How to Make Automation Work for Government

Automation has the power to completely change the way we work. But getting that technology into government organizations isn't always easy, especially when adding automation to legacy systems that perhaps are a little outdated.

In a recent GovLoop event, experts from Maricopa County, Arizona, and RedHat shared how to overcome some of these automation adoption challenges and highlighted potential benefits for government.

The good news first: "Robots are never going to replace us," said **Lester Godsey, Chief Information Officer for Maricopa County**. Instead, automation promises to make government IT more efficient, and government agencies more responsive.

How to Make a Go at Automation

Godsey shared three pieces of advice for agencies looking to leverage automation.

THINK IN TERMS OF VALUE

IT leaders need to lay the groundwork for successful automation within their core enterprise systems. That means "understanding what the scope of the effort is … and how technology should be implemented to ensure that those business needs are being met," Godsey said. "We're not automating — hopefully — just for the sake of being able to say we've automated."

It makes sense to ask first: Where will automation have the greatest impact? This will help align the effort with business goals. "You really start off on the right foot with regards to: Why is it that we're getting involved? And how can we add value to the organization?" he said.

If automating a bad process just makes that process run more efficiently, "it's still bad," he said. To automate effectively and efficiently, "you have to have a clear, concise understanding of what your business processes and workflows are."

FOCUS ON THE BORING-AT-SCALE

With business objectives in mind, the next step is to determine which specific processes are ripe for automation.

"No. 1, pick those things that are tedious and time-consuming," Godsey said. Focus especially on those that are boring-at-scale. Although a process might take only a minute or two, "if you do that same process 1,000 times a day, the individual task itself is maybe not so time-consuming, but in in the aggregate, it's significant."

It makes sense, too, to look at those areas that represent the lowest level of organizational risk. Don't automate a process that is so essential that a misfire will derail critical operations.

And aim for simplicity. For example, don't try to automate the entire building permitting application process right out of the gate. "Especially if you're brand new to the effort or you don't have mature processes in place, my recommendation is to start simple," he said.

DON'T AUTOMATE UNCLEAR PROCESSES

Don't move toward automation without a good grasp on the process you're trying to automate. "If you're unclear about the intended outcome, or there're too many unknowns associated with this, stay away from it," Godsey said.

"Work out the kinks of what that process looks like," he said. When you have a more mature understanding of how automation comes to life in a given system, "then maybe explore expanding your scope and into areas that are more enterprise-impactful."

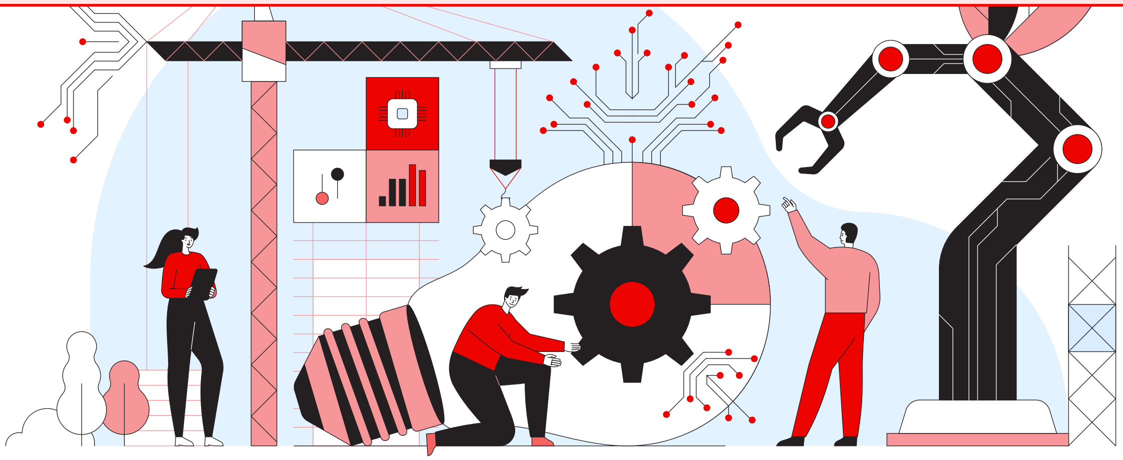
MARICOPA COUNTY USE CASES

In Maricopa County, Godsey's team has successfully leveraged automation in support of a number of key functions.

With **security orchestration and automated response**, the cyber team receives intelligence from trusted sources on questionable domains and sketchy IP addresses. The system will then "take that information, ingest it automatically — without an analyst having to manually get involved," he said. This helps speed remediation.

Automation also supports **data enrichment**, adding context to security event data in order to generate actionable insights. Analysts do this hundreds or thousands of times a day: Automation makes it happen faster and more consistently.

Maricopa also uses automation in support of its **migration to the cloud**. Customer service departments, for example, can "actually request virtual resources, like a virtual server or space," he said. With automation tools, the end user "can immediately consume that service."



Spotlight on Network Automation

For government IT teams, network management is often one of the most time-consuming tasks. It's crucial to mission success, but it's also labor-intensive. Automation promises to streamline these efforts, freeing IT talent for higher-value work, said Ajay Chenampara, Automation Strategist at Red Hat.

During his presentation, Chenampara discussed how to leverage automation to improve the performance of network infrastructure.

THE CASE FOR NETWORK AUTOMATION

Because networks are both fragile and mission-critical, some agencies are reluctant to tinker here. "It's one of the last places in the IT infrastructure where automation is talked about," said Chenampara.

In fact, automation can play a key role in ensuring that networks are secure and performing optimally. With automation, IT teams can more effectively configure the network stack, test and validate existing network state, and discover and correct network configuration drift.

More broadly, network automation supports digital transformation and encourages public trust, which can be eroded by "performance hindered by old technology behind the scenes," Chenampara said.

When agencies tap automation to improve system performance, "the user experience keeps improving" and trust increases, he said.

NETWORK AUTOMATION IN ACTION

Government can look at a number of key uses for network automation.

There's **blackholing**, for instance. This automated technique can help mitigate the impact of a distributed denial of service (DDoS) attack, Chenampara said, by redirecting suspicious network traffic to a "black hole," a virtual void that drops all incoming traffic without delivering it to the intended recipient.

In addition, network automation supports **configuration compliance**. IT teams are tasked with configuring routers, switches, firewalls and load balancers, with the aim of ensuring that "all are in compliance with some known good configuration template," Chenampara said.

Automation makes that happen not only efficiently but consistently, eliminating the potential for human error in these key processes.

A PATH TOWARD INFRASTRUCTURE AUTOMATION

Chenampara pointed to Gartner data showing that by 2025, 70% of organizations will implement some sort of "structured infrastructure automation." What is meant by structured?

In traditional automation, IT teams may download free software without adequate controls. That's problematic. "How do you know that they are not introducing a new attack vector by downloading something free and pointing it at your production endpoint?" Chenampara said.

Structured automation, on the other hand, refers to "something formal, something commercial off the shelf that can be supported, that can be secured, that can be quality-tested," he said.

Structured infrastructure automation offers simplicity. It's intrinsically secure, and readily scalable. "A large number of my engineers and subject-matter experts can start using this automation without too much friction," he said.

OVERCOMING OBSTACLES

Government agencies may encounter a number of obstacles on the road to network automation.

Endpoints may be hard to access, from a configuration point of view, and there's a lack of standardization across "disparate systems with different types of configurations," Chenampara said.

He described the Red Hat Ansible Automation Platform as offering a way forward. "It is built to be simple," he said. "Anybody can read it and understand what's happening."

It's scalable across multiple systems. "It works with hundreds of OEMs (original equipment manufacturers)," he said. "Whether you're a Cisco shop, or Juniper shop or whether you're a Windows or a Linux shop, it doesn't matter. Ansible works with all these endpoints."

Finally, it is secure. "Security is inherent in anything that Red Hat builds," he said, adding that the Ansible platform "is the only automation platform where you can enforce a secure software supply chain for automation."

With network automation, government IT teams can block malicious traffic, ensure configuration compliance and take the human effort out of routine tasks such as updating the access-control lists and implementing operating system patches and upgrades.

Rather than take jobs away from skilled technologists, this promises to free them up, empowering government to do more with the talent it has on hand and to serve constituents more effectively.

Watch the on-demand session to get more insights into the art and science of automation.