

YOUR
LOGO
HERE

MSP-Demo THREATDEFEND FOR AEROSPACE & DEFENSE SUPPLY CHAIN

PROTECTING NATIONAL SECURITY. SECURING SUPPLY CHAINS. ENSURING CMMC COMPLIANCE.

Top Cybersecurity Threats Facing Aerospace & Defense Supply Chains

- 1 Nation-state cyber espionage targeting sensitive contracts and IP
- 2 Supply chain infiltration via third-party vendors
- 3 Insider threats compromising sensitive data and systems
- 4 Non-compliance with defense mandates (e.g., CMMC 2.0, ITAR, NIST 800-171)
- 5 Ransomware attacks halting production, logistics, or development

Pain Points

Aerospace & Defense

- ✓ Stringent and evolving compliance requirements
- ✓ Complex networks involving contractors, suppliers, and subcontractors
- ✓ Protection of Controlled Unclassified Information (CUI) and export-controlled data
- ✓ Risk of advanced persistent threats (APTs) and data exfiltration

Why It Matters

Defense contractors and their suppliers face heightened threats from foreign adversaries seeking access to sensitive military technology and data. MSP-Demo ThreatDefend supports compliance, secures mission-critical systems, and protects the defense industrial base.

RELEVANT THREATDEFEND MODULES



Falcon Identity Protection

Enforce strict access control and monitor user behavior



Falcon Discover

Map and secure assets across defense supply chain systems



Falcon Exposure Management

Real-time vulnerability detection and compliance reporting



Falcon LogScale (Next-Gen SIEM)

Detect insider threats, APTs, and system misuse



24/7 SOC Monitoring

Continuous protection with response aligned to CMMC standards

Take Action



Schedule a Defense Supply Chain Cybersecurity Consultation with MSP-Demo to assess your compliance readiness, protect CUI, and strengthen your cyber defenses.