CAPSULE8

Capsule8 Protect for File Integrity Monitoring

Solution Brief

File Integrity Monitoring with Compliance and Security Built-in

File integrity monitoring (FIM) is an important tool for you to monitor changes to critical systems, configuration and content files within your enterprise. To understand changes, the system gives you the current state compared with a previous trusted version. Most FIM solutions are limited to ensuring compliance. But compliance is only one aspect of protecting a company's infrastructure.

Most FIM Solutions Lack Critical Security Capabilities, Until Now

Capsule8 Protect—designed with security in mind—takes care of all the compliance issues your current FIM solution handles and adds key security capabilities. That's because it was designed from the ground up with security in mind.

All-in-one Compliance and Security that Works Right Out of the Box

POLICIES

Capsule8 Protect delivers out-of-the-box policies that immediately protect standard core Linux components like inappropriate program execution, file monitoring, traditional indicators of compromise, and overall indicators of attack.

ALERTS

Alerts contain the context of the triggering event. This information not only reduces false positives but can help craft business-specific policies for monitoring and alerting on even the most restricted and proprietary Linux systems.

Capsule8 Protect includes everything you need to meet compliance *and* help secure your production Linux

THE RIGHT RESPONSES

In real time, an operator can launch custom responses to specific file events or actions. If there's a problem, Capsule8 Protect sends a high, medium or low-risk alert. Based on your configuration, you can trigger stop, kill, quarantine, or delete responses.

BUILT FOR LINUX

Out of the box, Capsule8 Protect monitors your Linux systems for changes to file permissions, file attributes, file or directory security settings, and security settings. It also monitors the creation or removal of files or directories and tracks the details on file actions, including the user and process responsible for the action.

BUILT-IN COMPLIANCE

Regulatory requirements for monitoring and logging file events can happen on your Linux components. Capsule8 Protect enables the storing of FIM telemetry in standard logging stacks regardless of archival, reporting, and data retention needs.

SMART SECURITY STRATEGIES

Capsule8 Protect includes more than just logging and monitoring. It prompts you on response actions you can take on FIM telemetry. Plus, it takes the telemetry into account when identifying indicators of attack, which prevents unwanted actions. To keep monitoring simple, you can display FIM alerts on your Capsule8 console or existing tools.

Click Here to Request a Demo of Capsule8 Protect for FIM

CAPSULE8

About Capsule8

Founded in fall 2016 and headquartered in Brooklyn, NY, Capsule8 is the only company providing high-performance attack protection for Linux production environments—whether containerized, virtualized, or bare metal. Capsule8 frees-up SecOps teams, while being safe for even the busiest workloads, on the busiest networks. Founded by experienced hackers and seasoned security entrepreneurs, and funded by Bessemer Venture Partners and ClearSky, Capsule8 is making it possible for Linux-powered enterprises to modernize without compromise.

Learn more at www.Capsule8.com.