SOLUTION OVERVIEW

AQUA SECURITY FOR VMWARE ENTERPRISE PKS

Secure Cloud Native Workloads with a Comprehensive Approach

Kubernetes has quickly risen in popularity to become the leading container orchestration technology. Building and operating an enterprise-grade Kubernetes service, however, is a complex undertaking that requires astute architects and experienced operators who can implement container networks, lifecycle management, and cloud native security.

VMware® Enterprise PKS helps you overcome these challenges by providing an enterprise-grade Kubernetes platform that radically reduces the complexity of container networking, multitenancy, and lifecycle management. Aqua works with VMware Enterprise PKS to add comprehensive security for container workloads.

VMware Enterprise PKS includes advanced networking from VMware NSX® Data Center and a secure image registry named Harbor. NSX provides micro-segmentation, load balancing, and network security policies. Harbor secures container images with vulnerability scanning, image signing, and role-based access control.

The solution simplifies the deployment and operation of Kubernetes clusters so you can orchestrate containers at scale on VMware vSphere®, Google Cloud, Amazon Web Services, or Microsoft Azure. Supporting products and services can be added for logging, monitoring, visibility, and additional security.

How Aqua Secures Workloads on VMware Enterprise PKS

Aqua provides a comprehensive container security platform for VMware Enterprise PKS. Aqua's Cloud Native Security Platform (CSP) adds a layer of robust security that delivers multifaceted image assurance, runtime controls, and protection against attacks. The Aqua platform gives you visibility into the containerized applications that run on VMware Enterprise PKS to help ensure compliance with regulations.

Securing Applications from Development to Production with Aqua’s Cloud Native Security Platform

By using a modern zero-touch approach to detect and prevent threats while simplifying compliance, Aqua provides granular visibility and security automation across the entire application lifecycle, including the build and runtime stages.

Secure Your Development Pipeline in the Build Stage

Scan your images for known security issues and evaluate the scan findings by using Image Assurance policies that you define and configure. Using Aqua’s Image Assurance capabilities, you can determine whether your container images are compliant. Through Aqua’s integration with CI/CD technologies, you can fail builds of container images that are above a certain risk threshold. You can also review the results of your security evaluations in the Aqua CSP console or export the results of the scans to your preferred SIEM solution.

AQUA SECURITY FOR VMWARE ENTERPRISE PKS

Bringing together best-of-breed technologies and capabilities to create a functional and secure container management solution, VMware and Aqua Security provide the services that enterprises need to effectively manage Kubernetes at scale.

The combination of VMware Enterprise PKS and Aqua’s Cloud Native Security Platform eliminates concerns about developing, deploying, and managing container workloads securely. The result is a comprehensive and flexible approach to securely evolving your enterprise cloud strategy.

AUTOMATE SECURITY IN YOUR ENTERPRISE WITH AQUA

Aqua's security platform can help you automate security in your enterprise by delivering the following capabilities:

- **Continuous Image Assurance:** Integrate with a CI/CD pipeline to automate security testing in the pipeline, and with Jira for developer feedback. Scan container images for known vulnerabilities, malware and sensitive data, based on a continuous feed correlated across multiple sources.
- **Automatic Vulnerability Mitigation:** Aqua's vShield is a virtual patching mechanism that can detect and prevent the exploitation of a known vulnerability in a runtime without the need for human intervention.
- **Runtime Protection:** Customized runtime policies will put intended container activity on a whitelist to prevent changes in running containers compared to the original image, and granularly block suspicious executables or escalations.
- **Secrets Management:** Securely inject, rotate and revoke secrets in running containers without stopping or terminating the container, ensuring application uptime.
- **Microservices Firewall:** Visualize container networking and apply container firewalls based on pod names, namespaces, IP addresses, and DNS.
- **Auditing and Compliance:** Automate CIS benchmarking and predefined runtime policies for regulatory compliance. Maintain granular event logging and generate reports of container activity and policy changes.

LEARN MORE ABOUT AQUA

If you'd like to learn more about how you can secure your cloud native workloads, please contact Aqua at contact@aquasec.com, or visit our website at www.aquasec.com

Find out more about Aqua's Cloud Native Security Platform for VMware Enterprise PKS by visiting the VMware Solution Exchange.

LEARN MORE ABOUT VMWARE ENTERPRISE PKS

To learn about how VMware can help you deploy, manage, and secure cloud native applications on VMware Enterprise PKS, visit: cloud.vmware.com.

Protect Your Container Workloads During Runtime

By deploying the Aqua Enforcer to protect your workloads in runtime, you can configure runtime policies to restrict container activity based on images that have been found to be non-compliant during Image Assurance. To ensure application uptime, you can block anomalous activity such as blacklisted executables or privileged escalations without having to terminate the container. Aqua can also apply predefined compliance checks to ensure you meet regulatory standards, such as the EU General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI), and HIPAA.

In order to ensure you have full visibility of your container environment, Aqua provides granular audit trails of access activity, scan events and coverage, Docker commands, container activity, and secrets activity and system events. Aqua aggregates these data streams to send them to your SIEM tool of choice.

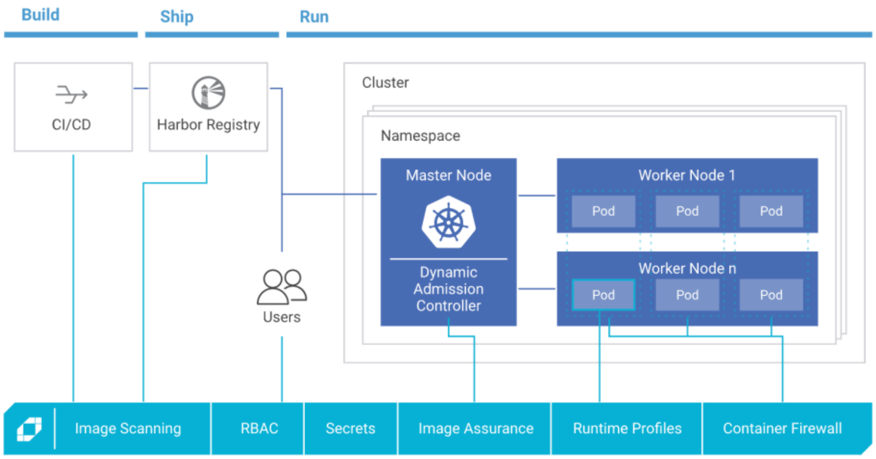

Figure 1: Aqua Security on VMware Enterprise PKS.

PARTNER READY
VMWARE PKS

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com