Achieving mission success: Continuous diagnostics and mitigation

Fusing data to reduce and remediate risk

Red Hat solutions for CDM

- Red Hat Integration
- Red Hat Fuse
- Red Hat Ansible Automation Platform
- Red Hat Decision Manager
- Red Hat Data Grid
- Red Hat OpenShift Container Platform
- Red Hat OpenShift Container Storage

Why Red Hat?

- **Increased security:** Our solutions meet stringent federal security requirements.
- **Reduced costs:** Our subscriptions can cost less than proprietary software licenses and support contracts.
- **Partner ecosystem:** You can work with our extensive network.
- **Open source leader:** We are a leading proponent and developer of open source software and work closely with the open source community to deliver solutions that work.

f 𝕏 in

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

redhat.com

The federal government's security challenges

The federal government faces many urgent challenges, including the need to:

- **Build a stronger cybersecurity posture.** Threat vectors are rapidly evolving, and government agencies must do whatever they can to keep up. To do that, they need to gain a better understanding of their overall risk profiles.
- **Collect real-time information from multiple sources.** This means gathering and analyzing information from disparate devices and sources and presenting it in a way that allows users to take action quickly. And collecting and managing such a voluminous amount of data, from many different places, is a massive challenge.
- **Constrain resources.** While expectations are growing, budgets are not. Additionally, long-time IT employees are retiring, and their potential replacements are looking for employers with modern IT tools and processes.
- **Speed project timelines.** Software development timelines need to shrink from years or months to weeks or days to be responsive to evolving agency and citizen needs.

Defending against cyber threats with continuous diagnostics and mitigation (CDM)

Getting in front of malicious attackers will always be a top priority within the public sector. The Department of Homeland Security (DHS) is tackling this challenge by:

- **Implementing cybersecurity dashboards.** The DHS has implemented the CDM Dynamic and Evolving Federal Enterprise Network (DEFEND) program, an ambitious effort to collect and normalize data and help government agencies fortify their risk initiatives.
- **Working with outside partners to bolster cybersecurity.** DEFEND integrators are trusted partners that process and collect the data, to ensure its quality and integrity. They make sure the information flows up to CDM dashboards to present in easy-to-understand ways.
- **Automating data distribution and analysis.** CDM DEFEND calls for fast access to critical information so that administrators can make better decisions in real-time, which is not achievable through traditional, manual methods. Data distribution and analysis must be automated.
- **Using an open source infrastructure.** The success of CDM DEFEND is dependent upon a common platform for the delivery, collection, sharing, and processing of data. Agencies need to be able to use this data to quickly take action by closing vulnerabilities and reacting to potential threats.

- **Experience:** We've worked with government agencies across the U.S. to modernize their application development processes.

Open source: Changing cybersecurity dynamics call for a flexible and agile infrastructure. Open source software delivers, providing agencies like the DHS with the ideal platform to support its cybersecurity initiatives.

Automation: Automating data collection and analysis allows administrators to receive insights and make decisions faster than ever. Automation also allows staff members to focus on the activities that attracted them to public service.

Data analysis: Government agencies are collecting data from many sources and devices. Administrators need to be able to understand what the data is telling them so they can take action. They need solutions to collect, analyze, process, and present the information so they can respond in real time.

Building a more secure, scalable integration platform for CDM

Red Hat's flexible approach to integration and process automation is ideal for CDM DEFEND and similar efforts. Our open standards-based solutions integrate with all data types and sources. Our subscription model provides choice, flexibility, and value. And our enhanced security controls allow data to be traced back to its source and can be used across all CDM components.

Red Hat® Fuse is a tested, trusted, and scalable cloud-ready platform that allows agencies to assess and maintain the accuracy and quality of their data. Agencies can add new data sources, audit the information, and receive assurance that there have been no discrepancies or data manipulation. Security for integration points is built-in. For agencies moving to event-driven architectures, AMQ streams provides commercial support for Kafka, allowing for data streaming.

Red Hat Decision Manager is a platform for developing containerized microservices that automate decision-making processes. Organizations can maintain data consistency and currency with verification and validation rules to determine data completeness. In future phases, agencies may be able to look to create business rules for remediation based on CDM dashboard data.

Red Hat Ansible® Automation Platform is a foundation for building, operating, and scaling automation across an organization. Agencies can access collections of supported, pre-composed content–such as that collected through the CDM program and provided by certified partners–and distribute that content throughout their organizations. Organizations can also automate the configuration of various security and networking tools in a common language.

Red Hat Data Grid is an in-memory, distributed, NoSQL datastore that allows applications to access, process, and analyze data at in-memory speed. The result is a superior end-user experience.

Red Hat OpenShift® is a hybrid cloud, enterprise Kubernetes application platform that makes it easier to deploy and scale CDM architectures across on-premise and cloud environments. Agencies can also use Red Hat OpenShift to deploy their CDM dashboards in a security-focused, repeatable, and automated fashion.

Learn more

Collecting and presenting data from multiple sources is not a CDM-specific challenge. As the amount of data and connected sources continues to grow, all agencies will need the flexibility to integrate resources from multiple solutions and evolve to include cloud and mobile data.

To learn more about how Red Hat can help you get a clear picture of all of the data that is most important to your organization, visit redhat.com/gov.

About Red Hat
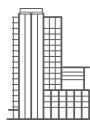
Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America	Europe, Middle East, and Africa	Asia Pacific	Latin America
1 888 REDHAT1	00800 7334 2835	+65 6490 4200	+54 11 4329 7300
www.redhat.com	europe@redhat.com	apac@redhat.com	info-latam@redhat.com

redhat.com
#F23995_0720