MeriTalk
Improving the Outcomes of Government IT

Red Hat

From Data to Real Time Intelligence:

Edge Computing for National Security Missions

The Department of Homeland Security (DHS) and the Department of Justice (DOJ) are central to safeguarding national security, with dedicated employees who secure the nation's infrastructure, fight terrorism, and enforce Federal laws. Agents and officers are spread from cities to borders and beyond, and law enforcement and homeland security investigations are growing in urgency and complexity. As a result, technology is more important than ever in the quest to respond to incidents in real time and – ideally – stay ahead of bad actors.

As law enforcement-focused agencies expand and evolve their data ecosystems, Federal investigators are becoming fluent in new investigative techniques and digital forensic tools. Those tools require robust computing power in or near the field of operations.

A potential game-changer is edge computing, which can improve agility and enable rapid decision-making in support of DHS, DOJ, and other Federal agency missions. Both departments maintain offices, stations, and field agents worldwide to address some of the most critical and urgent issues affecting national security. They need technology that quickly delivers data processing and analytical capabilities in any location, under any condition.

Faster and More Agile Computing at the Edge: Use Cases for Homeland Security and Law Enforcement

Traditional cloud computing requires data transfer across a network – to and from a centrally located data center. In contrast, edge computing takes place at or near the physical location of the user or the data source and as an example, supports faster and more robust access to Federal, state, and local law enforcement databases for DHS and DOJ personnel on the scene of an active probe. FBI personnel could query local law enforcement data by connecting with jurisdictions that use pre-

configured edge compute appliances to enable data sharing. This would eliminate the need for local law enforcement entities to clean, transform, and submit data to the FBI centrally, and it would reduce demand on FBI IT infrastructure.

Edge computing capabilities can also help investigators quickly retrieve and analyze data gathered by small form factors such as drones and body cameras. By bringing analytical capabilities to the field, DHS and DOJ agencies can assist in investigations through greater data collecting and processing, regardless of the proximity and connectivity to central IT.

Opportunities for edge computing to support law enforcement missions include:

Stopping cyber threats. Cybersecurity monitoring at the edge can identify suspicious actions on a network, prevent compromises, and gather evidence to support investigations. Black hat activities such as deploying edge "agents" in peer-based systems can intercept bad actor traffic closer to its source, saving valuable time

Securing borders and transportation. At the nation's borders, connectivity is often limited, making the transfer of data to and from headquarters slow or intermittent. Edge computing can enable agents to leverage artificial intelligence **on data available at the border in real time**. Then, with help **of computer vision and object classification**, agents can more easily detect illegal border crossings and cargo. At transportation hubs such as airports and ports, these capabilities can help identify suspicious passengers or personnel

Responding to disasters. In disaster response, where every second counts, edge computing's speed and agility are especially important. Tactical edge networks can support surveillance of disasters, such as wildfires, to gather intelligence to effectively deploy responders and evacuate residents. Edge-enabled facial recognition technology can help identify survivors

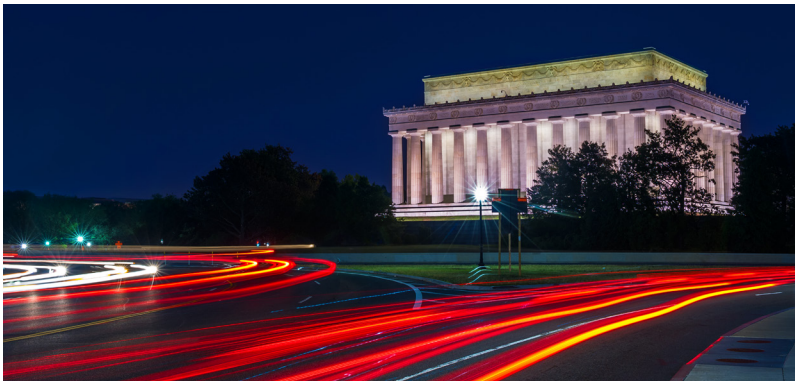
Powerful Building Blocks for Edge Computing

Red Hat helps agencies realize edge computing potential with platform, application, and developer services. These powerful building blocks help agencies solve their most challenging edge computing use cases:

Establish a common infrastructure across compute, storage, and network, from headquarters to the edge. With the Red Hat Enterprise Linux (RHEL) operating system, agencies can manage edge computing with the same tools and processes as their centralized infrastructure, yet their edge computing solutions can operate independently in a disconnected mode

Build applications once and deploy anywhere at scale. Red Hat OpenShift, the leading enterprise Kubernetes platform, delivers consistency in operations and application development from the core to the edge of the network. Through built-in tools and supporting services such as Red Hat Advanced Cluster Management and Red Hat Advanced Cluster Security, Red Hat OpenShift helps agencies make the art of the possible in edge computing a reality

Gain consistent tooling for automating workloads and standardizing configuration and deployment across the entire IT landscape. With Red Hat Ansible Automation Platform, agencies can connect, track, and manage devices and run workloads at the edge



By providing consistent tooling across the enterprise, Red Hat empowers agencies to:

- Extend computing to the field for faster, more accurate decision-making
- Provide the consistent computing experiences that users expect, from headquarters to the field
- Simplify IT operations through automated provisioning, management, and orchestration

Security Automation at the Edge

Red Hat solutions enable agencies to implement edge computing securely, relieving some of the cybersecurity burden from understaffed or overstretched Federal IT teams. Security-Enhanced Linux (SELinux), a security architecture for Linux systems, is just one example of the security protections built into Red Hat technology by default.

Downstream, Red Hat platforms enforce best practices for modern application development, preventing coding errors that could introduce vulnerabilities into agency systems. At the edge, the Red Hat Ansible Automation Platform, coupled with Ansible Playbooks, enables agencies to deploy software updates and remediate vulnerabilities at scale. In addition, Red Hat Insights, a managed service, monitors RHEL systems at the edge for vulnerabilities, configuration issues, and other potential security issues and can generate Ansible Playbooks.

Your Partner in Digital Transformation

Built upon the foundation of Red Hat Enterprise Linux, Red Hat OpenShift, and Red Hat Ansible Automation Platform, Red Hat's broad portfolio of products and solutions emphasize stability, speed, scale, and security to help national security agencies modernize and achieve their missions to defend and protect the nation.

Working with our extensive ecosystem of partners, agencies can realize long-term cost savings and avoid vendor lock-in, while enjoying the flexibility to run programs anywhere, any time. As your partner in digital transformation, we focus on modernization, hybrid cloud, and automation while maintaining the important balance among technology, process, and people.

To learn more, visit
redhat.com/en/solutions/public-sector/national-security

Thank you for downloading this Red Hat resource! Carahsoft is the Master GSA and SLSA Dealer and Distributor for Red Hat Enterprise Open Source solutions available via GSA, SLSA, ITES-SW2, The Quilt and other contract vehicles.

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

For additional resources:
carah.io/RedHatResources

For upcoming events:
carah.io/RedHatEvents

For additional Red Hat solutions:
carah.io/RedHatSolutions

For additional Open Source solutions:
carah.io/OpenSource

To set up a meeting:
redhat@carahsoft.com
877-RHAT-GOV

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