Securely build, deploy and iterate apps everywhere with IBM Container Security Services

Highlights

- Cloud and app modernization is increasing container adoption
- Despite high adoption rate, containers are a major security concern
- Containers introduce new threat vectors
- Image, registry, orchestration, container and host are major risk areas
- Our services are designed to help secure full app container lifecycle
- Consulting and integration services for design and implementation
- Fully-managed container security services for steady state
- Automated vulnerability ranking to prioritize remediation services
- Threat management services to proactively monitor and respond to threats
- Safeguards app development by bringing Security and DevOps together

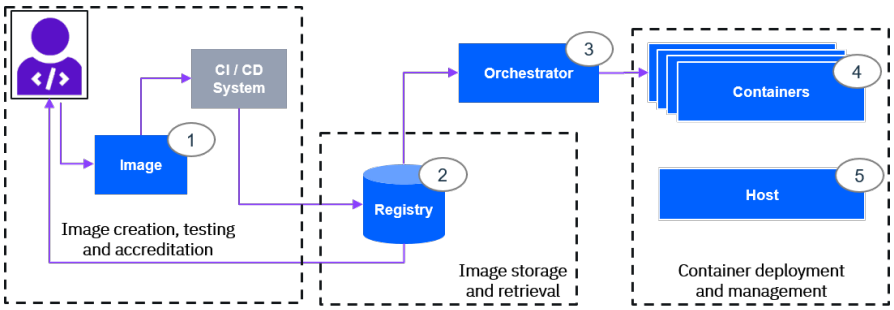
Application Containers introduce new threat vectors

Application modernization and migration to cloud is significantly increasing container adoption. Despite the high adoption rate, container security continues to be a concern for IT Professionals. Containers introduce a new set of threat vectors that require specialized security in the following key risk areas: Image, registry, orchestration, containers and host. But implementing and managing container security can be complex. Deployment speed and the short life span of containers leave little time for security scanning. The use of containerized microservices results in increased data traffic and complex access control. In addition, cloud-native environments and portability of containers also makes them difficult to monitor without the right security tools and expertise.

How IBM Container Security Services can help

As part of your cloud journey, IBM Container Security Services are designed to help secure your container workloads in a hybrid multi-cloud environment, including on-premises, public clouds and private clouds. Our security services include assessment, solution design, implementation and managed security services for all phases of container lifecycle, backed by expertise and technologies to automate security processes within the development pipeline. As a trusted security advisor and partner, we can help your enterprise overcome the security challenges of all major container risk areas.

IBM Container Security Services cover five major risk areas



Container security risk areas: image, registry, orchestrator, container and host

1) Image: Design of "validation stage"; detection of configuration defects; policy definition to block the instantiation

2) *Registry*: Audit of processes; use of secure connections; development of policies for effective authentication

3) *Orchestrator:* Implementation of role-based access control (RBAC) policies; implementation of proper API controls; design and implementation of workload security zones

4) *Container:* Setup of vulnerability management capabilities; monitor and control of unbounded network access; detection and fix of insecure container run-time configurations

5) *Host:* Hardening and scanning of host OS and running apps; segregation of host resources; use of configuration management & effective authentication

Key Benefits

- *Consulting & integration services* - Our security experts can help you assess, design and implement container security for your organizations' security and compliance needs
- *Application policy management* - Automated app behavior analysis, policy assignment to apps; custom app policy optimization; L3 and L7 firewall optimization and configuration
- *Managed security services* - Optimizes time of limited resources by providing expertise that helps monitor and manage the security of your container environment through build, ship and run-time phases
- *Threat management services* - End-to-end threat management strategy that helps you identify, protect and detect advanced threats and if necessary helps you respond and recover from disruptions
- *X-Force Red vulnerability management* - Automated vulnerability ranking to visually identify rogue containers, registries, images or applications for prioritized remediation
- *Centralized visibility* - Minimizes security risk with 24 x 7 x 365 proactive container event monitoring, alerting and threat management to achieve compliance across app container environment
- *Container security governance* - Enables container security governance by establishing container security policy, management and enforcement to protect app containers
- *Secure app development* - People, process, and technology transformation to bring Security and DevOps together; integration of security into development pipeline and software development lifecycle (SDLC)
- *Innovate securely at cloud speed* - Infrastructure automation and scalable security at the speed of cloud

Let us secure your journey to cloud

IBM Security professionals can perform a holistic assessment of your current cloud and container security strategy, identify the gaps, develop a future state and the roadmap to get there, to meet your specific enterprise container security needs. We can help you securely build, deploy and iterate applications by integrating security at all stages of the software development lifecycle, including shift-left secure design, DevSecOps best practices and fully-managed container security solutions. Let us help you create a robust enterprise security program, no matter where you are in your journey to cloud, enabling you to focus on cloud transformation and drive business innovation.

Why IBM?

IBM Container Security Services can help protect your application container environment and help support hybrid multi-cloud security by combining technologies from IBM Business Partners with IBM Security Services expertise. IBM Security Services span consulting, systems integration and managed security services to help support security for the full application container lifecycle.

Next steps

→ Schedule a consultation by calling 1-877-426-3774 with Priority code: Security

For more information

To learn more about IBM Container Security Services, please contact your IBM representative or IBM Business Partner, or visit the following website(s): ibm.com/security/services/application-security-services