aws | NetApp®

How Agencies Can Bolster Cyber Resilience

in an Increasingly Cloud-Focused World

Introduction

State and local government agencies have increasingly turned to cloud in their efforts to streamline constituent services, optimize data use and storage, and improve internal workflows. However, shifting critical information to a cloud environment can introduce new cybersecurity concerns if not done properly.

> **The security of all data is critical, regardless of being on-premise or in cloud. Putting data in the cloud moves the data further away from the physical control of the user, which increases the requirement for best security practices for data in cloud to avoid additional cyber risk or exposure.”**
>
> **JIM COSBY,**
> Chief technology officer for public sector, NetApp

While the cloud itself has proven secure, it also “can make some tasks so easy that a person unaware of good security practices could expose their organization to more risk,” said Sean Phuphanich, Sr. Solution Architect at Amazon Web Services (AWS).

If not done correctly, state and local entities can sometimes adopt cloud without organizational security awareness or controls resulting in unnecessary additional risk. “The security of all data is critical, regardless of being on-premise or in cloud. Putting data in the cloud moves the data further away from the physical control of the user, which increases the requirement for best security practices for data in cloud to avoid additional cyber risk or exposure,” said Jim Cosby, a CTO for public sector at NetApp.

What’s needed is a renewed focus on “cyber resiliency.”

Understanding resiliency

In state and local government, cybersecurity generally takes the form of multiple, often disaggregated, defensive solutions. Cyber resiliency calls for a more coherent and holistic approach. "It's all about layers and components that together make up an overall system," Cosby said.

Operational resilience and cyber resilience go hand in hand. It is not just about being able to defend against attacks, but also to recover quickly.

Public sector organizations often start improving their cyber resilience by using the guidelines laid out by the National Institute of Standards & Technology (NIST). The NIST cybersecurity framework helps organizations manage and reduce risk and categories core functions as identify, protect, detect, respond, and recover from cyber threats.

> "
>
> **Teams have practical limits to the time they can focus on cyber resilience. Operating in a cloud environment reduces the surface area and responsibilities for teams: The less time I'm troubleshooting or replacing hardware, the more time I have to thoughtfully plan, configure, and test my cyber security and recovery strategies.**
>
> **SEAN PHUPHANICH,**
> Senior solution architect, Amazon Web Services

That framework "is just as useful in the cloud as anywhere else," Sean said. In fact, cloud is ideally suited for implementing this kind of holistic cyber strategy. "Cloud's ability to deploy and throw away environments with ease means that updating and testing new best practices becomes a much easier task, compared to managing everything yourself."

In practice, cyber resiliency in the cloud starts with the vision of IT leadership across a range of interconnected functions, including both prevention and remediation.

"In order to have cyber resiliency, you first need to define what are your best practices in terms of preventing an attack. You need to look at privacy: encryption of data at rest and encryption of data during transit," Cosby said. "Then, in addition to prevention, your approach to recovery also needs to be a part of your plan. You need to have backups, and you want to have a way to recover that data."

Here again, cloud is ideally suited to this approach, in so far as cloud deployments lower the administrative burden on already-overtasked IT professionals.

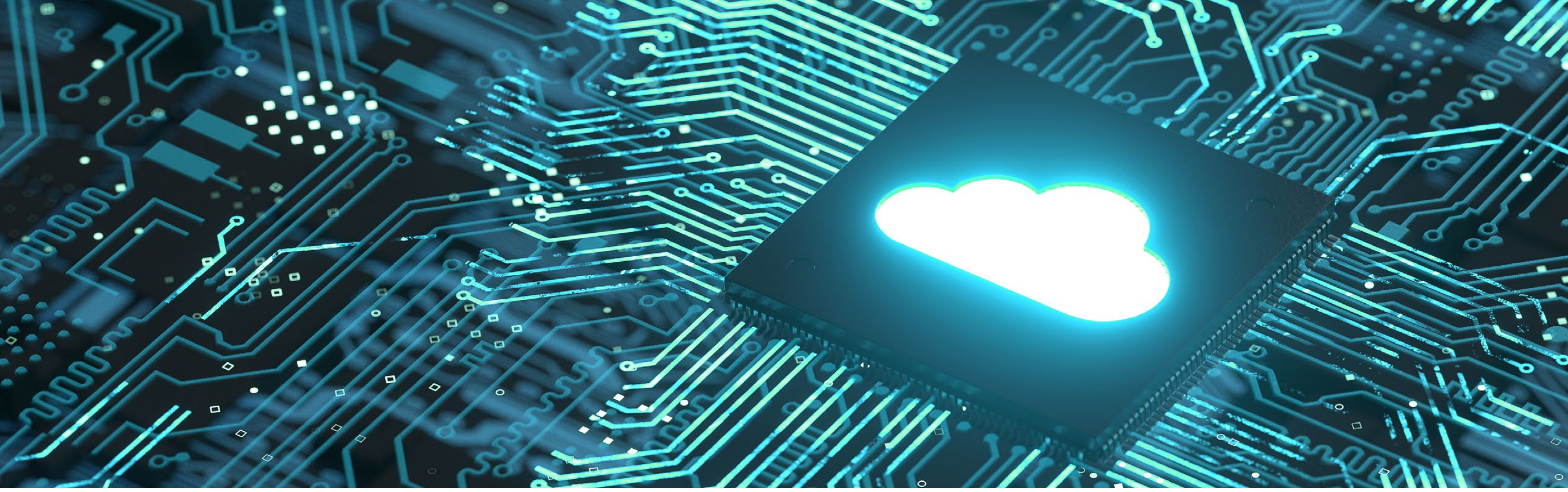
"Teams have practical limits to the time they can focus on cyber resilience," Sean said. "Operating in a cloud environment reduces the surface area and responsibilities for teams: The less time I'm troubleshooting or replacing hardware, the more time I have to thoughtfully plan, configure, and test my cyber security and recovery strategies."

How NetApp and AWS can help

Cloud doesn't ask you to sacrifice agility for security. AWS provides the environment and tools to rapidly build secure, testable environments. AWS managed services also have security features aligned to best practices and documentation includes common security setup.

For example, AWS offers Amazon FSx for NetApp ONTAP, a fully managed service that provides highly reliable, scalable, high-performing, and feature-rich file storage built on NetApp's popular ONTAP file system.

This solution — that has just achieved FedRamp Moderate and High status as well as Impact Levels



2, 4 and 5 — enables broadly accessible data that's protected and secure, compliant and governed, analyzed and monitored. It helps state and local entities to meet their needs for performance, data protection, and efficiency in the cloud.

"It effectively gives you all of the file and block data capabilities that customers have had on premise for 30-plus years," Cosby said. Agencies "can freely and easily lift-and-shift, backup-and-recover, or migrate their data from on prem to the cloud. They get security, with encryption of data at rest and in transit. They get snapshots and recovery points that allow them to recover and recoup data in seconds or minutes instead of hours or days."

This approach delivers de-duplication, compression, compaction, and tiering of data out to a lower-cost medium where appropriate. It gives agencies the flexibility to move data in or out of the cloud quickly and easily, all while ensuring the highest levels of cybersecurity.

Having a compatible NetApp service "makes it easier to lift and shift existing solutions to cloud," Sean said, while still maintaining NetApp's proven security features.

Going forward

Those looking to elevate their cyber posture in the cloud can take some practical actions right away.

The first step is to figure out where you stand. "You want to identify what you have and what you need," Cosby said. "Where does data reside and what's your risk? Do you have governance and compliance concerns? Then you want to set up your goals around cyber resilience and recovery, how you will be able to identify, respond, and recover."

For IT teams that may be new to the cloud environment, it's important to do some upfront education, and to give them a test space for learning how security operates in the cloud. "Access to a sandbox environment is important to getting over the fear of the unknown and rapidly improving cloud skills," Sean said. Making mistakes and learning from them through rapid iterations in a safe environment is what allows teams to consistently have great outcomes in production environments.

With an eye toward cyber resilience, close cooperation with a consulting partner can be "a powerful accelerant to the upfront work in planning and migration," Sean said. By laying a solid foundation, it becomes easier to implement and sustain cyber resiliency for the long haul.

Learn more about how NetApp and AWS can help your agency improve cyber resilience.