

File Integrity Monitoring Software

What it does, how the tools differ, and when monitoring isn't enough. A vendor-neutral reference to FIM, followed by an honest look at where detection stops and prevention starts.



MIMIC



Table of Contents

File Integrity Monitoring	3
■ What file integrity monitoring is	3
■ How FIM tools differ	4
■ Running FIM day to day	5
■ Key figures	6
When Monitoring Isn't Enough	7
■ Detection and prevention are different purchases	7
■ What enforcement looks like	7
■ Enterprise server use cases	7
■ What each control proves, and what it costs	8
■ Frequently Asked Questions	9

Disclosure. Mimic publishes this guide. Section 1 is a vendor-neutral reference and names no Mimic product. Mimic isn't a file integrity monitoring vendor, and Section 2 says where it fits.

File Integrity Monitoring

DEFINITION

What file integrity monitoring is

File integrity monitoring (FIM) is a security control that records a trusted baseline of critical files, configuration and, on Windows, registry settings, then compares the current state against it on a schedule or in real time. When something is added, changed or deleted, FIM alerts and records who, what and when. On its own, it detects change rather than preventing it.

How it works

Baseline. The tool records the approved state of the files, settings and registry keys you choose, usually as cryptographic hashes plus attributes such as permissions and owner.

Monitor. It compares the current state against that baseline, either on a schedule or continuously through an agent that watches the file system in real time.

Detect and alert. When a monitored item is added, changed or deleted, it raises an alert with the change, the time and, where the platform allows, the account and process responsible.

Report. It keeps a record of every change and maps that record to the requirements an auditor will test, which is where most of the buying decision is made.

Why organizations buy it

Most organizations buy FIM because a standard tells them to. PCI DSS v4.0.1 requirement 11.5.2 calls for a change-detection mechanism, with file integrity monitoring tools as its example, to alert on unauthorized changes to critical files and to compare critical files at least weekly. Microsoft's own documentation notes that FIM is often required by regulatory standards such as PCI DSS.

FIM vendors build policy libraries around these obligations. Fortra describes Tripwire Enterprise's built-in policies for PCI DSS, CIS benchmarks and DISA STIGs, and Netwrix holds CIS certification for Change Tracker's hardening checks. Beyond compliance, an unexpected change to a system file is one of the clearest indicators of compromise a team can get.



COMPLIANCE NOTE

If a standard names change detection, buy change detection. PCI DSS 11.5.2 asks for a mechanism that alerts on unauthorized changes to critical files and compares them at least weekly. A prevention control doesn't satisfy that requirement, however good it is.

COMPARISON

How FIM tools differ

We compared each option on the questions a buyer asks: what it detects, the evidence it gives an auditor, platform coverage including Linux, how it handles noise, and whether it prevents change or reports it. These criteria favor dedicated FIM products on compliance evidence, because that's where they lead.

Criterion	Why it matters
What it detects	Files only, or files plus registry keys, configurations, accounts and network devices. Scope decides what an attacker can change unseen.
Auditor evidence	Reports mapped to the standards you're tested against. This is the dedicated FIM vendors' strongest ground.
Platform coverage	Windows, Linux, Unix, databases and network devices. A server estate is rarely one operating system.
Noise handling	How the tool separates planned change from unplanned change. This decides whether the alerts get read.
Prevents or reports	Most FIM reports change. Some products add restore or deny features on top.

The options side by side

Option	What it detects	Auditor evidence	Platforms	Noise handling	Prevents or reports
Tripwire Enterprise (Fortra)	Changes to files and configurations, plus security configuration against policy	Strongest: built-in policies for PCI DSS, CIS and DISA STIG, over 4,000 platform and policy combinations, audit reporting	Operating systems, applications, servers and devices	Integrates with change management, ITSM and SIEM tools	Reports
Cimcor CimTrak	Files, directories, configurations, users, policies, Active Directory and databases	Compliance reporting with who, what, when and how detail	Physical, virtual and cloud servers	Trusted File Registry reconciles vendor patches; change tickets	Reports, and can restore or deny changes to monitored files
Netwrix Change Tracker	Files, folders, registry keys and configurations	Compliance reporting and CIS-certified hardening checks	Windows, Linux, Unix, network devices and databases	Reconciles changes against approved ITSM requests and planned-change rules	Reports; flags unplanned changes as potential breach activity
Microsoft Defender for Cloud FIM	Operating system files, Windows registry, application software and Linux system files	Change records in Defender for Cloud	Windows and Linux; Defender for Endpoint agent plus agentless scanning	Recommends what to monitor based on known attack patterns	Reports
Windows file system auditing	Use of audited access rights on files and registry objects, logged as event 4663	Raw Security log events, with no baseline comparison	Windows only	Scope set by the SACLs you apply	Reports access

Descriptions come from each vendor's own documentation. Microsoft Defender for Cloud FIM requires Defender for Servers Plan 2.

OPERATIONS

Running FIM day to day

Expect volume. Netwrix, a FIM vendor, says every server, workstation, database and network device generates thousands of file and configuration changes a day. PCI DSS's own guidance defines critical files as those that don't regularly change, and that's the first tuning decision: watch what shouldn't move, not everything.

Tuning is the work. Vendors cut noise in two ways. Netwrix's closed-loop change control matches detected changes against approved ITSM change requests and planned-change rules. Cimcor's Trusted File Registry reconciles vendor-verified patches. Microsoft's Defender for Cloud recommends what to monitor based on known attack patterns.

Someone owns triage. An unplanned change needs a person to decide whether it's an attack, a mistake or undocumented maintenance. Decide who that is, and connect FIM to your change tickets, before you deploy.

On the numbers. We didn't find an independent, dated statistic on FIM alert volume or tuning time. Vendors publish figures for their own products' noise reduction, so we haven't presented them as category data.

What Microsoft gives you

Two options, and they aren't the same. Windows file system auditing is native: set a system access control list on a file, folder or registry key, and Windows logs event 4663 when an audited access right is used. That records access, not integrity against a baseline, and the events land in the Security log, where something has to collect and review them.

Defender for Cloud includes FIM in Defender for Servers Plan 2. It scans operating system files, registry keys, application software and Linux system files, collecting data through the Defender for Endpoint agent and agentless scanning. If you already run Plan 2 across a Windows and Linux server estate, its FIM may be enough. If you need deep compliance reporting across many standards, a dedicated FIM product leads.

“For change-detection purposes, critical files are usually those that do not regularly change...”

PCI DSS V4.0.1, REQUIREMENT 11.5.2, APPLICABILITY NOTES

KEY FIGURES



Key figures

11.5.2	Weekly	4663
The PCI DSS v4.0.1 requirement that calls for a change-detection mechanism, with FIM as its example.	The minimum frequency PCI DSS 11.5.2 sets for comparing critical files.	The Windows event that records use of an audited access right on a file or registry object.



When Monitoring Isn't Enough

THE DISTINCTION

Detection and prevention are different purchases

File integrity monitoring reports a change after it lands; enforcement refuses an unauthorized change before it executes. They answer different questions, and many organizations need both. Enforcement doesn't satisfy a requirement that names change detection: PCI DSS 11.5.2 calls for a change-detection mechanism, so a regulated estate still needs FIM. FIM also has a structural blind spot on servers: a trusted, signed binary used for something it shouldn't do raises no FIM alert, because the file itself didn't change, the pattern the LOLBAS project catalogs and Mimic's Server Threat Library documents on servers.

A positive security model starts from the other end. Monitoring compares state to a baseline after the fact. A positive security model defines what's authorized for a system and refuses everything else before it happens, whoever or whatever attempts it.

The line isn't absolute. Some FIM products add remediation on top: Cimcor describes CimTrak restoring a changed file to its baseline or denying changes to monitored files. They're still built around detection and reporting, and that's what an auditor tests.

A WORKED EXAMPLE

What enforcement looks like

Mimic is one worked example of enforcement on servers. It enforces known-good state at the kernel on Windows and Linux servers, through a file system mini-filter driver on Windows and eBPF on Linux. Each attempted change to files, processes, registry keys or services is checked against the server's authorized baseline and blocked if it falls outside, whatever credential or tool makes it.

Because the test is whether a change was authorized, not whether it matches a known attack, a signed tool that's allowed to run still can't make an unauthorized change. Enforcement sits below the security agents on a protected server, so it can hold the change an attacker needs to disable them. ESET catalogued nearly 90 EDR killers in active use in March 2026. For servers waiting on a patch or past end of support, Mimic's Virtual Patching adds safeguards around the paths an exploit would use.

What it doesn't do

Mimic isn't a file integrity monitoring product. It doesn't produce FIM compliance reports, and it doesn't satisfy a requirement that names change detection. It runs only on servers, not laptops. Where a standard requires FIM, run FIM. Enforcement runs alongside it.

WHERE IT FITS

Enterprise server use cases

A production server runs a narrower, more predictable software set than a laptop, which is where enforcement fits best.

Domain controllers

The system every account depends on. Unauthorized changes to services, registry or policy files carry the most risk, and approved administrative tools are the likeliest vehicle.

Database and application servers

A stable software set, so a baseline holds and unauthorized change stands out. FIM records configuration drift; enforcement blocks the change that isn't authorized.

Payment servers in PCI DSS scope

FIM for the change detection 11.5.2 requires, and enforcement to stop what it can before it lands.

Systems that can't be patched

Windows Server 2012 R2 left extended support on 10 October 2023, with paid Extended Security Updates only through 13 October 2026. FIM tells you when servers like it change. Enforcement and virtual patching reduce what an attacker can change.

EVIDENCE AND TRADEOFFS

What each control proves, and what it costs

Evidence. A dedicated FIM tool produces change-detection evidence mapped to a standard's requirements. Mimic records each enforcement decision per host, per CVE and per timestamp: proof of what was blocked and allowed. That supports an audit conversation about control, but it isn't the change-detection report a FIM requirement asks for.

Cost. FIM's running cost is triage. Enforcement's running cost is the baseline: each server's baseline has to stay accurate as the server changes, and that's harder on dynamic applications. Many regulated server estates run both.



“If you try to succeed by understanding all the bad behavior in the world, instead of by understanding the known-good behavior in the world, you're just going to lose the race.”

BOB BLAKLEY, CO-FOUNDER AND CHIEF PRODUCT OFFICER, MIMIC

QUESTIONS

Frequently Asked Questions

■ What is file integrity monitoring?

File integrity monitoring is a security control that records a trusted baseline of critical files, configuration and registry settings, then compares the current state against it on a schedule or in real time. When something is added, changed or deleted, it alerts and records who, what and when. Teams use it to investigate unexpected change and to show auditors that critical systems are watched.

■ Is file integrity monitoring required for compliance?

Often, yes. PCI DSS v4.0.1 requirement 11.5.2 calls for a change-detection mechanism, with file integrity monitoring tools as its example, to alert on unauthorized changes to critical files and compare them at least weekly. Other frameworks and benchmarks expect change monitoring too. If your standard names change detection, a prevention control alone won't meet it. Confirm the specific requirement with your assessor.

■ How does file integrity monitoring differ from enforcement?

File integrity monitoring reports a change after it lands. Enforcement checks whether a change is authorized before it happens and refuses it if not. They answer different questions, so many organizations need both: FIM for change detection and compliance evidence, enforcement to stop unauthorized change on critical systems. Enforcement doesn't satisfy a requirement that names change detection, and FIM doesn't stop a change.

■ Is built-in Windows tooling enough for file integrity monitoring?

Sometimes. Windows file system auditing records use of audited access rights on files and registry keys as event 4663, but it logs access rather than comparing files to a baseline, and the events need collecting and review. Defender for Cloud includes true FIM in Defender for Servers Plan 2 for Windows and Linux. For deep compliance reporting across many standards, a dedicated FIM product leads.



■ **How much alert volume should I expect from FIM?**

More than you'd like at first. Netwrix, a FIM vendor, says every server and device generates thousands of file and configuration changes a day. Volume drops when you monitor only files that shouldn't change, reconcile alerts against approved change tickets, and recognize trusted vendor patches. We found no independent statistic on alert volume, so treat vendor figures as claims about their own products.

■ **Can file integrity monitoring catch misuse of trusted tools?**

Not by itself. FIM watches whether files change. When an attacker misuses a trusted, signed binary that's already on the server, the binary doesn't change, so FIM has nothing to flag unless the misuse alters a monitored file. The LOLBAS project catalogs Microsoft-signed binaries attackers repurpose. Catching that pattern takes controls that watch behavior or enforce what each change is allowed to do.

■ **Do I need both FIM and enforcement?**

Many regulated server estates do. FIM gives you change detection and the compliance evidence a standard asks for. Enforcement stops unauthorized change before it lands, including change made with valid credentials. The costs differ: FIM's is alert triage, and enforcement's is keeping each server's baseline accurate. Start with what your standard requires, then add prevention where unauthorized change is the bigger risk.

■ **Is Mimic a file integrity monitoring product?**

No. Mimic is an enforcement product. It checks whether a change to files, processes, registry keys or services on a Windows or Linux server is authorized before it happens, and blocks it if not. It doesn't produce FIM compliance reports, and it doesn't satisfy a requirement that names change detection. Where a standard requires FIM, run FIM. Mimic runs alongside it.

Sources

PCI Security Standards Council, PCI DSS v4.0.1, requirement 11.5.2 and its applicability notes (2024): https://www.pcisecuritystandards.org/document_library/

Microsoft Learn, accessed October 2026: Defender for Cloud file integrity monitoring overview, <https://learn.microsoft.com/azure/defender-for-cloud/file-integrity-monitoring-overview>; Event 4663, <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4663>; Windows Server 2012 R2 lifecycle, <https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2012-r2>

Vendors: Fortra Tripwire Enterprise, <https://www.fortra.com/products/tripwire-enterprise>; Netwrix Change Tracker, <https://netwrix.com/en/solutions/file-integrity-and-configuration-monitoring/> and <https://netwrix.com/it/lp/file-integrity-monitoring-tool/>; Cimcor CimTrak for Servers, <https://cimcor.com/solutions/servers>

ESET Research, EDR killers analysis, March 2026, <https://thehackernews.com/2026/03/54-edr-killers-use-byovd-to-exploit-34.html>; LOLBAS project, <https://lolbas-project.github.io/>; Mimic, Server Threat Library, <https://mimic.com/server-threat-library>, and Kernel-Level Enforcement Guide, <https://mimic.com/whitepapers/kernel-level-enforcement-guide>



FILE INTEGRITY MONITORING SOFTWARE

Thank You

If your critical servers need changes stopped as well as reported,
that's the conversation we'd want to have.

SALES@MIMIC.COM