EXTRAHOP

ExtraHop RevealX™ for Federal Defense and Intelligence Agencies: Mission Assurance and Nation-State Defense

Meet Mission Objectives with Unalterable Network Truth

SOLUTION BRIEF

Industry Challenge

In the 2026 landscape, the Department of War and Intelligence Community operate under a state of continuous engagement with advanced persistent threats. The operational threat has pivoted from simple cyber espionage to persistent nation-state pre-positioning and the functional sabotage of mission-critical military infrastructure. According to the 2026 National Security Agency and Department of War Zero Trust Implementation Guidelines, defense forces must move away from static, perimeter-based defenses. The mission demands a platform that monitors internal network context to intercept sophisticated actors utilizing valid credentials and "living off the land" tactics inside tactical and cloud-integrated weapon systems before destructive commands execute.

- **The Pre-Positioning of Nation-State Sabotage:** Geopolitically motivated groups use living-off-the-land techniques and valid credentials to maintain a persistent presence inside networks for crisis leverage. Moving from data theft to functional destruction, these actors aggressively target infrastructure and communications to systematically degrade operational readiness and undermine mission assurance.
- **The Invisibility of Encrypted Command and Control:** Advanced state-sponsored adversaries hide their lateral movement and exfiltration staging within standard encrypted HTTPS tunnels, which account for the vast majority of theater operations. Without non-intrusive, line-rate decryption capable of observing live payloads, defenders remain blind to malicious activity that easily evades perimeter security and signature-based tools.
- **The Zero Trust Target Level Mandate:** Organizations are under pressure to meet Department of War Zero Trust Strategy requirements by 2027, focusing heavily on the Visibility and Analytics pillar. Static architecture diagrams are insufficient under active adversary pressure, yet many environments still lack the deep internal network monitoring required to detect unauthorized enclave pivots.
- **The Agent Blind Spot in Tactical Edge Systems:** Mission assurance relies heavily on connected weapon systems, tactical field devices, and automated logistics networks that cannot host traditional endpoint protection software. These unmanaged nodes communicate via implicit trust models and specialized protocols, serving as prime initial access points for near-peer actors to compromise restricted military enclaves.

KEY CAPABILITIES

Depth and Breadth of Network Detection and Response Performance

Decrypts and decodes over 90 protocols at speeds up to 100 Gbps to secure high-throughput tactical communication lines, Joint All-Domain Command and Control systems, and massive defense data centers.

Definitive Data Source for the AI-Enabled Security Operations Center

Powers defense and intelligence Security Operations Center automation applications with unalterable network data, eliminating investigative friction to accelerate response times for critical theater incidents.

AI-Powered Cyber Threat Detection

Utilizes cloud-scale machine learning and behavioral baselining to identify stealthy near-peer nation-state attacks, lateral movement, and early-stage ransomware targeting critical military infrastructure.

Unified Agentless Visibility

Automatically discovers 100% of assets across the mission fabric, including unmanaged weapon systems, specialized tactical edge devices, and hybrid-cloud workloads without software installs or risking platform stability.

Strategic Line-Rate Decryption

Analyzes modern encrypted traffic, including Transport Layer Security 1.3 and Perfect Forward Secrecy workflows, to expose hidden threats and living-off-the-land tactics without adding latency to time-sensitive command and control communications.

High-Fidelity Performance Metrics

Uses over 5,000 wire data metrics to troubleshoot complex disruptions, map critical asset interdependencies, and verify operational resilience for mission-essential defense workloads.

Continuous Forensic Capture

Maintains unalterable network audit trails and packet-derived evidence to satisfy advanced logging directives, support 72-hour reporting mandates under Cyber Incident Reporting for Critical Infrastructure Act, and provide empirical validation for Department of War Zero Trust Target Levels.

The Solution: RevealX Network Intelligence

ExtraHop RevealX provides the unalterable ground truth required to secure the defense mission and maintain an operational advantage. By turning network traffic into a continuous source of behavioral intelligence, RevealX gives defenders the evidence needed to detect near-peer adversaries after initial access, specifically when they are conducting reconnaissance, abusing credentials, moving laterally, or hiding command and control inside encrypted administrative traffic. In an era where nation-state actors frequently modify or suppress logs, RevealX ensures mission continuity by turning the network into a definitive record of truth that cannot be tampered with.

RevealX solves the weapon system blind spot by providing agentless, passive monitoring of over 90 protocols. Critical infrastructure, from tactical sensors to legacy diagnostic systems, is fully visible without risking system stability or crashing fragile controllers. By baselining normal behavior, defense security teams can instantly detect anomalies indicating that an adversary is establishing a foothold or staging data for exfiltration. This out-of-band approach is essential for identifying threats like fileless malware and living-off-the-land tactics that blend with legitimate command and control traffic.

To counter strategic espionage, RevealX identifies subtle shifts in network behavior signifying data exfiltration staging. Strategic, line-rate decryption of Transport Layer Security 1.3 and Perfect Forward Secrecy traffic up to 100 Gbps exposes hidden payloads within encrypted management streams without adding latency to time-sensitive tactical workflows. Furthermore, the platform operationalizes Zero Trust execution by providing empirical proof that microsegmentation policies, workload communications, and access paths are working as intended in real, contested environments.

Beyond detection, RevealX accelerates investigations by 63%, helping cyber teams rapidly determine the path, blast radius, and operational impact of an incident. This unified approach bridges the gap between security and tactical network operations, ensuring defensive measures preserve the availability, speed, and reliability of critical military infrastructure.

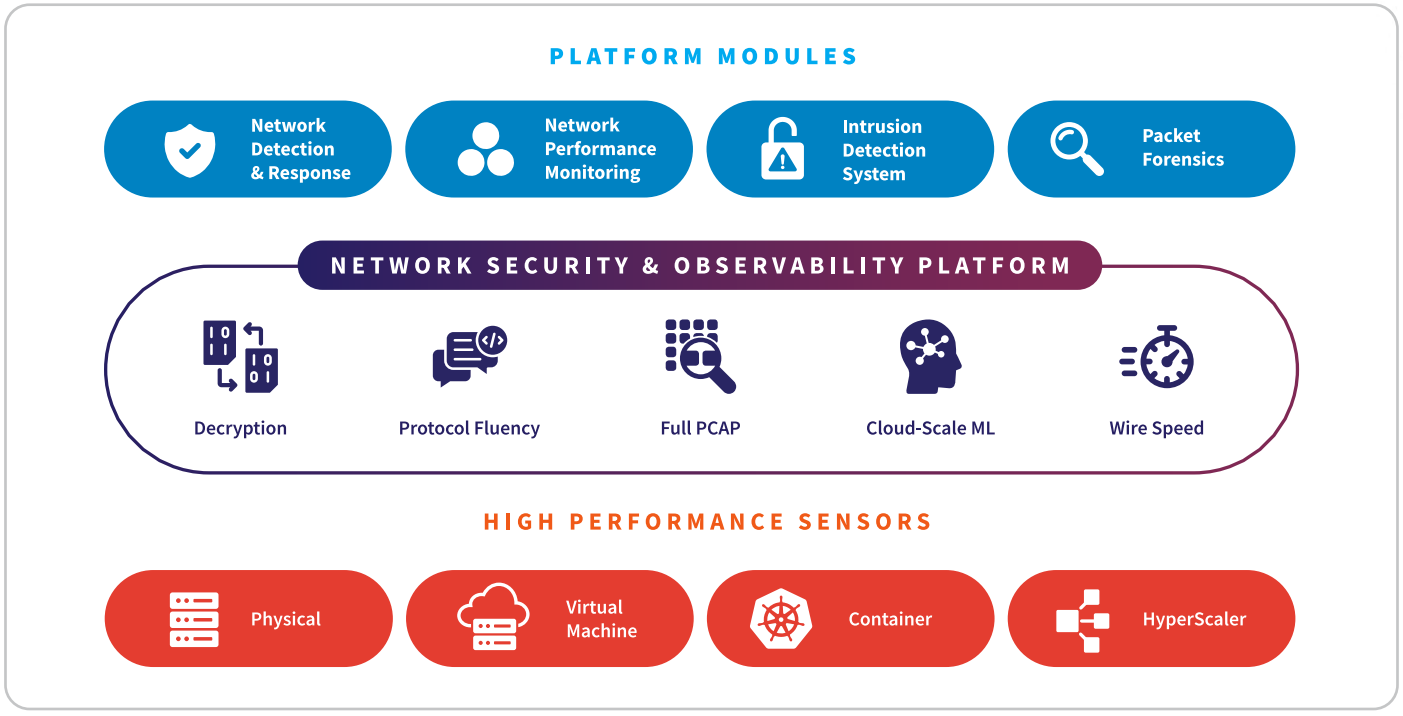
FedRAMP®

As global events and nation-state threats grow more sophisticated, the urgency to accelerate cyber defenses goes beyond compliance. It's essential for protecting critical infrastructure, public services, and national security.

RevealX Federal, the FedRAMP-authorized NDR platform for government, delivers the visibility and real-time network intelligence federal agencies need to modernize cyber defenses. By eliminating blind spots, RevealX ensures mission resilience, allowing cyber and IT teams to investigate faster, stop threats faster, and move at the speed of risk.

FedRAMP™

ExtraHop NDR Platform



NDR Technology Use Cases for Defense & Intelligence Agencies

Nation-State Attacks	Detects stealthy lateral movement and data staging in campaigns targeting military enclaves, strategic intelligence, and command and control infrastructure.
Threat Detection and Response	Investigates hidden threats across converged information technology and specialized weapon systems, filling visibility gaps in tactical field operations and automated logistics hubs.
Threat Hunting	Leverages behavioral baselining to find signatureless anomalies and protocol deviations before they impact mission assurance or tactical communications.
SOC Modernization	Unifies security operations center and network operations center workflows with artificial intelligence prioritization to ensure lethality and operational advantage, accelerating response times for critical theater missions.
Incident Response and Investigation	Delivers forensic visibility and unalterable records of administrative commands for rapid root-cause analysis of mission failure or system outages.
Lateral Movement	Uses peer group clustering and protocol decoding to detect pivots between sensitive enclaves and toward critical mission controllers or safety systems.
Cloud Workload Security	Provides agentless visibility for hybrid and multi-cloud environments, discovering unmanaged assets across AWS GovCloud and Azure Government.
Identity-Based Attacks	Correlates network behavior with identity and access management to unmask credential abuse targeting high-value tactical workstations and privileged administrative gateways.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate infected hosts before exfiltration of strategic intelligence or total paralysis of mission systems.
Unmanaged Devices	Monitors network traffic for unmanaged assets, including weapon systems, tactical sensors, and field hardware that cannot host traditional security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity even when endpoint agents are disabled, ensuring persistent visibility across legacy platforms and human machine interface kiosks.
AI Security	Monitors interactions with generative artificial intelligence tools and autonomous agents used for battle management, predictive maintenance, or route optimization to prevent data leaks.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that microsegmentation and internal network security monitoring policies remain effective across the mission fabric.

NPM Technology Use Cases for Defense & Intelligence Agencies

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for Joint All Domain Command and Control and tactical transactions.
Operational Resilience	Resolves infrastructure degradation before it hits mission continuity, ensuring survival during kinetic operations and emergency response services.
Troubleshooting and Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between tactical field operations, HQ network teams, and mission partners.
Migrate Workloads to the Cloud	Maintains performance during large-scale mission migrations to impact the cloud by auto mapping dependencies and validating successful delivery.
Monitor Critical Workloads	Provides deep visibility into mission-essential applications and Kubernetes, ensuring performance for command and control and supply chain application program interfaces.
Forensic-Grade Investigations	Combines metadata and scalable packet capture for an unalterable record, enabling deep-dive analysis into past mission outages or telemetry drops during active ops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols, providing real-time insights into command processing time versus network latency in high-volume tactical hubs.

Defense & Intelligence Agencies Compliance & Regulatory Use Cases

Zero Trust Mandates	United States	DoD Zero Trust Strategy and EO 14028	Visibility and Analytics Pillar: Satisfies Target Level requirements and federal advanced logging mandates by providing full internal network monitoring and segmentation validation.
Asset Visibility	United States	CISA BOD 26-02	Tactical Edge Modernization: Automatically inventories all field-deployed routers, firewalls, and sensors to identify and replace end-of-support hardware, preventing nation-state actors from exploiting legacy vulnerabilities in unagentable mission hardware.
Cloud Security Standards	United States	DoD Cloud SRG	Enclave Protection: Provides the required visibility for workloads in AWS GovCloud and Azure Government to maintain authorization.
Supply Chain Integrity	United States	CMMC 2.0	Blueprinting and Data Protection: Automates protection of controlled unclassified information by identifying unauthorized exfiltration of engineering data and blueprints.
Enhanced Security Controls	United States	NIST SP 800-172	APT Defense: Automates advanced technical controls for continuous monitoring and system integrity to defend high-value assets against persistent threats.
Mandatory Incident Disclosure	United States	CIRCIA	72-Hour Reporting: Delivers the unalterable ground truth evidence required to meet mandatory reporting windows for incidents affecting critical infrastructure.

Customer Benefits: Ensuring Mission Resilience and Operational Advantage

Visibility into network truth is the foundational requirement for securing the defense mission. RevealX provides the real-time insights required for Joint All-Domain Command and Control systems, tactical logistics, and forward-deployed operations. By monitoring the wire, defense and intelligence agencies safeguard against near-peer nation-state sabotage and protocol anomalies that jeopardize weapon platform continuity and warfighter readiness.

- **Eliminating the Investigative Friction of Tactical Audits:** RevealX provides the unalterable ground truth needed to satisfy rigorous military readiness evaluations and advanced federal security standards. By observing actual wire traffic instead of modifiable host logs, defenders gain definitive forensic evidence required to map the complete blast radius of an intrusion and support high-consequence national security decisions.
- **Securing the Agentless Tactical Edge:** RevealX protects the sprawling ecosystem of unmanaged weapon systems, tactical communication links, and field devices that traditional security agents cannot reach. This agentless visibility identifies stealthy lateral movement, living-off-the-land tactics, and credential abuse before adversaries can compromise restricted military enclaves.
- **Meeting 2026 Mandates for Operational Transparency:** With federal directives requiring the continuous monitoring of defense environments, RevealX provides an automated discovery process to map asset interdependencies. This passive visibility ensures operators stay ahead of advanced persistent threat activity while maintaining perfect uptime for mission-essential networks.
- **Safeguarding Modernization and Cloud Migration**: As agencies transition to hybrid environments across AWS GovCloud and Azure Government Impact Levels 5 and 6, RevealX ensures that security measures do not introduce latency. By performing line-rate decryption of Transport Layer Security 1.3, the platform exposes threats hidden within encrypted streams without disrupting tactical communication streams.

Ultimately, these capabilities transform defense cybersecurity into a strategic asset, protecting institutional stability and operational readiness in contested domains. RevealX ensures that every entity on the network is identified and classified, providing the Visibility Pillar essential for a validated Department of War Zero Trust Target Level architecture.

> "[An attacker's] worst nightmare is that out-of-band network tap that really is capturing all the data, understanding anomalous behavior that's going on, and someone is paying attention to it. You've gotta know your network. Understand your network, because [the attacker] is going to."

ROB JOYCE
Director of Cybersecurity at the National Security Agency (NSA)

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.

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

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