Arizona simplifies cybersecurity with the cloud

Arizona follows a cloud-first model, with 80% of its infrastructure — including more than 2,800 applications — in the cloud. The state has become more flexible and resilient by closing 90 data centers and saving nearly $11 million in recurring costs annually.[1]

The cloud also helps Arizona manage cybersecurity risks.

"It allowed the state to roll out a shared security model throughout our AWS [Amazon Web Services] cloud infrastructures," says Randy Wheaton, director of cloud and data center infrastructure for Arizona Strategic Enterprise Technology (ASET), a division of the Arizona Department of Administration. "We took advantage of native cloud services geared toward identifying weaknesses and gaps in cloud architectures and access control management processes."

Arizona's IT structure

Wheaton and the ASET team are responsible for the statewide technology strategy and operational readiness of mission-critical systems. ASET supports cloud-based enterprise resource planning, human resources, and other applications shared by all state agencies; provides a variety of IT services to individual agencies; and sets technology strategy and policies for the state.

Before migrating to the cloud and consolidating data centers, ASET managed a number of on-premises cybersecurity solutions requiring physical hardware, maintenance, and on-site staff. An ongoing concern was physically securing the state's data centers.

As ASET migrated applications and workloads to the cloud, some, but not all, concerns were alleviated. ASET still needed to confirm all policies and controls traditionally used in an on-premises environment were applied in the cloud.

Cybersecurity made simple

ASET recognized it needed to use cloud-native security solutions to support the state's cloud-based environments. ASET's cyber goals included:

- ☑ Consolidating enterprise cybersecurity tools for cost savings and standardization
- ☑ Securing the state's rapidly deployed remote workforce
- ☑ Focusing on Zero Trust and endpoint detection

The department chose a number of cloud-native tools from Amazon, including Amazon CloudWatch, AWS CloudTrail, Amazon Guard Duty, and AWS Key Management Service (KMS). By improving visibility and control across the new environment, these tools strengthened cybersecurity and compliance, streamlined monitoring and policy enforcement, and improved key management. ASET has also observed greater service stability and reduced downtime.

"Both CloudWatch and CloudTrail are critical to seeing how the environment is performing, as well as where the security gaps are coming from," Wheaton says.

Complete visibility. With CloudWatch, ASET collects and visualizes metrics about its infrastructure, monitors real-time log files, and automates operational processes based on changes in the environment.

Better controls. By tracking user activity and API usage across AWS accounts, CloudTrail improves event logging, operational risk auditing, governance, and compliance.

"A lot of our databases had been running enterprise or standard SQL,

and none of it was encrypted on premises," Wheaton says. "Once we started moving into the cloud, we started putting controls in place to have everything encrypted in transit and at rest."

CloudTrail also helps ASET prioritize gap remediation efforts across the state.

"It points out our deficiencies right inside the AWS environment," he says. "It tells me where my multifactor authentication issues are. It tells me if I have S3 [Amazon Simple Storage Service] buckets that aren't versioned or if there's no encryption. It gives me a plethora of data. Using that data, I can prioritize and assign remediation tasks to my engineers based on the urgency of the issue."

Faster threat management. ASET recently rolled out GuardDuty to detect malicious activity in its AWS accounts and initiate automated responses and escalation to its security operations centers. GuardDuty continuously monitors AWS accounts and workloads while delivering detailed security findings.

GuardDuty combines machine learning, anomaly detection, network monitoring, and malicious file discovery, using both AWS-developed and third-party sources to help protect workloads and data on AWS. GuardDuty can be integrated with CloudWatch Events to automate responses to findings.

"We've just started working with our assigned AWS architect on putting GuardDuty across all accounts," Wheaton says. "He's helping us understand how to best use GuardDuty and implement AWS best practices for it. For agencies that need highly specific, detailed information for different types of environments, the sessions with an architect will help them configure the tool."

Encryption key management. ASET uses AWS KMS and AWS CloudHSM to manage encrypted keys and perform other tasks related to key management. CloudHSM lets ASET and other state agencies manage and access keys on Federal Information Processing Standards (FIPS) validated software. AWS KMS allows these entities to create, manage, and control cryptographic keys across applications and AWS services.

AWS KMS also automates routine tasks such as key rotation to alleviate staff management burdens and enforce best practices and policies.

"Making sure everyone is rotating their keys is very important to us," Wheaton says. "Key rotation is a challenge for a lot of the agencies. They put the key in and forget it. We want them to stay on top of rotations by automating rotations."

Why a cloud partner?

Migrating efficiently, knowing how to utilize cloud-native security tools, and filling in skills gaps can be a challenge for state and local governments starting their cloud journeys. Wheaton stresses the importance of working with a partner like AWS.

"You should lean on the cloud expertise of providers before moving any workloads to the cloud," Wheaton advises. "Our cloud partners brought a vast amount of knowledge and skills to the table when we started our cloud journey conversations and provided excellent guidance in building out our statewide strategies."

He says cloud providers help agencies reduce risk and simplify life for IT staff as they move workloads to the cloud. They also help agencies see what's possible.

"The leading cloud providers all offer best practice guides for architecting and designing resilient and secure environments in which to build and deploy your solutions," he says. "Take advantage of all partner-sponsored immersion day training to strengthen your IT and business teams' understanding of cloud technologies and shared security models."

This piece was written and produced by the Government Technology Content Studio, with information and input from AWS.

1. https://webinars.govtech.com/Best-Practices-in-the-Cloud-from-Arizona--140961.html

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.govtech.com**

Sponsored by: aws

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation across the globe. With AWS, you only pay for what you use, with no up-front physical infrastructure expenses or long-term commitments. Public Sector organizations of all sizes use AWS to build applications, host websites, harness big data, store information, conduct research, improve online access for citizens, and more. AWS has dedicated teams focused on helping our customers pave the way for innovation and, ultimately, make the world a better place through technology. To learn more about AWS in the public sector, visit us at **aws.amazon.com/stateandlocal.**

IMAGE: ADOBESTOCK/PHOENIX ARIZONA CITY OVERLOOK