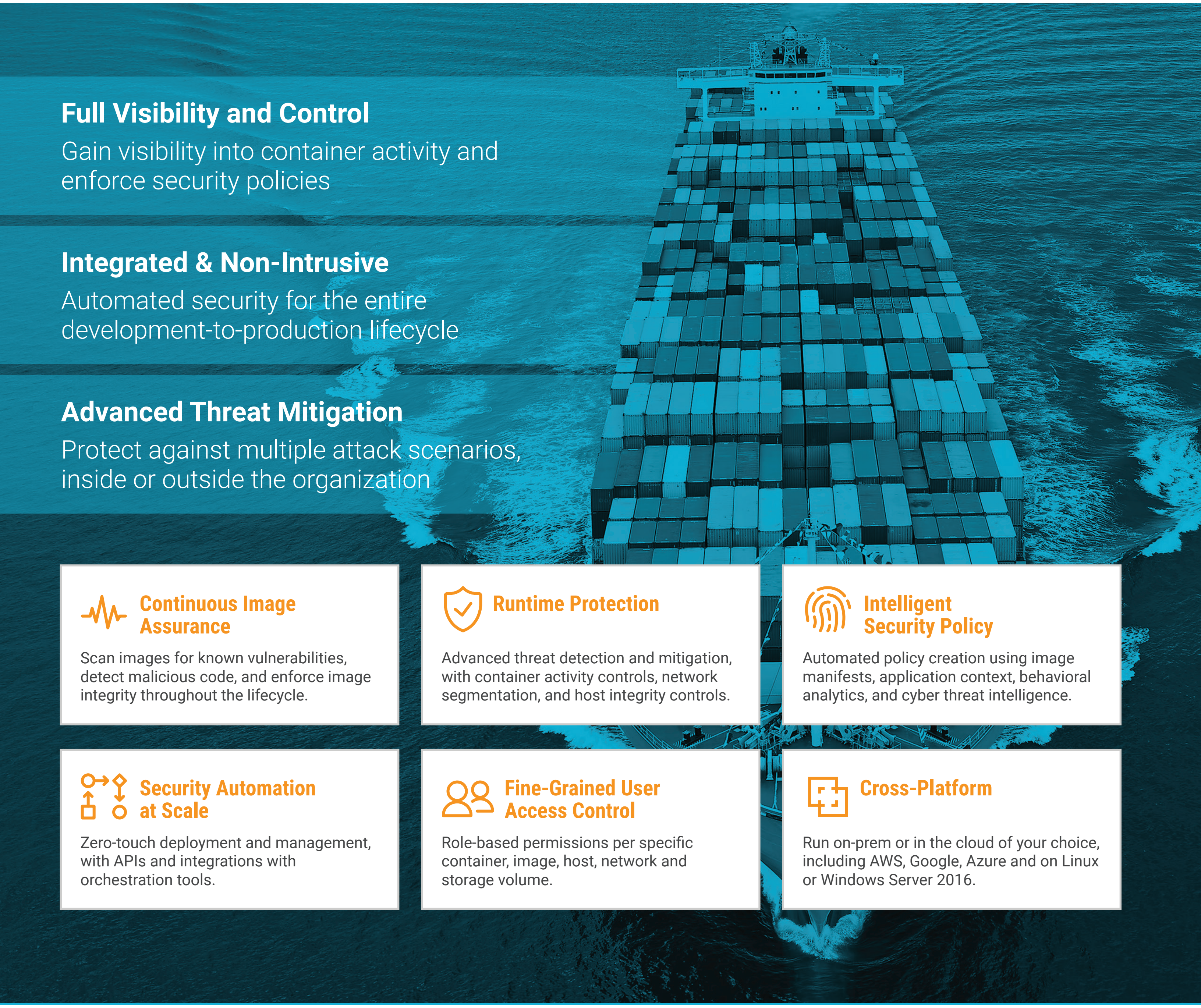
aqua

Solution Sheet

The Comprehensive Security Platform for Container Environments

Software containers represent unique security challenges, due to the scale, agility and open nature of container environments. Aqua's platform is **natively architected for containers**, providing IT security with **full visibility and control** over container activity across the lifecycle, while remaining transparent and unintrusive to DevOps.



Full Visibility and Control

Gain visibility into container activity and enforce security policies

Integrated & Non-Intrusive

Automated security for the entire development-to-production lifecycle

Advanced Threat Mitigation

Protect against multiple attack scenarios, inside or outside the organization

Continuous Image Assurance

Scan images for known vulnerabilities, detect malicious code, and enforce image integrity throughout the lifecycle.

Runtime Protection

Advanced threat detection and mitigation, with container activity controls, network segmentation, and host integrity controls.

Intelligent Security Policy

Automated policy creation using image manifests, application context, behavioral analytics, and cyber threat intelligence.

Security Automation at Scale

Zero-touch deployment and management, with APIs and integrations with orchestration tools.

Fine-Grained User Access Control

Role-based permissions per specific container, image, host, network and storage volume.

Cross-Platform

Run on-prem or in the cloud of your choice, including AWS, Google, Azure and on Linux or Windows Server 2016.

www.aquasec.com

aqua

Solution Sheet

The End-to-End Platform for Container Security

Continuous Image Assurance

- Scan for known vulnerabilities, based on a continuously updated feed based on multiple sources
- Scans OS packages (RPM and Deb) and language packages: Java, NodeJS, Ruby, PHP, Python, C/C++
- Integrates with CI/CD to automate security testing in the pipeline, and with Jira for developer feedback
- Automated scanning in private registries upon image push

Intelligent Security Policies

- Image fingerprinting for integrity assurance across the pipeline
- Lock down and prevent unauthorized images from running
- Automatically create security profile based on runtime parameters
- Disable unneeded executables, network connections, ports and file paths
- Out-of-the-box profiles for popular Docker images

User Access Control

- Role-based privilege definition per container/host/application/network/storage volume
- Allow/disallow specific user actions, e.g. start/stop, log access, read/write access, volume access

Secrets Management

- Manage secrets securely and inject into containers as needed
- Integrates with HashiCorp Vault

Network Nano-Segmentation

- Map containers onto applications
- Network nano-segmentation between containers based on their applications
- Detect and prevent malicious container network activity

Runtime Protection

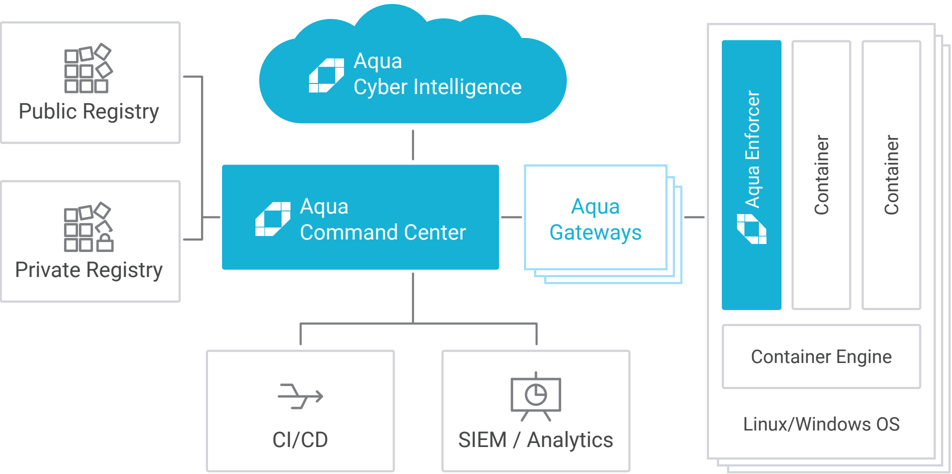
- Real-time monitoring of container activity against security policies
- Isolation prevents a container from accessing resources on another container or host
- Block bad reputation IP addresses
- Central event logging and full audit trail

Integrations

- Orchestration: Kubernetes, Docker Swarm, Mesos, Amazon ECS
- CI/CD tools: JFrog, Jenkins, CodeFresh, GoCD, TeamCity, Microsoft VSTS
- SIEM, Analytics and Alerts: Sumologic, Syslog, ArcSight, Loggly, Logentries, Microsoft OMS, ElasticSearch, Slack, PagerDuty
- Identity Mgmt: Active Directory / LDAP, SAML Single Sign-On
- REST API and webhooks for other integrations

Supported Environments

- Container format: Docker 1.10 or newer, Windows containers
- Registries: DockerHub, Amazon ECR, Google GCR, CoreOS Quay, JFrog Artifactory, Azure ACR or any v1/v2 registries
- On-Prem Deployment: Major Linux distributions including CentOS, Ubuntu, CoreOs, RedHat and Windows Server 2016
- Cloud Deployment: AWS, Google Cloud, Microsoft Azure



About Aqua

Aqua enables enterprises to secure their virtual container environments from development to production, accelerating container adoption and bridging the gap between DevOps and IT security.

Aqua is privately held, founded and backed by IT security veterans, and is based in Israel and San Francisco, CA.

Contact

contact@aquasec.com

www.aquasec.com

@aquasecteam

linkedin.com/company/aquasecteam

US HQ:
201 Spear Street, Suite 1100,
San Francisco, CA 94105

Intl. HQ:
20 Menachem Begin Rd.,
Ramat Gan, Israel 52700