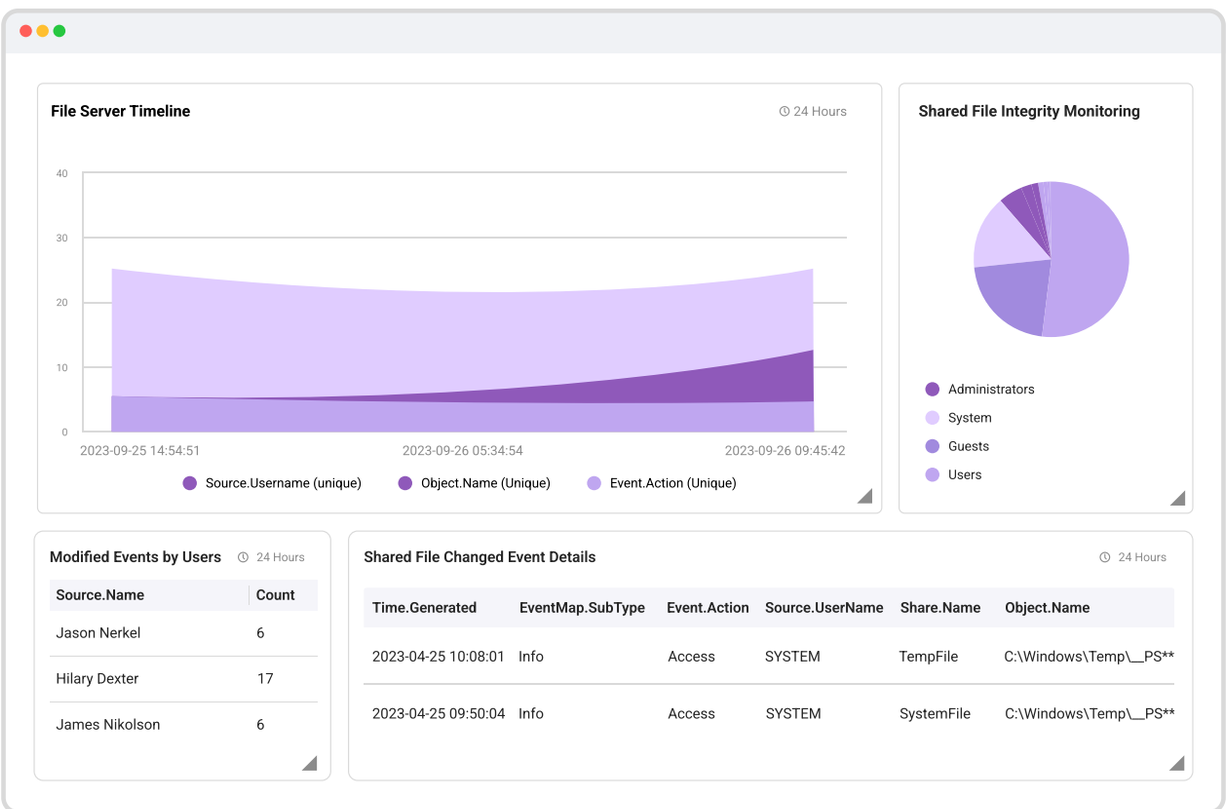
File Integrity Monitoring with Logsign USO Platform

Discover the power of Logsign's File Integrity Monitoring (FIM) capability - a critical pillar in today's cybersecurity landscape. With the ever-growing threats to data integrity, FIM emerges as a safeguard, providing tailored extraction and analysis of specific data patterns. This datasheet unveils how Logsign USO Platform ensures, thanks to its FIM function, precision in identifying security threats, allowing proactive action to protect your digital assets. Explore how our solution transforms the way you secure your crucial files and maintain compliance.

Protecting Data Integrity with Logsign USO Platform's FIM Capability

Experience excellent and constant data security with Logsign's File Integrity Monitoring (FIM) capabilities. In the ever-evolving and -growing landscape of cybersecurity, maintaining the integrity of your critical files and systems is paramount.

Logsign USO Platform empowers organizations through File Integrity Monitoring to detect and respond to security incidents swiftly by monitoring changes and modifications across files, folders, and operating systems. Thanks to our FIM capability, unauthorized alterations are promptly identified, insider threats are mitigated, and compliance requirements are seamlessly met. Discover how Logsign's FIM capability can fortify your cybersecurity defenses and keep your digital assets secure.



Detect and Respond with Precision:

→ **Incident Detection:** Logsign USO Platform becomes your vigilant eye through FIM, identifying security breaches like malware infections, unauthorized access, insider threats, and configuration errors.

→ **Real-time Monitoring:** Stay in the know with instant alerts whenever file integrity threats arise. Our platform ensures you catch early signs, empowering swift responses before threats escalate.

→ **Unauthorized Changes:** Logsign USO Platform monitors critical files and directories, flagging unauthorized or malicious alterations caused by malware or insiders. Detect changes to system files, applications, and configurations with precision.

→ **Insider Threats:** Guard against risks from within. The platform spotlights changes made by users or authorized individuals, preventing accidental or malicious alterations that could jeopardize your data.

→ **Forensic Insights:** Delve into historical records of file changes for incident analysis. Uncover the who, what, when, where, and why of alterations to understand the full impact.

Assure Compliance and Strengthen Security:

→ **Data Breach Prevention:** Shield critical data from unauthorized access or interference. Prevent breaches that compromise the confidentiality of user information.

→ **Regulatory Compliance:** Meet industry standards and regulations like PCI DSS and HIPAA by implementing FIM. Our compliance features help you avoid penalties and maintain your reputation.

→ **Comprehensive Auditing:** Gain a complete audit trail for every change. Logsign USO Platform provides real-time answers to crucial questions, ensuring you know what changed, when, where, who, and whether the change was authorized.

Enhance Reporting and Control:

→ **Customized Reports:** Logsign USO Platform crafts tailored reports with pinpoint precision, capturing every integrity detail. These comprehensive reports can be generated in formats like PDF or CSV.

→ **Automated Scheduling:** Stay organized effortlessly with automatic report scheduling. Receive reports at regular intervals, ensuring you're always up-to-date.

Logsign USO Platform's FIM capability is your partner in securing your digital landscape, empowering you to safeguard data, respond swiftly, and maintain compliance with the ever-evolving cybersecurity landscape.