aqua

Solution Sheet

Pivotal NETWORK

Aqua Security for Pivotal is available to download as a tile from the Pivotal Network

Aqua Security for Pivotal Platform
Full Lifecycle Security for Pivotal Application Service (PAS)

Pivotal Platform enables developers and operators to iterate rapidly, help expand and launch new businesses fast, as well as deliver extraordinary user experiences to their customers. This new way of deploying and running applications requires a comprehensive approach to security.

Aqua provides a natively-deployed, full lifecycle solution for Pivotal Application Service workloads, from scanning to assurance policies and runtime controls that include both behavioral and network security enforcement. Since Aqua also natively support Kubernetes (including Pivotal Container Service - PKS), it is the optimal solution for securing applications across both PAS and K8s, as well as securely migrating applications from one to the other.

Scan apps in CI
for vulnerabilities, secrets, malware and configuration issues

Secure the Blobstore
to identify risks in apps and prevent them from being deployed

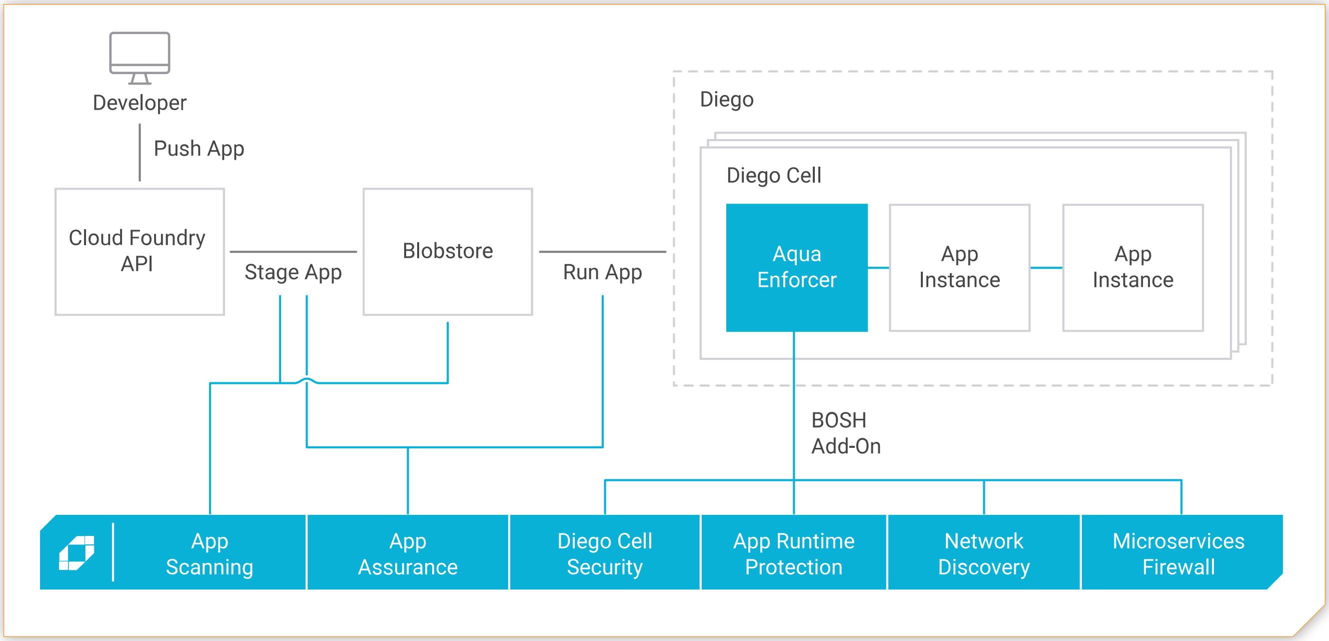
Detect and block
configuration drift and suspicious activity in apps during runtime

Protect Diego cells
and continuously assess their compliance and security posture

Discover and map
network connections and automatically create firewall policies

Gain visibility and control
Unified across your PAS and Kubernetes-based environments

Solution Sheet



Vulnerability Scanning and Droplets Assurance

Scan Droplets in CI and the Blobstore for vulnerabilities across multiple language packages, sensitive data such as private keys, and malware

Provide developers with actionable remediation advice for fixing security issues

Block non-compliant applications from being staged, or acknowledge vulnerabilities with a grace period for fixing them

PAS Runtime Protection

Automatically profile application behavior and whitelist capabilities and executables

Prevent drift by blocking executables that were not in the original application

Collect forensic data on processes, command arguments, and network activity

Mitigate threats including port scanning, fork bombs, and connections to suspicious IP addresses

Network Discovery and Firewall

Automatically discover network connections within and across applications

Implement micro-segmentation to limit an intruder's "blast radius"

Apply firewall rules based on IP address, application service identity, or DNS URLs

Alert on or block non-whitelisted connections

Diego Cell Security and Compliance

Scan Diego cells for known vulnerabilities, sensitive data such as private keys, and malware

Evaluate Diego cells for compliance against the CIS Linux Benchmark configuration best practices,

Monitor Diego cell admin user access and behavior

Apply File Integrity Monitoring to ensure no tampering with the file system

Aqua csp v.4.5

contact@aquasec.com
www.aquasec.com
@AquaSecTeam
AquaSecTeam