Taking Cloud Security to the Next Level

MICROSOFT

The evolving cloud security landscape

Emerging tools such as zero trust and artificial intelligence help agencies stay ahead of threats to cloud environments

As cloud adoption grows and security threats multiply, holistic security across clouds and between clouds and on-premises systems has become a key concern for agencies. Fortunately, security tools and techniques are evolving as well.

A zero trust framework is one proven approach agencies can employ for better cloud security. Zero trust requires continuous verification and validation of identities, devices, data, applications and more. It allows agencies to enforce more granular security policies and prevent unauthorized access. If there is a breach, it blocks lateral movement within and across clouds or on-premises systems.

A second opportunity is the use of artificial intelligence and machine learning to tackle security challenges. AI and ML can help agencies automate threat detection and response while also automating anomaly detection in network activities and user behavior. With AI, agencies will be able to respond to ever-changing and sophisticated threats more quickly while optimizing security operations.

Agencies can take advantage of the security tools that are embedded in cloud platforms to create a cross-cloud, holistic approach to security.

At Microsoft, we’re excited about the promise of AI, which is why we are incorporating key AI-enabled features into the Security Copilot product we’re developing to help users stay ahead of cyberattackers.

In addition, agencies can take advantage of the security tools that are embedded in cloud platforms to create a cross-cloud, holistic approach to security. For example, many agencies use Microsoft Sentinel to conduct intelligent security analytics; Microsoft Defender for threat prevention, detection and response; and Azure Arc to simplify governance and management of multi-cloud environments.

Cloud-native development and continuous ATOs

The ability to develop and deploy secure applications is also important. Agencies have the most success when they think about development from a software-first perspective. That involves defining an outcome for an application or workload and working towards it through an automated infrastructure as code mentality, embracing continuous integration and deployment with a measurable DevOps pipeline. In addition, some agencies are integrating security more deeply into software development and deploying tools that enable them to continuously assess and monitor applications.

Another exciting development is the concept of a continuous authority to operate. Receiving an ATO has typically
been a paperwork exercise that is done at a specific point in time. By contrast, a continuous ATO involves assessing applications and cloud environments against controls on an ongoing basis so the agency's network operators, security operations center and application owners can constantly evaluate their security posture.

However, an ATO per release is no longer about version updates that span months or years; it's about two-week sprints. A new approach to risk management is required, one that involves using automation, continuous improvement and data-driven decisions to support risk identification and mitigation.

**Tracing decisions back to the data**

Where and how their data is stored are key considerations for government agencies, along with questions about encryption, access management, logging, monitoring and data auditing. All those concerns will increase in importance as we move toward a world in which AI-enabled systems help us make decisions. Security teams must understand why a system made a particular decision and be able to trace the decision back to the data. Therefore, storing data on a secure, transparent and trusted platform will be critically important.

The latest advances in multi-cloud, AI and zero trust are based on data — where it's located, who has access rights to it and what insights can be derived from it. As a result, the basic principles of good data governance and data cataloging remain important. By adhering to those principles and adopting proven security practices, agencies can maximize the benefits of cloud technology.

Jason Payne is CTO at Microsoft Federal.