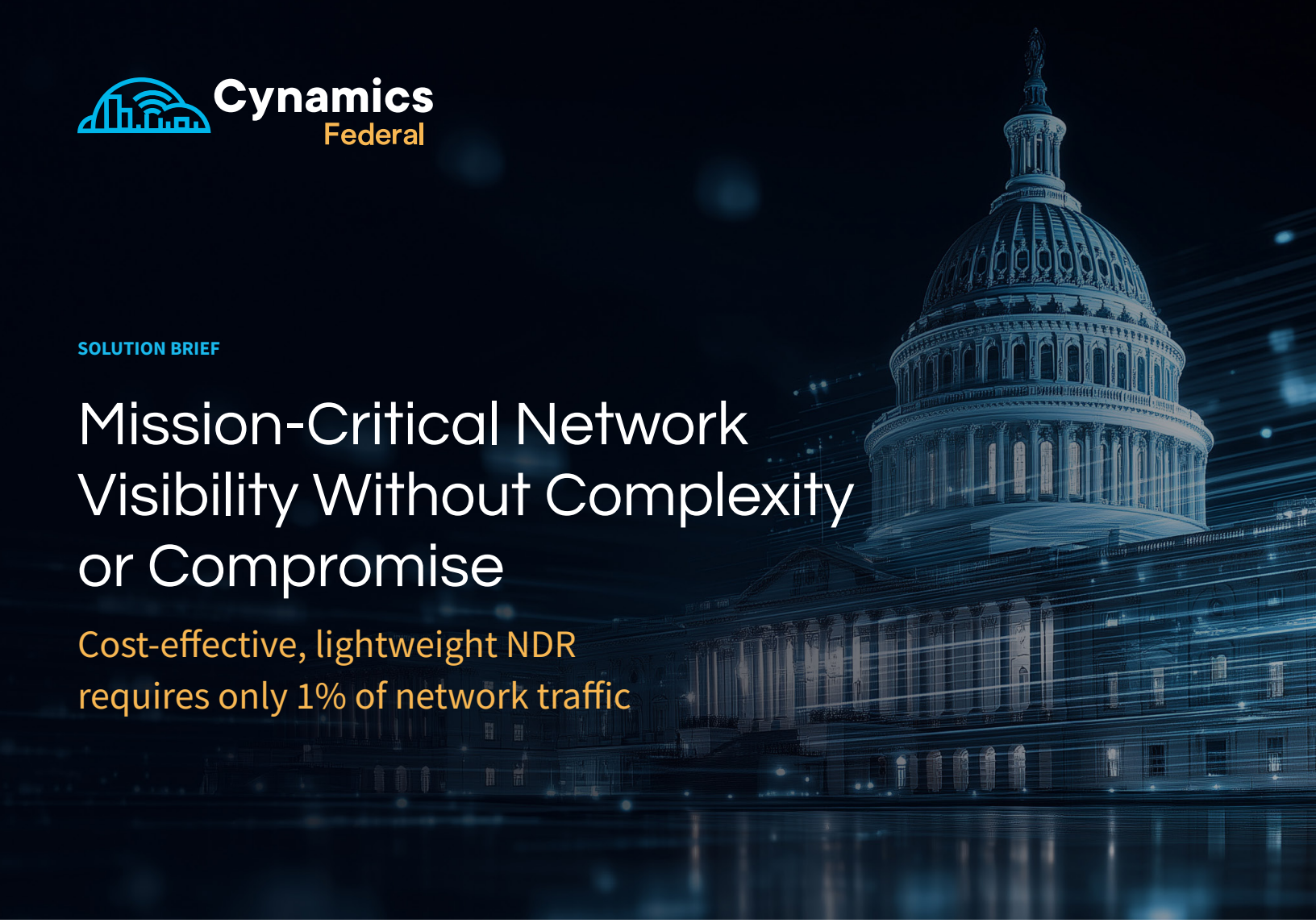
Cynamics Federal



SOLUTION BRIEF

Mission-Critical Network Visibility Without Complexity or Compromise

Cost-effective, lightweight NDR requires only 1% of network traffic

THE CHALLENGE

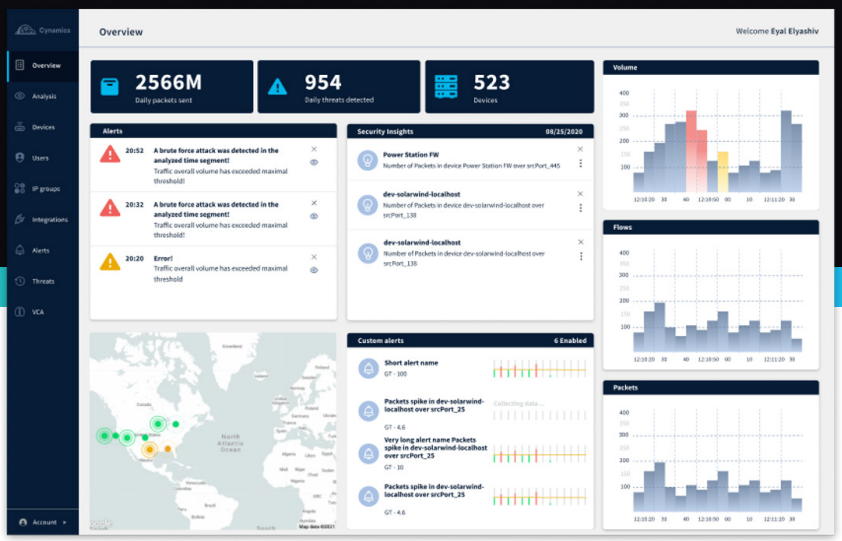
Network Blind Spots Agencies Can't Ignore

Network edge. OT and IoT. Distributed and shared sites.

Federal agencies are under increasing pressure to secure distributed on-premises, hybrid, and multi-cloud network environments while also contending with a myriad of challenges: blind spots, budgetary constraints, complex deployments, evolving compliance mandates, and limited staffing. Legacy NDR tools require intrusive hardware, miss east-west and encrypted traffic, and increase ongoing operational burden.

CISA's Advisory AA25-239A alerts that the federal network edge is increasingly vulnerable to advanced persistent threat (APT) actors, with prolific cyber-attacks like Salt Typhoon jeopardizing national security. Routers, VPN gateways, and IoT/OT devices are targeted entry points, yet these are exactly the spaces where traditional NDR tools lack visibility and control. Agencies must defend themselves against cyber adversaries increasingly exploiting network devices and GenAI misuse to enroot themselves in government networks and exfiltrate sensitive data.

© 2025 Cynamics Federal. All rights reserved.



THE SOLUTION

AI-Driven NDR. No Hardware. Scalable.

Cynamics Federal brings a fundamentally innovative approach to NDR with a patented AI-driven, FedRAMP-authorized platform to deliver macro-level visibility across every enclave, without the limitations of typical legacy NDR approaches using heavy hardware, full-packet capture, TAPs, sensors, or intrusive appliances.

Cynamics Federal inspects ~1% of traffic to assess the security posture of the entire network, reducing resource requirements, network impact, and bandwidth consumption. This enables significant cost savings, rapid deployment, and faster, more accurate threat detection and response. By sampling a fraction of the total network traffic for assessment, AI-driven analytics continuously build inferences on network vulnerabilities and potential attacker pathways. This cloud-native, lightweight platform deploys in minutes and scales seamlessly across distributed federal IT environments.

Reduce blind spots

Gain visibility across hybrid and multi-cloud environments, including mission-critical IoT, OT and remote enclaves. Continuously monitor encrypted, east-west, and cloud-based traffic.

Accelerate and future-proof compliance

Ensure compliance with mandates such as CISA Advisory AA25-239A, OMB M-21-31, and M-22-09.

Efficiency for lean Security Operations Center (SOC) teams

The Virtual Cyber Analyst (VCA) and CynLLM reduce SOC alert fatigue with automated detection, actionable reporting, AI-enabled triage, and eliminating false positives.

Maintain resilience under encryption

Detect anomalies even in TLS 1.3, VPN tunnels, and encrypted east-west traffic. Thwart low-and-slow activity, lateral movement, and zero-day attacks before they escalate.

© 2025 Cynamics Federal. All rights reserved.

USE CASES

Common Challenges Agencies Encounter.

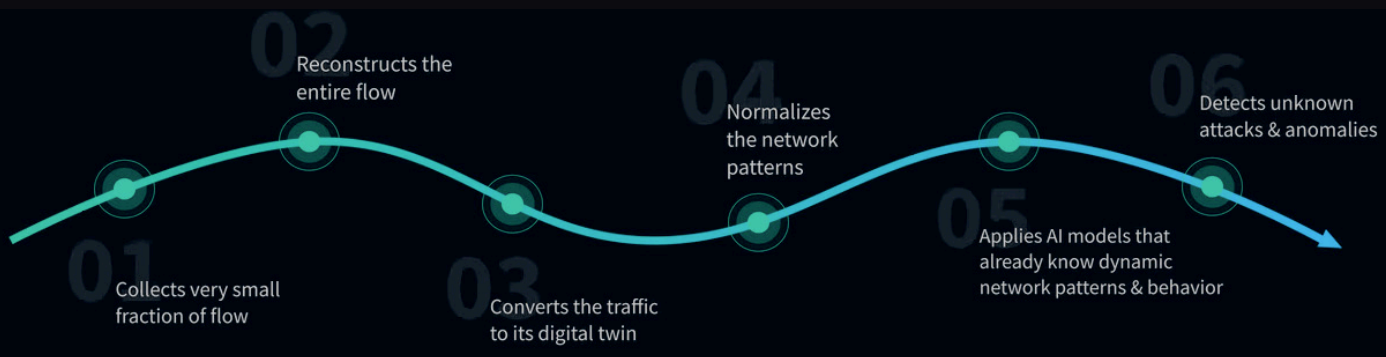
Cynamics Federal's AI-based sampling approach to NDR covers environments that are ideal for flow-based network detection — the network edge, OT environments, and distributed offices. Think of Cynamics Federal as a trip wire for those spaces where it is too expensive, cumbersome, or technically challenging to deploy a full packet capture solution. It addresses operational inefficiencies and security gaps, providing:

- **Network edge protection**
  Protection from attacks on edge environments where it is difficult to to deploy packet capture, either for cost or infrastructure reasons such as a fixed static environment, ship borne networks, small office spaces, and rapidly deployed IR-based detection for responsive blue teaming.
- **Encrypted and east-west traffic visibility**
  Detection of threats in encrypted traffic without decrypting data.
- **OT and ICS protection**
  These devices tend to operate in environments that are short on bandwidth and rarely touched, so anomalous communications can be rapidly discovered.
- **GenAI misuse**
  Flagging sensitive data uploads to LLM platforms and automating data loss prevention (DLP) rules to stop hidden exfiltration without looking into the payload.
- **Distributed or shared offices and labs**
  Agencies with shared spaces at universities and locations where they do not own much of the network, there typically is a lack of available network or cybersecurity personnel.

These outcomes ensure an improved cybersecurity posture that is more aligned with the operational challenges facing federal agencies. Instead of deploying more hardware or hiring more staff, Cynamics Federal provides an immediate, scalable, and future-proof path to improved network security outcomes.

HOW IT WORKS

AI-Enabled. Autonomous.



Traditional NDR solutions rely on heavy infrastructure: packet capture, mirrored feeds, and large-scale appliances. These may work in centralized data centers, but they fail to scale across the highly distributed and bandwidth-constrained environments that define federal networks today. Cynamics Federal was purpose-built to overcome these limitations and ensure mission continuity and success.

© 2025 Cynamics Federal. All rights reserved.

WHY CYNAMICS FEDERAL

Cost Effective. Easy Deployment.

Rapid deployment

FedRAMP authorized on the CGC platform and integrates with AWS, Google Cloud, Zscaler, and Netskope. Operational in minutes, not months, ensuring faster mission-readiness for agencies with limited resources.

Patented AI sampling

VCA and CynLLM deliver AI-driven baselines and continuous anomaly correlation using 1% of network traffic. This means real-time, complete visibility and control, even across encrypted or east-west flows.

Lightweight virtual collection

An easily deployed virtual collector collects NetFlow, IPFIX, and routing metadata for robust network sampling and analysis.

Future-proof detection

Capable of identifying stealthy nation-state tactics, insider misuse, and zero-day behaviors, even as encryption becomes universalized.

Cynamics Federal delivers a fundamental shift toward lightweight, AI-driven, and cost-effective network defense tailored for the evolving requirements of federal missions and IT infrastructures.

GET STARTED

Free Proof of Value

3 Weeks. No Cost. Immediate Value.

cynamicsfederal.com

Cynamics
Federal

© 2025 Cynamics Federal. All rights reserved.