

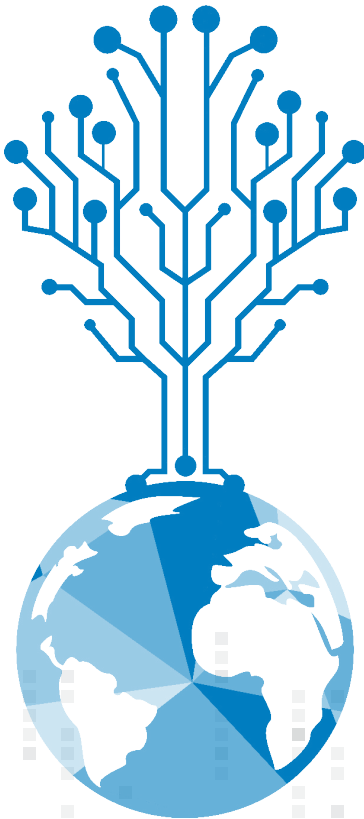
BROUGHT TO YOU BY



# Protecting American Innovation

# Table of Contents

PROTECTING AMERICAN INNOVATION .....	2
CHOOSE TECHNOLOGIES THAT COMPLEMENT EACH OTHER .....	3
<i>OpenShift as a Secure Platform for Data Science</i>	
<i>MongoDB as a Database for Developers</i>	
<i>Vault as a Scalable Secrets Manager</i>	
LEAN ON ENTERPRISE TOOLS TO HELP ENSURE A SAFE CONFIGURATION .....	5
RAPIDLY ENABLE SECURE DATA SCIENCE COLLABORATION .....	5
EFFICIENTLY ELIMINATE THE CREDENTIAL SPRAWL .....	6
TOOL SYNERGY ADVANCES INNOVATION .....	6

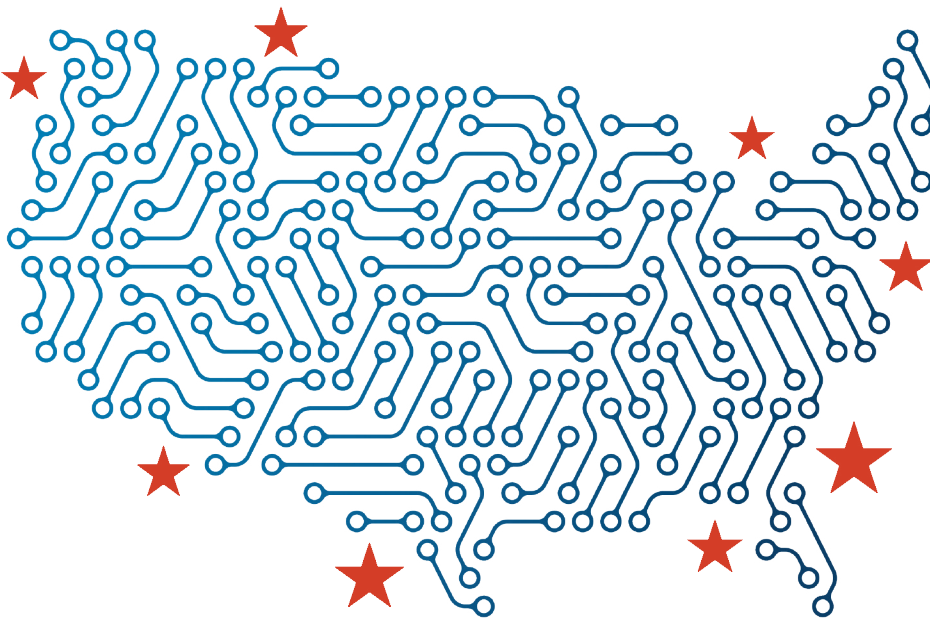


# Protecting American Innovation

**Research plays a pivotal role in American technical excellence, and we have a duty to protect it. At no time is this more important than when the funds for research come from our tax dollars.**

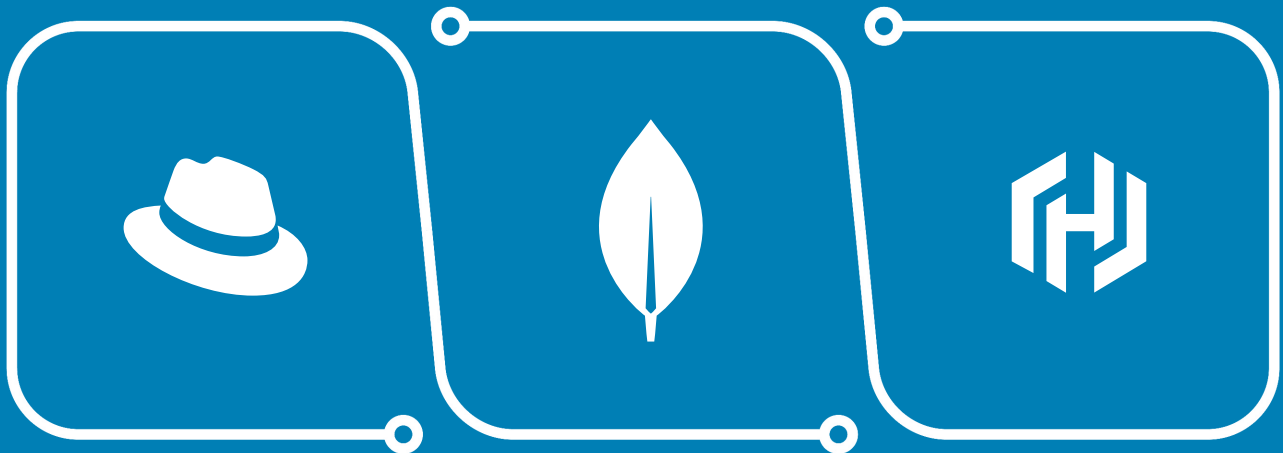
The DoD alone spent more than 122 billion dollars last fiscal year on advanced research. Investment of public funds from the DoD and other entities happens in private companies, universities, and labs, making these research organizations targets for cyber espionage and cyber theft. From the small businesses participating in the Small Business Innovation Research programs to the largest universities or defense contractors, criminals and advanced persistent threats follow the money with the intent of taking this valuable intellectual property. Consequently, teams choosing the tools they need for their projects should seek out the best features in the market and tools that complement each other, making initial setup and enabling advanced security features easier.

Take, for example, a research organization that wants to set up a data science experience for its team to develop machine learning models that take advantage of a unique data holding. They might also want to collaborate with other remote researchers or outside labs. This team needs a secure, scalable platform and data science experience, a secure, scalable database, and a scalable way to manage data access that accounts for the transient nature of students, outside researchers, or outside organizations.



## Choose Technologies that Complement Each Other

As research organizations embark on their projects, they must carefully curate their toolkit to maximize efficiency and security. This entails choosing tools that synergize effectively, facilitating higher-level activity, and reducing the burden of lower-level tasks.



Integrating three powerful technologies - Red Hat OpenShift Data Science, MongoDB Enterprise Advance, and HashiCorp Vault - offers a compelling example of how complementary tools can create a robust and secure environment for research and development endeavors.



## OPENSIFT AS A SECURE PLATFORM FOR DATA SCIENCE

Red Hat OpenShift Data Science delivers a comprehensive environment for deploying, managing, and scaling machine learning and analytics workloads. Running on OpenShift, OpenShift Data Science is emerging as a vital element for organizations looking to develop with Jupyter, PyCharm, PyTorch, scikit-learn, or TensorFlow. Providing a common cloud-native AI development platform supports and encourages collaboration across data science teams, it democratizes the use of AI tools and allows teams to implement and accelerate intelligent application development. Its Kubernetes-based architecture enables research teams to encapsulate applications into containers, ensuring consistent behavior across various environments. The OpenShift security features aid in isolating more sensitive research applications, reducing the risk of data leakage, and the integrated monitoring and logging capabilities empower organizations to detect and respond swiftly to any anomalous activities.



## MONGODB AS A DATABASE FOR DEVELOPERS

MongoDB Enterprise Advance is a widely adopted NoSQL database and serves as the backbone for storing and managing large volumes of unstructured and semi-structured data. Its flexible document-based model enables research teams to work with diverse data types, thereby supporting a wide array of applications. MongoDB's scalability ensures that research organizations can seamlessly manage data growth without compromising performance, a crucial feature when dealing with the resource-intensive scientific simulations or experiments that come from AI/ML.



## VAULT AS A SCALABLE SECRETS MANAGER

Complementing both Red Hat's OpenShift Data Science platform and MongoDB's database capabilities, HashiCorp Vault is an indispensable component for safeguarding sensitive information. Vault provides a secure platform for secrets management, ensuring that critical authentication tokens, passwords, and encryption keys remain protected from unauthorized access.

## Lean on Enterprise Tools to Help Ensure a Safe Configuration

The value delivered by these tools together starts with installation and configuration. Research teams might be capable of making the community editions work, but that comes at a cost. Valuable time is spent on configuration and integration rather than on the next technology and data advances. It also deprives the organizations of key metrics and audit insights that might call into question data integrity later. For each integration, Red Hat, MongoDB, and HashiCorp have worked closely together to remove all the guesswork. In addition to rich integration documentation, Vault and MongoDB have Red Hat OpenShift certified operators, making the three vendors a natural fit.



## Rapidly Enable Secure Data Science Collaboration

MongoDB Enterprise Advance running on OpenShift delivers the benefits of an enterprise grade system that supports data science collaboration across organizations. As an OpenShift Data Science user, an ideal world is focusing on data science and not on the database setup or schema. MongoDB enables this streamlined experience for these users. OpenShift Data Science developers just access the data, select the fields, and go. For large data sets with multiple project hypotheses, this management efficiency is significant, returning time for advancing the project.

Sharing data is the cornerstone of collaboration and research projects often involve sharing among teams located across different geographical regions or organizational boundaries. Teams can expand to include outside collaborators by simply adding a user group in Openshift Data Science and providing an API key to the MongoDB database with the dataset. Taking advantage of the field level security in MongoDB, the data owner can even redact specific fields to keep the most sensitive data hidden while fostering and getting the value of collaboration. This layered security supports collaboration out-of-the-box, enabling data owners to allow access with the confidence they can protect their data.



## Efficiently Eliminate the Credential Sprawl

To share a MongoDB API securely for this use case, organizations must address both database and service account credential rotation. Especially for teams with transient staff collaborators, this kind of credential rotation is vital to ensuring persistent access does not expose new data that was not intended to be shared. The MongoDB + Vault solution automates creating and rotating database credentials, eliminating long-standing shared credentials and reducing the risk of breach and credential leakage. Similarly, MongoDB + Vault simplifies credential management and reduces organizational complexity around managing access and secrets for service accounts. This reduced administrative overhead optimizes security and identities across platforms in a seamless workflow.

Vault's robust encryption and access control mechanisms guarantee that only authorized personnel can access sensitive research data, regardless of physical location. By integrating Vault with MongoDB, research organizations can enforce fine-grained access controls, bolstering security while maintaining seamless data accessibility for authorized users.



## Tool Synergy Advances Innovation

The synergy among Red Hat OpenShift Data Science, MongoDB, and HashiCorp Vault exemplifies the power of adopting complementary tools to establish a secure research environment. By leveraging the strengths of each technology, research organizations can store and process data effectively, collaborate across dispersed teams and with other organizations, and safeguard critical information from cyber threats. The tools mitigate key risks, preserving the integrity of research investments and empowering innovation. Only by fortifying the research infrastructure with such well-integrated tools can we ensure that American innovation remains uncompromised and continues to thrive.

### FIERCE SOFTWARE IS YOUR INNOVATION RESOURCE

Fierce Software is standing by to help project teams assemble an enterprise-ready, layered approach to securing research data without sacrificing the ability to share and collaborate across teams. Our team makes the connections between market-leading vendors and government requirements. We are your Innovation Broker. Contact [sales@fiercesw.com](mailto:sales@fiercesw.com) to get started.



[SALES@FIERCESW.COM](mailto:SALES@FIERCESW.COM)  
888-576-1572  
**FIERCESW.COM**