A New Approach to Security in a Cloud-Based World

How Identity-Centric Security Can Help Agencies Protect Critical Data and Applications

The cloud gives government agencies the ability to quickly stand up new applications and has been a key enabler of digital services during the pandemic. In addition, the flexibility of the cloud consumption model provides capacity on demand so organizations don't waste scarce budget dollars.

However, when migrating critical workloads to the cloud, agencies must not overlook the need to ensure secure, compliant and efficient access to this infrastructure. Specifically, they need to create an identity-centric security approach that can help them protect critical data and applications.

This approach involves knowing which users have access to which platforms and with what privileges. To help make this possible, agencies can leverage artificial intelligence (AI) and machine learning (ML) technologies to model and define access policies, automate the provisioning and monitoring of cloud access to receive alerts of any suspect behavior, and implement governance for compliance and audit requirements.

Identity-Centric Security: What It Is and Why It's Important Now

As government agencies deploy and maintain more digital services and cloud-based applications, the need to implement identity-focused security becomes increasingly important.

Identity-centric security can minimize the risks associated with providing access to a diverse and dispersed workforce, by enabling the management and governance of access for every digital identity within an organization. It emphasizes security as well as enablement, providing users with the access they need but properly controlling that access.

Commonly known identity tools such as single sign-on and multi-factor authentication are only part of an identity security strategy. With identity security, access "is something that's based upon attributes of that user: their role, their location, their department, whatever it may be," said Cullen Landrum, senior systems engineer at SailPoint, during a recent *Government Technology* webinar focused on the topic.

Leveraging AI and ML

Agencies can take advantage of the latest AI and ML capabilities to enhance identity security. These technologies enable identity to be autonomous. By using them as part of the analytics process, agencies can proactively identify risky users and determine which access rights might pose threats to the organization's security.

Change is a constant with security. Since AI learns and adapts with changes, agencies can ensure all users have the appropriate access they need, when they need it. AI capabilities such as access modeling allow agencies to analyze identity information to gain insights about their identity program and act if something needs to be changed.

Automating Provisioning and Monitoring of Services

Automating some of the processes associated with identity security can save time and expenses as well as improve the accuracy of findings. Among the key benefits of technologies such as AI and ML is that they can help agencies automate the creation of new roles that align with their changing goals and use recommendations to help them decide whether to grant or remove access for particular users.

Given the large volume of identity-related data, the ability to automate the process of determining access rights using AI and ML is vital for government entities, Landrum says.

With the threat landscape changing so quickly and identity attributes frequently shifting because of changes in responsibilities, for example, the ability to automate identity security processes is invaluable.

Enhancing Governance to Improve Compliance

Good governance is a key component of identity-centric security, particularly from the standpoint of standards compliance and auditing.

Governance ensures agencies are taking the right steps with regard to things like provisioning access rights to users, onboarding new hires, addressing changing job roles and responsibilities, and revoking access once someone leaves the organization.

"A critical aspect of compliance is revoking access when someone leaves an organization," Landrum said. "Nobody ever calls up three months after leaving to ask if their access has been removed."

Cloud service providers design their offerings to enable customers to implement identity governance.

"We have identity and access management services that let you create rules and assign them permissions, and these rules can be defined for individual users," Pradeep Singh, solutions architect at Amazon Web Services, said at the webinar.

"Once you define the policies, then you need to manage them on a constant basis," Singh said. He pointed out that security needs to be a shared responsibility between the cloud provider and the customer.

Leading cloud providers address FedRAMP security controls, such as the National Institute of Security Standards (NIST) framework, so agencies can ensure NIST compliance. Providers may also offer automated auditing reports that significantly reduce the time it takes to complete audits for security and compliance.

Conclusion: Identity at the Center of Security

Government agencies are under growing pressure to improve cybersecurity. A recent White House executive order issued in May 2021 specifically focused on boosting the nation's security. "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy," it stated. "The federal government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors."

A strong identity security solution can help agencies enable users to have the access they need while at the same time securing critical data and systems. This includes securing hybrid and cloud environments, remote work, multiple devices and more. Agencies have found that identity security provides multiple layers of value such as reducing risk, automating IT processes and enhancing the employee experience.

Identity security achieves these results by properly provisioning access, protecting infrastructures at scale and ensuring compliance. As they continue to move further into the cloud to deliver services more efficiently to the public, an identity-centric approach can help agencies step up their efforts to ensure the safety of information.

View the webinar, "How Identity Governance Can Help Governments Reduce Their Cloud Attack Surface," for more information about this critical topic.

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

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:

SailPoint

SailPoint is the leader in identity security for the modern enterprise. Harnessing the power of AI and machine learning, SailPoint automates the management and control of access, delivering only the required access to the right identities and technology resources at the right time. Our sophisticated identity platform seamlessly integrates with existing systems and workflows, providing the singular view into all identities and their access. We meet customers where they are with an intelligent identity solution that matches the scale, velocity and environmental needs of the modern enterprise. SailPoint empowers the most complex enterprises worldwide to build a security foundation grounded in identity security. www.sailpoint.com/fed

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. Contact us to learn how AWS can help you with your biggest IT challenges. aws.amazon.com/stateandlocal/digital-government

IMAGE PROVIDED BY SHUTTERSTOCK.COM