ARMOR FILE INTEGRITY MONITORING (FIM)

When traditional firewalls or intrusion detection systems (IDS) fail to prevent or detect a threat, monitoring operating system (OS) and application changes at the host level provides an additional layer of detection for indicators of compromise (IOC) or a breach of your environment. Security teams are largely in the dark to an attacker's presence, activities, and movements without monitoring processes and applications at the host level.

FILE INTEGRITY MONITORING

Armor FIM watches your hosts 24/7/365 for anomalous and unauthorized activities to detect potential threats. It monitors critical system file locations on your hosts as well as critical OS files for changes that may allow threat actors to control your environment.

ARMOR FILE INTEGRITY MONITORING LOOKS FOR:

- Changes to critical OS files and processes such as directories, registry keys, and values
- Changes to application files
- Rogue applications running on the host
- Unusual process and port activity
- System incompatibilities

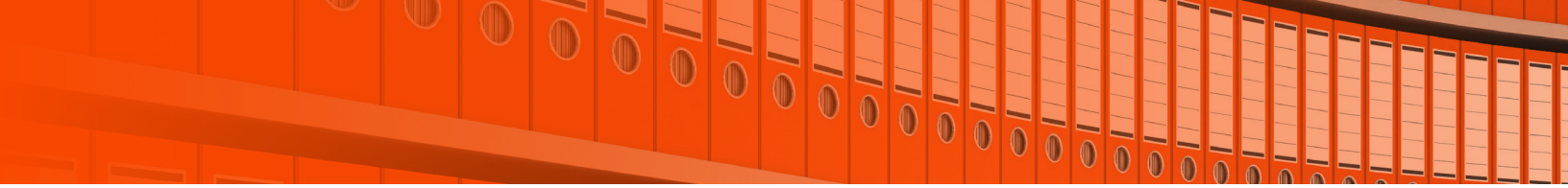
DEPLOYMENT AND MANAGEMENT

Delivered through an agent and installed on your virtual servers/instances/workloads, the Armor FIM service is designed to monitor critical OS files, configurations, and processes, as well as monitor application files and related activities for potential IOC.

The service establishes a baseline that future activities are compared against and applies standardized monitoring policies for each workload (Linux/Windows).

Event data is fed into Armor's Spartan threat prevention and response platform for analysis and correlation, with alerted items reviewed further by Armor security operations center (SOC) personnel.

ARMOR



ARMOR FILE INTEGRITY MONITORING DELIVERS TRUSTED SECURITY

- Unify protection across your cloud, on-premise, hybrid, and hosted environments through correlation of FIM events with other security controls under Armor's management
- Get access to time-tested security and compliance experts monitoring your environments 24/7/365
- Address key compliance controls involved in FIM
- Go beyond simple alerting and respond to incidents faster

GET CRITICAL PROTECTION ACROSS YOUR HOSTS IN ANY ENVIRONMENT

POWERED BY SPARTAN

Armor FIM is powered by Spartan—the IT security industry's leading threat prevention and response platform. Armor integrates advanced analytics, global threat intelligence, and continuous response capabilities into a single platform that bolsters your defenses, uncovers hidden threats, and prevents security breaches. Whether your sensitive data and workloads are stored in a private, public, or hybrid cloud—or in an on-premise IT environment—Spartan provides a proactive approach to cyberthreats.

Armor FIM inspects your OS files, configurations, activities, and processes at the host layer for indicators your environment may have been breached. Leveraging Spartan, Armor analyzes and correlates event information to identify when a single FIM event could be part of a broader security incident.

ADDITIONAL LAYER OF DEFENSE AGAINST THREATS

Armor FIM provides an extra layer of protection at the host level to detect suspicious activity and alert you to potential threats.

ADVANCED ANALYSIS AND CORRELATION

Events are analyzed and correlated with event data from your other devices under Armor management through our Spartan threat prevention and response platform, delivering enhanced detection of potential threats across your cloud, on-premise, hybrid, and hosted environments.

AUDIT-READY COMPLIANCE

Armor FIM addresses key change control processes required by PCI DSS, HIPAA, HITRUST, SAN CSC, NIST, and other frameworks.

RESPONSE THAT GOES BEYOND ALERTING

Unlike traditional managed-security-service-providers (MSSPs), Armor goes beyond simple alerting to a problem. Our SOC analysts monitor your environment 24/7/365, while also working closely with your team to investigate and respond to potential incidents.

ARMOR