Solutions brief

CYBERSECURITY

CYBERSECURITY: IT'S IN OUR DNA

You should take cybersecurity seriously, because inflight threats are real.

That's why at Gogo, we realize the ever-pressing need to be vigilant in staying ahead of potential security threats. Security isn't something we have added after the fact. Since our start, we've built security into the design and delivery of our networks and systems. You could say, security is in our DNA. We've secured and protected tens of millions of flights over the lifetime of our network.

Gogo is the only inflight connectivity provider that owns, protects, and optimizes its whole network infrastructure, and is the only provider that manufactures the equipment for its onboard systems. Because we operate and manage our systems end to end, we can monitor and analyze the security of our network and onboard systems. And, through our own standards or in partnership with the FAA and other aviation stakeholders, we've been a leader in defining and implementing best practices for airborne cybersecurity. We're solving cybersecurity problems before they happen, so you can connect confidently when you fly.

OUR SECURE AIR-TO-GROUND (ATG) NETWORK

We leverage the most advanced network designs to provide comprehensive security for our air-to-ground (ATG) network covering the continental U.S., and parts of Canada and Alaska. And, we stay current with the latest innovations in secure network design. Our Business Operations Center (BOC) provides continuous monitoring and troubleshooting of our broadband network. This allows us to quickly identify, detect, respond, and recover from potential cyber threats.

The following information details how we provide secure airborne connections 24/7/365 through our ATG network connections, onboard aircraft equipment configurations, and the Gogo BOC.

Gogo Biz ATG network communications: Gogo secures all communications that occur on its ATG network. This includes any data transferred between the aircraft, network ground stations and Gogo's two data centers.

The Gogo Biz network adheres to the latest developments in enterprise networking design. We provide secure network design with firewall protection, intrusion prevention, and utilize geographic redundant data centers for resiliency and high availability.

Onboard aircraft equipment: The process of protecting your inflight Wi-Fi experience starts from day one in engineering design and development. Gogo is proud to say that security is built in all of our connectivity solutions. Gogo secures all onboard aircraft equipment that is manufactured and delivered as part of the Gogo Business Aviation inflight connectivity system.

REAL SECURITY BUILT IN, END TO END.

Gogo
Network

Air-to-Ground (ATG) network secured through Gogo cybersecurity practices and policies.

Gogo Data Center
Includes multiple data centers for redundancy and failover.

Gogo Business
Operations Center
(BOC)

Your
work
life

Your
personal
life

Internet

Securely send emails, presentations, spreadsheets, and conduct video conferences. Supports access to VPN.

Securely shop, bank, share, and send messages online.

By design, Gogo onboard aircraft equipment is secured through network isolation, which includes:

- Open 802.11 and secure 802.11 Wi-Fi/wireless via WPA-2 encryption.

- Aircraft system intrusion security is provided by the Gogo-supplied router.

- All Gogo AVANCE products, L5, L3, and SCS, are shipped with the router technology built in and receive digitally signed software updates approximately every six months.

- Any connection to avionics and other flight systems are listen-only, meaning that the other systems are not accessible through the Wi-Fi components.

- Other airborne system components are inaccessible from the Wi-Fi clients due to network isolation.

The BOC staff consists of data systems, wireless and IP support analysts. Security is assured through industry-grade secured networking between the access-controlled BOC and the secured Gogo data centers.
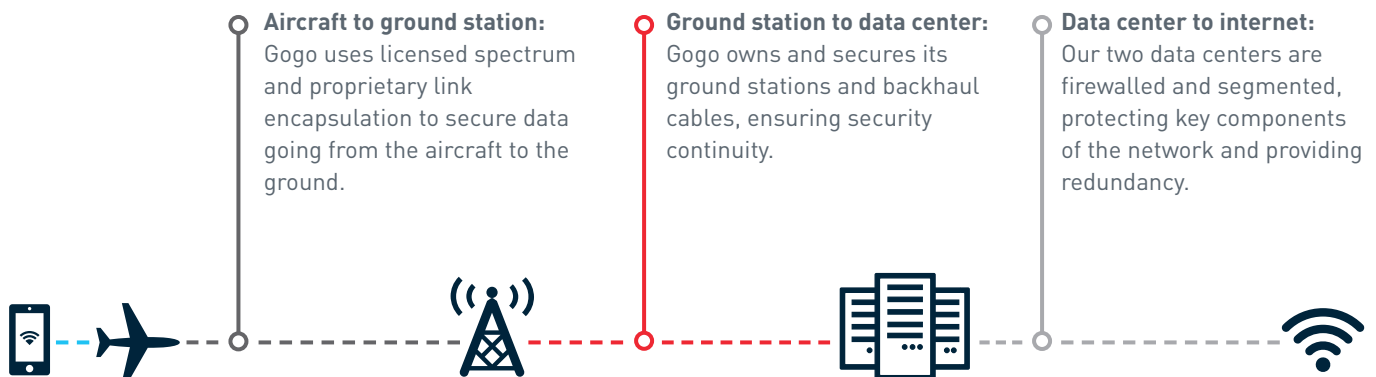
PLANS TO ENHANCE OUR SECURITY MEASURES

At Gogo, we strive to improve on everything with do. Our goal is to deliver a better, safer inflight connectivity experience. So, we will be rolling out cybersecurity innovations that include remote software updates to quickly deliver patches through Gogo DASH.

Gogo Business Operations Center (BOC): The Gogo Business Operations Center (BOC) provides Tier 1 & Tier 2 monitoring and troubleshooting of all elements of the Gogo Business Aviation mobile broadband network. Located in Broomfield, Colorado, the BOC provides continuous, round-the-clock operations support.

WHAT HAPPENS WHEN YOU PUSH SEND

Aircraft to ground station: Gogo uses licensed spectrum and proprietary link encapsulation to secure data going from the aircraft to the ground.

Ground station to data center: Gogo owns and secures its ground stations and backhaul cables, ensuring security continuity.

Data center to internet: Our two data centers are firewalled and segmented, protecting key components of the network and providing redundancy.

GOGO CYBERSECURITY BEST PRACTICES

Gogo Business Aviation adheres to the following best practices to ensure security at all stages in design and development of its network, products and processes. This is not intended to be a comprehensive list of all activities performed by Gogo's cybersecurity personnel.

MONTHLY SYSTEM VULNERABILITY ASSESSMENTS	The Gogo team performs monthly assessments of its assets. Results of these assessments are reviewed and any noted deficiencies are tracked and remediated.
ROUTINE PENETRATION TESTS	Routine and ad-hoc external and internal penetration tests are performed against Gogo's assets. Results of these penetration tests are reviewed and any noted deficiencies are tracked and remediated.
SCHEDULED FIREWALL AUDITS	Security audits are performed against all production firewalls. Both a manual review process and automated toolsets are utilized to ensure configurations are secure. Online backups of firewall configurations are maintained to make sure a rapid rollback can be performed successfully if there are any issues identified.
GENERAL SECURITY AWARENESS TRAINING	Both full-time employees and contractors are required to attend security awareness training within 30 days of their hire date and again at least annually. Supplemental training is conducted on an on-going, weekly basis to highlight current cybersecurity topics and trends.
SECURE CODING AWARENESS TRAINING	Both full-time employees and contractors who are members of the application development departments are encouraged to participate in awareness training focused on secure coding standards and best practices.
FAA CYBERSECURITY	Gogo works closely with the FAA and other aviation stakeholders to define new cybersecurity standards to anticipate and protect against current and future cyber threats. Gogo's certification process follows the latest FAA and RTCA policies to ensure safety of flight for Gogo-equipped aircraft.

SECURITY POLICIES	Cybersecurity policies are maintained and updated on an internal corporate site which is accessible to all employees and contractors. The policies, standards, and configuration guide are based on requirements sourced from the NIST CSF and ISO 27001:2015 frameworks.
EVENT LOG MONITORING	Gogo utilizes a trusted third-party security firm's Security Operations Center (SOC) to monitor production system event logs 24/7/365. Any anomalies are reported immediately and thoroughly investigated.
ENDPOINT SECURITY	All Gogo employee workstations are encrypted and have updated anti-virus, anti-malware, intrusion prevention and firewall technology installed.
PRIVILEGED USER ACCESS REVIEWS	Ongoing user access reviews are performed against production systems. Business stakeholders verify appropriate access levels for identified users.
CYBERSECURITY GOVERNANCE COMMITTEE	Quarterly meetings of key business stakeholders ensure security is addressed for various departments of the organization. Updates are provided to key business stakeholders from the Cybersecurity team and takeaways are implemented based on the criticality of the information provided.
RISK ASSESSMENTS	Ongoing risk assessments ensure new risks to Gogo are quickly identified and remediation efforts are prioritized and implemented.

For more information about our cybersecurity solutions and best practices, see
gogoair.com/solutions/cybersecurity

Connect with us:

+1 888.328.0200 *(Toll-free)*
+1 303.301.3271   *(Worldwide)*

connect@gogoair.com

gogoair.com