Integrity Monitoring

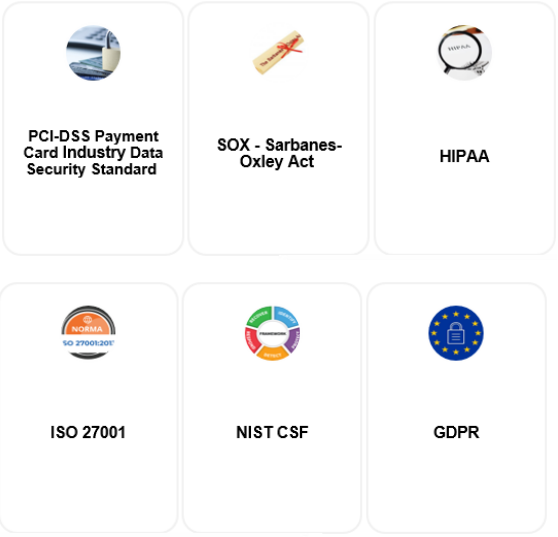
Monitor more than file level activity in real time with Integrity Monitoring

The ever-increasing number of sophisticated threats targeting organizations, irrespective of size means a breach is likely to occur, if it hasn't already. This is one of the reasons why organizations who operate under regulatory mandates and standards or must comply with security frameworks are required to have a File Integrity Monitoring (FIM) solution as part of their security measures. To maintain compliance in standards like Payment Card Industry Data Security Standard (PCI DSS) or ISO 27001, organizations must demonstrate data governance, FIM solutions allows organizations to prove compliance. Integrity Monitoring offers capabilities beyond the standard FIM solution.

Integrity Monitoring offers more than file monitoring by assessing entities (File, Directory, Registry, Installed Apps, etc) across protected assets throughout the entire organization.

Out of the box anomaly detection and threat intel is used to identify integrity and configuration changes, allowing organizations to gain complete visibility of critical files and can seamlessly monitor and identify file creation, editing, modification, movement and deletion across cloud and/or On-premises environments with a single pane of glass view.

Cybersecurity Standard and Framework Compliance: Ensure your organization meets compliance standards and recommendations with Integrity Monitoring.



And more...

At-a-Glance

Integrity Monitoring is an Out-of- the Box integrity monitoring solution which provides real time visibility and monitoring of confidential and regulated data, configurations, and OS files to ensure their fidelity. Enabling organizations to meet regulatory mandates and empower security teams to proactively act against malicious activity and prevent significant damage.

Key Benefits

- Satisfy multiple standards and regulatory framework compliance mandates.
- Unify and streamline security solutions under one platform including FIM, server workload security, container security, endpoint protection and responses and XDR to bring together device intelligence across the enterprise network.
- Gain flexibility to responses by taking action manually or automatically based on defined rules and reduce alert fatigue by leveraging intel to prevent detection on trusted activity.

Protect sensitive data from tampering and benefit from ease of use

Integrity Monitoring brings advanced features which allows administrators set rules to identify configuration changes, performance optimization scanning options, and corrective action features empowering security teams to act to an incident accordingly and minimize damage or disruptions.

- **Manage change control** – Changes of critical systems or file modifications are often an early indicator that an attacker has gained access to the environment. Integrity Monitoring assesses changes in in real-time, allowing security teams to stay on top of incident management.
- **Mitigate risk due to unauthorized changes** – View integrity events in real-time as they occur. Identify meaningful configuration changes as they happen and distinguish between approved VS unapproved changes.
- **Prioritize alert severity** – Alerts can be very noisy and overwhelming, but Integrity Monitoring provides teams with automatic actionable recommendations tied to rules allowing teams to act on events. Security teams can filter by categorized events to quickly drill down to the most critical events
- **Straightforward Configuration** – Reduce time and effort in configuring integrity monitoring. Eliminate assigning rules or policies manually to endpoints every time. Limiting CPU utilization to scan files in a sequence, pause between scans or simply with lowest priority for a longer interval.

KEY CAPABILITIES:

- **Scanning** – Real-time scanning for visibility into your environment
- **Monitoring Rulesets** – Define the areas and specific parameters/entities that Integrity Monitoring should look for
- **Corrective Actions** – Control actions to be automated, manual based on recommendations
- **Performance Optimization** – Reduces time and effort spent on configuration with an intuitive interface and turnkey configurations

Integrity Monitoring is cloud-based and easy to deploy across on-premises, cloud or virtualized environments without impacting performance.

MyCyberIQ™
STAY AWARE. STAY SMART. STAY SECURE.™