KubeArmor

Cloud-Native Runtime Security Enforcement

KubeArmor is an open-source, cloud-native runtime security enforcement system that proactively hardens your infrastructure and protects critical workloads. Leveraging the power of Linux Security Modules (LSMs) like AppArmor, SELinux, and eBPF-LSM, KubeArmor enforces user-defined policies at the system level, preventing malicious behavior before it can impact your applications.

The Challenge: Post-Attack Mitigation Falls Short

Traditional security approaches often focus on detecting and reacting to attacks after they've occurred. This "post-attack mitigation" leaves a critical window for attackers to execute code, exfiltrate data, and escalate privileges, potentially evading detection. Furthermore, the complexities of managing native Kubernetes Pod Security Contexts across diverse cloud environments with varying LSMs present significant operational hurdles.

The KubeArmor Solution: Proactive, Inline Mitigation

KubeArmor provides inline mitigation, fundamentally shifting security from reactive to proactive. By enforcing granular policies at runtime, KubeArmor stops malicious activity at its source, minimizing the attack surface on pods, containers, and virtual machines.

Core Capabilities: Why KubeArmor is Unique

Behavior Restriction
Limits process execution, file access, networking, and resource utilization within workloads. Hardens infrastructure against unauthorized actions.

Runtime Policy Enforcement
Real-time security policy enforcement based on workload identities using LSMs. Preemptively mitigates security attacks.

Kubernetes-Native
Policy development based on Kubernetes metadata for enhanced, native security. Seamless integration into existing Kubernetes workflows.

Policy Violation Logging
Generates rich alerts/telemetry events with container/pod/namespace identities via eBPF. Provides deep visibility into attempted policy breaches for forensic analysis.

Simplified Policy Descriptions
Abstracts LSM complexity, making policy creation and management intuitive. Reduces operational overhead and simplifies security posture management.

Network Security
Regulates communications between containers using network system calls. Enforces micro-segmentation and prevents lateral movement.

Use Cases

Harden Infrastructure
- Protect critical paths (e.g., cert bundles)
- Implement MITRE, STIGs, and CIS-based rules
- Restrict access to raw DB tables

Least Permissive Access (Zero Trust)
- Process Whitelisting
- Network Whitelisting
- Control access to sensitive assets

Application Behavior Monitoring
- Monitor process executions and file system accesses
- Track service binds, ingress, and egress connections
- Sensitive system call profiling

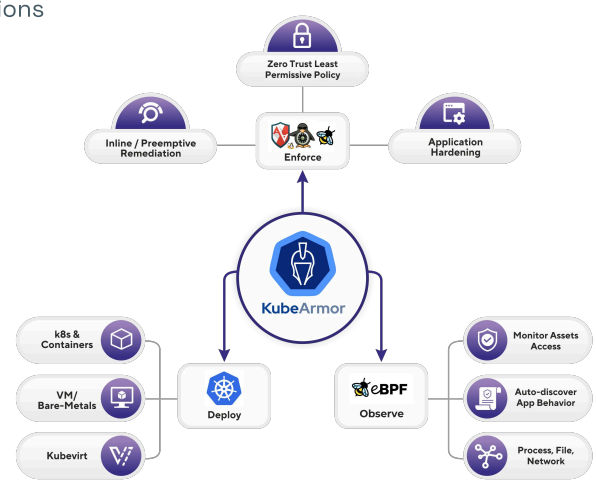
Deployment Models

KubeArmor offers flexible deployment options to suit diverse environments:

Kubernetes Deployment
Native integration with Kubernetes clusters

Containerized Deployment
Run within containerized environments

VM/Bare-Metal Deployment
Secure traditional VMs and bare-metal servers



Trusted by the Community

With over **1.2 Million+ Downloads**, KubeArmor is a CNCF Sandbox open-source project, maintained by a vibrant community, and actively used by developers and organizations to secure their cloud-native workloads.

KubeArmor | CLOUD NATIVE SANDBOX | THE LINUX FOUNDATION

KubeArmor: Proactive Runtime Security for a Cloud-Native World.