Counter-Unmanned Aircraft Systems (C-UAS)

Market Intelligence Report · Physical Security · 2026

$6.6B	$20.3B	9,000+	55%	16
Global market 2025 (MarketsandMarkets)	Projected by 2030 (25.1% CAGR)	CNI facilities eligible for UAFR	Military segment share of market	CNI sectors in FAA UAFR framework

Detection	Identification / Tracking	Mitigation / Defeat	C2 Software
Finding the drone. Radar, RF, acoustic, EO/IR, AI tracking. Multiple sensors required — no single technology is reliable alone.	Determining what the drone is, where the pilot is, whether it is authorized, and its flight path. Remote ID is now a key data source.	Stopping the drone. RF jamming, GPS spoofing, protocol takeover, kinetic intercept, nets, directed energy. Heavily restricted in U.S. commercial use.	The single pane of glass. Integrates sensors, alerts, maps, AI, and incident response. Where SaaS recurring revenue models are being built.

U.S. Legal Constraint — Read First: *Most private and commercial operators in the United States cannot legally jam, spoof, or kinetically disable drones. Defeat authority is restricted to federal agencies (DHS, DOJ, DoD) and limited FAA-approved programs. The FAA Section 2209 NPRM (May 2026) proposes airspace restriction authority for CNI operators — but does NOT authorize defeat technology. Commercial deployments today are: detect, identify, track, alert, document, and coordinate with law enforcement.*

New additions highlighted in green. *Updated rows highlighted in gold. Updated data reflects 2025-2026 market changes.*

Vendor Comparison Table

VENDOR	CATEGORY	DEPLOYMENT	KEY CAPABILITIES	MARKET FOCUS	DIFFERENTIATOR / STRATEGIC POSITION
Dedrone (Axon) UPDATED	C2 Software / Detection	On-prem / Cloud / Air-gapped	RF detection, AI classification, multi-sensor fusion, single pane of glass C2; Remote ID integration; BVLOS DFR support	Enterprise / Airport / CNI / Government / Law Enforcement	Acquired by Axon (Oct 2024) for undisclosed sum after $127M in VC funding. Deployed at 800+ locations, 40 cities, 30 airports, 50 stadiums, 50 correctional facilities, 36 countries, 9 U.S. federal agencies. DHS SAFETY Act certified. Strongest commercial enterprise C2 ecosystem.
Anduril Industries	AI Platform / Autonomous Defense	Edge / Distributed / Self-contained	Lattice AI platform; autonomous sensor fusion; multi-domain C2; AI-driven threat classification and neutralization; installation protection	DoD / Military / Federal Government / CNI	$642M IDIQ 10-year U.S. Marine Corps contract for Installation C-sUAS. Lattice integrates radar, RF, EO/IR, and effectors into autonomous C2. Most transformative defense-tech player in the market. Defense-first, but CNI relevance growing.
DroneShield	Detection / Defeat Systems	Mobile / Fixed / Vehicle-mounted	RF detection, DroneSentry fixed system, DroneSentry-X mobile, DroneCannon defeat, AI-powered classification; SaaS layer	Military / Law Enforcement / CNI / Government	ASX-listed; AU$57.5M revenue (2024), AU$52M in 2025 commitments. NATO framework agreement. SaaS revenues doubling. DroneCannon and handheld systems deployed in active conflict zones. Strong global tactical + fixed-site presence.
Fortem Technologies	Radar / Interceptor	Fixed / Mobile	TrueView radar; DroneHunter autonomous interceptor drone; AI tracking; net capture	Airport / Stadium / CNI / Military	Only major vendor with a purpose-built autonomous interceptor drone (DroneHunter) as its primary defeat method. Physically captures drones rather than jamming. Strong airport and stadium deployments. Kinetic intercept avoids RF jamming legal issues.
SRC Inc.	Radar / Electronic Warfare	Fixed / Mobile / Vehicle-mounted	Silent Archer C-UAS system; GRYPHON radar; electronic warfare; multi-sensor integration	Military / DoD / Federal Government	Defense contractor heritage. Silent Archer is a mature, deployed DoD system. Less visible commercially but serious radar and EW capability. Often the detection layer inside larger integrated programs.
BlueHalo	Directed Energy / Electronic Warfare	Fixed / Mobile	Directed energy systems; RF defeat; high-power microwave; electronic countermeasures	Military / Intelligence Community / DoD	Primarily defense and intelligence community. Directed energy and RF defeat position. Less commercially accessible but relevant as a defeat layer for classified/sensitive CNI sites where kinetic options are restricted.

VENDOR	CATEGORY	DEPLOYMENT	KEY CAPABILITIES	MARKET FOCUS	DIFFERENTIATOR / STRATEGIC POSITION
OpenWorks Engineering	Kinetic Intercept	Fixed / Portable	SkyWall net launchers; compressed gas projectile capture; SkyWall Patrol (portable), SkyWall 300 (tripod)	Military / Event Security / CNI / Government	Specialized net-capture intercept. No jamming or RF defeat — legally cleaner for some deployments. SkyWall used at high-profile events. Niche but important for close-in defense where RF solutions are operationally constrained.
Teledyne FLIR	Sensor / Enterprise Platform	Fixed / Mobile / Integrated	SkyRaider radar; Ranger thermal cameras; R80D SkyRaider integrated; multi-sensor drone detection kits	Military / Border / CNI / Enterprise	Thermal and radar heritage gives strong detection credibility. Increasingly integrated as detection layer in multi-vendor C-UAS stacks. Enterprise and CNI deployments growing as their cameras become AI-capable.
Motorola Solutions	C2 Integration / Enterprise Platform	Cloud / On-prem / Hybrid	Integrated C-UAS detection into Avigilon and VESTA platforms; command center integration; alert workflows	Enterprise / Public Safety / Airport / Venue	Integrating C-UAS detection into existing physical security platform play. Natural extension of Avigilon camera + Calipsa analytics stack. Strong channel for enterprise buyers already in Motorola ecosystem.
Dedrone / Axon DFR Platform NEW	Drone-as-First-Responder	Cloud-managed / BVLOS	DedroneBeyond BVLOS; autonomous drone dispatch; airspace awareness; incident response integration	Law Enforcement / Public Safety / Campus	Post-acquisition capability: BVLOS drone dispatch for first responder programs layered with C-UAS airspace awareness. Unique dual-use: protects against bad drones while enabling good ones. Growing public safety segment.
Axis Communications	Detection / Enterprise Camera	Edge / Fixed	ACAP-based drone detection apps; radar integration; AI tracking; integration with Milestone and Genetec	Enterprise / CNI / Airport	Leveraging open edge AI platform (ACAP) to enable drone detection on existing camera infrastructure. Natural upgrade path for enterprise customers. Detection only — no defeat capability.
Leonardo S.p.A.	Integrated C-UAS / Defense	Fixed / Mobile / Naval	Falcon Shield; multi-layer detection and defeat; AESA radar; electronic warfare; kinetic options	Military / Government / CNI / Airport	Major European defense prime. Falcon Shield is a mature integrated C-UAS system covering detection through defeat. Strong NATO and European critical infrastructure positioning. Less visible in U.S. commercial market.
D-Fend Solutions NEW	Protocol Takeover / Cyber Defeat	Fixed / Mobile / Portable	EnforceAir takeover technology; safely lands rogue drones; no RF jamming; cyber-based drone defeat	Airport / Prison / CNI / Government / Military	Unique cyber-based defeat: takes control of drone's communication protocol and safely lands it rather than jamming or destroying. No collateral RF interference. Legally cleaner than jamming in many jurisdictions. Used at airports, prisons, CNI.

VENDOR	CATEGORY	DEPLOYMENT	KEY CAPABILITIES	MARKET FOCUS	DIFFERENTIATOR / STRATEGIC POSITION
Skyfend NEW	Portable Defeat / Detection	Handheld / Mobile	AFA100 handheld jammer/detector; multi-band RF defeat; compact design; field deployable	Military / Law Enforcement / Event Security / CNI	Compact handheld C-UAS for field teams. Multi-band jamming in portable form factor. Positioned for tactical response teams and mobile security details. Growing commercial interest despite legal constraints on jamming.

U.S. Regulatory Landscape

FAA Section 2209 NPRM — May 6, 2026	The most significant recent development. Nearly a decade after Congress first ordered it, the FAA published its Notice of Proposed Rulemaking implementing Section 2209 of the FAA Extension, Safety, and Security Act of 2016. Comment period runs through July 6, 2026. Final rule expected 2026-2027. Creates a new 14 CFR Part 74 framework with two tiers: Standard UAFR: Restricted airspace up to 400 feet AGL within the facility's property lines. Unauthorized drone operations generally prohibited. Renewable every 5 years. Special UAFR: Stricter controls for high-threat sites. Often sponsored by federal intelligence or security agencies. Eligibility: Facilities meeting the federal definition of critical infrastructure under 42 U.S.C. 5195c(e) and falling within the 16 sectors in National Security Memorandum 22. Estimated 9,000+ eligible facilities nationally. Data centers qualify under the Information Technology sector. CRITICAL: The NPRM explicitly does NOT authorize geo-fencing, jamming, drone capture, or any mitigation technology. It restricts airspace. It does not give operators defeat authority.
Executive Order 14305 — June 6, 2025	"Restoring American Airspace Sovereignty" — signed by President Trump. Directly ordered the FAA to submit the Section 2209 NPRM promptly and interpret critical infrastructure consistent with the order's definition. This EO is the reason the NPRM was finally filed a decade late.
FAA Reauthorization Act of 2024	Passed May 2024 with strong bipartisan support. Extended FAA authority through FY2028. Key C-UAS provisions: — Section 929: Added state prisons to list eligible for Section 2209 drone restrictions — Section 935: Authority for temporary flight restrictions around large public gatherings — Section 1112: Extended DHS/DOJ counter-UAS authorities to Oct. 1, 2024 — Sections on BVLOS rulemaking and drone infrastructure inspection grants ($12M/year) Criticism: Dedrone's CEO publicly called out Congress for failing to include enhanced counter-drone authorities for law enforcement and CNI operators.
NDAA 2025 — Chinese Drone Restrictions	The Countering CCP Drones Act was removed from the final NDAA 2025, but similar language remained. DJI and Autel drones face national security review process. Federal agencies prohibited from acquiring covered drones. Significant market implication: accelerates demand for NDAA-compliant alternatives and U.S.-manufactured hardware across government and CNI deployments.
Who CAN Legally Use Defeat Technology	Currently restricted to: — U.S. Department of Defense (at military installations) — U.S. Department of Homeland Security — U.S. Department of Justice (limited) — FAA (testing programs) — Certain DHS-approved pilot programs Private companies, state/local law enforcement, and CNI operators generally CANNOT legally jam, spoof, or kinetically disable drones. This is the single biggest constraint on commercial C-UAS deployment in the U.S.
What Is Coming	Active legislative effort in both chambers to expand counter-UAS authorities to state/local law enforcement and critical infrastructure operators. The NJ drone sightings (Dec 2024) — over 5,000 reports — created significant congressional urgency. The Section 2209 UAFR framework, once finalized, gives CNI operators an airspace restriction tool. Future legislation is expected to eventually extend limited defeat authority to designated CNI operators, but timeline is uncertain.

Market Structure & Where It Is Going

The C-UAS market is undergoing a structural shift identical to the pattern seen in physical security AI: from single-purpose detection tools to integrated, AI-driven operational platforms. The threat driver is economics — a $1,500 consumer drone can now conduct facility reconnaissance, map access points, carry contraband, disrupt cooling systems, or act as a delivery mechanism for a small explosive payload. Traditional perimeter security has no answer to that threat vector. That is why this segment is growing at 25%+ CAGR.

1 Sensor Fusion

2 AI-Driven Autonomous Response

Automatic drone classification, autonomous tracking, predictive threat scoring, and automated dispatch. The market is moving from human-in-the-loop to human-on-the-loop. Anduril's Lattice platform leads here. Key players: Anduril, DroneShield (SaaS AI layer), Dedrone/Axon.

3 CNI & Data Center Protection

Fastest-growing commercial segment. Data centers, substations, water treatment, nuclear, ports. Primary concern is nation-state reconnaissance, insider threat facilitation, and targeted sabotage. FAA Section 2209 UAFR framework (when finalized) will accelerate procurement. Key players: Dedrone/Axon, Fortem, Teledyne FLIR, D-Fend Solutions.

4 Managed C-UAS Services

Emerging business model: remote monitoring subscription, drone incident response, SOC integration. Mirrors managed cybersecurity. Small and mid-market CNI operators cannot staff a C-UAS program internally. This segment is where SaaS recurring revenue will be built. Key players: Dedrone/Axon, DroneShield (SaaS push), Motorola Solutions ecosystem.

Strategic Ranking — Commercial Enterprise and CNI Focus

COMPANY	POSITION	CNI/DATA CENTER RELEVANCE	KEY 2024-2026 DEVELOPMENT
Anduril Industries	Most transformative overall	High — growing from DoD into CNI	$642M Marine Corps IDIQ; Lattice expanding to commercial
Dedrone (Axon)	Strongest commercial enterprise player	Very High — deepest CNI/airport/prison footprint	Acquired by Axon (Oct 2024); DFR integration; 800+ sites; DHS SAFETY Act certified
DroneShield	Strong global tactical player	Moderate-High — defense + CNI crossover	AU$57.5M 2024 revenue; NATO framework; SaaS revenues doubling
Fortem Technologies	Best interceptor innovation	High — airports, stadiums, CNI	DroneHunter kinetic intercept avoids jamming legal issues
D-Fend Solutions	Cleanest defeat method commercially	High — airports, prisons, CNI	EnforceAir cyber-takeover: no jamming, no RF interference, soft landing
BlueHalo	Strong defense/intelligence positioning	Low-Moderate — classified/sensitive sites only	Directed energy and RF defeat for cleared facilities

Threat Vector Analysis — Why C-UAS Matters for Data Centers and CNI

Surveillance & Reconnaissance

- Facility mapping from above — identifies generator locations, cooling infrastructure, security camera positions, emergency access points
- Pre-attack intelligence for kinetic or cyber operations
- Nation-state actors use commercial drones for CNI reconnaissance
- OPSEC failure: drone footage leaks design of security zones

Physical Attack Vectors

- Payload delivery: small explosive, incendiary device, EMP generator
- Targeting data center cooling towers, utility cooling towers, voltage stations
- Substation and transformer targeting for cascading grid failures
- Contraband delivery at prisons, secure facilities

Cyber & Electronic Threats

- Wi-Fi / RF reconnaissance — maps wireless networks from above
- Man-in-the-middle attacks on unencrypted facility communications
- Rogue access point insertion via drone-mounted hardware
- Signal jamming of radio communications, GPS timing systems
- Targeting synchronization signals on which power grid operations depend

Source Material Validation Notes

STATUS	ITEM	DETAIL
VALIDATED	**Dedrone as strongest commercial enterprise C-UAS player**	Confirmed. Dedrone now Axon-owned (Oct 2024). 800+ locations, 40 cities, 30 airports, 50 stadiums, 50 correctional facilities. DHS SAFETY Act certified. No other commercial player matches this footprint.
VALIDATED	**Anduril as most transformative overall**	Confirmed. $642M IDIQ Marine Corps contract. Lattice platform is the most capable AI-native C2 in the market. Defense-first but CNI relevance clear.
VALIDATED	**DroneShield as strong global tactical player**	Confirmed. ASX-listed, AU$57.5M 2024 revenue, NATO framework agreement. DroneCannon and DroneSentry widely deployed internationally.
VALIDATED	**Fortem as best interceptor innovation**	Confirmed. DroneHunter is unique — autonomous net-capture interceptor. TrueView radar. Strong airport and stadium deployments.
VALIDATED	**U.S. legal constraints on defeat technology**	Confirmed and current. The FAA Section 2209 NPRM (May 2026) creates airspace restriction authority for CNI operators but explicitly does NOT authorize defeat technology. Jamming, spoofing, and kinetic defeat remain federally restricted for private operators.
UPDATE NEEDED	**Dedrone standalone — now Dedrone/Axon**	Axon completed the acquisition October 2024. Dedrone is now part of the Axon public safety ecosystem. The combined entity adds BVLOS drone-as-first-responder capability alongside C-UAS defense.
ADDITION	**D-Fend Solutions — cyber takeover defeat**	Not in source material. EnforceAir protocol takeover technology is the commercially cleanest defeat method available in the U.S. — no jamming, no RF interference, softly lands the drone. Used at airports, prisons, and CNI. Should be in the vendor table.
MARKET DATA	**Market sizing varies significantly across analysts**	Range: $2B to $8.4B for 2025 depending on methodology (military-only vs. total). MarketsandMarkets at $6.64B is widely cited and includes commercial. CAGR consensus 24-26% through 2030+. Use $6.64B as the working figure with 25.1% CAGR to $20.3B by 2030.

Drone-as-a-Service (DaaS) Operators — Managed Aerial Security

The vendors on the preceding pages are technology companies — they build and sell detection hardware, defeat systems, and C2 software. This section covers a separate but adjacent category: **managed aerial security operators** who deploy drone technology as a subscription service, supplying the hardware, FAA-certified pilots, monitoring infrastructure, and operational response on behalf of clients. This model is the physical security equivalent of managed detection and response (MDR) in cybersecurity. The client does not buy technology — they buy a monitored, operational outcome. For enterprise and CNI security leaders, DaaS operators are often the most immediately actionable option because they absorb the FAA complexity, pilot staffing, and hardware lifecycle entirely.

Why DaaS Matters for Data Centers and CNI

A hyperscale data center operator evaluating drone security faces three barriers: (1) FAA BVLOS waiver complexity — obtaining a site-specific waiver can take months and cost up to $80,000 per location; (2) pilot staffing — FAA Part 107 certified remote pilots are specialized and expensive to hire and retain; (3) hardware management — drone-in-a-box systems require maintenance, firmware management, and weather operations expertise. DaaS operators eliminate all three barriers. The tradeoff is operational control — you are dependent on a third-party service model rather than an owned capability. For most enterprise security programs, especially those without dedicated aviation expertise, DaaS is the correct starting point.

COMPANY	FOUNDED / HQ	MODEL	KEY CREDENTIALS	CAPABILITIES	MARKET FOCUS	CNI / DATA CENTER RELEVANCE
Titan Protection & Consulting NEW ADDITION	2008 Overland Park, KS	DaaS / Managed Service	First U.S. security company to receive nationwide FAA BVLOS waiver. Feb 2026: first company approved for one-to-many BVLOS operations (single operator, multiple simultaneous autonomous aircraft). 5-Diamond UL-certified monitoring center.	Drone-in-a-box weatherproof docking stations; autonomous patrol and response; 24/7/365 SOC with FAA-licensed remote pilots; VMS integration; perimeter detection triggering; geofenced flight boundaries; 2-min avg dispatch time; 60-day deployment. Powered by FlytBase software platform.	Commercial / Industrial / Utilities / Construction / Auto / Retail	HIGH for new deployments. Nationwide BVLOS waiver eliminates per-site FAA complexity. 60% cost reduction vs. guard models documented. Relevant for outdoor perimeter at data centers, substations, utility corridors. Current portfolio skews commercial — CNI/hyperscale is the logical next market.
Dedrone / Axon DFR Platform	2014 / 2024 Washington DC	C-UAS + DaaS Hybrid	DHS SAFETY Act certified. Post-Axon acquisition (Oct 2024): nationwide BVLOS DFR capability added via DedroneBeyond. 800+ deployed locations across airports, stadiums, prisons, CNI, and law enforcement.	DedroneBeyond BVLOS autonomous drone dispatch; airspace C-UAS detection layered with DFR response; single pane of glass C2; integration with Axon body cameras and VESTA command center; RF detection + AI classification running simultaneously with DFR operations.	Law Enforcement / Public Safety / CNI / Airport / Enterprise	VERY HIGH. Unique dual-use model: detects hostile drones AND dispatches friendly drones as first responders. Most complete integrated aerial security platform for CNI. The only vendor simultaneously covering C-UAS defense and DFR response from a single platform.

COMPANY	FOUNDED / HQ	MODEL	KEY CREDENTIALS	CAPABILITIES	MARKET FOCUS	CNI / DATA CENTER RELEVANCE
Stealth Monitoring	~2009 Dallas, TX	Managed Video / Drone Patrol	#1 ranked remote video monitoring company in North America (SDM Top 100, 2024). 2,000+ employees, 40+ offices, 8 monitoring centers. Proactively monitors 100,000+ cameras. Certified monitoring infrastructure.	Proactive live video monitoring with AI-assisted threat detection; drone patrol integration as escalation layer above fixed cameras; virtual guard services; alarm response; integration with existing camera and access control infrastructure. Moving toward autonomous drone patrol as complement to core video monitoring business.	Commercial / Retail / Industrial / Multi-site Enterprise	MODERATE. Strong monitoring infrastructure and scale. Drone capability is emerging rather than core. Better fit for facilities needing comprehensive remote guarding across mixed camera and drone estate than for pure aerial perimeter security.
Alert 360 Drone Patrol	Est. 2000s Tulsa, OK	Managed Service / Drone Patrol	Established commercial security monitoring company adding autonomous drone patrol to existing guard and camera service portfolio. Operating under Part 107 framework with site-specific authorizations.	Autonomous drone patrol triggered by perimeter intrusion detection; live video stream to monitoring center; manual pilot takeover on alert; integration with existing alarm and camera systems. Positioned as technology upgrade to traditional guard and camera monitoring programs.	SMB / Commercial / Light Industrial / Retail	LOW-MODERATE. Appropriate scale for small-to-mid commercial sites. Not positioned for hyperscale data center or critical infrastructure complexity. Useful context as a baseline comparison for what a mature DaaS model looks like at smaller scale.

DaaS vs. In-House Drone Program — Decision Framework

FACTOR	DAAS OPERATOR	IN-HOUSE PROGRAM	VERDICT FOR CNI
FAA BVLOS Authority	Operator holds nationwide waiver — no site-specific filing required	Each site requires individual waiver — months of process, up to $80K/site	DaaS wins strongly — Titan's nationwide waiver is a significant structural advantage
Pilot Staffing	FAA-certified pilots supplied and managed by operator	Must recruit, certify, train, and retain Part 107 pilots internally	DaaS wins — pilot shortage is real; aviation expertise is expensive
Hardware & Maintenance	Drone-in-a-box hardware managed by operator; firmware and maintenance included	Capital purchase; requires internal drone maintenance program	DaaS wins for most enterprise buyers; in-house wins at hyperscale with volume
Operational Control	Dependent on third-party SLA; limited real-time customization	Full operational control; integrate into SOC workflows directly	In-house wins for classified or highly sensitive CNI sites
Speed to Deploy	60 days or less (Titan); faster if operator already has site credentials	6-12+ months for internal program build, FAA authorization, and pilot hiring	DaaS wins — especially relevant for new data center campuses
Cost	~60% lower than equivalent guard deployment; subscription model	Higher upfront; lower per-site unit cost at scale	DaaS wins at 1-10 sites; in-house may win at 20+ sites
Regulatory Monitoring	Operator tracks FAA rule changes; automatically compliant	Internal team must monitor FAA rulemaking and adapt	DaaS wins — Section 2209 UAFR and Part 108 BVLOS rules are complex and evolving

Sources: MarketsandMarkets, Precedence Research, Frost & Sullivan, Holland & Knight, FAA NPRM (14 CFR Part 74), Congressional Research Service, Axon/Dedrone press releases, DroneShield 2024 Annual Results, Titan Protection / FlytBase case study, AUVSI, Commercial UAV News, company websites. CoreBastion Security Consulting | C-UAS Market Intelligence 2026 | Internal Use Only | Updated May 2026