Falco vs KubeArmor

Comparing Two Powerful Kubernetes Security Tools

Press Space for next page →

Introduction to Falco

What is Falco?

- CNCF's de facto runtime security project
- Real-time threat detection engine
- Observes system calls at runtime

How it Works

- Uses extended Berkeley Packet Filter (eBPF)
- Monitors container, application, host, and network activities
- Generates alerts based on rule violations

Common Use Cases

- Runtime threat detection
- Container security monitoring

Introduction to KubeArmor

What is KubeArmor?

- Container-aware runtime security enforcement system
- Operates at kernel level
- Focuses on policy enforcement

Kernel-level Security

- Uses Linux Security Modules (LSMs)
- AppArmor, SELinux integration
- Process-level security policies

Key Features

- Fine-grained policy enforcement
- Container-aware security

Falco vs KubeArmor Comparison

Feature	Falco	KubeArmor
Primary Function	Detection & Monitoring	Prevention & Enforcement
Architecture	Syscall-based	LSM-based
Security Approach	Rules-based detection	Policy-based prevention
CNCF Status	Graduated	Sandbox
Performance Impact	Lower (eBPF-based)	Moderate (LSM hooks)
Use Case Focus	Threat Detection	Policy Enforcement
Integration	Alert-focused	Policy-focused