It's no secret that constituent and mission expectations are evolving for government. Now, whether delivering services to constituents or maintaining critical defense operations, it's essential that an agency be able to balance agile service delivery with improving customer experiences — all while complying with increasingly strict security regulations. In order to strike that balance, organizations are employing tools that automate manual, time-consuming tasks and streamline operations using new and existing IT resources.

According to Sebastian Dunne, Principal Solution Architect at Red Hat who specializes in the Red Hat Ansible Automation Platform and supports their public sector customers in their IT transformation journeys, automation that supports digital transformation and cybersecurity has never been so important for mission success.

The Need for Automation

The last few years have proven taxing for government IT teams.

When COVID-19 hit, government agencies shifted their operations online and had to endure a new set of challenges that came with remote work, from accessing critical applications and documents remotely to combating new waves of cyberattacks targeted at the remote worker. Meanwhile, a record number of Americans were — and still are — applying for government services like unemployment benefits or healthcare.

As insurmountable amounts of data poured into agencies, legacy software simply could not keep up. Databases became flooded with substantial amounts of data, making not just storage a challenge, but organization and management, as well, as data became obscured or difficult to access among the mountains of information.

For citizens, this means applications they had spent time trying to interpret and fill out were getting lost, further prolonging the time they would need to wait to receive government benefits. Additionally, as public servants and government call centers became overwhelmed, it meant constituents experienced longer wait times and frustrating or labor-intensive interactions with government systems and agencies.

While many agencies were able to valiantly put fixes in place that allowed them to deliver critical services to constituents during the pandemic, the IT challenges they faced are far from solved. For many agencies — if not all — the pandemic served to expose the need for technology that can improve data management operations to ensure they are able to deliver services to constituents when and where they need them and keep critical information secure from bad actors.

In the midst of this need to transform is also the need to keep data and systems secure. Cybersecurity is a main focus for organizations at all
levels of government, and after the recent mandate for Zero Trust adoption from the White House, IT teams are looking for ways to do more with the infrastructure they already have that can help them digitally transform the security landscape.

The good news is that agencies can tackle digital transformation, improve citizen services and overhaul cybersecurity to keep up with increasingly sophisticated attacks by implementing one useful process: automation.

**Bringing Automation Agencies**

Automation offers many benefits, but the primary one for agencies is the ability to take time-consuming, repetitive tasks off their staffs’ plates, so they can focus more time on serving constituents and finding more effective ways to meet the mission.

“Automating routine manual IT tasks gives time back to IT professionals for the more important work of the agency. Not only is IT automation effective, but it also stands out among most IT initiatives as being cost-effective and easy to get started, providing immediate results and ROI.”

SEBASTIAN DUNNE, PRINCIPAL SOLUTION ARCHITECT AT RED HAT

Data management, for example, is an often manual and time-consuming task and interpreting and organizing data can be immensely difficult without the right technology — not to mention that it’s only getting more difficult as endpoints that collect data proliferate such as sensors, improved government websites, and more. Moreover, agencies need to organize this data, while still ensuring its authenticity and availability for use and analysis when needed. Automation makes it possible for IT teams to identify and remove data duplicates or bad data in order to increase data visibility and security.

Advanced technologies that automate repetitive tasks can also be taken advantage of on the consumer end. Emerging technologies can translate government documents, help citizens navigate agency websites and submit applications, making obtaining government services a much simpler experience for constituents. And with automated methods of data management, organizations can also ensure forms and applications are being processed in a secure and time-efficient manner.
When it comes to cybersecurity, many IT managers subscribe to the idea that you can’t protect what you can’t see. By tapping into automation to boost data visibility and give clarity as to what needs to be protected, agencies can more successfully employ automation to protect information with automated identity controls that authenticate users and regulate who sees what. And for agencies working toward a Zero Trust framework, that means finding ways to make identity authentication more effective.

To Dunne, cybersecurity is so critical and moving so quickly that automating security tasks, responses, and remediations is not just preferred, but required.

Red Hat’s Automation Artillery

As agencies continue to struggle against the rising tide of data, cyberattacks and citizen expectations, moving quickly to put automation in place to remedy these challenges is key. Red Hat’s automation technology allows developers to move faster and deliver modern applications quicker than ever before, making important movements in IT that require automation — such as cloud adoption, DevOps and DevSecOps — more successful. Additionally, Ansible does not use any agents for management, so agencies do not have to install any agents on managed hosts to use it within their environment — resulting in no additional product security certifications requirements.

Red Hat’s Ansible Automation Platform is a force multiplier for federal government developers looking to achieve automation at scale. With the ability to automate just about any process within an organization, Ansible is helping agencies transform quickly and effectively by making it easy for them to automate time-consuming, repetitive, and laborious tasks and improve upon how they deliver services to citizens.

Ansible collections composed of Ansible playbooks, roles, and modules for key, leading-edge OEM’s provides valuable resources to automate management of almost any IT infrastructure component, be it a server, network device or network appliance.

Custom Ansible modules written using programming languages, like Python and C++ Ruby, will allow agencies to develop and integrate custom functions in programming languages they are familiar with and provide seamless collaboration with their environment.

For example, Ansible playbooks are written in YAML format, which is a human-readable data-serialization language and can play a large role in version control. By providing an audit trail of changes, users receive consistent results every time a Ansible playbook is executed.

"Ansible Automation Platform excels at scale because it is built around a containerized architecture that ensures maximum consistency and reliability,” explained Dunne. “Government agency teams can build automation content once, then deploy it across any environment they need to with confidence, because it will run and produce the same result everywhere.”

Ansible can configure systems, deploy software, and orchestrate advanced workflows to support application deployment, all with a central focus on consistency, security, and reliability. Whether it’s operating system management, security management or data management, with Ansible, agencies can identify and automate the necessary tasks to digitally transform as efficiently as possible.

According to Dunne, “Another key benefit Ansible Automation Platform offers government agencies is a trusted automation supply chain. Maintain security and compliance with features and tooling that help ensure all content developed in-house is signed and verified, along with access to a large ecosystem of Certified and Validated Content integrations.”

He added, “It provides consistency across the organization, and can integrate with existing organizational processes and governance as they scale.”

“The mission across Red Hat with our customers and partners is to design, adopt, and evangelize zero trust architectural patterns, replacing implicit trust with the principle ‘Never Trust, Always Verify,’”

SEBASTIAN DUNNE, PRINCIPAL SOLUTION ARCHITECT AT RED HAT
Red Hat’s OpenShift is another platform that agencies can use to modernize operations. It’s an enterprise-ready, highly available, and highly scalable, Kubernetes container platform that eliminates complexity, removes adoption barriers, and includes a variety of built-in platform security and DevOps features. Red Hat OpenShift Market Place provides access to tools and applications agencies may already be familiar with in their non-containerized environment.

OpenShift gives agencies the ability to take digital transformation into their own hands with tested and trusted services that streamline and automate the container management process. The software enables efficient container orchestrations which means container provisioning, deploying, scaling and management of an application can happen at a rapid pace.

With OpenShift, users can work with traditional, modernized and cloud-native applications to support AI/ML, Java, data analytics, databases and more by automating deployment and management. Compatible with Red Hat’s Ansible Automation Platform, OpenShift users can access a library of supported tools, databases and frameworks that help organizations get faster and more secure outcomes at the edge. Using OpenShift’s application update strategy, an application can be updated with zero or near-zero downtime.

Both Ansible and OpenShift provide federal agencies with the tools they need to modernize their missions and accomplish tasks in a much more efficient manner, saving them time and money while reducing the risk of human error and giving employees greater bandwidth to serve the agency.

“Organizations that are mature in their adoption of automation are able to establish governance and standardization around their automation practices, which helps them approach their operations with an automation-first mentality.”

SEBASTIAN DUNNE, PRINCIPAL SOLUTION ARCHITECT AT RED HAT

Learn more about how together Presidio Federal and Red Hat are working to advance automation for federal agencies.