FILE INTEGRITY MONITORING FOR CLOUD ENVIRONMENTS

Collect, Identify and Report

on File Changes

Lacework™

FILE INTEGRITY MONITORING FOR CLOUD ENVIRONMENTS

Collect, Identify and Report on File Changes

File tampering is a critical indicator of compromise so it's easy to understand why File Integrity Monitoring (FIM) is a critical requirement in most compliance mandates. Lacework recognizes that FIM is more than a compliance checklist item, so the Lacework solution identifies the instance of malicious files and other anomalies in cloud and container environments, as well as the actors who are involved, and then delivers contextual alerts.

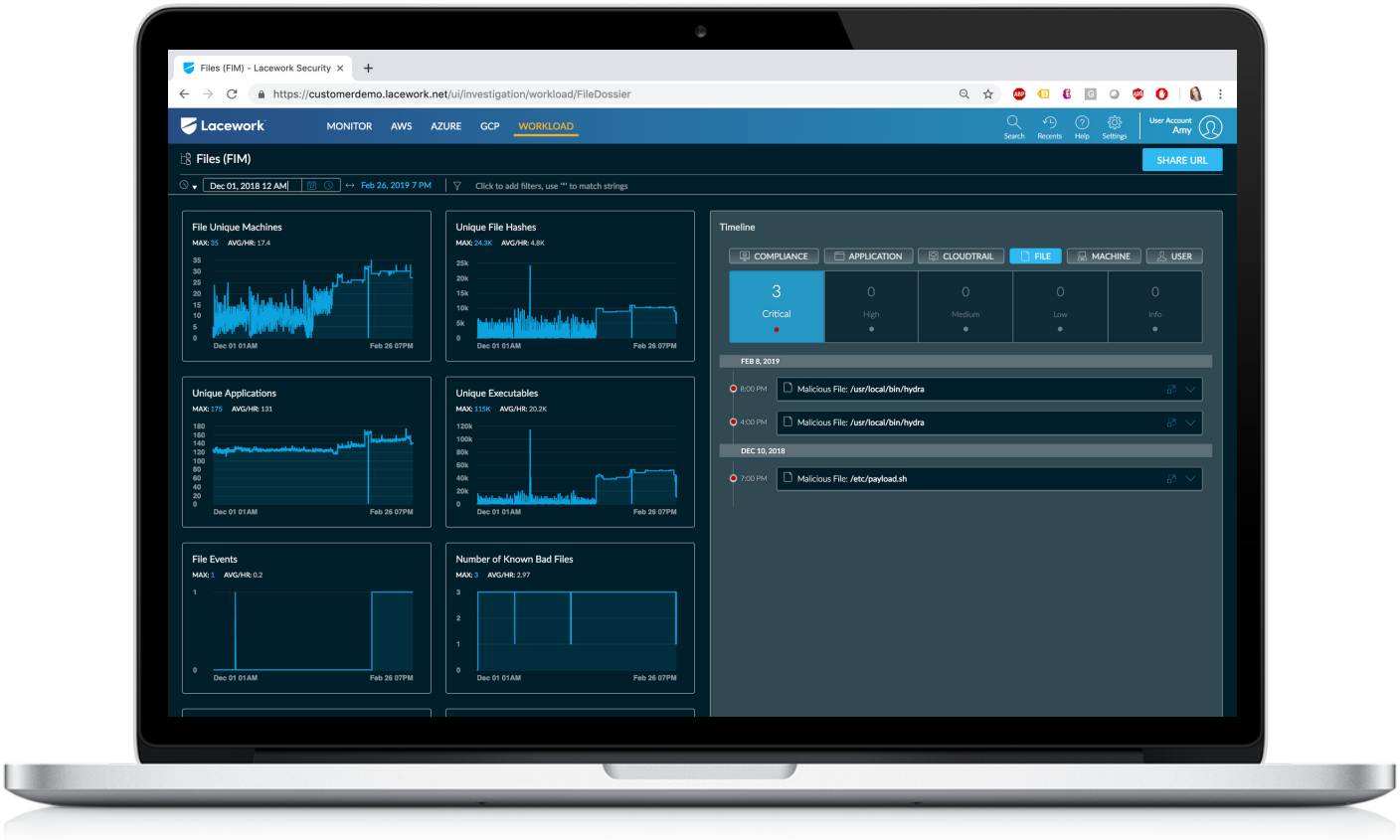
Designed for high-velocity cloud implementations, Lacework's FIM solution automates setup and eliminates the need for operations-intensive rule development and management.

With our innovative baselining technology, Lacework keeps up with cloud changes while dramatically reducing false positives so security teams can focus on the FIM changes that really matter.

AUTOMATING FILE DETECTION

The Lacework agent automates the process of collecting and recording files. The agent records new files as they are added and records the hashes of the files as they change, displaying the old and new for easy comparison. The agent streams this data back to the cloud platform to ensure that the information is reliably collected and stored.

Additionally, Lacework any files that are known to be malicious using external Threat feeds. Once the hashes have been collected, the checksum is compared against curated threat databases to ensure that no known malicious files exist within monitored environment. If a known malicious file is found within the environment, Lacework will trigger a critical alert. From there, you can investigate quickly to determine what systems does this file exist on and also can do additional research on the files linking back to VirusTotal database for threat summary. This expedites the process of identifying files as well as the research needed to understand the impact of the malicious file.



INTEGRATED AND COMPREHENSIVE

- Pinpoint exactly how a file changed: content, metadata, and whether the file was modified or simply appended
- Extended information on executables, such as files created without a package installation, command lines used at launch, currently running processes (with users and network activity), and suspect versions
- Expanded file intelligence with integrated threat feeds from ReversingLabs' library of 5 billion files
- One-click investigation of events and activities related to FIM signals
- Cloud-wide capabilities for search, file type summaries, and detection of new files

CLOUD SCALE AND SPEED

- Automated configuration, file discovery, and operations
- Scalable architecture with no added complexity or performance penalties
- Included with all Lacework Cloud Security agents

MEET COMPLIANCE MANDATES

- Protect log and configuration files against tampering
- Daily re-check of all monitored files
- Pre-defined directory maps monitor critical files and directories
- Easily configurable; users can add directories to the watch list

SECURITY VISIBILITY

Get deep observability into your cloud accounts, workloads, and microservices to give you tighter security control.

THREAT DETECTION

Identify common threats that specifically target your cloud servers, containers, and IaaS accounts so you can action on them before your company is at risk.

ANOMALY DETECTION

Detect and resolve anomalous changes in behavior across your workloads, containers, and IaaS accounts that represent a security risk or an IOC.

HOST COMPLIANCE

Achieve compliance for SOC 2, PCI DSS, HIPAA, and other compliance measures that require host intrusion detection (HIDS).

CONFIGURATION COMPLIANCE

Spot IaaS account configurations that violate compliance & security best practices the could put your company at risk.