End-to-End Security Automation in Government Today

MARKET TRENDS REPORT

govloop

Red Hat

Introduction

It's not news to anybody in government that new, complicated cyberthreats are emerging every day, battering organizations. And simple oversights — like not keeping up with the latest security patches — can lead to breaches with significant ramifications.

Governments are also increasingly moving more workloads to the cloud on their modernization journeys. As the growing adoption of hybrid and multi-cloud environments makes the government IT landscape more complex, many governments — especially at the state and local levels — simply don't have the IT staff to keep up with it all.

States and cities are also easier targets for hackers than federal agencies with bigger security budgets; and therefore, they may often find themselves in the crosshairs of hackers, with devastating consequences.

"State and local governments are responsible for safeguarding everything from election systems to an increasing amount of sensitive personal data – from Social Security numbers and credit card information to detailed medical records," said Michigan Sen. Gary Peters. "Despite being targeted by hackers and bad actors, states and local communities don't always have access to the resources and expertise needed to protect your information from a breach."

Additionally, constituents are engaging electronically with state and local governments at an increasing rate, expecting seamless online experiences like the ones they receive in the private sector. It is difficult for state IT teams to keep up with these expectations while maintaining good security postures.

There is a path forward, though. State and local governments can leverage automation to enable a more effective and proactive security and incident response strategy.

By automating security capabilities like enterprise firewalls, intrusion detection systems, security information and event management, organizations can better unify responses to cyberattacks. Through the coordination of multiple, disparate security solutions, unifying responses will help these technologies act as one in the face of an IT security event.

In the following pages, we'll explore why automation is critical for state and local governments and how they can implement it to stay secure. We also gain insights from Ryan Kraus, RHCSA Senior Cloud Solutions Architect at Red Hat, a leading open source technology provider.

BY THE NUMBERS

90%

Networkwide, holistic automation can save IT departments more than 90% of their workload on these maintenance requests.

12 months

Ransomware attacks on state and local governments have more than tripled over the last 12 months.

42%

of local governments have successfully adopted a cybersecurity framework based on national standards and guidelines.

67%

of states report they lack adequate funding to develop sufficient cybersecurity.

Budget and staffing remain top barriers to an effective cyber program in state and local governments.

200

There have been nearly 200 publicly acknowledged ransomware attacks against state and local governments since late 2013.

THE CHALLENGE

An Increasingly Complex Security Environment

In a complex IT environment, even small tasks can take extended time to complete. Sprawling and legacy systems are hard to develop, deploy and maintain. Constituent demands only increase the complexity, and IT teams struggle with management, availability and cost.

Unfortunately, despite this growing complexity of systems, state and local IT professionals often have limited resources. This makes proactively combating changing security vulnerabilities challenging and leaves their data and applications exposed.

Additionally, many organizations lack a basic ability to determine what software runs on their systems, due to years of intertwining legacy systems built over one another. This means state and local governments are sometimes operating in the dark when it comes to their attack vectors and potential remediation.

Deploying security patches is a critical remedy for many of these issues. Unfortunately, it can be an extremely complicated, manual and time-consuming process. According to the National Institute of Standards and Technology (NIST), "Timing, prioritization, and testing are intertwined issues for enterprise patch management. Ideally, an organization would deploy every new patch immediately to minimize the time that systems are vulnerable to the associated software flaws." But the reality is that prioritization and limited resources affect when and which patches are applied, causing many governments to patch behind schedule.

Furthermore, state and local IT departments don't always have the staff to constantly survey their assemblage of systems, networks and applications. Problems have to be taken care of retroactively, and it can often take months to find and patch a failure, even with IT departments working quickly.

"A lot of security today, for these reasons, is reactive," said Kraus. "This means you're reacting to scan results as they come in, rather than being proactive and upfront with hardening and securing the system."

What's the best way for state and local governments to overcome these issues and meet security and compliance demands? The answer is moving to an operationalized and automated process for better IT security and protection.

Solution: End-to-End Security Automation

Automation tools make it easier for cybersecurity professionals to enforce security best practices, as well as meet internal and external security mandates.

Security automation refers to the use of automatic systems to detect and prevent cyberthreats while contributing to the overall threat intelligence of an organization to plan and defend against future attacks.

As we've discussed, due to the entanglement of IT systems, patching or maintenance isn't as simple as it should be. Networks have dependencies, and if a vulnerability is patched, the temporary fix could throw off a string of intertwined applications.

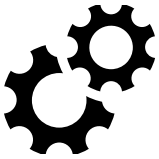
Automation, however, can patch, maintain and protect systems as soon as a vulnerability is detected. Tests can also be conducted automatically to ensure connected applications are still in working order.

"Humans are notoriously bad at repetitive tasks," Kraus said. "With the expanded complexity of IT systems, a small fat-finger mistake can cause massive security implications. But if you build a culture of automation, when security teams codify their requirements for systems, they can be assured that systems will be stood up the correct way every time."

End-to-end security automation is key to staying on top of today's growing threat environment. In today's complex IT environments, security is paramount – security of your systems, security of your data and security of your citizens' data. Not only must you be able to define what it means for your systems to be secure, but you also need to be able to simply apply that security, constantly monitor your systems and remain compliant with that security.

Using automation is a necessary first step for security. The proper automation tooling allows you to apply the security you need in a simple, consistent manner, allowing you to concentrate on more mission-critical tasks.

BEST PRACTICES
Accelerating Automation



Automate legacy deployment processes

Manual approaches to packaging and deploying workloads are naturally lengthy, error-prone and difficult to maintain. Even in situations where you've used automation, any initial understanding between business, development and operations fades quickly over time as resources move up or out of the team, documentation lags and specialized technical skills dwindle. An appropriate IT automation strategy can enable teams to treat legacy systems like DevOps, predictably automating provisioning and deployment with tools that foster understanding and involvement across the organization.

Establish standard approach and management

In areas where you use automation, an array of tools and approaches lead to increasing chaos that prevents efficient operations and effective governance. Gaining understanding across business, development and operations is difficult amid a sea of scripting languages, automation tools and ad hoc management solutions. Further, initial understanding fades quickly as new hires come on, documentation lags and the selected tools lose popularity or support. Standardizing tooling, approach, monitoring and management is crucial to delivering effective and efficient automation at enterprise levels.

Develop a culture of continuous improvement

Establishing an intelligent approach to developing, deploying and managing automation requires more than a reliable and understandable platform. It requires informed governance that ensures reliable operations and responds readily to new challenges. Teams must collaborate across traditional departmental boundaries to share their latest challenges and insights.

HOW RED HAT HELPS

Red Hat believes automation is a strategic and foundational component of IT modernization and digital transformation. As such, it provides a full set of management solutions that use a common, simple automation language. The solutions help to transform IT operations and create a comprehensive automation approach to support digital business. Based on open source projects and standards, these products deliver more control and choice for your IT infrastructure.

Ansible by Red Hat is a simple-to-use IT automation engine that transforms the repetitive, inefficient tasks of software release cycles into predictable, scalable and simple processes. It automates cloud provisioning, application deployment, configuration management and service orchestration to let developers spend more time on their work and help operations more easily support deployment pipelines.

"Ansible is easy to learn and universally applicable," said Kraus. "The goal of automating security should be in reducing technical debt, not increasing it. If every IT department is managing automation in their platform, your organization will build silos, increase technical debt and never realize the full efficiencies of a true enterprise capable automation platform."

Red Hat also provides OpenShift, an enterprise-ready Kubernetes container platform with full-stack automated operations, to manage hybrid cloud and multicloud deployments.

"Ansible works across the entire enterprise, and it's a very approachable language," said Kraus. "And OpenShift provides the automated infrastructure beginning to end so you can codify your security requirements and enforce them throughout the lifecycle of the application."

Learn more here.

CASE STUDY

Increasing Simplicity in the Cloud at NASA

The National Aeronautics and Space Administration (NASA) is the agency responsible for the nation's civilian space program and aeronautics and aerospace research. As advanced as NASA is, even it can get bogged down with its technology environments.

NASA needed to move roughly 65 applications from a traditional hardware-based data center to a cloud-based environment for better agility and cost savings. The agency migrated many of its applications "as-is" to a cloud environment as a result of the rapid timeline. This created an environment spanning multiple virtual private clouds (VPCs) and AWS accounts it could not easily manage.

Even simple things, like ensuring every system administrator had access to every server or simple patching, were extremely burdensome.

To remedy this, NASA turned to Red Hat and Ansible Tower to manage and schedule the cloud environment.

As a result of implementing Ansible Tower, NASA is better equipped to manage its AWS environment.

Tower has allowed NASA to provide better operations and security. It has also increased efficiency as a team.

Other results included:

- Updating nasa.gov took over one hour, but now takes under five minutes
- Patching updates, which used to be a multi-day process, now takes 45 minutes
- Achieving near real-time RAM and disk monitoring (accomplished without agents)
- Provisioning OS accounts across the entire environment in under 10 minutes
- Baselining standard AMIs went from one hour of manual configuration to becoming an invisible and seamless background process
- Application stack set up went from one to two hours to under 10 minutes per stack

"Ansible Tower has allowed us to provide better operations and security to our clients. It has also increased our efficiency as a team," a NASA IT leader concluded.

Conclusion

Automating existing methodologies and systems will help your security teams make more efficient use of resources: people, processes and technology. In today's intricate government IT environments, security is critical. State and local governments must be able to define what it means for their systems to be secure – but they also need the ability to simply apply that security and constantly monitor systems to ensure they remain compliant. Moving to automation as part of your IT best practices is a necessary first step.

ABOUT RED HAT

Red Hat is the world's leading provider of open source solutions, using a community-powered approach to provide reliable and high-performing cloud, virtualization, storage, Linux and middleware technologies. Today, Red Hat is at the forefront of open source software development for enterprise IT, with a broad portfolio of products and services for commercial markets. That vision for developing better software is a reality, as CIOs and IT departments around the world rely on Red Hat to deliver solutions that meet their business needs. Solutions that provide technology leadership, performance, security, and unmatched value to more than 90 percent of Fortune 500 companies.

Learn more here.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop