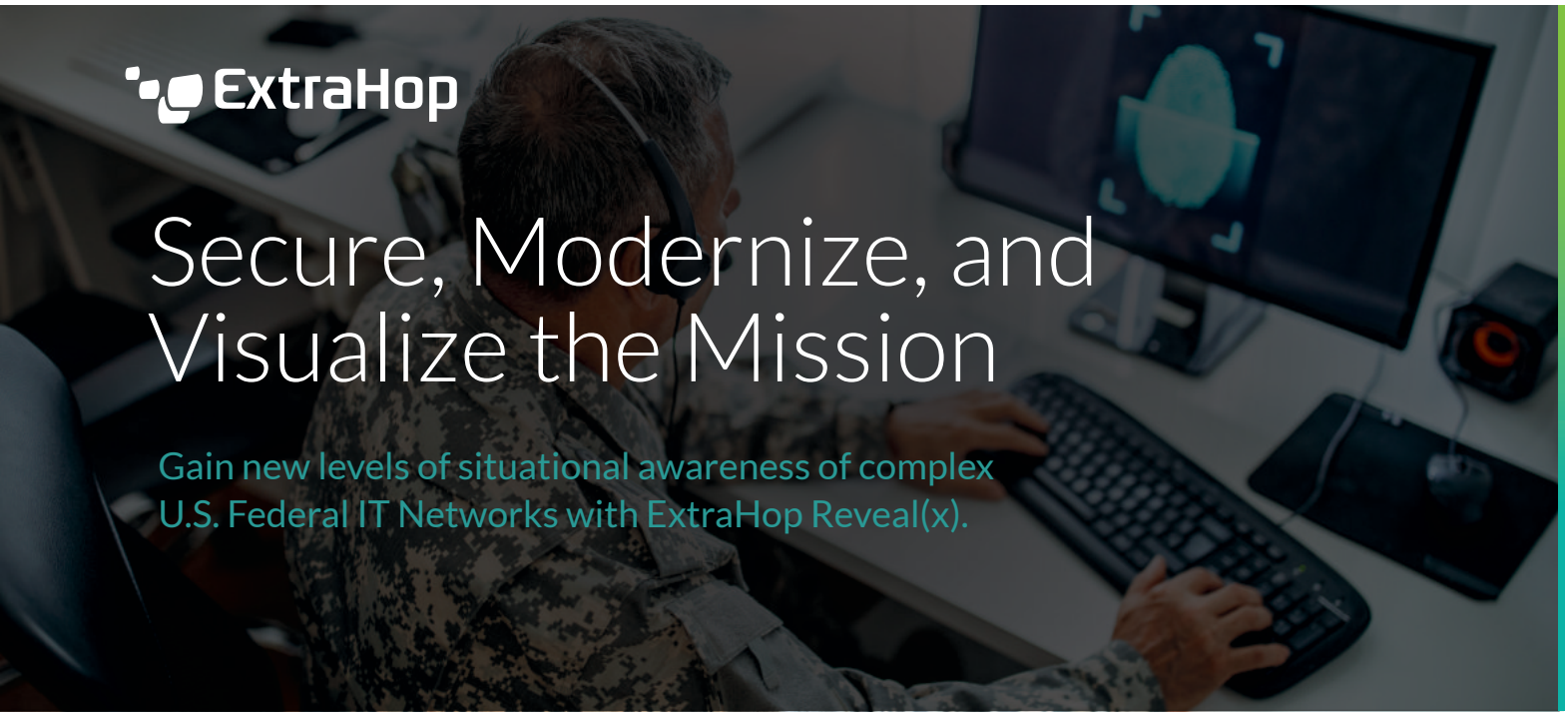

Secure, Modernize, and Visualize the Mission

Gain new levels of situational awareness of complex U.S. Federal IT Networks with ExtraHop Reveal(x).

Federal government IT operations and cyber teams are on a mission. Each day they are tasked to ensure every digital interaction a government employee, military service member, or contractor experiences is safeguarded from ever-present cyber threats and free from performance issues.

The consequences of one missed network intruder, one outage due to a malicious software attack, or one broken user experience jeopardize the mission. It risks the Federal government's ability to meet its mandate. Despite what's at stake, IT and cyber teams face constant headwinds:

> "Without full operational visibility, actionable insight suffers.

Modernization and consolidation efforts accelerate the adoption of cloud computing and connected Internet of Things (IoT) devices.

Highly scalable and reliable digital experiences powering agency workflows result in a complex hybrid of IT systems, legacy applications, and Software-as-a-Service (SaaS).

Increased teleworking demands driven by workplace safety measures and flexible work options introduce new risks to the confidentiality and integrity of sensitive data.

Compliance with Federal regulatory requirements including the Federal Information Security Modernization Act (FISMA), Risk Management Framework (RMF), and NIST guidance and policies add increased overhead and reporting obligations.

The Challenge: New IT Realities Demand New Levels of Operational Visibility

Traditional systems management and security controls at the edge or end-point—like Next-Generation Firewalls, Log monitoring, Intrusion Detection Systems, and Network Access Control—are insufficient by themselves to address dynamic risk management, data protection, and service level challenges. They lack the proper visibility, situational awareness, and real-time data necessary to detect and correlate events to rise above the noise. The impact of lean budgets, tool sprawl, and skill shortages further exacerbate these mission realities.

Without full operational visibility, actionable insight suffers. Without actionable insight, bad actors can hide their malicious activities and degraded user experiences can fester in the dark spaces created by the absence of a complete picture.

The Opportunity: Closer Collaboration, Lower Risk, and Faster Response

Federal government cyber and network operations—whether as different functional teams or individuals wearing multiple hats—often act like siloed entities. Each with its own culture, tools, and processes. These barriers are beginning to stand between mission outcomes and mandated modernization.

Bringing these groups, processes, and separate tools closer boost an agency's ability to support the best user experience and secure the environment. It creates a new opportunity for Federal government IT organizations to provide faster response to unplanned downtime, strengthen security measures, and achieve new efficiencies across all functions.

UNIFY VISIBILITY TO IMPROVE CYBER HYGIENE AND APPLICATION PERFORMANCE

Visibility is a cornerstone of security frameworks and methodologies like Continuous Diagnostics and Mitigation (CDM), NIST Cybersecurity Framework (CSF), and MITRE ATT&CK. Gaining complete, real-time visibility is important for maintaining compliance and defending against cyber threats. It is also critical for staying ahead of network or application issues before they can have an impact on users.

Federal government IT functions that closely collaborate to identify gaps, blind spots, troubleshoot degraded experiences, and uncover threats increase the speed and scale of an agency's digital workflows by:

- Identifying user experience issues to reduce troubleshooting time through real-time operational awareness
- Continuously monitoring and automating audits to stay compliant with Risk Management Framework requirements
- Detecting suspicious behaviors and prioritizing forensic investigations and remediation to ensure the highest risk cyber threats are rapidly addressed.

OPTIMIZE CYBER AND IT OPERATIONS

The pervasiveness, velocity, and scope of today's sophisticated threats demand an integrated approach. However, Federal government agencies face difficult trade-offs as different functions grapple with tool sprawl and skill shortages. This leads to slow response times to issues and distracts from delivering the outcomes of major modernization initiatives.

Federal government IT teams that break down silos by standardizing on a single source of truth eliminate operational friction and boost productivity by:

- Consolidating and converging objectives between cyber protection and network operations teams.
- Embracing advanced encryption—like TLS 1.3—without losing the ability to detect any malicious behavior or performance issues hiding within encrypted traffic.
- Gaining cost efficiencies while still answering operational questions like "what is on the network?", "who is on the networking?" and "what is happening on the network?"

ENACT A HOLISTIC AND FUTURE PROOF APPROACH

Cloud infrastructure as a service (IaaS) offers Federal government IT tremendous benefits and new options to meet the scalability, flexibility, and consolidation demands placed on agency networks. Similarly, the implementation of sanctioned enterprise IoT devices like printers, smart video cameras, and IP phones, lead to modernized and secure experiences. However, these advancements introduce new performance and security challenges which can quickly erode the expected benefits.

Federal government cyber, IT, and DevSecOps teams that embrace a holistic and cloud-ready approach to operations achieve comprehensive visibility by:

- Discovering, identifying, and mapping all assets across these complex, hybrid networks.
- Maintaining a real-time inventory of all devices—whether managed or not—based on observed behavior
- Unifying inside-the-perimeter threat hunting, forensic investigation, and remediation from a single operational pane of glass—for all workloads—across on-premises, remote sites, and the cloud.

The Solution: Cloud-Ready Network Detection and Response

Securing modern Federal Agencies means protecting a complex web of workloads consisting of hardware, applications, and data spread across the edge, core, remote sites, cloud deployments, and mobilized workforces. ExtraHop Reveal(x) cloud-ready network detection and response (NDR) provides vital intelligence to understand, modernize, and secure Federal agency hybrid environments from the inside out.

Unlike perimeter-focused tools that rely on fixed agents or gateway devices, Reveal(x) agentless network traffic analysis passively monitors all network interactions. The result is the complete visibility, real-time detection, and intelligent response needed to solve problems ranging from slow applications to addressing gaps in both the east-west and north-south corridors.

Eliminate Blind Spots

Continuous visibility across all devices and workloads

Monitoring of all East-West and North-South Traffic

Line-rate decryption of SSL/TLS 1.3 encrypted traffic

Detect Threats That Other Tools Miss

Cloud-scale ML applies over one million predictive models

Threat intelligence derived from petabytes of data per day

Behavioral analysis using more than 5000 features of data

Act Quickly to Defend Your Business

Investigate from detection to forensics in a few clicks

Integrated response automation to immediately act on threats

With this more complete picture, Federal government cyber and IT teams can identify vectors of attack ahead of disruption, understand the full implication security events have on application performance, and speed resolution for greater peace of mind.

86% REDUCTION IN UNPLANNED DOWNTIME

95% SPOT ISSUES FASTER

59% REDUCTION IN TIME-TO-RESOLUTION

HOW TO BUY

ExtraHop has been selling into Federal Agencies since 2011 and has production units supporting a number of Federal Civilian, DoD, and Intelligence Agencies. All engineering and support for the ExtraHop platform resides within the United States, and ExtraHop has dedicated Federal sales and product management teams located within the Washington D.C. Metropolitan Area. We're dedicated to simplifying your acquisition process. ExtraHop's solutions are available on the GSA Schedule GS-35F-0119Y and numerous other contract vehicles.

ABOUT EXTRAHOP NETWORKS

Cyber attackers have the advantage. ExtraHop is on a mission to help you take it back with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats––before they can compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, enterprises can detect malicious behavior, hunt advanced threats, and forensically investigate any incident with confidence. ExtraHop has been recognized as a market leader in network detection and response by IDC, Gartner, Forbes, SC Media, and numerous others.

When you don't have to choose between protecting your business and moving it forward, that's security uncompromised. Learn more at www.extrahop.com

ExtraHop

520 Pike Street, Suite 1600
Seattle, WA 98101
877-333-9872 (voice)
206-274-6393 (fax)
info@extrahop.com
www.extrahop.com