CROWDSTRIKE

FALCON FILEVANTAGE FOR SECURITY OPERATIONS

Gain central visibility and relevant threat intelligence data efficiently with a streamlined file integrity monitoring solution

SIMULTANEOUSLY STREAMLINE FILE MONITORING AND REDUCE ALERT FATIGUE

Falcon FileVantage, CrowdStrike's file integrity monitoring (FIM) solution, offers central visibility around changes made to critical configuration, system and content files, as well as critical folders and registries across your entire organization. Security operations teams can use predefined or custom policies and groups to reduce alert fatigue, while broad and detailed dashboards help them keep an eye on all changes regarding these critical files and registries.

In addition to offering central visibility around relevant files and folders, Falcon FileVantage goes beyond compliance requirements by supplying additional context through the CrowdStrike Falcon® platform, with detection data to provide more insight to file, folder and registry changes — allowing your organization to improve its security posture.

Falcon FileVantage offers all of these capabilities by leveraging the same lightweight agent used for the Falcon platform.

KEY CAPABILITIES

GAIN CENTRAL VISIBILITY INTO ALL RELEVANT FILES AND FOLDERS

Falcon FileVantage offers central visibility into all critical file changes — offering relevant, intuitive dashboards displaying information on registry setting, which files/folders have been created or changed, and who was accessing those files/folders.

In addition, this FIM solution offers real-time visibility for all files and systems relevant to your organization, and allows you to:

- **Fulfill compliance requirements:** Gain visibility over all relevant files and folders using Falcon FileVantage to support file integrity monitoring regulatory compliance requirements, including the Payment Card Industry Data Security Standard (PCI DSS) and the Sarbanes-Oxley (SOX) Act.
- **Gain real-time visibility into file/folder changes:** Use real-time monitoring to watch for the creation, modification and deletion of all files and folders relevant to your organization's monitoring process.

KEY BENEFITS

Go beyond fulfilling compliance requirements for relevant regulatory policies/regulations

Gain real-time visibility for all harmful file/folder changes

Utilize a comprehensive set of dashboards to monitor for alerts, changes made and more

Pivot quickly to threat intelligence data relating to file/folder changes directly from the module

Increase efficiency with predefined policies — as a result, staff can cut down on event volume and reduce alert fatigue

See the big picture: Dial in on what file/folder changes have occurred across multiple hosts in your environment

- **See changes across hosts:** Get notified if similar changes have occurred for files/folders across multiple hosts.
- **Enhance staff monitoring abilities with intuitive dashboards:** See what's immediately relevant — streamline visibility over large systems throughout your organization with dashboards that show a variety of targeted information, including:
  - Systems with the most violations
  - Top types of changes being made to files/folders
  - Systems by mode in groups
  - Change trends — showing alerts from Critical to Low ratings
  - Change log views

USE RICH THREAT INTELLIGENCE DATA FOR CONTEXT

Unlike other FIM solutions, Falcon FileVantage* allows even greater visibility and context through added threat intelligence and detection data. FileVantage provides staff the ability to quickly target file change data with any relevant adversary activity. For example, if your organization suffered an attack, IT staff could identify which file/folder changes relate to the attack and pivot from FileVantage directly to CrowdStrike's Threat Intelligence console. This data allows your teams to move fast, pinpointing the adversary activity within your environments, allowing for quick prioritization of remediation efforts around the affected files.

REDUCE ALERT FATIGUE AND INCREASE MONITORING EFFICIENCY

Security operations staff often have only a limited number of hours each week to review all essential files and system changes. However, when that's applied at scale, it can become nearly impossible to monitor what's necessary without alert fatigue.

Falcon FileVantage changes that with real-time monitoring and custom file policies to monitor critical operating system files. With Falcon FileVantage, staff can oversee all file and system changes with both summary and detailed dashboards. This allows staff to seamlessly improve overall security posture while reducing alert fatigue. They can focus on analyzing relevant data in real time. This unique FIM solution increases your team's efficiency by:

- Utilizing predefined policies and workflows to reduce alert fatigue, cutting down on event volume
- Creating new and customized policies based on your organization's specific needs
- Setting a severity rating for each policy you establish
- Controlling false alarms with enable/disable functionality

CONSOLIDATE SOLUTIONS: REDUCE COSTS AND SOLUTION STACK

File monitoring should not cost an arm and leg in solution sets, eat into valuable productivity time and create even more work for your team. Falcon FileVantage allows you to simplify your solution stack while reducing operational costs. By integrating this solution, your team can streamline monitoring processes — eliminating redundant tools, improving alert monitoring and gaining valuable data around other detection data to quickly cross-reference changes occurring in your environments.

*Falcon FileVantage requires CrowdStrike Falcon Insight™.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.