TD SYNNEX
Public Sector

Red Hat

Using open source to support explainable AI in the public sector

Executive summary

The public sector is about to enter into the "third wave" of artificial intelligence (AI), according to the Defense Advanced Research Projects Agency (DARPA). Agencies are preparing to move beyond "reasoning over narrowly defined problems" (the first wave) and "nuanced classification and prediction capabilities" (the second wave) toward "AI that understands and reasons in context."[1]

The last two words of that sentence–"in context"–are critical. To advance to the third phase, machines must be able to understand the context in which they are making decisions—and be able to show users how they came to their conclusions.

While today's predictive analytics and AI capabilities can provide valuable insights and actionable intelligence, public sector agencies need more. They must be confident that the AI is coming to the correct conclusions within the context of the data that it is being fed.

The "black box" aspect of AI may give some government agencies pause. From national defense to healthcare and beyond, the data modeling being done in the public sector is too important and impacts too many people for the processes behind the modeling to remain a mystery. Agencies need to understand how their technology is coming to certain conclusions, providing citizens and patients with assurances that their data analysis processes are being performed in the most transparent ways possible.

Gaining better visibility into the AI process can improve "explainable AI"–the ability for machines to clearly demonstrate and explain the rationale behind their recommendations–leading to increased trust in the systems.[2] Agencies can now get closer than ever before to this ultimate goal by:

- Bringing together teams with different talents and expertise to build solutions that meet this criteria, similar to the creation of DevOps teams.
- Creating AI solutions on stable, trusted, and open platforms that allow public sector organizations to gain better visibility into AI data modeling and analysis processes while minimizing uncertainty and risk.

In this whitepaper, we will examine how open source software, along with the core cultural tenets of the open source community, can help the public sector achieve its AI objectives. With the right combination of technology and development methodology, agencies can build more transparent AI solutions, faster, resulting in greater efficiencies and more accurate and trusted decisions.

1 *TechRadar, "Ushering in the third wave of AI," February 20, 2020.*

2 *Dr. Matt Turek, "Explainable Artificial Intelligence." Defense Advanced Research Projects Agency. Accessed June 2020.*

US$13T

AI has the potential to deliver additional global economic activity of around US$13 trillion by 2030.[3]

51%

of enterprises indicate that their current AI infrastructure will not be able to meet future demands.[4]

Figure 1. Enterprises are investing in platforms for artificial intelligence (AI) and machine learning (ML)

AI in the public sector: A baseline for excellence, yet ethical questions remain

The importance of AI is felt throughout the public sector. The healthcare industry is investigating how to use AI to diagnose diseases and in other aspects of patient care.[5] State and local agencies are using AI to minimize repetitive tasks so their workers can focus on providing more value-added services to citizens.[6]

AI is becoming particularly prevalent in the defense industry. The Joint Artificial Intelligence Center (JAIC), for example, was created by the Department of Defense (DoD) to form a Center of Excellence (CoE) that aligns with the White House's belief that "a CoE model can be an important mechanism for agencies to share AI expertise and best practices."[7]

Using open source technologies, the JAIC built a Joint Common Foundation (JCF) platform that provides DoD stakeholders with the ability to access the software and contribute to the program. The JAIC also employs agile development processes, including DevSecOps best practices, to maintain and build the platform.

3 *McKinsey Global Institute, "Notes from the AI frontier: Modeling the impact of AI on the world economy," September 2018.*

4 *451 Research's Voice of the Enterprise: AI & Machine Learning, Infrastructure 2020.*

5 *U.S. National Laboratory of Medicine, National Institutes of Health, "The potential for artificial intelligence in healthcare," June 2019.*

6 *StateTech, "How AI-based tech improves state and local government," June 26, 2019.*

7 *The White House Office of Science and Technology, "Summary of the 2019 White House Summit on Artificial Intelligence in Government," September 9, 2019.*

Yet while the JAIC is providing a stable baseline framework for the development and implementation of AI solutions, agencies will still need to introduce their own AI projects. The DoD is encouraging developers to consider the ramifications of "ethical AI" when working on these projects.[8] These standards include the ability to trace and understand how the AI systems came to its conclusions. Per the Defense Innovation Board:

> *DoD's engineering discipline should be sufficiently advanced such that technical experts possess an appropriate understanding of the technology, development processes, and operational methods of its AI systems, including transparent and auditable technologies, data sources, and design procedure and documentation.*[9]

To solve this challenge–to increase transparency and visibility in the actual process through which AI makes recommendations–public sector agencies should continue to use open source software and methodologies to implement AI responsibly, effectively, and ethically.

Open source software as an explainable AI-enabler

Building a trusted AI system is essential for enabling a wide swath of people, from the warfighter to frontline hospital workers. They all need to make quick decisions, and they may rely on AI to provide the needed information for those decisions. But they also need assurance that those conclusions are correct and were made free of bias. Understanding the process that went into the AI, how specifically it came to a calculation, can help users feel more confident that the solutions they are being presented with are the right solutions.

Closed, proprietary software can make this process difficult. By design, proprietary software tends to be very opaque. The developers do not want to give away their secrets. As such, it is exceedingly difficult to tell how a piece of software actually works–the paths that it takes to process and analyze data, from ingestion to recommendation. Without understanding the process, it can be difficult to achieve trusted, explainable AI.

Open source is different. True to its name, open source software is built on the concept of transparency. Where proprietary software makes its decision-making pathways unknown to users, open source software allows users to see how a particular data set led to a specific conclusion. This visibility helps agencies better understand how their AI processed and analyzed the data, and how it came to its recommendations.

Thanks to its flexibility, open source software allows developers to continually iterate and build upon existing applications–work that can lead to truly explainable AI. For example, Red Hat has worked with CognitiveScale, which specializes in tackling black box AI issues, to create trusted, explainable AI using Red Hat® OpenShift®.[10] This type of collaboration is rare in the proprietary software industry.

While open source cannot solve the black box problem entirely (yet), it can help agencies better understand how their tools are using and processing information. This ability will prove important as federal and state and local agencies strive to remain compliant with regulations that require transparency into their AI processes.

---

8 *U.S. Department of Defense, "DOD adopts ethical principles for artificial intelligence," February 24, 2020.*

9 *Defense Innovation Board, "AI principles: Recommendations on the ethical use of artificial intelligence by the Department of Defense," October 31, 2019.*

10 *Red Hat, "Building trusted AI applications on Red Hat OpenShift enterprise Kubernetes platform," April 9, 2020.*

Bringing teams together with DevOps

The software is only the beginning. Agencies still need people who can interpret the information that the AI provides and execute upon those recommendations.

Making AI work for government agencies will require collaboration from different teams so their collective work can be shared and democratized for the good of their agencies. By breaking down barriers between teams, organizations can also avoid the challenges detailed in the seminal paper "Hidden Technical Debt in Machine Learning Systems." The paper posits that the hard lines between machine learning (ML) research and engineering can create "cultural debt."[11] It states:

> *It is important to create team cultures that reward deletion of features, reduction of complexity, improvements in reproducibility, stability and monitoring to the same degree that improvements in accuracy are valued. In our experience, this is most likely to occur within heterogeneous teams with strengths in both ML research and engineering.*[11]

Essentially, organizations will need to deploy a new form of DevOps. In this model, data scientists and engineers work together with developers and operations managers to create solutions and solve challenges related to AI, including questions related to explainability and ethics. Their work will be instrumental in helping agencies understand the integrity of their data, what information to feed into their systems, how the systems interpret that information, how to use information to achieve mission objectives, and how to develop and deliver AI-powered applications.

While DevOps did not originate in the open source community, it shares many of the community's core tenets. DevOps and open source developers value the power of collaboration, agility, and flexibility. Indeed, open source software development is a key component of DevOps because it allows developers and operations managers to use multiple tools and technologies across common platforms, essentially bringing those teams closer together.

That mentality can be applied to the new form of DevOps. Agencies can employ the open source principles of teamwork and rapid innovation to bring together talented people with different experiences to create better AI solutions.

Combining this core cultural aspect of open source with a trusted and stable open source technology platform can help public sector organizations get closer to their goal of creating a sophisticated, trustworthy, and explainable AI system.

Why the time is right for AI in the public sector

We have explained how open source technologies can help illuminate the black box aspect of AI, and we have addressed how open source methodologies can be used to bring teams together to create smarter AI solutions. But there are other obstacles to AI adoption within the public sector, including a big one that open source could also address: the effective use of data.

11 *Google Inc., "Hidden Technical Debt in Machine Learning Systems," 2014.*

When the World Economic Forum (WEF) outlined five challenges for government adoption of AI, "effective use of data" was at the very top.[12] According to the WEF:

> *IBM estimated in 2017 that 90% of the world's data had been created in the past two years. The problem is, our organizations, both public and private, were not created to handle and take advantage of this volume and variety of data. Most organizations have a very rudimentary understanding of their data assets (i.e., the data they hold and the infrastructure that holds that data) and trying to answer even basic questions such as how many databases exist within the organization, which database contains what information, or how data is collected in the first place, can be challenging.*[12]

In other words, the sheer complexity of understanding, managing, and analyzing data is an enormous challenge for organizations. But two important advancements offer hope that now is the right time for AI in the public sector.

First, organizations now have the ability to run complex workloads on single platforms instead of within silos. Standard open source platforms like Red Hat OpenShift allow users to run complex workloads on a single platform. This ability creates data democratization, allowing multiple teams to access and interpret the same information and gain a better understanding of their organization's data.

Second, agencies can now perform resource-intensive operations on commodity hardware they may already have in place. There is no longer a need for expensive proprietary systems. Organizations can run complex computations simply by overlaying an open source platform on whatever hardware they are currently using. This ability is a massive leap forward for organizations that may be operating legacy systems or using a number of different tools from various vendors.

All of these advancements–more explainable AI, breaking down data segments, and performing large-scale data calculations on commodity hardware–have been made possible by open source technologies. Indeed, open source is bringing public sector organizations to the cusp of what is possible with AI.

How Red Hat is powering AI

Red Hat is engaged in a number of initiatives to help public sector organizations realize the potential for each of the aforementioned advancements. These initiatives focus on implementing AI solutions that lead to actionable intelligence which, in turn, supports fast, accurate, and reliable decision-making.

- Open Data Hub. Built on Red Hat OpenShift, the Open Data Hub provides a centralized self-service solution that government agencies can use to develop their own analytic and data science workloads. It provides a set of predefined AI models that organizations can use to launch, monitor and manage their own AI initiatives, making it an ideal starting point for the development of innovative and explainable AI systems.

12 *World Economic Forum, "5 challenges for government adoption of AI," August 16, 2019.*

- Israel's Ministry of Defense. The Ministry used Red Hat OpenShift to create an "AI-as-a-Service" platform that allowed their data scientists to experiment and deliver models into production iteratively through self-service and automation. They are using the service to run massive machine learning pipelines automatically and improve those models.
- HCA Healthcare. Clinicians, data scientists, and technologists use Red Hat solutions for real-time predictive analytics and data insights to more accurately and rapidly detect sepsis, a potentially life-threatening condition.

Red Hat's efforts stretch from the halls of federal agencies to the streets of local municipalities. Our solutions support the work that enables the Internet of Things (IoT) and 5G technologies, which power smart cities and other edge use cases.[13]

Indeed, edge computing will likely be AI's next frontier. As the number of connected devices continues to expand–across the battlefield, within autonomous vehicles, inside street lights, and more–data science at the edge will become increasingly important. Decisions will need to be made in real-time at each connection point, and they will need to be supported by thorough, trustworthy explanations that can easily be understood by human beings.

Red Hat will be there to support this effort through open source platforms that bring real-time intelligence to data and shine a brighter light on AI's black box–wherever that box resides.

To learn more about AI and how Red Hat can help your agency ride AI's third wave, contact your Red Hat representative or read about AI and ML on Red Hat OpenShift.

13 *Red Hat, "From the core to the edge: How Red Hat is helping to drive accelerated AI into the mainstream," November 5, 2019.*

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
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#F23975_0720