EXTRAHOP

Aerospace and Defense: Protecting Mission Readiness and Sovereign Innovation

Keep Critical Aerospace and Defense Applications and Processes Free from Threats and Disruption with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: Defending the Tactical Edge and Sovereign Innovation

The aerospace and defense industry in 2026 operates in a state of continuous gray-zone conflict. As global tensions escalate, the defense industrial base has become the primary target for adversaries seeking to degrade military readiness before kinetic engagement begins. Aerospace and defense firms face unique, high-stakes pressures where digital vulnerabilities translate directly into national security crises:

- **The Escalation of Nation-State Espionage and Sabotage:** Geopolitically motivated actors are aggressively targeting sovereign research and development, specifically the proprietary algorithms behind hypersonics, stealth materials, and autonomous flight. These adversaries utilize living-off-the-land techniques to blend with legitimate traffic, exfiltrating blueprints and flight test data over months without triggering traditional alerts. Protecting these crown jewels requires absolute internal visibility to contain lateral movement before sensitive intellectual property is siphoned.
- **The Weaponization of the Multi-Tier Supply Chain:** Adversaries have shifted focus from prime contractors to the vulnerable sub-tiers of the supply chain. In 2026, destructive campaigns target Tier 2 and Tier 3 suppliers to freeze the production of critical components or inject malicious code into hardware. Securing this ecosystem requires more than perimeter defense. It requires real-time monitoring of how data and commands flow between partners, vendors, and the production floor.
- **The Convergence of IT, OT, and Mission Systems:** The line between corporate networks and tactical weapon systems has vanished. Modern aircraft, satellites, and autonomous drones are effectively flying data centers. This convergence creates a massive agent blind spot, as traditional security software cannot be installed on sensitive flight hardware or legacy manufacturing controllers. These unmanaged assets are ideal targets for stealthy pivots into the core mission environment.
- **Regulatory Rigor and the Zero Trust Mandate:** With the full implementation of CMMC 2.0 and NIST SP 800-171 Rev 3, compliance is no longer a periodic checklist but a continuous operational requirement. Defense contractors must provide empirical proof of their security posture to maintain contract eligibility. Meeting these standards requires a definitive source of truth to validate that micro-segmentation and Zero Trust controls are actually effective across hybrid and tactical edge environments.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all interactions by decrypting and decoding 90+ protocols at 100 Gbps to protect sovereign research and high-precision manufacturing operations.

The Definitive Data Source for the AI-Enabled SOC

Provides high-fidelity wire data to power the next generation of aerospace and defense SOC automation and defenses against sophisticated nation-state actors.

AI-Powered Cyber Threat Detection

Identifies advanced attacks, lateral movement, and early-stage ransomware targeting flight telemetry, proprietary defense blueprints, and autonomous system algorithms.

Unified Agentless Visibility

Automatically discovers every asset, from legacy flight controllers and robotic production lines to cloud workloads, without installing software or impacting mission performance.

Strategic Line-Rate Decryption

Analyzes modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats in command-and-control (C2) channels and maintenance APIs.

High-Fidelity Performance Metrics

Troubleshoots complex disruptions and verifies service level agreements (SLAs) using over 5,000 wire data metrics for deep operational insight into tactical edge latency and mission-critical application performance.

Continuous Forensic Capture

Maintains an unalterable record of all network transactions to satisfy the rigorous audit and evidentiary requirements for CMMC 2.0 and NIST SP 800-171 Rev 3.

The Solution: RevealX Network Intelligence

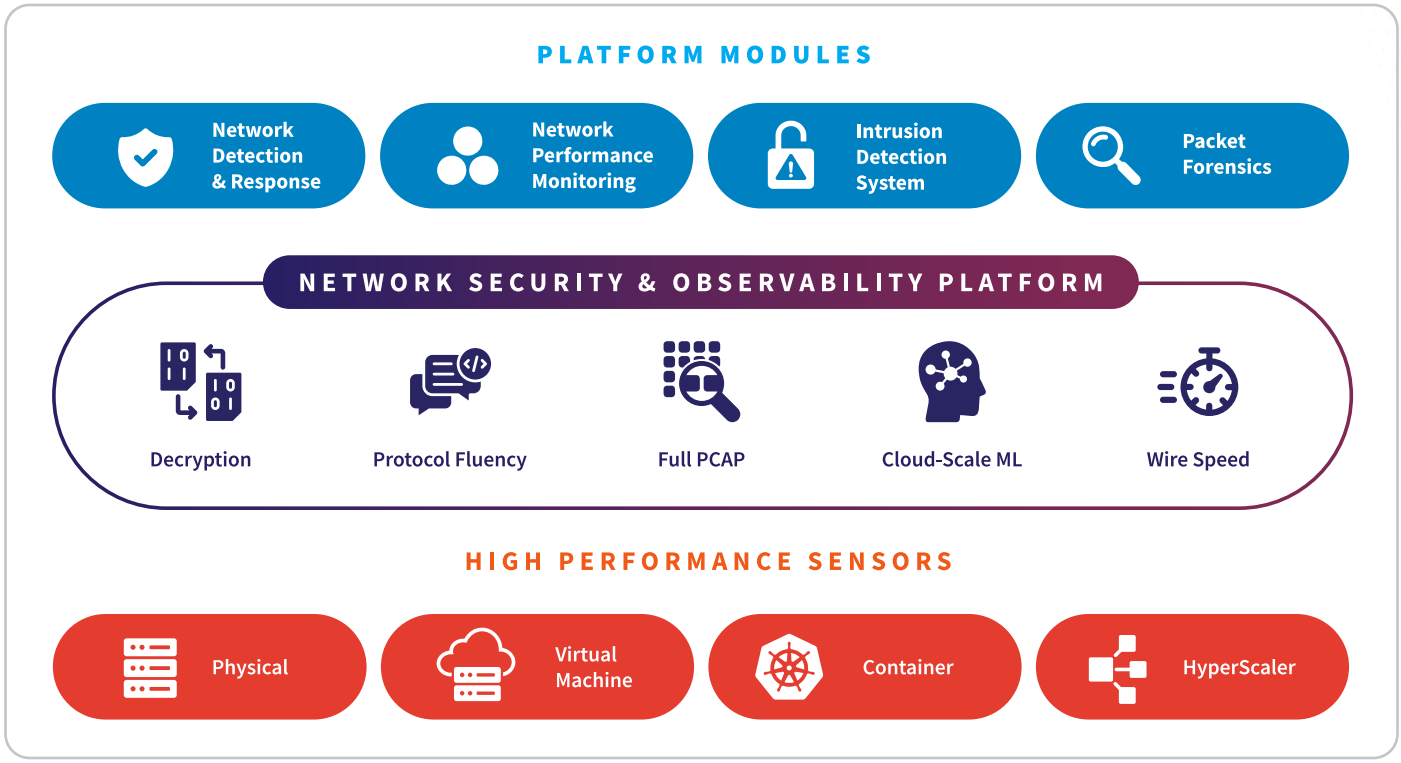
ExtraHop RevealX provides the unalterable ground truth required to secure the aerospace and defense industrial base and protect sovereign innovation. By analyzing traffic at 100 Gbps, it eliminates visibility gaps across hybrid clouds and high-precision manufacturing zones. In a sector where a single breach can compromise national security or jeopardize multi-billion-dollar research, RevealX maintains mission readiness. The platform turns the network into a definitive record of truth, allowing security teams to see every interaction without the need for intrusive agents.

RevealX resolves the agent blind spot through passive monitoring. Critical assets, including autonomous flight controllers, robotic production lines, and legacy mission systems, remain fully visible without risking stability. By baselining normal behavior, RevealX detects the subtle anomalies that indicate an adversary is manipulating telemetry or establishing a foothold in the engineering pipeline. This visibility is vital for stopping living-off-the-land tactics used by nation-state actors to blend with legitimate mission traffic.

To counter espionage and IP theft, RevealX identifies the network shifts that signal data staging for exfiltration. By exposing threats within encrypted command-and-control channels, the platform stops attackers before they can pivot from office zones into restricted tactical segments. This visibility extends across the supply chain, monitoring sub-tier partners and vendors to prevent lateral contagion. Line-rate TLS 1.3 inspection ensures that attackers cannot hide malicious payloads within encrypted mission-critical streams.

Finally, RevealX accelerates the transition to continuous compliance. It provides the unalterable record necessary for November 2026 third-party CMMC Level 2 assessments, moving firms from periodic self-attestation to permanent audit readiness. This ground truth satisfies NIST SP 800-171 Rev 3 and DFARS 252.204-7012 requirements, ensuring every transaction involving sovereign research data is accounted for. This forensic trail is essential for meeting 72-hour CIRCIA reporting windows and mitigating contract risks posed by the False Claims Act. By bridging the gap between the SOC and mission engineering, RevealX ensures defense standards are met without compromising tactical performance or production velocity.

ExtraHop NDR Platform



NDR Technology Use Cases for the Aerospace and Defense Industry

Nation-State Attacks	Detects lateral movement and exfiltration in campaigns targeting sovereign R&D, proprietary flight algorithms, and stealth material blueprints.
Threat Detection & Response	Investigates hidden threats across converged IT/OT environments, filling gaps in mission systems and manufacturing execution systems where agents fail.
Threat Hunting	Leverages behavioral baselining to find signature-less threats before they impact weapon system integrity, flight safety protocols, or production quality.
SOC Modernization	Unifies SOC and engineering workflows with AI prioritization, accelerating response times for the defense industrial base (DIB) against sophisticated actors.
Incident Response & Investigation	Delivers forensic visibility and unalterable records of mission protocols (e.g., DICOM, SATCOM, MIL-STD) for one-click root-cause analysis of system failures.
Lateral Movement	Uses peer-group clustering to detect pivots bypassing perimeters toward restricted engineering zones, sovereign clouds, and CUI segments.
Cloud Workload Security	Provides agentless visibility for cloud-integrated R&D workloads and digital twins, discovering shadow IT across AWS GovCloud and Azure Government.
Identity-Based Attacks	Correlates behavior with IAM to unmask credential abuse targeting high-value researcher workstations and privileged system administrator accounts.
Ransomware Attacks	Identifies ransomware staging and exfiltration patterns to isolate hosts before intellectual property is stolen or JIT logistics for critical parts are disrupted.
Unmanaged Devices	Monitors network traffic for unmanaged PLCs, robotic controllers, and test equipment that cannot support traditional security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled, ensuring visibility across legacy hardware and tactical edge stations.
AI Security	Monitors generative AI used for autonomous flight simulation and weapon design to prevent model poisoning or sensitive data leaks.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that NIST SP 800-207 micro-segmentation and CMMC Level 3 access controls are effective.

NPM Technology Use Cases for the Aerospace and Defense Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for flight-test systems and PLC-to-HMI production sessions.
Operational Resilience	Resolves infrastructure degradation before it hits mission continuity, ensuring availability for critical telemetry monitoring and satellite communication services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between flight operations, IT, and engineering teams.
Migrate Workloads to the Cloud	Maintains performance during R&D or logistics migration by auto-mapping dependencies and using baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps, ensuring performance for CAD/CAM servers, supply chain portals, and Kubernetes clusters.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past mission outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols, providing real-time insights into command processing time vs. network latency for mission-critical apps.

Aerospace and Defense Industry Compliance & Regulatory Use Cases

Contract Eligibility	US	CMMC 2.0 (Level 2/3)	Audit Readiness: Provides the continuous behavioral monitoring and unalterable records required for mandatory third-party assessments starting in late 2026.
Data Protection	US	NIST SP 800-171 Rev 3	Control Verification: Satisfies enhanced mandates for protecting controlled unclassified information (CUI) by offering a definitive source of network truth.
Reporting Velocity	US	CIRCIA	Incident Disclosure: Enables compliance with 72-hour reporting windows by providing instant forensics into the scope and blast radius of a breach.
Export Control	Global	ITAR / EAR	Data Sovereignty: Audits access to technical data to prevent unauthorized international transfers and ensure compliance with US Munitions List (USML) protocols.
Systems Engineering	Global	NIST SP 800-160	Integrity Assurance: Supports secure system lifecycles by detecting unauthorized changes and validating the integrity of weapon and mission systems.
Legal Risk Mitigation	US	False Claims Act	Evidentiary Support: Maintains a persistent record of security posture, providing technical proof to defend against litigation related to cybersecurity failures.

Securing Mission Readiness and Technical Superiority

ExtraHop RevealX transforms cybersecurity from a defensive cost into a strategic asset for mission success. By providing absolute visibility into the agent blind spots of tactical systems, legacy manufacturing hardware, and the sprawling sub-tier supply chain, the platform helps to ensure that aerospace and defense organizations can innovate with new technologies without creating new exploitable vulnerabilities.

RevealX reduces the risk of catastrophic intellectual property theft by identifying the subtle network shifts that signal a nation-state actor is present. This proactive defense preserves the billions invested in sovereign research and development while hardening the digital supply chain against lateral movement and unauthorized firmware manipulation. By monitoring the integrity of traffic across the entire defense industrial base, RevealX identifies threats that bypass traditional perimeters to protect sensitive production lines and proprietary blueprints.

Furthermore, by streamlining the path to CMMC 2.0 and NIST compliance, the platform protects multi-year contract revenue and reduces the administrative burden on security teams through automated, continuous evidence collection. Ultimately, the solution ensures that security never becomes a bottleneck for operational velocity. Whether at the tactical edge or across the global supply ecosystem, RevealX provides the intelligence needed to defend against sophisticated threats while ensuring the absolute reliability and availability of the systems that protect national security.

ExtraHop Can Help

ExtraHop NDR provides a critical advantage by delivering the comprehensive network intelligence required to surface sophisticated lateral movement and internal threats that legacy tools often miss.

Learn more about our successful customer deployments:
Leading Aerospace Manufacturer
Viasat

Or contact us to schedule your personalized demo and security assessment.

> "You can't secure what you can't see. With ExtraHop, we've got eyes on every interaction that takes place on our network. That is the first step to protecting our environment."

SENIOR CYBER SECURITY ENGINEER
Telecommunications Company

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com