A GOVERNMENT TECHNOLOGY Q&A

government technology

CYBERSECURITY RESILIENCE

MAINTAINING CLOUD CONFIDENCE WITH BUILT-IN CLOUD SECURITY

In this Q&A, Jackson Thomas, Senior Director at Oracle Government and Education, discusses how state and local governments can take advantage of their migration to cloud infrastructure to also reset and strengthen cybersecurity.

How has the cybersecurity landscape changed over the last 12 to 18 months?

With state and local agencies expanding their network perimeter to cloud, more infrastructure, applications and data are exposed to attack, especially because of remote work habits and public-facing digital services. There has also been an uptick in ransomware attacks on cities and schools. For example, we've seen cybercriminals infiltrate agency networks with phishing attacks that target remote workers with administrative access privileges. The employee opens a phishing email on his or her private email account and inadvertently downloads malware such as a key logging bot that captures the password to the employee's administrative account. Once criminals gain administrative privileges, they can do almost anything, including accessing other agencies, bringing down the entire system or demanding ransom. Cryptocurrency transactions have made it even easier for criminals to hide and extort payments.

How does the evolution of infrastructure from on-premises to cloud-first change the cybersecurity conversation?

In effect, moving workloads to the cloud becomes more than just a business enabler. It is also an opportunity for organizations to reset their approach to cybersecurity. State-of-the-art cloud infrastructure includes a breadth of built-in controls to address cybersecurity issues. Features like Zero Trust architecture, principles of least privilege, encryption and network segmentation can be adopted by default and are huge steps to prevent exploitation by cybercriminals. The cloud also facilitates adoption of newer cybersecurity capabilities around artificial intelligence (AI), machine learning (ML) and blockchain, fostering a new category of security solutions called User and Event Behavioral Analytics (UEBA) as defined by Gartner.

How does a "data to edge" cloud security approach strengthen cybersecurity and business resilience?

As agencies move more functions to the cloud, cloud service providers also bear responsibility from a security perspective. However, every organization needs to understand the shared security responsibility matrix and its own responsibilities within it. Organizations need to embed security at very early stages of the software development life cycle — what's called the "shifting left" mindset. In addition, an organization's security is only as strong as its weakest link and that weakest link can be anywhere or anybody in the chain. So, the idea is to adopt a comprehensive "data to edge" cloud security solution. This end-to-end, security by design approach entails building in security at each layer of the stack — from network and infrastructure to applications and data. Not every cloud service provider offers security at the stack layer level.

What foundational cybersecurity tactics enable state and local government organizations to more confidently leverage cloud infrastructure?

Organizations need the right foundational elements regardless of their deployment model. That includes adopting a Zero Trust security model, providing different access controls, using multifactor authentication, and encrypting data in transit and at rest. Second, cloud infrastructure should leverage technologies such as AI and ML to perform UEBA analysis, automatically filter through the noise of traditional security incident and event management (SIEM) alerts, and address other cybersecurity challenges more quickly and efficiently. In multi-tenant environments, network segmentation and tenant isolation capabilities are extremely important. Many of these capabilities come default with advanced cloud infrastructure solutions. Finally, cloud infrastructure should have verified compliance with key government regulations such as HIPAA, CJIS, PCI, FedRAMP and others.

Learn more about security best practices at: www.oracle.com/security

ORACLE

Oracle offers suites of integrated applications plus secure, autonomous infrastructure in the Oracle Cloud. For more information about Oracle (NYSE: ORCL), please visit us at **oracle.com**.

IMAGE PROVIDED BY SHUTTERSTOCK.COM