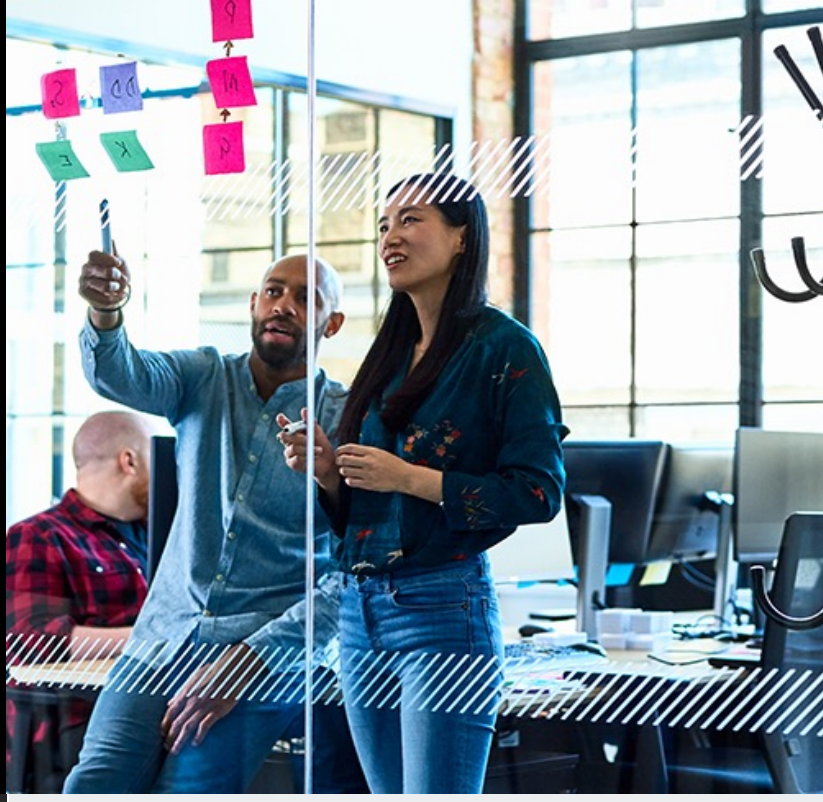
IBM Security

Securely build, deploy, and iterate apps with IBM Security Cloud Workload Protection Services



Are you securing your application cloud-native environments?

With any new technology, there will always be new threat vectors to consider – containers and serverless environments are not the exception.

IBM Security's Cloud Workload Protection services were built to help by providing assessment, solution design, implementation, and managed security services that will help you to secure your cloud workloads.

Member of Microsoft Intelligent Security Association

Microsoft

Gold Microsoft Partner

Microsoft

IBM

IBM Security offers coverage for cloud workloads regardless of where they are running

Securing the image

- Design of the "validate stage"
- Detection of configuration defects
- Define registry scanning policies

Securing orchestration

- Implement RBAC policies
- Implement proper API controls
- Design/implement workload security zones

Securing containers

- Set up vulnerability management
- Monitor/control unbounded network access
- Detect and fix insecure runtime configs

Securing hosts

- Harden and scan host OS and running apps
- Segregation of host resources
- Ensure the use of configuration management and effective authentication

Securing serverless infrastructure

- Audit processes
- Implement runtime controls
- Develop policies for effective authentication

Managed security services for build, ship, and run-time

We will provide managed security services with dedicated security expertise that helps monitor and manage the security of your cloud-native environments through build, ship, and run-time phases:

- **Application policy management**: Automated app behavior analysis, policy assignment to apps; custom app policy optimization; L3 and L7 firewall optimization and configuration
- **Vulnerability management**: Automated vulnerability ranking to visually identify rogue containers, registries, images or applications for prioritized remediation
- **Threat management:** End-to-end threat management strategy that helps you identify, protect, and detect advanced threats – and if necessary, respond/recover from disruptions

Key value

Assessment: Assess your current state of existing container environment by analyzing DevSecOps processes, application design, and solution requirement to find gaps and build a roadmap for your future state

Design: After assessment, our security experts can design solutions based on the future state roadmap – including macro and micro design, process definitions, and workload-centric security policies

Implementation: We will help implement appropriate security tooling to help deployment planning, container solution implementation, and 3rd party integrations

Management: Once at steady state, we can provide continuous monitoring and compliance reporting, incident analysis and response, policy governance, and proactive vulnerability management through our X-Force Red services that allow for vulnerability ranking for prioritized remediation

Key benefits

IBM Security experts
Optimizes time of your limited resources by helping identify/analyze vulnerabilities with shift-left expertise

Centralized visibility
Minimizes risks with 24x7x365 proactive container event monitoring, alerting, and vulnerability and threat management

Security policies governance
Enables security governance for workload-centric security policies, IT policy management and enforcement

Secure application development
Transforms people, process, and technology to unify Security and DevOps

Security at cloud speed
Innovate securely through infrastructure automation and scalable security