aqua

The Cloud Native Security Checklist

Key Concepts and Principles

With the move to cloud native development, organizations are now continuously deploying ephemeral workloads across multiple diverse environments, dynamically orchestrating them with Kubernetes. To efficiently protect this new stack, you need to apply security across every stage of the application lifecycle. What are the critical elements of a successful cloud native security strategy and what capabilities do you need to securely build and run cloud native applications?

Build

“Shift Left” with automated scanning

Embedding security as early as possible into the SDLC is key to securing cloud native applications right from the start. “Shift left” and integrate security tools into the CI/CD pipeline to find and remediate vulnerabilities and other risks as the code is created.

□ Detect vulnerabilities in open source components

□ Scan multiple languages and binaries, including C++, PHP, NodeJS, Golang, .NET, Java, & Python

□ Automatically scan Linux and Windows hosts for OS vulnerabilities, malware, and login attempts

□ Scan artifacts for embedded secrets, OSS licensing issues, hidden malware, configuration issues, & sensitive data

Risk-based vulnerability management

To effectively manage your vulnerability posture, you need to prioritize CVEs based on their actual impact on your environment. A risk-based approach considers contextual factors, with recommended prioritization for remediation and mitigation of vulnerabilities.

- □ Prioritize vulnerabilities based on actual risk to the environment (e.g., exploitable workloads)
- □ Provide the capability to remediate, mitigate, or acknowledge the vulnerability upon discovery
- □ Automatically mitigate vulnerabilities with surgical policies that can prevent exploits in runtime in a non-intrusive way

Protect against supply chain attacks

Malicious actors are increasingly looking to infect the software supply chain with malware to carry out sophisticated attacks that evade traditional application security testing. To detect such hidden malware in your CI/CD pipeline, you need to run images in a secure sandbox before production.

- □ Control access to public registries and open source components
- □ Scan images using dynamic threat analysis tools like Aqua DTA
- □ Monitor runtime environment to detect any behavioral anomalies inside the container while it's running

Implement assurance policies

Assurance policies act as a compliance gate between development & production, only allowing images or workloads that adhere to security & compliance requirements to be deployed.

- □ Prevent unapproved images from running in your environment
- □ Create flexible rules based on the security needs of different applications
- □ Enable multiple image assurance policy settings (per image name, label, registry) for effective mitigation

Kubernetes assurance policies

- □ Block Kubernetes workloads that don't meet assurance policies based on pod or node configuration
- □ Apply out-of-the-box best practice rules for secure Kubernetes configurations

Infrastructure

Cloud account security

With cloud adoption accelerating at a rapid pace, enterprises are overwhelmed by the sheer number of cloud configurations. To ensure a secure and compliant cloud infrastructure, you need to automatically detect, assess, and remediate misconfigurations across all your cloud accounts.

□ Implement a Cloud Security Posture Management (CSPM) solution and gain visibility into hundreds of configurations across multiple services and multiple clouds

□ Detect configuration issues in popular IaC solutions (e.g., Terraform, AWS CloudFormation)

□ Set up auto-remediation to fix the biggest issues quickly via a RESTful API

Kubernetes security

To identify and remediate risks in the Kubernetes environment, you need to automate K8s security configuration and compliance with policies across namespaces, nodes, containers, and network connections.

□ Gain continuous visibility into the Kubernetes environment and get clear visibility on any policy violations

□ Conduct automatic penetration tests of your Kubernetes clusters against a variety of attack vectors

□ Assess the Kubernetes environment according to the CIS Kubernetes Benchmark, and provide daily scans and a detailed report with the findings

Workloads

Runtime protection

Runtime protection should secure cloud native workloads across a mixed environment of VMs, containers, and functions, with purpose-built controls for each.

- □ Enforce immutability of container workloads, detecting and preventing changes to containers against their originating images
- □ Apply virtual patching as a compensating control that prevents the exploitation of specific CVEs, e.g., when there's no fix available
- □ Alert on suspicious host activities, such as brute force login attacks

Identity-based segmentation

To prevent lateral movement of attackers in the cloud native environment, you need to divide workloads into logical segments based on service or application identity and apply authentication and least privilege access between each of them.

- □ Automatically discover and visualize the workload attack surface, relationships between namespaces, deployments, pods, and network traffic
- □ Detect and prevent unauthorized network connections based on automated policies
- □ Define zero-trust network connections based on service-oriented firewall rules, regardless of where the workload runs

Conclusion

Developing an efficient security strategy for cloud native applications should focus on integrating security into the fabric of the cloud native environment, from CI/CD pipelines to Kubernetes and public cloud infrastructure. Holistic cloud native security embeds security early in the development cycle and seamlessly bakes it in all the way into production, protecting the build, infrastructure, and workloads.

Cloud Native Security Maturity Assessment

Take the 5-minute questionnaire ›

Aqua Security is the largest pure-play cloud native security company, providing customers the freedom to innovate and run their businesses with minimal friction. The Aqua Cloud Native Security Platform provides prevention, detection, and response automation across the entire application lifecycle to secure the build, secure cloud infrastructure and secure running workloads wherever they are deployed. Aqua customers are among the world's largest enterprises in financial services, software, media, manufacturing and retail, with implementations across a broad range of cloud providers and modern technology stacks spanning containers, serverless functions, and cloud VMs.