Security

FAQ

Security

brinc

TABLE OF CONTENTS

1055N. 38TH ST.
SEATTLE, WA 98103
www.BrincDrones.com I contact@brincdrones.com I (886) 849-0282

1055N. 38TH ST.
SEATTLE, WA 98103
www.BrincDrones.com I contact@brincdrones.com I (886) 849-0282

1. Security & Trust

1.1. Who is your Cloud provider?

LiveOps is hosted in Amazon Web Services (AWS) only in United States regions. Our current cloud is hosted in Oregon, US.

1.2. Is your Cloud provider CJIS compliant?

Yes. Information about AWS CJIS compliance can be found here (https://aws.amazon.com/compliance/cjis/).

1.3. Can AWS employees access my data?

No, the FBI has worked with AWS to acknowledge that the commercial AWS environment is CJIS compliant and employees cannot access the data.

1.4. Is LiveOps hosted only in the US?

Yes. LiveOps is only hosted in CJIS compliant regions and data is not sent outside of the US.

1.5. Do you Encrypt at REST?

Yes. LiveOps abides by CJIS encryption at REST requirements when storing data in the cloud.

1.6. Do you Encrypt in TRANSIT?

Yes. LiveOps abides by CJIS encryption in TRANSIT requirements.

1.7. Do Brinc employees access my evidentiary data?

No. Brinc employees will not access your evidentiary data unless directly requested by the customer admin to resolve data access, corruption issues, etc. Any Brinc employee that will access your data per the customers approval, will have gone through the CJIS Security Awareness training.

1.8. Does LiveOps require Two Factor Authentication (2FA)?

Yes. LiveOps requires 2FA for all login attempts by all user types.

1.9. Will my evidence be CJIS compliant?

Yes. Evidence stored in LiveOps will be stored in BRINC Vault which is CJIS compliant once evidence management is offered.

1.10. Is cellular data Encrypted in transit during livestream?

Yes. Data is encrypted using TLS 1.2 or greater during livestream and is separate from evidentiary data, and thus separated from CJIS requirements.

1.11. Is data transmitted over the local mesh network Encrypted?

Yes. Mesh radio transmissions between controller and drone are AES-256 encrypted

1.12. Will my data be CJIS compliant if I download it locally?

Yes. The data is Encrypted at REST per CJIS and will be Encrypted in Transit to your local computer pursuant to CJIS compliance requirements.

2. Data Storage & Streaming

2.1. How is my evidentiary data from the drone stored in LiveOps?

Your data is stored on your drone's SD card which can then be uploaded to LiveOps for storage.

2.2. Are Streamed 3D Maps Stored In LiveOps?

3D map data is streamed live from the drone to the cloud and to your computer. This data is stored for 24 hours in the cloud. The original file can then be uploaded via the SD card to be stored in LiveOps indefinitely.

2.3. Is the streamed telemetry data I see on the video stored in the cloud?

You will see telemetry such as cell signal strength and battery percentage on your livestream which is only provided for real-time information. This data is also accessible once uploaded from the drone's SD card into LiveOps.

2.4. Can a drone be taken over remotely by a hacker?

Lemur 2 drones have no remote pilot capability. Outdoor drones with teleoperation capability via LiveOps have remote control messages encrypted to the same standards as CJIS for evidence storage. Direct pilot control of all drones, via our handheld controller, is also secured by AES-256 encryption.

2.5. Is piloting of my drone secure?

Brinc has taken extensive measures to encrypt all traffic between the drone and the computer to ensure a secure connection. All connections are encrypted to AES-128 or AES-256 depending on the link. Each drone has unique credentials which Brinc can revoke at any time if requested by the customer.

2.6. Streaming Data Reference Diagram

Appendix (a.) Data Flow Diagram shows how streaming and stored data moves from *drone* to *cloud* to *liveops.brincdrones.com* on your computer.

2.7. Does LiveOps store any payment information?

No, LiveOps does not store any payment information (credit card, account numbers, etc.)

2.8. How are encryption keys managed

Encryption keys are fully managed in our AWS cloud management.

3. Password Management

3.1. Are there password requirements?

Yes, passwords require a minimum of 12 characters and require uppercase letters, lowercase letters, numbers, and symbols. Password changes are required and forced to be changed every 90 days.

3.2. Do you require Multi Factor Authentication (MFA)?

Yes, all users require MFA with a One Time Passcode (OTP) of 6 digits sent to a phone number.

4. Accessibility & Updates

4.1. Do I need to download anything to enable LiveOps?

No, LiveOps is fully cloud hosted and works best through the Chrome browser. No local program installation is required.

4.2. Can I use LiveOps on a mobile device?

Yes, LiveOps is fully functional on a mobile device such as a phone or tablet. Some features are only available on desktop such as data upload due to requiring an SD card being plugged in.

4.3. Is LiveOps available 24/7?

Yes, LiveOps is available 24/7 around the clock.

4.4. How do I get the newest version of LiveOps?

LiveOps updates are done automatically in our cloud environment and will be available immediately upon deployment.

4.5. How do I know if a new update or feature is available?

Emails are sent to all of our LiveOps users when new features or improvements are deployed to LiveOps.

4.6. Does my computer need internet access to use LiveOps?

Yes, your computer will need a stable internet connection to be able to access LiveOps.

4.7. Do I need to do anything with our firewall or IT security to enable LiveOps?

Generally LiveOps will work on day one without any changes. The only changes we've needed to help customers through is enabling VOIP traffic if your firewall blocks it, and you would like to use the calling features in LiveOps. Brinc Customer Success will help with your department and your IT team during onboarding to ensure accessibility.
https://www.twilio.com/docs/voice/sdks/network-connectivity-requirements

5. NDAA Compliance & Country of Origin

5.1. Are BRINC drones NDAA compliant?

Yes, the Lemur 2 and Responder drones, controllers, and battery packs are all NDAA compliant. This includes compliance with section 889 introduced in the FY19 NDAA bill, section 848 introduced in the FY20 NDAA bill and the American Security Drone Act introduced in 2024.

5.2. Where are BRINC drones assembled?

Final manufacturing, calibration, and configuration of BRINC devices (including drones, controllers, battery packs, drone accessories, and nests) is performed at BRINC headquarters in Seattle, WA, USA.

5.3. Who supplies the PCBAs and chipsets used in BRINC drones?

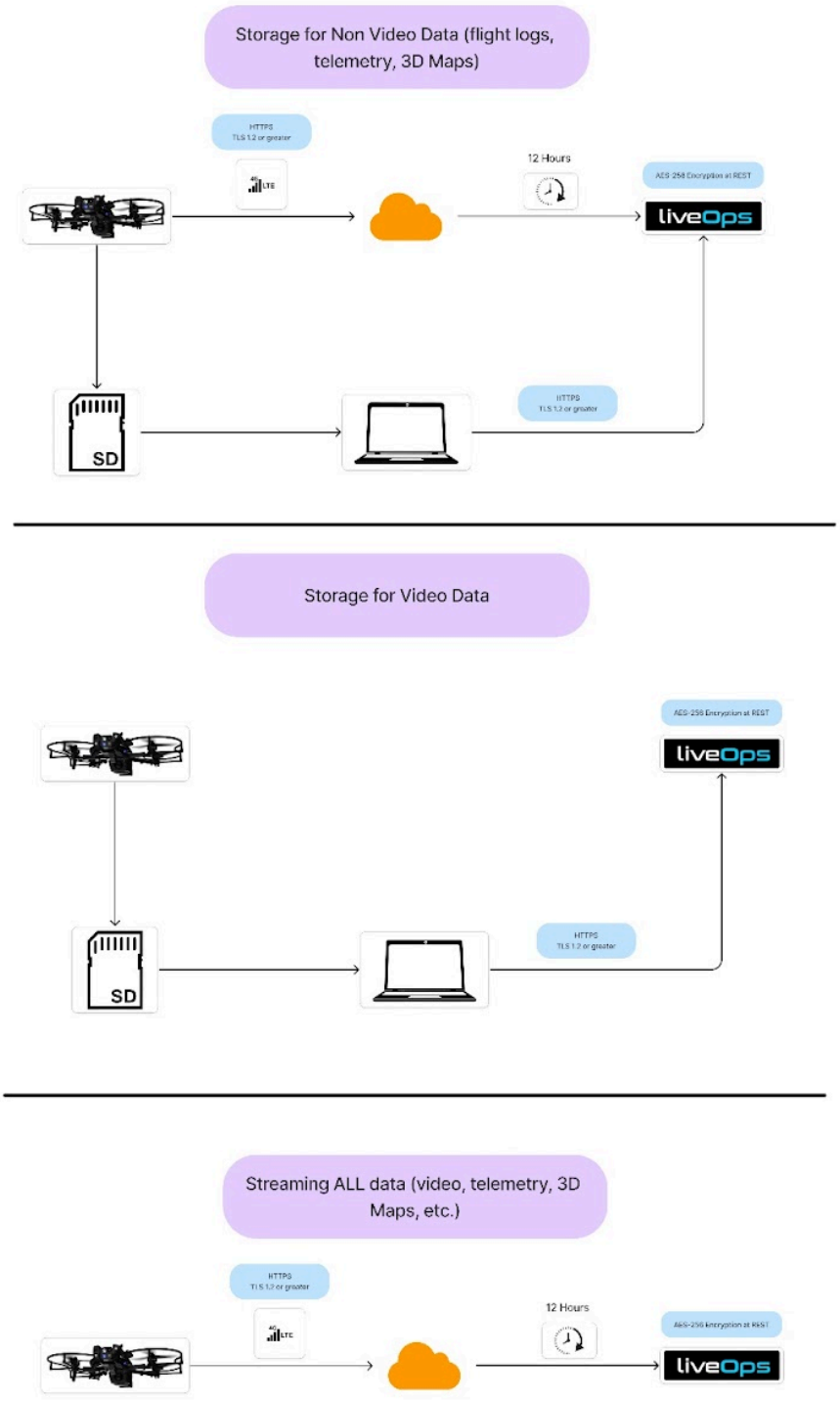
The BRINC Lemur 2 and Responder drones are composed of a combination of BRINC designed custom printed circuit board assemblies (PCBA) and modules sourced from trusted suppliers in allied nations. No PCBAs or compute (CPU, MCU, GPU) components are sourced from suppliers or semiconductor companies based in Foreign Adversary nations.

5.4. Where is BRINC software developed?

The software & firmware in the Lemur 2 drone, Responder drone, Pilot controller, and Station nest are all developed by a combination of BRINC and trusted USA and UK based suppliers. Software updates are provided directly by BRINC. No software is developed by or sourced from companies based in Foreign Adversary nations.

A. Appendix

a. Data Flow Diagram



1055N. 38TH ST.
SEATTLE, WA 98103
www.BrincDrones.com I contact@brincdrones.com I (886) 849-0282