DRONESENSE

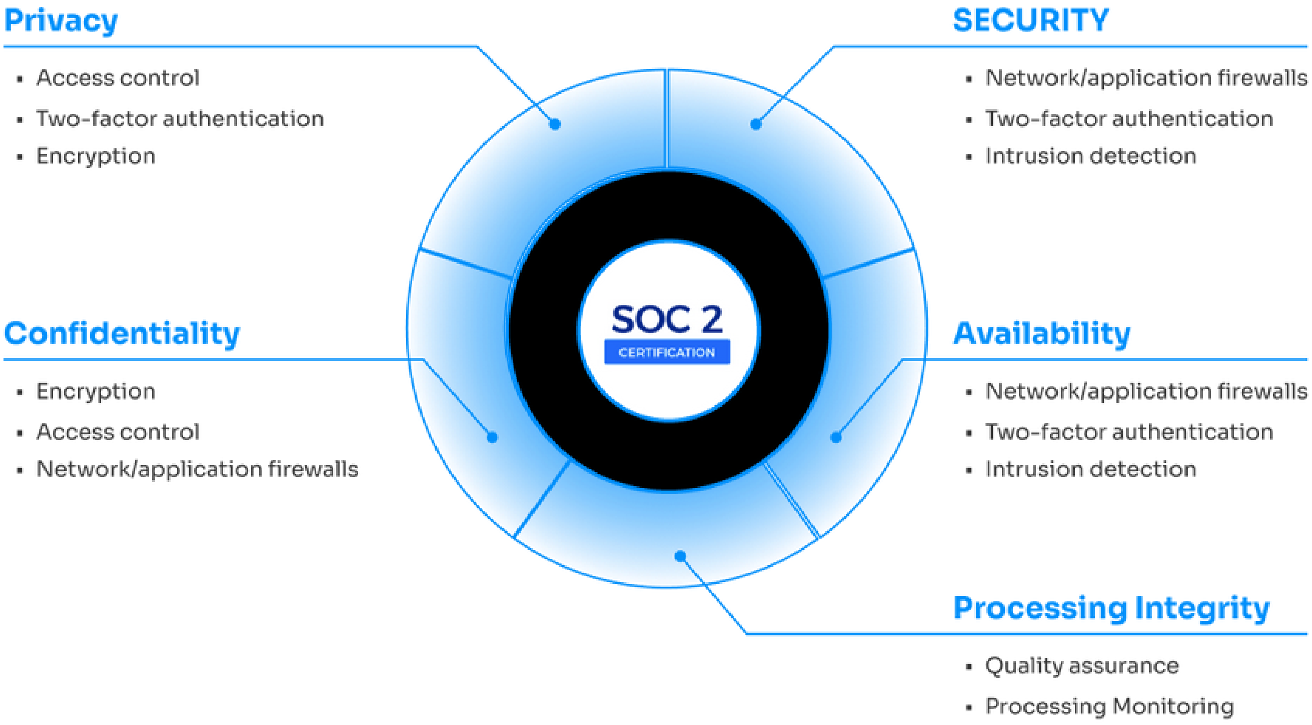
SECURITY

Our Commitment to Data Security at DroneSense

At DroneSense, our unwavering commitment to data security is at the forefront of everything we do. As a proudly American corporation, we are headquartered in the USA, with an ownership and investment structure that is entirely domestic, lacking any foreign involvement in terms of investors, stakeholders, owners, or subsidiaries. Our mobile applications and web platform are crafted by a dedicated team of professionals who are not only 100% US citizens but also reside within the country, ensuring a deep alignment with our core values and security principles.

Central to our approach is the DroneSense Application Security Program, a proactive initiative designed to continuously seek out and address vulnerabilities within our software and supporting infrastructure. This rigorous program plays a pivotal role in fortifying the DroneSense platform against external threats, ensuring robust protection for our users.

Moreover, our commitment to excellence extends to our Security Governance, Risk, and Compliance Program. This comprehensive program guarantees that DroneSense, along with our services, not only adheres to but often surpasses the stringent requirements set forth by industry standards, legal mandates, and regulatory frameworks related to information security, including SOC2 Type 2, CMMC 2.0 Level 2, and ISO27001, among others.



Privacy

- Access control
- Two-factor authentication
- Encryption

SECURITY

- Network/application firewalls
- Two-factor authentication
- Intrusion detection

Confidentiality

- Encryption
- Access control
- Network/application firewalls

Availability

- Network/application firewalls
- Two-factor authentication
- Intrusion detection

Processing Integrity

- Quality assurance
- Processing Monitoring

What Makes the DroneSense Platform Secure?

DroneSense Mobile Applications (Pilot and CoPilot)

DroneSense's mobile applications, Pilot and CoPilot, harness the power of third-party Software Development Kits (SDKs) to deliver the essential functionality needed for controlling Unmanned Aerial Systems (UAS) and capturing data from them. These SDKs are sourced from open and publicly accessible code repositories, such as GitHub, ensuring transparency and accessibility. Our team of engineers meticulously examines this code to confirm its safety for use, ensuring that there are no hidden "backdoors" or any form of potentially malicious code.

To maintain the highest standards of security, DroneSense conducts regular security assessments under real-world conditions. This proactive approach allows us to swiftly detect and address any unauthorized, suspicious, or malicious activities that could arise during the use of our mobile application. In alignment with recommendations from the Cybersecurity and Infrastructure Security Agency (CISA), DroneSense functions as a standalone application, eliminating the need for the UAS manufacturer’s native app to operate the UAS.

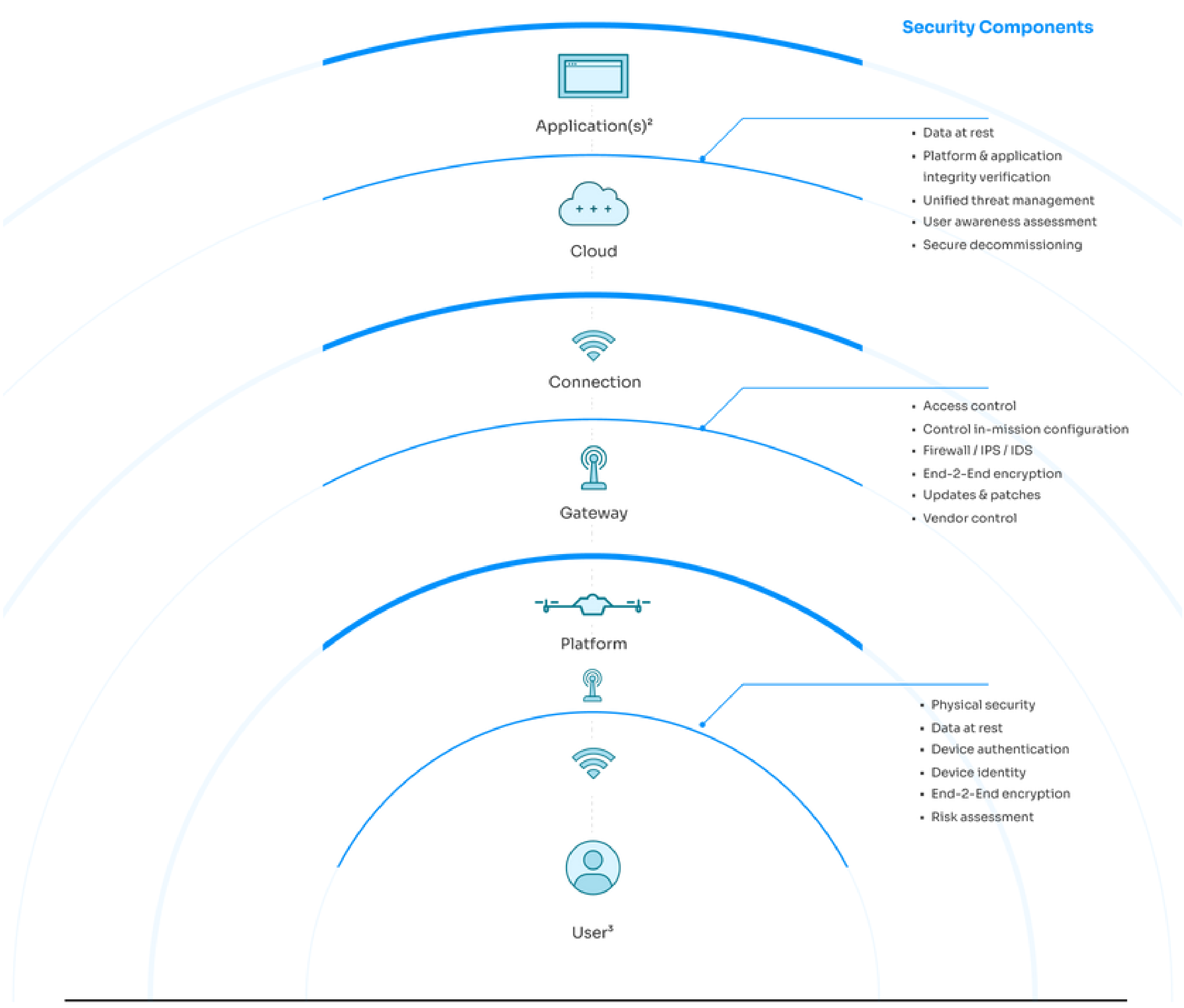
Furthermore, DroneSense prioritizes the privacy and integrity of flight data by storing it in a distinct file system, separate from the manufacturer's native flight logs. Additionally, DroneSense offers the capability to operate entirely offline, enhancing operational flexibility and security for all missions.

DroneSense Cloud Applications

The DroneSense Platform establishes a secure, end-to-end encrypted network, seamlessly connecting the Drone, the Controller/Mobile Device, the DroneSense Mobile App, and the DroneSense Cloud Application. Our cloud applications and infrastructure are rigorously audited, achieving SOC2 Type 2 Certification annually. This certification underscores our unwavering commitment to maintaining robust technical controls that protect the confidentiality, integrity, and availability of our cloud application, infrastructure, and the data within.

We prioritize the security and sovereignty of customer data on the DroneSense platform. Data is encrypted, access-controlled, and isolated from other customer or company data to prevent unauthorized access. We champion data ownership, allowing customers to manage their data with options to retrieve, modify, or delete as needed. Vigilant monitoring for external threats ensures rapid response strategies are in place to mitigate any potential risks, safeguarding the uninterrupted and secure availability of DroneSense services.

The Layer-Cake of Drone Data Protection



Security Components

- Data at rest
- Platform & application integrity verification
- Unified threat management
- User awareness assessment
- Secure decommissioning

- Access control
- Control in-mission configuration
- Firewall / IPS / IDS
- End-2-End encryption
- Updates & patches
- Vendor control

- Physical security
- Data at rest
- Device authentication
- Device identity
- End-2-End encryption
- Risk assessment

- DroneSense utilizes the drone manufacturer's SDK and API to access the drone using our mobile applications
- The drone hardware stores all of the data on an SD card and the software controls communication between the controller and the drone, segmenting and isolating the data storage from the hardware.
- DroneSense accesses the drone video feed, location, telemetry and Command & Control solely through the API/SDK.

- The DroneSense mobile app connects to our secure cloud-based infrastructure and delivers the data to the client
- DroneSense software manages the data, distribution etc, using the AWS enterprise cloud security mechanisms which complies with all requirements of data access and security.
- DroneSense does not store the video feed in any manner, all the data is ephemeral and real-time only

DRONESENSE

Where do we go from here?

The DroneSense team relentlessly pursues new ways to make sUAS operations more effective and secure. We deeply value the power of a fresh perspective and we've been quick to engage third-party experts to ensure that we continue to lead the industry in this key area. Likewise, we recognize that no one knows your security requirements better than you and we welcome you to contact us for a deeper discussion about your sUAS security needs. We are here to help you navigate these concerns and provide a solid foundation for any new threats that may arise.

For any security related concerns or questions, please reach out to us.

DroneSense Sales Organization

sales@dronesense.com or contact@dronesense.com

DroneSense Security

security@dronesense.com