File Integrity Monitoring

Real-time, kernel-level detection & prevention of unauthorized changes to critical system paths across VMs, containers, Kubernetes, and hybrid cloud.

ACCUKNOX
Secure Code to Cognition™

COMPLIANCE COVERAGE

PCI-DSS	Req. 6 & 10
NIST 800-53	AU-2, SI-4
CIS Linux	v2.0 - 6.3.5
MITRE ATT&CK	T1565, T1036
HIPAA	ePHI integrity
SOC 2	Change control
ISO 27001	Audit trails
SOX	Config integrity
GDPR	Data integrity

Read More →

TECHNICAL COVERAGE

Virtual Machines	Supported
Kubernetes / Containers	Supported
Bare Metal Linux	Supported
Enforcement Engine	KubeArmor
Visibility Layer	eBPF
Policy Action	Block Mode
Protection Scope	Recursive
Cloud Support	AWS, Azure, GCP
Integrations	Splunk-Grafana

Overview: What FIM Actually Is

File Integrity Monitoring (FIM) watches critical system files, binaries, and configurations for any unauthorized change. AccuKnox goes further. Instead of just alerting after the fact, it blocks the write at the kernel before the OS ever processes it. One silent config change can disable logging, escalate privileges, or plant ransomware. AccuKnox stops it at the syscall.

What Gets Protected

/sbin/
System executables

/bin/
Core OS binaries

/usr/bin/
User programs

/usr/sbin/
Admin binaries

/usr/lib/
Shared libraries

/boot/
Kernel & bootloader

All paths enforced recursively: every subdirectory and file inside is locked automatically.

Why It Matters

Attackers Target Config First
NetWalker, Conti, DarkSide all exploited writable system paths for privilege escalation and persistence.

Detection Is Too Late
Traditional FIM tools alert after the change lands. By then, logs are off and the attacker is in.

Compliance Demands It
PCI-DSS, HIPAA, NIST, SOX, and CIS all mandate continuous file integrity verification.

Fragmented Estates
VMs + Kubernetes + multi-cloud means inconsistent FIM tools and blind spots. One policy fixes that.

How It Works

01 Policy Applied
FIM policy targets VMs and containers, locking specified paths read-only. Zero app changes.

02 Kernel-Level Block
eBPF intercepts syscall. KubeArmor denies the write before the OS processes it.

03 Alert & Audit
Full event in SaaS console: file, process, PID, user, container, timestamp.

What Sets AccuKnox Apart

BLOCK
Block, Not Just Alert
Kernel enforcement denies writes before they land. Most tools only notify after the fact

EBPF
Deep Kernel Visibility
Captures exact syscall, process, PID, and file path with near-zero overhead

UNIFIED
One Policy, Every Surface
VMs, bare metal, K8s, and containers across AWS, Azure, GCP, on-prem.

CNCF
Open-Source Core
Built on KubeArmor, a CNCF project. Transparent and community-backed

Capability	AccuKnox	Fortra / Qualys	OSSEC / Wazuh	CrowdStrike Falcon / Filevantage
Kernel enforcement (Block mode)	✓ Block	✗ Alert only	✗ Alert only	— Limited
Kubernetes + VM in one policy	✓	✗ Separate tools	✗ VM only	— Endpoint focus
PCI-DSS / NIST out-of- the-box	✓	✓	— Manual setup	— Add-on

Read Blog →

About AccuKnox

AccuKnox is a Zero Trust CNAPP Cloud Security protects API Security, CDR, SIEM, Public clouds, Private clouds, Kubernetes, VMs, Bare metals, IoT Edge, and 5G security.

CLOUD NATIVE COMPUTING FOUNDATION SILVER MEMBER

NEPHIO

ACCUKNOX

linkedin.com/accuknox

@AccuKnox