TIGERA

Microsoft

7 security best practices for DevOps managing containerized workloads in Microsoft AKS with Calico Cloud

Microsoft Azure Kubernetes Service **(**AKS**)** is a managed Kubernetes service that runs and scales Kubernetes applications in Microsoft Azure. AKS ensures a secure, scalable, and managed Kubernetes environment with security patches automatically applied to your cluster's control plane. However, containerized workloads running in AKS are still at risk for security threats and vulnerabilities in your Azure environment.

Securing workloads from build time to runtime in AKS

Security is a constantly evolving challenge, and it doesn't take long for threat actors to expose and exploit container vulnerabilities—or for compliance and access issues to arise. Hence, improving container security architecture and automation from the build phase to the eventual runtime in production has become a priority for security teams.

Denial-of-service (DDoS) attacks and kernel and orchestration exploits have plagued containers, threatening enterprise cloud assets, productivity, and innovation. AKS addresses potential Kubernetes OS issues through patches and leverages Calico Cloud for container security, runtime threat defense, and observability and troubleshooting features to handle new vulnerabilities and risks at the workload level.

The following are seven security best practices used by the DevOps team to manage containerized workloads in AKS using Calico Cloud.

1. Least privilege access with microsegmentation

Workload isolation can initially be frustrating to implement for DevOps engineers, but it's one of the most important security best practices for all software development teams to establish within their applications. Restricting software access reduces the potential blast radius associated with software errors or malware injected into the container. Containers, with their portable, read-only image, have a smaller footprint, but lack true sandboxing. If an attacker exploits any host OS vulnerability, all containers sharing the OS could be compromised.

We can achieve user-level isolation and access restrictions through identity and access management (IAM) permissions within Microsoft AKS, restrict ports and protocols on Azure resources by creating security groups, and even enforce Kubernetes role-based access control (RBAC) to restrict the service accounts that can modify networking and security policies, which control the traffic within your AKS clusters.

Calico Cloud with AKS allows organizations to enforce workload isolation to limit the blast radius associated with potential privilege escalation incidents. Regardless of the permissions assigned to the service accounts within the cluster, Calico's security policy framework can limit the traffic permitted between workloads based on a well-defined Kubernetes label schema—and then limit that traffic further based on approved ports and protocols between those identity-aware workloads.

2. Reduce attack surface with zero-trust architecture

Docker and Kubernetes offer faster container deployment, but a vulnerable orchestration layer expands the attack surface. Misconfigured Kubernetes, like over-provisioned privileged access, could open direct control over the container fleet to an attacker. Application breakdown or exposed internals can also significantly broaden the attack surface.

Calico Cloud with AKS enables you to go one step further by enforcing the concept of least privilege via security policies. By limiting workload communications to specific ports and protocols between approved workloads, you can prevent much broader attack surfaces. You can also limit the user's create, read, update, and delete (CRUD) permissions on objects within Kubernetes with Kubernetes RBAC. That way, you could assign a team manager read-only access to a policy without worrying about any possible misconfiguration from that manager.

3. Misconfigured containers

Another attack vector is compromised container credentials (e.g., API key or username/password), which invites an attacker to spoof the database and cloud services.

Calico Cloud with AKS protects containers during development and production, reducing the attack surface with vulnerability and misconfiguration detection. With image assurance and configuration assessment based on standardized benchmarks such as CIS, you can detect misconfigured Kubernetes environments and address the gaps with recommended actions provided in Calico Cloud.

4. Strengthening security with rule-based controls

Rapidly changing container infrastructure rules and signature-based controls don't align well with static regulatory compliance requirements. Securing a dynamic container infrastructure using traditional network and endpoint controls won't work.

Calico Cloud, unlike traditional firewall technologies, has identity-awareness of application workloads running within a Kubernetes cluster. While traditional security tools worked better with legacy VMs with fixed IP addresses, to secure your AKS clusters, you need Kubernetes-native context about objects, such as label selectors and services. Conventionally, endpoint security teams target endpoints (mainly VM's/servers) by IP address. Calico's security policies allow organizations to target workloads based on a fixed label schema, which works consistently in highly distributed environments.

5. Automatic detection and blocking of vulnerable container images

Containers use images stored in publicly available repositories like GitHub, with dependencies on other images and libraries. Source code vulnerability can easily spread to thousands of other containers. A clever attacker can also run their malicious images, compromising host data.

Microsoft AKS integrates with Microsoft Azure Container Registry (ACR)—a managed Azure service that provides users the ability to push their software packed in containers into a Microsoft-managed registry. Unlike self-managed registries, users can benefit from this service model to speed-up delivery and avoid the worry associated with installing or scaling infrastructure to accommodate this workflow. Users within AKS can then pull down images over HTTPS protocol with the convenience of automatic encryption and access control. The obvious advantage here is if an organization uses a public registry to source its images, there's a very real possibility that those images are carrying some form of a vulnerability. With ACR, the access control of the registry is controlled by the IAM service. This means you can configure specific users or VM instances to access ACR, and restrict unwanted users or instances from pulling/modifying images in the registry.

Calico Cloud protects containerized workloads during build and runtime with a CLI-based image scanner, which can be integrated into your CI/CD pipeline. It assesses and mitigates risk associated with container image vulnerabilities for cloud-native workloads by continuously scanning for vulnerabilities and misconfigurations before they are deployed to AKS clusters, and automatically blocks deployments that fail to meet security requirements. It quickly assesses the risk of deployed applications when new vulnerabilities are discovered by providing a runtime view in Dynamic Service and Threat Graph. For runtime threats that manage to evade image scanning workflow or ones which are discovered during runtime, Calico Cloud also provides an extensive networking and security policy framework to identify and mitigate threats from workflows attempting to establish unusual connections within or outside of the AKS cluster—completing the end-to-end zero-trust initiative.

6. Keeping up with new attack vectors

Kubernetes pods running containers use unique IP addresses for connectivity. Attackers can exploit these IP addresses as gateways to launch attacks either internally or from external networks.

Regardless of whether the threat is known or unknown (zero-day incident), Calico Cloud allows organizations to monitor and troubleshoot security issues in real time. Users can use Calico's GlobalThreatFeeds to visualize and enforce restrictions against known bad IP sets associated with malware, ransomware, or botnet feeds. In case of a breach or vulnerability, users get instant granular information on compromised services and can evaluate and contain the blast radius via the following Calico features:

- Dynamic Service and Threat Graph
- Performance Hotspot Visualization
- Dynamic Packet Capture for workloads and namespaces
- Intrusion detection and prevention (IDS/IPS) to detect and mitigate advanced persistent threats (APTs)
- Workload-centric WAF

7. Adhering to regulatory compliance frameworks

Most enterprises are subject to corporate and/or regulatory compliance requirements. From an operational perspective, this may involve isolating workloads containing sensitive data, or restricting who can access specific resources. There may also be requirements to implement access control frameworks such as security zones (e.g., trusted, untrusted, and DMZ). Even more advanced controls are sometimes needed, like building a moat around PCI-DSS workloads or logging all HIPAA data transactions.

Auditors also need proof that you are enforcing these controls, but capturing the information required to show proof can be challenging, especially in a dynamic, distributed Kubernetes environment where workloads are ephemeral. Auditors will want to know what security controls are currently implemented, whether control changes be detected, and if compliance can be verified at any given day and time.

Calico Cloud provides controls and capabilities to fulfill auditing requirements and continuously monitor your cloud-native environment for compliance, and can retain a daily history of your compliance status. Calico also includes predefined compliance report formats, as well as a resource for creating customized reports.

Conclusion

Enforcing containerized workload security in Microsoft Azure and AKS is critical. Security and compliance are considered shared responsibilities when using a managed service like AKS. The cloud provider provides the security of the cloud platform, and the users on the platform build security within the cloud for their workloads. Calico and AKS together provide complete security for cloud-native applications using containerized workloads and Microsoft Azure. As an Azure user, you benefit from the ease of cluster deployment with a managed Kubernetes service while also having the option of benefitting from managed IAM and registry services that scale to meet the security requirements of the organization. Tigera provides additional security features to reduce the attack surface, and can detect known and unknown threats with automated mitigation of security threats and vulnerabilities with your build, deploy, and runtime. Try Calico Cloud for free today via the **Azure Marketplace**.