uptycs

Datasheet

Uptycs File Integrity Monitoring

A highly scalable way to streamline complex file monitoring, gain greater visibility on how files are being accessed, and help teams focus on the file changes that matter.

Understanding which files are accessed within your cloud, on-premises, and laptop infrastructure, as well as by whom, constitutes a crucial aspect of any mature security and compliance program. However, attaining the necessary visibility can pose challenges, especially when managing a hybrid infrastructure encompassing both cloud and on-premises systems across macOS, Linux, and Windows.

Scaling to millions of hosts, Uptycs File Integrity Monitoring (FIM) provides a robust method to identify and reconcile changes made to business-critical files. From a centralized console, Uptycs can pinpoint which user and process were responsible for the file access. If a file has been created or updated, the Uptycs Sensor will scan the file with a set of YARA rules that inspect the contents for malware signatures. Files requiring forensic investigation can be downloaded to an analyst's laptop to simplify and expedite the investigation.

Uptycs empowers security teams to integrate FIM with other components of their security and compliance program, thereby reducing the need for multiple point solutions and minimizing overhead. With Uptycs FIM and compliance reporting, not only can you ensure compliance with regulations, but you have evidence for external auditors and internal stakeholders.

Benefits:

- Streamline monitoring with a centralized console rather than using multiple products
- Attain comprehensive visibility across Windows, macOS, Linux, VMs, and cloud instances
- Speed up investigations with context-rich alerting, real-time querying, and historical forensics and reporting
- Demonstrate compliance through evidence-based reporting
- Scan changed files with YARA rules to detect malware drops
- Download FIM impacted files for forensic investigation

> "Uptycs simplifies investigations and saves time—about a 30% time savings per investigation. The additional context Uptycs delivers gives our security operations team a high degree of confidence that we're doing all we can to safeguard our workstations and our business."
>
> – **Sean McElroy**, Chief Security Officer, Lumin Digital

Uptycs provides comprehensive file integrity monitoring that scales across millions of hosts, offering capabilities such as real-time alerting, deep forensic insights, customizable monitoring and reporting, and precision controls.

Alerting and investigation

Real-time alerting: Continuous tracking of modifications made to your monitored files with context including machine name, username, process, host IP, file path modified, type of access, and more.

Alert forwarding: Forward notifications to Slack, Pagerduty, email, and other tools to fit into your existing remediation workflows.

Malware scanning: Scan modified files with YARA rules.

Download: Download modified files for further investigation.

Deep insights: Using over 200 system tables, Uptycs provides detailed insight into user login activity, open sockets, processes triggered, the user account that modified a given file, and other context-rich insights.

Investigative query: Incident investigators can query data across thousands of endpoints in real time, gaining instant insight on suspicious activity.

Forensics: Analyze historical data, recreating an asset at a given point in time to reveal exactly what happened to critical files, and how the incident occurred.

Monitoring and reporting

Customized monitoring: Tailor file integrity monitoring based on the unique needs of different environments. For example, develop rules to rapidly investigate external file changes in one environment while focusing on unapproved software changes in another.

Out-of-the-box alerting: Alert immediately when FIM activity is detected.

Out-of-the-box policies: Choose from existing file management alerts built around macOS, Linux and Windows operating systems or create customized rules to manage hybrid cloud environments.

Flexible policies: Ability to define FIM policies to monitor only certain folders, sub folders, file extensions while allowing the user the ability to skip certain folders or file paths. Optionally read-only activity monitoring can also be enabled for certain sensitive files. Ability to exclude FIM activity by trusted processes.

Evidence-based reporting: Report against historical file activity, providing evidence of routine file security monitoring to demonstrate compliance with the Payment Card Industry Security Standard (PCI), and other industry data regulations.

Out-of-the-box reporting: Ready-made reporting capabilities including tracking file events per day, top file event generators, and total alert instances to demonstrate compliance.

Precision and performance

Flexible controls: Select specific files and systems to monitor.

Optimized performance: Monitoring file changes at the OS level instead of analyzing every directory.

Deployment scale: The Uptycs Sensor collects data, normalizes it, and streams it to an SQL-powered data lake, enabling the system to monitor file activity across thousands of machines in real time and through a historical activity archive.

Demonstrate compliance with industry data regulations and best practices.

About Uptycs

Uptycs helps drive DevSecOps excellence, bringing teams together to master threat operations, meet compliance mandates, and reduce risk across clouds, containers, and endpoints. Take back control of your security data, get the correlated insights you care about most, and take decisive action.

Shift up your cybersecurity with Uptycs. Learn how at: Uptycs.com

uptycs