In Hybrid Cloud We Trust

How Datadog empowers US government with enhanced interoperability and security across on-premises and cloud environments

---

Thank you for downloading this Datadog resource. Carahsoft is the distributor for Datadog cyber solutions available via NASPO, Texas DIR-TSO-4288, MHEC, and other contract vehicles.

To learn how to take the next step toward acquiring Datadog's solutions, please check out the following resources and information:

For additional resources:
carah.io/DatadogResources

For upcoming events:
carah.io/DatadogEvents

For additional Datadog solutions:
carah.io/DatadogSolutions

For additional cyber solutions:
carah.io/cyber

To set up a meeting:
Datadog@carahsoft.com
(703) 921-4160

To purchase, check out the contract vehicles available for procurement:
carah.io/DatadogContracts

In Hybrid Cloud We Trust

How Datadog empowers US government with enhanced interoperability and security across on-premises and cloud environments

DATADOG

Introduction

Five years after the Office of Management and Budget's (OMB) announcement to update the Federal Cloud Computing Strategy from "Cloud First" to "Cloud Smart," US federal agencies have reached a new threshold in cloud adoption. According to a 2022 survey by FedScoop[1], two-thirds of federal IT leaders said that their agency was using or starting to use the cloud.

The survey looked at where agencies were in the adoption of cloud services—and how security concerns factored into their cloud decisions. It delved into the many factors IT leaders must consider when deciding whether to host their data and applications on-premises or in the cloud.

More than half of surveyed cloud adopters named "security assurance" as the main challenge that is preventing them from expanding their usage of cloud services. The difficulty of managing services across hybrid or multi-cloud environments was another key barrier.

To enhance security, 55 percent of respondents said their agency was prioritizing "improving network-wide observability of applications."

Many agencies, in their efforts to enhance security through observability, have inadvertently created tool sprawl. This results in a collection of disparate tools, leaving them without a consolidated view of their data. DevOps teams currently rely on an average of 12+ monitoring tools to gather and analyze trillions of data points in hybrid-cloud and cloud-native environments[2]. The proliferation of disconnected or outdated observability tools results in data silos, limited system visibility, and constant context switching for teams.

60%
of cloud adopters
named "security assurance" as the top challenge keeping them from taking greater advantage of cloud services[1]

To address the challenges of tool sprawl and fragmented observability, many organizations are pivoting toward a holistic solution: end-to-end unified observability and security. This comprehensive approach provides a cohesive, centralized view across the entire IT infrastructure. End-to-end observability and security is increasingly becoming an indispensable component of modern IT strategies, as it not only addresses the limitations of isolated monitoring tools but also offers a more efficient way to detect, diagnose, and resolve issues across complex environments.

This eBook provides an overview of the reasons why hybrid is the predominant architectural approach for an increasing number of US government agencies and service providers, the risks it introduces, and the role of observability in achieving end-to-end visibility across on-premises and cloud computing resources.

1. FedScoop, "Federal Perceptions of Cloud Security." 2022. Accessed March 2024.
2. Datadog, "Tool Consolidation." Accessed March 2024.

Table of Contents

Hybrid's driving forces

Understanding the reasons for hybrid cloud adoption in government

Hybrid's driving forces

The staying power of on-prem

While FedScoop's findings indicate a growing acceptance of cloud services, on-premises IT will continue to be vitally important until teams can satisfy the following requirements in their cloud environments:

– Achieve desired levels of control over system components—such as virtual machines, operating systems, containers, applications, logs, and security controls—which is perceived as easier on-premises due to direct access to hardware, software, and networks.

– Refactor and migrate legacy applications that have been running for decades on custom-built systems, and cannot be replicated in the cloud without substantial reengineering, full-time employee (FTE) resources, and downtime.

This means certain data sets and applications will continue to run in on-premises data centers for the foreseeable future. And as technology evolves, finding the right balance between on-premises and cloud services becomes essential for long-term organizational success.

The Hybrid advantages

Here are some of the key advantages and opportunities hybrid cloud environments offer to IT leaders.

Greater flexibility and scalability
Seamlessly scale computing resources based on demand and in near real time

More control over costs
Manage costs through economies of scale, pay-as-you-go pricing, and dynamic scaling

Keeping pace with innovation
Build on and leverage CSP-enabled advancements in analytics and machine learning, without creating those capabilities in house from scratch

Increased operational resilience against disasters and outages
Replicate critical data and applications between on-premises and the cloud (or additional environments for more data redundancy)

Fewer compliance burdens
Leverage the security controls owned by Cloud Service Providers (e.g., securing hardware, software, networking, and physical facilities), so hybrid cloud managers can worry less about compliance and focus on optimizing IT performance and security

Fig 1: Advantage of hybrid cloud environments

Managing new risks

Mitigating challenges through unified observability

Managing new risks

The importance of pairing hybrid cloud adoption with unified observability and security

In the ever-evolving landscape of hybrid cloud integration, IT leaders (including CIOs), Infrastructure Administrators, and Cloud Architects are confronted with significant monitoring and observability and security challenges. A cohesive and integrated observability strategy has become essential to achieving a consolidated view across diverse infrastructures. A unified approach addresses the inherent risks of using fragmented monitoring tools, such as a combination of in-house and CSP-native monitoring tools.

Effectively addressing these challenges is essential because improperly managed hybrid cloud environments can result in blind spots and operational inefficiencies. A disjointed approach to monitoring disrupts the flow of critical insights and introduces a variety of risks.

Data silos
When data is scattered across various tools, teams are unable to efficiently analyze data, derive meaningful insights, or identify cross-system issues

Security gaps
Switching between different interfaces and workflows requires specialized skill sets, increases risk of misconfigurations, and potentially limits automation and incident response capabilities

Resource waste
More tools result in higher costs— without improving operational efficiency

Increased complexity
The use of different interfaces, data formats, and operational processes can limit scalability and make it harder to maintain a streamlined and efficient monitoring approach

Fragmented visibility
Teams that use multiple point solutions are likely to experience gaps in monitoring and have difficulty correlating data across different sources

Operational inefficiencies
Switching between different interfaces and workflows potentially limits automation capabilities and delays incident detection, response, and resolution

Compliance challenges
A mix of disjointed tools may create obstacles in adhering to regulatory and compliance requirements, such as alignment with FedRAMP® security standards

Fig 2: Risks of using disparate monitoring tools
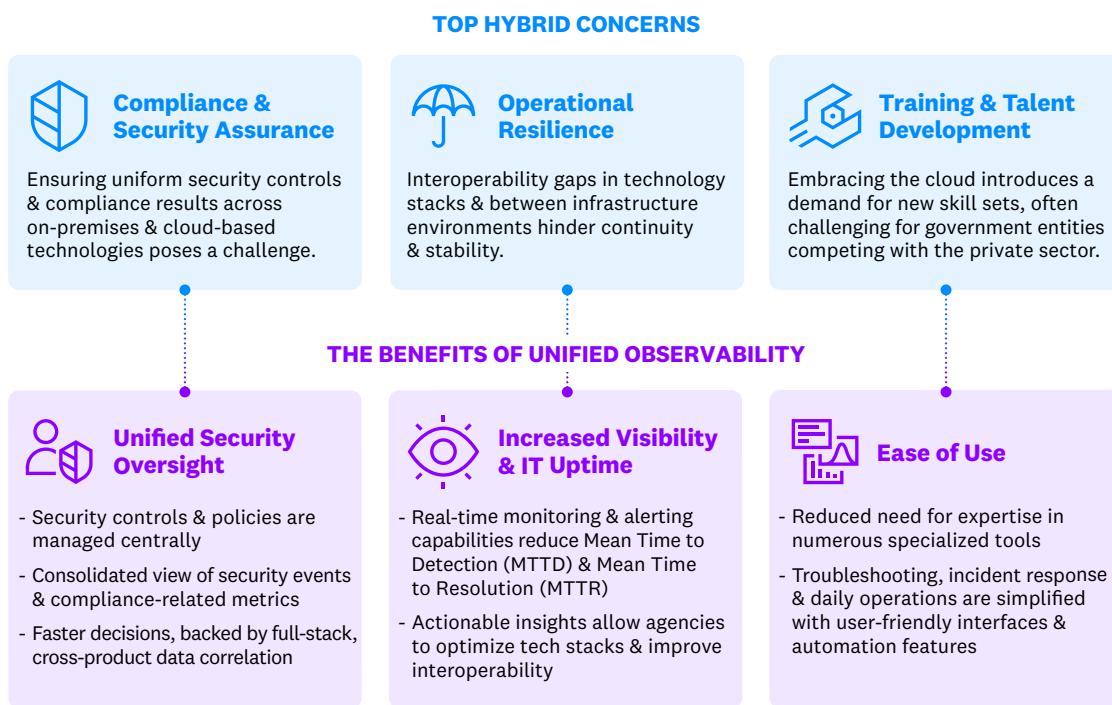
03

The role of observability

Enhancing insight and control in
hybrid cloud environments

The role of observability

Managing (and even detecting) these risks requires organizations to establish a single source of truth by embracing an end-to-end unified observability and security solution that provides a holistic view of components in their hybrid cloud environments. Datadog is a pivotal enabler for IT leaders in the US government because it offers a robust suite of tools to optimize success and to simplify the complex landscape of hybrid cloud environments. With Datadog's unified observability and security platform, IT leaders gain a unified view into both on-premises and cloud infrastructures, enabling faster and more informed decision-making.

The following infographic explains how you can unlock the potential of unified observability with Datadog to conquer hybrid cloud monitoring challenges.

Navigate the challenges of hybrid cloud for US government

TOP HYBRID CONCERNS

Compliance & Security Assurance

Ensuring uniform security controls & compliance results across on-premises & cloud-based technologies poses a challenge.

Operational Resilience

Interoperability gaps in technology stacks & between infrastructure environments hinder continuity & stability.

Training & Talent Development

Embracing the cloud introduces a demand for new skill sets, often challenging for government entities competing with the private sector.

THE BENEFITS OF UNIFIED OBSERVABILITY

Unified Security Oversight

- Security controls & policies are managed centrally
- Consolidated view of security events & compliance-related metrics
- Faster decisions, backed by full-stack, cross-product data correlation

Increased Visibility & IT Uptime

- Real-time monitoring & alerting capabilities reduce Mean Time to Detection (MTTD) & Mean Time to Resolution (MTTR)
- Actionable insights allow agencies to optimize tech stacks & improve interoperability

Ease of Use

- Reduced need for expertise in numerous specialized tools
- Troubleshooting, incident response & daily operations are simplified with user-friendly interfaces & automation features

6 key features of Datadog for Government

01 **FedRAMP® Authorization** for built-in security compliance & adherence to regulatory requirements

02 **Unified observability & security platform** with full-stack, automatic correlation and more than 700 built-in integrations

03 **Integrated, cloud-native security approach** for cloud & on-premises monitoring

04 **Superior breadth & depth of coverage** for maximum visibility & cost control

05 **Reliable, performant & available at virtually any scale** to optimize uptime and prevent outages

06 **Comprehensive adoption & support** with a network of cloud providers, MSPs, & system integrators

04

Customer story

Demonstrating operational excellence in hybrid cloud

Customer story

Digital Infrastructure Services Center of a Major US Federal Agency

Industry	**Employees**	**Location**	**Partner**
US PUBLIC SECTOR	100,000	WASHINGTON, DC	ECCO SELECT

Taming the complexities of hybrid cloud

The digital infrastructure services center of a major federal agency is responsible for managing and providing essential IT services for more than a dozen US federal government departments and bureaus. The organization has operated as a federated data center since 1973, meaning it employs a network of distributed data centers that work together seamlessly.

Over the years, the organization has embarked on a modernization journey that aims to enhance its own capabilities and improve the operational efficiency of its customers across the federal community. As a result of its recent modernization initiative, it has adopted a hybrid cloud infrastructure that utilizes both on-prem and cloud-based resources, integrating new capabilities with existing legacy technologies. This has led to significant benefits like on-demand scalability, improved resource utilization, and streamlined software development and deployment processes. However, this transformation also introduced complexities and challenges. Overcoming these hurdles would require more sophisticated monitoring capabilities than what the existing tools could provide. Moreover, the customer needed to consider the 2021 Executive Order (EO), which focused on improving the nation's cybersecurity and rendered many legacy monitoring tools noncompliant with federal security regulations.

"When the cybersecurity EO was issued in 2021, it caused us to stop and reevaluate the security and integrity of our entire software supply chain," says the Senior Vice President (SVP) of Technology Services for ECCO Select, the trusted Managed Service Provider (MSP) supporting the contract. "Suddenly, our 'good enough' monitoring solution was no longer compliant and we were forced into a state of change. We took the opportunity to think about our ideal state and began evaluating best-in-class observability platforms."

Enhancing operations with Datadog's federally authorized observability solution

To meet the customer's requirements, ECCO Select evaluated FedRAMP® authorized monitoring and observability solutions and selected Datadog to monitor and manage all aspects of its IT environment, from its foundational infrastructure to the delivery of end-user experiences.

With Datadog in place, ECCO Select can offer essential managed services that provide real-time or near-real-time visibility into the health, performance, and configuration of the customer's IT services and assets. These systems are not only observable at a macro level, but individual tenants can use the platform's self-service features to securely access and monitor their specific infrastructure resources and applications. DevOps teams across the service center's portfolio of customers now have unified visibility into the health of their IT systems and can observe the performance of systems, servers, applications, and other resources within the enterprise technology stack.

> *"Datadog transformed our approach to infrastructure monitoring. We now have a comprehensive solution that not only speeds up root cause analysis when there's an issue, but continuously provides the visibility we need to keep our systems secure and resilient."*
>
> **– Senior Vice President of Technology Services, ECCO Select**

Attaining rapid and tangible results

700→0
reduction in service desk tickets opened for a persistent memory issue

4,000
containers configured for end-to-end monitoring

95%
of hosts monitored within 75 days of the project start date

Within 75 days of the project start date, the team completed an automated deployment of the Datadog Agent to 4,800 hosts running in both on-prem data centers and cloud environments. This gave them full monitoring coverage of over 95 percent of their infrastructure, including thousands of containers as well as network and storage devices and databases. They were also able to seamlessly transition more than 1,100 observability templates—covering infrastructure services, logs, and synthetic tests—from their legacy monitoring system. The team validated this process through a carefully phased approach to ensure accuracy and reliability.

The customer realized the value of Datadog almost immediately when it helped them detect and resolve a recurring memory issue that had been plaguing them for months. The Enterprise Service Desk team had received more than 700 service desk tickets, which each required manual investigation.

Whereas the legacy monitoring tool's limitations left them in the dark by only offering "high" or "low" thresholds for memory utilization, Datadog immediately revealed a problematic process caught in a loop due to a (at the time) seemingly harmless change in a disaster recovery location. The change disrupted replication efforts, causing a widespread memory issue that affected the entire system.

Armed with this information, the team quickly identified the problem and used insights from Datadog to correlate standard high/low memory alerts with process log information to implement a straightforward fix. The problematic process, which had previously been undetectable with legacy monitoring tools, has since been successfully identified and permanently resolved. This has enhanced the customer's hybrid monitoring capabilities by ensuring the performance, resource utilization, and reliability of all applications across both on-prem and cloud environments.

"*Reflecting on our journey, we started with limited visibility— unable to see beyond top-level alerts, facing spotty access, and lacking meaningful log data. Datadog didn't just resolve a memory issue. It transformed our entire approach to infrastructure monitoring.*"

- Senior Vice President of Technology Services, ECCO Select

Today, the customer is fully equipped to address the challenges associated with hybrid cloud environments and provide exceptional service to its customers in the federal space. Currently, it supports 700 agreements that span across the federal government. With Datadog, it can continue to scale its operations in line with its vision to be the preferred business partner for the federal government, providing reliable, secure, and scalable enterprise IT services.

Use cases

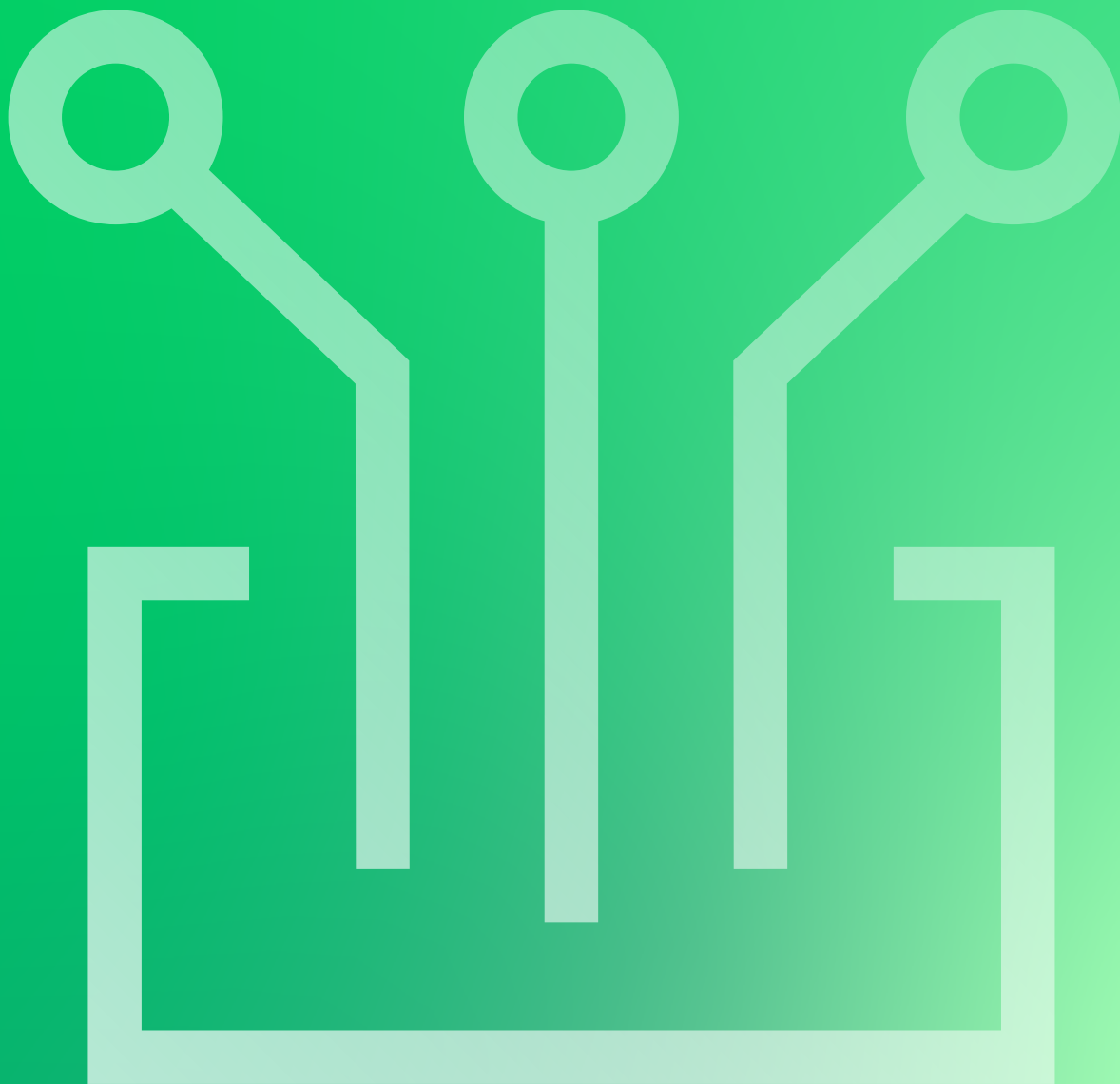|	
Infrastructure Monitoring	**Hybrid Cloud Monitoring**
Application Performance Monitoring	**Digital Transformation/Operations**
Log Management	**Digital Experience Monitoring**
Monitoring Tools Consolidation	**On-premises Monitoring**

05

Conclusion

How agencies can unlock the full
potential of cloud technologies

Conclusion

In an increasingly digital world, US government entities are faced with the challenge of securely managing vast amounts of data while also employing modern technologies.

Hybrid cloud architectures have become the standard for most government IT systems, necessitating improved network-wide observability.

Adopting a unified observability solution is transformative, offering agencies a comprehensive understanding of system behavior. This enables teams to respond more quickly to incidents, optimize performance, and strengthen IT ecosystem resilience. This approach also streamlines operations by eliminating the need for incompatible tools, enhancing overall efficiency.

Datadog's advanced observability and security platform serves as a linchpin, bringing together diverse telemetry from a range of technologies, so teams can access a single source of truth. This cultivates a collaborative culture and ensures better resource efficiency, resulting in service level improvements, optimal customer experience, more cost savings, and faster time to market.

By following best practices for monitoring hybrid systems, government agencies can unlock the full potential of cloud technologies while ensuring the integrity and security of their data.

As the cloud migration and IT observability partner to agencies like the US Department of Veterans Affairs, the US Department of Agriculture, the Federal Aviation Administration, and the US Census Bureau, Datadog has a nuanced understanding of the complexities associated with modern IT infrastructures. Our team brings specialized talent and domain expertise tailored specifically for the unique demands of the US public sector.

About Datadog

Government hybrid cloud monitoring products and capabilities

Datadog offers the following products and capabilities designed to help government agencies maximize their success in hybrid cloud environments:

- – Application Performance Monitoring
- – Cloud Security Management
- – Container Monitoring
- – Continuous Profiling
- – Database Monitoring
- – Infrastructure Monitoring

- – Log Management
- – Network Device Monitoring
- – Network Performance Monitoring
- – Real User Monitoring - Browser & Mobile Apps
- – Synthetic Monitoring
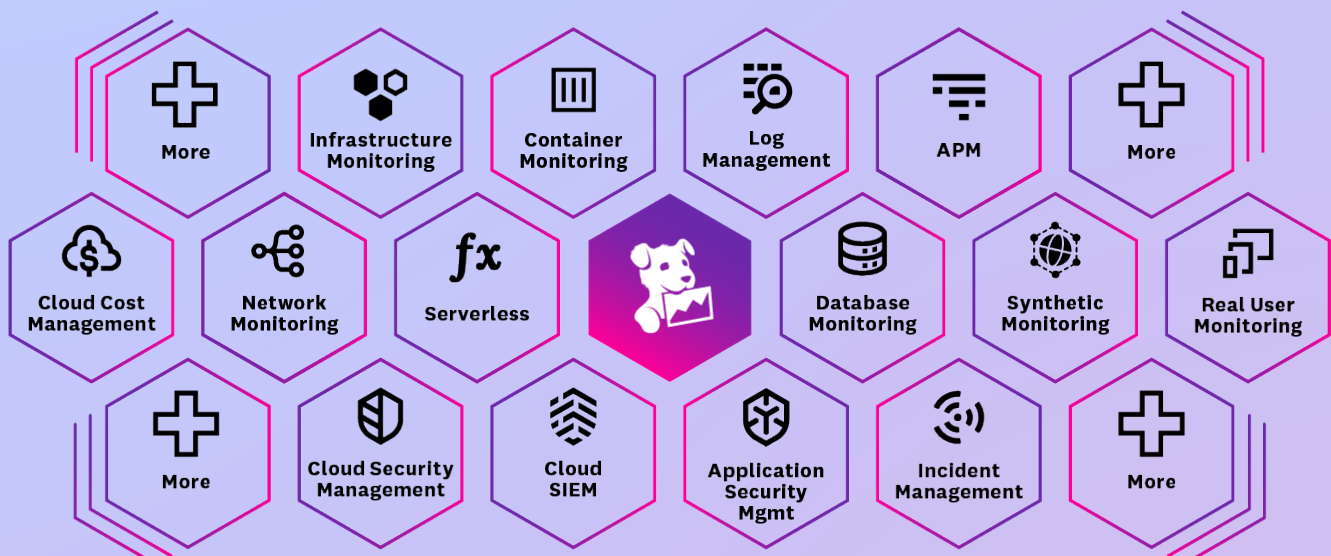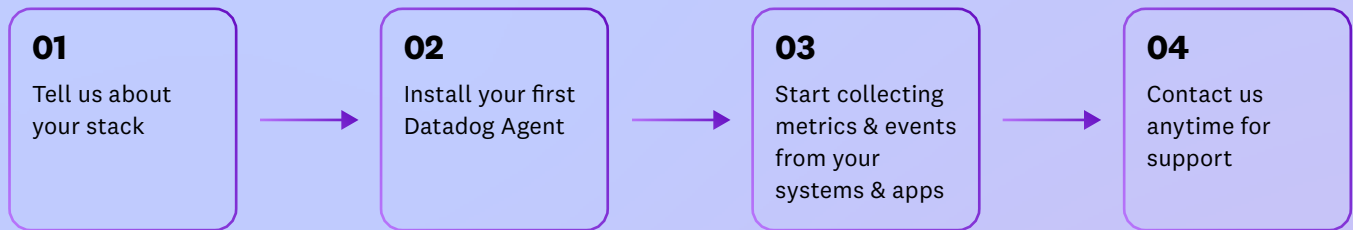
Get started with Datadog

Visit ddog-gov.com/signup & select "get started free" or "free trial"

Choose the region called "United States (US1-FED) – FedRAMP Moderate Authorized" & complete the quick form

Logging in

01	02	03	04
Tell us about your stack	Install your first Datadog Agent	Start collecting metrics & events from your systems & apps	Contact us anytime for support

Let's connect

Datadog has helped thousands of customers achieve observability across their technology stacks by unifying data from on-premises, hybrid, and cloud-based systems into a single source of truth. Contact us to learn more about how we can help advance your mission.

Contact our Public Sector Sales team (team-enterprisepublicsector@datadoghq.com)

Learn more about Datadog for Government