Best Practices for Cloud Development Security

Cloud-native development is on the rise. The global number of cloud-native developers grew to nearly 7 million last year. Based on Techstrong Research's work with clients, we offer the following best practices that organizations can take to "shift left" and secure their cloud development pipelines.

TREAT SECURITY AS A TEAM SPORT.

Security needs to be involved with development projects at the earliest possible point. There are many software offerings to help with this process, but "shifting security left" requires a culture change as well. If you don't, you'll likely face one of two consequences: projects will slow to a crawl as required security measures are bolted on, or the schedule will be met at the expense of adequate security.

The shift from traditional structures to DevOps united development, operations and engineering teams. Now, the evolution to DevSecOps requires further expansion of the roster. It's crucial that security architects, engineers and other cybersecurity professionals are also involved in the cloud-native life cycle.

REDUCE COMPLEXITY AND VENDORS WITH A PLATFORM APPROACH.

DevSecOps integration and security automation are necessary components to achieving successful cloud adoption. It's obvious but bears repeating ; high cloud spend does not equate to successful cloud development or adoption. Rather, success with DevOps in a cloud-native environment hinges on moving from a tangled web of disjointed solutions to a comprehensive platform. Research shows clearly that consolidation of multiple security vendors leads to successful cloud adoption efforts. Integrated tools can help prevent changes that cause breaks and otherwise mitigate risk by overlaying vulnerabilities, misconfigurations, dependencies and networks, to name a few, into context.

USE SECURITY TOOLS AND TECHNOLOGY DESIGNED FOR CLOUD-NATIVE DEVELOPMENT

Building effective cloud-native applications requires making interconnected, interlocked decisions about architecture, development and operations. DevSecOps teams require purpose-built tools and platforms that enable external configuration, health and metrics monitoring, service registry and service discovery, dynamic scheduling, multi-cloud implementation and a host of other new practices. Similarly, DevSecOps in cloud-native environments needs the ability to scan container images to identify vulnerabilities, for example – something that conventional tools simply cannot do.

AUTOMATE SECURITY IN YOUR CLOUD-NATIVE ENVIRONMENT

Traditional security reviews break agile development methods and slow the business down. Centralized incident and event management systems look for anomalous data and processes to safeguard the company IT assets. Automation is available everywhere, from configuration management and patching tools to database integrity monitoring and insider threat detection. It's the only way to prevent unintended breaches from happening in the first place.

Automation is essential to complex distributed systems for rapid development and continuous improvement with frequent releases. As manual efforts are too slow and error-prone to guarantee that, robust automation for a cloud-native application helps keep the app well-tested, secure, reliable and scalable.

GAIN CLOUD VISIBILITY ACROSS VENDORS WITH UNIFIED MANAGEMENT

Visibility into all of your cloud-native workloads and data, regardless of vendor, is the only way to ensure that your environment is secure. You need a solution that can use your cloud providers' APIs to provide visibility and control. Not just over your overall cloud infrastructure, but more granular control over containers and serverless elements, as well. It's important to choose a solution that isn't tied to one vendor or cloud. While you might be using a single cloud today, you want to be prepared for multi-cloud when the time comes.

Techstrong Research

COMMISSIONED BY PRISMA CLOUD BY PALO ALTO NETWORKS