

# LEADERS FOCUS ON AUTOMATION OPPORTUNITY

By 2023, nearly 30 percent of Federal employees will be eligible for retirement – a soon-to-be reality that keeps Federal agency and IT leaders up at night. How can leaders prepare for greater productivity, capture as much institutional knowledge as possible in the interim, and ensure mission continuity and efficiency as new employees onboard? Process and infrastructure automation is an essential part of the solution.

The Federal government has been chiseling away at business process automation for decades, but many processes [remain highly manual and even paper-based](#). But, the work doesn't end once agencies automate their processes. They must then turn their attention to automating the IT infrastructure that supports and sustains their digital processes. Automation has many layers and complexities, but it yields tremendous returns when executed strategically.

Agencies have built improved automation into their strategic plans – the Department of Justice IT Strategic Plan, for example, includes the goal of integrating self-service processes through automation, to enhance customer support and continuously improve service delivery.

Many are specifying the importance of automation in RFPs and RFIs, as the Department of Homeland Security Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) organization did this summer as it looked to consolidate IT systems into a single architecture.

The RFI requested that submitting vendors make use of emerging technologies, including AI, machine learning, and robotics process automation.

"When I meet with C-level executives, I often ask them 'Have you automated enough?' The answer is usually 'no,'" said David Egts, chief technologist, North American Public Sector, Red Hat. "Leaders need to make automation a priority, instead of relegating it to their someday list. Once they start automating, they'll build a productivity flywheel that continues to yield perpetually compounding benefits."

## Powerful Force

Automation has the potential to save Federal agencies up to 1.3 billion hours, and COVID-19 has accelerated agencies' automation adoption. A recent MeriTalk study found that 78 percent of Federal IT managers said the pandemic increased their agency's focus on process automation.

Digital signatures are one example of how the Federal government has accelerated and embraced automation in the last 18 months. Many agencies had continued to rely on wet signatures for critical documents that range from contracts to law enforcement directives. When the Federal government shifted to remote work at scale, agencies had to pivot quickly to electronic signatures to avoid critical service and mission disruption.

Beyond productivity gains and delivering faster/better services to citizens, Federal leaders also see automation playing an important role in efforts to support both employee retention and professional development. Nearly three-quarters of respondents in a recent study said that one of the greatest benefits of automation is moving employees away from redundant or low-value tasks. This can support vital retention initiatives as employees' more meaningful, higher-level work is much more closely aligned with agency missions.

U.S. Customs and Border Protection (CBP) leverages automation to drive both productivity and team engagement. It used robotic process automation (RPA) to automate 45 workflows in the past year, saving the agency thousands of hours of manual labor and giving team members more time to focus on mission-critical initiatives.

*"This is one of the fastest-growing technologies within CBP," said Sonny Bhagowalia, chief information officer, CPB. "RPA applies technology which is governed by business logic and structured inputs and aimed at automating repeatable mundane business processes, leaving people free to concentrate on knowledge-based activities."*

## Turning the Power of Automation to Infrastructure and Processes

Automation across IT infrastructure offers many of the same productivity, efficiency and cultural benefits, and is increasingly important as IT environments become more complex from the data center to the edge and beyond.

IT leaders seek ways to accelerate and ensure consistency of routine processes. For example, Egts said that they have worked with an agency to use automation to break down cultural silos between groups. The agency used Red Hat Ansible Automation Platform to create an organization-wide community of practice for automating common IT tasks such as provisioning and securing virtual machines. This allows team members across the organization to share best practices and make repetitive tasks faster, more consistent, and more cost-effective.

There are also important applications related specifically to law enforcement. Laws change, and law enforcement agencies need to rapidly incorporate those changes into their systems. Hardcoding the rules into an application is an expensive, time-consuming, and risky proposition. With automated business rules and a rules engine, agencies can immediately incorporate changes without needing to rebuild an entire application.



## The Security Connection

The recent Cybersecurity Executive Order calls on agencies to expand automation with zero trust, “which embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner.” Automation will be fundamental to enabling and enforcing at scale the granular permissions that underpin the zero trust methodology.

Automation can also help secure employee onboarding and offboarding processes. Employees and contractors joining and departing organizations present the opportunity to give people too much access and possibly overlook deactivating accounts when they leave. Keeping track of all of this by hand presents significant risk. Automated workflows can integrate with HR systems and make managing these processes instant and consistent, reducing the chance for human error and boosting overall security.

## Integrate Your Solutions

There is no shortage of automation options for Federal agencies. Egts recommends taking a holistic look when considering a tool. “Don’t look at any one tool as being the be all end all. It’s important to always consider, ‘What does this tool integrate with?’” For example, Egts explained, “Red Hat Ansible Automation Platform integrates tightly with ServiceNow, which allows customers to automate IT service requests originating from that system. Just configure it and go. You can also use Ansible Automation Platform to manage any system that you can log into remotely. People often think that Ansible Automation Platform is only for Linux systems but it can automate the configurations of so much more. Beyond Linux, Windows, and UNIX systems, it can also automate the configuration of network, storage, edge, and other devices that you can remotely log into.”

As Federal leaders consider opportunities to improve efficiency, strengthen security, and give employees the best possible experiences – the path forward is to accelerate IT automation. If even a portion of the anticipated Federal retirements occur in the next three years, improved automation will pay significant dividends.



# MERITALK Q&A:

## RED HAT'S DAVID EGTS TALKS AUTOMATION AS MODERNIZATION ACCELERATOR

Federal IT professionals often feel stuck between a rock and a hard place. Their “customers” – which include every U.S. citizen as well as legions of internal stakeholders – want them to deliver modern services faster, more securely, and more cost-effectively at a time when workloads and expectations have never been greater. Couple this with record employee transition and steep competition for talent, and IT professionals face a Herculean mission.

IT professionals are embracing process and infrastructure automation to help them win the day, especially in domains where requirements change rapidly, such as national security, justice, and law enforcement. The automation landscape, however, is changing rapidly in the age of cloud, artificial intelligence, and new security threats.

To understand best practices and new opportunities, MeriTalk recently connected with David Egts, Chief Technologist and Senior Director, North American Public Sector at Red Hat. He shares first-hand insight on how Federal IT leaders are advancing automation initiatives to improve productivity, boost retention, and elevate security.

### **MeriTalk: What specific challenges can Federal CIOs address with automation?**

**Egts:** The first challenge involves new service level expectations. Today, constituents hold government service delivery to the same standards that we see in the consumer space. Automation is essential to compressing delivery cycles and elevating service delivery.

Then there's cybersecurity, where challenges grow more complex daily. System misconfiguration opens the door to many breaches. Automate configuration, and you remove the potential for human error in this vital area.

Finally, let's look at the workforce challenge. We're in the midst of “The Great Resignation.” Unless you automate, people exiting organizations take valuable institutional knowledge with them. The Federal government cannot afford that loss, especially for agencies involved in national security and law enforcement. Automation also supports retention because it eliminates highly repetitive processes, freeing employees for more strategic and fulfilling tasks.

### **MeriTalk: How are Federal IT leaders and staff using automation today?**

**Egts:** We worked with one Federal agency that used automation to break down cultural silos between groups. The agency used Red Hat Ansible Automation Platform to create a uniform



practice for provisioning virtual machines. This allows team members to share best practices and makes the process faster and more cost-effective.

In the Department of Defense and Department of Homeland Security, there's a large focus on cloud computing at the edge. However, you can't always guarantee connectivity to a major cloud provider when you're in a remote location. With automation, you can centralize technology and equipment management, eliminating the need for skilled computer scientists at every location.

There are also important applications related specifically to law enforcement. Laws change frequently, and law enforcement agencies need to rapidly incorporate those changes into their systems. Hardcoding the rules into an application is an expensive, time-consuming, and risky proposition. With automated business rules, agencies can immediately incorporate the change. Automation also supports more consistent enforcement of laws and more equitable justice as it removes human judgment from certain processes.

**MeriTalk: Agencies are focused on integrating Artificial Intelligence (AI) tools into daily operations. How can automation help move this forward?**

**Egts:** Repeatability is essential to operationalizing AI, and it's extremely difficult to achieve without automation. Transparency is necessary for building organizational trust around AI. People often refer to AI algorithms as black boxes that prevent visibility into how developers train models. Automation enables developers to document and standardize the training process, providing much-needed transparency and repeatability.

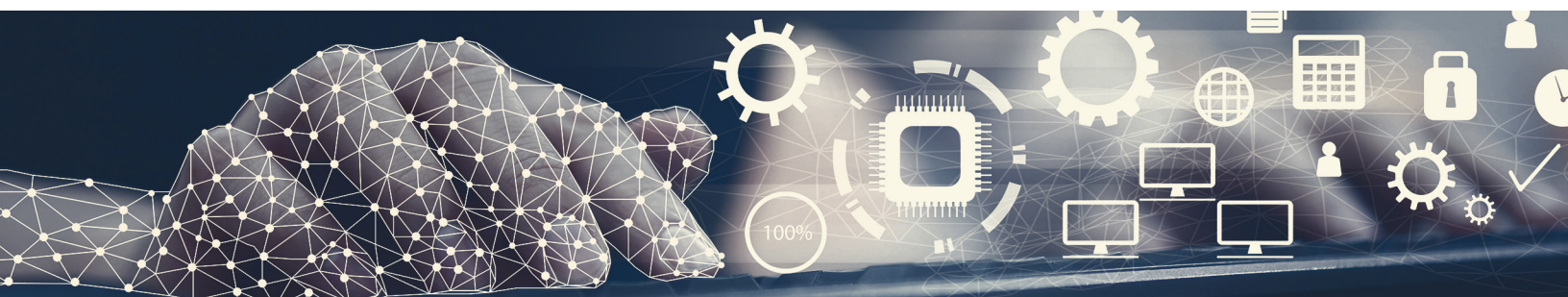
**MeriTalk: Where should Federal IT leaders focus as they implement automation across cloud and hybrid environments?**

**Egts:** When I sit down with C-level executives, the first thing I'll ask them is "Have you automated enough?" The answer is always "no." Some teams say, "We're too busy to automate. We're underwater." Well, they're underwater because they're not automating. Leaders need to make automation a priority, instead of relegating it to their someday list. Once they start automating, they'll build a productivity flywheel that continues to yield benefits.

**MeriTalk: Embracing automation will require integration. What steps can IT leaders take to properly integrate automation technology?**

**Egts:** My advice to IT leaders is "Don't look at any one tool as being the be all end all." It's important to take a holistic look and instead ask, "What does this tool integrate with?" For example, Red Hat Ansible Automation Platform integrates tightly with ServiceNow, which allows customers to automate tickets originating in that system. Just configure it and go. You can also use Ansible Automation Platform to manage any system that you can log into remotely. This means you can automate management of workloads running on Windows servers as well as network, storage, and even cloud services configuration.

Integration also plays an important role in the realm of virtual machines. Rarely does someone just want to provision a virtual machine. They also want software, connections to external databases, and more. That's where integration comes into play. You can define Ansible Automation Platform playbooks to automatically reconstitute an entire system, including Linux virtual machines, servers, network switches and cloud resources. This capability saves critical time and resources.



**MeriTalk: Zero trust architecture and automation are shaping the future of digital security. How do zero trust and automation go hand-in-hand?**

**Egts:** You can do a lot of good with automation tools, but you also can do a lot of damage. Red Hat Ansible Automation Platform supports zero trust and other security paradigms with extensive role-based access controls that limit access and actions.

Automation can also ensure a secure employee onboarding process. Relying on someone to manually lock or remove a departing employee's account can present significant risk. Automated workflow manages this process instantly and consistently, removing human error and boosting overall security.

**MeriTalk: How does Red Hat deliver automation solutions to help Federal IT teams improve internal processes and help IT leadership and staff perform daily tasks?**

**Egts:** Many automation solutions predate the cloud and weren't designed to support today's multi-cloud environments. Ansible Automation Platform, in comparison, was designed for the cloud and whatever comes next. For example, nobody was talking about edge computing five years ago, but Ansible Automation Platform was ready.

It's also cloud agnostic and vendor agnostic. If you train your team on Ansible Automation Platform, you can extend those skills to the cloud, no matter what cloud it is.

Application modernization is another priority. Ansible Automation Platform enables organizations to decouple business rules from the application, which accelerates modernization and reduces risk because you aren't rebuilding the application every time you make a policy or workflow change.

Simply stated, Ansible Automation Platform helps advance security, optimize your workforce, and accelerate service delivery – that's a powerful value proposition.

