UNIFIED OBSERVABILITY:

The key to defense readiness and AI confidence

How unified, real-time visibility elevates AI confidence, operational readiness and mission assurance.

By Scoop News Group

Sponsored by DATADOG

Defense organizations are racing to adapt to a new era of strategic and operational challenges. The rapid evolution of artificial intelligence and autonomous systems, and the convergence of digital and kinetic forces, have fundamentally reshaped the military's technical landscape.

At the same time, military leaders are under immense pressure to modernize their underlying IT systems and fragmented workflows, many of which were designed long before today's warfighters were born.

While the advent of cloud computing, containerized workloads, and AI has helped narrow many of the military's technical gaps, it has also contributed to massive "tool sprawl," making monitoring systems and securing data exponentially more complex.

Technology experts say that without a wholesale shift to unified real-time data visibility across their security and operations systems, defense agencies will continue to face significant challenges and blind spots in identifying IT stacks, pinpointing system bottlenecks, and remediating security vulnerabilities.

The military case for 'unified observability'

Among those making that argument is **Chris Goings**, strategic account executive for the Department of Defense at Datadog. Unified observability gives organizations real-time visibility across infrastructure, applications, networks, data, and AI workloads, helping teams identify risks, investigate incidents, and restore mission-critical services faster, Goings explained. As defense organizations adopt AI and manage increasingly complex hybrid environments, end-to-end visibility is essential to operational resilience and secure innovation.

> "As system complexity explodes, customers realize traditional monitoring is no longer sustainable."
>
> **Chris Goings**,
> DOD strategic account executive, Datadog

"As system complexity explodes, customers realize traditional monitoring is no longer sustainable. We need to be able to unify this data," said Goings.

"Observability represents a fundamental evolution beyond traditional monitoring," said **Joe Gavin**, director of federal business at Datadog. "Where monitoring gave IT teams siloed views into the reliability and performance of their stack, observability unifies metrics, traces, and logs across every layer of the environment — enabling faster root cause

analysis and significantly reducing mean time to resolution."

Less appreciated, but perhaps even more troublesome, is the ephemeral nature of today's microservice architectures, especially in a cloud environment, explained **Rick Stewart**, a senior engineer at Datadog. Workloads now execute and vanish within seconds to optimize resource costs. Traditional tools have no path to trace how an application performed or what security events occurred during that brief window.

> "Workloads now execute and vanish within seconds to optimize resource costs. We can determine what happened at a specific time, what various workloads actually did… and why."

Rick Stewart,
Senior engineer,
Datadog

"The challenge we can undertake and resolve is the ability to track all that information," said Stewart. "Whether we're tracking individual performance metrics or reviewing logs for a workload that's no longer there, with Datadog, we can determine what happened at a specific time, what various workloads actually did during that ephemeral window, and why."

However, the most compelling reasons to shift to a unified visibility platform, all three executives say, stem from a confluence of factors reshaping the military landscape:

THE NEW DEMANDS OF COMMAND AND CONTROL

The convergence of digital and kinetic forces and the increasingly dynamic nature of physical and cyber warfare depend on trusted, real-time data and resilient digital systems. This requires replacing siloed workflows with intelligent, automated observability and remediation to identify infrastructure flaws, fix application bottlenecks, and thereby strengthen mission assurance.

CYBER OPERATIONS IN A COMPLEX THREAT ENVIRONMENT

As attackers leverage automation and AI, defenders need faster, more unified visibility across their operational and security data pipelines to accelerate threat detection and response.

HUMAN-MACHINE TEAMING

The growing reliance on autonomous systems creates a critical need for real-time visibility into system health, communications, and security. Unified observability provides a zero-trust lens on agentic activity. It also helps teams monitor model behavior, detect

anomalous outputs, track data access patterns, and increase confidence in AI-enabled systems.

EVOLVING DEFENSE CYBERSECURITY REQUIREMENTS

DoD Zero Trust and continuous-monitoring priorities are increasing the need for consistent telemetry, centralized visibility, and faster threat detection and response across cloud, on-premises, and operational environments.

Moving beyond 'swivel-chair' management

While the logic behind unified observability is straightforward, the path forward with traditional monitoring tools is not. Even the best stand-alone data-monitoring tools that rely on deep table scans — and many embedded solutions — aren't designed to handle the dynamic telemetry from today's rapidly evolving AI-enabled applications and software-defined infrastructure.

Next-generation observability platforms operate differently by continuously analyzing metadata, logs, and telemetry across an agency's entire data ecosystem to provide true system-wide visibility. Datadog's observability platform, for example, can process trillions of data points per hour, gathered from over 1,000 native technology integrations across legacy, hybrid and multi-cloud platforms, according to Stewart.

By unifying metrics, traces, and logs into a single data layer, defense agencies can establish a centralized view of performance across systems and operational silos. This dramatically reduces the reliance on "swivel chair management" — and the time wasted jumping between vendor dashboards to analyze a security event.

"Not only do we have a single agent that collects all of this different telemetry for the various pieces of your technology stack," explained Goings, "but we put all of that telemetry into easy-to-consume, easy-to-view, easy-to-drill-down-and-share dashboards and visualizations inside the platform."

> "Observability unifies metrics, traces and logs across every layer of the environment — significantly reducing mean time to resolution."
>
> **Joe Gavin,**
> Director of federal business,
> Datadog

That gives defense agencies an added advantage by enabling security and operations teams to work from the same "kernel of truth" during a crisis, transforming incident response into a more unified mission.

"The problem in the past has been that the technology has not really existed to be able to send those logs to two different places — one set for operations and one for security. Now we're doing that in a way with things like filters and more flexibility around storage and indexing," said Goings. That's also more cost-efficient than what many vendors offer, since they typically charge for separate platforms."

5 Critical mechanisms for defense readiness

Adopting a modern, comprehensive observability and security solution — delivered as continuously updated Software-as-a-Service — is about more than gaining faster, real-time system awareness. It's also about how that capability drives immediate improvements in defense readiness and AI adoption through five critical mechanisms:

1 REDUCING CLOUD & HYBRID MODERNIZATION COMPLEXITY

Delivering observability as a managed service accelerates modernization by removing the operational overhead of installing, patching, and maintaining on-premises monitoring infrastructure. It also supports the ability to track ephemeral workloads, allowing teams to determine what happened at a specific time, even if the cloud resource is no longer running.

2 OPERATIONAL EFFICIENCY THROUGH CONSOLIDATION

By unifying disparate telemetry, agencies can consolidate operations, security, and FinOps (financial operations) onto shared platforms. This enables previously siloed teams to collaborate more effectively while allowing IT and financial leaders to measure actual cloud spend against infrastructure performance, helping optimize multi-million-dollar budgets.

3 CYBER THREAT INVESTIGATION & ZERO TRUST

Unified observability provides a continuous monitoring framework essential for Zero Trust architectures. It correlates infrastructure and security telemetry in a single interface, dramatically accelerating root cause analysis. When a misconfiguration occurs, the platform can calculate the blast radius and provide immediate, automated remediation recommendations.

4 MISSION-CRITICAL RELIABILITY

Observability platforms now provide end-to-end tracing, extending from backend data

stores to the end-user's web interface at the edge. This complete visibility ensures that military web applications deliver a commercial-grade user experience while enabling developers to simulate end-user behavior and improve mission assurance.

5 AI AND DATA PLATFORM OPERATIONS

As agencies deploy autonomous systems, Datadog's Agent Observability capability tracks token costs, monitors model behavior, and safeguards against hallucinations and unauthorized data access. This zero-trust lens for AI ensures that agents do not expose sensitive information, building greater confidence for human-machine teaming.

Collectively, unified observability leads to improved operational outcomes, faster, more informed decision-making, reduced risk, stronger security, increased trust in AI-enabled systems, and improved workforce efficiency.

"One of our mantras is, 'AI for observability and observability for AI,'" added Datadog's Rick Stewart. "In addition to safeguarding against unauthorized AI activity, AI-enabled observability helps non-technical operators quickly pinpoint the underlying causes of anomalies, reducing downtime."

Datadog's AI-powered capabilities also make it possible to query the platform and provide results and recommendations without having to know specific syntax or manually select facets, Stewart said. "If a signal occurs due to a misconfiguration in your IT stack, Datadog can surface it not only to your security team but also to anyone viewing a particular dashboard. They can immediately drill into that specific issue, and Datadog will tell them in layman's terms: 'This is what's happening, this is the resource affected, this is the blast radius of how it's affecting your environment, and here are a couple of recommendations that will allow you to address those issues in a controlled manner.'"

Enhanced capabilities; reduced risk

The ability of unified observability to streamline modernization and meet increasing data demands securely is one of the many reasons Datadog has gained a growing presence among federal agencies, including:

- **The U.S. Department of Agriculture** – At the U.S. Forest Service, Datadog unified visibility across a complex hybrid environment supporting more than 150 mission applications, replacing fragmented monitoring tools and helping reduce mean time to resolution by 60%.
- **The Department of Energy** – Lawrence Berkeley National Laboratory used

Datadog and the cloud to make the lab's materials research more accessible to an ever-growing number of users.

- **The National Institutes of Health** – The National Cancer Institute (NCI) used Datadog to modernize fragmented cloud monitoring tools, reduce costs, and improve operational visibility across hundreds of cloud accounts.

Importantly for government agencies: Datadog for Government recently achieved FedRAMP High certification, making it suitable for supporting the federal government's most sensitive civilian workloads. Datadog is also actively working with Department of Defense sponsors to achieve Impact Level 5 (IL5) authorization, enabling support for Controlled Unclassified Information (CUI) and unclassified National Security Systems (NSS) workloads.

The conflicts of today and the future will not be fought only in physical domains but also across the unseen architectures of cloud networks, AI models, and data pipelines. Operational readiness now dictates that data visibility, system security, and autonomous operations cannot exist in silos.

For defense leaders, the mandate is clear: Clinging to fragmented, legacy monitoring tools is an active operational risk. By embracing unified observability as a foundational data layer, agencies can illuminate the dark corners of their IT environments, secure AI-enabled systems, and transform complex telemetry into a decisive operational advantage.

For more on choosing the best-suited observability platform partner, see page 8

Learn more about why Datadog for Government is the leading observability and security platform for the AI era.

This report was produced by
Scoop News Group and sponsored by Datadog.

DATADOG SCOOP NEWS GROUP

Choosing the best-suited observability partner

When evaluating observability platforms for today's complex enterprise operations, the 2026 Gartner Magic Quadrant for Observability Platforms defines a set of capabilities every platform in the market must deliver. Five stand out for enterprise buyers:

1. Unified telemetry – Ingesting, storing and analyzing metrics, events, logs and traces together, with native support for OpenTelemetry.

2. Root cause and user impact – Detecting changes in application, service and infrastructure behavior to determine what caused an outage or slowdown — and how much it affected end users.

3. Context and dependency mapping – Enriching telemetry with service maps and topology, and automatically discovering how infrastructure, network and application components connect.

4. Business Transaction Visibility – Modeling the relationship between monitored services and the business transactions they support.

5. Multicloud coverage – Collecting telemetry across major public cloud providers, with interactive exploration spanning traces, metrics and logs.

Gartner recognized Datadog for the sixth consecutive year as a category leader in observability platforms, noting that, with over 30 integrated products, Datadog can replace multiple point solutions with a single platform. Gartner also highlighted several key platform capabilities, including:

- **Bits investigation –** autonomously investigates alerts, surfaces the root cause, and recommends and takes action across systems, accelerating incident response and reducing outages.
- **Agent observability –** provides visibility into the performance, quality, security, and cost of AI agents and LLM apps, enabling safe and scalable adoption of AI-native workloads.
- **End-to-end APM –** reduces mean time to resolution by connecting mobile and browser apps with backend services, providing deep visibility into every user action, line of code, and database query.
- **Digital experience monitoring –** gives organizations complete visibility into how customers experience their mobile and web digital products and uniquely ties those experiences to backend systems and business outcomes.

Datadog was positioned highest in "ability to execute" among all observability platforms Gartner evaluated.