orlando	6.3
Portland International Airport	PDX	Portland	6.3
McCarran International Airport	LAS	Las Vegas	6.2
Sacramento International Airport	SMF	Sacramento	6.2
La Guardia Airport	LGA	New York	6.2
Austin Bergstrom International Airport	AUS	Austin	6.1
George Bush Intercontinental Houston Airport	IAH	Houston	6.1
Seattle Tacoma International Airport	SEA	Seattle	6

COMPLETE RANKINGS (WORST TO BEST)

DMA	CODE	CITY	THREAT INDEX SCORE
Chicago O'Hare International Airport	ORD	Chicago	5.9
San Francisco International Airport	SFO	San Francisco	5.8
Indianapolis International Airport	IND	Indianapolis	5.7
Cleveland Hopkins International Airport	CLE	Cleveland	5.7
John F Kennedy International Airport	JFK	New York	5.7
Fort Lauderdale Hollywood International Airport	FLL	Fort Lauderdale	5.7
Dallas Fort Worth International Airport	DFW	Dallas-Fort Worth	5.7
Hartsfield Jackson Atlanta International Airport	ATL	Atlanta	5.6
Norman Y. Mineta San Jose International Airport	SJC	San Jose	5.6
Denver International Airport	DEN	Denver	5.6
Baltimore/Washington International Thurgood Marshall Airport	BWI	Baltimore	5.5
Los Angeles International Airport	LAX	Los Angeles	5.4
Salt Lake City International Airport	SLC	Salt Lake City	5.4
Philadelphia International Airport	PHL	Philadelphia	5.4
Tampa International Airport	TPA	Tampa	5.3
Miami International Airport	MIA	Miami	5.3
Lambert St Louis International Airport	STL	St. Louis	5.3
Kansas City International Airport	MCI	Kansas City	5.2
Louis Armstrong New Orleans International Airport	MSY	New Orleans	5.2
San Antonio International Airport	SAT	San Antonio	5.2
Washington Dulles International Airport	IAD	Washington	5.1
Nashville International Airport	BNA	Nashville	5.1
Raleigh Durham International Airport	RDU	Raleigh-Durham	4.9
Chicago Midway International Airport	MDW	Chicago	4.5

LIMIT CYBER RISK AT AIRPORTS WITH CORONET SECURECLOUD – ITS FREE, FOREVER

Coronet's FREE SecureCloud platform empowers business travelers with enterprise-grade cloud security, enabling them to prevent the inherent risks of airport Wi-Fi and the subsequent threats from impacting their company's cloud apps and devices. With Coronet, all travelers can safely access any cloud service, through any device and connect to any network and seamlessly be secured. All Coronet SecureCloud users benefit from:

- **Access Control** - Now that users can work from anywhere, using any device, Coronet ensures only authorized users using safe devices connected through safe networks from allowed locations have access to cloud applications and data
- **Cloud Control** – Once access is granted, Coronet controls who shares what with whom, prevents data leakage, malware and ransomware spread, suspicious activities, and regulatory violations (PCI-DDS, HIPAA, GDPR, etc.)

TO GET STARTED WITH CORONET, SIGN UP HERE:
www.coro.net/signup

CORONET

www.linkedin.com/company/coronet/

@coronetworks

www.facebook.com/coronetworks/