AIRSPACE SECURITY TECHNOLOGY:

A Buyer's Guide

AIRSPACE SECURITY TECHNOLOGY:

A Buyer's Guide

As drone technology continues to advance and improve, the possibilities for use expand and become more creative. According to Goldman Sachs, the drone technology industry as a whole stands to be a $100 billion opportunity by 2020. As with any technology, consumers will find ways to use it to solve problems, but also find ways to use it for unintended or malicious purposes.

The airspace security industry is growing rapidly, and laws involving the safe integration of drones to national airspace are slow to catch up. As more drone incidents and airspace intrusions are occurring, organizations protecting high-risk and high-value infrastructure must be proactive and protect their airspace from drone threats.

It is important now, more than ever, to understand and assess lower airspace activity and gain situational awareness on drones entering critical airspace.

In this buyer's guide, you will learn:

- How to assess your needs for airspace security technology
- Who should be involved with drone detection technology purchasing
- What to expect from the process

Contents

1. Defining Airspace Security Technology and Terminology

IN THIS SECTION:

- What is airspace security technology?
- What sort of information does airspace security technology provide?
- How can I take action against a drone threat?

A combination of hardware and software can be used to identify and classify drones and determine the location of the drone and pilot. Depending on the types of hardware and software, you should be able to identify the drone manufacturer, model, time and length of drone activity, and location of the pilot.

Airspace Security Hardware:
Hardware collects data and information about the drone and is installed outside in areas that need to be protected against drone threats.

- **Radio frequency sensors:** RF sensors are the cornerstone of airspace security, and detect commercial, consumer, and DIY or prototype drones, the flight path as well as the location of the pilot and the drone. RF sensors are capable of identifying drone type/model is used, which is critical forensic data used to bring legal action against trespassers.
- **Cameras:** Cameras have eyes on the movement of the drone, help identify the payload, and record forensic evidence of drone intrusions.
- **Radar:** When permitted to use, radar provides long-range detection including the position of the drone.
- **Acoustic sensors:** Drones "buzz" in a unique way, and acoustic sensors can pick up on unique sound signatures.

Airspace Security Software:
Software connects sensors, performs machine-learning analysis, and is the central nervous system for the complete solution.

- **User interface:** A user interface should be enterprise-grade, provide multi-user access, and give instant notifications of an approaching drone. Additionally, summary reports should be automatically produced and available on-demand for easy analysis of the most critical airspace security data.
- **Video analytics:** Using IP video cameras, video analytics differentiates between moving objects, such as a plane, car, helicopter or drone.
- **Machine learning platform:** A drone detection software should constantly be learning and upgrading, much like antivirus software and malware protection tools.

“Decoupled” technology system architecture:
Also referred as “sensor agnostic,” each computing element in your drone detection ecosystem should be able to stand alone. You should be able to integrate different brands, models or manufacturers with a drone detection software, in order to create a flexible and cost-effective solution that meets your needs.

Countermeasures and defeat technology:
This technology does not collect data about the drone, but is an important component of an airspace security solution. Countermeasures can be passive or active. Detection technology first locates and identifies the flightpath of drone, and then a defeat or countermeasure can be deployed.

- **Passive countermeasures** do not interfere with the drone and can include closing blinds, moving protected assets, or temporarily shut down operations.
- **Active countermeasures** are typically illegal for enterprises and individuals, as destroying or interrupting a drone is against the law in many countries. However, exceptions may exist when drone intrusions are a matter of national defense. Militaries are authorized to use active countermeasures to defeat drones if they are under attack or their safety is threatened, and can use technology such as jammers or lasers.

2.
Needs Assessment

IN THIS SECTION:

- Does my organization need to protect assets that are vulnerable to airspace threats?
- What are my needs and goals for an airspace security program?

With the rise of drones in our airspace, we need to consider building an aerial equivalent of a fence. Some major concerns organizations have include:

- **Arenas/Stadiums:** Protecting athletes and spectators from physical threats; protecting broadcasters and copyrights from unauthorized cameras
- **Corporations:** Cooling units on rooftops protecting data centers, sensitive IT infrastructure vulnerable to hacking, prototypes/intellectual property protection
- **Correctional facilities:** Contraband deliveries, including weapons and drugs
- **Major political or social events:** Protecting the physical safety of large crowds of people and VIPs from paparazzi or terrorists
- **Critical infrastructure:** Power plants, oil & gas refineries and pipelines, reservoirs and other resources can be compromised discretely and easily with an unauthorized drone

What are your current security needs?

Drones pose both physical and cyber security issues. Drones are capable of carrying payloads of any kind, up to hundreds of pounds. Cameras can be used for espionage, and payloads can drop weapons, drugs or other sensitive materials. Drones are also laptops in the sky and can be used by sophisticated hackers to conduct espionage and compromise data centers and IT networks.

Are there unauthorized drones in your airspace?

Situational awareness is difficult to assess without technology. Drones move quickly and can be hard to detect with the naked eye. A dedicated security officer may have limited resources, including visual range, line of sight distractions, such as inclement weather, and even with the best attention span, can easily miss a fast-moving, discrete drone.

Does your organization already have a drone program?

Drones are coming to work across a variety of industries for surveillance, inspection, delivery, and entertainment. It's important to differentiate between an authorized drone and unauthorized drone so that your operations remain intact and existing drone programs operate safely.

What are your goals?

You may want to catch contraband deliveries, locate snooping trespassers, protect intellectual property, or collect data on your airspace activity to ensure your skies are clear during certain operations. Define what success means for an airspace security system. Some examples could include:

- Increase the rate of locating trespassers and apprehending spies
- Locate vulnerabilities on your property to protect against espionage or interruptions
- Strategically advance perimeter security programs
- Capture drone contraband deliveries before they reach an intended recipient

This information will help determine the tools you will need to accomplish your goals.

3.
Getting Started

IN THIS SECTION:

- What do I need to do to get started with a drone detection program?
- Who should be involved with this process?
- What should I look for when narrowing down technology options?
- What's my threat level and urgency for a drone detection program?

Inform your team members of your research and their role in the process.

While it's important that security team members and leaders are fully informed of airspace security threats, it's also helpful to get your information technology team and facility maintenance team onboard to ensure seamless integration and long-term success.

- **Security:** These are the front-line operators of a drone detection program, and include the decision-makers (CSO, CISO), and those who would be operating on-site security and responding to drone threats.
- **IT:** Members of this team will help you understand the power and connectivity needs for a drone detection program, and how information from your drone detection program may be able to integrate into other programs. They may also be involved with the installation process.
- **Operations/facility:** From site managers to groundskeepers, these team members will have a greater knowledge of your area's landscape and will help identify ideal locations for different sensors.
- **Finance/procurement:** Discuss your discretionary budget and confirm any details needed to engage a new vendor.

Evaluate your technology options

Airspace security is an emerging market. It's important to be critical of the technology you purchase and ensure their platform aligns with your needs. Your technology solution needs to be:

- **Proven with a variety of customers:** A simple search should show whether or not your technology provider has reference customers across verticals who have deployed the solution. You should be able to contact the technology company to gain insight on their history of success with the product.
- **Scalable and future-proof:** Once you install your technology and collect data, you should have the opportunity to expand your operations and protected area. Additionally, all software should be regularly updated and learn from new data collected from your protected site. No installation is a one-size-fits-all, and your detection program should continually be advancing or learning from itself, much like a machine-learning platform or anti-virus software.

- **Enterprise-grade:** Enterprise customers require solutions that meet security standards, integrate with existing procedures and systems, and enable multi-user management at scale.
- **Automatic and immediately actionable:** You should not need a dedicated monitor for your airspace security system. Detection analytics should be instantaneously available to enable security personnel to assess and analyze drone threats.
- **A layered, sensor-agnostic security program:** Multiple detection technologies should be incorporated to create a complete system, including acoustic sensors, cameras, RF/WiFi and radar, among others. Each detection technology provides additional layers of data, and you should be able to integrate a variety of brands/makes/models of sensors to fit your exact needs.
- **Intuitive and easily integrated into standard operating procedures:** The interface should be clearly designed for different levels of users.
- **Cost-effective:** The cost of entry to a new technology program should not be a barrier. Detection technology needs fit your budget and allow room to expand your airspace security program over time as you learn more about your airspace activity.

Determine Your Threat Level:

Severe: Your organization has been threatened, or drones are already in your airspace and threatening your security. This includes those protecting critical infrastructure, or organization where being offline due to an airspace breach could cause catastrophic damage.

High: Your organization is aware of drones in your airspace and are actively developing security protocols. Drone detection is needed to gain situational awareness of your airspace activity to plan and react to a drone intrusion. You may be a stadium that has seen drones above your games, or a correctional facility already intercepting drone contraband deliveries.

Guarded: Your organization is aware of the threats that drones pose, but do not see them immediately in your area. Drone detection technology will help assess your risks. This could include event organizers looking to elevate their security program, or a corporation protecting intellectual property.

Low: Your organization is aware that drones are a problem for some organizations, but not sure what kind of risks they would pose to your operations. Security teams may also want to incorporate drone detection technology to help existing drone operations on their site, to differentiate between an approved or rogue drone.

Determine your budget and timeline:

Based on your threat level, you'll need to determine how much you can invest in hardware, software licenses, and other purchasing costs. It may be that you need to make a purchase immediately. Determine this early on in the process to make sure your budget matches your needs.

Timing milestones you need to consider include:

- **Research and introductions:** Set aside time to research your options and hold initial meetings with technology providers.
- **Internal purchasing cycle:** Know ahead of time what sort of process is in place for your company to approve purchases, and what information you need ahead of time to make it a seamless process.

- **Sensor procurement and production:** You may need to purchase additional hardware from third parties or wait for the production of new hardware. A technology provider will be able to advise on a timeline.
- **Installation and training:** Depending on the complexity of your installation, a site visit from a technology provider may be required. Also plan time for the installation, calibration, and testing before your system is fully deployed.

Once you start the conversation with a technology company, you can work out these details to ensure the start of a drone detection program is in accordance with your threat level and other needs.

4.
Engaging a Technology Provider

IN THIS SECTION:

- When I'm ready to buy, what should I expect from a technology provider?
- What sort of technical information should I expect to collect during the buying process?

When you're ready to engage a technology provider, they should be ready for your questions and able to immediately assist you in your purchasing process. A technology provider should be able to immediately make available some introductory materials, including:

- **Training and introduction materials:** You should be able to easily sign up for a webinar, view videos, or read guidebooks.
- **Reference materials and research:** A technology provider should have a library of educational resources available to you, including white papers, blog posts, or annual reports.
- **Success stories:** Ensure a technology provider can readily provide case studies on how their technology can solve problems for organizations such as yours and can connect you directly to existing reference customers to discuss their installation and success.
- **Dedicated account management team:** From research to installation and maintenance, you should have easy access and clear communication with your team.

Prepare for the purchasing process

You may already have sensors in your security ecosystem that could be incorporated into a drone detection program. Additionally, it's important to go into a conversation with an understanding of your physical landscape and any

considerations that may require special installation. While you don't need this information immediately for the first contact with a provider, it will eventually need to be considered to ensure you're developing a successful program.

Below is a checklist to help you find airspace security technologies. This will help in your conversations with technology providers, who can then help identify and narrow down your solution needs

Resource checklist:

SENSOR	LOCATION	PRIMARY FUNCTION	MAKE/MODEL
IP Camera			
Radar			
Acoustic Sensor			
RF Sensor			
Other Sensor			

Technology checklist:

Confirm ahead of time if you have the following technology requirements for a successful deployment:

- ☐ Cell signal reception at the protected site (4G-LTE) and/or internet connectivity at deployment locations
- ☐ Accessible flat surface on a raised structure to attach any sensors
- ☐ A 120V electrical connection within 100 feet of the installation site

Installation area checklist:

While some of these may not apply to you, it's helpful to make a note of the environment that you're protecting.

- ☐ **Location:** Urban or rural location
- ☐ **Size of property:** Height of buildings and roof access considerations
- ☐ **Airspace elements:** Proximity to other buildings; if they are taller or shorter than your building
- ☐ **Proximity to critical infrastructure:** Military bases, data centers, arenas/stadiums, prisons, power plants
- ☐ **Proximity to transportation:** Airports, highways, rail systems
- ☐ **Proximity to acoustic or frequency sensors:** Cell phone towers, radio/television/broadcast network stations, DAS
- ☐ **Landscape details:** Open space or forest, hills/changes in elevation, proximity to a body of water

NOTES

GLOBAL HEADQUARTERS
1099 Folsom St
San Francisco, CA 94123

Published June 2018

dedrone.com