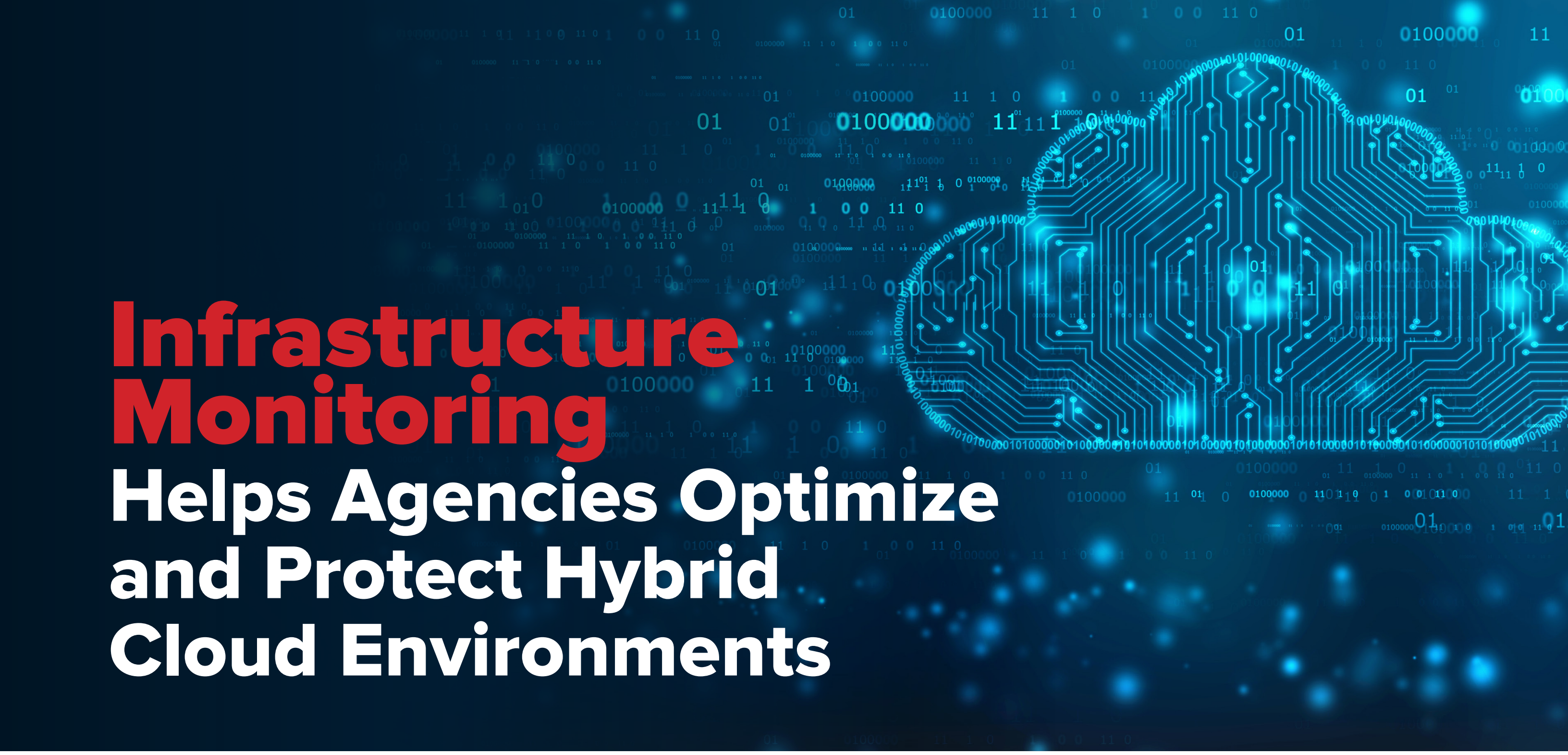

# Infrastructure Monitoring

## Helps Agencies Optimize and Protect Hybrid Cloud Environments

State and local governments moving to hybrid cloud environments need powerful tools to control costs, streamline operations and harden security. Increasingly, they're turning to infrastructure monitoring software, which helps them grapple with the inherent complexities of hybrid cloud. This is especially true for agencies modernizing their IT environments with tools like application programming interfaces (APIs), containers and microservices.

Infrastructure monitoring gives agency IT leaders tools to ensure the core components of a cloud environment — storage, compute, networking and security — work together to the best of their ability. Moreover, a robust monitoring solution gives agencies a unified platform to manage and optimize hardware and software from a wide range of vendors.

There's plenty at stake for agencies that ignore the potential of monitoring tools.

"If you fail to monitor, then you could have cost overruns, data leakage and compliance-related data sets landing in places you don't want them to be," says Matt Lawson, director of solutions engineering for state, local and education at NetApp, a market leader in infrastructure monitoring technologies.

Infrastructure monitoring drives value in state and local governments by:

**Optimizing complex environments.** Monitoring software reveals opportunities to reduce costs, improve performance and predict compliance problems before they arise. Orchestrating containers, microservices, APIs and other modern tools in hybrid environments adds even more complexity.

Infrastructure monitoring makes it easier to optimize these disparate elements from a single software interface. The software can be tuned to match uptime goals and service level agreements (SLAs). Hardware can be scrutinized for signs of wear and tear or excessive heat.

"You can make sure everything's working functionally," Lawson says. "If something's not working within the spec, you can quickly identify what that is and then zero in on it." This capability extends to container management on platforms like Kubernetes and Docker.

How can a CIO determine that a hybrid cloud environment needs to be optimized? "The biggest symptom of poor optimization is a huge cloud bill," Lawson adds. Monitoring tools help identify the drivers of cloud cost overruns.

**Streamlining cloud transitions.** Monitoring helps avoid unnecessary expenses in migrated workloads. State and local governments often discover that public cloud services generate expenses that exceed budget expectations because agency IT departments are paying for resources they aren't using — or they are using resources in ineffective ways.

"As you put infrastructure in the cloud, you're paying by the minute and the hour for any idle resources," Lawson says. Moreover, workloads that require high-powered virtual machines on-premises might not need all that power in the cloud — driving unnecessary costs that pile up quickly across dozens or hundreds of workloads.

"Agencies need to right-size their infrastructure to match the workloads they're actually running — so they're not overbuying in the cloud," Lawson advises.

With hybrid cloud, IT leaders must balance capital expenses in on-prem hardware versus operating expenses in the cloud. Infrastructure monitoring helps CIOs strike this balance.

**Detecting ransomware and other cyber threats.** Hybrid cloud environments are not immune to cyber risks like ransomware, hacking and unauthorized use of agency data.

"The bad guy has to be right only one time, while the team protecting the infrastructure has to be right every single time," Lawson cautions. This requires a comprehensive approach to data protection in the hybrid cloud.

Security appliances and endpoint protection software provide essential protections, for instance, but they do not go far enough. "You want to make sure you're doing security checks at every layer," Lawson says. This includes monitoring at the data level for signs of encryption that reveal a ransomware attack. Monitoring can also detect evidence of an employee exfiltrating data improperly.

"The worst is when you're hit by ransomware and don't even know it," Lawson says. "When it finally shows up two or three weeks later, you're not dealing with remediating 30 seconds worth of damage. Now you're remediating three weeks of damage. In situations like that, recovery is extraordinarily difficult."

Monitoring tools can also help automate difficult data protection challenges, like maintaining compliance and protecting personal data.

"The software can look at the data and automatically identify compliance-related data sets, and then report that out to that agency," Lawson says. This helps agencies certify their data is properly protected.

## Guidance for Agencies Implementing Infrastructure Monitoring

Agencies that recognize the appeal of infrastructure monitoring need to embrace a few core principles when implementing a monitoring toolset:

**Hybrid cloud is here to stay.** "The predominant IT sourcing model for at least the next 10 years is going to be hybrid cloud," Lawson says. Thus, government agencies need infrastructure monitoring software that excels across on-prem and public cloud environments. "You don't want to learn one toolset to help you manage your cloud workloads and a different toolset to help you manage your on-prem workloads," Lawson adds.

Why is this unity so important? Because more workloads will span the hybrid cloud. A business process workload might start in an on-prem data center, move to the public cloud and then return to on-prem.

"You'll want that single pane of glass for both on-prem and the cloud," he says.

### What to Look for in a Hybrid Cloud Monitoring Solution

✓ **Optimization.** The software should clearly identify opportunities to reduce costs and improve performance.

✓ **Comprehensive scope.** Architecture monitoring must work with all the hardware, software, virtual machines and containers in a hybrid cloud environment.

✓ **Unified perspective.** All monitoring must happen in a single interface that's easy to operate and intuitive for users.

✓ **Intelligence.** Software should use artificial intelligence/machine learning to identify patterns and automate complex processes.

✓ **Data-layer coverage.** Monitoring should extend to the data layer to flag anomalies that point to security threats.

✓ **Compliance.** Monitoring tools should help agencies anticipate and resolve regulatory challenges.

**Agentless tools are more flexible.** Some monitoring platforms require software agents that perpetually scan infrastructure for signs of trouble. Agentless tools, by contrast, operate passively, using advanced algorithms that flag problems as they arise. It is important to distinguish between the two varieties.

"Agent-based monitoring tools are a bit more difficult and unwieldy to use because you have to go out and install them on every single asset or component in the infrastructure for them to work," Lawson says. "With the agentless approach, you don't have to install software or toolsets on individual components."

Some specific use cases may be better suited to software agents, but agentless tools are a better choice for complex hybrid cloud environments because they're much simpler to deploy, manage and run.

**Experienced partners are essential.** There's no substitute for working with a vendor that has deep experience with hybrid environments in public sector agencies.

Otherwise, the path to monitoring may be fraught with pitfalls. "Either you might implement it incorrectly, or you might not leverage all the value that the monitoring tool can help you achieve," Lawson cautions. "We find that those who work with professional service implementers who have done it before have the best outcomes and the most success with these toolsets."

*This piece was written and produced by the Center for Digital Government Content Studio, with information and input from NetApp.*

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: NetApp®

In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds. As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services, and applications to the right people—anytime, anywhere.

IMAGE PROVIDED BY SHUTTERSTOCK.COM