
# Modern Log Management with Datadog

How US government agencies can meet requirements of Executive Order (EO) 14028 and M-21-31

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

# Modern Log Management with Datadog

How US government agencies can meet requirements of Executive Order (EO) 14028 and M-21-31

## Role of log management in improving cybersecurity

US agency IT teams prioritize information security above any other objective. When cyber incidents occur, they rely on logs to investigate what happened and develop protective measures to prevent future issues. With the increasing role of digital information and technology in society, log management has become an operational necessity enabling agencies to investigate vulnerabilities and improve their overall security posture.

## Upholding federal log requirements

This is why the Office of Management and Budget (OMB) issued M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* in accordance with Executive Order 14028 on Improving the Nation's Cybersecurity.

The memorandum established federal agency requirements to increase the government's visibility into cybersecurity incidents and defines logs that agencies must capture as well as the required retention times. It also establishes a maturity model to track agency implementation.[1]

Today, most US agencies operate a complex environment of legacy applications and systems coexisting with modern tools. The amount of data being generated every day is beyond the capabilities of most legacy monitoring systems. Establishing a common, scalable data platform creates visibility of an entire technology system, whether its components are legacy, modern, cloud-based, on-premises, or hybrid, so event logs can be reviewed and synthesized effectively.

## Datadog: The essential log management solution for government agencies

Datadog provides a comprehensive monitoring and security platform that helps agencies and their IT service providers meet the policy requirements outlined in M-21-31, plus:

- ✓ Our FedRAMP® Moderate authorization reduces friction from the Authority to Operate (ATO) process, simplifying procurement and adoption
- ✓ Our team has a deep understanding of agency mandates and the cybersecurity challenges government leaders and their IT partners face
- ✓ We simplify the complexities of logging, log retention, and log management at enterprise scale

[1] "*Improving the Federal Government's Investigative and Remediation Capabilities,*" CISA.gov, accessed November 7, 2023.

## Implementing M-21-31 with Datadog

Datadog's unified observability and security platform can help you meet the policy requirements outlined in M-21-31, regardless of your organization's logging maturity level.

| M-21-31 Requirements | Why Datadog? |
|---|---|
| **LOG RETENTION AND MANAGEMENT**<br>M-21-31 addresses the requirements in section 8 of EO 14028 for logging, log retention, and log management.<br><br>Specifically, agencies and organizations must retain logs for 30 months: 12 months in "active" or "hot" storage—which can be accessed instantly—and another 18 months in "cold" data storage that can be retrieved upon request. | To meet these requirements, **Datadog Cloud SIEM** supports 15 months of "active" or "hot" storage (three months longer than is required by M-21-31).<br><br>**Cloud SIEM** enables you to visualize security insights and investigate activity with greater historical context across your cloud environments. Use it for:<br><br>- Threat detection and hunting with legacy, historical data<br>- Infrequent investigations, historical investigations, retrospective investigations<br>- Meeting regulatory, security, and compliance requirements<br>- End-user analytics<br>- Fast indexing, search, and analysis<br>- Cost-effective pricing<br><br>For cold data storage, your Datadog account can be configured to forward logs to a cloud storage system of your own to meet M-21-31 requirements while also keeping auditability for ad-hoc investigations. **Datadog's Log Rehydration** enables you to capture log events from your archives back into **Datadog's search-optimized Log Explorer**, so that you can investigate log events that are older than 15 months. |
| **CENTRALIZED ACCESS AND VISIBILITY**<br>M-21-31 contains several provisions focused on aggregating logs to ensure centralized access and visibility across teams. | Datadog serves as an aggregator for all logs and events and allows you to process, enrich, and route all your logs from one central control plane for complete observability. The platform also simplifies cybersecurity incident investigations by giving teams across the organization access to the same data through a single pane of glass. |
| **CONTINUOUS MONITORING**<br>M-21-31 requires federal agencies to establish and maintain a continuous monitoring program for their networks. | Datadog's observability platform provides real-time monitoring and alerting for infrastructure and application performance, as well as security-related events, which can help you establish and maintain a continuous monitoring program. |

| M-21-31 Requirements | Why Datadog? |
| --- | --- |
| **THREAT MANAGEMENT**<br>M-21-31 emphasizes the importance of vulnerability management to identify and remediate security threats in a timely manner. | The threat management capabilities in **Datadog Cloud SIEM** enable you to automatically tie vulnerabilities to cyber threats and misconfigurations.<br><br>**Datadog Cloud Security Management (CSM)** delivers real-time threat detection and continuous configuration audits across your entire cloud infrastructure for faster remediation. Powered by observability data, security teams can determine the impact of a threat by tracing the full attack flow and identify the resource owner where a vulnerability was triggered. |
| **AUTOMATION**<br>To improve the efficiency and effectiveness of their cybersecurity programs, M-21-31 recommends that agencies leverage automation and artificial intelligence. | **Datadog Workflow Automation** can help you automate routine tasks, reduce the risk of human error, and free up resources to focus on higher value work.<br><br>Datadog's machine learning capabilities can help you identify potential security threats and anomalies in your logs, enabling you to respond quickly. |
| **COLLABORATION AND INFORMATION SHARING**<br>M-21-31 emphasizes the importance of information sharing and collaboration between federal agencies and industry partners on cybersecurity issues. | Datadog's collaboration features, including the ability to pivot to video conferencing or share incident updates via Teams or Slack, can help you share information and insights with other agencies and industry partners. |
| **COMPLIANCE REPORTING**<br>M-21-31 requires agencies to report on their cybersecurity posture and compliance with federal regulations and guidelines. | **Datadog Cloud Security Posture Management (CSPM)**, a part of **Datadog's CSM**, performs configuration checks across your cloud accounts, hosts, and containers. Scanning is continuous and surveys every resource, and Datadog's executive reporting provides summaries to track conformance to M-21-31 and other federal guidelines. |

## Datadog for government

Datadog is the essential monitoring and security platform for government technology architectures. Our FedRAMP® Moderate authorization reduces friction in the Authority to Operate (ATO) process, so you can innovate with fewer roadblocks and less red tape. Our specialized teams have a deep understanding of agency mandates and the cybersecurity challenges government leaders face. Visit the FedRAMP® Marketplace to see a list of federal agencies using Datadog to accelerate their missions including:

- Bureau of Fiscal Service
- Department of Agriculture
- Department of Veterans Affairs
- Federal Aviation Administration
- Federal Energy Regulatory Commission
- United States Geological Survey

## 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 pane of glass. Contact us to learn more about how we can advance your mission.

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

Open a trial account at **app.ddog-gov.com/signup**

Learn more about **Datadog for Government**