EXTRAHOP

ExtraHop RevealX™ for Federal Civilian Agencies: Operational Resilience and Compliance

Achieve Operational Resilience and Federal Compliance with Unalterable Network Truth

SOLUTION BRIEF

Civilian Agency Challenges: Transparency Under Pressure

Federal Civilian Executive Branch (FCEB) agencies are the stewards of the nation's most sensitive citizen data and essential public services. By 2026, the digital perimeter has vanished, replaced by a hyper-connected mesh of hybrid cloud workloads, citizen-facing SaaS portals, and an explosion of unmanaged internet of things (IoT) devices. While these innovations improve the citizen experience, they have created a visibility gap where sophisticated adversaries use AI-powered social engineering and living-off-the-land tactics to bypass traditional perimeter defenses.

- **The Escalation of Nation-State Sabotage:**
  Geopolitically motivated actors and nation-state-aligned ransomware groups have transitioned from data theft to functional destruction. In 2026, these actors persistently target congressional communications and federal infrastructure, utilizing gray-zone tactics to disrupt economic stability and undermine public trust.
- **The Investigative Friction of Office of Management of Budget (OMB) M-21-31:**
  Agencies are held to a four-tier maturity model demanding comprehensive logging and rapid incident response. Many still struggle with dark corners of the network, such as shadow IT, unknown cloud services, and misconfigured sensors that create broken audit trails, thwarting the ability to rapidly respond to alerts on high-priority systems.
- **The Agent Blind Spot in Public Service:**
  Critical services rely on legacy infrastructure and specialized IoT, such as mail sortation, building sensors, and 4K surveillance, that cannot host security agents. These unmanaged nodes serve as entry points for ransomware groups to move laterally toward sensitive citizen databases while remaining invisible to traditional endpoint detection and response (EDR) tools.
- **Reporting Convergence and Compressed Timelines:**
  2026 mandates like M-21-31 and Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) have set a new standard for transparency, with 72-hour windows for incident disclosure. Without an immutable source of ground truth, agencies spend precious hours manually correlating fragmented logs instead of executing remediation during mandatory reporting windows.

KEY CAPABILITIES

Depth and Breadth of Network Detection and Response (NDR) Performance

Decrypts 90 plus protocols at 100 Gbps to secure high-volume citizen service portals and large-scale federal data centers.

Definitive Data Source for the AI-Enabled Security Operations Center (SOC)

Powers federal SOC automation with high-fidelity wire data to eliminate investigative friction and accelerate remediation for public sector incidents.

AI-Powered Cyber Threat Detection

Uses cloud-scale machine learning and behavioral baselining to detect sophisticated nation-state attacks and ransomware targeting critical government infrastructure.

Unified Agentless Visibility

Automatically discovers 100% of cyber assets, including unmanaged IoT and legacy edge devices, without software installs to satisfy FY24/25 Federal Information Security Modernization Act (FISMA) (M-24-04) and Cyber and Infrastructure Security Agency (CISA) BOD 26-02 requirements.

Strategic Line-Rate Decryption

Analyzes TLS 1.3 and Transport Layer Security (TLS) 1.3 and Perfect Forward Secrecy (PFS) traffic to expose hidden threats and living-off-the-land tactics without adding latency to time-sensitive federal workflows.

High-Fidelity Performance Metrics

Uses 5,000 plus metrics to troubleshoot disruptions and verify service level agreements (SLAs) for mission-critical applications and hybrid cloud government workloads.

Continuous Forensic Capture

Maintains unalterable network audit trails to meet OMB M-21-31 (EL1-EL3) logging tiers and support 72-hour reporting mandates under CIRCIA for agencies managing critical infrastructure.

The Solution: RevealX Network Intelligence

ExtraHop RevealX provides the unalterable ground truth required to secure the federal civilian mission and maintain essential public services. By analyzing every packet at line rates up to 100 Gbps, RevealX eliminates visibility gaps across hybrid cloud environments and distributed agency networks. In an era where logs are often suppressed or modified by sophisticated adversaries, RevealX ensures operational continuity by turning the network into a definitive record of truth that cannot be tampered with.

RevealX solves the agent blind spot by providing agentless, passive monitoring of over 90 protocols. Critical infrastructure, from specialized mail sortation and building sensors to legacy diagnostic systems, is fully visible without risking system stability or service delivery. By baselining normal behavior, federal security teams can instantly detect anomalies indicating that an adversary is establishing a foothold or manipulating telemetry. This visibility is essential for identifying living-off-the-land tactics and fileless malware that blend with legitimate administrative traffic.

To counter nation-state sabotage and strategic espionage, RevealX identifies subtle shifts in network behavior signifying the staging of sensitive data for exfiltration. By exposing threats within encrypted management traffic via strategic decryption, the platform stops attackers before they pivot from public-facing segments into restricted agency cores. Line-rate inspection of TLS 1.3 ensures attackers cannot hide malicious payloads or command and control patterns within cloud-integrated service streams.

Beyond detection, RevealX accelerates investigations by 63%, helping agencies meet the rigorous reporting requirements of OMB M-21-31, FISMA, and CIRCIA. It provides a definitive forensic record of all network transactions, enabling agencies to achieve Event Logging Tier 3 (EL3) logging maturity and support 72-hour reporting mandates. This unified approach bridges the gap between SOC and information technology (IT) operations teams, combining real-time security detection with high-fidelity performance metrics to ensure security measures do not introduce latency.

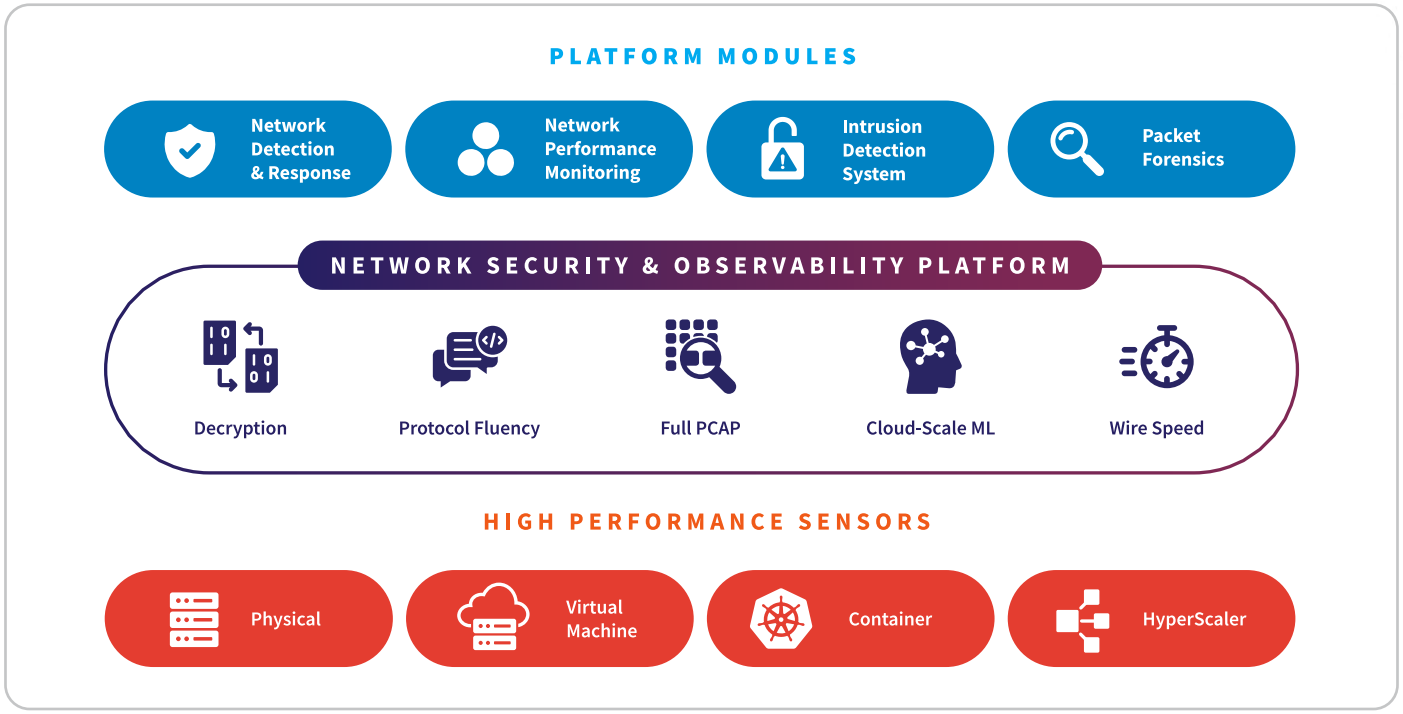
FedRAMP®

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 Federal Civilian Agencies

Nation-State Attacks	Detects stealthy lateral movement and data staging in campaigns targeting federal personally identifiable information (PII) databases, Congressional communications, and strategic citizen service infrastructure.
Threat Detection and Response	Investigates hidden threats across converged IT and specialized operational technology (OT) environments, filling visibility gaps in high-volume mail sortation centers and automated federal warehouses.
Threat Hunting	Leverages behavioral baselining to find signatureless anomalies and protocol deviations before they impact critical public safety, energy distribution, or national healthcare systems.
SOC Modernization	Unifies SOC and Network Operations Center (NOC) workflows with AI prioritization to reduce alert fatigue, accelerating response times for critical agency mission delivery and high-traffic citizen portals.
Incident Response and Investigation	Delivers forensic visibility and unalterable records of administrative commands and protocol interactions for rapid root-cause analysis of federal system outages.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots from corporate IT toward critical infrastructure controllers, building automation, and safety systems.
Cloud Workload Security	Provides agentless visibility for hybrid and multi-cloud environments, discovering shadow IT and unmanaged assets across AWS GovCloud, Azure Government, and Google Assured Workloads.
Identity-Based Attacks	Correlates network behavior with identity and access management (IAM) to unmask credential abuse targeting high-value federal workstations, administrative gateways, and privileged system accounts.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate infected hosts before exfiltration of sensitive PII or total paralysis of essential public services.
Unmanaged Devices	Monitors network traffic for unmanaged federal assets, including IoT sensors, medical devices, and handheld scanners, 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 federal systems and specialized human-machine interface (HMI) kiosks.
AI Security	Monitors interactions with generative AI tools and autonomous agents used for federal route optimization, citizen support, or predictive maintenance to prevent data leaks.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that micro-segmentation and internal network security monitoring (INSM) policies remain effective across the agency.

NPM Technology Use Cases for Federal Civilian Agencies

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for citizen-facing applications and high-frequency federal transactions.
Operational Resilience	Resolves infrastructure degradation before it hits mission continuity, ensuring availability for critical agency management and emergency response services.
Troubleshooting and Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between federal field operations, IT network teams, and third-party contractors.
Migrate Workloads to the Cloud	Maintains performance during large-scale enterprise resource planning (ERP) or database migrations by auto-mapping dependencies and using on-premises baselines to validate successful cloud delivery.
Monitor Critical Workloads	Provides deep visibility into high-value apps and Kubernetes, ensuring performance for citizen portals, payment gateways, and supply chain APIs.
Forensic-Grade Investigations	Combines metadata and scalable packet capture (PCAP) for an unalterable record, enabling deep-dive analysis into past agency service outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols, providing real-time insights into command processing time versus network latency in high-volume federal hubs.

Federal Civilian Agencies Compliance & Regulatory Use Cases

Advanced Event Logging	United States	OMB M-21-31	Investigative Maturity: Provides the unalterable network records and persistent forensic storage required to achieve packet capture (PCAP) (advanced) maturity.
Asset Visibility	United States	CISA BOD 26-02	Unsupported Edge Replacement: Automatically inventories all edge devices, including routers and firewalls, to identify and replace end-of-support (EOS) hardware by 2026 deadlines.
Zero Trust Adoption	United States	Executive Order 14028	Visibility Pillar: Validates internal segmentation and identifies lateral movement to satisfy federal Zero Trust requirements for non-signature threat detection.
Mandatory Incident Disclosure	United States	CIRCIA	72-Hour Reporting: Delivers the ground truth evidence required to rapidly assess materiality and meet mandatory 72-hour reporting windows for federal incidents.
Security Controls	United States	NIST SP 800-53 Rev 5	Audit & Accountability: Automates technical controls for continuous monitoring (CA-7), system integrity (SI), and incident response (IR).

Customer Benefits: Ensuring Mission Resilience and Public Trust

Visibility into network truth is the foundational requirement for securing the federal civilian mission. RevealX provides the real-time insights required for high-volume citizen service delivery, automated mail sortation, and distributed emergency response. By monitoring the wire, federal agencies safeguard against nation-state sabotage and protocol anomalies that jeopardize mission continuity and public safety.

- **Eliminating the Investigative Friction of Federal Audits:** RevealX provides the unalterable ground truth needed to satisfy OMB M-21-31 requirements, enabling agencies to achieve EL3 (advanced) logging maturity. By observing actual traffic instead of modifiable logs, agencies gain the definitive forensic evidence required for Congressional testimony and Inspector General audits.
- **Securing the Agentless Public Infrastructure:** RevealX protects the sprawling ecosystem of unmanaged IoT, legacy building sensors, and 4K surveillance systems that traditional security agents cannot reach. This agentless visibility identifies lateral movement and credential abuse before adversaries can compromise high-value citizen databases or exfiltrate sensitive PII.
- **Meeting 2026 Mandates for Operational Transparency:** With CISA BOD 26-02 requiring the immediate inventory and replacement of unsupported edge devices, RevealX provides an automated discovery process to identify end-of-support hardware. This continuous monitoring ensures agencies stay ahead of mandatory reporting windows while maintaining the 99.9% uptime expected for essential services.
- **Safeguarding Modernization and Cloud Migration:** As agencies transition to hybrid cloud and AI-integrated architectures, RevealX ensures that security measures do not introduce latency. By performing line-rate decryption of TLS 1.3, RevealX exposes threats hidden within encrypted service streams without disrupting the performance of mission-critical citizen portals.

Ultimately, these capabilities transform federal cybersecurity into a strategic asset, protecting brand reputation and institutional stability in an era of constant risk. RevealX ensures that every entity on the network is identified and classified, providing the Visibility Pillar essential for a Zero Trust Architecture and uninterrupted government innovation.

> "[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